НАУЧНЫЙ ЖУРНАЛ

ТЕЛЕКОММУНИКАЦИИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

№2-2018

(*Дата издания:* декабрь *2018 г.*)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Орлов Владимир Георгиевич (Главный редактор) к.т.н., начальник отдела организации научно-исследовательской работы студентов Московского технического университета связи и информатики (МТУСИ), начальник Центра научной работы и технического творчества молодёжи МТУСИ, Москва, Россия

Андреев Владимир Александрович д.т.н., профессор, Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Бачевский Сергей Викторович д.т.н., профессор, ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. Бонч-Бруевича, Санкт-Петербург, Россия

Зимин Игорь Викторович Кыргызский государственный технический университет имени И.Раззакова. Институт электроники и телекоммуникаций, Бишкек, Кыргызстан

Ланчиков Павел Николаевич НП Учебный центр Huawei (Москва), Шеньчжень, Китай

Маркосян Мгер Вардкесович к.т.н., доцент, Ереванский НИИ средств связи, Ереван, Армения

Прохода Александр Николаевич к.воен.н., доцент, Балтийский военно-морской институт им. Ф.Ф. Ушакова, Калининград, Россия

Рябко Борис Яковлевич д.т.н., профессор, ректор Сибирского государственного университета телекоммуникаций и информатики, Новосибирск, Россия

Самойлов Александр Георгиевич д.т.н., профессор, заместитель директора института информационных технологий и радиоэлектроники Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Владимир, Россия

Рогачев Александр Александрович д.т.н., в.н.с., Гомельский государственный университет имени Франциска Скорины, Гомель, Республика Беларусь

Суржиков Анатолий Петрович д.ф.-м.н., профессор, Национальный исследовательский Томский политехнический университет, Томск, Россия

Титов Евгений Вадимович к.т.н., профессор, Московский технический университет связи и информатики, Москва, Россия

УЧРЕДИТЕЛЬ:

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ» (МТУСИ)

РЕДАКЦИОННАЯ ПОДГОТОВКА:

Отдел организации научно-исследовательской работы студентов (ОНИРС МТУСИ)

СОДЕРЖАНИЕ

«Цифровые технологии радиосвязи и телерадиовещания»

«Сетевые технологии и системы телекоммуникаций»

«Информационные технологии и автоматизация процессов в системах связи»

СИНТЕЗ ФИЛЬТРА КАУЭРА И РАСЧЕТ ЕГО ХАРАКТЕРИСТИК

Мирошниченко Антон Валерьевич
студент группы М61801 МТУСИ
Mirosh.A.V@yandex.ru
Волчков Валерий Павлович
МТУСИ, д.т.н., профессор кафедры ОТС
volchkovvalery@mail.ru

Ключевые слова: *амплитудно-частотная характеристика, фаза-частотная характеристика, комплексный коэффициент передачи, импульсная характеристика, фильтр Кауэра, фильтр Золотарёва, эллиптический фильтр, синтез фильтра.*

Для ряда специальных задач связи и радиолокации синтез фильтров фиксированного порядка с максимально возможной крутизной ската АЧХ и заданным уровнем пульсаций имеет первостепенное значение. Такой критерий оптимальности реализуется в фильтрах Кауэра, теоретический синтез и анализ которых весьма сложен из-за использования эллиптических функций. В работе приводятся математическая формализация всех этапов синтеза фильтра Кауэра, включающая расчет его нулей, полюсов, а также вывод аналитических выражений для импульсной и частотной характеристик.

Один из важнейших методов синтеза цифровых фильтров основан на дискретной аппроксимации известных аналоговых фильтров-прототипов, среди которых особое место занимают фильтры Кауэра, часто именуемые эллиптическими БИХ фильтрами. Эти фильтры позволяют при высокой добротности получить наиболее сильное подавление в полосе задержания среди всех известных на данный момент аналоговых БИХ фильтров. В тоже время, это наиболее сложный фильтр, как с точки зрения теоретического описания, так и последующего синтеза/анализа. Хотя технологический скачек в виде быстродействующих АЦП позволил во многих случаях отказаться от подобных фильтров в пользу КИХ фильтров высокого порядка, но до сих пор существуют области радиотехники, где применение аналоговых и цифровых фильтров Кауэра не теряет своей актуальности.

Интерес к фильтрам Кауэра последнее время возрос и по другим обстоятельствам. Этот фильтр был разработан в середине 20 века и с тех пор развитие теоретической базы по данному фильтру была прекращена. В результате практически отсутствуют современные источники, позволяющие получить подробную информацию по синтезу данного фильтра. Поэтому современный инженер вынужден пользоваться очень ограниченным набором готовых решений, позволяющих синтезировать фильтр Кауэра, но не позволяющий провести аналитику или точный синтез фильтра под требуемые условия. Следует отметить два источника [1, 2], где наиболее полно рассмотрены эллиптические функции и синтез фильтра Кауэра. Однако при получении формул и выводе аналитических выражений в предыдущих своих работах [3, 4] авторы указали на ряд трудностей, связанных с решением уравнений, содержащих неявные функции, которые могут поставить в затруднение разработчика радиоэлектронного оборудования.

В данной работе показано, как можно преодолеть эти трудности, приводятся математическая формализация всех этапов синтеза фильтра Кауэра, расчет его нулей, полюсов, а также вывод аналитических выражений для импульсной и частотной характеристик. Последнее оказывается очень важным для задач, связанных с синтезом и моделированием радиолокационных приемников [5, 6] и оптимальных канальных прекодеров [7 - 14].

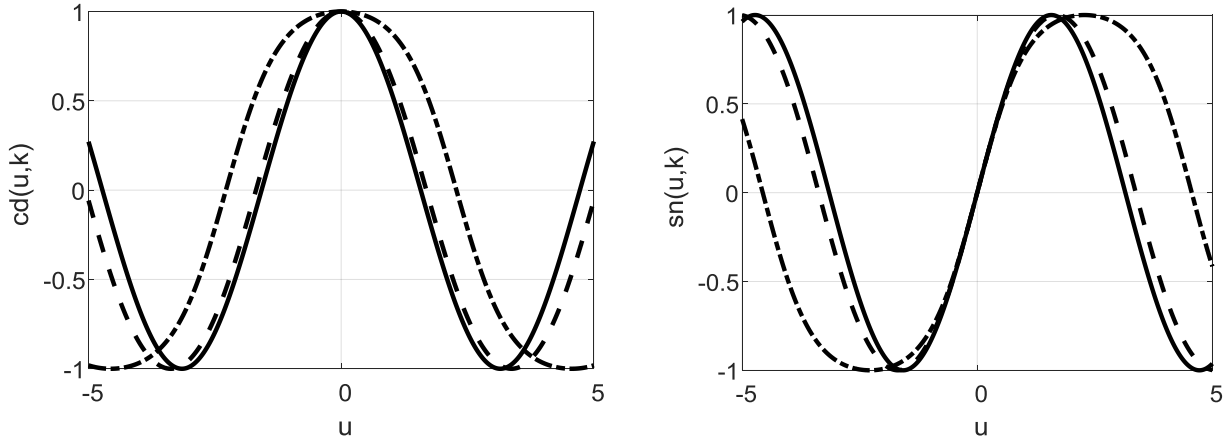
Синтез фильтра Кауэра

Квадрат модуля комплексного коэффициента передачи фильтра Кауэра описывается выражением

$$\left|H(j\omega)\right|^2 = \frac{1}{1+\varepsilon_p^2 R_n^2(\omega)}, \qquad (1)$$

где $R_n(\omega) = cd(n \cdot arccd(\omega,k),k)$, cd и $arccd$ - эллиптические функции Якоби [2,4].

Отметим, что при синтезе и анализе фильтров Каура часто используются эллиптические функции $cd(x,y)$, $arccd(x,y)$, $K(x)$ и другие, описания и свойства которых представляют самостоятельный интерес. Однако в виду ограниченного размера данной статьи, авторы вынуждены отослать читателя к [2, 4], где приведена полная теоретическая база по эллиптическим функциям и описан их расчет. Здесь лишь приведем графики функций $cd(u,k)$ и $sn(u,k)$ при различных значениях k (см. рисунок 1), которые демонстрируют, что данные функции являются чем то «средним» между тригонометрическими и гиперболическими функциями. При $k \to 0$ эллиптические функции вырождаются в тригонометрические, а при $k \to 1$ в гиперболические.



А Б

Рис. 1. А - График функции $cd(u,k)$, Б - График функции $sn(u,k)$. $k = 0.1$ – сплошная линия, $k = 0.5$ - штриховая линия, $k = 0.9$ – штрихпунктирная линия

Для синтеза фильтра Кауэра необходимы следующие исходные параметры (см. рисунок 2): $\omega_в$ - верхняя частота переходной полосы; R_p - максимальное ослабление в полосе пропускания в дБ; R_s - минимальное ослабление в полосе задерживания в дБ.

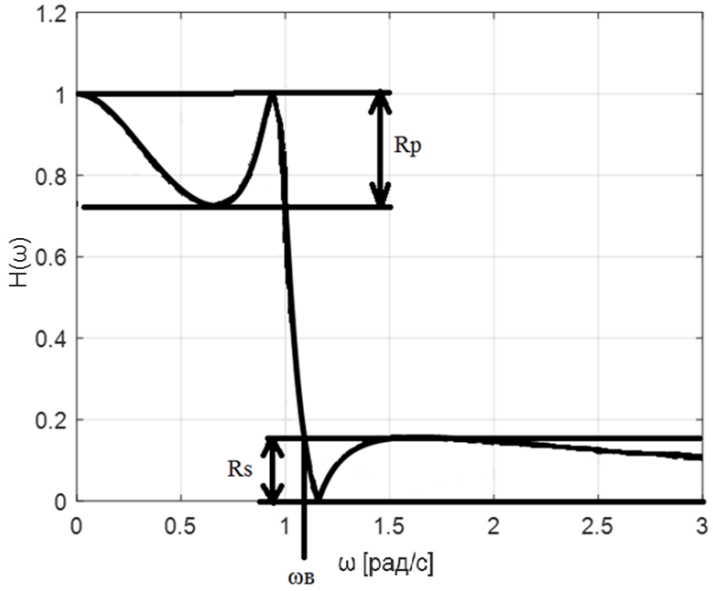


Рис. 2. Исходные параметры для синтеза фильтр Кауэра

Отметим, что $\omega_н$ - нижняя частота переходной полосы в расчете участие не принимает и зафиксирована на значении 1.

После выбора исходных параметров, необходимо рассчитать два вспомогательных параметра

$$\varepsilon_p = \sqrt{10^{R_p/10} - 1},\ \varepsilon_s = \sqrt{10^{R_s/10} - 1}.$$

Первым и самым важным этапом синтеза любого фильтра является выбор его порядка, но уже на этом этапе начинаются трудности. Обязательное условие адекватности фильтра Кауэра предполагает выполнение соотношения [1]

$$n\frac{K\left(\sqrt{1-k^2}\right)}{K(k)} = \frac{K\left(\sqrt{1-\left(\frac{\varepsilon_p}{\varepsilon_s}\right)^2}\right)}{K\left(\frac{\varepsilon_p}{\varepsilon_s}\right)}, \qquad (2)$$

где n - порядок фильтра, k - параметр эллиптических функций, $K(x)$ - полный эллиптический интеграл. Поэтому, расчет порядка фильтра Кауэра состоит из двух шагов.

1.. Принимаем $k = \frac{\omega_н}{\omega_в}$ и рассчитываем минимальный порядок фильтра n по формуле

$$n \geq \frac{K\left(\sqrt{1-\left(\frac{\varepsilon_p}{\varepsilon_s}\right)^2}\right)K(k)}{K\left(\frac{\varepsilon_p}{\varepsilon_s}\right)K\left(\sqrt{1-k^2}\right)}.$$

2. Пересчитываем параметр k так, что бы он удовлетворял выражению (2). Для упрощения расчета мы приведем график функции $y(k) = K\left(\sqrt{1-k^2}\right)\Big/K(k)$ (см. рисунок 3), который позволит проводить примерный графический расчет, однако для точного расчета необходимо прибегать к численным методам [4].

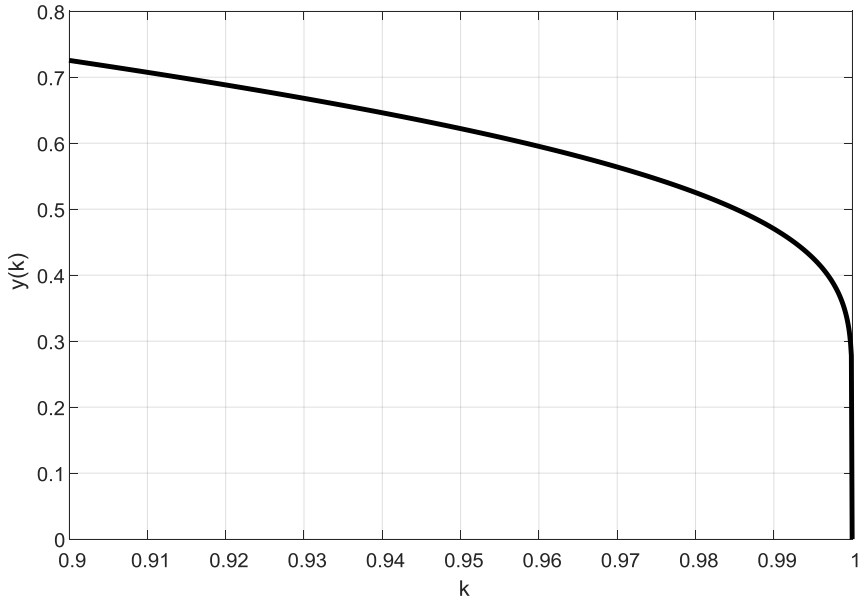


Рис. 3. Зависимость y(k) на участке $k \in [0.9,...,1]$

Сложность аналитики фильтра Кауэра заключается в особенностях выражения (2) для нахождения порядка фильтра n. Выбор порядка любого классического фильтра (Баттерворта,

Чебышева, Бесселя) можно представить как функцию одной переменной $R_s = f(n)$, где n - порядок фильтра, R_s - минимальное ослабление в полосе задерживания, на границе этой полосы $\omega_в = const$ (см. рисунок 1). Для фильтра Кауэра формула принимает несколько другой вид $(R_s, \omega_в) = f(n,k)$, т.е. R_s и $\omega_в$ зависят от двух переменных n и k. Действительно, параметры n и k связанны жестким соотношением (2), где n - может принимать только целые положительные значения. Но тогда параметр k тоже будет дискретным и определяется, как некоторая неявная функция $k = \varphi(n, \varepsilon_p, \varepsilon_s)$. Причем поскольку $\omega_в$ зависит от параметра k через соотношение $k = \omega_н / \omega_в$, изменение порядка фильтра n влечет изменение параметра k, а значит и изменяет границу полосы задерживания $\omega_в$.

Отметим, что, если параметр k равен 0, то эллиптические функции вырождаются в тригонометрические, а фильтра Кауэра превращается в фильтр Чебышева 1-го рода, с передаточной характеристикой вида.

$$\left|H(j\omega)\right|^2 = \frac{1}{1+\varepsilon_p^2 cd^2(n \cdot arccd(\omega,k),k)}\Bigg|k=0 = \frac{1}{1+\varepsilon_p^2 \cos^2(n \cdot \arccos(\omega))}.$$

У такого фильтра Чебышева максимальное ослабление в полосе пропускания совпадает с аналогичным ослаблением у исходного фильтра Кауэра. В то же время, граница полосы задерживания $\omega_в$ и максимальное ослабление в полосе задерживания R_s у фильтра Чебышева 1-го рода будут хуже, чем у фильтра Кауэра.

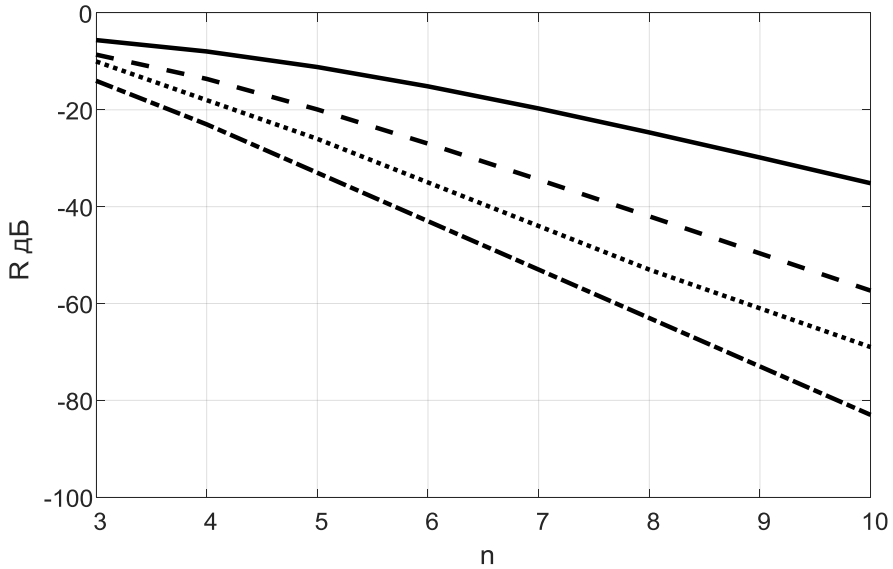


Рис. 4. Зависимость максимального ослабления R_s от порядка фильтра, при $R_p = 1.5 дБ$. Сплошная линия – фильтр Чебышева 1-го рода при $\omega_н / \omega_в = 0.95$, штриховая линия – фильтр Чебышева 1-го рода при $\omega_н / \omega_в = 0.9$, пунктирная линия – фильтр Кауэра при $\omega_н / \omega_в = 0.95$, штрих-пунктирная линия – фильтр Кауэра при $\omega_н / \omega_в = 0.9$.

Анализируя рисунок 4, можно установить, что в случае $\omega_н / \omega_в = 0.95$ при замене фильтра Чебышева 1-го рода 4-го порядка фильтром Кауэра 4-го порядка мы получаем выигрыш в 10 дБ, а для 8-го порядка выигрыш уже составляет 28 дБ. Так же рисунок 4 показывает, что фильтр Чебышева 8-го порядка вносит такое же ослабление, как фильтр Кауэра 5-го порядка, т.е. переход к фильтру Кауэра позволяет уменьшить порядок фильтра с 8-го до 5-го.

Таким образом, чем больше порядок заменяемого фильтра, тем больше будет выигрыш как в затухании, так и в снижении порядка фильтра.

Нахождение нулей и полюсов фильтра Кауэра

Нахождение нулей и полюсов эллиптического фильтра мало чем отличается от нахождения нулей и полюсов других фильтров, описанных в [3]. Требуется найти такие значения числителя и знаменателя дроби (1), при которых она превращается в ноль или бесконечность.

Говоря математическим языком, для нахождения нулей требуется решить уравнение

$$\lim_{s\to q_i}\left(1+\varepsilon_p^2 cd^2(n\cdot arccd(-js,k),k)\right)=\pm\infty,$$

а для нахождения полюсов

$$\lim_{s\to p_i}\left(1+\varepsilon_p^2 cd^2(n\cdot arccd(-js,k),k)\right)=0.$$

Решая данные уравнения, получим формулы для нахождения нулей и полюсов фильтра Кауэра.

$$q_l=\pm\frac{cd\left(\frac{a}{n}K(k)+jK\left(\sqrt{1-k^2}\right),k\right)}{j}, \tag{3}$$

где $a=\frac{2l-1}{n}$, $l=1,\ 2,\ldots,m$; $m=\left\lfloor\frac{n}{2}\right\rfloor$, $\lfloor\ \rfloor$ – *оператор округления вниз.*

$$p_l=jcd\left(\left(\left(1-\frac{arcsn\left(\frac{j}{\varepsilon_p}K\left(\sqrt{1-k^2}\right),\sqrt{1-k^2}\right)}{K\left(\sqrt{1-k^2}\right)}\right)K(k)+2lK(k)\right)\cdot\frac{1}{n},k\right), \tag{4}$$

где $l=1,\ \ldots,2n$.

Для физической реализуемости фильтра следует отбросить все полюса, лежащие в правой полуплоскости.

Нахождение АЧХ, ФЧХ, ИХ фильтра Кауэра

Зная нули и полюсы фильтра, можно представить комплексный коэффициент передачи в виде дробно рациональной функции.

$$H(j\omega)=\frac{(j\omega-q_1)(j\omega-q_2)\ldots(j\omega-q_m)}{(j\omega-p_1)(j\omega-p_2)\ldots(j\omega-p_l)}, \tag{5}$$

где m - количество нулей фильтра, l - количество полюсов фильтра, p_k - k-ый полюс фильтра, q_k - k-ый ноль фильтра. Тогда амплитудно-частотную характеристику и фаза-частотную характеристику можно представить в виде

$$H(\omega)=\left|H(j\omega)\right| \tag{6}$$

$$\Phi(\omega)=\arg\left(H(j\omega)\right), \tag{7}$$

где $\arg\left(H(j\omega)\right)\in(-\infty,\infty)$ - угловой аргумент комплексной функции $H(j\omega)$ с устраненными скачками фазы на 2π.

Подробный алгоритм расчета импульсной характеристики был приведен в работе [3]. Импульсная характеристика любого фильтра может быть представлена в виде

$$h(t)=\sum_{k=1}^{l}g_k e^{p_k t},\qquad g_k=\frac{(p_k-q_1)(p_k-q_2)\ldots(p_k-q_m)}{(p_k-p_1)\ldots(p_k-p_{k-1})(p_k-p_{k+1})\ldots(p_k-p_l)}, \tag{8}$$

где m - количество нулей фильтра, l - количество полюсов фильтра, p_k - k-ый полюс фильтра, q_k - k-ый ноль фильтра. Несложно убедится, что импульсную характеристику (8) можно привести к двум другим формам синус-косинусной и косинусной.

Синус-косинусная форма задается как

$$h(t)=h_0+\sum_{k=1}^{\lfloor l/2\rfloor}2e^{\sigma_k t}\Re(g_k)\cos(\omega_k t)-2e^{\sigma_k t}\Im(g_k)\sin(\omega_k t),$$

где $\sigma_k = \Re(g_k)$, $\omega_k = \Im(g_k)$, l - количество полюсов фильтра, h_0 добавочный член в случае наличия комплексно несопряженного полюса p_r (в случае когда l нечетно).

$$h_0 = \begin{cases} g_r e^{p_r t}, & l - нечетно \\ 0, & l - четно \end{cases}.$$

Косинусная форма задается как

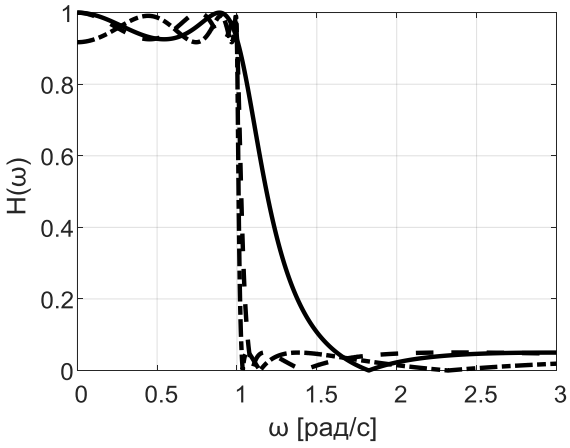
$$h(t) = h_0 + \sum_{k=1}^{\lfloor l/2 \rfloor} A_k \cos(\omega_k t + \phi_k),$$

где $A_k = \pm 2e^{\sigma_k t}\sqrt{\Re(g_k)^2 + \Im(g_k)^2}$, знак должен совпадать со знаком величины $\Re(g_k)$, $\phi_k = -arctg\left(\Im(g_k)/\Re(g_k)\right)$, $\omega_k = \Im(g_k)$, l - количество полюсов фильтра, h_0 добавочный член в случае наличия комплексно несопряженного полюса p_r.

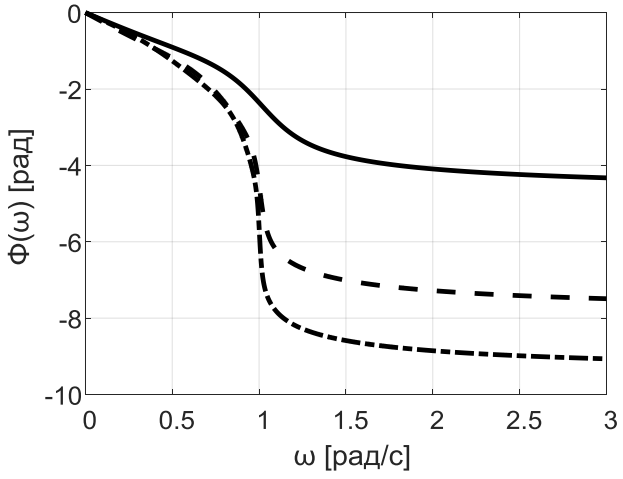
На рисунке 5 в качестве примера представлены АЧХ, ФЧХ и ИХ для 3-х фильтров Кауэра различного порядка, с параметрами, представленными в таблице на рисунке 5А, и рассчитанные по изложенной в статье методике с использованием формул (3)-(8).

n	$\omega_н$ $рад/с$	$\omega_в$ $рад/с$	R_p $дБ$	R_s $дБ$
3	1	1.625	1.5	30
4	1	1.077	1.5	30
5	1	1.029	1.5	30

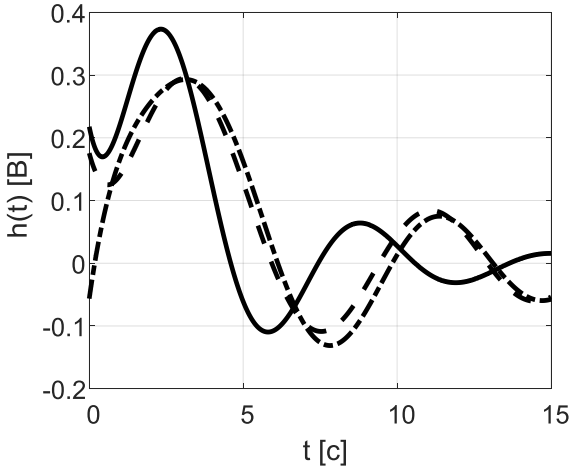
А



Б



В



Г

Рис. 5. Характеристики синтезированных фильтров Кауэра: А – параметры синтезированных фильтров, Б – амплитудно-частотная характеристика, В – фаза-частотная характеристика с устраненным скачками на 2π, Г – импульсная характеристика. Сплошная линия – фильтр 3-го порядка, штриховая – фильтр 4-го порядка, штрихпунктирная – фильтр 5-го порядка.

Выводы

1. Синтез фильтров Кауэра связан с вычислением эллиптических функций, которые требуют применения численных методов. Однако, применение фильтров Кауэра позволяет получить более сильное внеполосное затухание при фиксированном порядке фильтра, или существенно снизить порядок фильтра, при неизменном затухании. Причем, чем большего порядка был заменяемый фильтр, тем больший выигрыш будет получен при замене.

2. В отличии от других классических фильтров, выбор порядка фильтра Кауэра сводится к вычислению сложной неявной функцией от нескольких переменных и требует особого подхода, связанного с перерасчетом дополнительного параметра k. В частном случае, при k=0, фильтр Кауэра вырождается в фильтр Чебышева 1-го рода. Это позволяет унифицировать алгоритмы синтеза фильтров Кауэра и Чебышева 1-го рода.

3. Приведенные выражения могут быть использованы для разработки специального программного обеспечения, позволяющего производить синтез фильтров для радиолокационных приемников и оптимальных канальных прекодеров.

Литература

1. *Parks T.W., Burrus C.S.* Digital Filter Design. New York: John Wiley & Sont, Inc., 1987. -360с.
2. *Абрамовиц М., Стиган И., Липман Д., Мак Ниш А*. и д.р. Справочник по специальным функциям с формулами, графиками и математическими таблицами. Под ред. Абрамовиц М., Стиган И. Москва: Наука, 1979. -832.
3. *Мирошниченко А.В.* Обобщенный метод вывода канонических форм импульсных характеристик аналоговых фильтров // Фундаментальные проблемы радиоэлектронного приборостроения. -2017. Т. 17. № 4. –с.1194-1197.
4. *Волчков В.П., Мирошниченко А.В.,* Вычисление эллиптических функций Якоби для расчета характеристик фильтра Кауэра // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2018. Т. 45. № 2. -с.298-311.
5. Вопросы подповерхностной радиолокации / Под ред. А.Ю. Гринева. М: Радиотехника, 2005. – 416 с.
6. Вопросы перспективной радиолокации / Под ред. А.В. Соколова. М: Радиотехника, 2003. – 512
7. *Волчков В.П., Санников В.Г.* Синтез оптимальных предыскаженных финитных сигналов на основе желаемого эталона // Электросвязь, №5, май, 2018, с. 80-84.
8. *Волчков В.П., Санников В.Г.* Синтез оптимальных канальных прекодеров с весовым окном // Системы синхронизации, формирования и обработки сигналов. 2016. Т. 7. № 1. С. 19-21.
9. *Санников В.Г., Алёшинцев А.В.* Синтез финитных сигналов, согласованных с характеристиками фильтра Баттерворта, по критерию максимума среднего значения его отклика // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 4. С. 477-481.
10. *Волчков В.П., Санников В.Г.* Синтез канальных прекодеров для систем связи с финитным сигнальным базисом // Системы синхронизации, формирования и обработки сигналов. 2015. Т. 6. № 3. С. 152-154.
11. *Волчков В.П., Санников В.Г.* Синтез предыскаженных финитных сигнальных базисов для борьбы с межсимвольной интерференцией // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 3. С. 28-30.
12. *Санников В.Г., Алёшинцев А.В.* Математическое моделирование многочастотного модема с повышенной помехоустойчивостью // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 52-58.
13. *Волчков В.П., Уваров С.С.* Аппроксимация узкополосных случайных процессов с помощью комплексной рекурентной М-модели скользящего окна второго порядка // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 3. С. 54-61.
14. Безруков И.М., Волчков В.П. Исследование помехоустойчивости цифровой системы связи с канальным прекодером и финитной посимвольной передачей // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 146-150.

SYNTHESIS OF CAUER FILTERAND CALCULATION OF ITS CHARACTERISTICS

Anton V. Miroshnichenko
Student of group M61801, MTUCI
Mirosh.A.V@yandex.ru
Valery P. Volchkov
MTUCI, Doctor of Science., professor of General Communication Theory
volchkovvalery@mail.ru

Keywords: *amplitude-frequency characteristic, phase-frequency characteristic, complex transfer coefficient, impulse characteristic, Cauer filter, Zolotarev filter, Elliptic filter, filter synthesis.*

For a number of special communication and radar tasks, the synthesis of filters of a fixed order with the highest possible slope of the frequency response and a given level of pulsations is of paramount importance. Such an optimality criterion is implemented in Cauer's filters, the theoretical synthesis and analysis of which is very complex and associated with elliptic functions. The paper presents a mathematical formalization of all stages of the synthesis of the Cauer filter, including the calculation of its zeros, poles, as well as the derivation of analytical expressions for the impulse and frequency response.

РАЗРАБОТКА БАЗЫ ЗНАНИЙ КАСКАДОВ ПРИНЦИПИАЛЬНЫХ СХЕМ РАДИОТЕХНИЧЕСКИХ УСТРОЙСТВ В ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ ЭКСПЕРТНОЙ СИСТЕМЕ

Балашов Виталий Олегович
студент группы МИТ1702 МТУСИ
balash1996@list.ru
Долин Георгий Аркадьевич
МТУСИ, к.т.н., доцент кафедры РОС
dolin1974@gmail.com

Ключевые слова*: радиотехнические устройства, РТУ, экспертная система, ЭС, САПР, синтез, проектирование, система, БЗ, база знаний, каскад, принципиальная схема, структурная схема*

Развитие систем и устройств связи требует полной автоматизации процесса их проектирования для быстрого обновления РТУ. В статье описывается алгоритм работы сквозной САПР РТУ, включающий гибридную продукционную и объектно-ориентированную экспертные системы для синтеза структурных и принципиальных электрических схем РТУ, моделирование методами узловых потенциалов и переменных состояния и распределенную динамическую базу данных параметров электронных компонентов.

База знаний (БЗ) объектно-ориентированной экспертной системы (ЭС) структурирована так, чтобы обеспечивать быстроту проектирования и легкость модификации [2]. В качестве основной структуры представления моделей принципиальных схем узлов и каскадов радиотехнических устройств (РТУ) выбрана иерархическая структура, в которой движение вниз по иерархии подразумевает введение методов определяющих значения дополнительных компонентов принципиальной схемы РТУ, т.е. специализацию функционирования элементов РТУ (компоненты РТУ – потомки в иерархической структуре наследуют характерные свойства или особенности компонентов РТУ более низкой иерархии (предков) и затем их детально раскрывают).

Для иллюстрации формирования знаний в БЗ объектно-ориентированной ЭС рассмотрим описание базовых электронных компонентов РТУ [1, 6].

«Сопротивление» резистора может быть фиксированным при комнатной температуре. Текущее состояние характеристик устройства определяется температурой окружающей среды. Оно может изменяться при ее увеличении или уменьшении. Такой объект описывается в БЗ следующим образом:

ОБЪЕКТ РЕЗИСТОР:
ВНУТРЕННЯЯ ПЕРЕМЕННАЯ Сопротивление,
МЕТОД Увеличить (ВНЕШНЯЯ ПЕРЕМЕННАЯ Сколько):
{ Сопротивление = Сопротивление * (1 + exp((Ut - Сколько)/Ut)); }

В БЗ объектно-ориентированной ЭС могут существовать несколько различных экземпляров объектов данного абстрактного типа в соответствии с резисторами, имеющимися в проектируемом устройстве. Однако важной особенностью объектно-ориентированного подхода является уникальность каждого из созданных объектов такого типа, что отражает привязку объекта БЗ ЭС к реальному электронному компоненту и дает возможность отделить его от прочих объектов данной БЗ ЭС.

Иерархия позволяет создавать сложные типы объектов в виде наследования, когда один объект использует структурную часть одного или нескольких других объектов (соответственно

простое или множественное наследование). Новый объект с использованием наследования записывается следующим образом:

ОБЪЕКТ электронный компонент:

Тип;

ОБЪЕКТ резистор НАСЛЕДУЕТ электронный компонент:

Сопротивление;

ОБЪЕКТ емкость НАСЛЕДУЕТ электронный компонент:

Емкость.

Каждый из объектов «резистор» и «емкость» имеют общий атрибут «тип», а также индивидуальные атрибуты согласно специфике модели представления [3].

Дочерние объекты могут быть дополнены и модифицированы относительно родительских объектов. Также существует возможность изменения реализации методов, наследуемых у суперклассов. Сохраняя интерфейс метода, описанного в суперклассе, метод подкласса содержит описание его собственных действий. Это важное свойство позволяет иметь в обобщающем классе только имя и параметры вызова метода, оставляя вопросы реализации каждому классу-наследнику, обладающему общим свойством, но имеющему индивидуальные особенности. Типичным примером служит метод определения требуемого электронного компонента, в зависимости от того, является он «резистором» или «емкостью». Поэтому структуру наследования можно записать следующим образом:

поля

ОБЪЕКТ электронный компонент:

X Тип;

ОБЪЕКТ резистор НАСЛЕДУЕТ электронный компонент:

Y Сопротивление;

Аналогичное описание структуры типов в Delphi приведет к тому, что в оперативной памяти будет выделена область для хранения поля X объекта электронный компонент и независимая область для хранения полей X и Y объекта резистор. Иными словами, язык программирования формирует независимые сегменты знаний на каждый сложный тип, образующийся в результате наследования [2, 4].

Один из важных принципов технологии объектно-ориентированных БЗ состоит в неизбыточности хранимой информации. Помимо экономии ресурсов, это способствует большей надежности при манипулировании данными. Действительно, в случае дублирования знаний, при внесении в них изменений, необходимо иметь механизм контроля за поддержанием целостности (не допуская расхождений) и производить, в итоге, как минимум в два раза больше работы (выполняя модификацию знаний в двух местах). Поэтому оптимальным является разделение знаний и метазнаний сложных типов, образующихся в результате наследования. Используем для иллюстрации тот же пример. Та часть объектов типа резистор, которая наследована у объектов суперкласса электронный компонент (поля X) сохраняется так же, как если бы это были экземпляры объектов типа электронный компонент. Собственная же часть объектов типа резистор (доля Y) хранится отдельно так, как хранились бы объекты, содержащие только поля Y. Можно сказать даже, что объекты резистор наследуют механизм хранения в той своей части, которая состоит из поля X - заимствованной у объекта электронный компонент.

Описанная ситуация отражает следующий взгляд на структуру объектов электронный компонент и резистор. Объекты электронный компонент обладают свойством X, а объекты резистор – свойствами и X и Y.

Что касается знаний, для моделирования которых используется подобная структура, то при описываемом подходе объекты типа B продолжают существовать и как объекты типа электронный компонент, т.е. электронный компонент, будучи резистором, не перестает быть электронным компонентом, сохраняя неизменной ту часть знаний, которая характеризует его как электронный компонент, а не как резистор. Нельзя исключить также и возможность перехода объекта из класса в класс. Конечно, наследование может быть использовано и для конструирования типов объектов

при помощи более сложных абстрактных типов, но для разработанной БЗ принципиальных схем каскадов и узлов РТУ характерным является именно случай уточнения объектов в подклассах [5].

Для обеспечения работы со сложными объектами, образующимися при наследовании, ЭС использует специальные связи между «наследованными» и «собственными» частями объектов. Эти связи не видны проектировщику и используются для внутреннего контроля за операциями с объектами. Понятно, что имеют место следующие ограничения целостности: в БЗ не могут существовать отдельно собственные части подклассов; каждой наследованной части сложного объекта должна соответствовать только одна собственная часть.

ОБЪЕКТ электронный компонент:

X целое;

ОБЪЕКТ резистор НАСЛЕДУЕТ электронный компонент:

Y целое;

ОБЪЕКТ переменный резистор НАСЛЕДУЕТ резистор:

Z целое;

В итоге, внутреннее представление сложных объектов, образуемых в результате наследования, выглядит в виде цепочек, как изображено на Рис. 1.

Сложный объект переменный резистор содержит три поля: X, Y, Z. Его собственная часть состоит из элемента Z. Последовательность связей, реализующих иерархию наследования, будем далее называть цепочкой наследования. Так, можно сказать, что хранение значений всех полей объекта Z обеспечивается по отдельности хранением собственных элементов всех объектов, участвующих в цепочке.

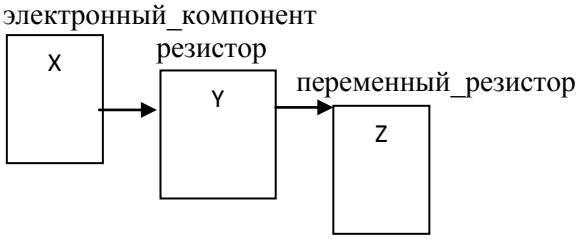


Рис. 1. Цепочка наследования

При попытке объединения структур знаний разработанного языка представления (ЯП) знаний в БЗ объектно-ориентированной ЭС возникает неопределенность в установлении соответствия между элементами объектов БЗ и объектов ЯП. То есть, при переносе из БЗ в рабочую память значения, например, элемента component, неясно, должно ли оно соответствовать значению component.X, resistor.X или var_resistor.X.

Чтобы избавиться от указанной неопределенности, предлагается следующий подход: переменный резистор формирует описание структуры знаний, соответствующей языку Delphi. В процессе работы ЭС эти структуры используются в качестве буфера для переноса знаний из внешней памяти в прочие программные переменные.

Таким образом, представление формируемых в БЗ ЭС знаний происходит путем замены значений типов элементов на динамические указатели на их значения, а при установлении связи между БЗ и ЭС в момент ее запуска указатели component.X, resistor.X или var_resistor.X устанавливаются на тот участок памяти, в который будут переноситься значения элементов. Таким образом, значением указателей component.X, resistor.X или var_resistor.X будет один и тот же адрес. В итоге образуется довольно органичное сочетание классов и неизбыточность знаний в БЗ. Если аналогичную иерархическую структуру описать на Delphi, оперативная память [3], отводимая под значения элементов объектов, будет иметь иной вид, т.е. описание типов будет таким:

```
component = OBJECT
X : INTEGER;
END;
resistor = OBJECT ( component )
```

Y : INTEGER;
END;
Var_resistor = OBJECT (resistor)
Z : INTEGER;
END;

что соответствует приведенной на Рис. 1. цепочке наследования. Но под значение объекта component будет выделен объем памяти, равный размеру элемента X, под значение объекта resistor - равный сумме размеров элементов X и Y, а под var_resistor - равный сумме размеров X, Y и Z.

Для того чтобы завершить описание объекта, нужно определить различные методы, которые объект может выполнять, и все переменные, чьи значения объект может получать и передавать.

В качестве примера приведем фрагмент классификации усилительных каскадов РТУ (см. Таблицу 1) на электронных лампах, биполярных и полевых транзисторах. Кроме того, при формировании БЗ учитывается наличие или отсутствие трансформатора, одно- или двухтактная работа УЭ, составные или одиночные УЭ, наличие обратных связей и др. В качестве родительских классов выступают классы, описывающие особенности каскадов УУ, связанные со способом включения УЭ [9]. Далее, последующим увеличением параметров и усложнением методов их использующих, формируется набор объектов усилительных каскадов.

Таблица 1

Фрагмент классификации усилительных каскадов в объектно-ориентированной базе знаний ЭС

	Схемы включения	режимы работы	цепи питания, смещение с	цепи коррекции
БТ	ОЭ, ОБ, ОК, каскодные, составные	A, B, AB, C, D...	фиксацией тока базы, напряжением на базе, эмиттерной стабилизацией, коллекторной и эмиттерно-коллекторной стабилизацией	ВЧ эмиттерная коррекция, ВЧ индуктивная коррекция, НЧ коррекция
ПТ	ОИ, ОЗ., ОС каскодные, составные		фиксацией напряжения на затворе, истоковой стабилизацией	ВЧ истоковая и катодная коррекция, ВЧ индуктивная коррекция, НЧ коррекция
ЭЛ	ОК, ОС, ОА каскодные, составные		катодной стабилизацией, фиксацией напряжения на сетке, цепью питания накала и экранирующей сетки	ВЧ индуктивная коррекция, НЧ коррекция

Таким образом, формирование БЗ объектно-ориентированной ЭС для синтеза РТУ состоит из следующих основных этапов:

- определение объектов для поставленной задачи;
- определение правил, связанных с каждым объектом, позволяющих определить параметры узла или каскада РТУ;
- разработка последовательности правил, которая позволяет определить параметры всего РТУ в целом.

Объектно-ориентированная ЭС, предназначенная для синтеза принципиальных схем РТУ [2], включает следующие блоки: подсистемы приобретения знаний, позволяющий формировать БЗ; ввода ТЗ из файла на проектирование узлов и каскадов РТУ, определенного в продукционной экспертной системе; механизма вывода, осуществляющего выбор и инициализации объектов, хранящих процедуры определения значений параметров компонентов принципиальной схемы РТУ; вывода результатов проектирования. В режиме “ОБУЧЕНИЕ” в БЗ объектно-ориентированной ЭС экспертами вводятся переменные и методы объектов, содержащие методику определения параметров компонентов принципиальных схем узлов и каскадов РТУ [1, 6].

Разработанный алгоритм формирования БЗ объектно-ориентированной ЭС. Эксперт вносит в БЗ название объекта, соответствующего каскаду РТУ и, при необходимости и возможности, имя объекта предка этого каскада. Для каждого объекта экспертом вводится набор внешних и внутренних переменных. Через внешние переменные объект получает информацию о типе

усилительного элемента, особенностях его включения, входных и выходных параметрах каскада и др [3, 4]. Внутренние переменные используются для определения параметров компонентов синтезируемого каскада. Кроме набора переменных, вводится и набор методов, позволяющих определить по функциональным соотношениям значения параметров компонентов каскада.

Алгоритм автоматического схемотехнического проектирования принципиальных схем РТУ в объектно-ориентированной ЭС приведен на Рис. 2. В соответствии с ТЗ, формируемым в виде текстового файла продукционной ЭС, выбираются объекты, соответствующие узлам и каскадам синтезируемого РТУ. В эти объекты передаются определенные ранее значения параметров отдельных каскадов. По формульным соотношениям, заложенным в методы объектов, определяются значения параметров компонентов принципиальной схемы синтезируемых каскадов. При этом неизвестные параметры электронных компонентов, требуемые при синтезе РТУ, выбираются автоматически из БД. Далее вычисленные значения компонентов сохраняются в текстовом файле в формате Spice. И, при необходимости, проводится моделирование синтезированной схемы РТУ в других блоках разработанной САПР [3, 6].

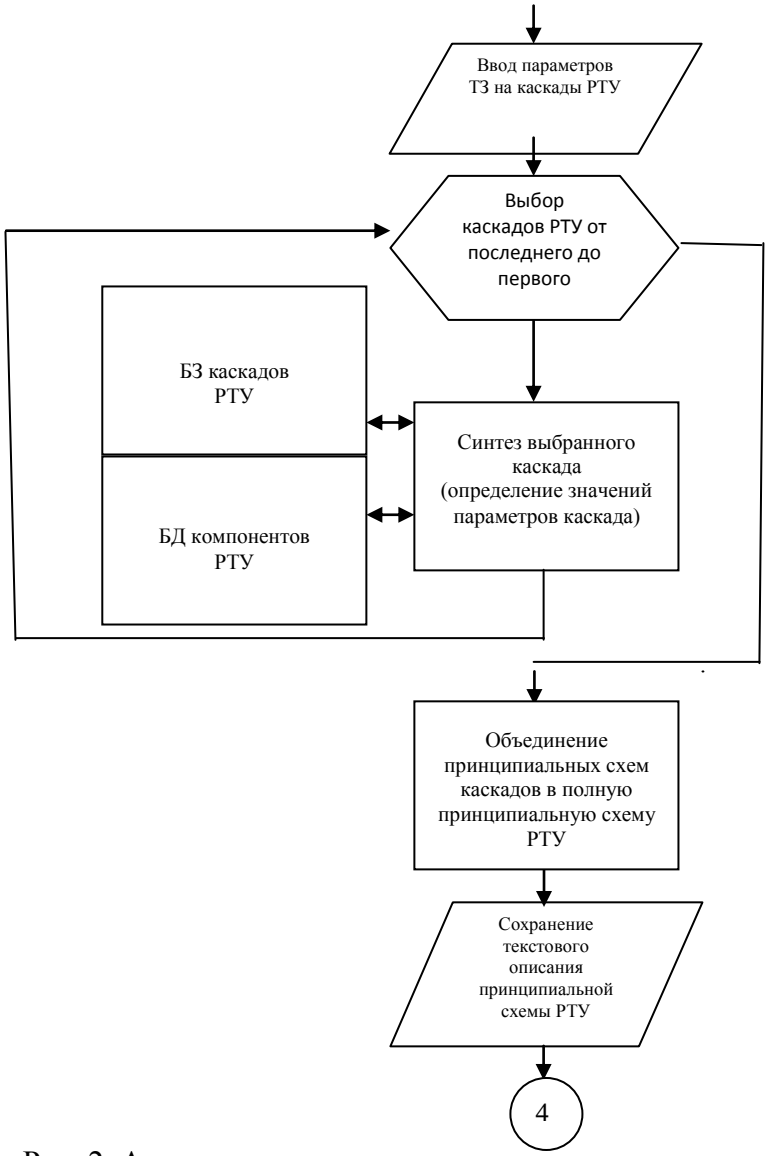


Рис. 2. Алгоритм автоматического синтеза принципиальных схем РТУ в объектно-ориентированной ЭС

Таким образом, приведенные алгоритмы работы объектно-ориентированной ЭС позволяют сформировать и гибко модифицировать иерархическую БЗ узлов и каскадов РТУ, а также проводить синтез принципиальных схем узлов, каскадов и всего РТУ в целом.

Литература

1. *Балашов В.О., Долин Г.А.* База данных электронных компонентов для автоматизации схемотехнического синтеза радиотехнических устройств // Телекоммуникации и информационные технологии. 2017. Т. 4. № 2. - Стр. 98-102.
2. *Головицына М.* Интеллектуальные САПР для разработки современных конструкций и технологических процессов: курс.- М.: Национальный Открытый Университет «ИНТУИТ», 2016.
3. *Долин Г.А*. Использование технологий интернет при формировании базы знаний экспертных систем проектирования радиооборудования (Аннотация доклада). Седьмая отраслевая научная конференция "Технологии информационного общества". Программа научно-технических секций 20-21 февраля 2013. - М.: МТУСИ, 2013. - Стр. 27.
4. *Долин Г.А*. Сквозное автоматизированное схемотехническое проектирование радиотехнических устройств // В сборнике: Прикладные исследования и технологии ART2015 сборник трудов Второй международной конференции- М: МТИ, 2015. С. 61-65.
5. *Малышев Н. Г.* Управление автоматизированным проектированием. Кн. 2. Принципы и модели построения информационного и программного обеспечения. - М.: Физматлит, 2017.
6. *Малышев Н. Г.* О системах и их моделировании. - М.: Физматлит, 2017.

THE DEVELOPMENT OF A KNOWLEDGE BASE OF THE CASCADES SCHEMATIC DIAGRAMS OF ELECTRONIC DEVICES IN AN OBJECT-ORIENTED EXPERT SYSTEM

Vitaly O. Balashov
Student of group MIT1702 MTUCI
balash1996@list.ru
Georgy A. Dolin
MTUCI, Ph. D., associate professor of ROS department
dolin1974@gmail.com

Keywords*: radio engineering devices, RED, expert system, ES, CAD, synthesis, design, system, KB, knowledge base, cascade, circuit diagram, block diagram*

The development of communication systems and devices requires full automation of their design process to quickly update. The article describes the algorithm of end-to-end CAD system, including production and hybrid object-oriented expert system for the synthesis of structural and schematic diagrams of the radio engineering devices, the modeling methods of nodal and state variables and a distributed dynamic database of parameters of electronic components.

АНАЛИЗ ЗАВИСИМОСТИ ТОЧНОСТИ ГНСС-ИЗМЕРЕНИЙ ОТ ГЕОГРАФИЧЕСКОЙ ШИРОТЫ

Кузнецов Андрей Владимирович
магистр группы АМЗГЗ-21 АСА ДГТУ
rabotarmo@gmail.com
Яковлев Владимир Викторович
ДГТУ, к.т.н., доцент кафедры Геодезия

Ключевые слова: *GPS, ГЛОНАСС, Галилео, геометрические факторы ГНСС*

При написании этой работы был проведен анализ зависимости значений геометрического фактора Галилео/GPS/ГЛОНАСС от географической широты. Данный эксперимент проводился с использованием специализированного программного комплекса компании Trimble. Фактор геометрии – один из важнейших при расчете ошибок в системах радионавигации. Рассчитав предполагаемые значения данного фактора появляется возможность для точной оценки при решении навигационной задачи на одной из начальных стадий планирования спутниковых наблюдений.

Глобальные навигационные спутниковые системы создавались с целью оперативного решения проблем по определению местоположения отдельных объектов, а также скорости перемещения ряда потребителей [1, с. 8] и др. В данной статье рассматриваются данные, полученные при анализе таких глобальных навигационных спутниковых систем как Галилео, GPS, ГЛОНАСС.

Для получения качественных и однозначных решении навигационной задачи требуется провести двухэтапную обработку данных.

Анализируя двухэтапную обработку сигналов, полученных со спутников, становится ясно, что точность спутниковых наблюдений характеризуется следующими видами ошибок:
ошибки обработки первой фазы;
ошибки обработки второй фазы.

Первая фаза обработки характеризуется образованием погрешности определения псевдоскорости и псевдодальности.

Ошибки второй фазы определяются факторами, влияющими на эффективность расчета оценки псевдодальностей и псевдоскоростей.

В работе рассматривается исключительно фактор геометрии [2, с. 300], входящий в состав погрешностей обработки второй фазы радионавигационных сигналов.
На сегодняшний день существует возможность прогнозирования, а также анализа коэффициентов геометрии для любых точек размещения аппаратуры потребителя на земной поверхности для любой ГНСС.

В данной работе исследование геометрического фактора проводилось с использованием программного комплекса, созданного компанией Trimble. Программный комплекс предназначен для анализа и прогнозирования орбитального движения НКА, а также расчетов геометрии ГНСС.
Актуальная информация, передаваемая с каждого навигационного космического аппарата ГНСС, включающая в себя данные о шкале времени ГНСС, данные о бортовых шкалах времени всех навигационных космических аппаратов и данные об элементах их орбит и техническом состоянии предоставлена сервисом https://www.gnssplanning.com.

Анализ влияния геометрии расположения НКА ГНСС Галилео/GPS/ГЛОНАСС на точностные характеристики проводился для 19 точек на земной поверхности. Точки размещения наблюдателей были выбраны на фиксированной долготе 38° в.д. (L), широта точки наблюдения менялась от 90° с.ш. до 90° ю.ш (φ). Изменение положения точки наблюдения производилось с шагом равным 10°. Высота точки наблюдения над земной поверхностью 50 м (H). Для получения

данных для анализа использовалась информация с 24-х навигационных космических аппаратов ГНСС ГЛОНАСС, 31-го навигационного космического аппарата ГНСС GPS, 14-ти навигационных космических аппаратов ГНСС Галилео, резервные навигационные космические аппараты не регистрировались, данные с них не учитывались. Угол отсечки спутника равен 6°(β). Время наблюдения: 10:00:00 часов по Московскому времени 08.10.2018 г.

Результаты расчетов представлены в Табл. 1.

Таблица 1

Координаты точки наблюдения		Число космических аппаратов			Position Dilution of Precision (PDOP)			Geometric Dilution of Precision (GDOP)			Horizontal Dilution of Precision (HDOP)		
φ	L	Галилео	ГЛОНАСС	GPS	Галилео	ГЛОНАСС	GPS	Галилео	ГЛОНАСС	GPS	Галилео	ГЛОНАСС	GPS
90°с.ш.	38° в.д.	8	9	10	2.07	1.89	2.35	2.29	2.15	2.64	0.87	0.91	0.81
80°с.ш.		7	9	11	2.89	2.04	1.86	3.25	2.32	2.06	1.11	1.01	0.71
70°с.ш.		7	9	12	2.57	2.02	1.6	2.82	2.29	1.76	0.98	0.97	0.69
60°с.ш.		7	9	12	2.57	2.06	1.47	2.82	2.34	1.61	0.98	1.02	0.72
50°с.ш.		7	9	9	2.56	2.06	1.99	2.78	2.34	2.28	0.88	1.02	0.97
40°с.ш.		6	9	9	7.72	1.72	2	8.51	1.9	2.29	1.08	0.89	1.03
30°с.ш.		7	8	8	3.69	2.62	2.24	4.01	2.92	2.61	0.88	1.21	1.2
20°с.ш.		7	8	10	3.96	1.75	1.44	3.96	1.92	1.61	1.15	0.86	0.85
10°с.ш.		7	9	11	2.03	1.52	1.65	2.19	1.65	1.85	0.99	0.79	0.85
00°с.ш.		5	8	11	2.46	2.01	1.61	2.74	1.75	1.85	1.44	0.9	0.78
10°ю.ш.		5	9	10	2.44	1.43	1.92	2.72	4.54	1.12	1.53	0.87	0.87
20°ю.ш.		4	6	10	7.01	2.42	1.67	8.97	2.82	1.88	3.71	1.52	0.87
30°ю.ш.		4	6	10	6.96	2.6	1.48	8.92	2.98	1.66	3.94	1.41	0.83
40°ю.ш.		5	7	10	2.93	2.47	1.47	3.47	2.8	1.65	2.2	1.35	0.87
50°ю.ш.		6	8	10	1.81	1.91	1.32	1.99	2.14	1.46	1.13	1.12	0.85
60°ю.ш.		5	8	11	3.68	2.08	1.26	4.11	2.39	1.4	1.58	1.09	0.78
70°ю.ш.		5	9	12	3.7	1.83	1.78	4.13	2.08	2.01	1.33	0.9	0.92
80°ю.ш.		5	9	12	3.76	1.83	1.76	4.19	2.08	1.98	1.38	0.85	0.75
90°ю.ш.		9	9	10	2.1	1.9	2.4	2.2	2.2	2.2	1.9	1.7	2.2

Для каждой точки наблюдения из таблицы 1 анализировались следующие значения основных составляющих коэффициента геометрии:

– снижение точности по местоположению - Position Deletion Of Precision (PDOP);

– общее геометрическое снижение точности по местоположению и времени- Geometric Dilution Of Precision (GDOP);

– снижение точности в горизонтальной плоскости - Horizontal Dilution Of Precision (HDOP),

и количество «видимых» спутников в каждой точке наблюдения.

По результатам измерений (представленных в Табл. 1) построены графики (Рис. 1-10).

На Рис. 1 показано количество видимых спутников трех исследуемых ГНСС Галилео/GPS/ГЛОНАСС. Данные анализа результатов показывают:

– наименьшее количество спутников ГНСС ГЛОНАСС определяется на широтах φ=20° ю.ш. и φ=30° ю.ш. Для СРНС ГЛОНАСС это количество равно 6.

Для ГНСС GPS, наименьшее количество НКА определяется на широтах φ=30° с.ш. Для ГНСС GPS это количество составляет равно 8.

Для ГНСС Галилео наименьшее количество НКА определяется на широтах φ=20° с.ш. и φ=30°ю.ш. Для СРНС Галилео это количество составляет равно 4.

Такой разброс в полученных результатах объясняется тем, что на момент проведения измерений в СРНС ГЛОНАСС по целевому назначению использовалось 24 спутника, для СРНС Галилео – 14 спутников, а для СРНС GPS – 31 спутник;

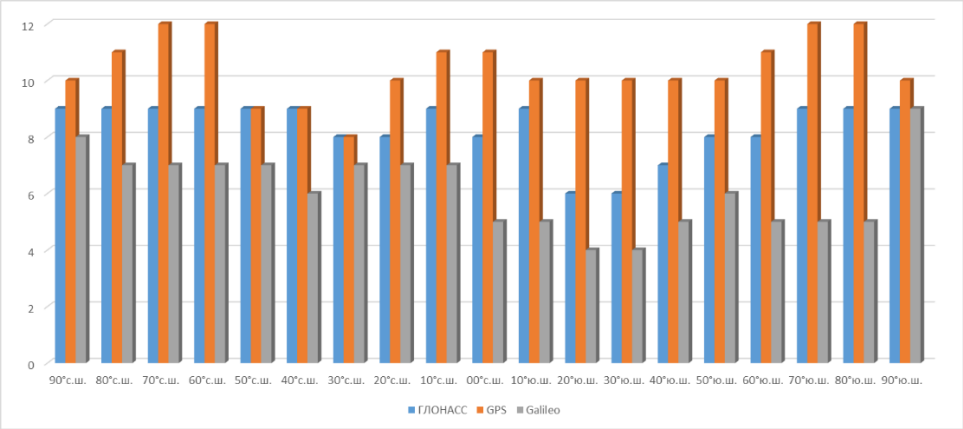


Рис. 1 Количество видимых НКА ГНСС ГЛОНАСС, GPS, Галилео в 10:00:00, 08.10.2018 г., L 38° в.д.

Максимальное количество спутников СРНС ГЛОНАСС, GPS, Галилео фиксируется на широтах от φ=90° с.ш., до φ=60° с.ш. и φ=90° ю. ш. Для ГЛОНАСС это значение равно 9 НКА. Для СРНС Галилео 9. Для GPS 12.

Рис. 2−4 отображены мгновенные показатели коэффициентов геометрии GDOP ГНСС Галилео/GPS/ГЛОНАСС для определенных точек наблюдения. Анализ результатов проведенных измерений показывает:

– значения полученных коэффициентов геометрии НКА ГНСС возможно описать обратной пропорцией к количеству видимых НКА;

– наименьший показатель GDOP ГНСС ГЛОНАСС определяется на 10° с. ш. и равняется 1,65 (Рис. 2);

– наибольший показатель GDOP ГЛОНАСС определяется на 10° ю. ш. и равно 4,54 (Рис. 2);

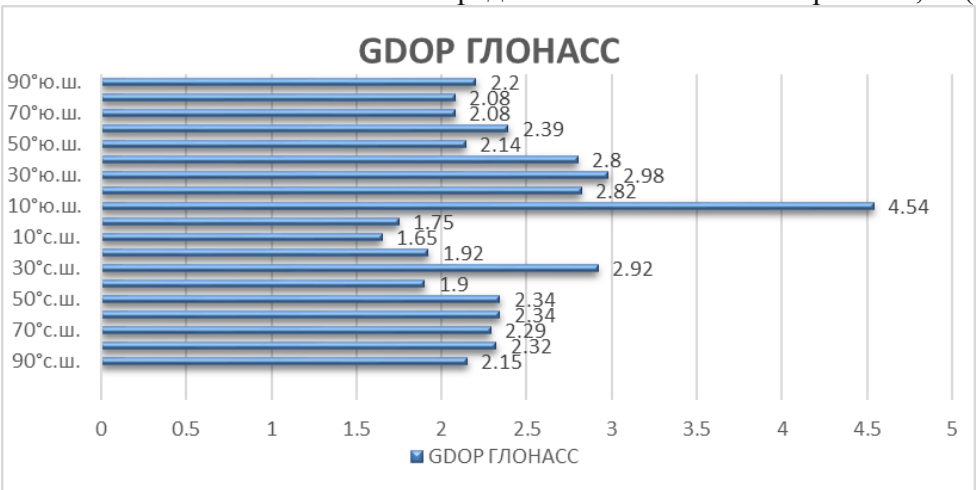


Рис. 2 Отображение min, max показателей GDOP ГНСС ГЛОНАСС.

– наименьший показатель GDOP ГНСС GPS определяется на 10° ю.ш., и равно 1,12 (Рис. 3);

– наибольший показатель GDOP ГНСС GPS определяется на 90° ю.ш., и равно 2,64 (Рис. 3);

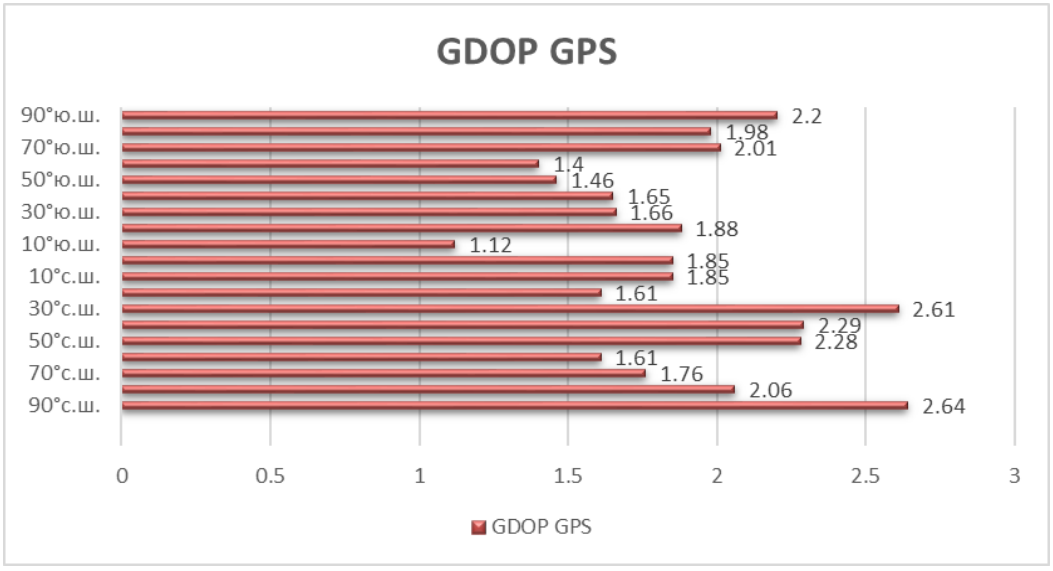


Рис. 3 Отображение min, max показателей GDOP ГНСС GPS.

– наименьший показатель GDOP ГНСС Галилео определяется на 50° ю.ш. и равно 1,99 (Рис. 4);
– наибольший показатель GDOP ГНСС Галилео определяется на 20° ю.ш. и равно 8,97 (Рис. 4).

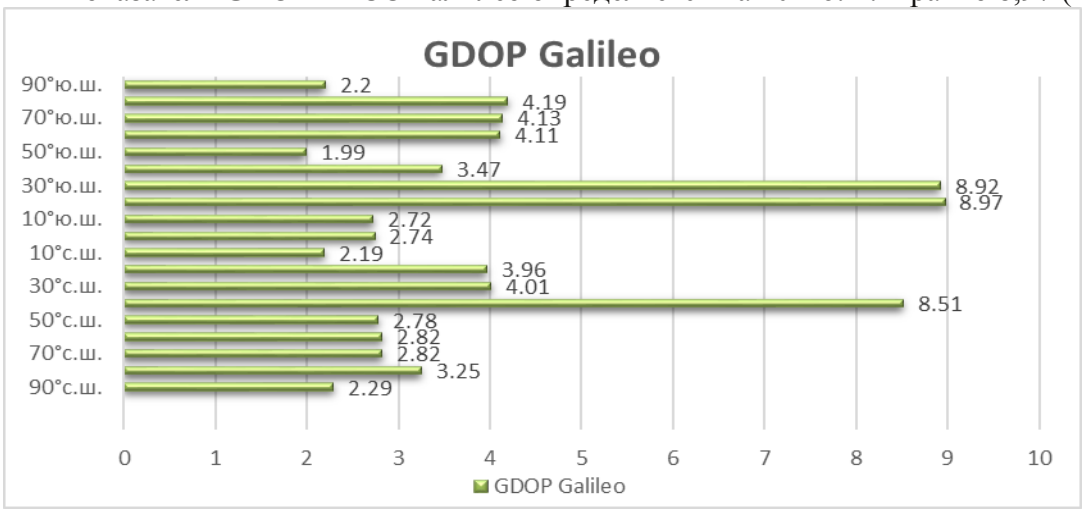


Рис. 4 Отображение min, max показателей GDOP ГНСС Галилео.

На Рис. 5,6,7 представлены графики коэффициентов геометрии (GDOP, PDOP, HDOP) ГНСС Галилео/GPS/ГЛОНАСС. Графики построены по данным, полученным после анализа измерений. Результаты показывают:

– для ГНСС GPS в исследуемых точках (за исключением полярных, и близких к ним областей) наблюдаются наименьшие значения всех составляющих коэффициента геометрии (GDOP, PDOP, HDOP);

– значения всех составляющих коэффициента геометрии (GDOP, PDOP, HDOP) для ГНСС Галилео стремятся к значениям ГЛОНАСС;

– увеличение значений геометрического фактора ГНСС Галилео, в сравнении с другими системами спутниковой навигации, компенсируется в северном и южном полушариях за широтой выше 60°. Однако стоит заметить, что численность ГНСС Галилео на момент исследования составляла 14 НКА против 31 НКА ГНСС GPS и 24 НКА ГНСС ГЛОНАСС.

Данные значений, отображенные на рис. 5, 6, 7, показывают, что коэффициенты геометрии (GDOP, PDOP, HDOP) подвергаются изменениям в значительном диапазоне.

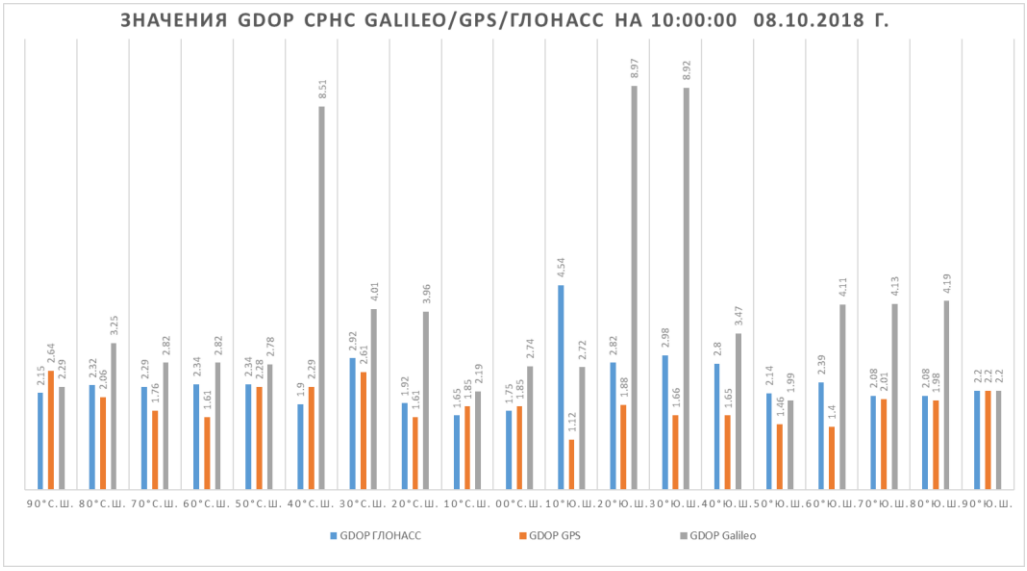


Рис. 5. Показатели GDOP СРНС Галилео/GPS/ГЛОНАСС на 10:00:00 08.10.2018 г.

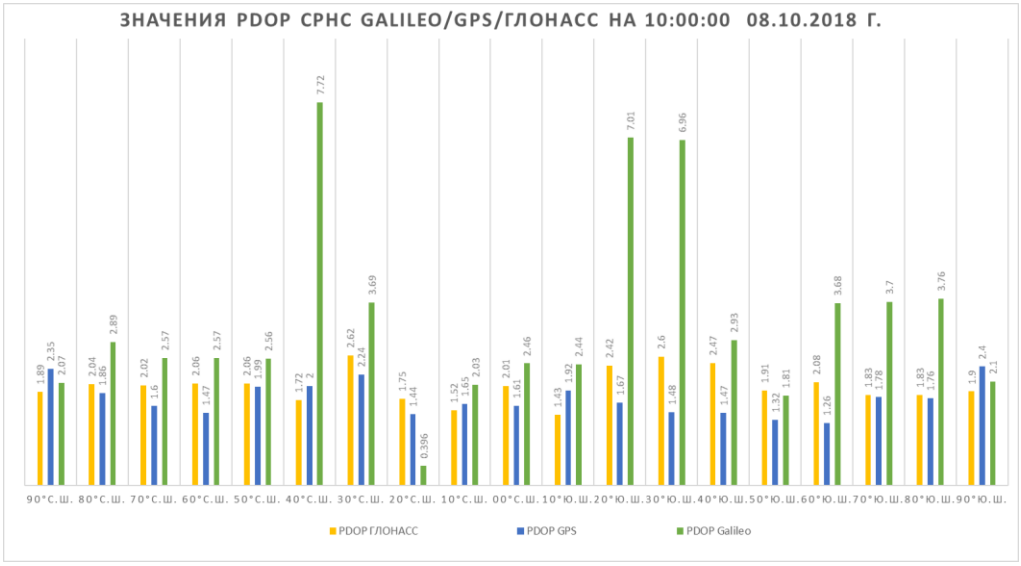


Рис. 6. Показатели PDOP СРНС Галилео/GPS/ГЛОНАСС по состоянию на 10:00:00 08.10.2018 г.

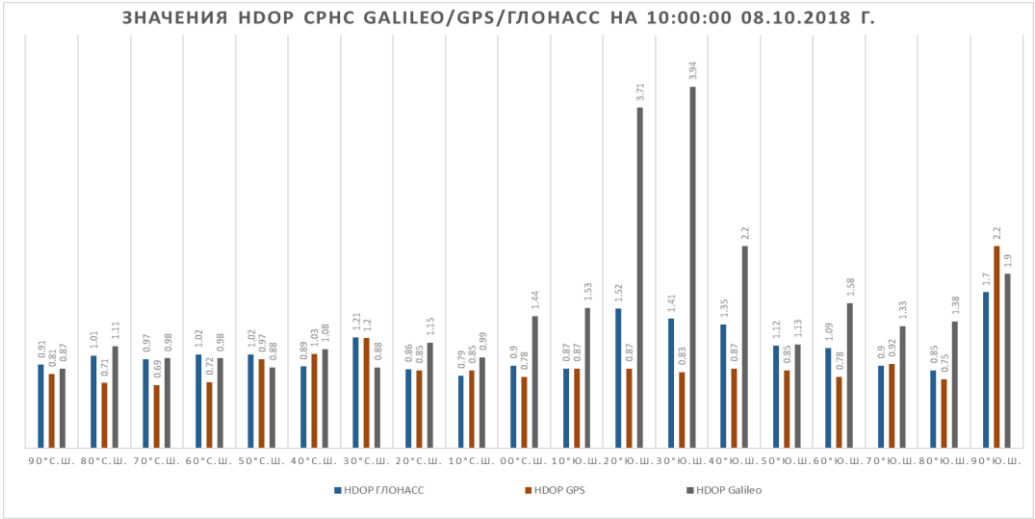


Рис. 7. Показатели HDOP СРНС Галилео/GPS/ГЛОНАСС по состоянию на 10:00:00 08.10.2018 г.

Заключение

Существующее построение группировки НКА ГНСС ГЛОНАСС, отличное от GPS и Галилео, при использовании меньшего количества НКА позволяет достигать лучших значений геометрического фактора. В северных и южных широтах значения геометрического фактора всех исследуемых ГНСС эквивалентны. Для GDOP это широты выше φ=70° с.ш. и ниже φ=70° ю.ш., для PDOP и HDOP – выше φ=50° с.ш. и ниже φ=50° ю.ш. , при L = 38° в.д.

Расчет структуры коэффициента геометрии в различных географических условиях имеет огромное значение.

Спрогнозированные показатели геометрического фактора дают возможность рассчитать погрешность решения навигационных задач определения радионавигационных параметров на этапе планирования ГНСС-наблюдений.

Литература

1. Глобальная навигационная спутниковая система ГЛОНАСС: интерфейсный контрольный документ. Навигационный радиосигнал в диапазонах L1, L2 с открытым доступом и частотным разделением (редакция 5.1). М., 2008.

2. *Дубошин Г. Н.* Справочное руководство по небесной механике и астродинамике. М.: Наука (Глав. ред. физ.-мат. лит.),1976. 864 с.

3. ГЛОНАСС. Принципы построения и функционирования / под ред. А. И. Перова, В. Н. Харисова. Изд. 4-е, перераб. и доп. М.: Радиотехника, 2010. 800 с.

4. Альманах современной науки и образования Тамбов: Грамота, 2015. № 11 (101). С. 94-100. ISSN 1993-5552.

5. ICD-GPS-200C. Navstar GPS Space Segment / Navigation User Interfaces. Interface Control Document, 2003.

ANALYSIS OF THE DEPENDENCE OF ACCURACY OF GNSS MEASUREMENTS FROM GEOGRAPHIC LATITUDE

Andrei V. Kuznetsov
master of group АМЗГЗ-21 ASA DGTU
rabotarmo@gmail.com

Key words: GPS, GLONASS, Galileo GNSS geometric factors

When writing this work, we studied the dependence of the geometric factor of Galileo / GPS / GLONASS on the geographical latitude. The analysis was carried out using a specialized software company Trimble. Geometry factor is one of the most important in calculating errors in radio navigation systems. Having calculated the estimated values of this factor, it becomes possible to accurately estimate the solution of the navigation problem at one of the initial stages of planning satellite observations.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМ МОБИЛЬНОЙ СВЯЗИ 4G И 5G

Морозова Кристина Димитриевна
студент группы ЗМТТ1701 МТУСИ
mkd2016@bk.ru
Сорокин Александр Степанович
МТУСИ, к.т.н., доцент кафедры СиСРТ
alexorokin@rambler.ru

Ключевые слова: *эффективность, эффективность функционирования, технология мобильной связи, стандарт мобильной связи, энергетическая эффективность системы связи, частотная эффективность системы связи, информационная эффективность системы связи, пропускная способность системы связи.*

Приведены результаты качественного анализа существующего положения в вопросе разработки технологии мобильной связи 5G на основании сведений, имеющихся на данный момент в научно-технической периодике и на сайтах Интернет. Выполнена количественная сравнительная оценка характеристик функционирования систем мобильной связи 4G и систем мобильной связи 5G с использованием типовых условий работы для обеих, определяемых общими системными исходными данными. Количественная оценка характеристик функционирования систем мобильной связи выполнена на основе обобщенного критерия – эффективности функционирования. На основании полученных результатов количественного сравнения характеристик функционирования сделан ряд прогностических выводов о влиянии структурных параметров на эффективность функционирования систем мобильной связи 5G.

Системы мобильной связи (СМС) 5G будут основываться на разрабатываемой в настоящее время новой технологии мобильной связи (ТМС) 5G, которая, как ожидается, может быть стандартизирована под кодовым наименованием IMT-2020 примерно в 2020 году. Таким образом, на настоящий момент неизвестны конкретные параметры ТМС 5G и имеется лишь возможность проведения прогностических оценок тех или иных характеристик будущих СМС 5G. В то же время, учитывая, что ТМС 5G позиционируется как универсальная и единая мировая ТМС и с учетом возросших и возрастающих требований к характеристикам функционирования (ХФ) современных и перспективных СМС, оказывается значительной ответственность за выбор характеристик стандарта ТМС 5G. В связи со сказанным, как в учебном, так и в научно-техническом отношении, является крайне актуальной задача прогностического анализа показателей функционирования будущих СМС 5G.

Целью статьи является разработка методики получения опорных данных для прогнозирования характеристик ТМС 5G путем сравнительного количественного анализа ХФ систем мобильной связи 5G и 4G на основе критериев обобщенной эффективности и частных эффективностей. Указанное сравнение проводилось в эквивалентных условиях работы рассматриваемых СМС, определяемых приведенными в табл. 1 общими исходными данными.

Таблица 1. Общие системные данные сравниваемых СМС

Параметр	Значение
Тип территории обслуживания (ТО)	Большой город (БГ)
Процент блокировки абонентского канала (АК), %	5
Процент нарушения связи в АК, %	7
Число абонентов, обслуживаемых СМС, тыс. чел.	300

Анализ состояния вопроса разработки ТМС 5G

В разработке ТМС 5G в настоящее время участвует множество телекоммуникационных компаний по всему миру, продвигая при этом свои собственные варианты [1]. При этом, однако, можно отметить общую тенденцию, связанную не только со значительным повышением скорости передачи, но и с повышением интеллектуализации оборудования СМС и всей сетевой инфраструктуры.

Основой сказанного будет являться параллельно развивающаяся информационная технология SDN (Software Defined Net), хотя представляется, что в ТМС 5G к моменту принятия стандарта вряд ли ее возможно встроить.

Вместе с тем при разработке ТМС 5G рассматриваются возможности примененения ряда инфраструктурных локальных технологий, существенно определяющих качество функционирования СМС. Ниже кратко рассмотрены 2 такие технологии.

На рис. 1 показаны два типа сетевых архитектур СМС 5G: неавтономная – Non-Standalone (стандарт которой был принят в 2017) и автономная – Standalone (стандарт которой будет принят позднее) [1, 4].

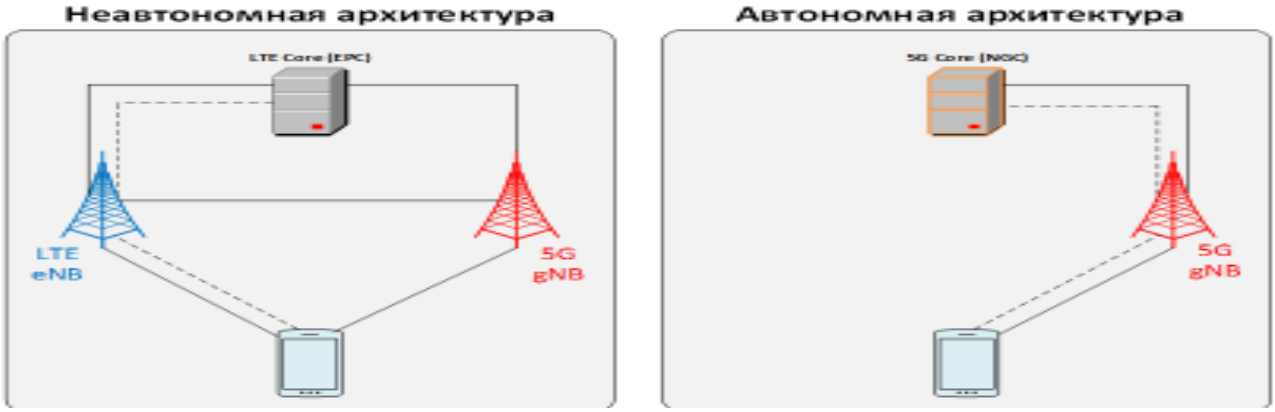


Рис. 1. Альтернативные виды архитектуры СМС 5G

Особенность неавтономной структуры заключается в том, что она позволяет строить СМС 5G на основе существующей архитектуры СМС 4G. Ядро остается прежним, либо просто добавляются дополнительные базовые станции (БС) сети 5G (gNB), либо на существующих станциях СМС 4G (eNB) разворачиваются модули СМС 5G. Автономная архитектура описывает разворачивание СМС 5G полностью с нуля, в том числе и ядра сети.

На рис. 2 проиллюстрирована новая технологическая концепция Network Slicing («сетевая нарезка»), которая предположительно будет использоваться в СМС5G [1].

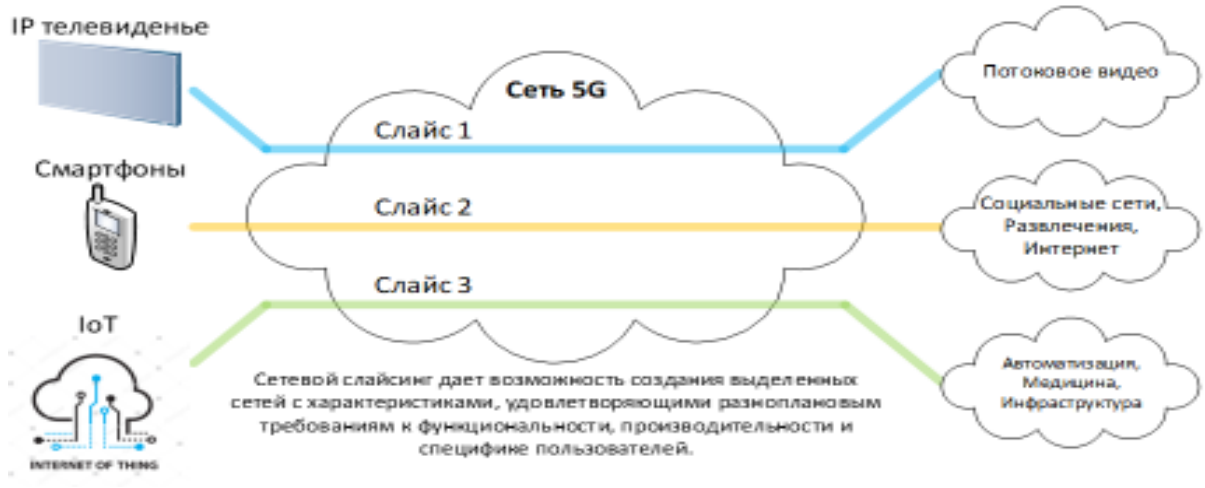


Рис. 2. Иллюстрация новой технологии Network Slicing («сетевая нарезка»)

Суть данной технологии заключается в том, что сетевая инфраструктура СМС 5G может быть логически разделена (нарезана) на «сетевые слои» — «слайсы», (от англ. slice — слой) для разных бизнес приложений и для разных технологий радиодоступа (RAT). Такие сетевые слои могут быть раздельно оптимизированы под различные требования (скорость передачи данных для различных RAT, приоритет, задержка и пр.). Например, видео-приложение 4К требует высокой скорости и некритична к задержке пакетов, а приложение NB-IoT, наоборот, нетребовательно к скорости, но, в ряде случаев, требует достаточно быстрой доставки информации. Приложение «Тактильного Интернета» почти всегда требует самой минимальной задержки. И это только три приложения из многочисленных применений услуг мобильной связи 5G.

В табл. 2 для сравнения приведены актуальные характеристики ТМС 4G [2] и предположительные характеристики ТМС 5G [4].

Таблица 2

Основные характеристики стандартов ТМС 4G и ТМС 5G

ПАРАМЕТР	4G (IMT-Advanced)	5G (IMT-2020)
Пиковая скорость передачи для абонентов с низкой мобильностью, Uplink	500 Мбит/с	10 Гбит/с
Пиковая скорость приема для абонентов с низкой мобильностью, Downlink	1000 Мбит/с	20 Гбит/с
Пиковая скорость приема для абонентов с высокой мобильностью, Downlink	100 Мбит/с	100 Мбит/с
Пиковая скорость для абонентов с высокой мобильностью, Uplink	50 Мбит/с	50 Мбит/с
Задержка (User Plane)	<10 мс	< 1 мс
Спектральная эффективность, нисходящий канал	15 бит/с/Гц	30 бит/с/Гц
Спектральная эффективность, восходящий канал	6.75 бит/с/Гц	15 бит/с/Гц
Частотный диапазон	до 6 ГГц	до 73 ГГц
Ширина полосы пропускания	20 МГц	до 100 МГц при частоте < 6 ГГц до 1 ГГц при частоте > 6 ГГц
Объединение несущих	до 32	до 16
Плотность абонентов	100000 на км²	1000000 на км²
Максимальная скорость движения абонента	до 350 км/ч	до 500 км/ч
Энергоэффективность		> 90 % улучшение по сравнению с LTE

Как видно из приведенных в табл. 2 данных, некоторые характеристики ТМС 5G существенно улучшаются по сравнению с ТМС 4G, а некоторые являются сравнимыми или даже одинаковыми, что тоже вполне логично.

Широко распространенный в настоящее время процесс тестирования вариантов ТМС 5G, разрабатываемых компаниями разных стран, сейчас прозвали «5G-гонкой». Лидирует в этой гонке *Россия*, Европа, Азиатский регион, Австралия.

Так в уже 2017 году компании Ericsson и МТС создали прототип СМС 5G и успешно завершили его тестирование, в том числе при использовании стационарного и мобильного оборудования. Компаниям удалось добиться пиковой скорости передачи данных 25 Гбит/с. Это стало возможным благодаря технологиям Multi-User и Massive MIMO, Beam Tracking и Dynamic TDD [3, 4].

Компания Samsung в партнерстве с японским оператором KDDI объявила о завершении тестирования 5G на движущемся поезде (его скорость была выше 100 км/ч). Скорость передачи данных во время эксперимента достигла 1,7 Гбит/с при нисходящем и восходящем соединении.

Приведенные примеры и темпы процесса тестирования ТМС 5G указывают на то, что планы предположительного принятия стандарта ТМС 5G состоятся, как и намечено, в 2020 году.

Предположительные характеристики технологии мобильной связи 5G

Общесистемные характеристики [3, 4]:

- скорость передачи данных: рост в 10–100 раз в расчёте на абонента — до 10 Гбит/с (UL) и до 5 Гбит/с (DL);
- объем допустимого абонентского трафика: рост в 1000 раз — до 500 Гб на пользователя в сутки;
- увеличение количества подключаемых абонентских устройств соте в 10–100 раз;
- десятикратное увеличение времени автономной работы абонентских устройств с небольшим энергопотреблением, таких как сенсоры M2M;
- сокращение времени задержки вызова до 1 мс и менее;
- снижение стоимости эксплуатации и энергопотребления сетей 5G до 10% от текущего потребления сетей 4G;
- мобильные базовые станции;
- широкое применение облачных технологий на разных уровнях инфраструктуры;
- виртуализация функций сетевого управления;
- применение технологии координированной работы сотовой инфраструктуры.

Характеристики радиоинтерфейса [4, 5]:

- множественный доступ на физическом уровне (PHY) со скоростями несколько Гбит/с;
- использование новых диапазонов частот от 28 ГГц до 100 ГГц;
- полосы радиоканалов со значительной шириной: от 100 МГц до 2 ГГц;
- очень короткие задержки в сети радиодоступа: время переспроса менее 1 мс;
- низкая стоимость узлов доступа и низкая стоимость абонентских устройств;
- «бесшовная» мобильность между инфраструктурой 5G (UDN) и сотовыми системами для больших зон покрытия LTE/2G-3G;
- использование новых сигнально-кодовых конструкций для повышения спектральной эффективности СМС за счет применения новых сигнально-кодовых конструкций на основе неортогональных сигналов и FTN-сигналов.

Ключевые услуги [2, 3]:

- сервисы M2M (энергетика, транспорт, здравоохранение, торговля, общественная безопасность, промышленность, ЖКХ);
- сервисы виртуальной реальности (образование, развлечения);
- сервисы дополненной реальности (здравоохранение, военная промышленность, образование, развлечения);
- сервисы социальных сетей (развлечения, торговля);
- персональные услуги (транспорт, здравоохранение, бытовая техника, развлечения);
- мультимедийные услуги (Ultra HD видео, 3D видео, онлайн игры);
- облачные сервисы (государственные услуги, бизнес приложения).

Ключевые методы обработки сигналов [4]:

- прогрессивные виды многоантенных технологий: массивное MiMO (MMIMO); многопользовательское MIMO (MU-MIMO); формирование луча BeamForming и др.;
- усовершенствованные разновидности технологии OFDM: F-OFDM, N-OFDM, G-OFDM;
- метод D2D: прямая связь между мобильными станциями;
- метод V2V: прямая связь между мобильными станциями на автомобилях;
- метод виртуализации сетевой инфраструктуры «сетевая нарезка».

Критерии сравнения ХФ СМС

В качестве критерия сравнения ХФ СМС предлагается использовать показатель – эффективность функционирования (Э) [2, 4]. Эффективность является обобщенной характеристикой, учитывающей все влияющие свойства СМС, и показывающей насколько полно используются ресурсы связи и материальные ресурсы данной СМС.

Математически Э может быть выражена соотношением, являющимся расширением соотношения для Э, предложенного в [2], путем введения дополнительных эффективностей,

учитывающих максимальную скорость абонента (мобильность), мультисервисность трафика и время задержки доставки сообщений

$$Э = Э_ч \cdot Э_э \cdot Э_и \cdot Э_с \cdot Э_о \cdot Э_м \cdot Э_т \cdot Э_з , \quad (1)$$

в котором: $Э_ч$ – частотная эффективность; $Э_э$ – энергетическая эффективность; $Э_и$ – информационная эффективность; $Э_с$ – стоимостная эффективность; $Э_о$ – эффективность обслуживания; $Э_м$ – эффективность мобильности; $Э_т$ - эффективность трафика; $Э_з$ – эффективность по задержке.

Частотная эффективность СМС определяется соотношением [2, 4]

$$Э_ч = R_{аб\sum} / \Delta f_{смс} , \quad (2)$$

в которой $R_{аб\sum}$ - суммарная скорость передачи абонентских сигналов для данной СМС в "Час наибольшей нагрузки" (ЧНН) ; $\Delta f_{смс}$ - общая ширина полосы радиочастот, занимаемая в эфире данной СМС [2].

В (2) показатель $R_{аб\sum}$ рассчитывается по формуле

$$R_{аб\sum} = N_{аб} \cdot R_{аб} , \quad (3)$$

где $N_{аб}$ – число абонентов, обслуживаемых в СМС; $R_{аб}$ – минимальная гарантированная скорость передачи абонентских сигналов в ЧНН.

В (2) значение показателя $\Delta f_{\sum}$ при анализе рассчитывается по формуле [2]

$$\Delta f_{смс} = \Delta f_{рк1} \cdot N_{рк\ сек} \cdot M_{сек} \cdot N_{кл} \cdot N_f , \quad (4)$$

где $\Delta f_{рк1}$ – ширина полосы частот 1 радиоканала, МГц; $N_{рк\ сек}$ – число радиоканалов в 1 секторе БС; $M_{сек}$ – число секторов в соте; $N_{кл}$ – размерность кластера; N_f – коэффициент переиспользования частот в секторах сот.

В (4) все входящие параметры являются известными: $\Delta f_{рк}$ – определено в стандарте соответствующей технологии мобильной связи, если он принят и действует, как например в случае 4G, или принимается некоторое предполагаемое к использованию в будущем, как например в случае 5G; типовое значение параметра $N_{рк\ сек}$ равно 1 и тенденции к его изменению не наблюдаются; произведение $M_{сек} \cdot N_{кл} \cdot N_f$ является обобщенным параметром, описывающим конфигурацию кластерно-секторной структуры СМС [2], который может принимать ряд типовых значений вида: 1x1x1; 1x3x3; 3x1x1; 3x3x3; 3x3x1. Качественный анализ показывает, что в большинстве практических условий функционирования СМС условно оптимальной можно считать конфигурацию 3x3x1, которая и принята для сравнительного анализа в данной работе.

Энергетическая эффективность СМС определяется соотношением, аналогичным соотношению, предложенному в [2, 4]

$$Э_э = R_{аб\sum} / (Q_{шп\ доп} \cdot N_{рк\sum}) , \quad (5)$$

где $N_{рк\sum}$ - суммарное число радиоканалов, используемых в СМС

$$N_{рк\sum} = N_{рк\ сек} \cdot M_{сек} \cdot N_{бс} , \quad (6)$$

в которой $N_{бс}$ – число БС в СМС, рассчитываемое по методике, изложенной в [2];

$Q_{шп\ доп}$ – допустимое отношение сигнал-(шум+помеха) (ОСШП) на входе приемника (в разах), которое определяется по формуле [5]

$$Q_{шп\ доп} = 10^{0,1 \cdot (q_{ш\ доп} + \Delta q_п)} , \quad (7)$$

в которой $q_{ш\ доп}$ - допустимое отношение сигнал-шум (ОСШ) на входе приемника в дБ; $\Delta q_п$ – энергетический запас на воздействие внешних помех, дБ. Отметим, что значения данных параметров зависят от вида используемой в канале связи модуляции и скорости передачи сигнала.

Допустимое ОСШ рассчитывается по соотношению [2]

$$q_{ш\ доп} = q_{ш0\ доп} + \Delta^- - \Delta^+ , \quad (8)$$

в котором $q_{ш0\ доп}$ – допустимое ОСШ (дБ) для идеального канала связи при заданном значении допустимой вероятности ошибок $P_{ош\ доп}$, типовое значение которой в СМС принимается равной

$P_{\text{ош доп}}=10^{-2}$ [1, 2]; Δ^- - энергетические потери из-за неидеальностей приемопередающего тракта, дБ; Δ^+ - энергетический выигрыш от помехоустойчивого кодирования, дБ.

Значение параметра $\Delta q_{\text{п}}$ для модуляции вида 16-КАМ…256-КАМ лежит в пределах (3…7) дБ [5].

Информационная эффективность СМС определяется соотношением [2, 4]

$$\text{Э}_{\text{i}} = R_{\text{аб}\sum} / R_{0\sum}, \qquad (9)$$

в которой $R_{\sum}$ – суммарная пропускная способность данной СМС, рассчитываемая по формуле Шеннона [4]

$$R_{0\sum} = \Delta f_{\sum} \cdot log_2(1+Q_{\text{шп доп}}), \qquad (10)$$

где $\Delta f_{\sum}$ - суммарная физическая ширина полосы частот всех используемых в СМС радиоканалов

$$\Delta f_{\sum} = \Delta f_{\text{рк1}} \cdot N_{\text{рк}\sum}. \qquad (11)$$

Стоимостная эффективность СМС определяется соотношением

$$\text{Э}_{\text{с}} = C_{\text{смс0}} / C_{\text{смс}}, \qquad (12)$$

в которой $C_{\text{смс}}$ - стоимость сооружения данной СМС; $C_{\text{смс0}}$ – предположительная минимальная стоимость СМС. Для определения $C_{\text{смс}}$ можно использовать методику расчета стоимости оборудования СМС новых поколений [3]. Однако, в данной работе показатель $C_{\text{смс}}$ определяется приближенно по формуле, учитывающий стоимость структурных элементов, в основном определяющих его значение

$$C_{\text{смс}} = C_{\text{цс}} + C_{\text{бс1}} \cdot N_{\text{бс}}, \qquad (13)$$

где $C_{\text{цс}}$ – стоимость центральной станции данной СМС, млн. долл.; $C_{\text{бс1}}$ - стоимость 1 БС данной СМС, млн. долл.

Эффективность обслуживания в СМС определяется соотношением

$$\text{Э}_{\text{о}} = 1- [T_{\text{нс}} + T_{\text{бл}}]/100, \qquad (14)$$

где $T_{\text{нс}}$ – процент нарушения связи (ПНС) в абонентском канале (АК); $T_{\text{бл}}$ – процент блокировки (ПБл) АК [2]. В дальнейшем показатель $\text{Э}_{\text{о}}$ принимается равным 1, поскольку значения параметров $T_{\text{нс}}$ и $T_{\text{бл}}$ при сравнительном анализе принимаются постоянными.

Эффективность мобильности СМС определим следующим соотношением

$$\text{Э}_{\text{м}} = V_{\text{max}} / V_0, \qquad (15)$$

в котором V_{max} – максимальная допустимая скорость перемещения абонента в данной СМС, км/час; V_0 – эталонное значение показателя V_{max}, которое в данной работе принято равным V_0=1000 км/час.

Эффективность трафика СМС определим следующим соотношением

$$\text{Э}_{\text{т}} = N_{\text{т max}} / N_{\text{т0}}, \qquad (16)$$

где $N_{\text{т max}}$ – число видов трафика (мультисервисность), передаваемых в данной СМС; $N_{\text{т0}}$ – эталонное значение показателя $N_{\text{т max}}$, которое в данной работе принято равным $N_{\text{т0}}$=20.

Эффективность доставки трафика в СМС, обусловленная задержками передачи трафика на маршруте следования, определим соотношением

$$\text{Э}_{\text{з}} = \tau_{\text{з0}} / \tau_{\text{з max}}, \qquad (17)$$

в котором $\tau_{\text{з max}}$ – допустимая максимальная задержка доставки пакетов, мс; $\tau_{\text{з0}}$ – эталонное значение показателя $\tau_{\text{з max}}$, которое в данной работе принято равным $\tau_{\text{з0}}$=0,5 мс.

Таким образом, определены все необходимые расчетные соотношения, необходимые для получения количественных оценок показателей функционирования сравниваемых СМС по соотношениям (1)-(17).

Количественные оценки ХФ СМС4G и СМС5G

В связи с большой вариативностью исходных параметров в данной работе было решено ограничиться сравнением двух характерных вариантов построения СМС, рассматривая полученные результаты в качестве опорных данных для результатов более общего сравнения,

которое предполагается выполнить в процессе продолжения данной работы. Такой подход позволяет использовать такую простую и лаконичную форму представления результатов количественной оценки большого числа характеристик функционирования СМС, как табличная, и максимально акцентировать внимание на ключевых моментах.

В табл. 3 параметры сравниваемых СМС, которые использовались для получения количественных оценок для проведения сравнения ХФ.

Таблица 3

Параметры СМС4G и СМС5G, использованные для оценки ХФ

Параметр	**4G**	**5G**
Диапазон частот, ГГц	2,6	28
Ширина 1 радиоканала, МГц	100	500
Максимальная скорость передачи в радиоканале, Гбит/с	1,5	20
Вид модуляции (срединный)	16-КАМ	256-КАМ
Вид помехоустойчивого кодирования	Турбокод (LPDC)	Турбокод+ (LPDC+)
Максимальная конфигурация MIMO	4x4	64x8
Максимальная спектральная эффективность	15	40
Коэффициент скругления	0,25	0,15
Тип территории обслуживания СМС	БГ	БГ
Число абонентов, тыс. чел	300	300
Допустимый ПНС в АК, %	7	7
Допустимый ПБл в АК, %	3	3
Минимальная гарантированная скорость передачи абонентского трафика, Мбит/с	10	100
Примерная стоимость 1 БС, млн. долл.	0,12	0,2
Примерная стоимость ЦС, млн. долл.	1,5	2
Максимальная скорость абонента, км/час	350	500
Мультисервисность (кол-во видов трафика)	10	15
Максимальная задержка доставки информации, мс	5	1

В табл. 4 – приведены рассчитанные по приведенным выше соотношениям (1)-(17) основные технические и стоимостные показатели сравниваемых СМС. Кроме этого в табл. 4 включены значения ряда рабочих параметров, которые были приняты как условно оптимальные и использовались при расчетах, как например, конфигурации кластерно-секторной структуры ($M_{сек}$ x $N_{кл}$ x N_f)=3x3x1.

Таблица 4

Расчетные технические и стоимостные показатели сравниваемых СМС

Параметр	**4G**	**5G**
Площадь ТО, км^2	800	800
Высота антенн БС, м	45	45
Параметр глубины замираний, дБ	12	14
Конфигурация кластерно-секторной структуры	3x3x1	3x3x1
Абонентская нагрузка от 1 абонента, Эрл	0,075	0,09
Средняя спектральная эффективность	2,6	8
Средняя скорость передачи, Мбит/с	260	4000
Число каналов трафика в секторе	26	40
Число абонентов, обслуживаемых в 1 секторе	834	1149
Число сот/БС	360	262
Условная суммарная скорость передачи трафика в СМС, Тбит/с	3	30
Требуемая полоса радиочастот, МГц	300	1500

Допустимое ОСШ при $P_{ош\ доп}=10^{-2}$, дБ	22	28
Энергетические потери из-за неидеальностей, дБ	2	4
Энергетический выигрыш от помехоустойчивого кодирования, дБ	7	10
Энергетический запас на внешние помехи, дБ	5	8
Максимальное допустимое ОСШП при $P_{ош\ доп}=10^{-2}$, дБ	22	30
Общее число радиоканалов в СМС	1080	786
Пропускная способность СМС, Тбит/с	0,65	4,3
Стоимость СМС (∑БС+ЦС), млн. долл.	37	80,6

В табл. 5 представлены итоговые расчетные оценки эффективностей для СМС 4G и в табл. 6 - для СМС 5G, рассчитанные по соотношениям (1)-(17) для трех значений минимальной гарантированной скорости передачи абонентского трафика $R_{аб}$.

Таблица 5

Расчетные значения эффективностей СМС 4G

Э / СМС	$Э_ч$	$Э_э$	$Э_и$	$Э_с$	$Э_м$	$Э_т$	$Э_з$	Э
4G $R_{аб}$=5 Мбит/с	$1,6\cdot10^3$	48,9	5,1	0,52	0,43	0,58	0,18	$1,0\cdot10^4$
4G $R_{аб}$=10 Мбит/с	$3,3\cdot10^3$	44,1	4,6	0,24	0,43	0,58	0,18	$7,8\cdot10^3$
4G $R_{аб}$=30 Мбит/с	$5,0\cdot10^3$	34,2	3,5	0,12	0,43	0,58	0,18	$3,6\cdot10^3$

Таблица 6

Расчетные значения эффективностей СМС 5G

Э / СМС	$Э_ч$	$Э_э$	$Э_и$	$Э_с$	$Э_м$	$Э_т$	$Э_з$	Э
5G $R_{аб}$=50 Мбит/с	$3,3\cdot10^3$	20,7	7,5	0,41	0,62	0,88	0,9	$1,0\cdot10^5$
5G $R_{аб}$=100 Мбит/с	$6,6\cdot10^3$	19,2	6,9	0,2	0,62	0,88	0,9	$9,0\cdot10^4$
5G $R_{аб}$=150 Мбит/с	$1,0\cdot10^4$	13,6	4,9	0,1	0,62	0,88	0,9	$3,3\cdot10^4$

Сравнительный анализ ХФ СМС4G и СМС5G

Из табл. 5 и 6 видно, что все виды эффективностей функционирования СМС 5G, как и следовало ожидать, существенно превышают таковые для СМС 4G, если делать сравнение в абсолютном масштабе, т.е. в данном случае при одинаковых $R_{аб}$. Но даже и при относительном сравнении, т.е. при прямом сравнении значений соответствующих показателей, видно, что обобщенная эффективность функционирования СМС 5G примерно в (9…12) раз больше обобщенной эффективности функционирования СМС 4G. Конечно, практический интерес представляет именно сравнение характеристик функционирования в абсолютном масштабе и, как было отмечено ранее, бесспорное преимущество принадлежит СМС 5G.

Выводы

На основании полученных расчетных оценок характеристик функционирования, приведенных в табл. 5 и табл. 6, и сказанного выше, можно сделать следующие выводы:

1. Сравнение характеристик функционирования по критериям эффективности в относительном масштабе свидетельствует о более, чем на порядок, высокой эффективности СМС 5G по сравнению с СМС 4G.

2. Сравнение характеристик функционирования по критериям эффективности в абсолютном масштабе, очевидно, будет еще больше в пользу СМС 5G, чем указано в п.1,.

3. Количественное сравнение характеристик функционирования по критериям эффективности показывает безусловное преимущество технологии мобильной связи 5G перед технологией мобильной связи 4G в условиях их применения для организации мобильной связи.

Литература

1. *В.И. Попов, В.А. Скуднов.* Основы проектирования сотовых сетей мобильной связи. - М.: Горячая линия-Телеком, 2017. – 400 с., ил.
2. *М.С. Лохвицкий, А.С. Сорокин, О.А. Шорин*. Мобильная связь: стандарты, структуры, алгоритмы, планирование. - М.: Горячая линия-Телеком, 2018. - 264 с., ил.
3. *В. О. Тихвинский*. Сети подвижной связи третьего поколения: экономические и технические аспекты развития в России. – М.: Радио и связь, 2002. – 312 с., ил.
4. *А.Г. Зюко и др*. Помехоустойчивость и эффективность систем передачи информации. – М.: Радио и связь, 1985. – 272 с., ил.
5. *А.С. Сорокин*. Технические основы анализа ЭМС РЭС. – М.: МТУСИ, 2013. – 55 с., ил.

COMPARATIVE ANALYSIS OF 4G AND 5G MOBILE COMMUNICATION SYSTEMS FUNCTIONING EFFICIENCY

Kristina D. Morozova
Student of group ZMTT1701, MTUCI
mkd2016@bk.ru
Alexander St. Sorokin
MTUCI, PhD., associate professor of SiSRT department
alexorokin@rambler.ru

Keywords: *efficiency, functioning efficiency, mobile communications technology, mobile standard, communication system energy efficiency, communication system frequency efficiency, communication system information efficiency, communication system frequency bandwidth.*

The results of qualitative analysis of the current situation in the development of 5G mobile communication technology on the basis of information available at the moment in scientific and technical periodicals and on Internet sites are presented. The quantitative comparative evaluation of the characteristics of 4G mobile communication systems and 5G mobile communication systems using standard operating conditions for both, determined by the General system initial data, is performed. Quantitative assessment of the characteristics of mobile communication systems is based on a generalized criterion-the efficiency of operation. On the basis of the obtained results of quantitative comparison of the functioning characteristics, a number of prognostic conclusions about the influence of structural parameters on the efficiency of 5G mobile communication systems are made.

АЛГОРИТМ АУТЕНТИФИКАЦИИ В СЕТЯХ СВЯЗИ МОДЕРНИЗИРОВАННОЙ СИСТЕМЫ ЭНЕРГООБЕСПЕЧЕНИЯ SMART GRID

Бельфер Рувим Абрамович
МГТУ им. Баумана Н.Э., к.т.н. доцент
a.belfer@yandex.ru
Глинская Елена Вячеславовна
МГТУ им. Баумана Н.Э. ст. преподаватель
glinskaya-iu8@rambler.ru
Орлов Владимир Георгиевич
МТУСИ, к.т.н. доцент кафедры ТиЗВ
ovg250846@gmail.ru

Ключевые слова*: Advanced Metering Infrastructure, smart grid, аутентификация, информационная безопасность, уязвимости.*

Приведён анализ иерархического построения и угроз безопасности в усовершенствованной подсистеме счёта (Advanced Metering Infrastructure), используемой в модернизированной технологии современных энергосистем (smart grid). Рассмотрены механизмы защиты несанкционированного управления приборами, потребляющими электроэнергию, и дано описание алгоритма взаимной аутентификация между прибором - потребителем электроэнергии UD (User Device) и интеллектуальным счетчиком SM (Smart Meter).

Иерархическая инфраструктура и угрозы безопасности в AMI

Согласно утвержденной «Стратегии развития электросетевого комплекса Российской Федерации» в течение ближайших 10 - 15 лет России предстоит внедрять технологии, которые уже используются в сетевых комплексах развитых стран. В частности, предстоит внедрять технологии "умных" электрических сетей, позволяющих повысить пропускную способность и стабильность энергоснабжения, сократить потери и издержки на техническое обслуживание, учёт и тарификацию оплаты электроэнергии потребителями [1]. Advanced Metering Infrastructure (AMI) состоит из инфраструктуры связи и двух оконечных систем: интеллектуальных счетчиков SM (Smart Meter) на оконечной стороне потребления электроэнергии и системы расчета данных потребления электроэнергией MDMS (Meter Data Management System) на другой оконечной стороне. MDMS проводит обработку и вычисление информации, зарегистрированной в интеллектуальных счетчиках. Эти вычисления используются для расчета биллинга, проведения аудита и других задач управления и администрирования.

Иерархическая инфраструктура связи AMI состоит из трех уровней, каждый из которых включает односторонние функции сетей связи для передачи данных о потреблении электроэнергии пользователями и двусторонние функции для передачи различных команд. В соответствие с этими командами должно обеспечиваться: изменение режима нагрузки с установлением цены потребления электроэнергии; переключение источника генерации электроэнергии в том числе с возможностью использования возобновляемых солнечных или ветряных источников; включение или отключение энергообеспечения и др.)

- Самым нижним уровнем инфраструктура AMI является сеть домашней зоны HAN (Home Area Network), в которой счетчики SM осуществляют мониторинг потребления электроэнергии домашними бытовыми приборами (стиральная машина, ТВ, холодильник и др.). HAN может быть реализована на беспроводных и проводных технологиях сетей стандартов ZigBee, Ethernet и др. Данные в интеллектуальный счетчик SM, в отличие от существующих счётчиков типовых энергосистем, поступают от пользователей не один раз в месяц, а с интервалом порядка несколько секунд от предприятий, и с периодом до 15 минут от потребителей электроэнергии в жилых домах. Данная информация содержит приватные

данные потребителя электроэнергии, в частности его имя, адрес и др. Реализация атак злоумышленника в системе управления промышленного производства может привести к нарушению обеспечения электроэнергией, финансовым потерям, а также ухудшению репутации предприятия. Примером атаки на систему управления может быть передача нелегитимного сообщения на отключение, например, миллиона счетчиков. В промышленно-коммерческой сфере бизнеса вычисления на базе приватных данных интеллектуальных счетчиков таких показателей, как число работающих на предприятии сотрудников, объём производства продукции за определенный период времени и др. могут быть использованы конкурентами. Выявление этой информации может привести к финансовым потерям, так как, например, если компания знает, что ее конкуренты производят слишком большие объёмы продуктов, она может снизить цены на свою аналогичную продукцию.

- Данные потребления электроэнергии с нескольких HAN передаются в концентратор DCU (Data Concentrator Unit) сети зоны AMI верхнего уровня - NAN (Neighborhood Area Network). Сеть NAN доставляет данные от концентратора в сеть зоны AMI более высокого уровня - глобальную сеть WAN (Wide Area Network). NAN может быть реализована на беспроводных и проводных технологиях сетей Wi-Fi, на использовании сотовых сетей, сетей связи на линиях электропередачи PLC (Power Line Communication) и др;
- Сети нескольких NAN доставляют данные от концентратора в сеть зоны AMI более высокого уровня - глобальную сеть WAN (Wide Area Network). Данные потребления электроэнергией потребителей в SM поступают через сети NAN и WAN в MDMS. WAN может быть реализована на беспроводных и проводных технологиях сетей 3G/LTE, радиолиниях микроволнового диапазона, а также Ethernet.

Для сетей связи AMI характерны уязвимости, связанные с такими угрозам, как зашумление, “подслушивание“, атаки DDoS, “затопление” и др. [3]. Злоумышленник может “подслушивать” информацию HAN о потреблении электроэнергии и затем использовать для злонамеренных действий. Поэтому необходимы сильные механизмы шифрования для защиты данных от такого рода пассивных атаки. Для защиты этих данных от подмены необходимо использовать механизм аутентификации.

В NAN предусматривается защита угроз данных от HAN. Ущерб от реализации атаки на концентратор DCU, входящий в NAN, может быть таким же, как и в HAN с разницей в том, что если DCU скомпрометирован, то ущерб может быть более серьезным и выражаться в отключении электроэнергии одновременно у значительно большего числа потребителей.

Алгоритм взаимной аутентификации потребителя электроэнергии и интеллектуального счетчика

Во многих зарубежных, а так же в отечественных работах [2-4, 6-8] отмечается, что информационная безопасность (ИБ) в ИЭС представляет особенно сложную задачу. В частности, в AMI необходимо выполнять функцию защищенного от угроз управления приборами, потребляющими электроэнергию. В качестве механизма защиты необходима взаимная аутентификация между прибором - потребителем электроэнергии UD (User Device) и интеллектуальным счетчиком SM. Приведем описание предложенного в [5] алгоритма такой взаимной аутентификации для защиты от угроз ИБ управления приборами, потребляющими электроэнергию.

Удостоверяющий центр CA (Certificate Authority) in Smart Grid санкционирует MDMS выпускать сертификаты в UD и SM. В основу алгоритма положено использование инфраструктуры открытых ключей PKI (Public Key Infrastructure) и аутентификации на основе идентификатора ID. Такая аутентификация обеспечивает повышение информационной безопасности.

Взаимная аутентификация между потребителем электроэнергии и интеллектуальным счетчиком осуществляется в четыре этапа.

1. CA предоставляет функцию аутентификации MDMS.

- MDMS формирует запрос на аутентификацию (зашифрованное закрытым ключом MDMS его хэш, временное значение) и отправляет его в CA;
- CA после дешифрации открытым ключом MDMS принятого сообщения убеждается в достоверности идентификатора MDMS и отправляет в MDMS каталог сертификатов.

2. MDMS отправляет сертификаты в SM.
   - в SM имеется его сертификат;
   - SM формирует зашифрованное открытым ключом MDMS сообщение запроса на аутентификацию (идентификатор SM, суммированный по модулю 2 с хэшем закрытого ключа SM, временное значение, идентификатор SM) и отправляет в MDMS;
   - MDMS дешифрирует принятый запрос своим закрытым ключом, осуществляет аутентификацию SM, проверяя принадлежность идентификатора SM. MDMS генерирует новый сертификат;
   - MDMS отправляет новый сертификат в SM.
3. MDMS отправляет сертификаты в UD.
   - в UD имеется его сертификат;
   - UD формирует зашифрованное открытым ключом MDMS сообщение запроса на аутентификацию (идентификатор UD, суммированный по модулю 2 с хэшем закрытого ключа UD, временное значение, идентификатор UD) и отправляет в MDMS;
   - MDMS дешифрирует принятый запрос своим закрытым ключом, осуществляет аутентификацию UD, проверяя принадлежность идентификатора UD. MDMS отправляет новый сертификат в UD.
4. Взаимная аутентификация между SM и UD.
   - UD и SM обмениваются сообщениями запроса на аутентификацию;
   - UD и SM обмениваются собственными сертификатами, зашифрованными открытыми ключами. Сертификат UD шифруется открытым ключом SM и наоборот;
   - выполняется взаимная аутентификация UD и SM с дешифрацией сертификатов закрытыми ключами.

Выводы

Положения данного алгоритма могут быть использованы при создании имитатора сети ПД категории специального назначения с использованием центра эксплуатации сети. Эта работа с использованием учебного лабораторного стенда проводится на кафедре “Информационная безопасность” МГТУ им. Н.Э. Баумана по дисциплине “Защищенные сети связи” с привлечением студентов к самостоятельному проведению научных исследований.

Литература

1. *Воропай И.И., Осак А.Б*. Будущие электроэнергетические системы –тенденции и проблемы. // ЭЛЕКТРО. Электротехника. Электроэнергетика. Электрическая промышленность. 2015.№4. С. 2-4.
2. *М. Басараб, Р. Бельфер, Е. Глинская, Якушева Н.* Требования к инфраструктуре сетей связи в составе Smart Grid // Первая миля. №4. 2018. С.78-84.
3. Eric D. Knapp, Raj Samani, Joel Langill, Applied Cyber Security and the Smart Grid. Elsevier, 2013, P. 202.
4. *Sangji Lee; Jinsuk Bong; Sunhee Shin; Yongtae Shin*. A security mechanism of Smart Grid AMI network through smart devicemutual authenticatio. The International Conference on Information Networking 2014 (ICOIN2014). 2014. 592–595 pp.
5. *Rajiv. K. Bhatia; Varsha Bodade*, Defining the framework for wireless- AMI security in smart grid, 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, 1-5 pp.
6. *Орлов В.Г., Пушкарев А.В.* Перспективы развития мобильного видео // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 115-117.

7. *Гуров В.В., Орлов В.Г.* Обзор и сравнение протоколов mptcp и cmt-sctp // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 115-119.
8. *Пушкарев А.В., Орлов В.Г.* Эволюция технических средств формирования и доставки ТВЧ на мобильные терминалы пользователей // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 1. С. 11-16.

ALGORITHM OF AUTHENTICATION IN THE NETWORK OF COMMUNICATION OF MODERNIZED ENERGY SYSTEM SMART GRID

Ruvim Ab. Belfer
BMSTU, PhD., associate professor
a.belfer@yandex.ru
Elena V. Glinskaya
BMSTU, senior teacher
glinskaya-iu8@rambler.ru
Vladimir G. Orlov
PhD., associate professor, TaSB department, MTUCI
ovg250846@gmail.ru

Keywords: *Advanced Metering Infrastructure, smart grid,authentication, information security, vulnerabilities.*

An analysis of the hierarchical construction and security threats in the advanced account subsystem (Advanced Metering Infrastructure) used in the modernized smart grid technology is presented. Mechanisms of protection of unauthorized control of the devices consuming the electric power are considered, and the description of algorithm of mutual authentication between the device - the consumer of the electric power UD (User Device) and the intelligent counter SM (Smart Meter) is given.

РАЗРАБОТКА ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ИЗУЧЕНИЮ ВИРТУАЛЬНОЙ ТЕЛЕФОННОЙ СТАНЦИИ IP-АТС ASTERISK

Пелевин Илья Игоревич
Транспортная группа FESCO, ИТ-аудитор
ilya.pelyovin@gmail.com
Маликова Елена Егоровна
МТУСИ, к.т.н., доцент каф. ССиСК
emalikova@gmail.com

Ключевые слова: *IP-телефония, учрежденческая телефонная станция, показатели качества обслуживания, операционная система Linux, лабораторный комплекс, системы виртуализации.*

Статья посвящена разработке лабораторных работ на учебном комплексе для обучения студентов принципам функционирования виртуальной телефонной станции IP - АТС Asterisk. Лабораторный комплекс установлен на кафедре СС и СК. На базе данного комплекса были созданы четыре лабораторные работы, охватывающие как теоретические вопросы, так и типовые практические задачи, которые решают инженеры-связисты в процессе эксплуатации телефонных сетей. Рассмотрены четыре лабораторные работы, в которых исследуются параметры качества IP- телефонии, сигнальные протоколы и дополнительные виды обслуживания. Реализованная на данном лабораторном комплексе технология виртуализации является одной из важнейших технологий концепции Будущих сетей.

Введение

В настоящее время наиболее актуальной темой в инфокоммуникациях является применение технологий виртуализации и самоорганизующихся сетей для удовлетворения запросов клиентов, расширения спектра предоставляемых услуг и снижения стоимости владения телекоммуникационным оборудованием. Следуя сложившимся тенденциям, бизнес все чаще требует наличие у инженеров квалификации в современных способах организации связи. В сложившейся экономической и политической ситуации рынок труда нуждается в специалистах, способных не просто организовать связь, но и сделать это наиболее оптимальным образом, найдя баланс между критериями «быстро», «качественно» и «недорого».

Роль учреждений высшего образования в выпуске высококлассных специалистов не может быть переоценена. МТУСИ, как ведущий в стране университет, выпускающий связистов, должен быть оснащен передовыми технологиями для организации учебного процесса, в том числе современными лабораторными комплексами, в которых будущие инженеры связи будут формировать и совершенствовать свои навыки.

Цель работы

Целью данной работы являлось создание на кафедре «Сети связи и системы коммутации» МТУСИ лабораторного комплекса для изучения студентами принципов функционирования виртуальной телефонной станции IP - АТС Asterisk. Данная станция обеспечивает различные функции классических АТС, поддерживает протоколы VoIP, предлагает большой выбор функций, таких как IP- телефонию, голосовая почту, конференции и другие.

К данному лабораторному комплексу изначально предъявлялись следующие требования:

1. Надежность и управляемость.
2. Организация одновременной независимой работы 10 бригад студентов.
3. Интеграция с имеющимися оборудованием кафедры.
4. Возможность подключения оборудования различных производителей.

5. Поддержка протоколов SIP, IAX2, MGCP.

6. Возможность подключения софтфонов, в том числе под управлением мобильных операционных систем (Android, IOS, Windows Phone).

7. Низкая стоимость внедрения и эксплуатации лабораторного комплекса.

Особенную роль в разработке лабораторного комплекса сыграло последнее требование. Для снижения стоимости внедрения было принято решение максимально использовать технологии виртуализации и opensource-решения.

При выборе системы виртуализации из списка существующих технологий (KVM, Xen, VMWare ESXi, Proxmox, QEMU) учитывалась не только стоимость, но и такие параметры, как управляемость и надежность системы, а также требуемая квалификация обслуживающего персонала. В результате выбор был остановлен на гипервизоре Citrix XenServer 7.1.

Выбор модели виртуальной АТС также был непростой задачей. В настоящее время на рынке представлено несколько моделей виртуальных АТС, таких как Digium Asterisk, 3CX, FreeSwitch и openSIPS. Для организации учебного процесса необходимо, чтобы программная АТС была одновременно универсальной, полнофункциональной и простой в освоении. На эту роль идеально подошла АТС Asterisk [1, 5].

АТС Asterisk работает под управлением POSIX-совместимых систем, таких как GNU/Linux и семейства xBSD. В целях упрощения конфигурации была выбрана ОС Debian GNU/Linux 8 (Jessie).

Результаты работы

Структурная схема лабораторного стенда представлена на рисунке 1.

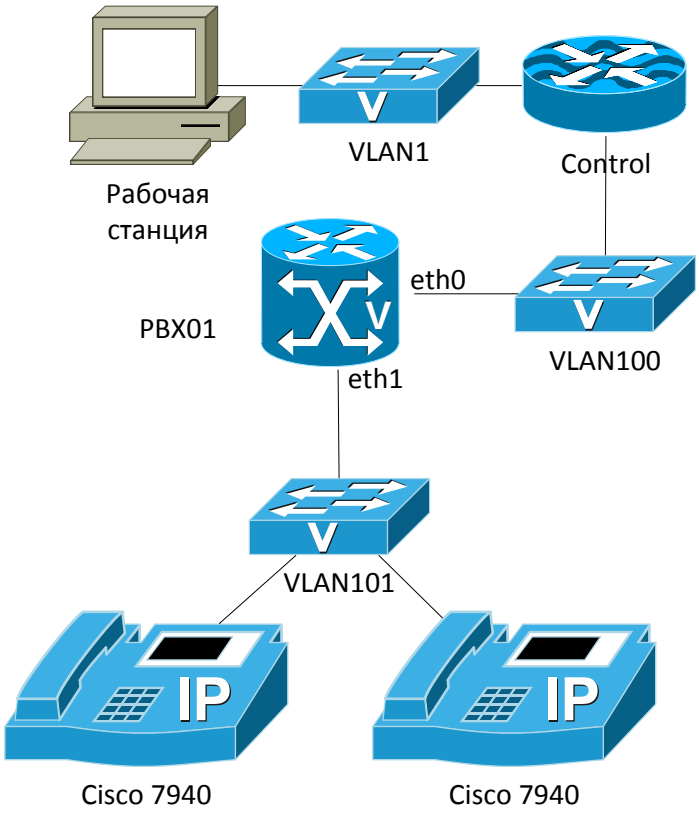


Рис. 1. Структурная схема лабораторного стенда

Стенд состоит из рабочей станции, виртуальной машины с установленной АТС, коммутаторов и двух IP-телефонов. Конфигурирование АТС осуществляется студентами с рабочей станции под управлением ОС Windows при помощи протокола SSH.

Таких стендов было сформировано 10. Стенды полностью независимые, и действия одной бригады студентов не влияют на работу остальных бригад. Схема всего лабораторного комплекса представлена на рисунке 2. Студентам предоставлены полные права на виртуальной машине с АТС, т.к. это необходимо для выполнения привилегированных операций, таких как снятие

трафика с сетевого интерфейса или перезапуск сервиса Asterisk. Таких стендов было сформировано 10. Стенды полностью независимые, и действия одной бригады студентов не влияют на работу остальных бригад.

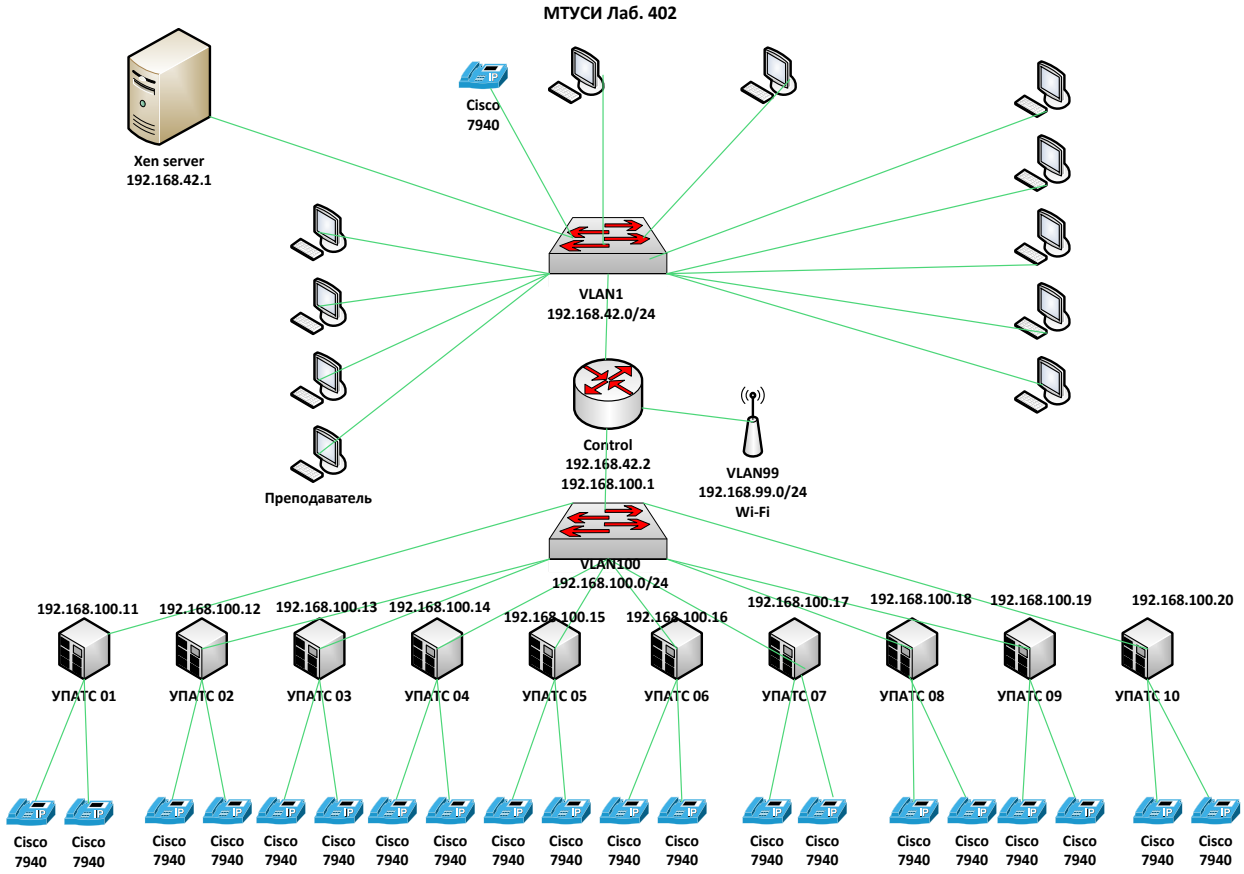


Рис. 2. Схема лабораторного комплекса

На данном комплексе были созданы четыре лабораторные работы, охватывающие как теоретические вопросы, так и типовые практические задачи, которые решают инженеры-связисты в процессе эксплуатации телефонных сетей.

Первая лабораторная работа знакомит студентов с основами работы в командной строке Linux и базовым конфигурированием АТС Asterisk. В этой же работе студенты изучают влияние параметров линии связи (задержка, джиттер и потери пакетов) на качество передачи голоса [2]. Студент должен определить при каких значениях этих параметров возможна разборчивая передача речевого сигнала.

Во ***второй лабораторной работе*** студенты выполняют коммутацию между абонентами разных АТС и изучают процесс прохождения сигнального и голосового трафика между ними. Далее они анализируют данный трафик с помощью программы анализатора трафика Wireshark, составляют стрелочные диаграммы IP-диалогов между телефонными аппаратами и АТС (рис. 3) и получают визуализацию аудиопотоков протокола RTP (рис. 4).

Третья лабораторная работа посвящена изучению языка программирования плана набора. Студенты строят по заданной блок-схеме план обработки вызовов и организуют голосовое меню и голосовую почту.

Четвертая лабораторная работа знакомит студентов с дополнительными видами обслуживания АТС Asterisk: конференц-связь, перевод и перехват вызова, парковка вызова и обработка исключительных ситуаций [4, 6]. Также через точку доступа Wi-Fi, которая имеется в данном лабораторном комплексе, студенты могут позвонить со своих смартфонов на телефонные аппараты лабораторного комплекса. Для этого каждой бригаде необходимо создать и настроить абонентов АТС Asterisk и создать учетные записи для подключения мобильных телефонов.

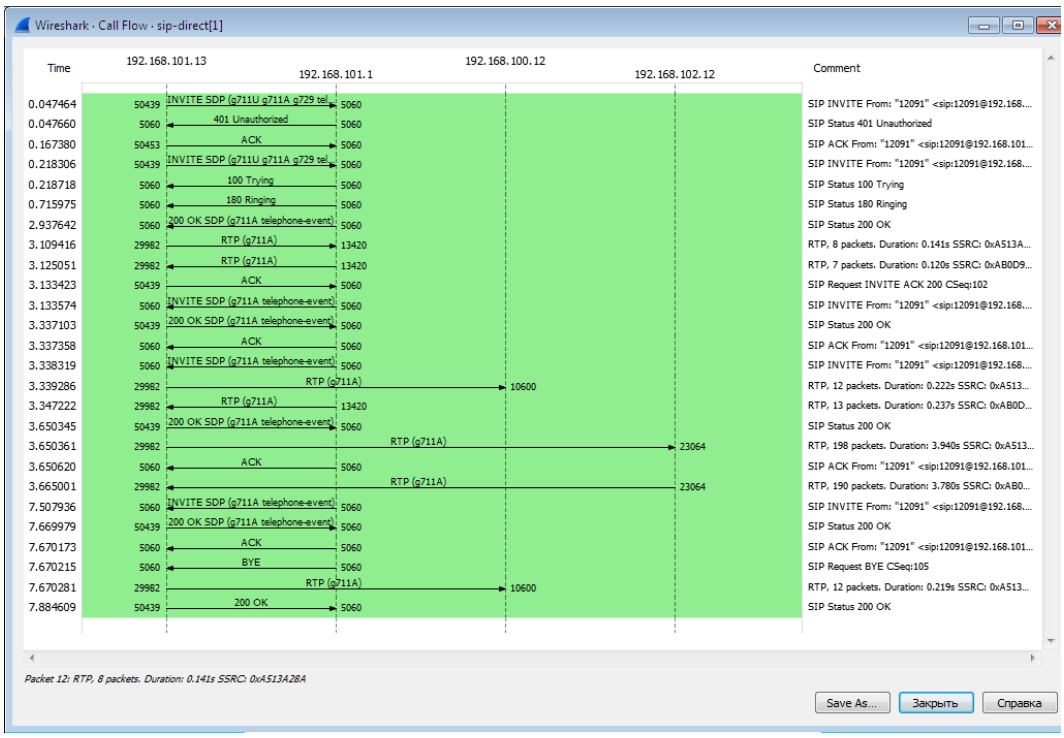


Рис. 3. Построение стрелочных диаграмм

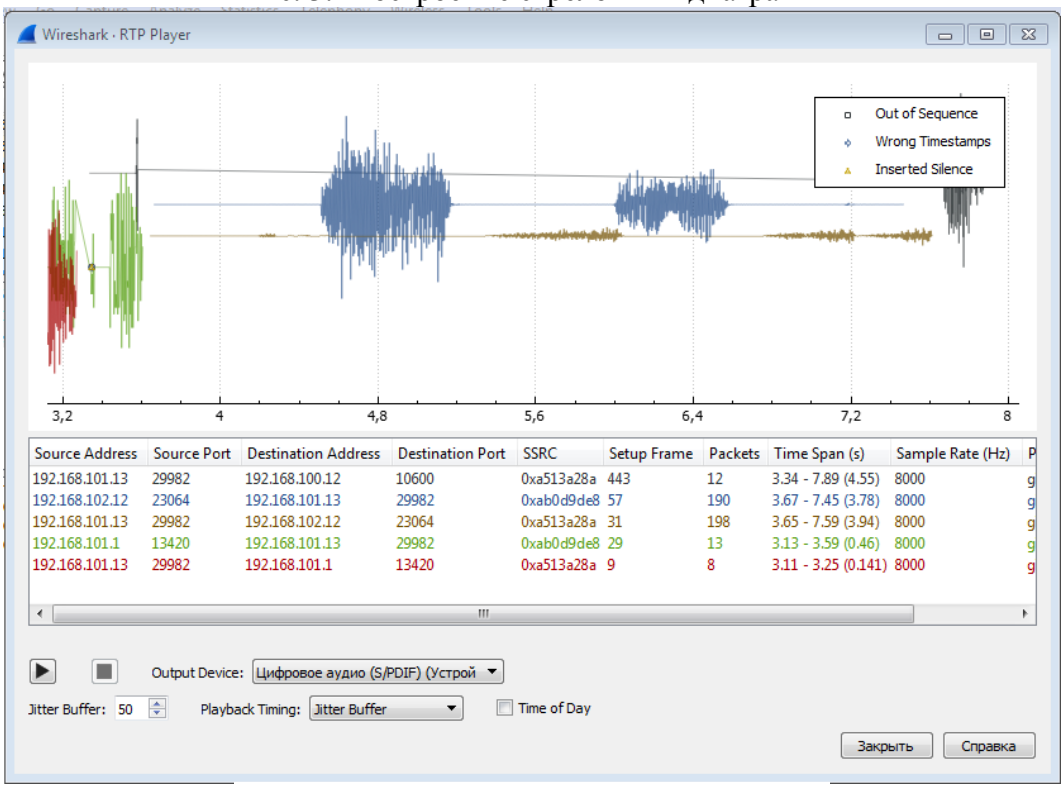


Рис. 4. Пример визуализации аудиопотоков

Заключение

Реализованная на данном лабораторном комплексе технология виртуализации является одной из важнейших технологий концепции Будущих сетей [3, 8 - 10]. Новый лабораторный комплекс предоставляет большие возможности по организации учебного процесса для изучения данной технологии. Выполняя лабораторные работы на данном комплексе, студенты не только знакомятся с технологиями пакетной коммутации, но и получают навыки работы с IP-АТС. Также работа с технологиями виртуализации способствует мотивации студентов максимально

использовать свой творческий потенциал и пробуждает интерес к самостоятельному изучению современных средств организации связи.

Данные работы выполняются студентами бакалавриата и магистратуры при изучении основных дисциплин кафедры СС и СК [7].

Литература

1. IP-PBX ASTERISK [Электронный ресурс].– Режим доступа: http://asterisk.ru/
2 Рекомендации МСЭ-Т Y.1541 (02/2006). Требования к сетевым показателям качества обслуживания.
3. *Росляков А.В*. Будущие сети (Future Networks) / *А.В. Росляков, С.В. Ваняшин*. – Самара: ПГУТИ, 2015. – 274 с.
4. *Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г.* Сети связи: Учебник для ВУЗов. СПБ.: БХВ-Петербург, 2014. - 400 с.
5. *Антонова В.М., Богомолова Н.Е., Маликова Е.Е.* О новом лабораторном практикуме по изучению виртуальной телефонной станции IP-АТС Asterisk // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 3. С. 20-22.
6. *Богомолова Н.Е., Маликова Е.Е.* Стратегия динамического опроса датчиков, установленных на промышленных объектах, с учетом их зависимого срабатывания // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 26-30.
7. *Маликова Е.Е.* Особенности преподавания дисциплины "системы коммутации" по направлению инфокоммуникационные технологии и системы связи // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2015. Т. 4. № 2. С. 245-249.
8 *Антонова В.М., Маликова Е.Е.* . Исследование взаимного влияния полезного и служебного трафика в сетях LTE // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 17-21.
9. *Антонова В.М., Маликова Е.Е.* Исследование эффективности совместной передачи разнородного трафика в соте сети LTE // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 22-25.
10. *Антонова В.М., Маликова Е.Е.* Метод адаптивной диспетчеризации нагрузки на фрагменте сети LTE // REDS: Телекоммуникационные устройства и системы. 2013. Т. 3. № 1. С. 34-35.

DEVELOPMENT OF LABORATORY PRACTICE ON THE STUDY OF VIRTUALIZED SOFTWARE IP-PBX ASTERISK

Ilya I. Pelyovin
FESCO Transportation Group, IT auditor
ilya.pelyovin@gmail.com
Elena E. Malikova
MTUCI, PhD., associate professor
emalikova@gmail.com

Keywords: *IP telephony, Voice over IP, private branch exchange, service quality ratings, Linux, virtualization technologies*

The proposed article is dedicated to development of laboratory works which are to be used in University educational process. The laboratory complex has been installed IN Network communications and switching technologies sub-faculty. The laboratory works built on the current complex comprehend a number of theoretical and practical typical TASKS which are solved by communications engineers in course of telephone networks exploitation. The article describes four laboratory works in which VoIP service quality ratings, signaling protocols, and additional service types are being investigated. Virtualization technologies being used in the laboratory complex appear to be a crucial aspect in the conception of Future Networks.

ОСНОВНЫЕ ПРИНЦИПЫ ВЫБОРА ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ ДЛЯ СТРОИТЕЛЬСТВА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

Утетлеу Баглан
магистр группы М61702МТУСИ
bagi_1995@mail.ru
Хромой Борис Петрович
МТУСИ, д.т.н., профессор кафедры МСиИИ
p_khromoy@rambler.ru

Ключевые слова*: единство измерений, Стратегия обеспечения единства измерений, метрологическое обеспечение, рефлектометрия, профиль, апертура, затухание, дисперсия.*

В настоящее время выпускается большое измерительных приборов оптического диапазона, которые широко рекламируются и рекомендуются к применению. Однако выбор оптимального комплекса приборов зависит не только от измеряемых параметров, но и от конкретной решаемой задачи. Среди них задача оптимального выбора комплекса приборов на различных этапах строительства ВОЛС, которая рассматривается в статье.

Построение ВОЛС связано с применением комплекса средств измерений (СИ), в состав которого должны входить СИ с определенными техническими и метрологическими характеристиками. Их выбор определяется параметрами, измеряемыми при построении линии. Эти параметры отличаются от параметров, относящихся к эксплуатационным измерениям. Так же они отличаются от параметров, измеряемых при производстве отдельных устройств и их лабораторных испытаний.

Перечисленные задачи решаются разными предприятиями, каждое из которых должно иметь определенный комплекс метрологического обеспечения (МО). Измерительные приборы, которые входят в состав МО, должны обеспечивать выполнение конкретных работ. Эти приборы могут измерять одинаковые физические величины, но должны иметь разные условия применения, разные погрешности в зависимости от этапов строительства и условий эксплуатации ВОЛС. Оптимальный выбор состава измерительного комплекса для выполнения различных этапов строительства и эксплуатации ВОЛС является актуальной задачей.

Актуальность решаемой задачи определяется тем, что оптоволоконные сети безусловно являются одним из самых перспективных направлений в области связи. Такие свойства, как высокая пропускная способность оптических каналов, невосприимчивость к электромагнитным полям, малые потери сигнала при передаче на большие расстояния, делают актуальной задачу построения новых волоконно-оптических линий связи. В настоящее время в оптическом диапазоне строятся новые междугородние и международные линии связи, магистральные, зоновые и локальные компьютерные сети.

Кроме соблюдения требований к нормам, принятых на разных уровнях, при разработке метрологического обеспечения ВОЛС необходимо учитывать положения определяемые законом «Об обеспечении единства измерений» РФ, принятым в 2008 г. [5] и принятой Правительством РФ «Стратегией обеспечения единства измерений в Российской Федерации до 2025 года». В этом документе ставится задача развития импортнонезависимых технологий и приборной базы, полностью обеспечивающей единство всех измерений в сфере госрегулирования. Эти документы следует учитывать при выборе средств измерений в состав метрологического комплекса.

Измеряемые параметры компонентов ВОЛС

Несмотря на особенности проведений измерений на различных этапах строительства и эксплуатации ВОЛС существуют общие параметры подлежащие измерению [1,3,4, 6 - 11]:

- мощность сигнала, на входе в линию, дБм;
- затухание сигнала в линии, дБ;
- длина волны (мкм);
- расширение (дисперсия) импульса в тракте, пс;
- ширина спектральной линии оптического излучения, нм;
- поляризационная модовая дисперсия, пс·км;
- комбинационное рассеяние, %.

Состав измерений и испытаний на различных этапах производства оптических кабелей (ОК), строительства и эксплуатации ВОСП представлены в таблице 1.

Таблица 1

Измеряемые параметры	Этапы производства, строительства, эксплуатации			
	Производство		Строительство	Эксплуатация
	Световод	Кабель		
Мощность излучения	+	+	+	+
Затухание общее	+	+	+	+
Затухание в соединениях	-	-	+	+
Дисперсия, полоса пропускания	+	+	+*	+**
Апертура, диаграмма направленности	+	+	+*	-
Профиль показателя преломления	+	+	-	-
Диаметр поля моды (одномодовый световод)	+	+	-**	-
Критическая длина волны (одномодовый световод)	+	+	-**	-
Переходное затухание	-	+	-	-
* - только при входном контроле и выборочно; ** - Подлежит уточнению.				

Первый этап измерений, который необходимо осуществить перед непосредственной прокладкой кабеля – ***входной контроль***. Входной контроль подразумевает измерения параметров и проверки на целостность нового кабеля, закупленного у изготовителя. Данные измерения необходимы для исключения вероятности прокладки кабеля с поврежденным оптическим волокном, или волокном, имеющим дефекты, которые могли появиться при изготовлении самого кабеля или при его транспортировке. Входной контроль подразумевает выявление таких повреждений, а также выявление волокон разной длины или волокон, имеющих длину, меньшую заявленной в паспорте кабельного барабана.

Существует несколько способов тестирования нового кабельного барабана. Наиболее эффективным является способ, основанный на применении оптического рефлектометра (ОР), что обеспечивает минимальное количество времени на измерения и дополнительного оборудования. ОР применяется при измерении величины удлинения ОВ.

Величина продольного удлинения, вызванного напряжением оптического волокна (ОВ) в оптическом кабеле (ОК) является важным параметром, который необходимо учитывать при его производстве, прокладке и эксплуатации. Длительное воздействие нагрузки вызывает микроповреждения, а затем и обрыв ОВ. Некоторые конструкции ОК или процессы его производства могут вызывать постоянное статическое напряжение в ОВ. Во время прокладки к ОК прикладываются значительные нагрузки, которые могут передаваться на само ОВ, приводя к его растяжению. Напряжение ОВ может возникнуть также из-за провисания ОК, проложенного по воздушным линиям.

В большинстве применяемых методов и устройств измерение изменения длины ОВ проводится не непосредственно, а путем определения времени распространения оптического сигнала в ОВ

Однако удлинение ОВ вызывает не только увеличение времени прохождения сигнала, а так же изменяется (уменьшается) показатель преломления ОВ. Поэтому для получения правильного значения изменения длины ОВ результаты измерения должны быть скорректированы. Время распространения сигнала t_1 в ОВ при нормальных условиях равно:

$$t_1 = \frac{L \cdot n}{c} \qquad (1),$$

где L - длина волокна, n - показатель преломления, c - скорость света. Если в результате воздействия нагрузки одновременно изменяются длина ОВ и показатель преломления, то время распространения становится равным:

$$t_2 = \frac{(L+\Delta L)(n+\Delta n)}{c} = \frac{L \cdot n + \Delta n + \Delta L \cdot n}{c} = \frac{L \cdot n}{c}(1+\frac{\Delta n}{n}+\frac{\Delta L}{L}) . \qquad (2),$$

где AL, An - изменение длины ОВ и показателя преломления, предполагается, что они малы по сравнению с L и n. Отсюда следует связь между изменением задержки и изменением длины ОВ

$$\Delta t = t_2 - t_1 = \frac{L \cdot n}{c}(\frac{\Delta n}{n}+\frac{\Delta L}{L}) = \frac{\Delta L \cdot n}{c}(1+\frac{\Delta n / n}{\Delta L / L}) , \qquad (3)$$

Формула (3) используется для оценки связи изменения длины волны и времени распространения испытательного сигнала.

Следующий этап измерений осуществляется при монтаже оптических линий (ОЛ). На этапе соединения строительных длин волоконно-оптической линии производится сварка оптических волокон. В настоящее время этот процесс полностью автоматизирован. Аппарат автоматически производит юстировку и сварку волокон. После того, как волокна будут сварены, необходимо определить потери на сварном соединении.

Современные аппараты для сварки используют два разных метода оценки потерь. В основу технологии аппаратов Fujikura положен метод зондирования сваренных волокон тестовым импульсом и последующим анализом отраженного сигнала, то есть аппарат проводит прецизионные измерения, по результатам которых выдается оценка сварного шва. Сварочный аппарат Ericsson использует технологию анализа геометрии сердцевин сваренных волокон по «горячим» снимкам. И в том и в другом случае результаты могут отличаться от тех, которые будут получены при использовании оптического рефлектометра, так как первый аппарат не обладает достаточным измерительным потенциалом, а второй не учитывает всех возможных изменений в структуре ОВ. Средние оценки затухания на сварном соединении, выдаваемые обоими сварочными устройствами составляют порядка 0,02 Дб.

После монтажа производится измерение затухания ОВ кабеля в обоих направлениях передачи и полученные данные заносятся в паспорт. Результаты измерений должны соответствовать предельным значениям затуханий длин и стыков, измеренным в процессе строительства. Кроме того, на смонтированном участке измеряют затухание стыков ОВ в двух направлениях. Осуществляется также регистрация характеристик обратного рассеяния каждого из ОВ кабеля в двух направлениях с тщательной привязкой их к трассе прокладки ОК.

Следующий этап строительства предусматривает приемосдаточные измерения. Приемка смонтированного и настроенного оборудования ВОСП производится в соответствии с требованиями, изложенными в строительных нормах и правилах. Объем выборочных измерений

может изменяться приемной комиссией. Если при выборочных измерениях хотя бы один из параметров не соответствует норме, проводится 100% проверка.

В результате рассмотрения видов измеряемых параметров при строительстве ВОЛС можно перечислить основные измерительные приборы необходимые для выполнения работ. В основном, эти приборы используются для измерения параметров пассивных компонент в состав которых: мультиплексоры, демультиплексоры, разветвители, ответвители, разделители, аттенюаторы, изоляторы, переключатели, коммутаторы, пассивные компенсаторы дисперсии, коннекторы, соединительные муфты, ремонтные вставки. Измерение параметров пассивных компонент при строительстве осуществляется двумя приборами: источником излучения и измерителем оптической мощности.

Другим важным компонентом ВОЛС является кабель. При строительстве важным измеряемым параметром является длина кабеля, величина удлинения ОВ, качество сварного соединения. Перечисленные параметры измеряются с помощью оптического рефлектометра.

Поверка и калибровка компонентов ВОЛС

При строительстве ВОЛС, важное значение имеет задача обеспечения высокого качества оборудования. В состав оборудования: передающие устройства, оптические усилители, приемники света, оптические модуляторы, разветвители, фильтры и другие устройства. Кроме того, важное значение имеют метрологические характеристики измерительных приборов, применяемых в процессе настройки оборудования. Например, величина погрешности измерителя мощности может привести к недопустимому отклонению уровня затухания линии. По этой причине в процессе строительства ВОЛС необходимо применять поверку и калибровку используемых компонентов и средств измерений.

Выполнение этих работ необходимо проводить при определенных условиях, среди которых важное значение имеет выполнение следующих норм:

- температура окружающего воздуха должна быть (20 ± 5) °С;
- относительная влажность воздуха (60 ± 15) %;
- атмосферное давление (100 + 4) кПа.
- питание от сети переменного тока напряжением (220 ± 4,4)В, с частотой (50 ± 0,5)Гц.

Перед проведением поверки должны быть выполненные подготовительные работы в соответствии требованиями эксплуатационной документацией на поверяемый (калибруемый) прибор.

Поверка и калибровка измерительных приборов обычно осуществляется специализированными организациями. Однако поверка параметров оборудования, входящего в состав ВОЛС осуществляется строителями в процессе проведения работ.

Литература

1. *Портнов Э.Л.* Волоконная оптика в телекоммуникациях. – М,: Горячая Линия – Телеком, 2018– 391 с.

2.*Хромой Б. П.* метрология и измерения в телекоммуникационных системах (Том 2) – М.: ИРИАС 2008. – 560 с.

3.*Портнов Э. Л.* Оптические кабели связи и пассивные компоненты волоконо-оптических линий связи// М.: Горячая линяя – Телеком, 2007.

4. *Портнов Э.Л.* Оптические кабели связи их монтаж и измерение. – Горячая линия – Телеком, 2012. – 488 с.

5. Федеральный закон РФ № 102 от 26.06.2008 г. “Об обеспечении единства измерений”.

6. *Аджемов А.С., Хромой Б.П.* Обеспечение единства измерений хроматической дисперсии в оптическом волокне // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 8-10.

7. *Аджемов А.С., Хромой Б.П.* Электросвязь и оптика в историческом плане // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 2. С. 71-79.

8. *Портнов Э.Л., Григорьян А.К.* Поляризационная модовая дисперсия на волоконно-оптической линии передачи // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 62-64.

9. *Портнов Э.Л., Фатхулин Т.Д.* Анализ разрабатываемых технологий для достижения максимальных скоростей передачи информации в современных DWDM системах // REDS: Телекоммуникационные устройства и системы. 2015. Т. 5. № 2. С. 177-179.
10. *Портнов Э.Л.* Новый подход в определении параметров передачи и влияния в оптических линиях телекоммуникаций // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 5. С. 60-63.
11. Портнов Э.Л., Мариносян Э.Х. Определение отношения сигнал/шум для высокоскоростных систем передачи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2013. № 1. С. 139-141.

MEASURING COMPLEX TO BUILD FIBER-OPTIC LINES

Ytetleu Baglan
master of group M61702 MTUCI
bagi_1995@mail.ru
Boris P.Khromoy
MTUCI, Dr., professor of department MSaII
p_khromoy@rambler.ru

Keywords: *The unity of measurements, The strategy of ensuring the uniformity of measurements, обеспечение, metrological assurance, reflectometry, profile, aperture, attenuation, dispersion*

Currently available a large number of measuring instruments optical range, that are widely advertised and recommended. . However, the selection of the optimal set of instruments depends not only on measurable parameters, but also on the specific problem to be solved. Among them the problem of optimal choice of complex devices in various stages of construction of Fiber-optical communication line (FOCL), which is considered in the article.

РАСЧЕТ СТАЦИОНАРНЫХ ВЕРОЯТНОСТЕЙ СОСТОЯНИЙ МНОГОКАНАЛЬНОЙ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ В ДИСКРЕТНОМ ВРЕМЕНИ С КОНЕЧНЫМ ЧИСЛОМ ИСТОЧНИКОВ ЗАЯВОК И ОТКАЗАМИ

Курский Владислав Викторович
студент группы ЗМПП1601 МТУСИ
kurskiyv@gmail.com
Таташев Александр Геннадьевич
МТУСИ, д.ф-м.н., профессор кафедры МКиИТ
a-tatashev@yandex.ru

Ключевые слова: *системы массового обслуживания, многоканальные системы, конечные источники заявок, стационарное распределение числа заявок в системе, имитационное моделирование.*

Рассматривается система массового обслуживания, работающая в дискретном времени. Имеется n источников заявок. На любом такте каждый источник находится в одном из двух состояний — состоянии генерации заявки и состояния обслуживания заявки, посланной источником на обслуживание. Каждый источник с некоторой вероятностью, зависящей от источника, посылает заявку на обслуживание, если он находился в состоянии генерации, или с некоторой вероятностью, зависящей от приемника принявшего заявку, ожидает окончания обслуживания заявки. Предложена эквивалентная имитационная модель. Описаны процедуры генерации имитационной модели. Подтверждено ее соответствие теоретическим вычислениям.

Повышенное внимание к изучению систем массового обслуживания в последние десятилетия обусловлено тем, что такие системы описывают и формализуют работу многокомпонентных ассамблей взаимодействующих между собой элементов с разным временем обработки поступающего задания. Особый интерес вызывают системы массового обслуживания с дискретным временем [6]. В них переход из одного состояния в другое происходит в целочисленные моменты времени (такты). Рассмотрение подобных систем подходит для анализа многих разделов связанных с работой цифрового оборудования ввиду того, что дискретный подход является естественным для любых современных технических систем. Классическим сопряженным с СМО прикладным направлением являются телекоммуникационные системы.

В данной статье проводится исследование многоканальной системы массового обслуживания в дискретном времени с конечным числом источников заявок. Пусть имеется некоторое число источников заявок $n_и$ и соответствующее ему число обслуживающих приборов $n_п$. В любой момент времени каждый из источников (s) может находиться в одном из двух взаимоисключающих статусов – генерация заявки ($s_г$) или ожидание окончания обслуживания посланной им заявки ($s_{ож}$). На каждом такте работы системы выбирается некоторый набор из m источников, которые могут сменить свой статус на противоположный с вероятностью, зависящей от источника и его текущего статуса. Предложены расчетные формулы для вычисления стационарного распределения обслуживаемых заявок и рассмотрена соответствующая имитационная модель.

Описание системы

Формализуем рассматриваемую систему массового обслуживания в дискретном времени. Источнику $_i$ соответствует прибор с тем же номером i, $i = 1, \ldots, n$, $n_и=n_п$. В каждый момент времени выбирается набор, состоящий из m источников, статус которых может измениться, выбор источников происходит равновероятно независимо от статуса конкретного источника и от предыдущего выбора. Предположим, что в момент времени t источник i принадлежит такому набору. Его состояние в момент времени t+1 описывается следующим образом:

$$s(t+1)=\begin{cases} s_{ож}, \text{с вероятностью } 0<\lambda_i<1, & \text{при условии } s(t)=s_г \\ s_г, \quad \text{с вероятностью } 0<\mu_i<1, & \text{при условии } s(t)=s_{ож} \end{cases}$$

Смена состояния *i*-го источника означает поступление/окончание обслуживание заявки на *i*-ом приборе соответственно. Пусть $\rho_i = \lambda_i/\mu_i < 1$.

Стационарные вероятности состояний

Пусть вектор $X(t) = (x_1(t), \ldots, x_n(t))$ характеризует состояние системы в момент $t = 0, 1, 2, \ldots$, где $x_i(t) = 0$, если в момент t, i-й источник генерирует заявку и $x_i(t) = 1$, если в момент t i-й прибор обслуживает заявку, $i = 1, \ldots, n$. Случайный процесс $X(t)$ является цепью Маркова с конечным множеством состояний, причем всё множество состояний образует непериодический класс сообщающихся существенных состояний и, следовательно, [1], цепь эргодична.

Обозначим через $P(x_1, \ldots, x_n)$ стационарную вероятность состояния ($X_1(t) = x_1, \ldots, x_{n,,}$ где $x_i(t) = x_i$). Обозначим через A_k множество состояний, таких, что $x_1 + \cdots + x_n = k$.

Стационарная вероятность P_k того, что в системе обслуживается ровно k заявок, равна:

$$\sum_{A_k} P(x_1, \ldots, x_n)$$

(суммирование по множеству A_k), при этом:

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{n} p_i^{x_i} \Big/ \sum_{u=1}^{z} \prod_{i=1}^{n} p_j^{x_j} \qquad (1)$$

Доказательство представлено в [2].

Алгоритм для вычисления стационарных вероятностей

Все алгоритмы реализованы в среде *Matlab* 2017*b*.

Модуль в [3] отвечает за инициализацию массивов для последующей работы и обработки: генерируются массивы размером n содержащие численное значение λ, μ со строгим условием $\lambda > \mu$ и вычисляется p для всех n приборов. В дальнейшем, массивы λ и μ будут использоваться для составления имитационной модели.

Команды, представленные в [4], отвечают за вычисление численных значений стационарных вероятностей состояний, в результате возвращается массив, значения индексов которого соответствуют значению количества заявок в системе, а значения элементов вероятность этого состояния.

Сущность алгоритма представляет собой последовательность следующих этапов:

1. Создается массив, содержащий вычисленное значение числителя для всех состояний, одновременно с этим подсчитывается знаменатель (формула 1);
2. Затем вычисляется частное для каждого состояния по формуле 1;
3. Далее происходит создание массива, индекс которого – количество заявок, а значение соответствующего элемента представляет собой сумму стационарных вероятностей таких состояний, чтобы $x_1 \ldots + x_n = i$, где x_i – соответствующий прибор, i - число заявок;
4. Отдельно добавляется стационарная вероятность нахождения 0 заявок в системе;
5. Результатом работы алгоритма является массив с размерностью n+1, индексы которого представляют собой число заявок в системе +1(это обусловлено тем, что в *Matlab* индексация начинается с 1), а значение элемента — стационарная вероятность данного состояния;

Сложность алгоритма $O(2^n)$ (относится к классу алгоритмов с экспоненциальной сложностью), где n — количество источников.

Описание имитационной модели и алгоритма для генерации модели с произвольным количеством приборов и источников заявок

Имитационная модель создавалась с использованием средств *Matlab Simulink*. Для композиции имитационной модели удобно ввести понятие «модуля», состоящего из цепи последовательно соединенных ключевых элементов: генератор заявок(*EntityGenerator*); два

обслуживающих устройства(*EntityServer*), при этом первое обслуживающее устройство представляет собой корректный источник заявок, т.е. в последовательно соединенной цепи заявка существует строго одна(либо ее не существует вовсе); конечный пункт для заявок(*Terminator*).

Так же, имеются дополнительные элементы: ворота(*EntityGate*, открытые при запуске симуляции и пропускающие ровно одну заявку при каждом запросе на открытие), между генератором заявок и первым прибором; функция, ответственная за передачу сообщения воротам для их открытия, если заявка поступила в конечный пункт и наступило время начала генерации новой заявки; вспомогательная функция, генерирующая случайную величину с геометрическим распределением (общая для всех приборов). Генератор заявок инициализирует каждую заявку следующими атрибутами: lambda, mu и вычисляет время обработки заявки на первом и втором сервере соответственно. *EntityGenerator* генерирует заявки в каждый бесконечно малый момент времени работы симуляции (*period* =0). Схема модуля представлена на рисунке 1.

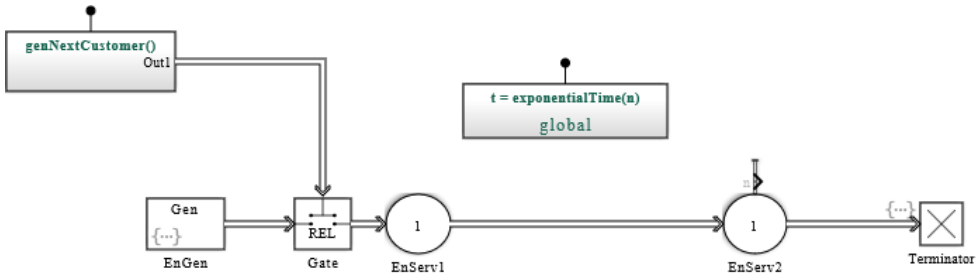


Рис. 1. Схема модуля.

Процедура [5] для генерации имитационной модели, использует описанный выше “модуль” в качестве готовой схемы, копирую все элементы, связывая их между собой и передавая необходимые значения атрибутов. Так же, добавляется сумматор (*Adder*), используемый для определения количества заявок во всех “вторых” приборах в системе и элемент, отвечающий за сохранение результат работы системы для последующей обработки(*out*).

Типовая схема представлена на рисунке 2.

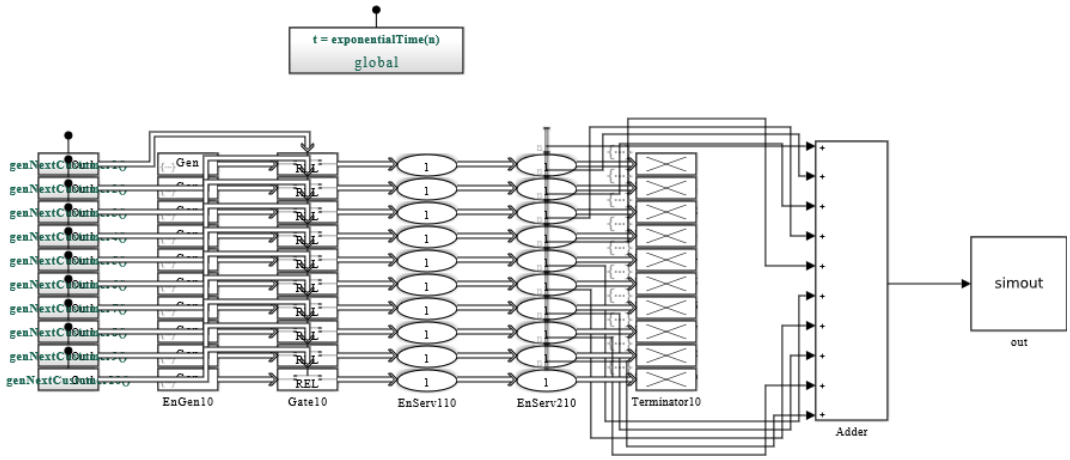


Рис. 2. Имитационная модель для *n*=10.

Результаты

В таблице 1 содержатся результаты сравнения имитационной модели и теоретической формулы, а именно среднеквадратической ошибки для стационарных вероятностей, полученных по формуле относительно полученных данных при работе имитационной модели. Видно, что формула точно предсказывает работу модели: в среднем среднеквадратическая ошибка для каждой смоделированной выборки не превышает 10^{-7} и полностью объясняется случайностью происходящего процесса. Моделирование имитационной модели происходило 10 раз для каждого n, в каждом из которых генерировалась новая модель со случайными свойствами. Время моделирования 300.000 относительных временных единиц.

Таблица 1

Оценка соответствия имитационной модели относительно математической.

n	3	4	5	6	7	8	9	10	11
MSE_{max}	2.9e-06	8.7e-07	5.9e-07	6.3e-07	4.9e-07	4.6e-07	3.4e-07	5.7e-07	1.0e-06
MSE_{min}	2.5e-07	1.0e-07	8.5e-08	5.0e-08	1.0e-07	4.7e-08	4.8e-08	1.5e-08	1.9e-08
MSE_{mean}	9.7e-07	3.61e-07	2.6e-07	2.4e-07	2.7e-07	1.7e-07	1.4e-07	1.7e-07	1.6e-07

Заключение

В данной работе была описана и рассмотрена система массового обслуживания с дискретным временем и конечным числом заявок, а также предложена эквивалентная схема имитационной модели, установлено ее соответствие математической модели.

Литература

1. *Бочаров П.П., Печинкин А.В.* Теория массового обслуживания. М.: Изд-во РУДН, 1995.
2. *Таташев А.Г., Курский В.В.* Многоканальная система массового обслуживания в дискретном времени с конечным числом источников заявок. Сборник трудов XII Международной научно–технической конференции «Технологии информационного общества». Том 2. М.: ИД «МедиаПаблишер», 2018.
3. Электронный ресурс *https://github.com/KurskiyVladislav/SMO/blob/master/MyInit.m*
4. Электронный ресурс *https://github.com/KurskiyVladislav/SMO/blob/master/MyCalcStProb.m*
5. Электронный ресурс https://github.com/KurskiyVladislav/SMO/blob/master/Model.m
6. *Таташев А.Г., Ахильгова М., Щебуняев С.А.* Дискретная многоканальная система массового обслуживания с отказами и групповым поступлением заявок // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 7. С. 23-26.

CALCULATION OF STATIONARY DISTRIBUTIONS OF STATES IN MULTI-CHANNEL QUEUEING SYSTEM IN DISCRETE TIME WITH LIMITED SOURCES OF CUSTOMERS WITH LOSSES

Vladislav V. Kurskiy
Student of groupZMPP1601 MTUCI
kurskiyv@gmail.com
Alexander G. Tatashev
MTUCI, D.Sc., professor of MCaIT department
a-tatashev@yandex.ru

Keywords: *Queueing systems, multi-channel systems, limited sources of customers, stationary distributions of number of jobs in system, mathematical simulation.*

We analyze a discrete-time queueing system. In this model there are *n* sources of customers (jobs). On any tick in which system works, every source is in one of two states: one is generating of the job and another one is waiting for the job is done. Any source with some probability, determined by the attributes of the source, will be sending job to the receiver, if one in generating state, or will be waiting for the job is done, with probability determined by the receiver, if one in waiting state. In this article we propose equivalent simulation model, describe generating procedures and confirms that our model is valid.

ОЦЕНКА ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ ПОВЫШЕНИЯ СКОРОСТИ ПЕРЕДАЧИ В ТРОПОСФЕРНЫХ СИСТЕМАХ СВЯЗИ

Гричаненко Виолетта Геннадиевна
студент группы ЗМТТ1601 МТУСИ
viola-grichanenko@mail.ru
Жарихина Людмила Вячеславовна
студент группы ЗМТТ1601 МТУСИ
viola-grichanenko@mail.ru
Сорокин Александр Степанович
МТУСИ, к.т.н., доцент кафедры СиСРТ
alexorokin@rambler.ru

Ключевые слова: *тропосферная связь, тропосферный канал, многолучевое распространение, медленные замирания радиосигнала, быстрые замирания радиосигнала, разнесенный прием, OFDM, MIMO, интегральная функция распределения*.

В статье получены количественные оценки (возможной скорости передачи и соответствующих ей допустимых значений дальности связи, мощности передатчиков и диаметра антенн) в тропосферных системах связи при использовании в них современных информационных технологий таких как: *OFDM, MIMO* и многоуровневая модуляция, в сочетании с базовыми тропосферными радиотехнологиями (разнесенный прием) и типовыми технологиями, используемыми в современных системах связи, к числу которых относится помехоустойчивое кодирование. При получении количественных оценок в качестве условно оптимальной максимальной скорости передачи принималась скорость (80…100) Мбит/с, в соответствии с которой рассчитывались допустимые значения основных параметров тропосферного радиоканала – его протяженность (длина), мощность передатчика и диаметр приемной и передающей антенн (который принимался одинаковым для обеих антенн). Расчеты в соответствии с типовой методикой планирования тропосферной связи проводились для худшего периода времени (зима) для частот 1,5 ГГц и 5 ГГц. При этом для всех вариантов расчетов использовались постоянные значения коэффициента шума приемника (2 дБ) и потерь в приемном и передающем антенно-фидерных трактах (1 дБ).

В настоящее время тропосферные системы связи (ТСС) обретают “новое дыхание” в связи с возможностями повышения их эффективности за счет использования современных информационных технологий, включающих, прежде всего, современные радиотехнологии, такие как *MIMO* и *MMIMO* (мульти-*MIMO*, то есть *MIMO* большой размерности), а также многократный разнесенный прием (МРП) [1]. Имеются примеры реализации перечисленных технологий в ТСС военного назначения за рубежом при очень ограниченной информации о них: в основном все сводится максимальной скорости передачи порядка 120 Мбит/с, которую можно принимать в качестве некого ориентира для анализа возможностей повышения скорости передачи на настоящий момент.

В нашей стране актуальность ТСС связывается с программами широкого освоения Арктического региона и территорий Крайнего Севера [3]. При этом имеются планы фактически восстановления легендарной сети тропосферных РРЛ “Север”, общая протяженность которой составляла более 13000 км, но, очевидно, на современном технологическом уровне.

Цель работы – проведение количественного анализа возможностей повышения скорости передачи в ТСС при использовании в них современных информационных технологий, а именно: технологии *OFDM* в сочетании с глубоким перемежением символов, помехоустойчивого каскадного кодирования (ПКК) в конкатенации сверточного кода и кода с малой плотностью

проверок на четность (*LDPC*), радиотехнологии МРП порядка 4…16 и технологии *MIMO* размерностью 4x4.

Особенности характеристик тропосферного канала

В тропосферном канале распространение волн происходит за счет их рассеяния на неоднородностях в верхних слоях тропосферы на высотах (12…15) км [1]. Такие неоднородности имеют примерно шаровидную форму и их называют глобулами. Каждая глобула является вторичным источником радиосигнала, переизлученного в точку приема; при этом доля переизлученного сигнала относительно первичного сигнала крайне низкая и составляет 10^{-6}…10^{-8}, т.е. радиосигнал ослабляется в (1…100) млн. раз по мощности.

В формировании радиосигнала в точке приема принимают участие глобулы, находящиеся в так называемом объеме рассеяния (ОР), который образуется за счет пересечения диаграмм направленности антенн (ДНА) передатчика и приемника. Поток переизлученной энергии радиоволн в направлении точки приема, как было установлено экспериментально и доказано теоретически, является неоднородным и состоит из группы лучей, число которых может меняться в зависимости от протяженности трассы тропосферного канала и ширины ДНА в пределах 1…20 [4].

В силу указанных особенностей механизма распространения радиоволн в тропосферном канале для него характерно наличие огромного среднего ослабления радиосигнала, доходящего до 230 дБ, и глубоких гладких и селективных замираний до 50 дБ. Безусловно, это является определенной проблемой при использовании технологии тропосферной связи [1, 4]. Наибольшую проблему представляют селективные замирания, так они ограничивают ширину полосы частот радиоканала и, соответственно, максимальную скорость передачи по нему.

Большие средние потери сигнала в тропосферном канале вызывают необходимость применения антенн достаточно больших размеров, а также передатчиков большой мощности и приемных устройств с очень низким коэффициентом шума. Так в современных ТСС широко применяются параболические антенны диаметром (3…7) м, передатчики мощностью до (3…5) кВт и приемники с коэффициентом шума (2…4) дБ [1].

Способы борьбы с селективными замираниями в ТСС

Традиционным способом борьбы с селективными замираниями являлся и является разнесенный прием (РП), который реализуется в различных видах и с различной кратностью [4]. Ниже перечислены типовые виды РП и отмечены их основные свойства:

- пространственный (в горизонтальной плоскости) РП (ПРП); необходимая величина разнесения антенн составляет 150λ;

– угловой (в вертикальной плоскости) РП (УРП);

– пространственно-частотный (в горизонтальной плоскости) РП (ПЧРП); расширяет используемую полосу радиочастот;

– пространственно-угловой РП (ПУРП); является сочетанием первых двух, перечисленных выше видов РП.

Кратность РП может обычно составляет от 2 или 4, но в настоящее время имеется тенденция ее повышения [1]. Следует особо отметить, что РП помимо подавления селективности существенно уменьшает также и средние потери сигнала при распространении [4].

В современных системах радиосвязи и в том числе в ТСС основным способом устранения влияния селективных замираний стало применение технологии *OFDM* с временным защитным интервалом [1-3].

Структура тропосферного канала с применением технологии MIMO/МРП

Повышение эффективности перспективных ТСС связывается с совместным применением технологий МРП и *MIMO*, а в дальнейшем *MMIMO* [1-3].

На рис. 1 и 2 показана упрощенная физическая структура тропосферного канала в вертикальной и горизонтальной плоскости, соответственно, с использованием радиотехнологий MIMO размерностью 4x4 и 16-ти кратного ПРП (16-ПРП) и вариант 32-х кратного ПУРП (32-ПУРП).

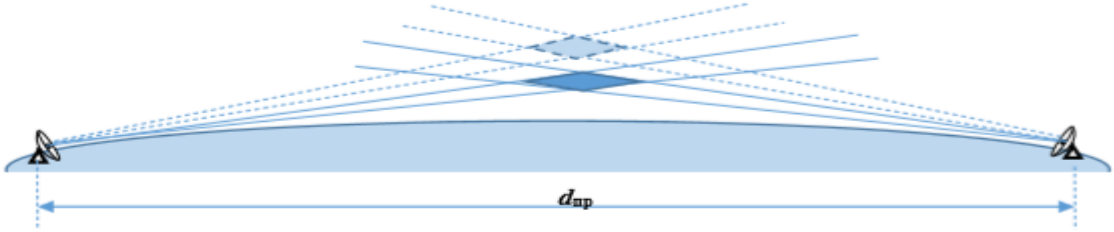


Рис. 1. Структура тропосферного канала в вертикальной плоскости (для одной пары антенн)

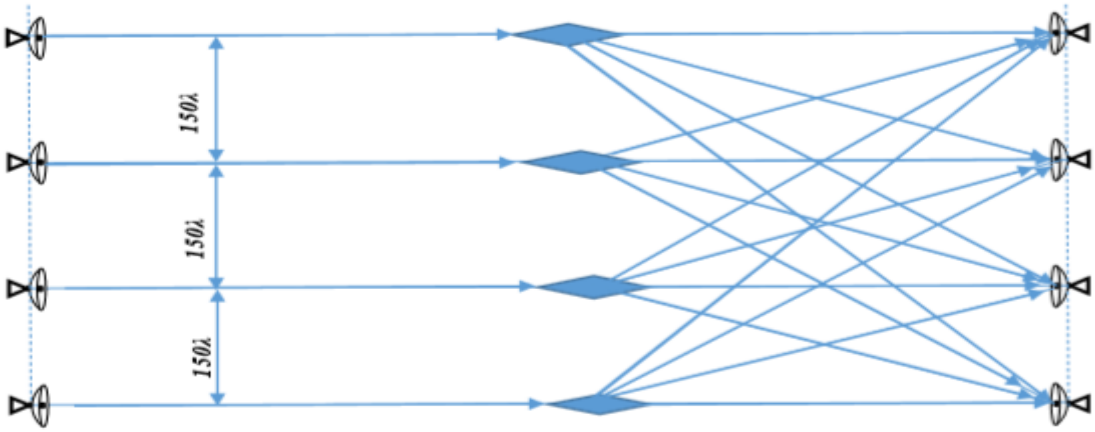


Рис. 2. Структура тропосферного канала (в плане) с применением 16-ПРП и технологии MIMO 4x4 для одного направления связи

На рис. 1 изображены два варианта структуры: - без РП (нижняя часть трассы); - с УРП, при котором дополнительно организуется еще один ОР (показано пунктиром). Дополнительно можно отметить, что структура канала, показанная на рис. 2 соответствует как 16-ПРП, так и 32-ПУРП (каждая линия обозначает 2 пути распространения сигналов, разнесенных в вертикальной плоскости). Реализация подобных структур достигается применением многолучевых антенн или фазированных антенных решеток (ФАР) [1]. Применение ФАР и адаптивных ФАР (АФАР) позволит в дальнейшем реализовать технологию MIMO и повысить кратность МРП, что позволит уменьшить размеры антенн и мощность передатчиков.

О применении технологии OFDM

Технология *OFDM* позволяет эффективно бороться с селективными замираниями радиосигнала в системах радиосвязи, причем это технически достигается весьма просто – введением в цифровой сигнал временного защитного интервала [2]. Однако, сам защитный интервал не пустой, а в нем для поддержания синхронизма передается так называемый префикс, образуемый путем копирования битов конца OFDM-символа (рис. 3).

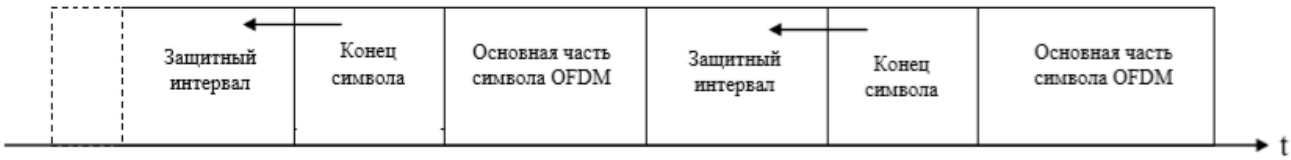


Рис. 3. OFDM-сигнал с защитными интервалами

Длительность защитного интервала должна быть не менее максимального времени лучей в радиоканале [2], которое для тропосферного канала составляет порядка 1 мкс [3, 4]. Следует отметить важнейшее обстоятельство: применение *OFDM* теоретически снимает ограничение на

скорость передачи по многолучевым радиоканалам и ее практическое ограничение определяется только максимально-допустимым энергетическим потенциалом радиоканала.

Расчетные соотношения для получения оценочных результатов

Для расчетов использовалось уравнение связи пролета ТСС

$$q'_{ш0(дБ)} = p_{пд1(дБВт)} - a_{ф\ пд(дБ)} - a_{ф\ пр(дБ)} - a_{тр(дБ)} + 2g_{а(дБ)} + 228{,}6 - \\ -10\lg\Pi_{ш1(Гц)} + \Delta_{пк(дБ)} - 10\lg(T_0 \cdot N_{ш(раз)}), \quad (1)$$

где $q'_{ш0}$ – допустимое ОСШ для идеальной системы с учетом энергетических потерь из-за неидеальностей приемопередающего тракта; $p_{пд1}$ – уровень сигнала передатчика в 1 mimo-канале, дБВт;

$a_{ф\ пд}$ и $a_{ф\ пр}$ – потери в передающем и приемном АФТ, соответственно, дБ; $a_{тр}$ – потери в тракте распространения, дБ; $g_а$ – коэффициент усиления антенн, дБ; $\Pi_{ш1}$ – шумовая полоса 1 mimo-канала, Гц; $\Delta_{пк}$ – энергетический выигрыш кодирования (ЭВК), дБ; T_0 – температура окружающей среды, К; $N_ш$ – коэффициент шума приемника, раз.

В (1) показатель $a_{тр}$ записывается в виде

$$a_{тр(дБ)} = a_{св(дБ)} + a_{мед(дБ)} - \Delta V_{м(дБ)} + \Delta g_{а(дБ)} + \text{прочие факторы}, \quad (2)$$

в котором $a_{св}$ – потери в свободном пространстве, дБ; $a_{мед}$ – медианные потери, дБ; $\Delta g_а$ – потери усиления антенн; $\Delta V_м$ – уменьшение множителя ослабления относительно долгосрочной медианы за счет быстрых и медленных замираний, которое определяется с помощью совместной интегральной функции распределения (ИФР) быстрых и медленных замираний сигнала [4].

Совместная ИФР быстрых и медленных замираний в тропосферном канале рассчитывается по формуле

$$T(V) = \frac{1}{\sqrt{2\pi}\, b_\sigma} \int_0^\infty e^{\frac{(\ln V_{мм} - \ln V_м)^2}{2 b_\sigma^{\,2}}} \left[1 - e^{-0{,}69\frac{V^2}{V_м^{\,2}}}\right]^m \frac{dV_м}{V_м} \quad (3)$$

в которой: V – множитель ослабления сигнала, обусловленный быстрыми и медленными замираниями; $V_м$ – медианный множитель ослабления быстрых замираний; $V_{мм}$ – медианный множитель ослабления медленных замираний; m – кратность РП; b_σ – параметр распределения: b_σ=0,115S_m (здесь S_m – параметр глубины медленных замираний, дБ) [4].

На рис. 4 и 5 представлены совместные ИФР при m=1 и m=16, рассчитанные по (3).

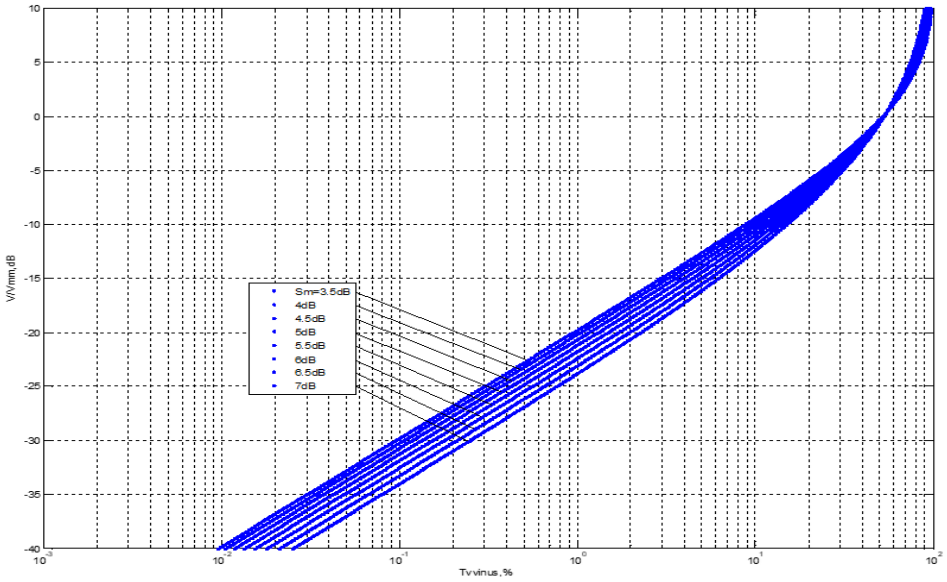


Рис. 4. Совместные ИФР быстрых и медленных замираний при m=1 для разных значений параметра глубины медленных замираний S_m

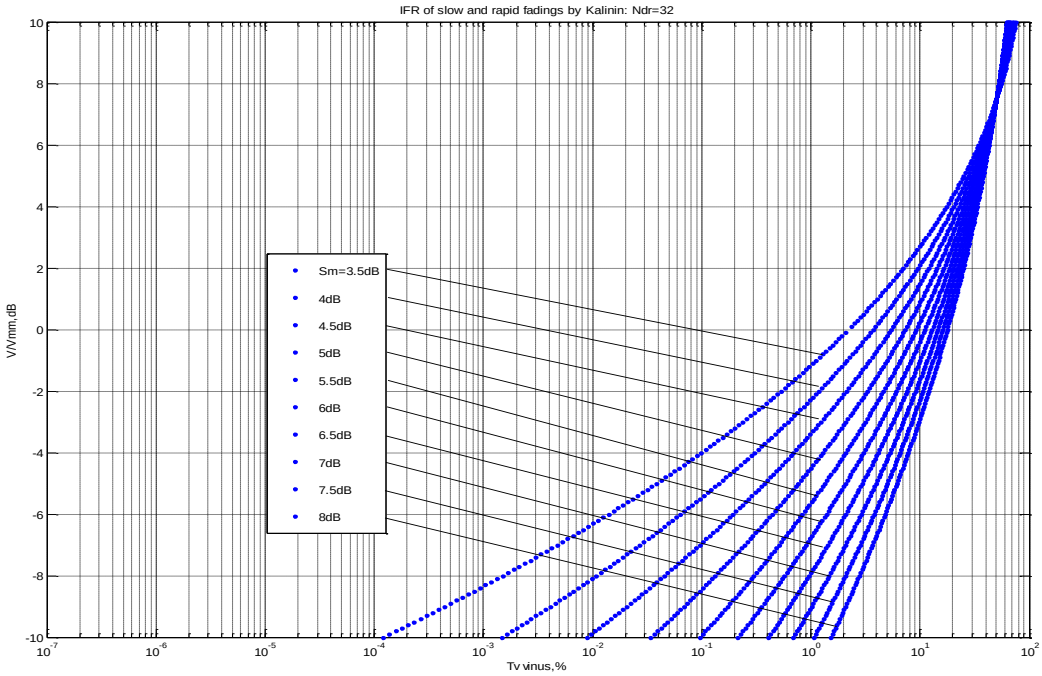


Рис. 5. Совместные ИФР быстрых и медленных замираний при m=16 для разных значений параметра глубины медленных замираний S_m

Результаты оценочных расчетов

На рис. 6 приведены зависимости допустимой мощности передатчика одного MIMO-канала ($P_{пд1}$) и требуемой ширины полосы частот (Δf) от скорости передачи в одном MIMO-канале при различной кратности РП.

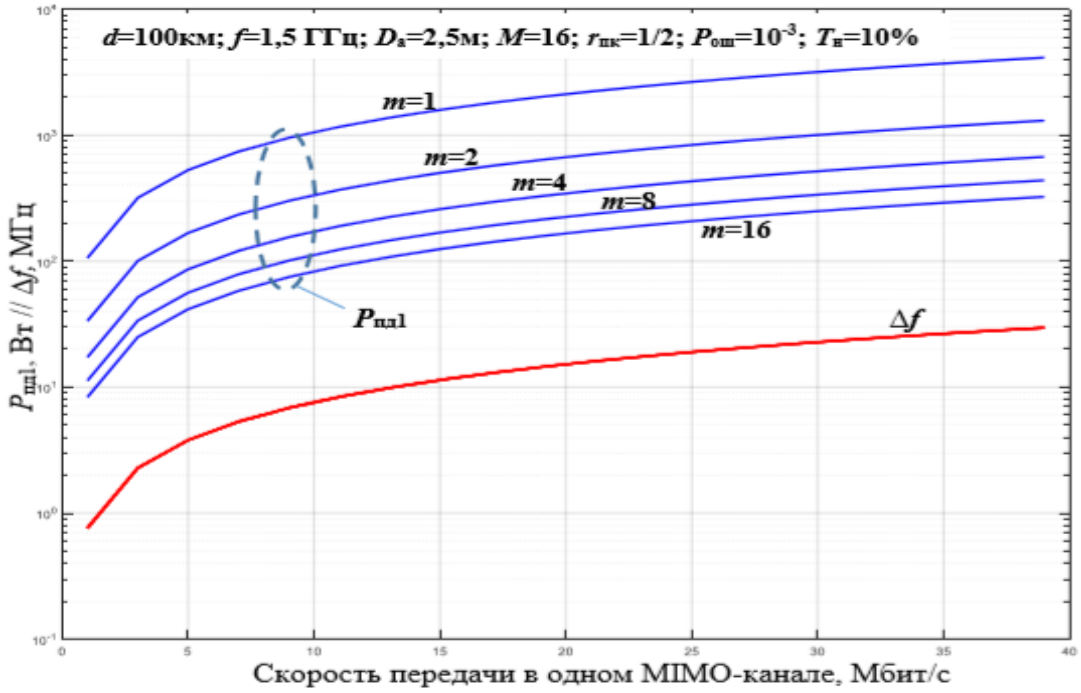


Рис. 6. Зависимость мощности передатчика ($P_{пд1}$) одного MIMO-канала и ширины полосы частот (Δf) от скорости передачи

В верхней части рис. 6 указаны основные исходные данные, использованные при расчете: $d_{пр}$ – длина пролета; f – диапазон рабочих частот; $D_а$ – диаметр антенн; M – число уровней модуляции; $r_{пк}$ – скорость помехоустойчивого кодирования; $P_{ош}$ – допустимая вероятность ошибки; $T_н$ – допустимый процент нарушения связи.

На рис. 7 приведены зависимости допустимой протяженности пролета ТСС (три верхние кривые) и требуемой ширины полосы частот канала от скорости передачи в одном MIMO-канале.

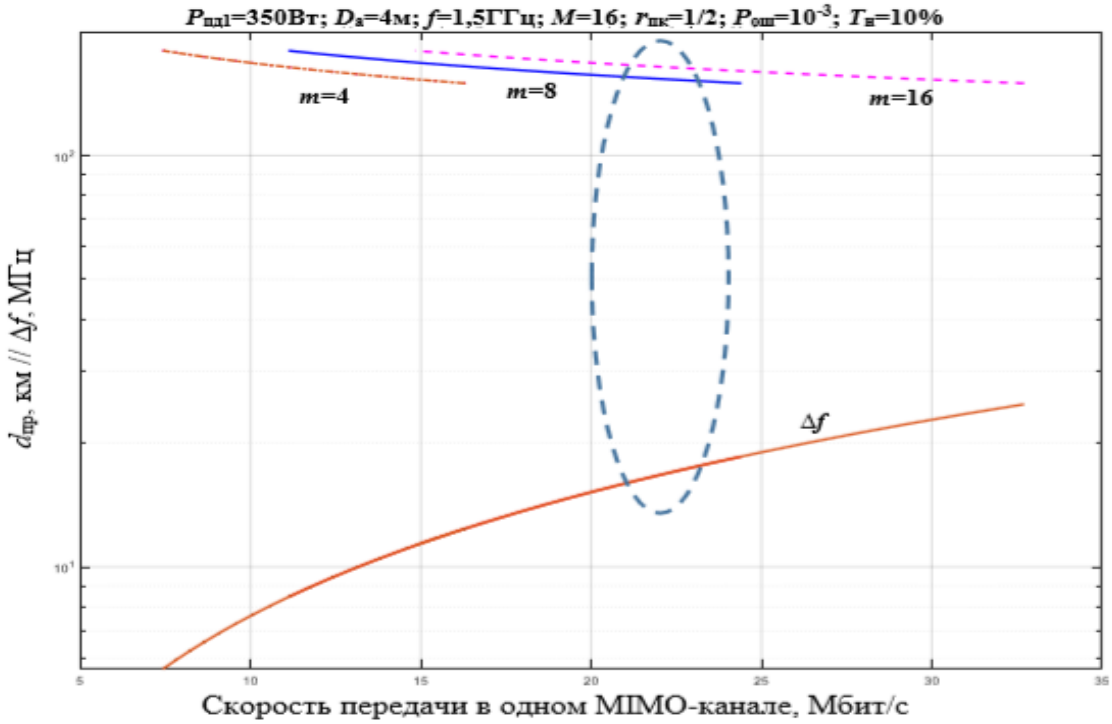


Рис. 7. Зависимости допустимой длины пролета ($d_{пр}$) и требуемой ширины полосы частот (Δf) от скорости передачи в одном MIMO-канале

Пунктирным эллипсом на рис. 7 показана область соответствующая общей скорости передачи в канале (80…100) Мбит/с при использовании MIMIO 4x4, при которых допустимая длина пролета составляет (120…160) км. В верхней части рис. 7 указаны основные исходные данные, использованные при расчете.

Выводы

1. Обеспечение высоких скоростей передачи в тропосферном канале (80…100) Мбит/с может быть достигнуто совместным применением технологий разнесенного приема высокой кратности (8; 16) и технологии MIMO в минимальной конфигурации 4x4. При этом, однако, требуются достаточно большие мощности передатчиков (1…3 кВт) и диаметры антенн (2,5…5 м) на расстояниях 100…200 км на частоте 1,5 ГГц.

2. В диапазоне частот 1,5 ГГц на расстояниях 300 км и выше (до 500 км) требуется применение антенн 9 м и более при одновременном снижении требований к качеству связи (увеличение допустимой ошибки до 10^{-2}), а также применения наиболее сильного помехоустойчивого кодирования (со скоростью ¼ и 1/6), приводящего к расширению необходимой ширины полосы частот канала до 45…60 МГц (вместо 15…25 МГц).

3. В диапазоне частот 5 ГГц длина пролета ограничивается расстоянием примерно 300 км и то при использовании всех энергетических возможностей аппаратуры (максимальная допустимая вероятность ошибок 10^{-2}; мощность передатчиков в 1 канале MIMO 1 кВт; диаметр антенн 15 м; скорость помехоустойчивого кодирования 1/6).

4. Длина пролета 500 км может теоретически обеспечена только в диапазоне частот 800 МГц или более низком, но также при использовании всех энергетических возможностей (см. п. 3).

5. Реализация высоких скоростей (80…100) Мбит/с в полосе канала порядка 20 МГц целесообразна при максимальной длине пролета (120…160) км, но, все же, требующих достаточно больших мощностей (порядка 1 кВт) и четырех антенн диаметром (4…5) м.

Литература

1. *Ильченко М.Е. и др*. Направления развития тропосферных станций нового поколения // Цифровые технологии, №16, 2014. - с. 8-18.
2. *М.С. Лохвицкий, А.С. Сорокин, О.А. Шорин*. Мобильная связь: стандарты, структуры, алгоритмы, планирование. - М.: Горячая линия-Телеком, 2018. - 264 с., ил.
3. *Сиваков И.Р., Малышев И.И.* Направления построения современных мобильных и стационарных тропосферных станций, в том числе для работы в условиях Крайнего Севера. //Информационно-телекоммуникационные технологии. Системы, средства связи и управления / АО «Концерн «Созвездие». Воронеж. 2017 №2. с. 216-227.
4. *А.И. Калинин*. Распространение радиоволн на трассах наземных и космических радиолиний. – М.: Связь, 1979. - 296 с.
5. Система научных расчетов и моделирования MATLAB. http://www.mathworks.com.

THE ASSESSMENT OF TECHNOLOGICAL OPPORTUNITIES TO IMPROVE SPEEDS OF TROPOSPHERIC COMMUNICATION SYSTEMS

Violetta Gen. Grichanenko
Student of group ZMTT1601, MTUCI
viola-grichanenko@mail.ru
Ljudmila V. Zharihina
Student of group ZMTT1601, MTUCI
viola-grichanenko@mail.ru
Aleksander St. Sorokin
MTUCI, PhD., associate professor of NiSRT department
alexorokin@rambler.ru

Keywords: *tropospheric communication, tropospheric channel, multipath propagation, slow fading of radio signal, fast fading of a radio signal, receiver diversity, OFDM, MIMO, the integral distribution function.*

The article quantitative evaluation (possible transmission speed and the corresponding permissible values of the transmission power, transmitter's power and the diameter of the antennas) in tropospheric communication systems, while using modern information technologies such as OFDM, MIMO and multi-level modulation, in conjunction with base tropospheric radio technology (diversity reception) and typical technologies used in modern communication systems, including the forward error encoding. When quantitative estimates were obtained, the speed (80...100) Mbit/s was taken as the conditionally optimal maximum transmission rate, in accordance with which the permissible values of the main parameters of the tropospheric radio channel were calculated-its length (length), transmitter power and the diameter of the receiving and transmitting antennas (which was assumed to be the same for both antennas). Calculations in accordance with the standard method of planning of tropospheric communication were made for the worst period of time (winter) for frequencies of 1.5 GHz and 5 GHz. The constant values of the receiver noise factor (2 dB) and the losses in the receiving and transmitting antenna-feeder paths (1 dB) were used for all variants of calculations.

ИСПОЛЬЗОВАНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ В АНАЛИЗЕ РЕФЛЕКТОМЕТРИЧЕСКИХ ИЗМЕРЕНИЙ И ОПРЕДЕЛЕНИИ МЕСТОПОЛОЖЕНИЯ НЕОДНОРОДНОСТЕЙ.

Бальдинкинов Алдар Викторович
аспирант кафедры МСиИИ, МТУСИ
a_baldinkinov@mail.ru
Хромой Борис Петрович
МТУСИ, д.т.н, профессор кафедры МСиИИ
p_khromoy@rambler.ru

Ключевые слова: *рефлектометрические измерения, неоднородности волоконно-оптической линии, непрерывное вейвлет-преобразование, погрешность измерений, коэффициенты преобразования.*

В статье предложен современный метод обработки рефлектометрических измерений линий связи, основанный на применении вейвлет-преобразования к данным рефлектограмм. На примере тестовых рефлектограмм и основных типов неоднородностей, которые можно встретить при работе с оптическим рефлектометром, показаны результаты применения данного метода. Метод основывается на использовании непрерывного вейвлет-преобразования в анализе рефлектограмм оптического рефлектометра. Данные полученные после переноса данных рефлектограммы, обрабатываются посредством приложения вейвлет-анализа, после этого строится спектрограмма преобразования, на основе которой вычисляются коэффициенты преобразования. Все это позволяет улучшить визуальное представление неоднородностей на графике рефлектограммы, а также точнее определять местоположение неоднородностей. Оценка полученных результатов проводится на основе сравнения погрешности измерений, при определении местоположения тестовых неоднородностей в рефлектограмме.

Введение

В настоящее время, волоконно-оптические линии связи пользуются огромной популярностью и постепенно заменяют медные аналоги повсеместно. Однако, данная популярность порождает высокие требования к контролю за функционированием таких сетей и требует постоянного и оперативного отслеживания различных неоднородностей и помех при их возникновении в линии связи [6 – 11]. Традиционным и самым распространенным способом для обеспечения такого контроля является использование оптического рефлектометра (ОР).

Одним из перспективных подходов к измерению на оптических линиях связи, а также обработке полученных результатов, является применение вейвлет-преобразования к рефлектометрическим измерениям [12 – 15]. Такое совместное использование для контроля параметров линий связи позволит повысить точность измерений.

Принцип работы ОР

Оптический рефлектометр (ОР) предназначен для определения расстояния до неоднородностей показателя преломления оптического волокна. Его работа основана на детектирование отраженных сигналов вследствие Релеевского рассеяния и Френелевского отражения. В ходе диагностики оптического волокна оптический рефлектометр посылает в него зондирующий импульс. Зондирующий импульс – это световой импульс определенной амплитуды и длительности. Одновременно с запуском зондирующего импульса рефлектометр начинает отсчет времени. Распространяясь по оптическому волокну, импульс сталкивается с различными препятствиями (повреждениями, неоднородностями), от которых происходит отражение части сигнала. Отраженный сигнал распространяется в обратном направлении и время его поступления

на вход рефлектометра фиксируется. Неоднородности оптического волокна делятся на отражающие (вызванные Френелевским отражением) и неотражающие (вызванные Релеевским рассеянием).

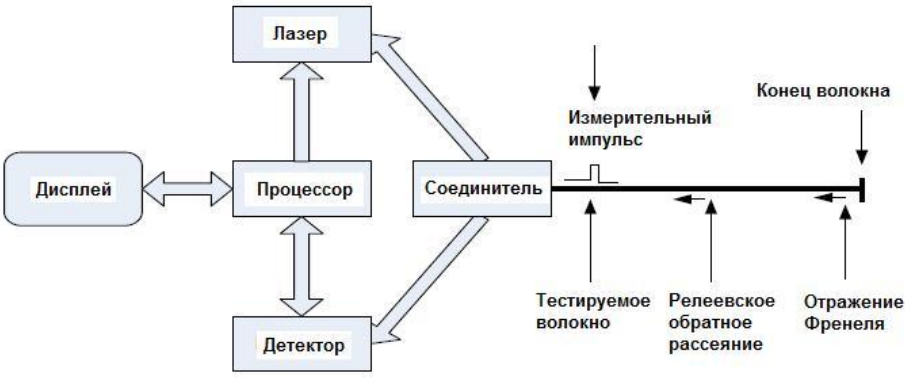


Рис. 1. Структурная схема оптического рефлектометра

.

Результат измерений рефлектометр представляет в виде графика, который называется рефлектограммой. Типовая рефлектограмма приведена на рисунке 2. Вертикальная шкала определяет уровень рассеянного (отражённого) сигнала в логарифмических единицах. Горизонтальная ось соответствует расстоянию от рефлектометра до тестируемой области волокна. Так как в ОР реально измеряется время, то расстояние определяется пересчётом с масштабным коэффициентом примерно равным 10 мкс/км, учитывающим, что свет проходит по волокну до тестируемой точки в прямом и обратном направлении. На рисунке обозначены: 1 – начало линии (оптический разъём); 2 – соединитель; 3, 4, 6, 7, 8 – сварные соединения; 5 – трещина в волокне (отражающая неоднородность); 9 – конец линии (торец волокна); 10 – шумы [1].

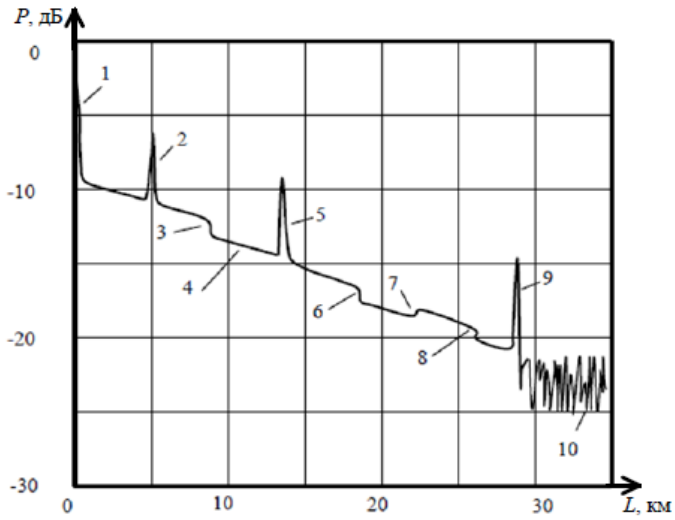


Рис. 2. Рефлектограмма импульсного рефлектометра.

Важной задачей является определение расстояний до выявленных ОР неоднородностей с возможно меньшими погрешностями. Величина погрешностей измерения зависит от способа математической обработки рефлектограмм. Одним из вариантов обработки заключается в применении вейвлет-преобразования (ВП). Применение ВП может быть осуществлено при совсем небольших затратах, так как вейвлеты широко представлены в доступных приложениях для персональных компьютеров, а данных рефлектограммы можно перевести в нужный для анализа формат.

Применение вейвлет-преобразования

ВП – это очень мощное средство анализа данных, которое используется во множестве приложениях обработки сигналов. ВП основано на наборе сигналов, которые были получены от базового материнского вейвлета, после изменения временных характеристик. В отличие от классического преобразования Фурье, ВП наиболее эффективно использует оконное преобразования сигнала, для низких частот сигнала используется широкое окно, а для высоких частот - узкое окно. Вейвлет анализ позволяет обнаружить нарушения непрерывности в данных рефлектограммы и строить, согласно анализу, график спектрограммы ВП [3, 5].

Пример применения ВП

Оптимальное применение ВП возможно при соответствующем выборе его типа и параметров. Поскольку в настоящее время разработано большое количество типов вейвлет-преобразований необходимо провести исследования результатов обработки тестов, в которых временное положение неоднородностей задано с высокой точностью. В результате обработки следует определить величины погрешностей обработки для вейвлет-преобразований различных типов.

В качестве примера можно рассмотреть результаты обработки рефлектограммы с неопределенностями без отражения. Этот вид неопределенности возникают в кабеле при наличии вставки со смещением сердцевины (рис.3). На данном рисунке так же представлен соответствующий участок рефлектограммы.

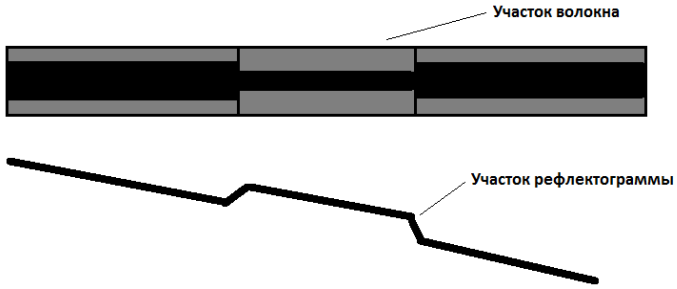


Рис. 3. Вставка в оптическом волокне и его рефлектограмма.

С помощью программы «*AQ7932*», которая позволяет симулировать работу рефлектометра и строить рефлектограмму с заданными параметрами неоднородностей на трассе, был смоделирован кабель, длиной 1 км 716 метров. В кабеле были определены две неоднородности, которые свидетельствуют о том, что в кабеле есть вставка со смещением сердцевины. Первая неоднородность была заложена на расстоянии 354 метров, вторая на расстоянии 1км 298 метров.

Программа«*AQ7932*» выполняет роль «программного оптического рефлектометра». Очевидно, что в процессе программирования возникает погрешность в расположении неоднородностей. Согласно данным отчета, программный ОР зафиксировал заложенные тестовые неоднородности с погрешностью измерений представленной в таблице 1.

Далее был осуществлен перенос смоделированной рефлектограммы в математическую среду приложения «*Matlab*» в котором, наиболее широко представлен функционал вейвлет-преобразования.

Таблица 1

Номер неоднородности	Действительное значение, м	Погрешность, м
1	354	2
2	1298	2,2

Были проведены сравнения обработки рефлектограммы и были выявлены типы вейвлет-преобразований, которые обеспечивали минимальную погрешность. К ним относятся вейвлет-преобразования: «Хаара», «Добеши 3», «Биортогонального вейвлета 1.3»

В таблице 2 представлены результаты определения местоположения неоднородностей после применения ВП, для анализа рефлектограммы.

Таблица 2

Тип НВП	Определение местоположения неоднородностей	
	Неоднородность №1, м	Неоднородность №2, м
«Хаар»	350	1292
«Добеши 3»	352	1294
«БВ 1.3»	353	1296

После простого вычисления погрешностей измерений, получены результаты представленные в таблице 3.

Таблица 3

Тип НВП	Определение местоположения неоднородностей		Абсолютная погрешность измерений	
	Неоднородность №1, м	Неоднородность №2, м	Абсолютная погрешность, №1 м	Абсолютная погрешность, №2 м
«Хаар»	350	1292	4	6
«Добеши 3»	352	1294	2	4
«Биортогональный вейвлет 1.3»	353	1296	1	2

Как видно из таблицы 3 применительно к решаемой задаче наименьшую погрешность обеспечивает «Биортогональный вейвлет 1.3».

Далее был рассмотрен вариант, когда в рефлектограмме отражены такие распространенные неоднородности как наличие коннектора или воздушный зазор в соединении со смещением сердцевины. Общий вид волокна в разрезе, при обнаружении такой неоднородности представлен на рис.4.

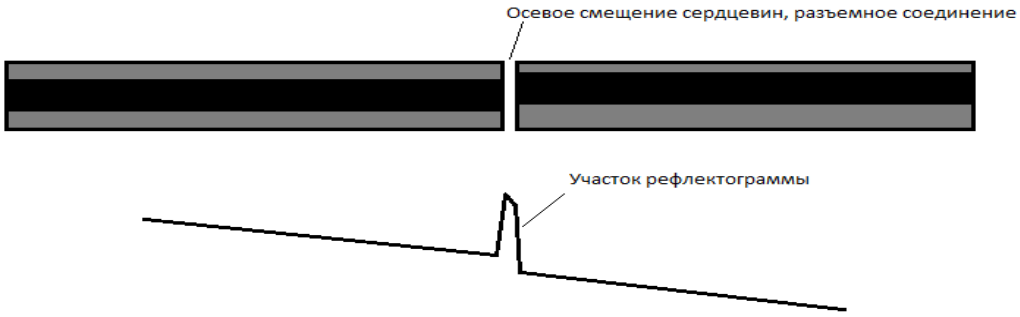


Рис. 4. Схематичное изображение наличия разъемного соединения в кабеле.

Для рассмотрения данного примера, в рефлектограмму были добавлены две неоднородности с осевым смещением сердцевины и без, на расстоянии 512 метров и 256 метров, соответственно. Программа эмулятор ОР, зафиксировала неоднородности на расстояниях, представленных в таблице 4.

Таблица 4

Неоднородность:	Расстояние, м.	Потери, дБ.
Коннектор	254	0,708
Разъемное соединение	515,1	0,983

Результаты определения местоположения неоднородностей после применения ВП для анализа рефлектограммы приведены в таблице 5.

Таблица 5

Тип НВП	Определение местоположения неоднородностей	
	Неоднородность №1, м	Неоднородность №2, м
«Хаар»	254	510
«Добеши 3»	253	509,7
«БВ 1.3»	254	510,5

Результаты вычисления погрешности измерений, которые мы получили в результате применения измерений коэффициентов вейвлет-преобразований, представлены в таблице 6.

Таблица 6

Тип НВП	Определение местоположения неоднородностей		Абсолютная погрешность измерений	
	Неоднородность №1, м	Неоднородность №2, м	Абсолютная погрешность, №1 м	Абсолютная погрешность, №2 м
«Хаар»	254	510	2	2
«Добеши 3»	253	509,7	3	2,3
«Биортогональный вейвлет 1.3»	254	510,5	2	1,5

Как видно по результатам измерений, применение «Биортогонального вейвлета 1.3» обеспечивает наиболее точные результаты»

Последним примером, который будет рассмотрен в данной статье, является применение тестовой рефлектограммы с наличием шумов. Основными источниками шумов в волоконно-оптической линии являются различного рода помехи (флуктуационные, межсимвольные, переходные), которые возникают, например, из-за несовершенных элементов схемы передачи данных, собственных шумов лазеров, повреждения волоконно-оптического кабеля и т.д. На рефлектограмме данные шумы могут скрыть от глаз оператора неоднородности в кабеле и, соответственно, со временем, привести к возможному обрыву связи в канале передачи данных.

Для этого примера была взята тестовая рефлектограмма, в которой были зафиксированы две неоднородности: первая неоднородность была заложена на расстоянии 354 метров, вторая на расстоянии 1км 298 метров. К этой рефлектограмме был добавлен шум, при этом соотношение сигнал/шум в данном случае равно 20 dB.

По результатам анализа, при наличии шума в оптической линии связи, программный ОР зафиксировал заложенные тестовые неоднородности со следующей погрешностью измерений (таблица 7).

Таблица 7

Номер неоднородности	Действительное значение, м	Погрешность, м
1	351	3
2	1294,2	3,8

В таблице 8 представлены результаты измерений и погрешностей при определении местоположения заданных тестовых неоднородностей

Таблица 8

Тип НВП	Определение местоположения неоднородностей		Абсолютная и относительная погрешность измерений	
	Неоднородность №1, м	Неоднородность №2, м	Абсолютная погрешность, №1 м	Абсолютная погрешность, №2 м
«Хаар»	348	1290	6	8
«Добеши 3»	350	1291	4	7
«БВ» 1.3	352	1295	2	3

Как и в предыдущем примере, применение вейвлет-преобразования для анализа рефлектограммы и определения местоположения неоднородностей, позволило улучшить результаты измерений, несмотря на присутствие шумов.

Выводы

Применение вейвлет-анализа в работе ОР имеет большой потенциал, и как показало сравнение результатов измерений, может облегчить и улучшить определение местоположения неоднородностей и обрывов в оптических линиях связи, в независимости от типа неоднородностей, а также наличия шумов. Прибавив к этому широкий функционал вейвлет-анализа, которым располагает приложение «*Matlab*», мы получаем в итоге множество способов анализа данных реальных рефлектограмм, и возможность их улучшения в дальнейших работах.

Литература

1. *Хромой Б.П.* Метрология и измерения в телекоммуникационных системах (Том 2) — М.: ИРИАС, 2008. — 560 с.
2. *Дьяконов В. П.* Справочник по применению системы PC MATLAB — М.: «Физматлит», 1993г. 112 с.
3. *Дьяконов В.П.* - Вейвлеты. От теории к практике. Солон-Пресс. 2005 г. 448 с.
4. *Смоленцев Н. К*. Основы теории вейвлетов. Вейвлеты в MATLab. ДМК-пресс. 2005 г. 304 с.
5. *Яковлев А.Н.* Введение в вейвлет-преобразования. Новосибирск: НГТУ, 2003. 104 с.
6. *Аджемов А.С., Хромой Б.П.* Обеспечение единства измерений хроматической дисперсии в оптическом волокне // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 8-10.
7. *Аджемов А.С., Хромой Б.П.* Электросвязь и оптика в историческом плане // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 2. С. 71-79.
8. *Портнов Э.Л., Григорьян А.К.* Поляризационная модовая дисперсия на волоконно-оптической линии передачи // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 62-64.
9. *Портнов Э.Л., Фатхулин Т.Д.* Анализ разрабатываемых технологий для достижения максимальных скоростей передачи информации в современных DWDM системах // REDS: Телекоммуникационные устройства и системы. 2015. Т. 5. № 2. С. 177-179.
10. *Портнов Э.Л.* Новый подход в определении параметров передачи и влияния в оптических линиях телекоммуникаций // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 5. С. 60-63.
11. *Портнов Э.Л., Мариносян Э.Х.* Определение отношения сигнал/шум для высокоскоростных систем передачи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2013. № 1. С. 139-141.
12. *Манонина И.В.* Использование вейвлет-анализа для оценки качества рефлектограмм // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 54-59.
13. *Манонина И.В.* Вейвлет-анализ рефлектограмм с использованием математического пакета MATLAB // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 61-66.
14. *Манонина И.В.* Определение оптимальных параметров для вейвлет-обработки рефлектограмм // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 5. С. 28-38.

15. *Манонина И.В.* Методика обработки данных измерений параметров линий связи с применением вейвлет-анализа к рефлектометрическим измерениям // автореферат дис. ... кандидата технических наук / Моск. техн. ун-т связи и информатики. Москва, 2016

THE USE OF WAVELET TRANSFORM IN THE ANALYSIS OF REFLECTOMETRY MEASUREMENT AND DETERMINING THE LOCATION OF FIBER OPTIC LINE EVENTS.

Aldar V. Baldinkinov
Postgraduate student of the department MSII, MTUCI
a_baldinkinov@mail.ru
Boris P. Khromoy
MTUCI, D.T.S, teacher of the department MSII,
p_khromoy@rambler.ru

Keywords: *reflectometry measurements, fiber optic line events, continuous wavelet transform, measurement error, wavelet-transform coefficients.*

In this article, a modern method for processing reflectometry measurements of communication lines, based on the application of wavelet transform to the trace data is claimed. Using the examples of test reflectograms and the main types of fiber optic line events that can be met when working with an optical reflectometer, the results of applying this method are shown. This method is based on the usage of a continuous wavelet transform in the analysis of reflectograms of an optical reflectometer. The data, which was obtained after the transfer of the trace data, is processed by the application of wavelet analysis, then the conversion spectrogram is built, on the basis of which the conversion coefficients are calculated. All this, allows improving the visual representation of the fiber optic line events on the trace graph, as well as more accurately determining the location of them. Evaluation of the obtained results is carried out on the basis of a comparison of measurement errors, in determining the location of test optic line events in the trace.

«Информационные технологии и автоматизация процессов в системах связи»

ПРОЕКТИРОВАНИЕ IoT СИСТЕМЫ «УМНЫЙ ДОМ» С КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ ДАННЫХ

Шишкин Артем Олегович
Студент группы 2МИБ1601 МТУСИ
mail.sao@mail.ru
Воронова Лилия Ивановна
МТУСИ, д.ф.-м.н. зав.кафедрой ИСУиА
voronova.lilia@ya.ru

Ключевые слова*: интернет вещей (IoT), умный дом, криптографическая защита данных, интерфейсы передачи данных, программируемая логическая интегральная схема, обеспечение безопасности.*

В статье рассмотрены проблемы обеспечения информационной безопасности *IoT*-системы «умный дом» с применением криптографической защиты данных. Обработка входных сигналов с датчиков, зашифрование и расширование данных, передача сигналов в канал связи осуществляется под управлением программируемой логической интегральной схемы (ПЛИС). Определен стандарт выполнения криптографических преобразований. Обоснован выбора устройства и разработана функциональная схема модуля, выполняющего обработку входных сигналов с датчиков системы и необходимые криптографические преобразования.

Введение

Интернет вещей (Internet of Things, *IoT*) — новая стадия развития информационных технологий, при которой различные технические средства взаимодействуют между собой по сети Интернет, обмениваясь информацией между собой в реальном времени и без вмешательства человека.

Внедрение интернета вещей стало возможным за счет широкого распространения смартфонов, беспроводных сетей, удешевления электронных компонентов и увеличения скорости обработки данных. IoT-системы обычно состоят из сети умных устройств и облачной платформы к которой они подключены.

Одним из основных направлений развития *IoT* является совершенствования промышленных систем. Некоторые мобильные приложения могут автоматически закрывать двери, включать сигнализацию и отключать отопление когда отсутствует пользователь, заменяя тем самым его физические действия. На кафедре ИСУиА МТУСИ ведутся активные исследования по направлению «промышленный интернет вещей» (*IIoT*) [1, 2]

Дальнейшее совершенствование IoT систем основано на совершенствовании датчиков по сбору информации, а также устройств обработки, хранения и преобразования сигналов, поступающих с этих датчиков.

Стандартизация *IoT* системы

Одно из основных препятствий для развития интернета вещей — отсутствие единых стандартов, затрудняющее объединение беспроводных сетей объектов в единую сеть. В разных сферах интернета вещей работают разные интерфейсы и протоколы передачи данных.

Ниже перечислены основные интерфейсы передачи данных, используемые в настоящее время.

Bluetooth – беспроводной канал передачи данных, используется в основном смартфонами, а так же устройствами, работающими от батарейки для беспроводной передачи данных. Скорость передачи данных до 1.4 MBit/s. Максимальное расстояние - до 5-10 метров.

Wi-Fi – беспроводной канал передачи данных, используется в основном в системах «умный дом» для беспроводной передачи информации. Скорость передачи данных до 300 MBit/s. Максимальное расстояние – до 100 метров.

Ethernet – проводной канал передачи данных, используемый в основном на промышленных предприятиях и для построения сетей передачи данных. Скорость передачи данных до 10 GBit/s. Максимальное расстояние в зависимости от используемой технологии – до 100 километров.

Использование программируемых логических интегральных схем (ПЛИС) при построении IoT систем решает проблему отсутствия стандарта объединения беспроводных сетей. Благодаря наличию встроенных, верифицированных сложно-функциональных интерфейсных блоков, входная информация с датчика может поступать как по проводному каналу связи, так и по беспроводному.

ПЛИС от фирмы Xilinx обладают встроенными высокоскоростными интерфейсами, такими как: Ethernet 10Mb/s, Fast Ethernet 100Mb/s, Gigabit Ethernet 1GB/s, 10G Ethernet 10Gb/s, USB 2.0, USB 3.0, RapidIO и т.д [3]. Для передачи информации по беспроводному каналу связи, на плату с установленной ПЛИС может быть установлен Wi-Fi модуль.

Пример обеспечения безопасности *IoT* системы «умный дом» на основе ПЛИС

Контроль за текущим состоянием *IoT* системы «умный дом» пользователь осуществляет через смартфон. Интерфейс передачи данных выбирается в зависимости от используемой модели телефона. Все данные передаются пользователю и на пункт охраны в зашифрованном виде. Алгоритм зашифрования по умолчанию – ГОСТ Р 34.12-2015 [4]. В зависимости от используемой системы пользователю может быть доступен любой алгоритм зашифрования. Передача тревожного сигнала на пункт охраны осуществляется пользователем при нажатии на смартфоне специальной кнопки вызова или системой безопасности «умного дома» автоматически.

Проект *IoT* системы представляет собой модель «умного дома», реализующий следующие функции:

1. Наблюдение за входной дверью. Если меняется состояние входной двери и нет соответствующего подтверждения от пользователя, через установленный промежуток времени, срабатывает тревожный сигнал.

Система отслеживает следующие положения входной двери:

- входная дверь открыта;
- входная дверь закрыта и заперта;
- входная дверь закрыта и не заперта.

2. Наблюдение за дверным звонком. Если кто-либо нажал на кнопку дверного звонка, пользователю системы выводится соответствующее оповещение и данные с камеры наружного наблюдения в режиме реального времени.

3. Анализ состояния датчика утечки газа. При срабатывании датчика, тревожный сигнал передается на пункт охраны автоматически.

4. Анализ состояния датчика пожарной безопасности. При срабатывании датчика, тревожный сигнал передается на пункт охраны автоматически.

5. Анализ состояний датчиков движения. После того, как пользователь покинул помещение и подтвердил свой выход, отправив соответствующий сигнал со смартфона, автоматически включаются датчики движения и продолжают свою работу до тех пор, пока авторизированный пользователь не вернется домой и не выполнит алгоритм авторизации, показанный на рис.1. При срабатывании датчика, тревожный сигнал передается на пункт охраны автоматически.

6. Анализ датчиков протечки воды. При срабатывании датчика, тревожный сигнал передается на пункт охраны автоматически.

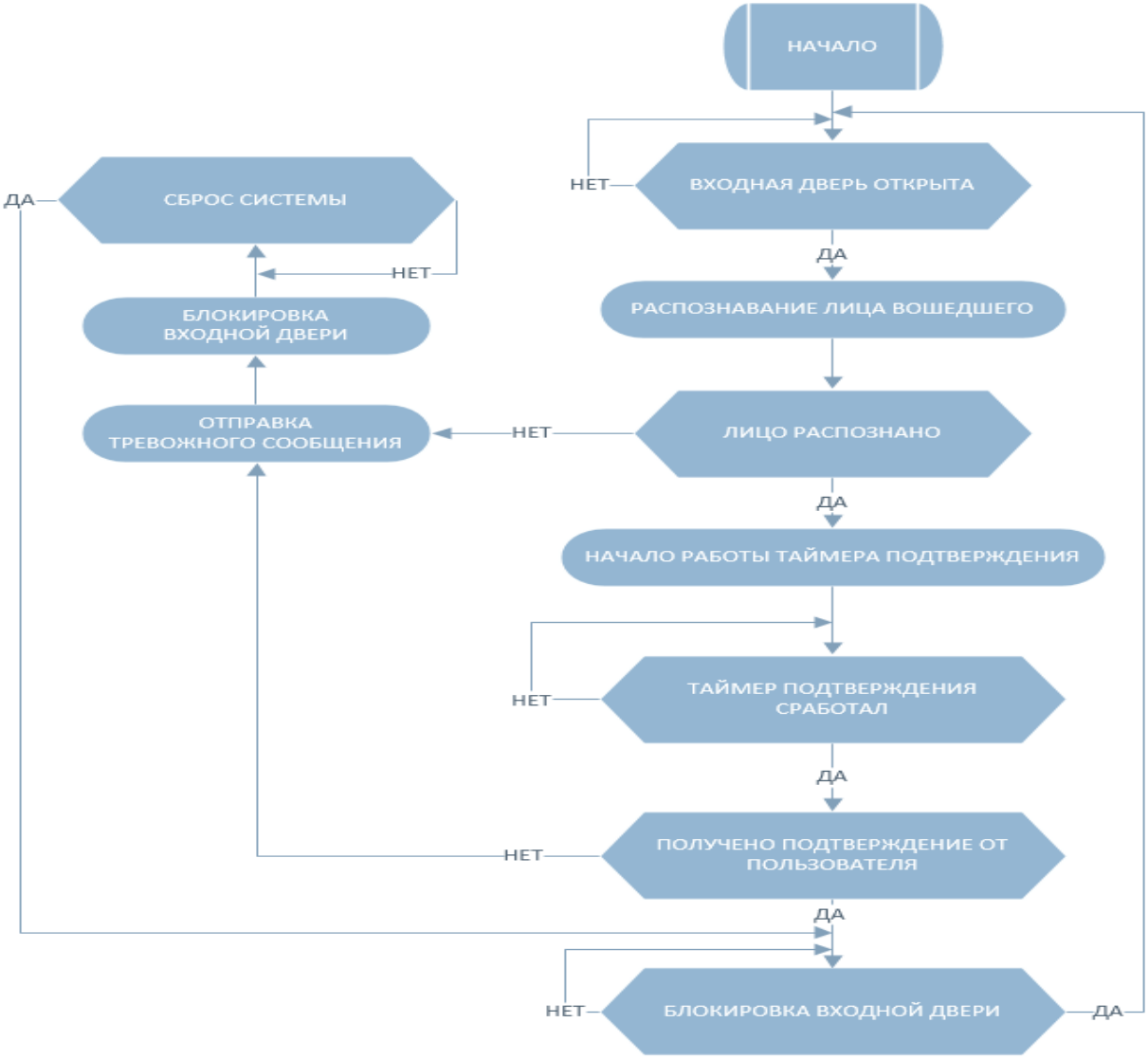


Рис. 1. Алгоритм авторизации пользователя

После открытия входной двери, система безопасности автоматически производит распознавание лица вошедшего человека. Если не найдены совпадения между вошедшим человеком и образами, хранящимися в базе системы, происходит автоматическая отправка тревожного сообщения пользователю и на пункт охраны. В случае если система по ошибке не распознала лицо пользователя, после отправки тревожного сообщения, пользователь может сбросить систему самостоятельно со своего смартфона или вручную, нажав на специальные, скрытно установленные кнопки в помещении, если радио-канал заблокирован.

Если лицо пользователя было распознано корректно, система безопасности автоматически запускает таймер, в течение которого пользователь должен произвести авторизацию со своего смартфона. Повторная авторизация необходима для предотвращения возможных ошибок системы распознавания лиц и на случай, если злоумышленники попытались копировать черты лица пользователя. Если после срабатывания таймера система безопасности не получила подтверждения от пользователя, автоматически отправляется сигнал тревоги на пульт охраны.

При срабатывании любого из установленных датчиков, пользователю и на пункт охраны отправляется тревожный сигнал с идентификационным номером ошибки, что позволит вызвать профильную службу реагирования.

Обработка входных сигналов с датчиков, зашифрование и расширование данных, передача сигналов в канал связи осуществляется под управлением ПЛИС [5].

Использование ПЛИС в разрабатываемой системе обусловлено:

1. Необходимостью одновременно обрабатывать сигнал от большого количества датчиков.
2. Необходимостью обрабатывать видеоданные высокого качества в режиме реального времени.
3. Необходимостью зашифрования и расшифрования передаваемых данных.
4. Возможностью использования любого интерфейса передачи данных.
5. Отсутствие программного обеспечения, что делает систему неуязвимой к вредоносным программам.

На рис.2 показан пример функциональной схемы системы «умный дом», подключенный через разъемы X4..X6 к трем датчикам.

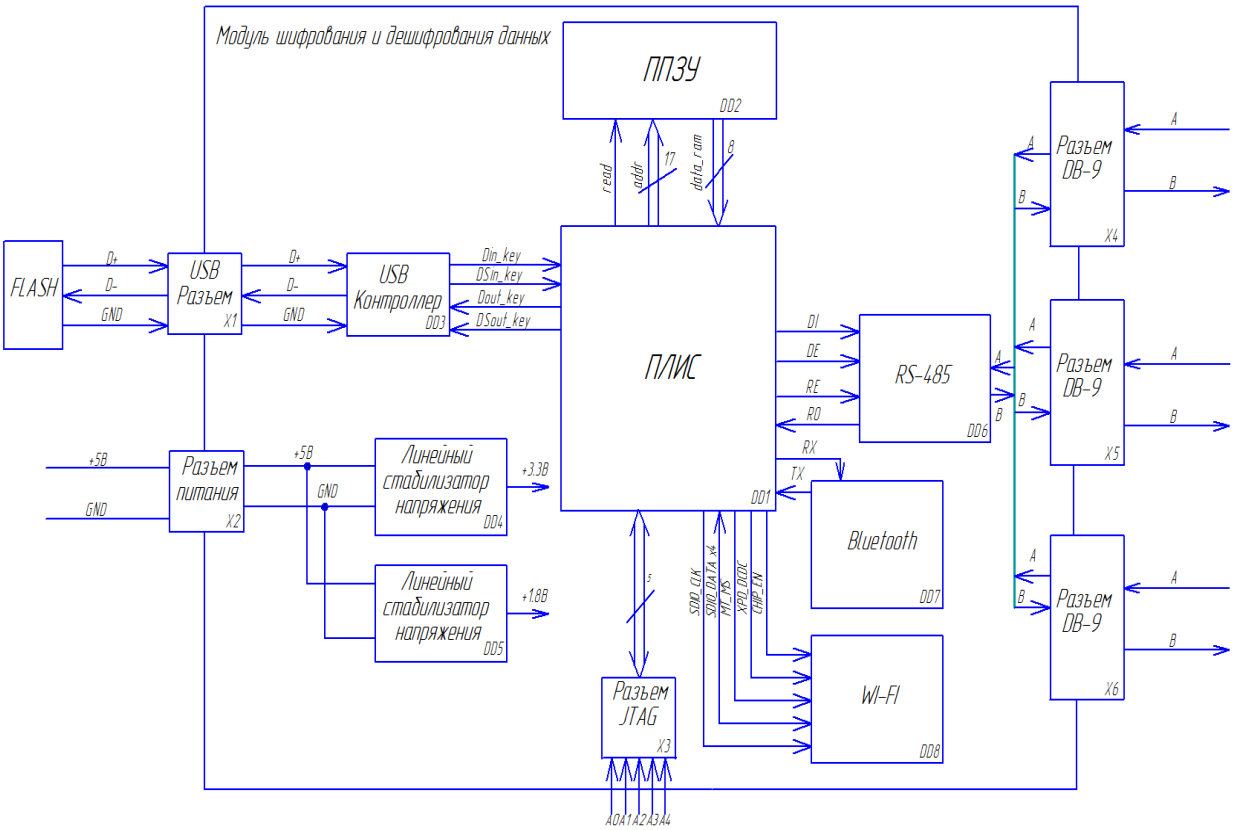


Рис. 2. Пример функциональной схемы системы «умный дом» на основе ПЛИС

где:

DD1 – микросхема ПЛИС, выполняет криптографические преобразования данных по ГОСТ Р 34.12-2015, опрашивает датчики, обрабатывает входные сигналы с датчиков;

DD2 – микросхема ППЗУ, необходима для хранения значений поля Галуа (2^{16}), таблицы замен, итерационных констант для криптографических преобразований и итерационных констант для выработки раундовых ключей.

DD3 – микросхема USB 2.0 контроллер, служит для передачи ключа, хранящегося на FLash-носителе по USB интерфейсу в память ПЛИС;

DD4, DD5 – микросхемы стабилизаторы напряжения, необходимы для подачи питания на ПЛИС, ППЗУ, Wi-FI, Bluetooth;

DD6 – микросхема приемопередатчика RS-485;

DD7 – микросхема приемопередатчика Bluetooth;

DD8 – микросхема приемопередатчика Wi-Fi.

Техническое описание функционирования системы защиты «умный дом»

Для защиты от несанкционированного доступа (НСД) ключ загружается через разъем X1 по шине «D+» на DD3 (USB 2.0). Flash-носитель с ключом должен быть недоступен для

пользователя, загрузка ключа, констант, таблицы замен, производится специалистом охранной организации лично.

После включения системы, DD1 (ПЛИС), последовательно опрашивает подключенные датчики. Сигнал запроса текущего состояния конкретного датчика поступает с ПЛИС в DD6 (приемопередатчик RS-485) по шине «DI». ПЛИС устанавливает режим работы DD6 используя сигналы «DE» (разрешение работы передатчика) и «RE» (разрешение работы приемника). Через разъемы X4-X6 в приемопередатчик RS-485, по сигналу «A», приходит информация о текущем состоянии датчика. Из DD6 информация с датчика поступает в DD1 по шине «RO».

ПЛИС неизменно поддерживает связь с пунктом охраны через Интернет путем отправки пакетов поддержки соединения. Это необходимо для срабатывания сигналы тревоги по посту охраны, если от охраняемого объекта перестал поступать сигнал поддержки соединения. Подобная ситуация может произойти при применении злоумышленниками устройств блокировки радиоканалов.

По умолчанию ПЛИС выполняет криптографические преобразования по ГОСТ Р 34.12-2015. После выполнения X-преобразований, по команде «read» поступает запрос на чтения информации, хранящейся в DD2 (ППЗУ). По шине «addr» передается адрес ячейки из которой нужно считать данные. Выходные данные из ППЗУ в ПЛИС передаются по шине «data_ram».

После 10-го раунда преобразований, зашифрованные данные передаются в канал передачи данных через DD8 (Wi-Fi модуль) по шинам «SDIO_DATA0» и «SDIO_DATA1». Обработка сигнала от смартфона пользователя может осуществляться через Wi-Fi модуль, либо через DD7 (Bluetooth модуль) по сигналам «RX» и «TX».

Заключение

В статье предложен пример устройства IoT системы «умный дом» с криптографической защитой передаваемой информацией. Устройством по сбору, хранению, шифрованию и передаче информации является программируемая логическая интегральная схема. Наличие большого числа портов ввода-вывод позволяет одновременно обрабатывать информацию от IoT устройств в сети не используя механизмов прерываний и не формируя искусственные задержки, связанные с недостаточным быстродействием вычислительной системы. В статье приводится пример организации системы безопасности внутри охраняемого объекта, защита канала передачи информации вне объекта не рассматривается.

Литература

1. *Безумнов Д.Н., Воронова Л.И*. О развитии и стандартизации технологии интернета вещей. // В сборнике: ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА Материалы XII Международной отраслевой научно-технической конференции. 2018. С. 293-294.
2. *Воронова Л.И., Воронов В.И.* BIG DATA. МЕТОДЫ И СРЕДСТВА АНАЛИЗА. Учебное пособие / Москва, 2016.
3. Рекомендуемые встроенные сложно-функциональные блоки от компании Xilinx. URL: https://www.xilinx.com/products/intellectual-property.html.
4. Федеральное агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации. ГОСТ Р 34.12-2015. Москва, стандартинформ, 2015.
5. *К. Максфилд*. Проектирование на ПЛИС. Издательство: М : Додэка-21, 2007. 408 с.

IoT SYSTEM «SMATR HOUSE» WITH CRYPTOGRAPHIC DATA PROTECTION

Artem O. Shishkin
Student of the group 2MIB, MTUCI
mail.sao@mail.ru
Lilia I. Voronova
MTUCI, Doctor of Physics and Mathematics,
Head of Department ISAM
voronova.lilia@ya.ru

Keywords: *Internet of Things (IoT), smart home, cryptographic data protection, data transfer interfaces, programmable logic integrated circuit, security.*

The article deals with the problems of ensuring the information security of IoT-system "Smart Home" using cryptographic data protection. Processing input signals from sensors, encrypting and expanding data, transmitting signals to a communication channel is carried out under the control of a programmable logic device(PLD). The standard for performing cryptographic transformations is defined. The choice of device is grounded and a functional diagram of the module that processes the input signals from the system sensors and the necessary cryptographic transformations is developed.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Походун Анжелика Игоревна
студентка группы М111701(73) МТУСИ
an.pokhodun@gmail.com
Осин Андрей Владимирович
МТУСИ, к.т.н., доцент кафедры ИБ
osin_a_v@mail.ru

Ключевые слова: *информационная безопасность, интернет вещей, блокчейн, Internet of Things, Blockchain, IOTA, Tangle, DAG.*

Описана актуальность проблемы безопасности сети интернета вещей. Дано определение интернет-вещи. Рассмотрена стандартная сеть с интернет-вещами и приведены возможные последствия от вероятных кибер-атак. Предложена технология блокчейн в качестве безопасного протокола сообщения между *IoT*-устройствами. Рассмотрены достоинства применения технологии блокчейн в сети с интернет-вещами и недостатки классической биткойновской блокчейн. Предложено использование алгоритма, лежащего в основе криптовалюты *IOTA*. Представлена предложенная защищенная архитектура интернета вещей.

Технология IoT в настоящее время особенно набирает популярность – не столько по причине того, что интернет вещи создают удобство в регулировании и управлении некоторыми ресурсами, а также позволяют человеку автоматизировать рутинные действия, сколько потому, что современные темпы «моды» на технологии таковы, что пользователи отдают предпочтение чему-то новому и совершенному, примерно так же, как и простые в использовании кнопочные телефоны исчезли с рынка в пользу многофункциональных и стильных смартфонов.

IoT-устройства – это небольшие запрограммированные микроконтроллеры, подключенные к глобальной сети, которые являются сенсорами (служат для сбора информации) и (или) актуаторами (исполняют пользовательские команды). В большинстве случаев эти устройства устанавливаются обычными пользователями (если защиту от атак в крупных IT-корпорациях обеспечивают специалисты, то небольшие организации и обычные пользователи входят в группу риска), не являющимися технически подкованными, которые, к примеру, могут оставить комбинацию «имя пользователя/пароль» заводскими, чем пользуются компьютерные злоумышленники, совершая кибер-атаки [6 – 11].

Но даже если пользователь обезопасил себя защищенной аутентификацией, это еще не делает его устройство безопасным: неверно прописанные разрешения доступа, простые пароли конфигураций, обычное обновление таких устройств, которое тяжело провести среднестатистическому пользователю, «мертвые» продукты, которые снимают с производства уже через год после их выпуска, и для которых уже нет обновлений, скрытые функции, добавленные производителями устройств – все это реальные угрозы для пользователей IoT устройств, которые из виртуального пространства могут приводить к материальному ущербу, создавая колоссальные денежные потери компаний, аварии на производствах, потерю имущества и несчастные случаи.

В связи с этим, актуальной задачей становится поиск дополнительных, более эффективных методов защиты интернет-вещей, которые обеспечивали бы безопасные и устойчивые к взлому архитектуры.

Для начала, определим, что «интернет-вещью» (IoT-устройством) называется устройство, которое обладает следующими свойствами:

1) подключено к глобальной сети, передает и получает информацию от подобных объектов или от других устройств;

2) на основе полученных данных имеет возможность принять решение самостоятельно и реализовать его, или выполнить команду пользователя;
3) имеет уникальный идентификатор в сети передачи данных – IP-адрес;
4) имеет интерфейс для взаимодействия с пользователем.

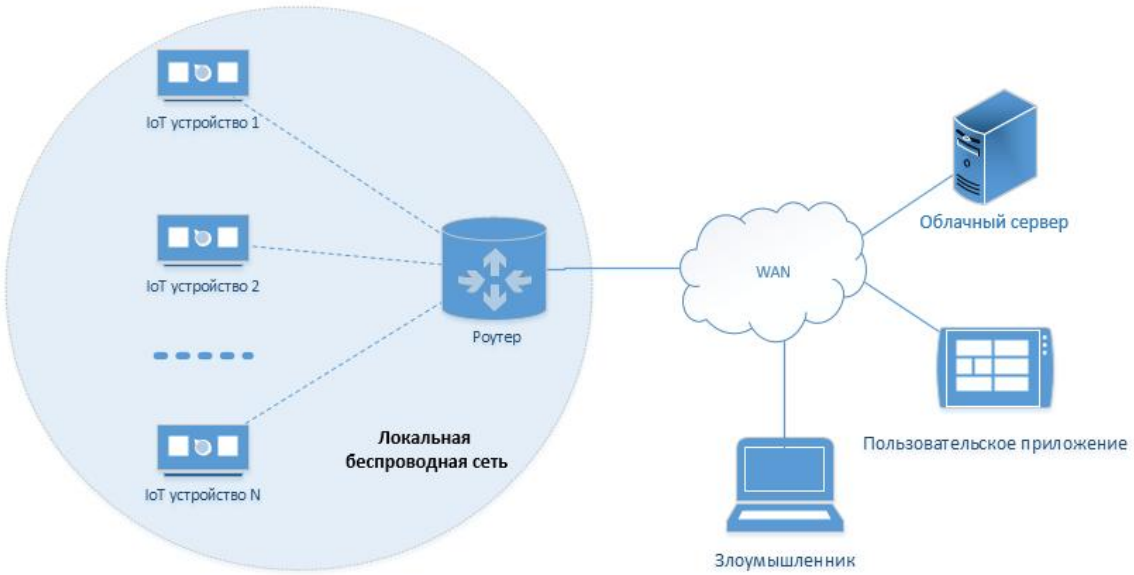


Рис. 1. Стандартная сеть интернета вещей, содержащая локальную сеть, облачный сервер, пользовательское приложение и злоумышленник, пытающийся подключится к ней

Итак, несмотря на миниатюрность и примитивность микроконтроллера IoT-устройства, кибер-атаки на интернет-вещи:

- могут скомпрометировать личные данные: пользователю неизвестно, что добавляется производителем в стандартную «прошивку» – например, если опустить очевидно «опасные» камеры, и рассмотреть обычный IoT-датчик температуры: устройство может быть запрограммировано отсылать данные на сторонние сайты сбора данных, такие как flymon.net, Gismeteo.ru, MajorDoMo, Narodmon.ru и другие – что создает, казалось бы, маленькую, неощутимую утечку не таких важных данных. Но любая, даже маленькая «брешь» в безопасности уже лишает систему статуса «защищенной», даже если пользователю не совсем очевидны последствия и будущий урон: неизвестно, знает ли пользователь об утечке, установит ли он датчик дома, а не на улице, как злоумышленник воспользуется «брешью» в своих целях – например, в этом случае даже простого датчика, вор, отслеживающий изменения датчиков на сайте, заметит, что один из них показывает необычно высокую температуру для улицы, а значит, это дом, а сейчас она понизилась – дома никого нет;
- могут навредить пользователю: взлом ПО умных автомобилей, медицинских агрегатов, носимых устройств, умных сетей электроснабжения (злоумышленник может удаленно установить модифицированную прошивку или просто поменять параметры системы, что приведет к аварии или несчастному случаю);
- могут достигать мирового масштаба: на интернет-вещи было совершено 5 глобальных атак компьютерными червями, диапазон действия которых охватил почти весь мир: Mirai, IoTWorm, BrickerBot, Persirai. Для нападения зловреды придерживаются следующей тактики: червь сканирует IP-адреса, и, затем, пользуясь списком из стандартных комбинаций «имя пользователя/пароль», задаваемых производителями

устройств по умолчанию, получает доступ к интернет-вещи. Затем объединяет все взломанные микроконтроллеры в единую бот-сеть (бот-сеть – также известна как ботнет) так называется сеть зараженных компьютеров, управление которыми осуществляет бот-мастер, а компьютеры могут контролироваться им удалённо без согласия владельца каждого компьютера) и осуществляет DDoS-атаки на крупные удаленные сервера.

Эти примеры и факты еще раз подтверждают важность защиты «глупых» умных солнечных батарей, тостеров и приставок, управляемых от локальной сети.

Предлагаемая архитектура

Для того, чтобы защитить пользователя и локальную сеть от нарушителя предлагается архитектура, построенная таким образом, что между локальной и глобальной сетью существует посредник, который выполняет функции прокси-сервера и межсетевого экрана, защищая устройство из глобальной сети (от всех атак, перечисленных в приложении Б), а также шифруя трафик между интернет-вещью и облачным сервером с помощью протокола SSL [0].

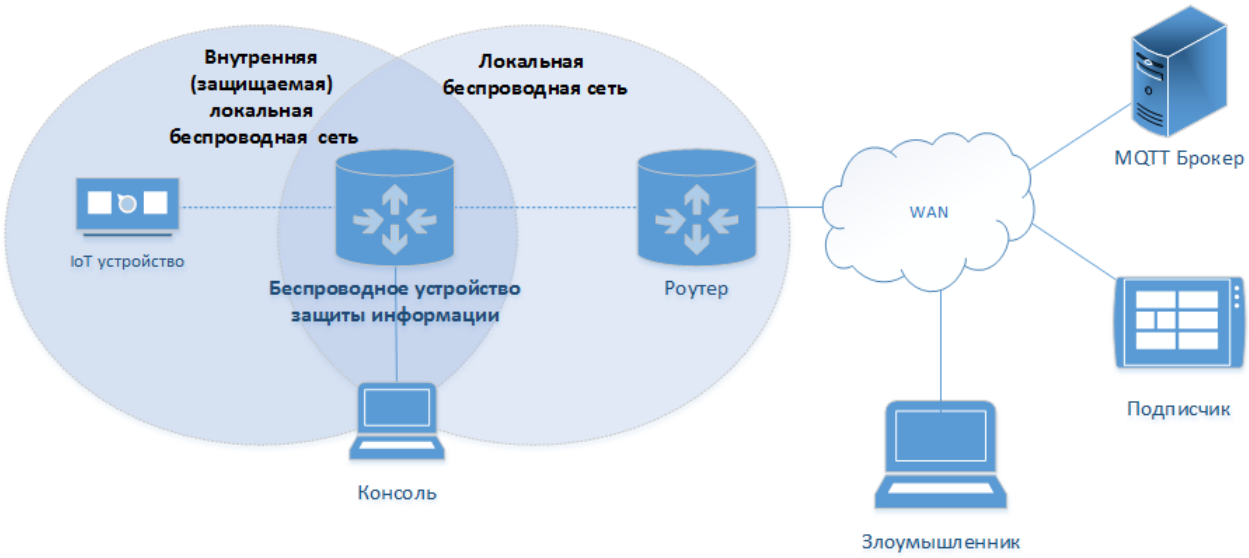


Рис. 2. Защищенная архитектура интернета вещей

Примерно такое же решение было представлено компанией Symantec в виде Wi-Fi роутера Norton Core, с отличиями, что он будет межсетевым экраном не только для IoT-устройств (но если интернет-вещь не общается по стандартным интернет-протоколам, то роутер уже не сможет защитить устройство), но и для вычислительных устройств, а также устройство не шифрует трафик.

Локальная сеть в предложенной архитектуре – сеть, построенная на основе технологии блокчейн. Она будет распределенной (отказ от центра сертификации, как, например, в популярном протоколе *MQTT*, использующихся для интернет-вещей, и всех сопутствующих «изъянов»), независимой от облачного сервера и от действий поставщиков ПО («подозрительные» устройства отстраняются от участия в создании блокчейн). Но также, эта сеть будет устойчива ко всем удаленным атакам и шифровать трафик.

Технология блокчейн в архитектуре с интернет вещами

В связи с многообразием интернет-устройств, трудностями в их настройке и с получением обновлений для них, брешами в протоколах связи в архитектурах интернета вещей – существует множество способов для взлома операционной системы устройства и получения прав суперпользователя, либо получения доступа на уровне web-приложения устройства. Участившиеся нарушения конфиденциальности и DDoS-атаки уже мирового масштаба,

совершающиеся с помощью IoT-устройств, зараженных червями и объединенных в ботнеты (так, в 2016 году ботнет, созданный червем Mirai, задействовал в своей кампании порядка 380 000 уязвимых устройств интернета вещей по всему миру: он сканировал интернет в поисках уязвимых роутеров, IP-камер, цифровых видеорегистраторов и т.п. Mirai совершенствуется злоумышленниками и продолжает функционировать и по сегодняшний день, а на его основе создаются новые зловреды) стали толчком к переосмыслению безопасности работы IoT-систем.

Прорыв биткойна в 2009 году – создание доверенной сети, где никто по определению не доверяет друг другу (без центра доверия), а также сама технология блокчейн – натолкнули разработчиков систем IoT на мысль об интеграции блокчейн в архитектуры с интернет вещами (достигнуть доверия там, где каждое из устройств может быть с легкостью взломано) – как выход на новый уровень безопасности.

С помощью блокчейн планируется уйти от многих минусов протокольных решений для интернета вещей. Использование блокчейн в архитектуре гарантирует:

I. Децентрализованность: отсутствие «доверенного центра», за счет того, что все транзакции проверены и подтверждены участниками. Также это позволяет построить одноранговую сеть и позволяет действовать участникам без подтверждения третьей стороной;

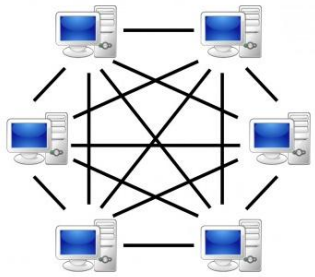


Рис. 3. Децентрализованная (одноранговая) архитектура, где каждый участник «наравне» с остальными

II. Устойчивость к отказам: транзакции записываются в цепочку и блокчейн хранится у каждого из участников – ни одна из записей не будет потеряна, изменена или удалена; из-за децентрализованной структуры выход из строя одного из участников не повредит всю систему (защита от DoS- и DDoS-атак);
III. Безопасность: шифрование транзакций криптографическим алгоритмом, их подтверждение консенсусным протоколом, невозможность подмены записи, и их доступность каждому из участников обеспечивает сети с блокчейн безопасность (например, защиту от атак «подмена доверенного пользователя») и прозрачность.

Существует немало работ, где исследователи пытались соединить блокчейн и технологию различных криптовалют (блокчейн биткоин и смарт-контракты эфириума) с интернет вещами [0][0][0]. Схематично архитектура сети в IoT (с одним устройством) с блокчейн выглядит следующим образом:

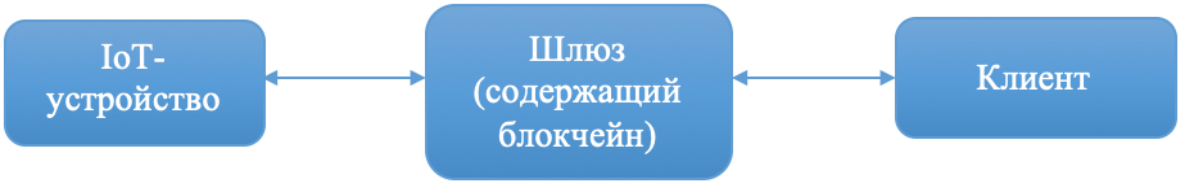


Рис. 4. Схема иллюстрирующая принцип работы части архитектуры с блокчейн.

При этом блокчейн в предложенной архитектуре отличается от принципа работы блокчейн в биткойне: больше нет майнеров, которые будут бороться за вознаграждение, и необходимость в

«сложности» вычисления (например, получить хэш, начинающийся с нуля, как в *PoW*) также отпадает.

Предложенная архитектура состоит из одной или нескольких локальных сетей IoT-устройств, «закрытых» шлюзами (контроллеры Raspberry Pi), которые будут являться прокси-серверами для каждой сети (защищенные также правилами ip-tables; таким образом интернет-вещи априори не будут доступны злоумышленнику из глобальной сети). Устройства передают зашифрованные транзакции шлюзам, а сами шлюзы соединены в блокчейн и хранить в себе ее локальную копию.

Транзакция в этом блокчейн – объединение всех показаний с нескольких устройств одной локальной подсети. За счет приватной блокчейн вместе они представляют одну большую «локальную сеть» в интернете. Такая сеть хорошо подойдет большой компании, где разным отделам или филиалам необходима будет актуальная информация собранная с IoT-устройств, которую можно будет легко запросить в любой момент.

Эффективность предложенной архитектуры подтверждается имитационным моделированием с помощью сетевого симулятора библиотеки NS-3.

Отметим, что решение блокчейн в настоящее время невозможно осуществить на микроконтроллерах интернета вещей: тогда необходимо реализовать блокчейн в виде протокола связи и подбирать специальные платы. Здесь рассматриваются интернет-вещи разных производителей, но сообщающихся со шлюзом по единому протоколу связи (например, MQTT).

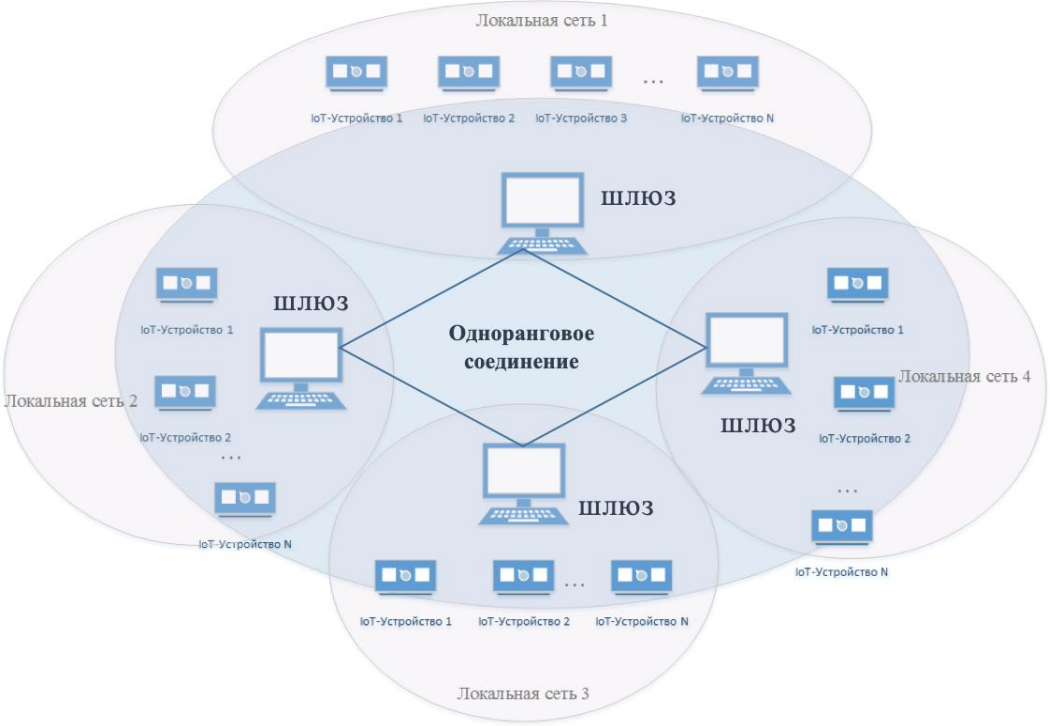


Рис. 5. Схема предложенной архитектуры с блокчейн

Недостатки классического блокчейн

Несмотря на то, что биткойновский блокчейн поможет защитить интернет-вещи от многих компьютерных атак, она также имеет недостатки и способы для совершения атак на сеть.

Недостатки (для работы с *IoT*):

1. **Блокчейн медленная:** создание одной транзакции занимает много времени (остальные транзакции «повисают» в некотором облачном сервере и ждут своей очереди: возникает ситуация «бутылочного горлышка») – после появления записи, необходимо ее подтверждение другими узлами (не менее 6 подтверждений), затем проходит наполнение блока такими подтвержденными транзакциями – все это тоже занимает время;

2. **Нехватка памяти для хранения записей:** каждый участник сети должен хранить копию всех записей блокчейн, что не будет препятствием для маленькой сети, но станет трудновыполнимой задачей для большой сети интрнета вещей, где у маленького устройства не хватит на это памяти (к примеру, каждый блок в сети биткойн весит 1 МБ); вопрос о месте хранения всех транзакций, особенно для огромных сетей интернета вещей остается открытым;

Также, архитектура, в основе которой будет лежать классический биткойновский блокчейн будет подвержена всем, характерным для него атакам.

Рис. 6. «Бутылочное горлышко», которое образует очередь в блокчейн.

В защищенной архитектуре интернета вещей предлагается использование технологии, применяемой в криптовалюте *IOTA*. *IOTA* (производная от буквы «йоты» греческого алфавита («крайне мало»)) – криптовалюта, транзакции которой планируется осуществлять с помощью интернета вещей. Алгоритм, используемый в *IOTA*, называется Tangle, он является *DAG* (направленный граф без циклов; представляет собой обобщение протокола блокчейн (блокчейн является частным случаем *DAG*; т.е. существует направленный граф без циклов (*DAG*) со множеством ответвлений и цепей, а цепью обычно называют «общепринятую историю» — цепь с наибольшей длиной, но создан специально для работы с интернетом вещей [0]. Tangle действует похожим на блокчейн образом – та же децентрализованная архитектура и механизм консенсуса – но в нем нет майнеров (все пользователи сети являются одновременно ее участниками) и нет блоков – только транзакции (то есть больше не надо ждать «наполнения» блока транзакциями). То, что делает архитектуру *IOTA Tangle* наиболее подходящим для работы с интернет вещами – это то, что чем больше транзакций приходит в сеть, тем быстрее они обрабатываются, а также независимость от постоянного подключения к сети (сеть может продолжать работать офлайн). Использование этого алгоритма в сети с интернет вещами увеличит производительность в сотни раз.

Заключение

Объединение блокчейн и IoT на сегодняшний день – имеет огромный потенциал, как в качестве криптовалюты (IOTA на данный момент на 10-м месте популярности криптовалют), так и в качестве непосредственной работы с интернет-вещами. Приспособленная к интернету вещей технология Tangle реализуется на устройствах IOTA и пока не готова к работе на реальных интернет вещах – и с помощью предложенной архитектуры предлагается проверить ее эффективность и показать, что Tangle и интернет вещи – могут быть еще и «безопасным сочетанием».

Литература

1. Исследование угроз и методов защиты трафика интернета вещей. *Походун А.И.* – Москва: МТУСИ, 2017. – 92.
2. An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain. Saptarshi Gan. – Kanpur: M.Tech, 2017. – 146.
3. *Y. Zhang, S.Kasahara Y. Shen, X. Jiang, and J. Wan* Smart Contract-Based Access Control for the Internet of Things. – 2018.
4. *S. Huh, S. Cho and S. Kim*. Managing IoT Devices using Blockchain Platform, in Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT). – 2017.
5. The Tangle. Version 0.5. Serguei Popov, for Jinn Labs December 28, 2015. – 25.
6. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии) / Учебное пособие для вузов / Москва, 2013.
7. *Шелухин О.И., Панкрушин А.П.* Оценка достоверности обнаружения аномалий сетевого трафика методами дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 110-115.
8. *Шелухин О.И., Панкрушин А.В.* Достоверность обнаружения аномалий сетевого трафика методом вейвлет-анализа // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2013. № 1. С. 176-179.
9. *Шелухин О.И., Филинова А.С.* Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 116-119.
10. *Шелухин О.И., Антонян А.А.* Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 6. С. 61-64.
11. *Шелухин О.И., Филинова А.С.* Сравнительный анализ алгоритмов обнаружения аномалий трафика методами дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 89-97.

PROVIDING SECURITY OF THE INTERNET OF THINGS ON THE BASIS OF THE BLOCKCHAIN

Anzhelika I. Pokhodun
Student of group M111701(73), MTUCI
an.pokhodun@gmail.com
Andrey V. Osin
MTUCI, PhD., associate professor of IS department
osin_a_v@mail.ru

Keywords: *Information Security, Internet of Things, Blockchain, IOTA, Tangle, DAG.*

Describes the relevance of the problem of security of the Internet of Things. The definition of an IoT device is given. A standard network with Internet of Things is considered and the possible consequences of feasible cyber attacks are presented. The blockchain technology is proposed as a secure communication protocol between IoT devices. The advantages of using the blockchain technology in a network with IoT devices and the disadvantages of the classic Bitcoin blockchain are considered. The use of the algorithm underlying the cryptocurrency IOTA is proposed. Proposed secure architecture of the Internet of Things is presented.

ОБЗОР ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СИСТЕМ ГЛУБОКОГО АНАЛИЗА ПАКЕТОВ DPI КОМПАНИИ ALLOT

Акопян Ваник Артакович
студент группы М091801(72), МТУСИ
ivanivan9668@gmail.com
Беленькая Марина Наумовна
МТУСИ, доцент кафедры МСиУС
mn.belenkaya@mail.ru

Ключевые слова*: Allot, DPI, анализ трафика, управление трафиком, блейд-модуль.*

Рассмотрено определение понятия *DPI*, представлены основные методы анализа трафика с помощью систем *DPI*, приведены основные направления использования технологии углублённой обработки пакетов, рассмотрена реализация *DPI* на аппаратном уровне компании Allot.

Анализ сетевого трафика – это очень обширная тема. Обычно под этим понимают совокупное название технологий и их реализаций по накоплению, обработке, классификации контролю модификации пакетов в зависимости от их содержимого в реальном времени.

Глубокий анализ пакетов *DPI* (Deep Packet Inspection или Deep Packet Processing) – это действия над пакетами, включающие их модификацию, фильтрацию и перенаправление. При этом системы DPI могут принимать решения не только по содержимому пакета, но и по косвенным признакам. Для этого может быть использован статистический анализ, расширенный список применений технологии классификации, приоритезации, маркировки и кэширования. DPI-технология разрабатывалась изначально для каналов связи со скоростью 100 Гбит/сек и для большого (порядка нескольких тысяч) идентифицированных приложений прежде всего седьмого уровня модели *OSI*.

С точки зрения реализации основным компонентом DPI является модуль классификации сетевых потоков. При этом может выполняться классификация по типу приложения (VoIp, P2P), по конкретному протоколу уровня приложения (HTTP, BitTorrent), приложению (Skype). В настоящий момент DPI является стандартом де-факто для средств анализа трафика и относится к области **критически важных** технологий для обеспечения сетевой безопасности и выполнения законодательства РФ и других стран в этой области. Поэтому принят целый ряд международных стандартов, например, ITU Y.2770 и ITU Y.2771.

Одна из тенденций последнего времени – централизация анализа, то есть реализация “DPI как сервис”. Суть концепции заключается в том, что при использовании большого количества различных средств анализа трафика (протокольные и кабельные анализаторы, оптимизаторы трафика, межсетевые экраны), имеет смысл вынести весь анализ на отдельное устройство. Оно будет выполнять полный разбор сетевых данных и рассылать результаты всем устройствам согласно их потребностей. Существуют программные реализации (Ipoque PACE, Widriver Contention Integration Engine), аппаратно-программные комплексы, привязанные к аппаратуре (Cisco NBAR), аппаратно – программные реализации отдельных производителей (Allot Communication). Рассмотрим более подробно последние решения.

Устройства компании Allot Communications серии NetEnforcer предназначены для корпоративных систем. NetEnforcer выполняет следующие функции: отслеживание сетевого трафика приложений и пользователей, управление трафиком. Последнее обеспечивает оптимизацию услуг доступа. Полоса пропускания варьируется в пределах от 10 Мбит/с до 8 Гбит/с в режиме Full Duplex (полнодуплексном). Также устройства серии NetEnforcer визуализируют сети, применяют политики и перенаправляют трафик с целью предоставления дополнительных услуг в разных сегментах корпоративных сетей и сетях провайдеров.

В таблице 1 представлены характеристики устройств серии Allot NetEnforcer.

Таблица 1

Характеристики устройств серии Allot NetEnforcer

Allot NetEnforcer	AC-500	AC-1400 / AC-3000	AC-6000
Полоса пропускания на платформу	От 10 до 200 Мбит/с	От 45 Мбит/с до 8 Гбит/с (4 Gbps Full Duplex)	От 2 до 16 Гбит/с (8Gbps Full Duplex)
Количество сетевых портов	2 или 4 x 10 / 100 / 1000BASE-T	8 x 10 / 100 / 1GESX/LX/ZX (медный кабель)	8 x 1GESX/LX/ZX (медный кабель) 8 x 10GE / 1GESR/LR/ER
Макс. количество подключений и потоков	256000 / 512000	2 / 4 млн	5 / 10 млн
Количество абонентов	20 000	160 000	400 000
Перенаправление трафика	4 медных порта 10 / 100 / 1 GEдля перенаправления трафика во внешние сервисы (No steering on AC500)		Любой порт может использоваться для резервирования или перенаправления трафика

Устройство поддерживает широкий спектр сигнатур (признаков протоколов и приложений). Это позволяет операторам фильтровать различные виды torrent-трафика (torrent - файл, который содержит метаданные о контенте, загружаемый пользователем), приложения в социальных сетях, предоставлять подробные отчеты по использованию трафика и дать возможность пользователям управлять своей полосой в виртуальных контекстах. Другим словом, предоставлять клиентам дополнительный сервис и повысить качество услуг. В таблице 2 представлены примеры поддерживаемых приложений протоколов.

Таблица 2

Примеры поддерживаемых приложений и протоколов 7-ого уровня модели OSI

P2P (Peer-to-Peer)	включая BitTorrent, eDonkey, Ares, Gnutella, Thunder, Winny, eMule, Vuze
VoIP (Voice over Internet Protocol) и IM (Instant Messaging)	включая Windows Live Messenger, SIP, Skype, Yahoo Messenger, GoogleTalk, Fring, WhatsApp, STUN, ICQ, Viber, и QQ
Игровые	включая World of Warcraft, Final Fantasy, Guitar Hero, Second Life, QQ Games, Lineage, CounterStrike, Call of Duty, Apple Game Center
Веб	включая HTTP,мобильные приложения и приложения социальных сетей
Потоковые	включая YouTube, RTMP, QQ live, PPStream, DailyMotion, HTTP потоковое, HTTP аудио, NetFlix, и Facebook
Обмен файлами	включая FTP, HTTP загрузки, Apple App Store и Android Market
Инкапсуляция трафика	включая L2TP, MPLS, PPPoE и Teredo

Устройства Allot Service Gateway включают в себя средства анализа и визуализации сети, а также применения политик и сервисы с целью увеличения доходов оператора связи. Данные оборудования предназначены для фиксированных, мобильных (3G/4G/LTE) и конвергентных сетей широкополосного доступа.

Allot Service Gateway безошибочно производит идентификацию абонентского трафика в реальном времени на скоростях до 160 Гбит/с. Полученные данные устройство использует для оптимизации использования полосы пропускания. Кроме того применяет политики качества обслуживания и управляет трафиком для различных абонентских и сетевых сервисов, развернутых на платформе и за ее пределами.

Allot Service Gateway является основой для предоставления услуг. Провайдеры с помощью устройств серии Service Gateway могут сократить эксплуатационные расходы путём создания новых источников дохода благодаря индивидуальному обслуживанию и высокому уровню взаимодействия с абонентами, ведущими образ жизни онлайн.

В состав устройств Service Gateway входят модули обработки трафика (Core Controller - CC), контроля потоков (Switch and Flow Balancer - SFB), backplane модуль (RBS) и Шасси (Chassis).

В таблице 3 представлены характеристики устройств серии Allot Service Gateway.

Таблица 3

Характеристики устройств серии Allot Service Gateway

Allot Service Gateway	Sigma E6	Sigma E14
Шасси	6 слотов	14 слотов
Модуль обработки трафика	1 - 4 (плата занимает 1 слот)	От 2 до 10 (плата занимает 1 слот)
Модуль контроля потоков	1 или 2 (плата занимает 1 слот)	От 2 до 4 (плата занимает 1 слот)
Bypass (BP) Blade	1 плата (8 портов) или внешний	От 1 до 2 плат (по 8 портов каждый) или внешних
Полоса пропускания на платформу	До 64 Гбит/с	До 160 Гбит/с
Полоса пропускания на кластер	До 360 Гбит/с	До 1 Терабит/с
Количество сетевых портов	До 8 портов 10GE или 32 портов 1GE	До 16 портов 10GE или 32 портов 1GE
Количество абонентов	До 3 200 000	50 млн / 100 млн
Макс. число соединений и потоков	20 / 40 млн	50 / 100 млн

Данные программно-аппаратные средства устройства обладают следующими функциями:

- Перенаправление трафика: трафик перенаправляется в сервисы, работающие на блейд-модулях (также блейд-сервер, представляет собой компьютерный сервер с вынесенными и обобщенными компонентами в корзине с целью уменьшения занимаемого пространства) в платформе, поддерживающее «горячую» замену, в реальном времени или развёртывание на внешних системах.
- Сбор данных: сбор данных, сессий и отчётов использования сети и дальнейший экспорт в системы анализа и биллинга.
- Обнаружение тетеринга (совместного доступа к мобильному интернету): выявление тетеринга, и применение политик оператора в отношении тетеринга в реальном времени.
- Предложение операторами связи таких услуг, как SLA, QoS, SelfProvisioning и др.

Кроме того в NetEnforcer реализованы ряд дополнительных функций:

- реализация технологии DART (Dynamic Actionable Recognition Technology – технология распознавания трафика не только по протоколам прикладного уровня или по приложениям, но и по принадлежности трафика тому или иному пользователю, по типу и производителя устройства, по контексту использования приложений и т.д.),

- обработка ассиметричных потоков (передаваемые с разными скоростями в прямом и обратном направлениях),
- поддержка протокола OpenFlow и т.д.

А в Service Gateway кроме всего вышеперечисленного реализовано:

- резервирование на уровне системы по схеме 1+1,
- резервирование на уровне модулей анализа сетевого трафика по схеме N+1,
- определение ассиметричных потоков при прохождении двух направлений одного потока по разным маршрутам, контролируемым несколькими платформами и др.

Последние перечисленные функции крайне необходимы в ЦОД (центрах обработки данных).

Аппаратное обеспечение, являющееся частью выше описываемых решений, использует специальные сетевые карты (NIC) для захвата трафика. Это интегральные схемы специального назначения – ASIC (Application Specific Integrated Circuit). Вся обработка буферов карт закладывается производителем в микросхемную базу (включая сигнатуры). Используются также специальные виды ассоциативной памяти для параллельного сравнения своего содержимого с поступившем на вход значением (CAM), специального вида процессоры для обработки сетевого трафика (NP) с поиском по шаблонам, ключам, управлению очередями.

Выводы

Все решения, предоставленные компанией Allot Communications, крайне перспективны и поддерживают весь диапазон требований к системам DPI.

При этом решения серии NetEnforcer относятся к младшему сегменту оборудования DPI и их пропускная способность составляет от 200 Мбит/с до 16 Гбит/с в зависимости от конкретной модели.

Решения Service Gateway относятся к среднему и старшему сегментам DPI, их пропускная способность оборудования – от 64 Гбит/с до 500 Гбит/с в зависимости от конкретной модели. Имеется возможность довести значение максимальной пропускной способности до 2 Тбит/с.

Изучение технологий компании ALLOT Communication, их программных и аппаратных реализаций необходимо для последующей разработки собственных систем DPI.

Литература

1. Allot NetEnforcer & Service Gateway Documentation // Allot Communications.
2. *Jakub Svoboda.* Network Traffic Analysis with Deep Packet Inspection Method. Masatyk University Faculty of Informatics
– Brno, Spring 2014.
3. *John Klein.* Digging Deeper Into DPI Network Visibility & Service Management // Allot Communications, 05.2007
4. *Д. О. Прохоров, А. В. Креймер, В. В. Трофлянин.* Вопросы анализа производительности в инфокоммуникационных сетях. Шестая межвузовская студенческая конференция, 2017.
5. *Беленькая М. Н., Малиновский С. Т., Яковенко Н. В.* Администрирование в информационных системах. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2018.
6. *Малиновский С.Т., Беленькая М.Н., Спиридонов А.А., А.А.* Метод повышения производительности транспортного протокола TCP в глобальных корпоративных сетях передачи данных // T-Comm: Телекоммуникации и транспорт. 2010. Т. 4. № 7. С. 39-42.
7. *Беленькая М.Н., Малиновский С.Т., Васильев А.В.* Разработка алгоритма планировщика выполняемых задач гипервизора XEN // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 28-30.

DPI SYSTEM FUNCTIONALITY OF THE ALLOT COMPANY OVERVIEW

Vanik A. Akopyan
student of group M091801(72), MTUCI
ivanivan9668@gmail.com
Marina N. Belenkaya
MTUCI, Associated professor of the department of multimedia networks and communication services
mn.belenkaya@mail.ru

Keywords*: allot, DPI, traffic analysis, traffic management, blade-module.*

Here is given the definition of the *DPI* concept, the main methods of analyzing traffic using *DPI* systems are presented, the main directions of using deep packet inspection technology are considered, the realization of *DPI* at the hardware level by Allot Communications.

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ПРИ ПРОЕКТИРОВАНИИ ИНТЕЛЛЕКТУАЛЬНОГО ДИАЛОГОВОГО ПОМОЩНИКА

Сидорина Светлана Александровна
магистр группы М151801(70) МТУСИ
sve82383357@mail.ru
Стрельников Владимир Геннадьевич
магистр группы М151701(70) МТУСИ
strel-prod@yandex.ru
Трунов Артем Сергеевич
МТУСИ, старший преподаватель кафедры ИСУиА,
greek17@yandex.ru

Ключевые слова: *Машинное обучение, классификация, SVM, диалоговые помощники, word2vec, tf-idf*

В работе описан выбор алгоритма машинного обучения для реализации модуля обработки входящих запросов и определению намерения диалогового помощника. Основная задача заключается в обучении алгоритмов машинного обучения на основе представления данных Count Vectors, TF-iDF, а также средствами предварительно обученной модели skip-gram как одной из реализаций алгоритма word2vec. Для повышения точности обучения модели применялись методы стемминга и лемматизации. В качестве алгоритмов рассматривались: логистическая регрессия, SVM, мультиномиальный наивный байесовский классификатор и RandomForest.

На сегодняшний день с помощью инструментов машинного обучения возможно научить компьютер понимать естественный язык, что является достаточно актуальной задачей. С помощью определенных алгоритмов и методик [1, 3-5] стало доступно осуществлять морфологический анализ фраз, извлекать именованные сущности из текста, управлять диалогом с сохранением контекста и выполнять другие манипуляции. Целью данной работы является проектирование интеллектуального диалогового помощника для студентов МТУСИ, способного методами машинного обучения выдавать пользователю осмысленный ответ, на основе запрашиваемой информации по: расписанию, текущей неделе, сайту и т.д. Запрашиваемая информация должна быть классифицирована, каждый класс определяет намерения пользователя, но основе которых выдается релевантный ответ.

Задача заключается в выборе алгоритмов машинного обучения для обучения модели, которая позволит определять намерения пользователя на основе введенных данных. Ожидается, что система будет обрабатывать запрос, введенный в свободной форме и выдавать наиболее релевантную информацию. При этом необходимо провести испытания на способность алгоритмов классифицировать новые данные и по результатам перекрестной проверки выбрать алгоритм с наилучшими показателями. Таким образом будет реализован модуль предварительной обработки запроса уже непосредственно при работе интеллектуального помощника.

Интеллектуальный диалоговый помощник

В качестве основных действий, которые реализует диалоговый помощник принято выделять задачи поддержания беседы на свободные темы (small-talk) и выполнение конкретных бизнес-задач (business-talk).

Доступ к интеллектуальному помощнику осуществляется под оболочкой готовой системы (мессенджера) посредством API (Application Programming Interface). За счет имеющегося набора методов и структур процесс разработки во многом упрощается. Как одно из преимуществ — это отсутствие необходимости локально хранить сообщения, идентификаторы и т.д., так как

благодаря API можно обращаться к серверам платформы и получать эту информацию. При этом не нужно знать, как устроена база данных, из каких таблиц и полей каких типов она состоит, так как синтаксис запросов и тип возвращаемых ими данных строго определены на стороне самого сервиса.

Взаимодействие с пользователем строится на модели клиент-серверной архитектуры как изображено на рисунке 1.

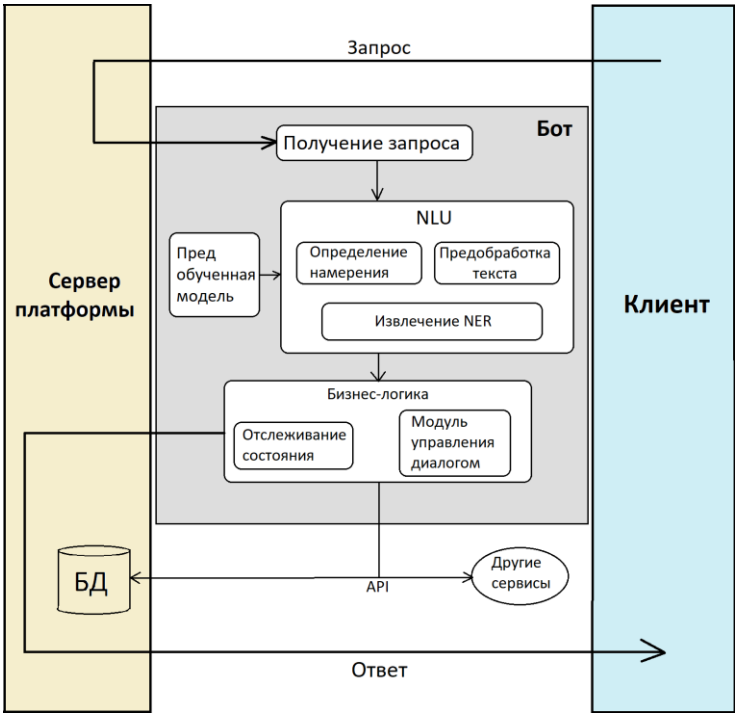


Рис. 1. Архитектура диалогового помощника

Изначально формируется набор намерений (бизнес-задач), которые решает диалоговый помощник. Сформированный запрос пользователя сначала отправляется на сервер платформы, после чего передается на разработанный сервер диалогового помощника. Далее запрос попадает в модуль NLU (Natural Language Understanding), где определяется намерение (intent) и извлекаются «именованные сущности». В общем виде блок состоит из предварительной обработки текста, классификации запроса, то есть соотнесение с одним из классов, известных системе, и извлечения параметров запроса.

В блоке бизнес-логики реализуется связь с предыдущими и последующими высказываниями за счет отслеживания состояния. Тут же на базе извлечённых данных выполняется управление диалогом в соответствии с заданным сценарием. При необходимости идет обращение к внешним ресурсам. В базе данных сохраняется контекст и параметры диалога для обработки последующих обращений. Затем генерируется текстовый ответ с использованием макроподстановок и функций согласования слов на естественном языке и отправляется пользователю.

Формирование обучающего набора

При проектировании интеллектуального помощника изначально сформировано 5 намерений, которые будут им обрабатываться. Для каждого намерения были продуманы списки фраз, которые могут быть сформулированы пользователем. Данные наборы фраз представляют собой обучающую выборку (705 фраз), на которой будут обучены и протестированы выбранные алгоритмы. В таблице 1 приведено их краткое описание, примеры фраз, на основе которых производится классификация намерения, а также число сформированных фраз для обучения алгоритмов.

Таблица 1

Описание сформированных намерений

Намерение	Описание	Пример фраз	Кол-во фраз
i_exam_period	Выводится информация о сессии	• когда будут зачеты • уточни, когда начинается сессия	223
i_my_shedule	Выводится информация о расписании для группы пользователя	• пары моей группы • выведи расписание группы	195
i_current_week	Выводится информация о текущей неделе	• какая текущая неделя • узнай какой номер недели	125
i_web_site	Выводится информация о сайте	• ссылку на сайт мтуси • пришли ссылку на сайт	90
i_my_group	Запрос на изменение номера группы	• добавь номер группы • измени мою группу	72

Работа с текстовыми документами вызывает определенные трудности в их визуализации, т.к. подходы, например, Bag of Words [1] формируют высокоразмерные векторы, описывающие документы. Для уменьшения размерности данных векторов воспользуемся алгоритмом машинного обучения – t-SNE.

t-SNE (t-Distributed Stochastic Neighbor Embedding) – метод уменьшения размерности, который особенно хорошо подходит для визуализации многомерных наборов данных [2]. Данный метод моделирует каждый высокоразмерный объект, например, в двухмерную точку таким образом, что подобные объекты моделируются близлежащими точками, а разнородные объекты с высокой степенью вероятности моделируются удаленными точками. То есть схожие объекты будут лежать недалеко друг от друга в пространстве, а объекты, которые отличаются друг от друга лежат на большем расстоянии.

В результате применения данного метода с двумя компонентами на обучающей выборке, преобразованной к «мешку слов», была получена визуализацию документов, представленная на рис. 2.

На рис. 2 можно заметить, что документы внутри класса образуют небольшие «облака» точек, которые хорошо разделимы между собой. Можно предположить, что алгоритмы машинного обучения для решения задачи классификации так же хорошо найдут данные зависимости, выдавая высокое значение точности.

Представление данных текстовых документов в векторную модель

Перед началом обучения необходимо привести исходный набор данных к понятному для алгоритмов машинного обучения виду. Для этого надо преобразовать фразы к векторной форме. Существует ряд методик, позволяющих выполнить данную операцию. Стоит обратить внимание, что на исходной выборке не надо проводить очистку данных, приводить к нижнему регистру и т.д., так как она генерируется вручную, и данные операции выполнены заранее. Однако на вновь

поступивших данных уже при работе интеллектуального помощника будет разработан модуль для предварительной обработки запроса пользователя.

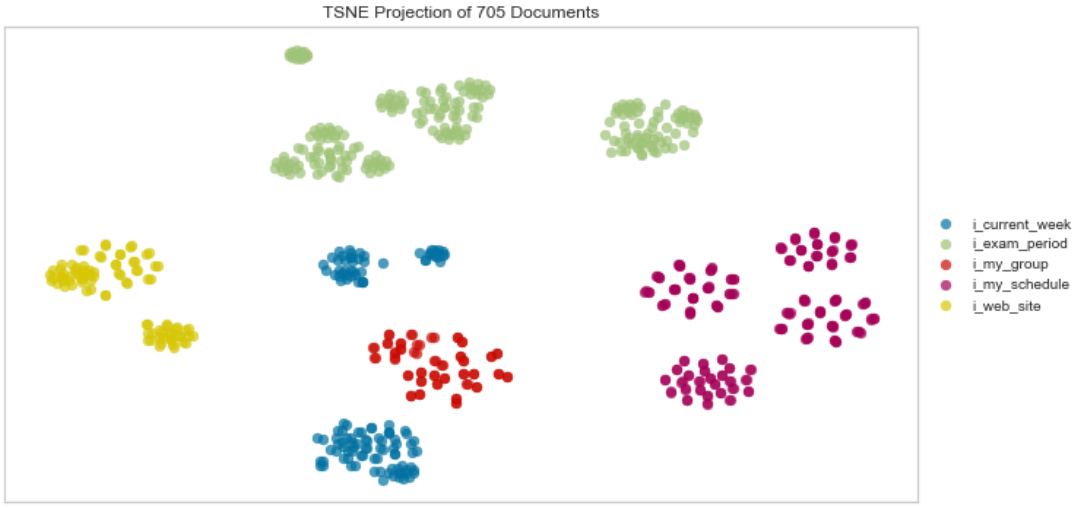


Рис. 2. Визуализация обучающей выборки алгоритмом t-SNE

Bag of Words (от англ. «мешок слов») [1] – в этой модели текст представляется в виде набора слов без учета грамматики и даже порядка слов. Формируется словарь всех уникальных слов из обучающей выборки, после чего каждому документу ставится в соответствие вектор из полученного словаря, заполненный нулями. Наличие слова в предложении, которое содержится в словаре, помечается единицей.

Count Vectors [1] – основан на модели «мешка слов». Он представляет собой матрицу, строки которой соответствуют отдельному тексту, а столбцы – определенным словам. Пересечение строки и столбца содержит число, определяющее количество вхождений слова в текст.

TF-iDF – основан на модели мешка слов [1]. Используется для оценки важности слова в документе, являющегося частью коллекции документов, рассчитывается по следующей формуле:

$$TF - IDF(t, d, D) = TF(t, d) \times IDF(t, D)$$, где

TF – частота слова в документе, определяет его «важность» в пределах отдельного документа, IDF – обратная частота документа, уменьшает вес широко употребляемых слов в коллекции документов. То есть общеупотребительные слова будут иметь меньший вес, а часто употребительные слова, но в рамках конкретного класса, имеют больший вес.

word2vec [3] – это инструмент (набор алгоритмов) для расчета представлений слов, реализует две основные архитектуры – CBOW и Skip-gram. word2vec обучается на прочтении огромного количества текста с последующим запоминанием того, какое слово возникает в схожих контекстах. После обучения на достаточном количестве данных, word2vec генерирует вектор из 100-500 измерений для каждого слова в словаре, в котором слова со схожим значением располагаются ближе друг к другу. В данной статье используется уже предварительно обученная модель Skip-gram [1] размерности 100. То есть word2vec формирует для каждого слова вектор из 100 значений. Так как фразы состоят из нескольких слов, то получаем набор из векторов. Однако разные фразы могут содержать разное количество слов, поэтому возникает проблема единой размерности, которая решается путем усреднения векторов слов в рамках фразы.

Кроме того, для возможного повышения точности обучения применяются подходы по приведению к нормальной форме слова. Предположим, что обучающая выборка содержит слово, которое пользователем будет введено с другим окончанием. В таком случае, данного слова не окажется в словаре, хотя они похожи. Для устранения таких проблем применяют: стемминг или лемматизацию.

Стемминг – это процесс нахождения основы слова, которая не обязательно совпадает с морфологическим корнем слова [1]. Стеммер Портера – одна из реализаций стемминга, алгоритм

которого не использует баз основ слов, а лишь, применяя последовательно ряд правил, отсекает окончания и суффиксы, основываясь на особенностях языка.

Лемматизация – это метод морфологического анализа, который сводится к приведению словоформы к ее первоначальной словарной форме (лемме) [1]. Например, существительное в именительный падеж и единственной число, глагол в инфинитивную форму.

Обучение моделей машинного обучения и их оценка

Описанные выше подходы по представлению данных могут применяться по отдельности. В данной работе произведено обучение алгоритмов на основе: Count Vectors, TF-iDF, word2vec, а также их вариации с применением стемминга и лемматизации.

В качестве алгоритмов для обучения выбраны: логистическая регрессия, SVM (с линейным и полиномиальным ядрами), мультиномиальный наивный байесовский классификатор [4] и RandomForest [5].

Предварительно обучающая выборка была разбита на тренировочную и тестовую (отложенную). На тренировочной выборке проводилась перекрестная проверка с разбиением на 5 частей. На отложенной выборке проводилась оценка способности алгоритма классифицировать новые данные. В результате перекрестной проверки были получены результаты, представленные на рис. 3. Оценка алгоритмов производилась то метрике “accuracy” – отношение верно предсказанных классов для фраз к общему числу фраз.

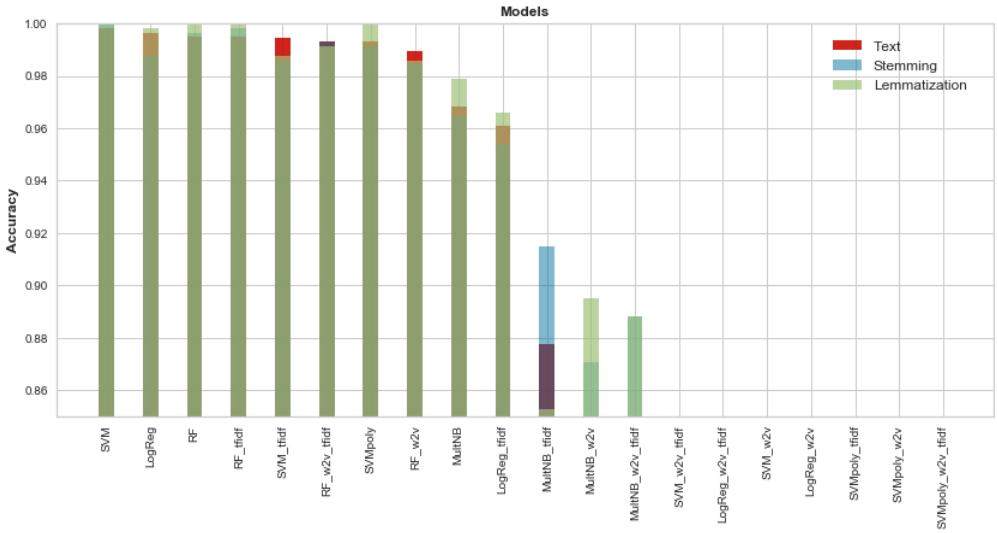


Рис. 3. Результаты перекрестной проверки

Было отобрано 5 алгоритмов с предобработкой, которые показали лучшие результаты для стемминга, лемматизация и без приведения слов к основе, на которых провелось тестирование на отложенной выборки.

Наилучший результат продемонстрировал SVM с линейным ядром для всех типов предварительной обработки слов. Все результаты сведены в табл. 2.

Таблица 2

Лучшие результаты на перекрестной проверке

Non preprocessed			**Stemming**			**Lemmatization**		
model	**accuracy**		**model**	**accuracy**		**model**	**accuracy**	
	CV	Holdout		CV	Holdout		CV	Holdout
SVM	0,9983	1	SVM	1	1	SVM	1	1
LogReg	0,9965	1	RF_tfidf	0,9982	1	RF	1	1
RF	0,9948	1	RF	0,9964	1	RF_tfidf	1	1
RF_tfidf	0,9948	1	RF_w2v_tfidf	0,9930	0,9929	SVMpoly	1	0,9929
SVM_tfidf	0,9947	0,9929	SVMpoly	0,9912	0.9929	LogReg	0,9982	0,9929

На основе полученных результатов выбран алгоритм SVM («метод опорных векторов») с линейным ядром для определения намерения пользователей. В методе опорных векторов строится разделяющая гиперплоскость таким образом, чтобы максимально далеко отстояла от ближайших к ней точек обоих классов. Первоначально данный принцип классификации возник из эвристических соображений: вполне естественно полагать, что максимизация зазора между классами должна способствовать более уверенной классификации.

Заключение

В результате проектирования интеллектуального помощника было произведено обучение модели на основе метода машинного обучения SVM с линейным ядром на основе матрицы Count Vectors с применением лемматизации. Данная модель была сохранена и может быть использована для работы модуля по определению намерения пользователя по введенной им фразе. Таким образом, разработан модуль, позволяющий определять вызываемые намерения пользователем. Стоит заметить, что при запуске помощника, необходимо вести логирование диалогов, которое позволит сформировать новый набор данных для обучения модели на большем числе фраз. Следующим этапом в проектировании интеллектуального диалогового помощника является формирование модуля по извлечению именованных сущностей.

Литература

1. *Ю.А. Осипова, Д.Н. Лавров.* Применение кластерного анализа методом k-средних для классификации текстов научной направленности - Математические структуры и моделирование, № 3(43), с. 108–121, 2017
2. *L. van der Maaten, G.E. Hinton.* "Visualizing Data Using t-SNE" - Journal of Machine Learning Research. 9: 2579–2605, 2008
3. T*omas Mikolov, Quoc V. Le, Ilya Sutskever* "Exploiting Similarities among Languages for Machine Translation" arXiv:1309.4168v1, 2013
4. Multinomial Naive Bayes Classifier for Text Analysis (Python) [Электронный ресурс]. – Режим доступа: https://towardsdatascience.com/multinomial-naive-bayes-classifier-for-text-analysis-python-8dd6825ece67 (дата обращения: 25.10.2018)
5. *T. Hastie, R. Tibshirani, J. Friedman.* Chapter 15. Random Forests // The Elements of Statistical Learning: Data Mining, Inference, and Prediction — Springer-Verlag, 2009.

THE USAGE OF MACHINE LEARNING METHODS IN THE DESIGNING OF INTELLIGENT DIALOG ASSISTANT

Sidorina A. Svetlana
Student of group M151801(70), MTUCI
sve82383357@mail.ru
Strelnikov G. Vladimir
Student of group M151701(70) MTUCI
strel-prod@yandex.ru
Trunov S. Artem
MTUCI, senior lecture of department ISMaA
greek17@yandex.ru

Keywords: *Machine learning, classification, SVM, dialog assistants, word2vec, tf-idf*

The paper describes the choice of machine learning algorithm for the implementation of the module processing incoming requests and determination of intent of the dialog assistant. The main task is to train machine learning algorithms based on data representation of Count Vectors, TF-iDF, as well as means of pre-trained model skip-gram as one of the implementations of the algorithm Word2Vec. Methods of stemming and lemmatization were used to improve the accuracy of the model training. Logistic regression, SVM, multinomial naive Bayesian classifier and RandomForest were considered as machine learning algorithms.

АНАЛИЗ РАБОТЫ КОМПИЛЯТОРОВ OPENWATCOM И GNU COMPILER COLLECTION (GCC) ДЛЯ УСЛОВИЙ ПРЕДОТВРАЩЕНИЯ ОШИБКИ ПЕРЕПОЛНЕНИЯ БУФЕРА

Корионов Игорь Павлович
магистрант группы М111801(73), МТУСИ
tyiiia_abr@mail.ru

Ключевые слова: *переполнение буфера, компилятор, линкер, уязвимость, GNU GCC, OpenWatcom.*

Приведены результаты сравнительного анализа компиляторов *GNU GCC* и OpenWatcom находящихся в свободном доступе. Рассмотрены некоторые вопросы безопасности информационных систем и определены типы, связанные с переполнением буфера. Проведен анализ актуальности уязвимости информационных систем обусловленной переполнением буфера. Предложено прогностическое решение по предотвращению атак использующих переполнение буфера.

Переполнение буфера — это наиболее распространенная ошибка в приложениях. На данный момент число вирусов, которые написаны на основе уязвимости *buffer overflow*, превысило две тысячи. Из всех возможных типов уязвимостей информационных систем переполнение буфера занимает 1-ое место по частоте появления. Ежедневно обнаруживается огромное количество ошибок на основе переполнения буфера, примерно 40-45 % от общего количества уязвимостей [1].

Обеспечение безопасности является невероятно сложной для решения проблемой [2]. До сих пор не разработана единая и связная теория обеспечения безопасности информационных систем. Это обусловлено не только сложностью, но и неординарностью задачи. В мире для борьбы с атакой типа buffer overflow используют сложнейшие средства анализа трафика *DPI* (*deep packet inspection*), а также продуманную глубокую настройку сетевого оборудования системы [3, 6].

Переполнение буфера является преднамеренной угрозой и всегда осуществляется по вине пользователей системы или прикладных программистов. Рассмотрим некоторые типы атак, для проведения которых используют переполнение буфера.

1. Атаки приложений. Эти атаки представляют собой попытки атаковать уязвимости в прикладном программном обеспечении. Как пример, атаки, направленные на сервера приложений. Администратору системы необходимо подписаться на официальную рассылку производителя для получения информации об уязвимостях приложений, своевременно устанавливать программные заплатки, предлагаемые производителем и связанные с защитой приложений, всегда контролировать ресурсы серверов.

2. Атаки «отказ в обслуживании» (*Denial of Service, DoS*). Атака заключается в том, чтобы привести атакуемую систему или части этой системы в неработоспособное состояние. Результат достигается, например, дискредитацией и блокированием учетных записей пользователя, или ищется неквотируемый ресурс, необходимый прикладному процессу, или некорректно обрабатываемая ошибка в программном коде, приводящая к «зависанию» процесса программы. Такие атаки могут привести к серьезной потере доходов предприятия. Вместе с входной и выходной фильтрацией администратор системы должен согласовать действия с оператором связи, например, контролировать число соединений, разрешенных для рабочей станции [2].

Рассмотрим работу компиляторов на предмет выявления ошибки переполнения буфера. Для анализа были выбраны компиляторы *OpenWatcom* и *GNU Compiler Collection*, так как они являются свободным программным обеспечением.

Как известно, компилятор — программа или техническое средство, выполняющее перевод исходного кода программы, составленного на языке высокого уровня, в программу на низкоуровневом языке, близком к машинному коду (позиционно-независимый код, машинно-ориентированный код, язык ассемблера). Входная информация для компилятора это описание

алгоритма или исходный код программы на предметно-ориентированном языке, а то, что получилось на выходе компилятора — эквивалентное описание алгоритма на языке понятном линкеру для последующей сборки программы.

Линкер — программа, которая производит компоновку, то есть принимает на вход один или несколько объектных модулей и собирает по ним исполнимый модуль.

OpenWatcom C/C++ это кроссплатформенный высокопроизводительный оптимизирующий компилятор языков *C/C++* с включенным набором средств для отладки и разработки. Отличительными чертами компилятора являются быстрая скорость компиляции исходных кодов, а также широкий спектр утилит, таких как: интегрированная графическая среда разработки *IDE* под *Windows* и *OS/2*; редактор *VI* под *Linux*. Также в компиляторе присутствуют средства отладки (встроенный debugger) и дизассемблер. Линкер позволяет отключить использование стандартных библиотек, что дает возможность создавать независимый от какой-либо определенной ОС код, что, в свою очередь, позволяет написать свою операционную систему [4].

GNU Compiler Collection (GCC) представляет собой комплект компиляторов для большого количества языков программирования. *GCC* является свободным программным обеспечением и определяется фондом свободного программного обеспечения (FSF) на условиях *GNU GPL (GNU General Public License*) и *GNU LGPL (Lesser General Public License*). Его используют в качестве компилятора в открытых *Unix*-подобных ОС, и в некоторых закрытых операционных системах, в том числе *Apple Mac OS X*. Компиляторы GCC используют интерфейсы стандартные для *Unix*. Драйвер *gcc* определяет аргументы вызова и решает, какой из компиляторов следует применить к входному файлу, после чего запускает его, ассемблирует и, если это требуется, линкует результат, чтобы получить окончательный исполняемый файл [5].

Анализ работы компиляторов *GCC* и *OpenWatcom* на предмет выявления ошибки переполнения буфера, проводился путем сборки в исследуемом компиляторе программы, код которой содержит ошибку переполнения буфера, с последующим запуском этой программы под управлением операционной системы *Windows*.

При этом программа собралась в компиляторе *OpenWatcom*, не смотря на то, что код содержал явную уязвимость, которую возможно использовать для переполнения буфера. При запуске этой программы она немедленно завершила свою работу и выдала сообщение об ошибке. В окне ошибки (Рис. 1) указана область в памяти где произошла ошибка, а также её характер. Встроенный дебаггер также указывает на тип ошибки (Рис. 2), её местоположение в коде и область в памяти. Набор полученных сведений и наличие дебаггера, помогает нам устранить ошибку и, впоследствии - уязвимость переполнения буфера в программе.

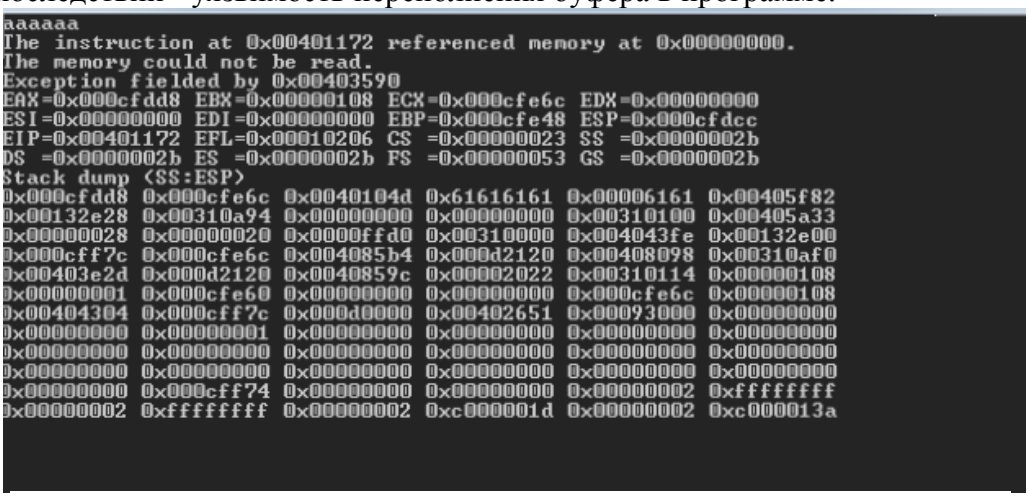


Рис. 1. Результат запуска программы, скомпилированной в OpenWatcom

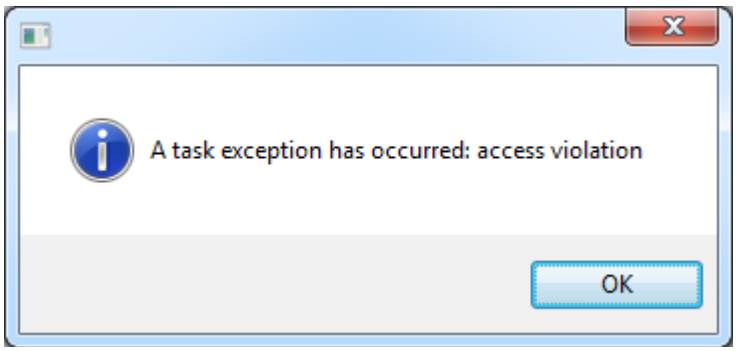


Рис. 2. Ошибка при запуске программы в дебаггере OpenWatcom.

Программа, собираемая в *GCC*, также собирается без каких либо сложностей и уведомлений. При запуске собранной программы на экран выводится стандартное сообщение об ошибке Windows. При этом из этого окна мы можем узнать только код ошибки, а сам компилятор не выдает никакой информации, (Рис. 3). Так как в *GCC* нет встроенного дебаггера, определение характера ошибки и место её возникновения является крайне сложной задачей.

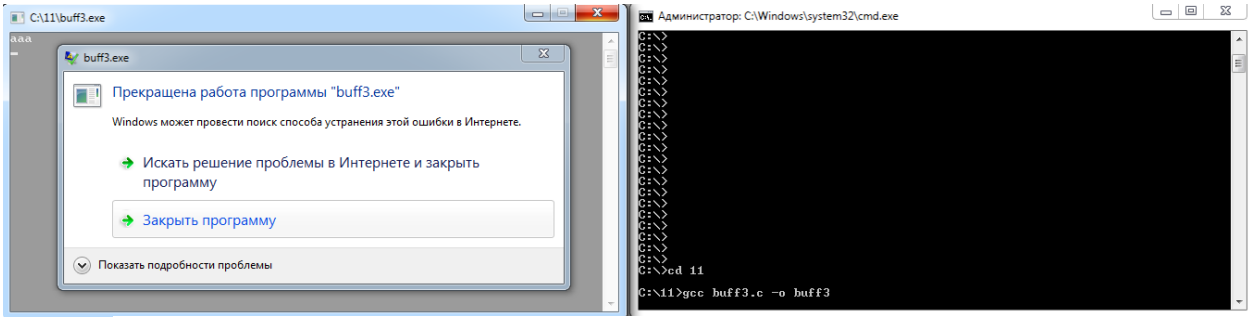


Рис. 3. Результат запуска программы, скомпилированной с помощью *GCC*.

Заключение

На основании анализа двух компиляторов, находящихся в свободном доступе было установлено, что компилятор OpenWatcom наиболее оптимален для решения задачи предотвращения переполнения буфера. Помимо этого OpenWatcom имеет графическую среду для работы (IDE) и встроенный дебагер, что значительно упрощает использование компилятора, а также поиск ошибок в разрабатываемых программах. С учетом изложенного можно сделать вывод, что создание достаточно строгого компилятора с мощными и быстрыми средствами отладки позволит исключить ошибки переполнения буфера в приложениях.

Литература

1. *Peter Bright*. How security flaws work: The buffer overflow. Ars Technika 2015.
2. *Беленькая М. Н., Малиновский С. Т., Яковенко Н. В.* Администрирование в информационных системах. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2014. 400 с.
3. *Прохоров Д.О., Беленькая М.Н.,* Исследование технологии глубокого анализа пакетов DPI для применения в корпоративных сетях // Телекоммуникации и Информационные Технологии. 2017. №2. с. 83 – 88.
4. Официальный сайт Open Watcom / URL: http://www.openwatcom.org/ (дата обращения 26.09.2018)
5. Официальный сайт GCC GNU / URL: https://gcc.gnu.org/ (дата обращения 27.09.2018)
6. *Беленькая М.Н., Малиновский С.Т., Васильев А.В.* Разработка алгоритма планировщика выполняемых задач гипервизора XEN // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 28-30.

ANALYSIS OF OPENWATCOM AND GNU COMPILER COLLECTION (GCC) COMPILERS FOR THE CONDITIONS FOR PREVENTING BUFFER OVERFLOW

Igor P. Korionov
student of group M111801(73), MTUCI
tyiiia_abr@mail.ru

Keywords: *buffer overflow, compiler, linker, vulnerability, GNU GCC, OpenWatcom.*

The results of a comparative analysis of free-access *GNU GCC* compilers and OpenWatcom are presented. Some security issues of information systems are considered and the types associated with buffer overflow are defined. The analysis of the relevance of the vulnerability of information systems due to buffer overflow has been carried out. A predictive solution has been proposed to prevent attacks using buffer overflow.

СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

Деревянко Илья Дмитриевич
М091701 (72) МТУСИ
derevyankoid@mail.ru
Якушев Владимир Валерьевич
М091701 (72) МТУСИ
yupinana@gmail.com
Иевлев Олег Павлович
МТУСИ, декан факультета ИТ, к.т.н., доцент
ievlev@mtuci.ru

Ключевые слова: *облачные технологии, облачные вычисления, информационная безопасность, облачные сервисы, стандартизация облачных сервисов.*

Проведен обзор методов организации безопасности и защиты данных в облачных вычислениях, рассмотрены примеры уже реализованных мер по организации защиты данных в существующих облачных сервисах. Выполнена классификация по основным четырем механизмам в соответствии с требованиями безопасности, которые они обеспечивают: аутентификация, конфиденциальность, контроль доступа и авторизация. Рассмотрены основные ключевые вопросы в организации защиты данных в облачной технологии. Рассмотрены основные рекомендации по организации безопасности хранения данных в облачных хранилищах, которые должны быть приняты во внимание.

Облачные сервисы включают в себя группу компьютеров, которые совместно используются для предоставления различных сервисов и выполнения различных задач. Облачные вычисления - одна из самых важных парадигм в последние несколько лет. Одно из ключевых преимуществ, которые предлагаются в этой ИТ-сфере – это технологии для компаний, которые сокращают время и затраты на рынке ИТ-технологий. Облачные вычисления предоставляют компаниям и организациям возможность использовать общие хранилища и вычислительные ресурсы.

Это лучше, чем развивать и приобретать собственную ИТ-инфраструктуру. Облачные вычисления также предоставляют организациям и компаниям гибкие, безопасные и экономичные ИТ-услуги, связанные с созданием и поддержкой работы ИТ-инфраструктуры. Их можно сравнить с национальными электрическими сетями, которые дают возможность организациям и частным домовладениям, подключаться и использовать централизованно-управляемый, эффективный и экономичный источник энергии.

Основные типы и модели облачных сервисов.

Основные корпорации, включая *Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP*, Oracle, и *Novell* инвестировали в облачные вычисления огромные суммы и предлагают ряд облачных решений для частных лиц и корпораций.

В облачных вычислениях существуют различные типы и модели, относящиеся к различным типам предоставляемых услуг. Облачные вычисления включают публичное облако, частное облако, гибридное облако и общественное облако [1]. С другой стороны, модели предоставления услуг могут классифицироваться как *SaaS* (программное обеспечение как услуга), *PaaS* (платформа как услуга) и *IaaS* (инфраструктура как услуга) [4].

Стандартизация облачных сервисов.

Так как технологии облачных вычислений только начинают свой путь к массовому потребителю, одной из главных проблем обеспечения безопасности является отсутствие общепринятых стандартов предоставления облачных сервисов. Проблема стандартизации в обеспечении информационной безопасности находится в процессе решения в трех основных областях.

Во-первых, ведущие компании предоставляющие услуги облачных вычислений создают внутренние корпоративные стандарты, которые не всегда становятся общедоступными. Первое на что должен обращать внимание потребитель облачных сервисов, в этом случае, это имя и репутация компаний, которые активно продвигают свои услуги. Среди таких компаний сегодня, можно отметить такие компании как *Microsoft, Google, Adobe, Amazon, IBM, Force.com, VMWare* и т.д. Возможно, разработанные этими компаниями стандарты будут опубликованы и общеприняты.

Во-вторых, поставщики услуг адаптируют свои предложения в соответствии с уже существующими установленными стандартами информационной безопасности (НАТО и *GIAC, BSI* и т.д.), проходят необходимые проверки, получив в результате сертификат соответствия на предоставление информационных услуг в соответствии с определенными нормативными документами. Эта работа сегодня особенно актуальна с точки зрения получения долгосрочного сотрудничества с государственными и общественными организациями как потребителями услуг облачных вычислений.

И, в-третьих, те же общественные, правительственные и коммерческие организации, разрабатывают свои собственные нормативные требования для создания безопасных облачных услуг по обработке информации. Таким образом, Европейское агентство по сетевой и информационной безопасности (*ENISA*), которое было создано в 2004 году для улучшения сетевой и информационной безопасности в Евросоюзе, выпустило документ. Группа компаний, включающая такие, как *AMD, IBM, CISCO* и *SUN* подписали «манифест открытого облака» (*Open Cloud Manifesto*), направленный на создание и поддержание максимально возможной открытости облачных систем. Ряд известных компаний в свою очередь сформировали «Альянс облачной безопасности».

Группой был выпущен документ, включающий в себя подробное руководство по безопасности облачных вычислений. Команда специалистов на форуме *Jericho Forum* консорциума *Open Group* разработала набор рекомендаций по защищенному использованию облачных вычислений, предлагая подход к выбору архитектуры облачной вычислительной системы для безопасной работы.

Еще один фактор в области безопасности и конфиденциальности для облачных вычислений, появившийся совсем недавно, - это создание стандартов. Например, *ISO* /*IEC* 27017 касается безопасности для общедоступных облачных сервисов, в то время как дополнительный стандарт ISO / *IEC* 27018 [5] касается защиты персональных данных для общедоступных облачных сервисов. Кроме того, стандарты *ISO* / *IEC* 19086 касаются соглашений об облачных сервисах и SLA. ISO /IEC 19086 часть 4 касается компонентов безопасности и конфиденциальности соглашений об уровне обслуживания облачных сервисов. *ISO* /*IEC* 27036-4 конкретно содержит рекомендации по рискам информационной безопасности, связанных с использованием облачных сервисов и эффективному управлению этими рисками, и реагированию на риски, связанные с приобретением или предоставлением облачных сервисов. Использование этих стандартов может помочь клиентам и поставщикам. Существует растущий список облачных сервисов, сертифицированных по стандартам 27017 и 27018. Также растет число стандартов, которые касаются конкретных отраслей, например, *Fast Healthcare Interoperability Resources* (*FHIR*) в секторе здравоохранения.

Известные эксперты в области информационной безопасности уже делятся с общественностью своим опытом в области облачных вычислений. Так, например, в одном из уважаемых издательств научной литературы Джон Уайли была опубликована серьезная работа по обеспечению безопасности облачных вычислений [2].

Средства обеспечения информационной безопасности облачных сервисов.

Рассмотрим основные преимущества облачных вычислений с точки зрения обеспечения информационной безопасности.

С ростом масштаба вычислительных систем стоимость любых мер по обеспечению безопасности для каждого пользователя значительно меньше. Концентрация ресурсов позволяет уменьшить как первоначальные и текущие затраты на защиту информации (например, для приобретения оборудования и средств защиты, резервное копирование, использование расширенной аутентификации, оплату работы специалистов в сфере информационной безопасности, затраты на разработку и поддержание концепции защиты информации, проектирование и стабилизацию производственных процессов и т. д.).

Облачные вычисления способствуют оптимизации двух ключевых показателей экономической эффективности информационной инфраструктуры компании. Возврат инвестиций в инфраструктуру (*return of investments*, ROI) можно легко запланировать и вернуть при использовании облачных сервисов. Первоначальные инвестиции уменьшаются, потребители платят только за действительно необходимые и упорядоченные использованные ресурсы, услуги и функции. Дополнительные и незапланированные инвестиции со стороны клиента исключены, ведь в случае отказа службы ответственность за это несет поставщик облачного сервиса.

Общая стоимость владения (*total cost of ownership, TCO*) чаще всего значительно ниже, чем в организации, которые используют собственные центры обработки данных. Расходы на техническое обслуживание, техническое сопровождение, минимизация рисков, обслуживание и масштабирование, затраты на обслуживающий персонал и связанные с этим расходы (электричество, помещение, страховые услуги, пожарная безопасность и т.д.) уже включены в стоимость услуг.

Наибольший эффект от оптимизации структуры инвестиций можно получить предприятиям малого и среднего бизнеса. Компании, для которых работа ИТ-инфраструктуры не связана с основным направлением деятельности, может избежать инвестиций в непрофильные активы [3, 6].

Услуги облачных вычислений включают в себя высоконадежное хранение и резервное копирование данных, быстрое восстановление в случае сбоя, сертифицированное шифрование данных во время хранения и при пересылке между поставщиком и пользователями. При правильном обеспечении всех вышеперечисленных условий поставщиком, хранение данных в облаке можно сравнить с арендой банковского сейфа. Проблема обеспечения информационной безопасности на соответствующих уровнях передается от потребителя поставщику облачного сервиса. При предоставлении системных ресурсов от поставщика потребителю в виде услуги ряд организационных рисков, связанных с обеспечением безопасности корпоративных данных предприятия, так же входят в ответственность поставщика.

Рассмотрим основные типы таких рисков, а также средства защиты, которые позволяют минимизировать данные риски.

1. Отсутствие общепринятых стандартов может поставить потребителя в зависимость от поставщика услуг. Необходимым условием минимизации этого риска является разработка, проверка и поддержание концепции миграции данных и приложений альтернативному поставщику.
2. Развитие бизнеса клиентов может создать новые требования к системе расчетов, которые не могут быть выполнены при работе с существующим поставщиком. Чтобы минимизировать этот риск требуется чтобы потребитель заранее разработал и внедрил в производство процессы для отслеживания, оценки и планирования реализации новых свойств и функций вычислительных процессов (*release management*).
3. Используя услуги облачных вычислений, потребитель имеет не только ограниченную ответственность за информационную безопасность, но и ограниченный контроль над эксплуатируемыми услугами. Степень ограничений определяется выбранной моделью

облачной инфраструктуры и условиями договора (*SLA*) между поставщиками и потребителем.

Концентрация и совместное использование вычислительных ресурсов также порождает ряд технических рисков, характерных для облачных вычислений.

4. Облачные вычисления из-за коллективного использования системных ресурсов требуют надежной изоляция пользовательских данных друг от друга. Потребителю следует обратить внимание на каких уровнях обобщенной модели обработки данных участие других пользователей в вычислительном процессе - на уровне инфраструктуры (например, виртуальные серверы, общие аппаратные ресурсы и т. д.), на уровне платформы (например, используемая система виртуализации и т.д.), на уровне приложений (например, системы управления базами данных, веб-приложения и службы и т. д.).

Наиболее опасными в этом отношении являются системы, которые не поддерживают разделение мандатов и (или) разделов, в которых один аппаратный модуль (например, центральный процессор), фрагмент базового программного кода (например, платформа виртуализации) или приложение (процесс) используются различными пользователями параллельно.

5. Данные, переданные и хранящиеся в облачной вычислительной системе, могут быть скомпрометированы или ложно обойдены против правил и процессов безопасности в результате использования возможных уязвимостей на разных уровнях облачной вычислительной системы.

Информация об этих уязвимостях может быть общедоступной до того, как проблема будет решена поставщиком.

Чтобы свести к минимуму этот риск, необходимо использовать шифрование передаваемых и сохраненных данных. В то же время заслуживает особого внимания организация управления ключами шифрования и сертификатами, используемыми для шифрования данных в организации-поставщике облачных вычислений.

6. Превышение уровня запросов на услуги по максимально допустимой нагрузке, в том числе атак *DDoS* (*Denial of Service* – отказ в обслуживании), может привести к недоступности облачной вычислительной системы для пользователей. В этой связи особое внимание следует уделить гарантированным параметрам доступности вычислительных систем и восстановлению в случае сбоя, которые предусмотрены в договоре (*SLA*) между поставщиком и потребителем.
7. Проблемы безопасности могут быть вызваны проблемами совместимости оборудования или программного обеспечения (например, разработка для конкретной платформы с *API*-интерфейсом платформы). Чтобы свести к минимуму такие риски, следует обратить внимание на сертификацию оборудования и программную часть компьютерных систем и услуг, предоставляемых поставщиком, с организацией поддержки в процессе эксплуатации (обслуживание, модернизация и т. д.),

Облачные вычисления не только создают новые риски безопасности и конфиденциальности, но также предоставляют возможности для предоставления улучшенных служб безопасности и возможностей конфиденциальности, которые лучше, чем те, которые многие организации реализуют самостоятельно. Поставщики облачных услуг могут предлагать расширенные функции безопасности и конфиденциальности, которые используют их масштаб и их навыки для автоматизации задач управления инфраструктурой, включая облачные сервисы, предоставляющие возможности безопасности и инструменты безопасности, встроенные в предложения *SaaS*. Это потенциально благо для клиентов, у которых мало квалифицированных сотрудников службы безопасности.

По мере того, как корпоративные клиенты переводят свои приложения и данные на облачные вычисления, для них крайне важно поддерживать уровень безопасности и защиты конфиденциальности, который они имели в своей традиционной ИТ-среде.

Рассмотрим некоторые шаги, направленные на оценку и управление безопасностью и конфиденциальностью использования облачных сервисов с целью снижения риска и обеспечения соответствующего уровня информационной безопасности:

Обеспечение эффективных процессов управления политикой безопасности.

Большинство организаций разрабатывают политику и процедуры обеспечения безопасности, конфиденциальности, которые используются для защиты их интеллектуальной собственности и корпоративных активов, особенно в области ИТ. Эти политики и процедуры разрабатываются на основе анализа влияния угроз и рисков на информационные активы. Для снижения информационных рисков создается система контроля, которая включает рабочие процедуры, и служит эталоном для выполнения и проверки. В стандарте *ISO* / *IEC* 38500 описаны руководящие принципы управления ИТ-инфраструктурой организации.

Наиболее широко признанным международным стандартом обеспечения информационной безопасности является ИСО / МЭК 27001, который включает национальные варианты и хорошо разработанные режимы сертификации. *ISO* имеет стандарты, специфичные для облачных вычислений: *ISO* / *IEC* 27017 «Свод практических правил контроля информационной безопасности на основе *ISO* / *IEC* 27002 для облачных сервисов», *ISO* / *IEC* 27018, которые конкретно касаются соображений безопасности и конфиденциальности облачных сервисов и которые основываются на *ISO* / *IEC* 27001 и *ISO* / *IEC* 27036-4.

Некоторые организации предоставляют неиндустриальные фреймворки для оценки мер безопасности, которые могут применяться к поставщикам облачных услуг, включая *American Institute of Certified Public Accountants* (*AICPA*), *Information Systems Audit and Control Association* (*ISACA*) и *Holistic Information Security Practitioner Institute* (*HISPI*), которые соответственно обеспечивают *SSAE* 16, *COBIT* 5 и *CAAP*. Другие организации предоставляют фреймворки для конкретных услуг или отраслей, таких как стандарт безопасности данных платежных карт (*PCI*) (*DSS*).

Группы, такие как *Cloud Security Alliance* (*CSA*), предоставляют руководство, которое включает в себя *Cloud Controls Matrix* (*CCM*), программу самооценки провайдера, *Consensus Assessments Initiative Questionnaire* (*CAIQ*), сертификация знаний облачной безопасности для персонала, *Certificate of Cloud Security Knowledge* (*CCSK*) и реестр поставщиков облачных услуг для публикации результатов самооценки (*STAR*). Существуют также кодексы поведения, связанные с обработкой персональных данных в облачных сервисах - конкретным примером является *EU Cloud Code of Conduct*.

Основная цель этой работы заключалась в обзоре методов организации безопасности и защиты данных в облачных вычислениях. С этой целью были рассмотрены примеры уже реализованных мер по организации защиты данных в существующих облачных сервисах. Выполнена классификация по основным четырем механизмам в соответствии с требованиями безопасности, которые они обеспечивают: аутентификация, конфиденциальность, контроль доступа и авторизация.

Рассмотрены основные ключевые вопросы в организации защиты данных в облачной технологии. Можно сделать вывод, что, если рекомендуемые меры по организации защиты данных принимаются во внимание, обеспечивая аутентификацию, конфиденциальность, контроль доступа и авторизацию, тогда облачным вычислениям можно доверять.

Также рассмотрены основные ключевые моменты, которые необходимо принимать во внимание при организации перехода ИТ-инфраструктуры компании на облачные сервисы. Рассмотрены основные рекомендации по организации безопасности хранения данных в облачных хранилищах, которые должны быть приняты во внимание. В дальнейшем планируется расширить данную работу, рассмотрев ряд проблем, которые следует учитывать для обеспечения повышенной безопасности данных в облачных вычислениях, например, правильное использование административных привилегий, беспроводной доступ, контроль данных в

системах, использующих беспроводные сети, восстановление данных и установление границы защиты в облаке.

Литература

1. *L. Badger, T. Grance, R. Patt-Corner and J. Voas*, "Cloud computing synopsis and recommendations (draft), nist special publication 800-146", Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011)
2. *Завгородний В.И.* Оценка целесообразности перехода предприятия к использованию облачных вычислений [Электронный ресурс]. – Режим доступа: http://www.fa.ru/ (дата обращения: 08.10.2016).
3. Развитие технологии облачных вычислений в России [Электронный ресурс]. – Режим доступа: http://mirtelecoma.ru/magazine/elektronnaya-versiya/28/ (дата обращения: 20.05.2016).
4. *Батищев Д. С., Михелев В. М.* Инфраструктура высокопроизводительной компьютерной системы для реализации облачных сервисов хранения и анализа данных персональной медицины //Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2016. – Т. 37. – №. 2 (223).
5. GIAC Mission Statement. Global Information Assurance Certification [Электронный ресурс]. – Режим доступа: http://www.giac.org/overview/ statement.php
6. *Ievlev O.P.* The paradoxes of modern telecommunication networks // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 5. С. 86-90.

MEANS OF INFORMATION SECURITY OF CLOUD SERVICES

Ilya D. Derevyanko
M091701 (72) MTUCI
derevyankoid@mail.ru
Vladimir V. Yakushev
M091701 (72) MTUCI
yupinana@gmail.com
Oleg P. Ievlev
MTUCI, Head: Dean of the Faculty of IT, Ph.D., Associate Professor
ievlev@mtuci.ru

Keywords: *Cloud technologies, Cloud computing, information security, Cloud services, standardization of Cloud services.*

The review of methods of organization of security and data protection in Cloud computing. Examples of already implemented measures to organize data protection in existing Cloud services are considered. The classification according to the main four mechanisms is carried out in accordance with the security requirements that they provide: authentication, confidentiality, access control and authorization. The main key issues in the organization of data protection in Cloud technology are considered. The main recommendations on the organization of data storage security in Cloud storage are considered, which should be taken into account.

БАЗА ДАННЫХ ДЛЯ SAP-СИСТЕМЫ. ORACLE ИЛИ SAP HANA?

Депутатов Евгений Алексеевич
Студент группы 3МАС1701 МТУСИ
Ev.dep@yandex.ru
Дорогина Анастасия Сергеевна
Студентка группы 3МАС1701 МТУСИ
dorogina.nst@gmail.com
Воронцов Юрий Алексеевич
МТУСИ, профессор каф. ИТЭУ
yvorontsov@newmail.ru

Ключевые слова: *базы данных, системы управления базами данных, Oracle, SAP HANA, производительность, высоконагруженная ИС, транзакционная ИС, SQL.*

Проведен анализ производительности системы. Выявлены «узкие места» в быстродействии. Сняты метрики выполнения разных видов запросов. Проанализирована необходимость перехода. Сняты метрики с новой БД, результат сравнивается с прошлыми показателями.

Постановка задачи.

На предприятии по продаже электроники и бытовой техники установлена система *SAP CRM*. Основа любой информационной системы – это база данных. Система управления БД на предприятии установлена от компании Oracle [4 - 6].

На *SAP CRM* завязано 5 ключевых бизнес процессов компании (более 400 филиалов, расположены по всей стране) – лояльность (начисление и списание бонусных баллов), маркетинг (осуществление рассылок постоянным клиентам), сервис (гарантийное и не гарантийное обслуживание техники), претензии (централизованная обработка претензий со всех филиалов одним отделом) и Call-центр (централизованный прием звонков от клиентов и регистрация взаимодействий).

В связи с масштабной кампанией по привлечению новых покупателей, количество данных в базе по клиентам и их операциям (звонки, претензии, сервисные заявки, транзакции и другое) стало расти в геометрической прогрессии. Постепенно скорость работы в системе снизилась – все операции, связанные с чтением/записью данных в базу данных, происходят довольно долго. Создание индексов на поля таблиц немного улучшило производительность, но она все еще остается на низком уровне.

Это сказывается на клиентах компании – появляются очереди на кассах, контактный центр долго консультирует клиентов. Необходимо разработать план по решению проблемы.

Исходные данные.

На момент постановки задачи были сняты исходные метрики, данные в таблице 1.

Было решено разработать план перехода на новую СУБД, перенести тестовую систему на СУБД HANA, снять метрики и принять решение о релевантности внедрения.

SAP HANA.

Как база данных, HANA - это передовой инструмент. Он был специально разработан с нуля, чтобы использовать современные достижения в технологии процессорных чипов, которые обеспечивают обильную память и до 16 компьютеров на одном чипе. Данные хранятся и обрабатываются в памяти, а не на внешних дисках, в столбцах, а не в строках. Такая архитектура (представлена на рис. 1) [1] и инновационный колонный подход HANA значительно увеличивает

скорость, потому что процессорам не нужно вращаться, искать фактические бизнес-данные на основе строк, используя такие средства, как агрегация и индексы, на которые может приходиться до 95% всех данных. HANA уменьшает и сохраняет все это дополнение в памяти, что позволяет уменьшить объем данных организации на целых 95%. Сниженный охват и более высокая скорость не только значительно улучшают обработку транзакций, отчеты и аналитику, но также уменьшают общую стоимость владения (англ. Total Cost of Ownership, TCO) за счет упрощения поддержки хранилища данных и инфраструктуры хранилищ.

HANA также является мощной платформой, которая легко интегрирует сторонние приложения и данные из других источников. Например, социальные медиа и показания датчиков, из быстро расширяющегося Интернета «вещей». В сегодняшней среде SAP почти 60% приложений, поддерживаемых HANA, являются сторонними. Платформа HANA позволяет быстро собирать данные из разных источников и интегрировать их с SAP Business Suite, а также поддерживает сторонние инструменты.

Фактически, HANA может помочь уменьшить общее количество инструментов аналитики и отчетности, что приводит к меньшему количеству лицензий и, соответственно, снижению совокупной стоимости владения. HANA также очень компактна и может работать на одном сервере, который включает в себя собственный сервер приложений. Организации могут выбирать из широкого набора предварительно сконфигурированных серверов от ведущих отраслевых поставщиков и не останавливаться на одной аппаратной платформе.

Таким образом, бизнес будущего неразрывно связан с HANA - появляются такие возможности, как доступ к данным в реальном времени, комплексное моделирование и аналитика в реальном времени, полезная и эффективная бизнес-аналитика в реальном времени в любом месте на любом устройстве. HANA является облачным сервисом и интегрированным в среду SAP S/4 ERP следующего поколения SAP, которая поистине меняет игру. [2]

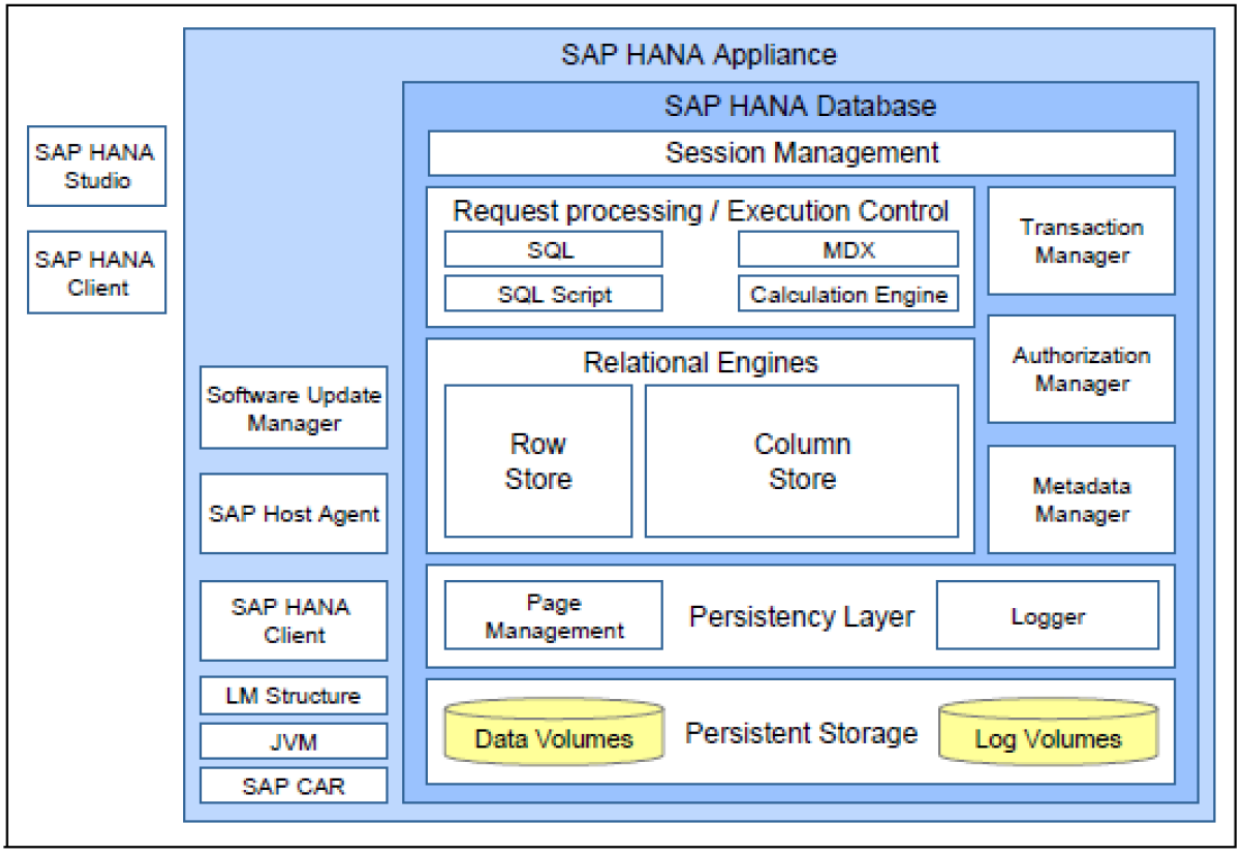


Рис. 1. Общая архитектура HANA.

SAP HANA: как это работает

Основным ядром в *SAP HANA* является компонент СУБД, позволяющий обрабатывать большие объёмы данных с помощью технологии In-Memory и на базе языкового инструмента *SQL*. В основе СУБД *SAP HANA* используется реляционная модель данных, но также существует возможность обращения к данным с помощью «графового» языка запросов WIPE. Гибкость в выборе языка запросов обусловлена архитектурными возможностями SAP HANA и заключается в использовании единого представления данных в In-Memory хранилище. Таким образом, у пользователя есть возможность обращения к данным с помощью различных семантических конструкций, используя при этом единую копию данных в памяти СУБД. Классический подход, принятый в ряде других OpenSource СУБД, отличается от вышеуказанного, потому что подразумевает использование как минимум двух хранилищ данных и разделение способа хранения графовых структур и реляционных таблиц.

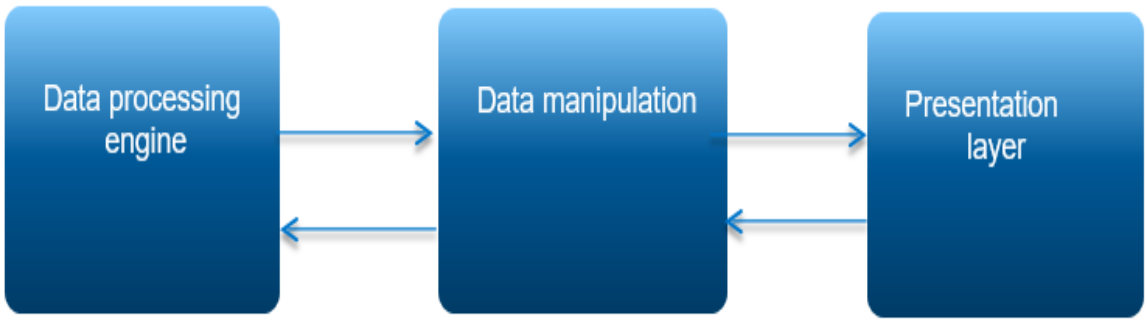


Рис. 2**.** Концепция управления данными.

На рис. 2 отражена общая схема управления данными в SAP HANA и суть концепции управления с помощью различных языков – в частности, SQL и WIPE. Используя движок Data Processing, можно сформировать на уровне Data Manipulation новый семантический уровень для работы с данными, но при этом будет применена единая копия исходных данных, что существенно повышает возможности платформы *SAP HANA* для решения задач, где требуется представление информации в виде графовых структур.

Технология In-Memory в СУБД *SAP HANA* позволяет хранить и обрабатывать данные в памяти, используя уникальные алгоритмы [3], разработанные в компании *SAP* и на базе платформы Intel x86. Недавно SAP также анонсировала поддержку платформы *IBM Power* для *SAP HANA*. Уникальность и высокая скорость обработки запросов к данным заключается в возможности их хранить и выполнять. Они находятся в сжатом виде в памяти RAM. Благодаря разработанному алгоритму обработки данных в *SAP HANA* удалось реализовать подход Unified Tables (рис. 3), который обеспечивает высокую скорость чтения и записи данных в таблицу поколоночного хранения. Поэтому одним из главных преимуществ *SAP HANA* является возможность выполнять аналитические запросы сразу на транзакционных данных, которые добавляются в реальном времени. Система автоматически берёт на себя обеспечение прозрачного доступа к данным. Таким образом, новые данные в таблице сразу доступны для анализа без предварительной обработки.

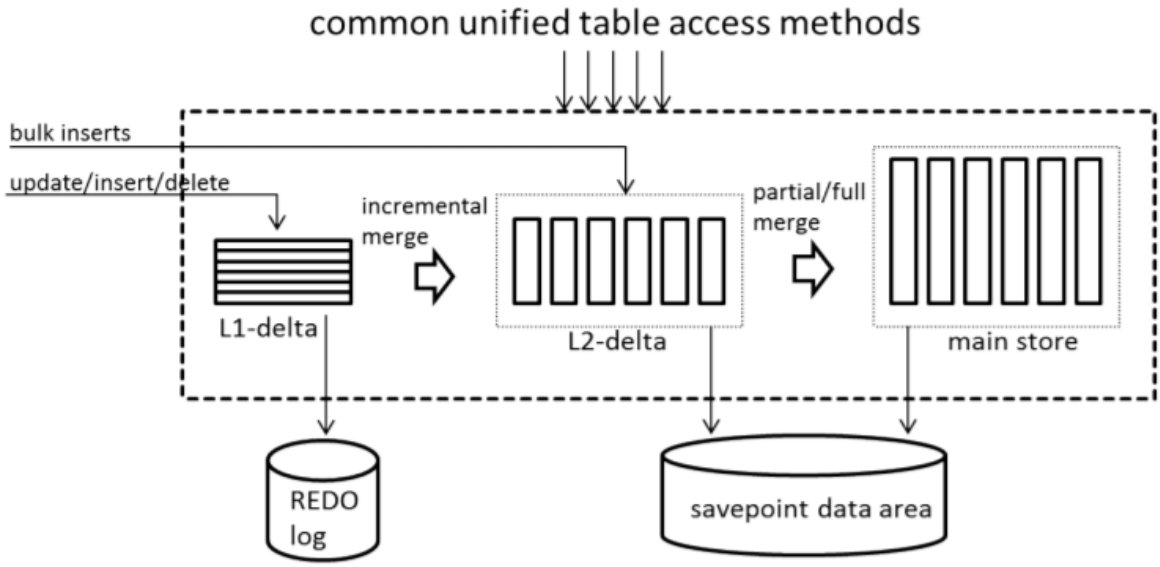


Рис. 3. Архитектура концепции Unified Table.

Результаты тестирования.

После внедрения на тестовую среду новой СУБД, а также переноса базы данных с продуктивной среды, были выполнены замеры производительности при помощи тех же скриптов и с теми же объемами данных. Результат замеров приведен ниже.

Таблица 1.

Сравнение производительности

Вид запроса	Кол-во возвращаемых значений	Oracle, сек	Hana, сек	Соотношение
Среднее кол-во запросов к БД в секунду		120		
select из 1 таблицы всех данных	59 000 000	87	4	22
select из 1 таблицы с условием	120 000	65	2	33
select из 2 таблиц с inner join	26 000 000	104	3	35
select из 2 таблиц с left outer join	30 000 000	187	3	62
select с условием на exists	12 000 000	286	6	48
select с group by выражением	950 000 000	793	5	159

Заключение

Как видно из таблицы, производительность выросла в среднем в 60 раз, при этом нет необходимости постоянно создавать индексы, следить за производительностью и т.д. Из восьми сотрудников, поддерживающих БД Oracle, на предприятии оставили двоих на поддержку БД HANA.

В последнее время практически все предприятия, внедряющие SAP, после анализа, отдают предпочтение СУБД HANA. Это помогает им добиться большей производительности, а значит, внедрение информационной системы будет более целесообразно.

Литература

1. Analysis of SAP HANA High Availability Capabilities [Электронный ресурс] — Режим доступа: https://www.oracle.com/technetwork/database/availability/sap-hana-ha-analysis-cwp-1959003.pdf, свободный (12.10.2018).
2. SAP HANA vs. Oracle and Other Traditional Databases – Think Business Transformation, not Databases [Электронный ресурс] — Режим доступа: https://symmetrycorp.com/blog/sap-hana-vs-

oracle-and-other-traditional-databases-think-business-transformation-not-databases/, свободный (23.10.2018)
3. Efficient Transaction Processing in SAP HANA Database – The End of a Column Store Myth /Vishal Sikka, Franz Färber, Wolfgang Lehner, и др. — Proceeding SIGMOD '12 Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data. — 2012. — 731-742с.
4. *Хуторов В.С., Беленькая М.Н.* Основные проблемы и цели мониторинга базы данных средствами СУБД Oracle // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 7. С. 133-134.
5. *Хуторов В.С., Беленькая М.Н.* Обзор параметров, влияющих на производительность СУБД Oracle, и средств мониторинга работы системы // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 372-376.
6. *Корогодова А.О., Беленькая М.Н.* Проблемы производительности СУБД Oracle под управлением сетевой ОС Windows // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 7. С. 72-74.

DATABASE FOR SAP SYSTEM. ORACLE OR SAP HANA?

Evgeniy Al. Deputatov
Student group 3MAS1701 MTUCI
Ev.dep@yandex.ru
Anastasia S. Dorogina
Student group 3MAS1701 MTUCI
dorogina.nst@gmail.com
Yuri Al. Vorontsov
Professor of the Department of ITUU MTUCI
yvorontsov@newmail.ru

Keywords: *Databases, Database Management Systems, Oracle, SAP HANA, performance, high load IP, transactional IP, SQL.*

Systems perfomance analysis has been done. According to it some bad spots in speed perfomance has been detected. Metrics of different types of requests has been writen down. The need in changing software has been analysed aswell. Metrics from new database has been writen down. At this moment result is comparing with the older ones.

АВТОМАТИЗАЦИЯ ОБРАБОТКИ БУМАЖНЫХ МАТЕРИАЛОВ ПРИ ПРОВЕДЕНИИ ОБРАЗОВАТЕЛЬНЫХ ОЛИМПИАД

Андреев Петр Александрович
студент группы БПМ1401 МТУСИ
gtnzgtmz@gmail.com
Скородумова Елена Александровна
МТУСИ, к.ф.-м.н., доцент кафедры ТВиПМ
eas@mtuci.ru

Ключевые слова: *интеллектуальный анализ данных, распознавание образов, автоматизация обработки данных, нейронные сети, олимпиада.*

Предметом настоящей работы стала разработка математических алгоритмов для обработки информации на бумажных носителях, реализованная для московских математических конкурсов «Весенний Олимп» и «Осенний Олимп». Была спроектирована структура данных, отвечающая потребностям организаторов. Для распознавания оцифрованных бланков были рассмотрены нейросети, компьютерное зрение и метод усреднения по яркости. Был обоснован выбор метода усреднения как наиболее быстрого и эффективного. Разработанная модель применена при проведении «Весеннего Олимпа» (март-май 2018 г.) и «Осеннего Олимпа» (сентябрь-октябрь 2018 г.).

Серьезной проблемой является перенос данных в электронный вид, когда требуется быстро и качественно обработать большие объемы информации на бумажных носителях. Решить эту проблему помогают интеллектуальные методы распознавания информации.

Информационные технологии применяются при организации массовых культурных и образовательных мероприятий. В России сейчас проводится большое количество предметных олимпиад, конкурсов и соревнований разного уровня для школьников и студентов. Организаторы собирают данные участников и оценки экспертов, чтобы составить рейтинг участников, делают информационные рассылки по выборкам из общей массы участников, а также собирают разного рода статистику. Требуются выходные печатные формы: необходимо выдать всем участникам документы, удостоверяющие их участие и особо отметить победителей. В некоторых случаях бывают нужны другие печатные формы (например, персонифицированные карточки участников, бейджики, списки участников, ведомость выдачи призов), а также электронные выходные формы (например, списки призеров для сайта).

Предметом данной статьи стала разработка математических алгоритмов для упрощения проведения массовых мероприятий, реализованное для московских математических конкурсов «Весенний Олимп» (для школьников 1-5 классов) и «Осенний Олимп» (для школьников 1-9 классов). Информационные сообщения о конкурсах размещены на ресурсах: *https://olimpiada.ru/* (*https://olimpiada.ru/activity/276* и *https://olimpiada.ru/activity/38*), *http://desc.ru/, http://matznanie.ru*.

На очные конкурсы приходят школьники, прошедшие предварительную электронную регистрацию и успешно решившие задачи отборочного интернет-тура. Количество очных участников в 2017/18 учебном году достигало 2500 человек.

С точки зрения организации массового мероприятия всё сводится к тому, что каждый участник должен в конце получить Сертификат участника с набранными баллами, а победители еще и заслуженные награды: Диплом I, II или III степени или Похвальную грамоту. Все сертификаты, дипломы и грамоты должны содержать верную информацию об участнике (ФИО, класс, школа, населенный пункт), а награды должны соответствовать продвижению в решении задач конкурсного варианта.

На сентябрь 2017 года была реализована следующая технологическая цепочка, включавшая частичную автоматизацию хранения и обработки информации:

1. Отборочный тур. Сбор информации через форму регистрации, онлайн выдача и проверка заданий отборочного тура. Подведение результатов.

2. Подготовка к финальному туру. Создание таблицы победителей очного тура и призеров прошлых лет. Создание каждому своего уникального *ID*, создание регистрационных листов. Рассылка приглашений и распределение участников по временным потокам.

3. Финальный тур.

3.1. Проведение очной письменной работы. После написания участниками работы информация сохраняется в бумажных протоколах.

3.2. Проверка работ. Жюри выставляет оценки за решения в виде цифр на бумажных работах в нарисованных или напечатанных табличках.

3.3. Внесение результатов в электронную таблицу. Осуществляется вручную в выгрузку таблицы Очные участники. Поиск каждого участника происходит по фамилии на листе нужного класса, далее сотрудник сличает имя и школу, вносит баллы за задачи из работы, номер аудитории и время начала работы из протокола.

3.4. Подведение предварительных итогов и показ работ с проведением апелляции.

4. Награждение призеров.

Основной задачей стало построение модели электронной обработки результатов, их реализации и тестирования, с целью оптимизации внесения результатов проверки: снижение затрат времени и устранение ошибок.

Развитие компьютерных технологий и рост вычислительных мощностей в настоящее время позволяют автоматизировать процесс обработки бумажных носителей. Для этого требуются:

1. разработка машиночитаемых бланков,
2. аппаратная платформа для считывания бланков,
3. программное обеспечение для распознавания изображений.

Существенной частью является также написание инструкций и четкое соблюдение их сотрудниками на всех этапах технологической цепочки.

Для этого были разработаны и внедрены следующие входные формы: регистрационный бланк участника и бланк варианта. В качестве считывающих аппаратов использовались мобильные телефоны с ОС *Android* и МФУ *Xerox WorkCentre* 7535.

Проектирование модели

1.1. Подготовка данных.

Каждый участник проходит предварительную регистрацию на сайте. Для участников очного конкурса генерируется его уникальный код участника и высылается «Регистрационный бланк», который он должен распечатать самостоятельно и с ним прийти на конкурс. Таким образом формируется таблица «Участники».

В регистрационном бланке: фамилия, имя, отчество, учебное заведение, уровень (класс), за который пишет участник, класс, в котором учится участник, *QR*-код с кодом участника, численно записанный код участника, область для вписывания дополнительной информации.

На месте проведения в аудитории каждому участнику выдают условия в запечатанном конверте. Листы с условиями имеют: *QR*-код, в который входит код комплекта; таблица для отметки баллов за задачу (используется проверяющим); область для подписывания листа (графы: фамилия и код участника); условие задачи; область для записи решения задачи и ответа.

В аудитории проведения дежурные проходят и специальным приложением на ОС *Android* считывают *QR*-коды с бланка регистрации и одного из листов комплекта условий (любого). Перед началом сканирования задается номер аудитории. По окончанию сканирования аудитории (по нажатию кнопки) приложение создает запись в таблице «Протокол», там же фиксируется время создания очередной записи. На основе пар *QR*-кодов, считанных между введением номера аудитории и окончанием сканирования аудитории, создаются записи в таблице «Работы».

После проверки все работы отправляются на сканирование. В результате сканирования их на МФУ *Xerox WorkCentre* 7535 получаются *pdf* файлы. Каждый файл содержит листы нескольких работ в виде изображений. С помощью программного комплекса мы распознаем, сколько баллов поставили эксперты в каждой работе к каждой задаче и создаем таблицу «Комплекты».

1.2. Построение кода участника и кода комплекта. Так как при переписывании чисел кода с одного бланка на другой могут возникнуть ошибки, или креативный участник решит немного раскрасить *QR*-коды, нужны коды, исправляющие ошибки. Имеет смысл использовать код Рида-Соломона (*RS*) [1].

Обработка полученных после сканирования работ

Полученный после сканирования многостраничный файл в расширении *Portable Document Format* (*PDF*), где каждая страница – один лист работы участника, содержит:

- Таблица с выставленными баллами за задачу на этом листе, в которой:
  - Строка – это номер проверки. Вторая проверка проводится строго после первой.
  - Заголовки столбцов – баллы от 0 до 7.
  - Крестик на пересечении строки с номером проверки и столбцом с баллом обозначает балл за эту задачу при этой проверке.
  - Подпись эксперта (проверяющего).
- *QR*-код, в котором содержится:
  - код комплекта, закодированный *RS*(8,6),
  - номер листа комплекта.
- Вручную записанная информация (фамилия участника и код участника).
- Условие задачи.
- Решение участника.

Наиболее важным является распознавание крестиков в графах с баллами за задачу. Для этого мы из полученного *pdf* файла извлекаем очередной лист и ищем на нем *QR*-код. Если не находим, переходим к следующему листу. Листы без *QR*-кода не содержат таблицы с баллами, и обрабатывать их не нужно.

Дальше для таблицы баллов выделяются 4 строки (первая, вторая, третья проверка и апелляция). Апелляции принимаются на показе работ. Каждая строчка обрабатывается отдельно. Примеры отметок приведены на рис. 1.

Строка разбивается на области (квадратики), в которых может стоять крестик (отметка о балле) или же закрашенный квадратик (зачеркнутая отметка о балле, ее учитывать не надо).

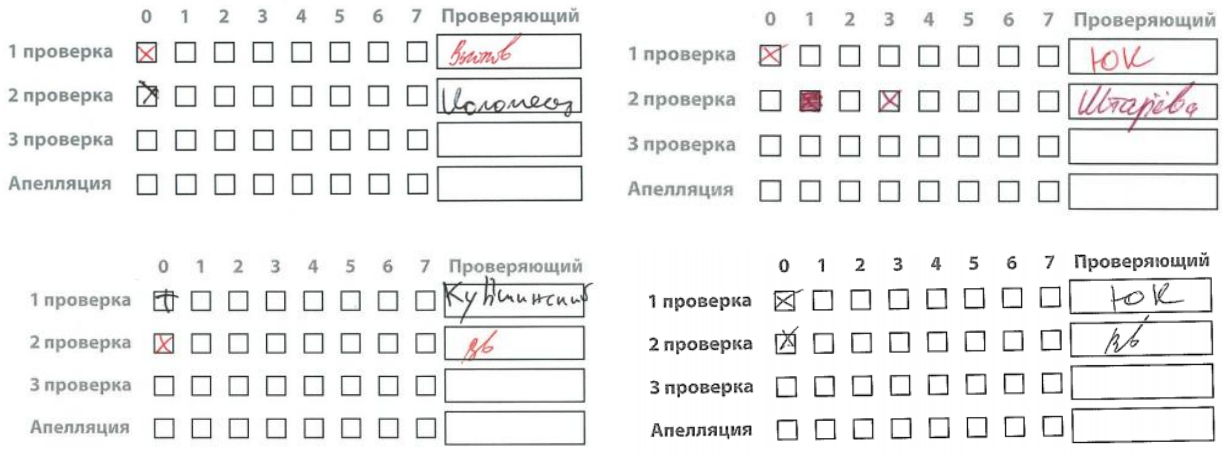


Рис. 1. Примеры отметок.

Разбивать на квадратики можно несколькими способами:

- Находить контур компьютерным зрением.
- Вырезать область по статическим координатам.

Метод компьютерного зрения в случае нарушения квадратного контура (отметка частично выехала из квадратика), работает с очень большим количеством ошибок и отказов. Исследования показали, что этот метод не подходит.

Достаточно ровное сканирование листов позволяет вырезать области и попытаться в них обнаружить отметки (крестики). Для обнаружения можно воспользоваться несколькими способами:

- Обучить нейросеть распознавать крестики и с помощью ее находить, в каких квадратиках стоят отметки.
- Находить контур крестика (две пересекающихся линии, или что-то другое) компьютерным зрением (работает медленнее, чем следующий вариант).
- Исследовать наличие отметок в анализируемой области по ее яркости.

Нейронные сети хорошо распознают однотипные данные, на которых их обучили.

Для решения поставленной задачи будем использовать нейросеть прямого распространения с одним скрытым слоем с 4 нейронами в нем. В качестве функции активации будем использовать сигмоидальную функцию [2].

На вход (O_{in}) нейросети подается вырезанная маленькая область (квадратик) в виде трехмерной матрицы (устройство которой рассмотрено ниже), в которой может быть отметка (крестик). На выходе (F_{out}) она выдает число от 0 до 1, равное классу принадлежности этой области к крестику. Выход из нейросети подается на трехуровневый квантователь, описываемый следующим соотношением (1):

$$a_{\text{квантователя}} = \begin{cases} 1; F_{out} > 0.8 \\ question; 0.8 < F_{out} < 0.4 \\ 0; F_{out} < 0.4 \end{cases} \quad (1)$$

где $a_{\text{квантователя}}$ — выход квантователя;
F_{out} — сигнал поданный на вход, полученный от нейросети,
question — сообщение об отсутствии решения, и эта область требует обработки руками.

На квантователь подается выход нейросети (F_{out}), а на выходе результат нейросети ($a_{\text{квантователя}}$). В случае выдачи quastin этот квадратик обрабатывается вручную. Это тестовый режим для отладки нейросети.

Обучаем нейросеть генетическим алгоритмом на выборке из 1000 крестиков (результат на выходе сети – 1), а также на 1000 пустых квадратиках (результат – 0) и 500 полностью закрашенных, зачеркнутых отметках (результат – 0).

После запуска на всей выборке квадратиков и анализа квадратиков, в которых нейросеть сомневается, было установлено, что эксперты слишком по-разному ставили отметку. Несмотря на инструкцию ставить в нужной области крестик «X», некоторые эксперты ставили «+» или даже «0» (см. примеры на рис. 1). При таком полиморфизме отметок обучение нейросети становится проблематичным. К тому же возникают проблемы с созданием обучающей выборки: это требует больших временных затрат и не исключены ошибки из-за человеческого фактора. По итогам тестирования можно заключить, что использование нейросетей для решения поставленной задачи не представляется целесообразным.

Попытка реализации обнаружения контуров с помощью компьютерного зрения привела к тем же проблемам, что и при использовании нейросетей (с отметками разных видов). Более этого, тестирование такого алгоритма показало, что он более затратен по времени и менее надежен.

Рассмотрим третий вариант – метод усреднения по яркости. Его реализация основана на использовании 3D матрицы:

$$img = \begin{pmatrix} (R_{11},G_{11},B_{11}) & (R_{12},G_{12},B_{12}) & \cdots & (R_{1n},G_{1n},B_{1n}) \\ (R_{21},G_{21},B_{21}) & & & (R_{2n},G_{2n},B_{2n}) \\ \vdots & & & \vdots \\ (R_{n1},G_{n1},B_{n1}) & (R_{n2},G_{n2},B_{n2}) & \cdots & (R_{nn},G_{nn},B_{nn}) \end{pmatrix} \quad (2)$$

где R_{ij} — яркость канала red в точке с координатами (i,j);

G_{ij}— яркость канала green в точке с координатами (i,j);

B_{ij} — яркость канала blue в точке с координатами (i,j).

Матрица (2) создается с помощью обработки изображения методом OpenCV [3]. Для распознавания отметки усредняем матрицу по каждому каналу *RGB*, и получаем вектор из 3 чисел (3):

$$\overline{img} = \left(\overline{R_{\text{img}}}, \overline{G_{\text{img}}}, \overline{B_{\text{img}}}\right) \tag{3}$$

где $\overline{R_{img}}$— средняя яркость канала *red* в изображении;

$\overline{G_{img}}$—средняя яркость канала *green* в изображении;

$\overline{B_{img}}$—средняя яркость канала *blue* в изображении.

Из вектора $\overline{img}$ берем самый большой элемент, т. е. самый яркий канал изображения, и отправляем на квантователь, описываемый соотношением:

$$A_{\text{квантователя}} = \begin{Bmatrix} 0; \overline{RGB_{\max}} > 250 \\ 1; 250 < \overline{RGB_{\max}} < 100 \\ 0; \overline{RGB_{\max}} < 100 \end{Bmatrix} \tag{4}$$

Где $\overline{RGB_{\max}}$ - максимальное значение в векторе $\overline{img}$.

В зависимости от выхода на квантователе принимается решение: 0 — нет отметки, 1 — есть отметка.

Этот алгоритм распознает более 99% отметок. В результате использования описанного алгоритма вручную пришлось обрабатывать всего несколько отметок из 35 тысяч. Такой алгоритм не пропускает отметки, но иногда принимает пустой квадратик за область с отметкой из-за съехавшей области (пример на рис. 2). На рис. 2 в качестве первой проверки воспринималась область с числами: они определились как отметки проверяющих**.** Эта ошибка была найдена при попытке записать в таблицу несколько баллов за одну задачу.

Рис. 2. Пример некорректного сканирования. Красным выделена область распознавания.

На рис. 3 приведены примеры некорректно распознанных отметок. Подобные случаи пришлось обрабатывать вручную. На левом нижнем примере плохо закрашена отметка (0 баллов), и в этом случае били распознаны две отметки вместо одной.

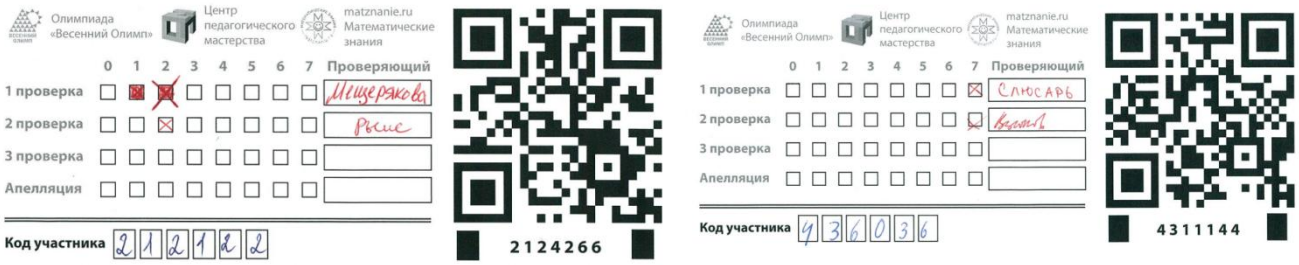


Рис. 3. Примеры, некорректно распознанные алгоритмом.

Заключение

В работе получены следующие результаты:

- Подготовлена компьютерная модель данных, что заметно упростило подведение итогов, и позволило построить дальнейшую информатизацию системы.
- Рассмотрены несколько алгоритмов распознавания информации с бумажных носителей: нейросети, компьютерное зрение, метод усреднения по яркости.
- Установлено, что самым быстрым и эффективным алгоритмом для поставленной задачи является метод усреднения по яркости. Он является достаточно простым в реализации, показал быструю работу алгоритма и почти 100%-ное распознавание отметок.

В 2017/2018 учебном году успешно опробовано распознавание результатов проверки на «Весеннем Олимпе» (2176 участников, 14834 проверенные задачи, более 35 тысяч сделанных и распознанных отметок). Попутно был улучшен контроль за участниками во время проведения конкурса (теперь оперативно отслеживается, в какую аудиторию попадает каждый ребенок, пришедший на очный конкурс), и дополнительно автоматизирована проверка соответствия полученного комплекта заданий заявленному уровню участника.

Литература

1. *Ушаков В.А.* О создании программы «Изучение кодов Рида-Соломона» // Решетневские чтения. 2016. №20. URL: https://cyberleninka.ru/article/n/o-sozdanii-programmy-izuchenie-kodov-rida-solomona (дата обращения: 04.11.2018).
2. *Гейдаров П.Ш.* Нейронные сети прямого распространения с вычисляемыми параметрами // Информационные технологии 2017, т. 23, №7, с. 543 – 552.
3. OpenCV library [Электронный ресурс]. — URL: http://www.opencv.org, (дата обращения 13.05.18).

THE AUTOMATIZATION OF THE ANALYSIS OF PAPER MATERIALS COLLECTED DURING CONDUCTION OF EDUCATIONAL COMPETITONS

Peter A. Andreev
Student of group BPM1401, MTUCI
gtnzgtmz@gmail.com
Elena A. Skorodumova
MTUCI, PhD, associate professor of TPandAM department
eas@mtuci.ru

Keywords: *Educational data analysis, identification of images, automatizationof data analysis, neural networks, academic competition.*

The subject of this work is the development of mathematical algorithms for analysis of information on paper conducted for Moscow mathematical competitions "Vesenniy Olymp" and "Osenniy Olymp". The data structure suitable for organizers' needs has been projected. For the identification of digitalized papers neural networks, computer vision and the method of averaging by brightness have been analyzed. The method of averaging has been chosen as the fastest and the most effective. The developed model was used during conduction of "Vesenniy Olymp" (from March till May, 2018) and "Osenniy Olymp" (from September till October, 2018).

СЕМАНТИЧЕСКАЯ СЕТЬ КАК ИНСТРУМЕНТ ОБРАБОТКИ ВИЗУАЛЬНОЙ ИНФОРМАЦИИ

Литвин Ярослав Сергеевич
магистрант группы М091701(72) МТУСИ
litvinyaroslav@gmail.com
Гадасин Денис Вадимович
МТУСИ, к.т.н., доцент кафедры МСиУС,
dengadiplom@mail.ru

Ключевые слова: *распознавание четких образов на изображениях, семантическая сеть, оптимизация семантической сети, граф, разработка экспертной системы, база знаний*.

В статье рассматриваются вопросы по распознаванию цифровых изображений с помощью семантических сетей, для чего производится построение семантической сети, определение логических связей и способа представления знаний, что находит отражение в программной реализации, с помощью которой производится эксперимент по распознаванию. В результате работы получен функционал, который подтверждает предположение о возможности применения семантических сетей при распознавании образов до определенных границ размытости.

Семантическая сеть — является одним из способов представления знаний, связанных с областью инженерии знаний или различными разделами искусственного интеллекта как научной дисциплины [1]. В названии соединены термины из двух наук: семантика в языкознании изучает смысл единиц языка, а сеть в математическом представлении является разновидностью графа — набора вершин, соединённых дугами (рёбрами), которым присвоено некоторое значение (вес) и (или) направление.

В семантической сети роль вершин выполняют понятия базы знаний, а дуги (направления) задают отношения между ними. Таким образом, семантическая сеть отражает семантику предметной области в виде понятий и отношений между ними.

Главным отличием семантических сетей от нейронных является то, что она уже в себе содержит структурированную информацию, которую, к тому же, может прочитать и понять человек немного ознакомившись с терминологией и синтаксисом, в то же время знания (опыт) в нейронной сети представлены в виде набора чисел (весов), что является куда менее понятным представлением знаний для восприятия человеком, к тому же для приобретения опыта нейронной сети нужно использовать обучающие выборки данных для её тренировки, на что уходит немало времени.

Использование семантических сетей в задачах распознавания чётких образов цифр является интересной альтернативой нейронным сетям. Основной сложностью при построении семантических сетей является большой объем работы, который необходимо выполнить для получения ресурса, из которого формируется сеть [2].

Цель работы заключается в доказательстве актуальности использования семантических сетей для распознавания четких образов на изображениях и получении навыка разработки подобного программного продукта и работоспособного прототипа в качестве доказательства.

Как уже отмечалось ранее, одним из главных достоинств семантических сетей перед нейронными заключается в представлении знаний, которые может понять, как человек, так и машина. Из этого вытекает еще одно преимущество: семантические сети легко модифицировать (как менять связи между уже существующими вершинами (понятиями), так и создавать новые вершины и связи между ними), чем не может похвастаться семантическая сеть – её, скорее всего придется переобучать, внося изменения в обучающую выборку или же изменяя размерность сети.

Работу подобной экспертной системы по распознаванию четких образов на изображениях можно разделить на два основных этапа:

1. Предобработка входных данных (изображения);
2. Распознавание.

Этап предобработки изображения подразумевает представление цифры в виде набора сегментов, аналогичном представлению цифр на 7-сегментном экране (рис. 1), что окажет сильное влияние на размер проектируемой семантической сети. Дадим каждому сегменту имя для простоты понимания о каком сегменте идет речь в данный момент: tc – Top Center; tl – Top Left; tr – Top Right; mc – Middle Center; bl – Bottom Left; br – Bottom Right; bc – Bottom Center.

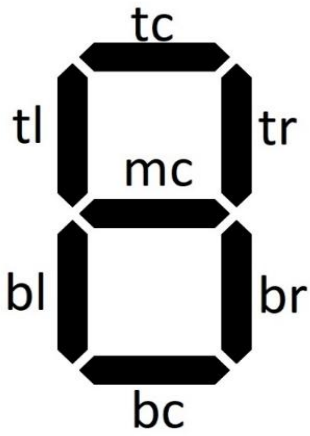


Рис. 1. 7-сегментное представление цифры.

Перед преобразованием в набор сегментов происходит вращение изображения вокруг его центра для избавления от наклона, обрезание по краям цифры и приведение к размеру 20x20 пикселей.

Представление цифры в виде набора сегментов происходит на основе анализа заполненности белыми пикселями на обработанном изображении определённых зон, каждая из которых закреплена за определенным сегментом. Если количество белых пикселей в зоне больше заданного порога, то считается, что в числе данный сегмент используется.

Такой подход к представлению цифр используется потому, что распознаваемые исходные изображения, пусть даже приведенное к определенному виду и размеру, имеют очень большой объем входных данных, а именно количество пикселей – этот фактор оказывает большое влияние на размер будущей семантической сети. Поэтому оптимальным вариантом является представлять цифры как набор сегментов в 7-сегментных экранах.

Определившись с видом входных данных для семантической сети можно переходить к её более глубокой, детальной проработке, определить количество видов вершин (понятий) и связей, а также архитектуру сети.

Одним из потенциальных вариантов организации семантической сети является построение на основе используемых в цифрах сегментов (табл. 1, рис. 2). В данной сети используется отношение ***has-a*** направленное от цифр (в кружочках) к сегментам (в квадратиках): *цифра 0 содержит в себе сегмент tc*. Как можно заметить такой способ организации семантической сети не является оптимальным по причине наличия большого количества связей.

Таблица 1

Используемые сегменты в цифрах.

Цифра	Используемые сегменты						
	tc	tl	tr	mc	bl	br	bc
0	■	■	■		■	■	■
1			■			■	
2	■		■	■	■		■
3	■		■	■		■	■
4		■	■	■		■	
5	■	■		■		■	■
6	■	■		■	■	■	■
7	■		■			■	
8	■	■	■	■	■	■	■
9	■	■	■	■		■	■

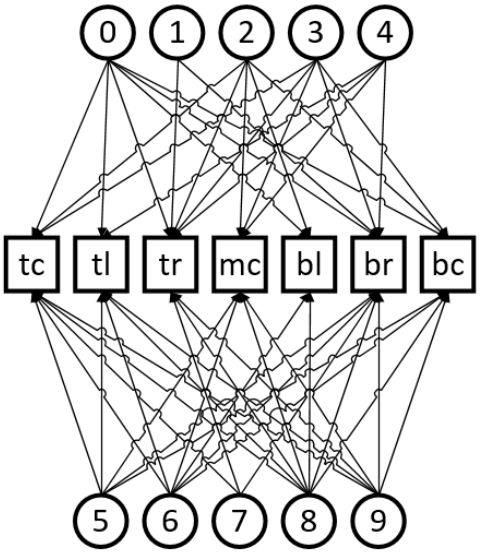


Рис. 2. Семантическая сеть на основе
табл. 1.

Следующий вариант представления информации в семантической сети основан на использовании сегментного сходства цифр (табл. 2): единица на пересечении обозначает, что цифра в строке использует точно такие же сегменты, что и цифра в столбце, то есть цифра в строке является частью (***a-kind-of***) цифры в столбце, или же цифра в столбце содержит в себе (***has-a*)** цифру из строки.

На основе данных из табл. 2 были получены графы всех зависимостей между цифрами (рис. 3). Для построения использовались все сочетания цифр, пересечение которых в таблице имеет значение 1. Данные графы имеют связь **has-a** между вершинами.

Таблица 2

Вычисление сегментного сходства цифр.

	0	1	2	3	4	5	6	7	8	9
0	1	1/3	2/3	2/3	1/2	2/3	5/6	1/2	1	5/6
1	1	1	1/2	1	1	1/2	1/2	1	1	1
2	4/5	1/5	1	4/5	2/5	3/5	4/5	2/5	1	4/5
3	4/5	2/5	4/5	1	3/5	4/5	4/5	3/5	1	1
4	3/4	1/2	1/2	3/4	1	3/4	3/4	1/2	1	1
5	4/5	1/5	3/5	4/5	3/5	1	1	2/5	1	1
6	5/6	1/6	2/3	2/3	1/2	5/6	1	1/3	1	5/6
7	1	2/3	2/3	1	2/3	2/3	2/3	1	1	1
8	6/7	2/7	5/7	5/7	4/7	5/7	6/7	3/7	1	6/7
9	5/6	1/3	2/3	5/6	2/3	5/6	5/6	1/2	1	1

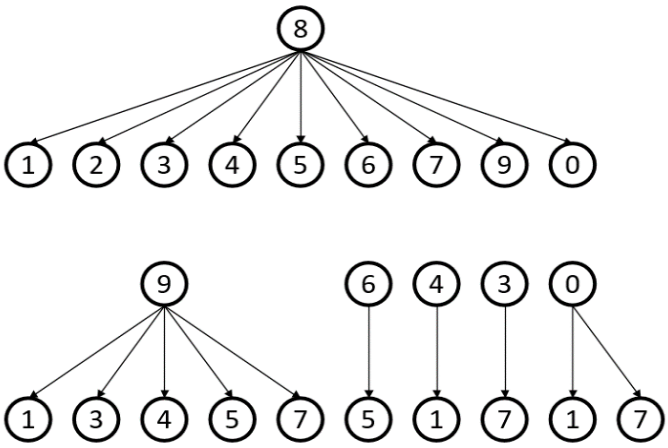


Рис. 3. Связи цифр на основе табл. 2.

Объединив все известные связи между вершинами в один граф была получена следующая картина отношения сегментов цифр между собой (рис. 4).

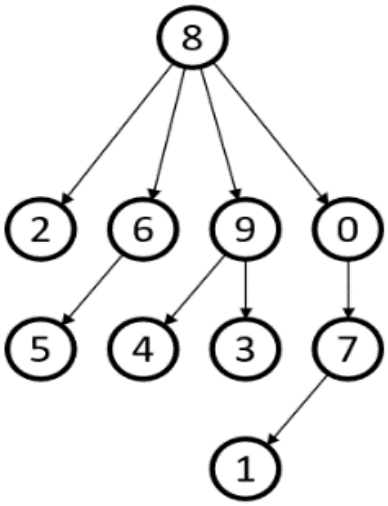


Рис. 4. Оптимизированный граф на основе табл. 2.

На данном этапе полученную сеть нельзя назвать полной, так как сами цифры состоят из более простых, атомарных, элементов – а именно сегментов.

Следовательно, в сеть необходимо добавить новый тип вершин – сегменты, при этом вид связи между вершинами можно оставить одного вида - ***has-a*** (рис. 5).

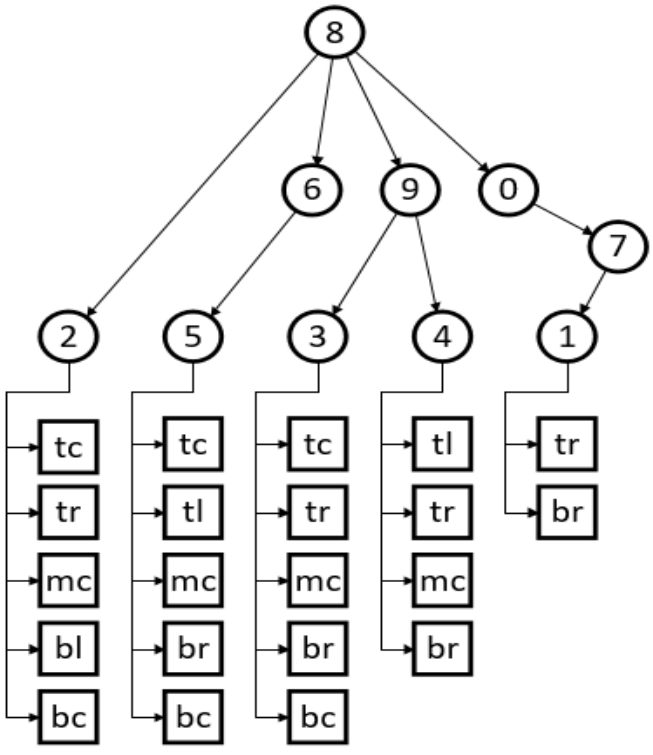


Рис. 5. Семантически полный граф.

Такой способ организации семантической сети вызывает необходимость модификации отношений между однотипными вершинами: отношение будет определять не только логическую взаимосвязь между вершинами, но и описывать какие сегменты не нужно использовать (или следует добавить) для получения следующей вершины. Это значит, что сеть будет обладать двумя типами вершин и тем же количеством типов связей (отношений). При этом модификация связей довольно существенно усложняет реализацию такой сети, а сеть по параметру избыточности не является оптимальной так как имеет повторяющиеся вершины-сегменты. Необходимо достичь минимального количества видов как вершин, так и связей.

Таблица 3

Сравнение количества исп. сегментов и сегментов-маркеров.

Цифра	Сегменты							Кол-тво используемых	
	tc	tl	tr	mc	bl	br	bc	сегментов	маркеров
0								6	2
1								2	2
2								5	1
3								5	2
4								4	2
5								5	2
6								6	2
7								3	2
8								7	4
9								6	4

Перспективным вариантом организации семантической сети может быть её построение на основе сегментов-маркеров – это сегмент или сочетание сегментов, количество которых меньше количества сегментов, используемых для описания данной цифры в 7-сегментном представлении цифр, которое однозначно идентифицирует проверяемую цифру. Использование сегментов-маркеров уменьшит количество проверок сегментов для однозначной идентификации, что существенно уменьшит размер и увеличит скорость работы сети (табл. 3, рис. 6).

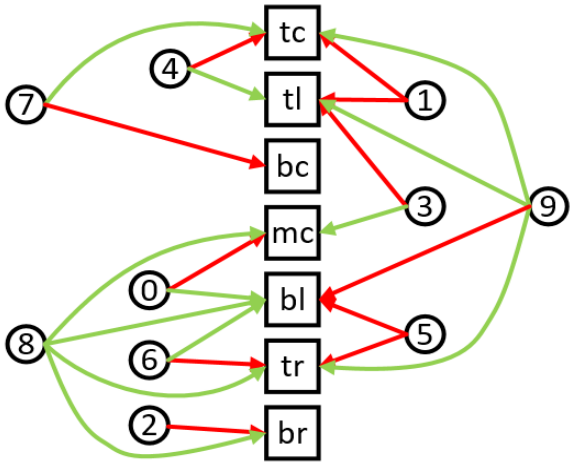


Рис. 6. Семантическая сеть на основе табл. 3.

Изначально предполагалось использовать в качестве маркеров только те сегменты, которые используются в данной цифре, но эмпирически было определено, что этого недостаточно: не удаётся достичь однозначной идентификации, поэтому в качестве маркера было решено дополнительно использовать отсутствующие сегменты в данной цифре. Это позволило не только добиться однозначной идентификации для всех цифр, но и уменьшить количество маркеров для некоторых цифр.

Построенная по такому принципу сеть является семантически полной [3] так как у неё отсутствуют дубликаты вершин и существует минимально возможное количество видов связей для такого представления данных. Данная сеть использует два вида вершин и связей.

Задача синтеза такой сети не трудозатратна, основным минусом для такой реализации является недостаток в виде необходимости сравнения проверяемой цифры со всеми вершинами-цифрами по сегментам-маркерам до тех пор, пока не будет найдено совпадение.

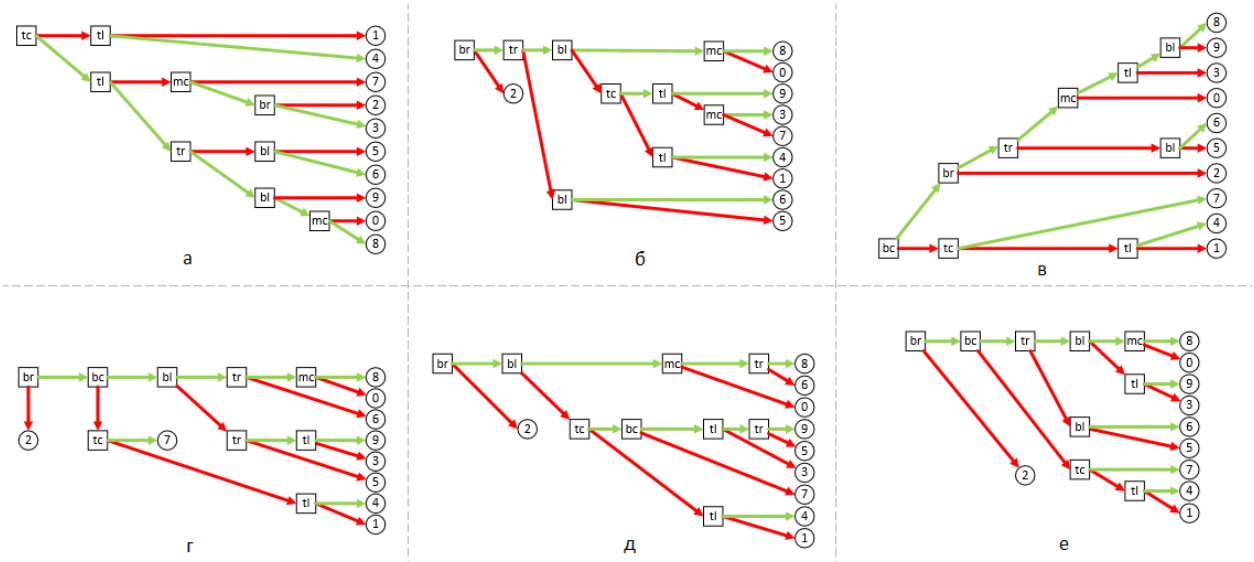


Рис. 7. Различные комбинации построения дерева.

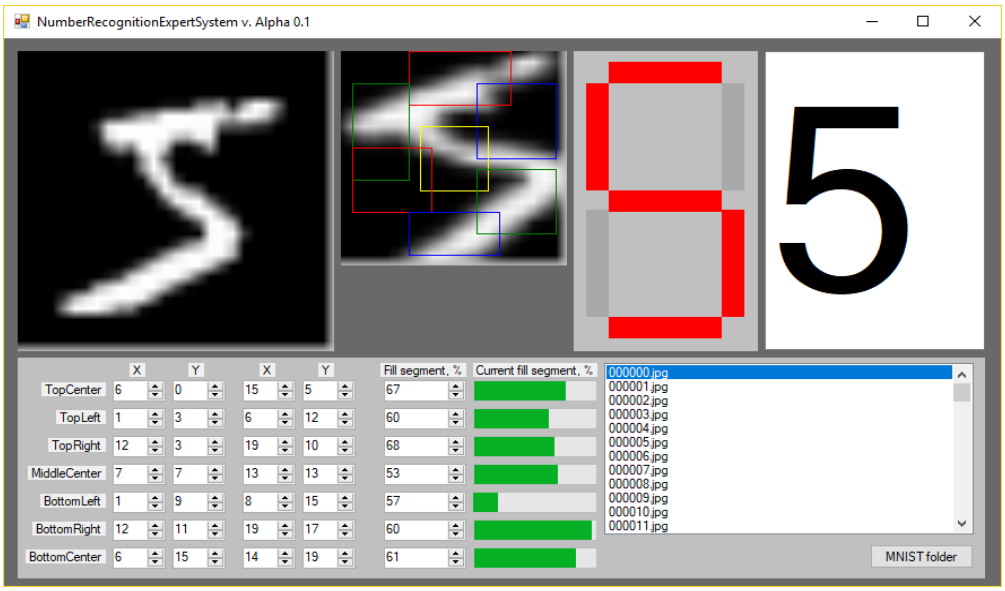


Рис. 8. Работа экспертной системы

Решение данной проблемы лежит в плоскости представления сегментов в виде древовидного графа (рис. 7). Преимущество данного подхода заключается в единственном входе, а поиск максимально простого пути, состоящего из наименьшего количества вершин-сегментов сети, строится на основе маркеров.

Данный подход нашел свою реализацию в разработанном прототипе экспертной системы, опирающейся на семантическую сеть. В возможности системы заложен механизм, распознающий четкие образы арабских цифр, которые предварительно преобразованы во входные данные в виде набора сегментов, механизм корректировки размеров и положения анализируемых зон изображения, а также подстройки порогового значения, выше которого система считает, что сегмент, закреплённый за данной областью, используется в распознаваемой цифре (рис. 8).

Анализ полученных результатов показал, что использование семантических сетей в качестве инструмента распознавания изображений является действенным способом решения задачи определения образов. По сравнению с нейронными сетями, в семантических, основное время тратится на формирование способа представления информации и установления логических связей между вершинами (понятиями), а не на обучение программного комплекса на основе обучающей выборки. Установление первичных логических связей в подавляющем большинстве

случаев задано в явном виде, следовательно, время на их установление минимально. В дальнейшем эти связи уточняются, что по своей идеологии сходно с обучением. Из этого можно сделать вывод что на первом этапе задачи распознавания образов автоматизированной системой целесообразнее применять семантические сети, с целью исключения безосновательной траты основного ресурса в виде времени, а на следующих шагах - подключать нейронные сети для более глубокого обучения и выявления скрытых зависимостей. Образуется своего рода симбиоз действий - дополняя друг друга развиваемся: если лучше с точки зрения "эксперта" работает семантическая сеть, то обучение нейронной происходит на основе семантической, если же лучше нейронная – переустанавливаются логические связи в семантической.

Литература

1. Советский энциклопедический словарь. // Изд. «Советская энциклопедия», 4-е издание — М.: 1989, 1632 с.
2. *Киселев Ю. А., Поршнев С. В., Мухин М. Ю.* Современное состояние электронных тезаурусов русского языка: качество, полнота и доступность // Программная инженерия. 2015. № 6. С. 34–40.
3. *Гаврилова Т. А., Хорошевский В. Ф.* Базы знаний интеллектуальных систем. СПб: Питер, 2000. 384 с.

SEMANTIC NETWORK AS AN INSTRUMENT FOR VISUAL INFORMATION PROCESSING

Litvin S. Yaroslav
Student of group M091701 (72), MTUCI
litvinyaroslav@gmail.com
Gadasin V. Denis
MTUCI, Ph.D., Associate Professor, Department of MSaCS
dengadiplom@mail.ru

Keywords: *recognition of clear images on pictures, semantic network, optimization of semantic network, graph, development of an expert system, knowledge base.*

The article deals with the issues of recognition of digital images using semantic networks, for which the semantic network is built, logical links are determined and the way knowledge is presented, which is reflected in the software implementation, which is used to make an experiment on recognition. Because of the work, a functional was obtained that confirms the assumption about the possibility of using semantic networks in recognizing patterns to certain limits of blurring.

ОБЗОР МЕТОДОВ ОБФУСКАЦИИ ИСХОДНОГО КОДА

Зайцев Евгений Сергеевич
студент группы М091801(72) МТУСИ
z.evg.serg@gmail.com
Беленькая Марина Наумовна
МТУСИ, доцент кафедры МСиУС
mn.belenkaya@mail.ru

Ключевые слова: *обфускация, виды обфускации, методы обфускации, защита исходного кода, запутывание исходного кода.*

Индустриальное программирование сопровождается необходимостью защиты разработанного исходного кода с целью предотвращения возможности кражи злоумышленником реализованных наработок и защиты интеллектуальной собственности программного обеспечения. Одним из способов такой защиты исходного кода является его запутывание (обфускация). В статье рассматриваются существующие методы обфускации исходного кода, приводятся поясняющие примеры некоторых видов обфускации, а также делаются выводы о том, какой из приведенных методов запутывания исходного кода является наилучшим и как целесообразно применять рассмотренные методы обфускации.

Проблема обфускации довольно новая, так как первые работы, связанные непосредственно с обфускацией, появились всего несколько лет назад. Тем не менее ряд публикаций на эту тему уже существует [1].

Обфускация (запутывание) – это преобразование исходного кода программного продукта таким образом, чтобы он стал максимально трудным для восприятия человеком или автоматизированными инструментами, осуществляющими реверсивную инженерию исходного кода. В процессе обфускации логика работы программы становится менее очевидной, при этом программа сохраняет свою работоспособность.

Существует ряд причин, по которым исходный код подвергается обфускации: улучшение безопасности кода, предотвращение фальсификации программного продукта, защита интеллектуальной собственности. Разработчики программного обеспечения могут также использовать методы обфускации, чтобы скрыть недостатки и уязвимости в своем продукте. Обфускация кода также защищает от вредоносных изменений в программном продукте и от нелицензионных копий, потому что злоумышленник должен сначала понять программное обеспечение, прежде чем он сможет внести определенные изменения. Коммерчески популярное программное обеспечение, такое как SkypeVoIP-клиент, SDCJavaDRM и большинство систем управления лицензиями используют, по крайней мере частично, обфускацию для своей безопасности.

Обфускация исходного кода затрагивает различные его элементы, в связи с чем различают несколько методов обфускации[2].

Обфускация представления

Обфускации представления связаны с изменением внешнего вида программы, а не с изменением семантики. Одной из простых обфускаций представления является удаление любых комментариев, которые программист может вставить в качестве части документации программы. Другой метод заключается во вставке фиктивных комментариев, чтобы часть программы, казалось, делала нечто иное по сравнению с тем, что требовалось. В любом случае комментарии часто удаляются при компиляции / декомпиляции программы.

Другой обфускацией представления является изменение форматирования программы, например, удаление всех ненужных пробелов и отступов. Также популярным методом обфускации

является изменение имен идентификаторов - не только для переменных, но также для классов, методов и т. д. Это преобразование направлено на изменение значимых имен, таких как «total» или «output», на такие имена, как «a» или «ghe251c». Еще одним из методов обфускации представления является переименование переменных таким образом, чтобы сбить с толку злоумышленника. Например, переменная, которая называется «total», может быть названа «average».

Инструменты, осуществляющие переименование, стараются иметь как можно больше элементов (включая методы, поля и классы) с одним и тем же именем либо путем определения области действия переменной, либо путем перегрузки.

Обфускацией представления может быть отменена компиляцией/декомпиляцией в зависимости от того, как компилятор именует свои переменные. Данная обфускация, как правило, не считаются очень действенной, поскольку ее часто можно легко отменить, а также она не связана с семантикой программы. Несмотря на это, обфускация представления часто используются в автоматизированных инструментах обфускации.

Обфускация управления

Обфускации представления, рассмотренные ранее, пытаются изменить синтаксис программы, а не ее семантику. Одним из видов семантических преобразований являются те, которые нацелены на поток управления, поэтому эти преобразования пытаются изменить условные утверждения, переходы и циклы.

Обфускация управления может использовать непрозрачные предикаты. Предикат P непрозрачен в программной точке s, если значение P в s известно во время компиляции. P_s^T обозначает предикат, который всегда находится в значении True (False) в s (программная точка s может быть опущена, если она понятна из контекста) и $P^?$ для обозначения предиката, который иногда находится в значении True, а иногда в False.

Непрозрачные предикаты могут использоваться для создания фиктивного кода в программах, например:

$$S => \boldsymbol{if}(P^T)\{S\} \quad (1)$$

$$S => \boldsymbol{if}(P^F)\{S_{bug}\}else\{S\} \quad (2)$$

$$S => \boldsymbol{if}(P^?)\{S\}else\{S_{copy}\} \quad (3)$$

Первое преобразование (1) пытается скрыть тот факт, что S всегда будет выполняться; второе (2) использует копию S, которая содержит ошибки; третье (3) использует функционально эквивалентную копию S.

Непрозрачные предикаты также могут быть использованы для добавления фиктивных переходов и особенно полезны для создания неприводимых графов потока, когда осуществляется переход в середину цикла. Например (4):

$$\begin{array}{l} \boldsymbol{if}(P^F)\{\boldsymbol{goto} L;\} \\ \ldots \\ \boldsymbol{while}(C) \\ \{\ldots \\ L\colon \ldots\} \end{array} \quad (4)$$

Языки, такие как C # и Java, не позволяют осуществлять такие переходы. Однако этот тип перехода будет разрешен на языках среднего уровня (CIL или Bytecode). Таким образом, возможно написать программу на языке высокого уровня, конвертировать в язык среднего уровня, где возможно добавить фиктивный переход, а затем перекомпилировать. Если декомпилятор попытался перестроить высокоуровневый код, будет создан более сложный код, так как декомпилятор будет пытаться превратить неприводимый переход в приводимый. Этот тип преобразования является примером преобразования, «ломающим язык».

Обфускация управления также включает в себя преобразования циклов следующего вида (5):

$$\textbf{while}(condition)\ \{\ body\ \} \tag{5}$$

Одним из таких преобразований является изменение переменной-счетчика с использованием кодирования. Например, имеется следующий цикл (6):

$$\begin{aligned} &i = 0; \\ &\textbf{while}(i < N) \\ &\{\dots i \dots \\ &i = i + 1;\} \end{aligned} \tag{6}$$

Заменяя *x* на выражение *(2x + 1)* можно преобразовать цикл следующим образом (7):

$$\begin{aligned} &i = 0; \\ &\textbf{while}(i < 2 * N + 1) \\ &\{\dots ((i - 1)/2) \dots \\ &\ \ i = i + 2;\} \end{aligned} \tag{7}$$

Еще одним методом является добавление фиктивной переменной-счетчика, которая может усложнить условие цикла. Например, можно добавить переменную *j* в условие цикла следующим образом (8):

$$\begin{aligned} &i = 0; \\ &j = 1; \\ &\textbf{while}((i < 10)\&\&(j < 120) \\ &\{\dots \\ &i = i + 1; \\ &j = j + 2 * i;\} \end{aligned} \tag{8}$$

В данном случае переменная j не играет роли, однако усложняет логику исходного кода.
Также существует метод, при котором такие конструкции, как *while (9)*

$$\begin{aligned} &init; \\ &\textbf{while}(cond) \\ &\{\ loop\_body;\ \} \end{aligned} \tag{9}$$

заменяются на конструкции вида switch, которые повторяются до достижения конечного утверждения (10):

$$\begin{aligned} &var = 1; \\ &\textbf{switch}(var) \\ &\{\ \textbf{case}1: \\ &\qquad init; var = 2; \textbf{break}; \\ &\textbf{case}2: \\ &if(cond) var = 3; else var = 4;\ \textbf{break}; \\ &\textbf{case}3: \\ &\qquad loop\_body; var = 2;\ \textbf{break}; \\ &\textbf{case}4: \\ &\qquad var = 1;\ \textbf{end};\ \} \end{aligned} \tag{10}$$

Переменная *var* действует как счетчик и контролирует выполнение блоков. В последнем блоке присвоение значения переменной является фиктивным.

Большинство преобразований, которые рассматривались ранее, были локальными и затрагивали только один метод. Существует множество преобразований, которые можно применить и к самим методам:

1. Методы внедрения. Вызов метода заменяется на само тело метода. Если имя метода перегружено, может потребоваться включить код, который проверяет тип метода и параметры.

2. Методы выделения. Замена последовательности операторов вызовом метода, в который выносятся данные операторы.

3. Методы клонирования. Создается множество копий одних и тех же методов с применением различных обфускаций. При вызове метода происходит выбор, к какому клону следует обращаться. Если есть разные вызовы исходного метода в программе, можно заменить каждый вызов вызовами на другой набор методов клонирования.

4. Методы перемежения. Объединение нескольких методов в один.

Помимо использования этих преобразований по отдельности, можно объединять эти преобразования, чтобы осуществить более сложную обфускацию. Например, можно внедрить метод *m* в вызывающий метод *c* и после выделить отдельный блок из *c*в новый метод *m'*.

Обфускация данных

Помимо обфускации управления, можно обфусцировать данные и структуры данных, которые может использовать программа. Возможно как изменение отдельных переменных, так и всей структуры типа данных.

Преобразование переменной заключается в замене переменной выражением. Например, $i => a * i + b$, где *a* и *b* являются константами. Преобразование должно быть обратимым на случай, если появится необходимость получить исходное значение переменной. Преобразование необходимо производить отдельно для определения и использования. Например, используя преобразование выше (11):

$$j = i + 1 => j = \frac{i-b}{a} + 1 \quad (11)$$

Выражение *i++* является и определением, и использованием, таким образом (12):

$$i++ => a * \left(\frac{i-b}{a} + 1\right) + b \quad (12)$$

Это выражение может быть упрощено (согласно правилам арифметики) до *i = i + a.*

Помимо обфускации отдельных переменных, также возможно обфусцировать несколько переменных вместе, то есть осуществить слияние переменных, при котором происходит объединение двух (или более) переменных в одну. Предположим, требуется объединить две переменные *x* и *y*, о которых известно следующее: $0 \le x < N;\ y \ge 0$. Такие переменные можно объединить в переменную *z*, например, следующим образом: $z = N * y + x$.

Помимо объединения двух или более переменных, можно разделить одну переменную на две (или более) другие переменные. Например, целочисленная переменная x может быть разделена на две переменные a и b такие, что $a = x\ div\ 10$ и $b = x\ mod\ 10$, а выражение *x++* преобразуется в $a = (10 * a + b + 1)\ div\ 10$ и $b = (b + 1) mod\ 10$. Эти утверждения эквивалентны следующему (13):

$$\boldsymbol{if}(b == 9)\{a = a + 1; b = 0;\}\boldsymbol{else}\{b = b + 1;\} \quad (13)$$

Помимо обфускации одной переменной (или небольшого набора переменных), также возможно запутывать массивы. Перед выполнением преобразований массива необходимо убедиться, что массивы безопасны для преобразования. Например, можно потребовать, чтобы целый массив не передавался другому методу, или необходимо убедиться, что элементы массива не генерируют исключения.

Один из простейших способов обфускации массивов - это изменение индексов массива. Такое изменение может быть достигнуто либо с помощью преобразования переменной, либо путем перестановки индексов. Два других метода преобразования, которые обфусцируют индексы, называются складыванием и развертыванием. Например, можно сложить одномерный массив в двумерный или развернуть двумерный в одномерный.

Также существует структурное преобразование, называемое разбиением массива (14):

$$\begin{array}{l} \boldsymbol{int}[]A = \boldsymbol{new}\ \boldsymbol{int}[10]; \\ \boldsymbol{int}[]A2 = \boldsymbol{new}\ \boldsymbol{int}[5]; \\ \ldots \\ A[i] = \ldots; \\ \boldsymbol{else}A2[i/2] = \ldots; \end{array} \Rightarrow \begin{array}{l} \boldsymbol{int}[]A1 = \boldsymbol{new}\ \boldsymbol{int}[5]; \\ \\ \ldots \\ \boldsymbol{if}\big((i\%2) == 0\big)\, A1[i/2] = \ldots; \end{array} \quad (14)$$

Наравне с разбиением массива существует слияние массивов. Как и при разбиении, необходимо определить порядок элементов в новом массиве. Предположим, есть массивы B_1 размера m_1, B_2 размера m_2 и новый массив A размером $m_1 + m_2$. Можно определить связь между массивами следующим образом (15):

$$A[i] = \begin{cases} B_1[i] if\, i < m_1 \\ B_1[i - m_1] if\, i \geq m_1 \end{cases} \quad (5)$$

Существует метод обфускации, при котором изменяется область действия переменной, чтобы, например, сделать локальную переменную глобальной. Это делается для того, чтобы создать иллюзию связи несвязанных методов, используя эту новую глобальную переменную при вызове методов.

Дополнительные методы обфускации

Большинство обфускаций, рассмотренных ранее, могут быть применены к различным языковым парадигмам. Однако имеются некоторые обфускации, которые требуют определенных языковых возможностей.

Многие языки программирования имеют функции, которые позволяют пользователю добавлять код, который может обрабатывать любые исключения, которые могут встретиться. Это можно использовать для изменения потока управления программами. Например, предположим, что имеется следующий цикл (16):

```
i = 0;
while(i < N)
{ loopcode                    (6)
i++; }
afterloop
```

Используя новую переменную s, можно изменить его на (17)

```
try
{ i = 0; s = 1;
```

```
while(true)
  { s = s + s/(N − i);
loopcode
i + +; }
}
catch(DivideByZero)
{s = dummy; }
finally
{ afterloop }
```

Можно заменить предикат *true* некоторым другим предикатом, который является истинным для цикла, но может быть ложным в противном случае - это делается для того, чтобы сделать менее очевидным тот факт, что цикл будет завершаться только путем выдачи исключения.

Некоторые преобразования подходят для запутывания объектно-ориентированных программ. Многие программы Java полагаются на вызовы стандартных библиотек, но эти вызовы нельзя обфусцировать. Вместо этого некоторые из этих вызовов библиотек могут быть реализованы в самой программе, которую затем можно запутать отдельно. Другие преобразования направлены на изменение отношений наследования между разными классами путем вставки фиктивного класса или рефакторинга. Рефакторинг - это метод поиска элементов, которые являются общими для классов, а затем перемещение этих элементов в новый класс. Если классы не имеют общего поведения, может применяться ложный рефакторинг.

Можно добавить указатели в программу, чтобы сильнее ее запутать, поскольку, как известно, выполнение точных анализов псевдонимов является сложной проблемой. Так, эффективность метода, при котором такие конструкции, как *while,* заменяются на конструкции вида switch, усиливается наличием указателей.

Все рассмотренные ранее обфускации были нацелены на языки программирования высокого уровня [3]. Однако многие из них могут также применяться к промежуточным языкам, таким как JavaBytecode и .NET CIL (CommonIntermediateLanguage). Оба эти языка основаны на стеках и являются целями компиляции для разных исходных языков, таких как Java и C#.

Преимущество использования языков промежуточного уровня заключается в том, в них можно использовать обфускации, которые могут не допускаться на исходном языке. Например, можно осуществить переход в середину цикла. В Java и C# переходы в циклы не допускаются, но их можно добавить на уровне промежуточного языка.

Также могут быть инструкции на промежуточном уровне, которые не имеют прямого перевода обратно на язык более высокого уровня. Например, CIL имеет тип, называемый типизированной ссылкой, который создает объект, содержащий указатель и тип – команда *mkrefany* создает типизированную ссылку, а команды *refanyval* и *refanytype*извлекают значение и тип из типизированной ссылки. Эти типы не могут быть легко преобразованы обратно в исходный код C#, и поэтому использование типизированных ссылок может сломать декомпилятор C#.

Трудно вручную добавлять обфускации на промежуточные языки, особенно те, которые направлены на обфускацию циклов, поскольку они записываются с использованием условий и переходов. Однако есть инструменты, которые автоматически добавляют обфускации к промежуточному языку, например,DashO и Dotfuscator.

Заключение

Чтобы добиться наилучшей защищенности исходного кода, необходимо использовать как можно больше видов обфускации в программном продукте. Только в этом случае применение реверсивной инженерии будет наиболее затруднено. Однако следует учитывать тот факт, что обфускация снижает быстродействие программного продукта, и подвергать обфускации лишь наиболее важные участки исходного кода.

Литература

1. *Gregory, Wroblewski*. General Method of Program Code Obfuscation / Wroblewski. Gregory. – Wroclaw, 2002. – 112 с.
2. *Stephen Drape*. Intellectual property protection using obfuscation / Oxford University Computing Laboratory. – 50 с.
3. *Bjarne Stroustrup*. The C++ Programming Language, 4th Edition // Pearson Education, Inc. 2013. – 1346 с.
4. *Беленькая М. Н., Малиновский С. Т., Яковенко Н. В.* Администрирование в информационных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 400 с.

SOURCE CODE OBFUSCATION METHODS REVIEW

Evgeny S. Zaytsev
Student of group M091801(72), MTUCI
z.evg.serg@gmail.com
Marina N. Belenkaya
MTUCI, associate professor of MNaCS department
mn.belenkaya@mail.ru

Keywords: *obfuscaction, obfuscation types, obfuscation methods, source code security, source code confuse.*

Industrial programming is accompanied by the need to protect the developed source code in order to prevent the attacker from stealing the implemented developments and protecting the intellectual property of the software. One way to protect the source code is to obfuscate it. The article discusses the existing methods of obfuscation of the source code, provides explanatory examples of some types of obfuscation, and also concludes which of the above methods for entangling the source code is the best and how appropriate it is to apply the obfuscation methods discussed.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ КЛАСТЕРИЗАЦИИ НЕЖЕЛАТЕЛЬНЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Шелухин Олег Иванович,
МТУСИ, профессор, д.т.н., зав., кафедрой «Информационная безопасность»,
sheluhin@mail.ru,
Неклесова Марина Дмитриевна,
МТУСИ, студент группы М111701(73),
neklesova_marisha@mail.ru

Ключевые слова*: метод k-средних, алгоритмы кластеризации, машинное обучение; приложения; EM-алгоритм, DBSCAN, Точность, Полнота, F-мера.*

Статья посвящена обзору алгоритмов кластеризации мобильного сетевого трафика в целях фильтрации трафика нежелательных приложений, а также их сравнительному анализу. Для проведения кластеризации используется трафик таких программ для мобильных платформ как Facebook, Google Chrome, Instagram, Messenger и WhatsApp. Данный выбор основан на мировой популярности этих приложений. Кластеризация выполняется при помощи программного продукта *WEKA*, который обеспечивает программную реализацию исследуемых методов. Рассматриваются такие алгоритмы кластеризации как метод k-средних, EM-алгоритм и *DBSCAN*. Эксперимент заключается в обработке экспериментально полученных данных трафика приложений каждым из алгоритмов кластеризации с целью определения соответствующего кластера. Для проведения сравнительного анализа используются характеристики точности, полноты и F-мера. С их помощью делаются выводы о качестве работы каждого алгоритма.

Показано, что наиболее эффективным методом кластеризации сетевого трафика мобильных приложений является алгоритм *DBSCAN*. Именно его целесообразно использовать при фильтрации трафика нежелательных мобильных приложений.

Постановка задачи

За последние годы популярность мобильных средств связи вышла на новый уровень, оставив позади громоздкие настольные устройства. В связи с этим расширяется поле для разработки программного обеспечения для мобильных платформ. К примеру, на начало 2018 года в магазине «AppStore» уже насчитывалось более 2,1 млн приложений. Стоит отметить, что в этот список входят лишь приложения, прошедшие тестирование на отсутствие вредоносного кода и соответствующие нормам цензуры. Однако существует множество непроверяемых ресурсов, где любой желающий может опубликовать свою разработку. Используя такой источник программного обеспечения, пользователь рискует информацией, которая хранится на его смартфоне, то есть своими денежными средствами и персональными данными. Поэтому остро встаёт вопрос выявления и фильтрации сетевого трафика нежелательных мобильных приложений [6 – 20]. Данная статья нацелена на решение этого вопроса методами кластеризации.

Цель работы

Целью работы является практическое выявление наиболее эффективного метода кластеризации трафика мобильных приложений на основе критериев точности и полноты.

База данных мобильных приложений

Кластеризация представляет собой метод статистической обработки данных, относящийся к классу задач «обучения без учителя». Данная методология позволяет разбить наблюдаемую выборку на группы схожих объектов (кластеры), выделяя при этом нетипичные элементы, которые не могут быть отнесены ни к одному из кластеров [3].

Для исследования данного вопроса были собраны данные сетевых приложений Facebook, Google Chrome, Instagram, Messenger и WhatsApp. Выбор программных продуктов осуществлялся

на основе их популярности как для устройств под управлением iOS, так и для платформ Android. Из наблюдаемого сетевого трафика были выделены потоки каждого из приложений. Объёмы полученных выборок отражены в таблице 1.

Таблица 1

Объём выборок для исследуемых приложений

Приложение	Выборка данных
Facebook	1286
Google Chrome	5598
Instagram	1437
Messenger	2159
Whatsapp	2005
Всего	12485

Для каждого наблюдаемого потока определялись следующие 14 атрибутов:

- PortA – номер порта источника;
- PortB – номер порта получателя;
- Packets –количество переданных пакетов в потоке;
- Bytes – количество переданных байт в потоке;
- PacketsAB – количество пакетов, переданных в направлении от источника к получателю;
- BytesAB – количество байт, переданных в направлении от источника к получателю;
- PacketsBA – количество пакетов, переданных в обратном направлении;
- BytesBA – количество байт, переданных в обратном направлении;
- RelStart – начало потока относительно момента начала захвата в секундах;
- Duration – продолжительность данного потока в секундах;
- Bits/sAB – средняя скорость передачи в направлении от источника к получателю;
- Bits/sBA – средняя скорость передачи в обратном направлении;
- Protocol – протокол транспортного уровня (*TCP/UDP*);
- Class – метка класса (совпадает с названием приложения и служит для проверки качества кластеризации).

Анализ методов кластеризации и критерии оценки качества их работы

Представленные в таблице 1 атрибуты характеризуют конкретный поток. Принадлежность потока к тому или иному классу определяет заранее добавленная метка. Исследование заключается в кластеризации сетевого трафика выбранных приложений исходя из 13 атрибутов и последующей оценки качества кластеризации путём проверки соответствия меток класса кластерам. Данное исследование проводились при помощи программного продукта *WEKA* [1,2].

Проводились исследования трех алгоритмов кластеризации: k-средних EM-алгоритм и DBSCAN (Density-based spatial clustering of applications with noise – плоскостная пространственная кластеризация приложений с шумом).

Алгоритм k-средних

Данный алгоритм предполагает, что число кластеров заранее известно. На первом этапе случайным образом для кластеров выбираются центроиды, которые затем для каждого кластера полученного на предыдущем шаге итеративно пересчитываются. Элементы с минимальным суммарным отклонением от величин центров масс приписываются этому кластеру. Расчет суммарного квадратичного отклонения производится по формуле :

$$V = \sum_{i=1}^{k} \sum_{x \in S_i} (x - \mu_i)^2 \quad , \qquad (1)$$

где k – число кластеров, S_i – полученные кластеры, $i = \overline{1,k}$, μ_i – центроид всех векторов x из кластера S_i.

В результате выборка, в зависимости от того, какой из новых центров оказался ближе по выбранной метрике [4], снова и снова разбивается на кластеры.

EM-алгоритм

Алгоритм включает в себя выполнение цикла итераций, каждая из которых включает в себя три шага.

На E-шаге (expectation) вычисляется ожидаемое значение функции правдоподобия.

На M-шаге вычисляется оценка максимального правдоподобия, увеличивая ожидаемое правдоподобие, вычисляемое на E-шаге (maximization).

Третьим шагом является повторение 2х предыдущих шагов, причём новое значение ожидаемого правдоподобия используется для E-шага на следующей итерации [4].

Алгоритм EM позволяет указать число создаваемых кластеров. Однако метод может и сам определить, сколько кластеров необходимо создать при помощи перекрёстной проверки.

DBSCAN

Алгоритм DBSCAN основан на плотности распределения элементов в многомерном пространстве. Размерность пространства определяется числом атрибутов элемента. То есть из заданного набора точек в каком-либо пространстве объединяются те точки, которые тесно связаны друг с другом (имеют близко расположенных соседей). Точки, которые расположены в областях с низкой плотностью (далеко от соседей), помечаются как шум и не включаются в какую-либо группу (кластер) [4].

Преимущества *DBSCAN* перед другими алгоритмами следующие:

- алгоритм позволяет находить нелинейно разделяемые кластеры (такой набор данных не может быть надлежащим образом сгруппирован с методами k-средних или EM);
- алгоритм не требует указывать количество кластеров;
- алгоритм позволяет находить кластеры произвольной формы. Могут также быть найдены кластеры, полностью окруженные (но не соединённые) другими кластерами;
- алгоритм устойчив к выбросам, так как имеет представление о шуме;
- алгоритм нечувствителен к порядку элементов выборки.

Метрики оценки качества кластеризации

Для оценки эффективности работы алгоритмов машинного обучения используются такие метрики, как Точность, Полнота и F-мера, которые вычисляются по следующим формулам [5]:

$$\text{Точность} = \frac{TP}{TP + FP}\ ; \qquad (2)$$

$$\text{Полнота} = \frac{TP}{TP + FN}\ ; \qquad (3)$$

$$F - \text{мера} = 2 * \frac{Precision * Recall}{Precision + Recall}, \qquad (4)$$

где TP – TruePositive (Истинно Положительный) – количество элементов, которые были правильно отнесены к рассматриваемому классу; FP – FalsePositive (Ложно Положительный) – количество элементов, которые были отнесены к классу, которому на самом деле не принадлежат; FN – FalseNegative (Ложно Отрицательный) – количество элементов, которые ошибочно классифицируется как экземпляры не данного класса, хотя на самом деле принадлежат ему.

Результаты экспериментов

Исследование алгоритма k-средних

После настройки алгоритма на поиск 5 кластеров *WEKA* вывела результат, представленный на рисунке 1. Рисунок 1 отображает данные о полученных значениях центроидов каждого из кластеров. Для реализации алгоритма было произведено 17 итераций, а построение модели заняло 0.67 секунды. В 3-х из 5-ти кластерах центральным оказался элемент с меткой класса Chrome. Такой результат свидетельствует о разнообразии атрибутов потоков приложения «Google Chrome». Элементы этого приложения оказались разбросаны по всему пространству. Это говорит о том, что целесообразно увеличить число кластеров, объединив в последствие те, что соответствуют одной и той же метке класса. Результат кластеризации для 10 кластеров приведён на рисунке 2.

```
kMeans
======

Number of iterations: 17
Within cluster sum of squared errors: 6047.779308226287
Missing values globally replaced with mean/mode

Cluster centroids:
                                Cluster#
Attribute          Full Data          0          1          2          3          4
                     (12485)     (3726)     (1363)     (4160)     (1308)     (1928)
=============================================================================================
Port A            41068.7333  43461.9321  42072.9479  35349.6185  43246.7928  46596.1255
Port B             1396.9748    648.0215    527.8401   2655.1553    546.6292   1320.9642
Packets            1085.1021   1016.1428   3767.4138     78.0995   2320.6843    656.6483
Bytes            786894.8006 721084.8983 2782720.3955  36432.4204 1750175.1544 468871.0498
Packets A > B       541.1909    505.4391   1881.9149     34.6724   1175.4618    325.0581
Bytes A > B       54157.7707  55413.5687 153485.5796  13200.5144  92337.4771  43981.5379
Packets B > A       543.9112    510.7037   1885.4989     43.4272   1145.2225    331.5902
Bytes B > A       732737.0299 665671.3296 2629234.8158  23231.906 1657837.6774 424889.5119
Rel Start           1666.7711    587.8987   2447.5906   1316.1945   3990.2824   2379.8767
Duration              98.5375     89.6374    156.877     92.9998     81.7696     97.819
Bits/s A > B       95490.6113  111835.7675  41036.8632  35641.8544  173676.6153 178489.5435
Bits/s B > A      775986.7392   559218.498  630789.2418 353182.1961 2582155.9003 984482.7415
Protocol                  TCP         TCP         TCP         UDP         TCP         TCP
Class                Chrome      Chrome   Instagram      Chrome      Chrome   Messenger


Time taken to build model (full training data) : 0.67 seconds
```

Рис. 1. Результат работы алгоритма SimpleKMeans

```
Number of iterations: 39
Within cluster sum of squared errors: 4397.440082786802
Missing values globally replaced with mean/mode

Cluster centroids:
                                Cluster#
Attribute          Full Data          0          1          2          3          4          5          6          7          8          9
                     (12485)     (1413)     (1201)     (1265)      (175)     (1806)      (590)      (605)     (1015)     (2778)     (1637)
=============================================================================================================================================
Port A            41068.7333  46975.8839  43997.9584  40255.6862  44887.8286  47063.7021  43122.2983  42771.4215  46087.5498  28041.7131  45052.6549
Port B             1396.9748    424.6065    592.144    418.732    440.9257   3066.8533    407.9305    414.8      1086.734    336.7369   4553.6823
Packets            1085.1021    335.3411   3574.8351   175.9375   11844.3429   654.8643    375.9542    453.0926   4179.4581    28.3006    296.6261
Bytes            786894.8006 242079.3984 2660418.3472 113031.6909 9313216.7429 463160.0377 237497.4898 325801.1884 2979446.4857 20555.4057 158473.7783
Packets A > B       541.1909    165.9469   1790.6162    87.6103   5954.4286    326.3283    212.7661    227.562    2083.3892    7.4507     141.1179
Bytes A > B       54157.7707  14759.8273  143424.0908 11001.1059 431584.2629  41947.7907  18628.7119  20805.7719 171345.3094 1541.1832  70907.2175
Packets B > A       543.9112    169.3942   1784.219    88.3273   5889.9143    328.536     163.1881    225.5306   2096.069    20.8499     155.5082
Bytes B > A       732737.0299 227319.5711 2516994.2565 102030.585 8881632.48  421212.247  218868.778  304995.4165 2808101.1764 19014.2225 87566.5608
Rel Start           1666.7711    492.928    2243.8148   377.6496   4872.5531   2191.1196   4266.9609   2331.9798   2367.9496   1191.7613   1519.9674
Duration              98.5375     45.9156    135.5592    59.0661    4.9258     104.9388    92.163      82.8919     206.4369    115.4488    62.7242
Bits/s A > B       95490.6113  23080.8467  43314.8017  8905.4645  702864.4905 38725.2002  32864.1669  21965.6278  14401.3508  45646.3188  445485.431
Bits/s B > A      775986.7392  270962.992  682072.9988  51538.85 14424953.7702 608339.5229 378019.4849 217430.6931 149389.9656 471682.2455 1821251.1716
Protocol                  TCP         TCP         TCP         TCP         TCP         TCP         TCP         TCP         TCP         UDP         TCP
Class                Chrome      Chrome   Instagram      Chrome      Chrome   Messenger      Chrome      Chrome    Facebook      Chrome   WhatsApp
```

Рис. 2. Результат работы алгоритма SimpleKMeans

Из рисунка 2 видно, что все метки класса хотя бы раз присутствуют в центроиде какого-либо из классов. Таким образом можно проводить кластеризацию на 10 кластеров, однако среди полученных выделять 5 классов: Кластеры 0, 2, 3, 5, 6, 8 – Chrome ; Кластер 1 - Instagram ; Кластер 4 - Messenger ; Кластер 7 - Facebook Кластер 9 - WhatsApp .

Для построения модели потребовалось 39 итераций, что более чем в два раза превышает число шагов при разбиении выборки на 5 кластеров.

Программный продукт WEKA позволяет выполнить кластеризацию с учётом метки класса и осуществить вывод матрицы ошибок. В этом режиме сначала происходит кластеризация методом k-средних, где метки класса игнорируются. Затем классы соотносятся с кластерами на основе значения большинства меток класса в каждом кластере. После этого вычисляется ошибка классификации, основанная на этом назначении. Матрица ошибок алгоритма k-средних представлена в Таблице 2. Построение модели заняло 1,07 секунды и 24 итерации.

Из таблицы видно, что наилучшая кластеризация методом k-средних была выполнена для класса Google Chrome, для которого 47% верно классифицированных потоков. Следующим по эффективности является кластер Whatsapp (39%). Хуже всего алгоритм справился с задачей определения класса Messenger (14%). По данным, представленным в таблице 2 можно отметить, что кластер Instagram имеет характеристики, сильнее всего отличающиеся от характеристик приложения Whatsapp. При этом кластер с меткой WhatsApp, часто содержит в себе элементы, относящиеся к классу Google Chrome. С точки зрения уязвимости кластеров для попадания данных из других классов, абсолютного лидера среди приложений нет (ко всем кластерам так или иначе были отнесены элементы других классов).

На основании таблицы 2 было проведено вычисление метрик Точности, Полноты и F-меры. Результаты представлены в таблице 3. F-мера является комплексной метрикой качества кластеризации, включающей в себя Полноту и Точность как это видно из (4). Таблица 3 наглядно иллюстрирует, что по обоим этим метрикам лидирует класс Google Chrome. Однако средние значения качества всех приложений не превышают 30%.

Таблица 2

Матрица ошибок при кластеризации алгоритмом SimpleKMeans

Тип трафика	0	1	2	3	4	Исх. кол-во потоков	Верно кластеризовано, %
Facebook	277	327	153	226	303	1286	23,561
Google Chrome	2642	1241	605	800	310	5598	47,195
Instagram	418	323	201	308	187	1437	21,433
Messenger	494	545	314	402	404	2159	14,543
Whatsapp	237	790	556	57	365	2005	39,401

Таблица 3

Метрики результатов кластеризации методом k-средних

Приложение	Точность	Полнота	F-мера
Facebook	0,193117	0,235614	0,212259
Google Chrome	0,649459	0,471954	0,546658
Instagram	0,171779	0,214335	0,190712
Messenger	0,171679	0,145438	0,157472
Whatsapp	0,244885	0,394015	0,302045
Среднее	0,286184	0,292271	0,28183

В итоге из 12 485 потоков после кластеризации методом k-средних на 5 кластеров всего 4 357 (35%) потоков были распределены в соответствии с меткой класса. Полученный результат требует изучения других, более эффективных, алгоритмов кластеризации.

Исследование EM-алгоритма

При помощи EM-алгоритма была выполнена кластеризация выборки данных, представленной в таблице 1. Построение модели заняло 729,47 секунд (около 12 минут). При автоматическом определении количества классов (перекрёстной проверке) было выделено 8 кластеров. Результаты попадания элементов с меткой класса в кластеры отражены в таблице 4

Таблица 4

Матрица ошибок при кластеризации EM-алгоритмом

Кластер / Класс	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	Верно кластеризовано, %
Facebook	219	3	23	101	455	400	82	3	17,0295
Google Chrome	762	1	26	928	1315	2038	274	254	36,4059
Instagram	226	0	98	171	413	230	257	42	17,8845
Messenger	273	94	9	146	565	801	242	29	26,1695
Whatsapp	125	99	15	92	222	847	26	579	28,8778

По результатам, приведённым в таблице 4, можно сделать вывод об ошибочной кластеризации почти в 70% случаев. Наиболее полно были включены в свой кластер элементы с меткой Google Chrome. Однако к этому кластеру были отнесены большие доли трафика с пометками Messenger, Facebook и Whatsapp. В результате класс Chrome можно назвать самым уязвимым для попадания в него других элементов. На основании таблицы 4 для EM-алгоритма было проведено вычисление метрик Точности, Полноты и F-меры. Результаты представлены в таблице 5.

В среднем, по критерию точности EM-алгоритм справляется с кластеризацией лучше, чем метод k-средних. Однако полученный результат в 34% является достаточно низким показателем для эффективной фильтрации трафика нежелательных приложений.

Исследование алгоритма DBSCAN

Результаты кластеризации в виде статистики попаданий элементов выборки в каждый из кластеров для алгоритма DBSCAN представлены в таблице 6.

Таблица 5

Метрики результатов кластеризации EM-алгоритмом

Тип трафика	Точность	Полнота	F-мера
Facebook	0,136449	0,170295	0,151505
Google Chrome	0,472196	0,364059	0,411136
Instagram	0,291714	0,178845	0,221743
Messenger	0,190236	0,261695	0,220316
Whatsapp	0,638368	0,288778	0,397665
Среднее	0,345793	0,252734	0,280473

Таблица 6

Матрица ошибок при кластеризации алгоритмом *DBSCAN*

Кластер / Класс	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	Верно кластеризовано %
Facebook	653	0	0	0	0	0	0	0	0	630	99,76672
Google Chrome	0	4047	1551	0	0	0	0	0	0	0	100
Instagram	0	0	0	927	510	0	0	0	0	0	100
Messenger	0	0	0	0	0	1210	949	0	0	0	100
Whatsapp	0	0	0	0	0	0	0	850	1155	0	100

Построение модели кластеризации алгоритмом *DBSCAN* заняло всего 25,15 секунд. На основании таблицы 4 можно сделать выводы о взаимосвязи кластеров и меток класса: Кластеры 0, 9 – Facebook ; Кластеры 1, 2 – Chrome ; Кластеры 3, 4 – Instagram ; Кластеры 5, 6 – Messenger; Кластеры 8, 9 – WhatsApp.

Отметим, что 3 элемента с меткой класса Facebook были приняты за шумовые . Полученные результаты наглядно иллюстрируют преимущества алгоритма DBSCAN по сравнению с другими методами кластеризации. Это означает, что если имеется представление о метке класса хотя бы одного элемента из кластера, то можно безошибочно соотнести кластер с приложением, сгенерировавшим трафик. Следует учитывать, однако, что некоторые классы (в данном случае Facebook) могут быть определены не полностью.

Показатели Точности, Полноты и F-меры представлены в таблице 7.

Таблица 7

Метрики результатов кластеризации алгоритмом DBSCAN

Приложение	Точность	Полнота	F-мера
Facebook	1	0,997667	0,998832
Google Chrome	1	1	1
Instagram	1	1	1
Messenger	1	1	1
Whatsapp	1	1	1
Среднее	1	0,999533	0,999766

По представленным результатам, можно сделать вывод , что алгоритм *DBSCAN* обеспечивает кластеризацию с точностью 100%, однако по критерию полноты алгоритм эффективен на 99,95%.

Сравнительный анализ результатов исследования

Для наглядности результаты экспериментов отражены в таблице 8.

Таблица 8

Сравнение алгоритмов кластеризации

Алгоритм	Точность	Полнота	F-мера	Время построения модели, с
k-средних	0,286184	0,292271	0,28183	1,07
EM-алгоритм	0,345793	0,252734	0,280473	729,47
DBSCAN	1	0,999533	0,999766	25,15

По сравнению с другими алгоритм k-средних требует меньше вычислительных ресурсов при построении модели, а время его работы составляет около секунды для исходной выборки данных. При этом значение F-меры оказалось всего 0,281. EM-алгоритму для построения модели потребовалось 12 минут, однако качество кластеризации осталось примерно аналогичным кластеризации алгоритмом k-средних (F-мера 0,28). Наилучшие результаты показал алгоритм *DBSCAN*. Построение модели заняло всего 25,15 секунд. Из всей выборки только 3 точки не были определены в свой класс, а были помечены как шумовые элементы. В результате точность кластеризации оказалась равной 100%, а полнота 99,95%.

Таким образом, наиболее эффективным методом кластеризации сетевого трафика мобильных приложений является алгоритм *DBSCAN*. Именно его целесообразно использовать при фильтрации трафика нежелательных мобильных приложений.

Литература

1. *Шелухин О.И., Ерохин С.Д., Ванюшина А.В*. Классификация IP-трафика методами машинного обучения. Горячая линия – телеком, 2018, 276 с.
2. *Шелухин О.И., Неклесова М. Д.* Автоматическая классификация вредоносных и нежелательных мобильных приложений сетевого трафика методами машинного обучения. Сб. трудов XII Международной отраслевой научно-технической конференции «Технологии информационного общества» г. Москва, МТУСИ. 14-15 марта 2018. В 2-х томах. Том.2. М.: ИД «Медиа Паблишер», 2018. – С. 24-26.
3. *Sholom M.W.* Text minig. Predictive methods of analyzing unstructured information. M. W. *Sholom, N.Indurkhya, T.Zhang, F.J.Damarau*. — 2004. — 236
4. *Sugato B.* Semi-supervised Clustering: Probabilistic Models, Algorithms and Experiments || URL: http://www.cs.utexas.edu/users/sugato/papers/sugatophdthesis.pdf
5. Критерии точности и полноты «Precision and Recall» || URL: http://mlwiki.org/index.php/Precision_and_Recall
6. *Шелухин О.И., Панкрушин А.П.* Оценка достоверности обнаружения аномалий сетевого трафика методами дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 110-115.
7. *Шелухин О.И., Филинова А.С.* Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 116-119.
8. *Шелухин О.И., Симонян А.Г., Ванюшина А.В.* Влияние структуры обучающей выборки на эффективность классификации приложений трафика методами машинного обучения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 2. С. 25-31.
9. *Шелухин О.И., Антонян А.А.* Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 6. С. 61-64.
10. *Шелухин О.И., Савелов А.В.* Имитационное моделирование аномалий трафика в локальной компьютерной сети // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 10. С. 103-109.
11. *Шелухин О.И., Филинова А.С.* Сравнительный анализ алгоритмов обнаружения аномалий трафика методами дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 9. С. 89-97.
12. *Шелухин О.И., Симонян А.Г., Ванюшина А.В.* Формирование исходных данных и анализ программного обеспечения для классификации приложений трафика методом машинного обучения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 1. С. 67-72.
13. *Костин Д.В., Шелухин О.И.* Сравнительный анализ алгоритмов машинного обучения для проведения классификации сетевого зашифрованного трафика // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 9. С. 43-52.
14. *Шелухин О.И., Чернышев А.И.* Исследование и моделирование нейросетевых алгоритмов обнаружения аномальных вторжений в компьютерные сети // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 12. С. 102-106.

15. *Шелухин О.И., Судариков Р.А.* Анализ информативных признаков в задачах обнаружения аномалий трафика статистическими методами // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 3. С. 14-18.
16. *Sheluhin O.I., Pankrushin A.V.* Detection of anomalies in network traffic using the methods of fractal analysis in real time // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 8. С. 108-112.
17. *Sheluhin O.I., Sirukhi J.W., Pankrushin A.V.* Wavelet type selection in the problem of anomaly intrusions detection in computer networks using multifractal analysis methods // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 4. С. 88-92.
18. *Шелухин О.И., Панкрушин А.В.* Сравнительный анализ характеристик обнаружения аномалий трафика методами кратномасштабного анализа // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 6. С. 65-70.
19. *Шелухин О.И., Филинова А.С., Васина А.В.* Обнаружение аномальных вторжений в компьютерные сети статистическими методами // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 10. С. 42-49.
20. *Шелухин О.И., Филинова А.С.* Обнаружение сетевых аномальных выбросов трафика методом разладки // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2013. № 1. С. 245-248.

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF ALGORITHMS FOR CLUSTERING NON-DESIRABLE MOBILE APPLICATIONS BY MACHINE-TRAINING METHODS

Oleg I. Sheluhin
Professor, Doctor of Technical Sciences, Head of the Information Security Department, MTUCI, Moscow, Russia,
sheluhin@mail.ru;
Marina D. Neklesova
Master student of the department "Information Security", a student of group M111701 (73), MTUCI, Moscow, Russia,
neklesova_marisha@mail.ru

Key words: *k-means method, EM-algorithm, clustering algorithms, machine learning, applications, DBSCAN, Precision, Recall, F-measure.*

The article is devoted to the review of clustering algorithms for mobile network traffic in order to filter traffic of unwanted applications, as well as their comparative analysis. For clustering, the traffic of such programs for mobile platforms such as Facebook, Google Chrome, Instagram, Messenger and WhatsApp is used. This selection is based on the worldwide popularity of these applications. Clustering is performed using the *WEKA* software, which provides software implementation of the studied methods. Such clustering algorithms are considered as the k-means method, EM-algorithm and *DBSCAN*. For a comparative analysis, the characteristics of Precision, Recall and F-measure are used. With their help, conclusions are made about the quality of the work of each algorithm. It is shown that the most effective method for clustering network traffic of mobile applications is the *DBSCAN* algorithm. That it is advisable to use when filtering traffic unwanted mobile applications.

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ДЛЯ РЕГУЛИРОВАНИЯ УГЛА КРЕНА КВАДРОКОПТЕРА С ПОМОЩЬЮ ПИД-РЕГУЛЯТОРА

Белов Никита Вадимович
студент группы М151701 МТУСИ
djnikone2777@yandex.ru
Буянов Борис Яковлевич
МТУСИ, к.т.н., с.н.с., доцент
b.buyanov@gmail.com

Ключевые слова: *квадрокоптер, ПИД-регуляторы, имитационная модель, стабилизация, JavaScript, автопилот.*

Разработана и исследована имитационная модель регулирования угла крена квадрокоптера на основе ПИД-регулятора. Модель отражает в 2-D один из углов наклона квадрокоптера. Рассмотрено несколько методов расчета коэффициентов ПИД-регуляторов и произведен выбор оптимального для решения поставленной задачи.

Системы автопилота обычно состоят из «внутреннего цикла», обеспечивающего стабильность и контроль, а также из «внешнего цикла» отвечающего за цели на уровне миссии, например, навигации по точкам. Системы автопилота для беспилотного летательного аппарата (БПЛА) преимущественно реализуются с использованием системы управления с пропорциональными, интегральными и дифференциальными регуляторами, которые продемонстрировали точность в стабильных условиях.

Автопилот представляет собой систему регуляторов для управления углами поворотов и координатами центра масс.

Большинство автопилотов разбито на несколько простых автоматов, которые контролируют только свой процесс, такие как курс, скорость, высота и т.д.

Автопилот на БПЛА состоит из ряда подобных по принципу действия автоматов (курса, продольно-поперечных кренов, скорости, высоты и др.), совместная работа которых управляет полётом и стабилизует его (рис.1). Чувствительные элемент каждого автомата измеряет один, определённый для него параметр режима полёта (например, или высоту, или курс), называется параметром регулирования, и вырабатывает сигнал, пропорциональный текущему значению параметра. Задатчик режимов полёта вырабатывает сигналы, каждый из которых соответствует требуемому значению определенного параметра регулирования. Эти сигналы сравниваются в вычислительном устройстве. Их разность (рассогласование) после усиления поступает на рулевую машинку автопилота, отклоняющую соответствующий руль самолёта или орган управления двигателем. Так происходит изменение режима полёта. Когда этот режим достигает заданного, сигнал рассогласования исчезает, рулевая машинка прекращает движение и наступает положение равновесия. Устойчивость систем автоматического управления летательными аппаратами достигается как регулированием по производным от регулируемых параметров, так и отрицательной обратной связью соответствующих видов [1].

Рис. 1. Функциональная схема регулирования управления

Главной функцией отрицательной обратной связи является обеспечивание устойчивости и отсутствия колебательности в переходном процессе. Формула закона регулирования, представлена ниже:

$$\delta_{e,r,a} = k_{e,r,a} * \Delta v, \quad (1)$$

где δ_e– угол отклонения по тангажу, δ_r - угол отклонения по рысканию, δ_a - угол отклонения по крену, k_e– передаточное число автопилота по тангажу, k_r-передаточное число автопилота по рысканию, k_r-передаточное число автопилота крену, Δv – угол отклонения от заданного значения БПЛА по тангажу, рысканию и крену соответственно.

В автопилоте следуют учитывать скорость изменения угла $\frac{d\Delta v}{dt}$, так как при резком отклонении должна оставаться плавной стабилизация. Уравнение стабилизации имеет следующий вид:

$$\delta_{e,r,a} = k_{e,r,a} * \Delta v + k'_{e,r,a} \frac{d\Delta v}{dt}, \quad (2)$$

где $k_{e,r,a}$, – передаточные числа автопилота по углам тангажа, рыскания и крена, $k'_{e,r,a}$ – передаточные числа автопилота по угловой скорости по тангажу, рысканию и крену.

На рис.2 представлена схема регулятора с обратной связью.

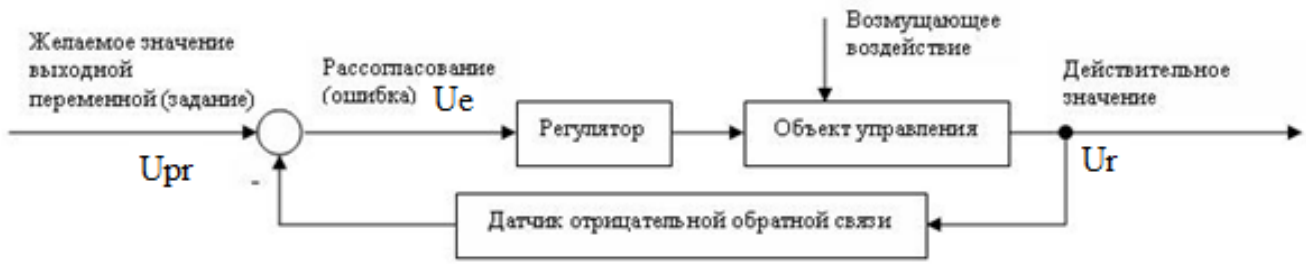


Рис.2. Схема автоматического регулирования с обратной связью

Блок ПИД (пропорционально-интегрально-дифференциальный) регулятора вычисляет "ошибку" значения Ue, как разность между текущем значением процесса Ur и целевым заданным значением Upr.

ПИД-регулятор широко используется в управлении с обратной связью промышленных процессов.

Расчет ПИД-регулятора (алгоритм) из расчетов трёх отдельных параметров: пропорционального - Kp; интегрального – Ki и дифференциального - Kd коэффициентов. Kp определяет реакцию на текущую ошибку, Ki определяет реакцию, основываясь на сумме последних ошибок и Kd определяет реакцию на скорость, с которой меняется ошибка.

$$U_{кон}(t) = U_p(t) + U_i(t) + U_d(t)$$

$$U_{кон}(t) = K_p U_e(t) + K_i \int_0^t U_e(t)dt + K_d\left(\frac{dU_e(t)}{dt}\right)$$

Частный случай ПИД регуляторов, когда отсутствует один или несколько из компонентов: пропорциональный, интегральный или дифференциальный, такие регуляторы называют И-, П-, ПД-, ПИ-регуляторами.

Дифференциальная составляющая $K_d\left(\frac{dU_e(t)}{dt}\right)$ позволяет повысить быстродействие регулятора, предсказывая будущее поведение процесса [2].

Интегральная составляющая $K_i \int_0^t U_e(t)dt$ призвана ликвидировать статические ошибки управления, поскольку интеграл даже от малой ошибки может быть значительной величиной, вызывающей реакцию регулятора [2].

Методики расчета коэффициентов ПИД – регулятора

Расчет коэффициентов ПИД регуляторов можно осуществить несколькими методами:

- Метод Циглера-Николса
- Метод биноминального распределения (Ньютона) корней
- Метод настройки AMIGO
- Метод настройки А.П. Копеловича

Рассмотрим каждый из методов более подробно

Метод Циглера-Николса:

Чтобы подобрать коэффициенты ПИД регулятора методом Циглера-Николса следует проделать следующие шаги:

a) Коэффициент передачи $k_п$ увеличивается до тех пор, пока система не выйдет на границу устойчивости

b) Значение $k_п$ фиксируется и обозначается $k_п^*$, измеряется период установившихся автоколебаний T^*.

c) Значения коэффициентов ПИД-регулятора, для метода Циглера-Николса, приведены в таблице 1:

Таблица 1

Значения ПИД-регуляторов для метода Циглера-Николса

Параметры типовых регуляторов

	$k_п$	$k_и$	$k_д$
П-регулятор	$0,50k_п^*$		
ПИ-регулятор	$0,45k_п^*$	$0,54k_п^*/T^*$	
ПИД-регулятор	$0,60k_п^*$	$1,2k_п^*/T^*$	$0,075k_п^*T^*$

Метод биноминального распределения (Ньютона) корней [3]:

Когда необходимо обеспечить сокращение время переходного процесса используют метод биномиального распределения корней. Стандартное биномиальное характеристическое уравнение имеет вид:

$$D(p) = (p + \Omega_0)^n = 0, \quad (3)$$

где Ω_0 – начальное время переходного процесса без регулирования; n - действительные и отрицательные корни характеристических уравнений; p – оператор Лапласа.

Характеристические уравнения выбираются из таблицы 2.

Таблица 2

Характеристические уравнения, зависящие от порядка системы:

Порядок системы	Время регулирования, tp	Характеристическое уравнение
1	3/ Ω0	D(p) = p + Ω0
2	4,5/ Ω0	D(p) = p2 + 2Ω0 p + Ω02
3	6/ Ω0	D(p) = p3 + 3Ω0 p2 + 3Ω02 p + Ω03
4	7,6/ Ω0	D(p) = p4 + 4Ω0 p3 + 6Ω02 p2 + 4Ω03 p + Ω04

Переходные процессы для уравнений из таблицы 2 принимают вид, как на рисунке 3:

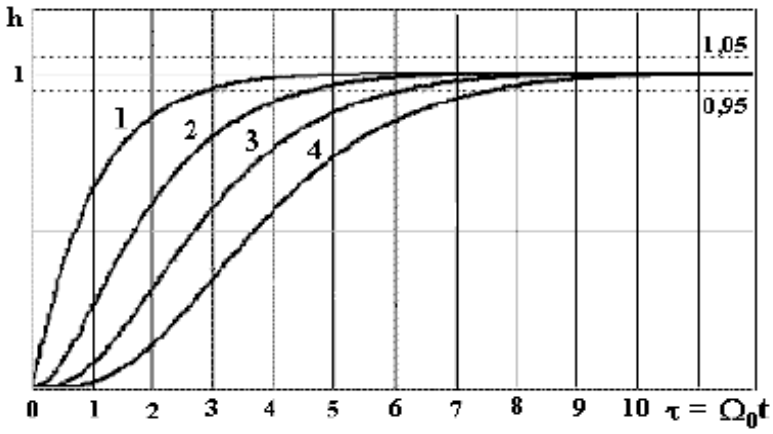


Рис. 3. Переходные процессы для характеристических уравнений с порядками системы от 1 до 4

Для расчета коэффициентов ПИД-регулятору по методу биномиального распределения корней, необходимо выполнить следующие шаги:

a) Определяем время переходного процесса $t_п$

b) По графикам на рисунке 3 определяем переходный процесс, удовлетворяющий нашей системе. По таблице 2 определяем характеристическое уравнение и время регулирования. В нашем случае подходит система третьего порядка $D(p) = p^3 + 2\Omega p^2 + 2\Omega^2 + \Omega^3$. Время регулирования для системы третьего порядка равно $\frac{6}{\Omega_0}$.

c) Производим преобразование Лапласа с выбранным уравнением.

Так же существуют такие методы настройки ПИД регуляторов, как AMIGO и метод настройки А.П. Копеловича.

Алгоритмы рассчитанные по методу AMIGO обладают более высокими показателеми быстродействия и малым временем регулирования по сравнению с остальными методами настройками.

Алгоритмы рассчитанные по методу А.П. Копеловича имеют низкое быстродействие и не имеют перерегулирования. Его можно использовать для тех типов процессов, к которым не предъявляют жестких требований по быстродействию [1].

Значения показателей качества регулирования приведены в таблице 3.

Таблица 3

Значения показателей качества регулирования.

Рассчитанные значения показателей качества регулирования

Метод	время нарастания, $t_н$, с	быстродействие, $t_{уст}$, с	перерегулирование, %	интегральный квадратичный критерий качества
AMIGO	19,3	40	4	8,67
Копеловича	200	92	0	8,06
Зиглер–Никольса	14,2	28	15	13,52

Реакция системы на единичное воздействие показано на рисунке 4.

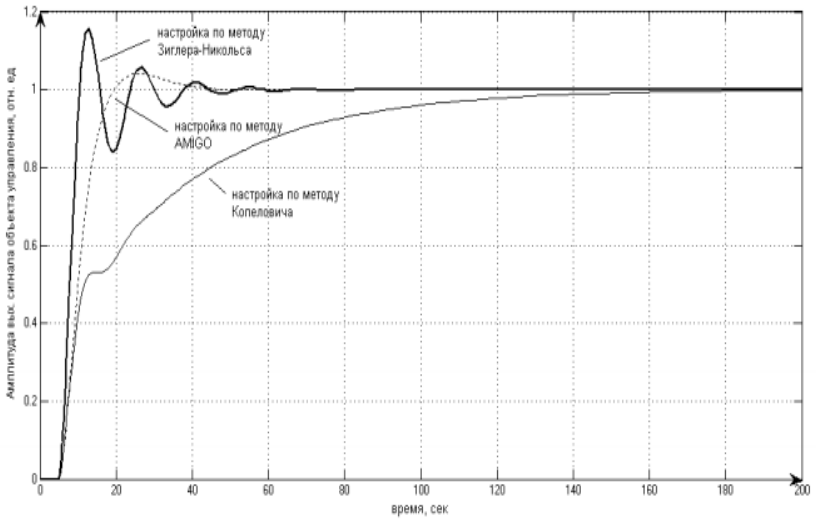


Рис. 4. Реакция системы на единичное ступенчатое воздействие

Далее мы будем рассматривать только метод Циглера-Николса и метод биномиального распределения корней, т.к. они имеют наименьшее время перерегулирования и чаще всего используются при проектировании управлении летательным аппаратом.

На рисунке 5-7 изображены графики переходного процесса с разными коэффициентами.

На рисунке 5 график с коэффициентами $K_p = 1, K_i = 1, K_d = 1$.

На рисунке 6 график с коэффициентами подобранными методом Циглера-Николса $K_p = 0.85, K_i = 0.055, K_d = 0.1375$

На рисунке 7 график переходного процесса с коэффициентами рассчитанными методом биномиального распределения корней $K_p = 0.2, K_i = 0.005, K_d = 0.1$.

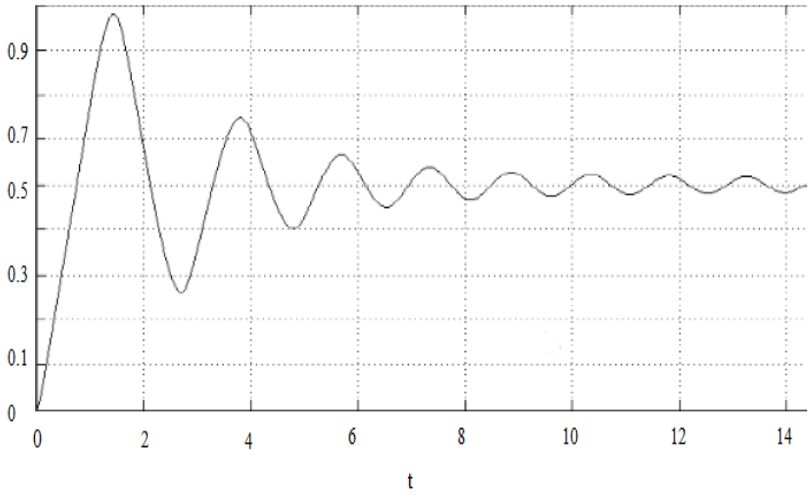


Рис. 5. График переходного процесса с коэффициентами $K_p = 1, K_i = 1, K_d = 1$

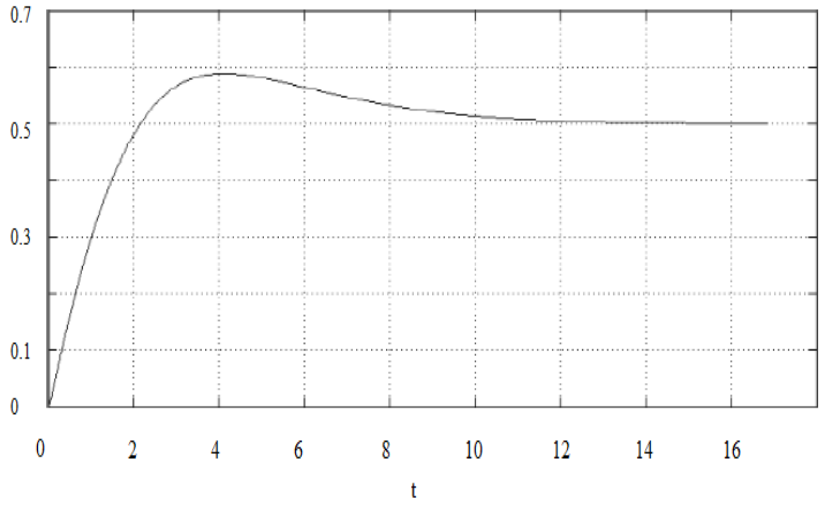


Рис. 6. График переходного процесса, с коэффициентами подобранными методом Циглера-Николса $K_p = 0.85, K_i = 0.055, K_d = 0.1375$

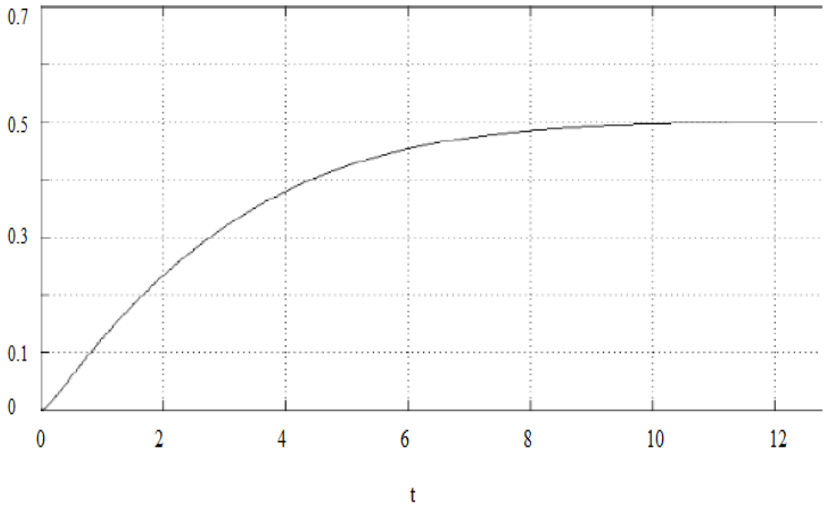


Рис. 7. График переходного процесса с коэффициентами рассчитанными методом биномиального распределения корней $K_p = 0.2, K_i = 0.005, K_d = 0.1$.

Параметры всех методов сведены в таблицу 4.

Таблица 4

Параметры переходного процесса, рассчитанные 3 разными способами.

Единичные коэффициенты	K_p, K_i, K_d	1,1,1	tп, с	28	Δt,	0.0342	б (%)	82
Метод Циглера-Николса	K_p, K_i, K_d	0.85,0.055,0.1375	tп, с	19	Δt,	0.0072	б (%)	9
Метод биномиального распределения корней	K_p, K_i, K_d	0.2,0.005,0.1	tп, с	14	Δt,	0.00041	б (%)	0

По приведенным графикам можно сделать следующие выводы:

При коэффициентах, подобранных вручную, система обладает большим значением перерегулирования и временем переходного процесса, что может сильно сказаться на процессе пилотирования.

В методе Циглера-Николса получен переходный процесс с малой ошибкой и перерегулированием, лежащим в допустимых параметрах, но большим временем схождения.

С помощью метода биномиального распределения корней удалось улучшить качество переходного процесса, который теперь занимает 14 секунд, в котором практически отсутствует перерегулирование и который содержит минимальную ошибку, что удовлетворяет всем требованиям автопилотирования квадрокоптера.

После расчета характеристик ПИД-регулятора проведено имитационное моделирование для стабилизации квадрокоптера по крену. Для этого написана JavaScript-страничка с виртуальным квадрокоптером представленная на рисунке 8. На этом рисунке видно, что можно изменять все три параметра ПИД-регулятора (пропорциональный, интегральный и дифференциальный), а так же интервал регулирования. При ручной настройки подобного регулятора можно потратить много времени и не прейти к удовлетворяющим значениям, поэтому коэффициенты были подобраны разными методами и выбран оптимальный.

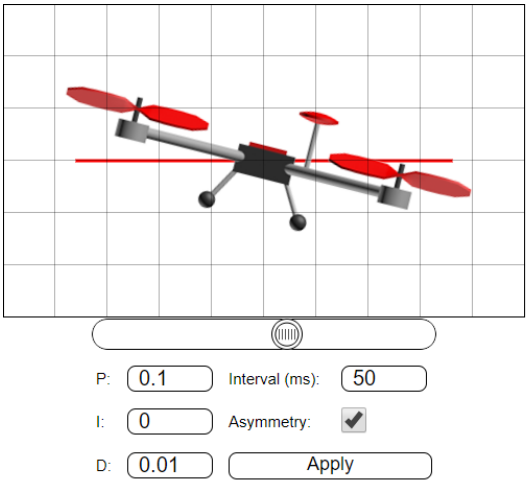


Рис. 8. Имитационная модель

Выводы

При ручной настройки ПИД-регуляторов очень сложно подобрать идеальные параметры регулирования, поэтому в данной работе рассмотрены различные методы подбора коэффициентов. Метод биномиального распределения корней Ньютона в данном случае оптимален, т.к. обеспечивает минимальное время переходного процесса и сводит ошибку перерегулирования к 0, что особо актуально для ЛА.

В данной работе построен ПИД-регулятор для одного из углов квадрокоптера, а именно угла крена, но в реальной модели таких угла три: крен, тангаж, рысканье из чего следует, что на реальном квадрокоптере применяется три ПИД-регулятора.

Построенная имитационная модель позволяет визуально оценить колебания ЛА в пространстве, что существенно сокращает время и затраты на настройку ПИД-регулятора.

Литература

1. *Боднер В. А.*, Теория автоматического управления полётом, М., 1964.
2. *Бураков М.В., Полякова Т.Г., Подзорова А.В.* «Теория автоматического управления: методические указания к выполнению лабораторных работ», 2006г.
3. *Воронцов Е. Ю.* «Исследование методов настройки ПИД-регулятора на примере моделирования объекта второго порядка с запаздыванием» - Екатеринбург : УрФУ, 2013. — С. 37-41.

DEVELOPMENT OF A SIMULATION MODEL FOR REGULATION OF THE ANGLE OF ROLL OF A QUADROCOPTER USING A PID CONTROLLER

Nikita V. Belov
student group M151701 MTUCI
djnikone2777@yandex.ru
Boris Y. Buyanov
MTUCI, Ph.D., senior researcher, associate professor
b.buyanov@gmail.com

Keywords: quadcopter, PID controllers, simulation model, stabilization, JavaScript, autopilot.

A simulation model of the angle of roll of a quadrocopter based on a PID controller was developed and investigated. The model reflects in two-dimensional space of the angles of inclination of the quadrocopter. Several methods for calculating the coefficients of PID controllers are considered and the choice of the optimal one for solving the set task is made.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ НЕЧЁТКОЙ ЛОГИКИ

Рогатнева Екатерина Александровна
студентка группы БП31502, МТУСИ
swamp.swift@gmail.com
Большаков Александр Сергеевич
МТУСИ, к.т.н., доцент кафедры ИБ
as.bolshakov57@mail.ru

Ключевые слова: *информационная безопасность, оценка рисков, нечёткая логика, алгоритм Мамдани, информационные активы.*

Проведено сравнение основных подходов в оценке рисков информационной безопасности. Обоснован выбор в пользу использования нечёткой логики. Рассмотрен алгоритм Мамдани, позволяющий сформировать чёткую оценку информационной безопасности на основе нечётких правил. Приведена база нечётких правил для рассматриваемой системы. Рассмотрен способ проведения оценки рисков информационной безопасности. Представлена концепция разрабатываемого программного обеспечения. Смоделированы результаты обработки пользовательского ввода.

Оценка рисков в области информационной безопасности является очень востребованным на данный момент направлением. Такая оценка позволяет понять, насколько исследуемая система доступна, как много в ней не устранённых критических уязвимостей.

Существует два подхода к оценке рисков ИБ – количественный и качественный. Так, количественный подход позволяет оценить ценность информационных активов в денежном эквиваленте, а также понять, какие издержки может понести предприятие в том случае, если кто-то из злоумышленников воспользуется не устранёнными вовремя уязвимостями. Качественный подход, в свою очередь, позволяет сделать заключение о состоянии информационной системы, а также позволяет сделать выводы об уровне риска на основании ценности информационного актива, вероятности реализации угрозы и возможности её реализации. В данном случае не говорится о реальной стоимости информационных активов.

Для того, чтобы упростить проведение аудита, сделать сам процесс более удобным для людей, которые им занимаются, было решено создать программный продукт, предназначенный для автоматизации сбора и обработки информации об информационной системе. В данном продукте предлагается использовать алгоритмы нечёткой логики, а именно – алгоритм Мамдани (Рис. 1).

Рис. 1. Демонстрация процесса обработки данных с помощью алгоритма Мамдани

Выбор в пользу нечёткой логики был сделан не случайно. Именно в этом разделе математики впервые стали использовать понятие «лингвистическая переменная» - переменная, которая может принимать значения фраз из естественного или искусственного языка [3]. Так как проведение аудита подразумевает под собой работу с людьми, а именно получение определённой экспертной оценки, необходимо было выбрать инструмент, который бы позволял переводить нечёткие значения лингвистических переменных, данных людьми, в чёткий ответ, выдаваемый программой.

В соответствии с описанием работы алгоритма Мамдани (рис.1), для корректного функционирования разрабатываемой программы необходимо составить систему из правил, составленных по схеме «ЕСЛИ …, ТО …».

Определим три лингвистические переменные: «Уровень программно-аппаратной защиты» информационного ресурса (далее – уровень ПаЗ), «Уровень организационной защиты» (далее – уровень ОргЗ), «Уровень инженерно-технической защиты» (далее – уровень ИнжЗ). Для каждой из этих переменных доступны значения «Очень низкий», «Низкий», «Средний», «Хороший», «Высокий». Затем составим набор нечётких лингвистических правил (Табл.1). При их создании используется схема «ЕСЛИ … И … И …, ТО …». «И» в данном случае – логический оператор.

Таблица 1.

Формирование базы правил

	Уровень ПаЗ	**Уровень ОргЗ**	**Уровень ИнжЗ**		**Оценка**
	Очень низкий	Очень низкий	Очень низкий		Очень низкий
	Очень низкий	Очень низкий	Низкий		Очень низкий
	Очень низкий	Очень низкий	Средний		Низкий
	Очень низкий	Очень низкий	Хороший		Низкий
	Очень низкий	Очень низкий	Высокий		Низкий
	Очень низкий	Низкий	Низкий		Низкий
	Очень низкий	Низкий	Средний		Низкий
	Очень низкий	Низкий	Хороший		Низкий
	Очень низкий	Низкий	Высокий		Средний
	Очень низкий	Средний	Средний		Низкий
	Очень низкий	Средний	Хороший		Средний
	Очень низкий	Средний	Высокий		Средний
	Очень низкий	Хороший	Хороший		Средний
	Очень низкий	Хороший	Высокий		Средний
Если…	Очень низкий	Высокий	Высокий	**То**	Хороший
	Низкий	Низкий	Низкий		Низкий
	Низкий	Низкий	Средний		Низкий
	Низкий	Низкий	Хороший		Средний
	Низкий	Низкий	Высокий		Средний
	Низкий	Средний	Средний		Средний
	Низкий	Средний	Хороший		Средний
	Низкий	Средний	Высокий		Средний
	Низкий	Хороший	Хороший		Средний
	Низкий	Хороший	Высокий		Хороший
	Низкий	Высокий	Высокий		Хороший
	Средний	Средний	Средний		Средний
	Средний	Средний	Хороший		Средний
	Средний	Средний	Высокий		Хороший
	Средний	Хороший	Хороший		Хороший
	Средний	Хороший	Высокий		Хороший
	Средний	Высокий	Высокий		Хороший

	Хороший	Хороший	Хороший		Хороший
	Хороший	Хороший	Высокий		Хороший
	Хороший	Высокий	Высокий		Высокий
	Высокий	Высокий	Высокий		Высокий

Затем необходимо выбрать функцию принадлежности, на основе которой будет обрабатываться вся информация, поступающая на вход программы. Наиболее популярными функциями являются:

- треугольная (Рис. 2)

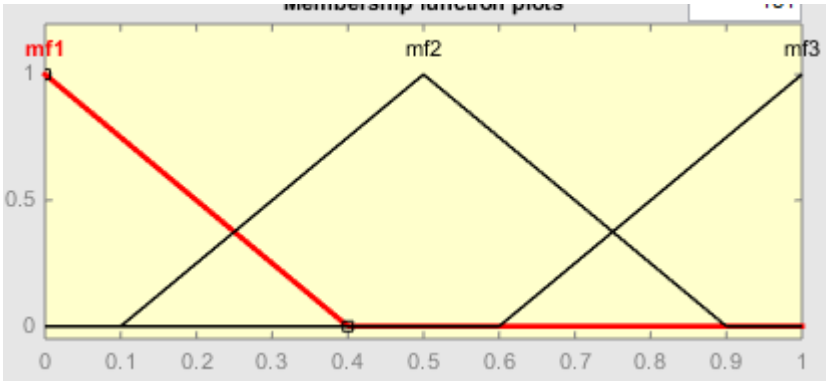


Рис. 2. Треугольная функция принадлежности

- трапециевидная (Рис. 3)

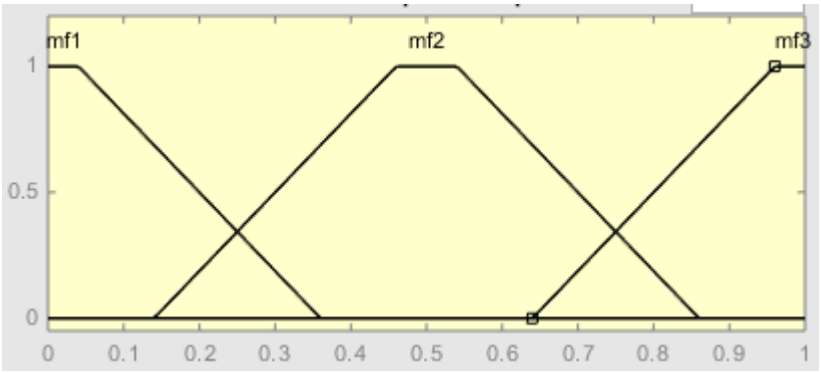


Рис. 3. Трапециевидная функция принадлежности

- квадратичный Z-сплайн (Рис. 4)

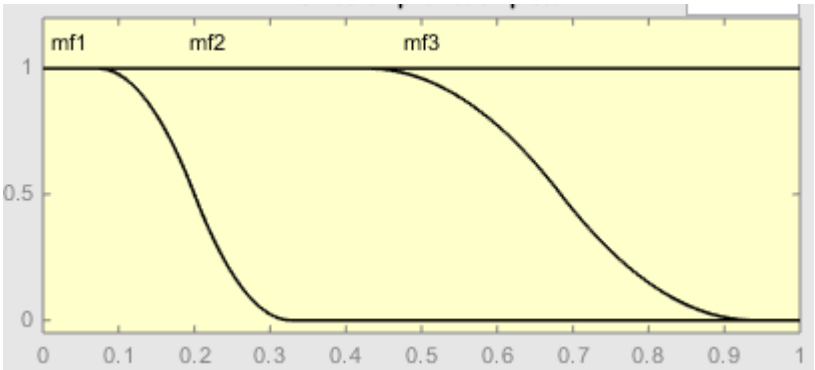


Рис. 4. Квадратичный Z-сплайн

- гармонический Z-сплайн (Рис. 5)

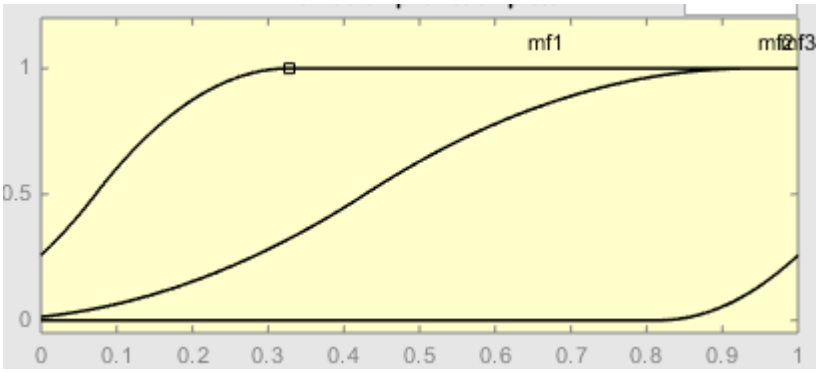


Рис. 5. Гармонический Z-сплайн

Как правило, вид функции подбирается опытным путём под требования конкретной задачи. Путём тестирования нескольких видов функций стало понятно, что оптимальной для использования в программе будет являться треугольная функция принадлежности.

Пользователю программы предлагается ответить на вопросы из опросного листа, который разделён на разделы в соответствии с определёнными выше лингвистическими переменными. Опросник разрабатывается в соответствии с требованиями [1] и [2]. Структура опросника представляет собой набор угроз для информационного ресурса предприятия и соответствующих им уязвимостей, а ответы пользователя должны содержать оценку вероятности реализации данной угрозы через предложенную уязвимость в течение года и критичность реализации угрозы, данную в процентах. Обратим внимание на то, что ответ пользователя скорее всего будет сделан на основе его личного опыта или интуитивно, без опоры на ранее сделанные расчёты. Также в программу интегрирована возможность просчитать общий уровень угроз по ресурсу и риск по ресурсу, выраженный в денежном эквиваленте.

Предположим, что пользователь оценил уровень программно-аппаратной защиты как «Низкий», уровень организационной защиты как «Средний» и уровень инженерно-технической защиты как «Хороший». В таком случае система «скажет», что уровень безопасности на предприятии «Средний» (Рис. 6)

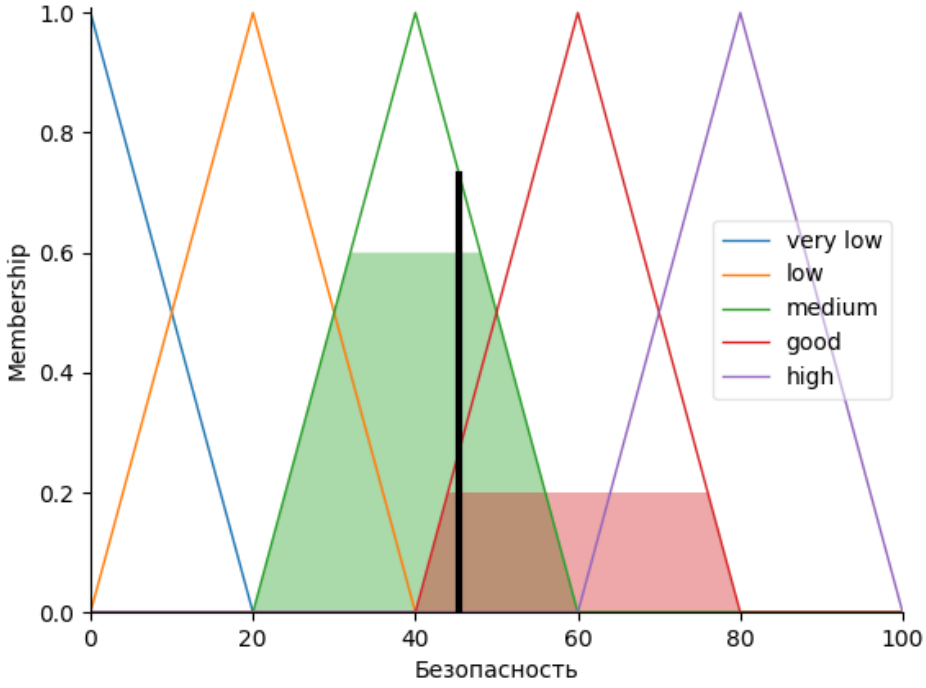


Рис. 6. Решение, выданное программным продуктом

Также существует возможность смоделировать трёхмерную поверхность оценки информационных рисков, которая отображает зависимость уровня безопасности информационного ресурса предприятии от значений различных входных данных (Рис. 7)

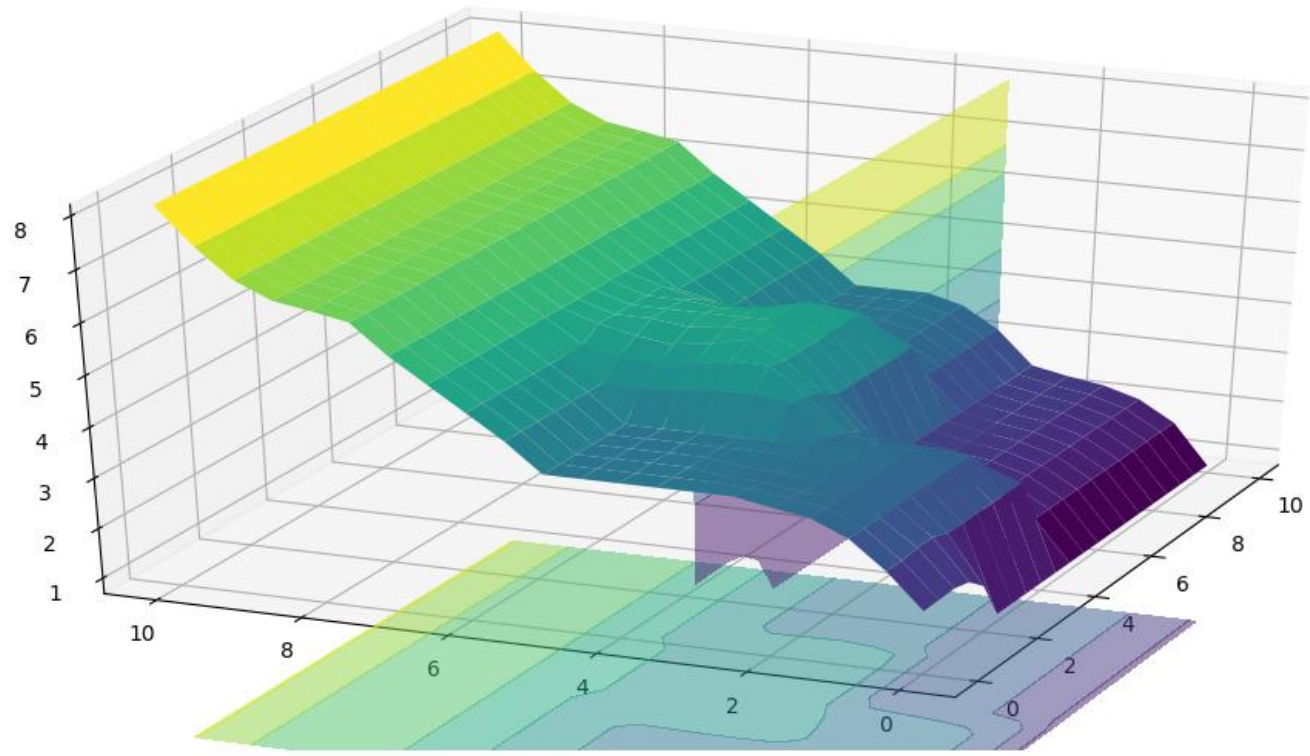


Рис. 7. Смоделированная трёхмерная поверхность уровней безопасности информационного ресурса

Здесь по осям X, Y могут располагаться соответственно оценки уровня программно-аппаратной защиты, организационной защиты и инженерно-технической защиты информации на предприятии. Смоделированная трехмерная поверхность уровней защиты информационного ресурса наглядно отображает эффективные области значений применения различных способов защиты информации для обеспечения требуемого уровня безопасности информационного ресурса.

Заключение

Таким образом, представленные результаты работы, позволяют идентифицировать взаимодействие угроз, уязвимостей и соответствующих активов, необходимые для анализа информационных рисков. Программа помогает сформировать простой и наглядный отчет об анализе рисков, основной целью которого будет презентация собранной информации о значимости и структуре рисков ИБ в организации. Алгоритмы нечёткой логики позволяют классифицировать и агрегировать риски для конкретных бизнес-процессов. Классификация рисков является инструментом для ранжирования их по вероятности возникновения и по значимости наносимого ущерба в случае возникновения инцидентов.

Отчёт позволит отразить следующие сведения:

- наиболее проблемные области обеспечения ИБ в организации;
- влияние угроз ИБ на общую структуру рисков организации;
- первоочередные направления деятельности отдела ИБ по повышению эффективности обеспечения ИБ.

Литература

1. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности М.: Стандартинформ, 2011.– 76 с.

2. ГОСТ Р ИСО/МЭК 27001-2005 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности М.: Стандартинформ, 2008.– 31 с
3. Нечёткие множества и нейронные сети: Учебное пособие /Г.Э. Яхъева. – М.: Интернет-Университет Информационных технологий; БИНОМ, Лаборатория знаний, 2006. – 316 с.

RISK ASSESSMENT OF INFORMATION SECURITY USING FUZZY LOGIC ALGORITHMS

Ekaterina A. Rogatneva
Student of group BPZ1502, MTUCI
swamp.swift@gmail.com
Alexander S. Bolshakov
MTUCI, PhD., associate professor of IS department
as.bolshakov57@mail.ru

Keywords*: information security, risk assessment, fuzzy logic, the Mamdani algorithm, information assets.*

The comparison of the main approaches in the assessment of information security risks is carried out. The choice in favor of the use of fuzzy logic is justified. The Mamdani algorithm allowing to form a clear assessment of information security on the basis of fuzzy rules is considered. The base of fuzzy rules for the considered system is given. The approach of information security risk assessment is considered. The concept of the developed software is presented. The results of user input processing are simulated.