ISSN 1818-0442
DOI: 10.21293/1818-0442

ДОКЛАДЫ

Томского государственного университета систем управления и радиоэлектроники

2018 • Том 21, № 2

Доклады ТУСУР. 2018 • Том 21, № 2

9 771818 044708 02007

Министерство образования и науки Российской Федерации

ДОКЛАДЫ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

2018, том 21, № 2

Периодический научный журнал

Выходит 4 раза в год
Основан в 1997 г.

ISSN 1818-0442
DOI: 10.21293/1818-0442

Адрес редакции: 634050, г. Томск, пр. Ленина, 40, ТУСУР, тел. (382-2) 51-22-43

Свидетельство о регистрации МНС РФ № 1027000867068 от 13 октября 2004 г.
Подписной индекс 20648 в каталоге Агентства «Роспечать»: газеты и журналы.

Издательство Томского государственного университета систем управления и радиоэлектроники
634050, Томск, пр. Ленина, 40, тел. (382-2) 51-21-21.

Верстка, техническое редактирование, подготовка оригинал-макета – В.М. Бочкаревой.
Корректор – В.Г. Лихачева.

Подписано в печать 25.06.2018.
Формат 60×84 1/8. Усл. печ. л. 10,3. Тираж 500. Заказ 18.

Содержание

ЭЛЕКТРОНИКА, ИЗМЕРИТЕЛЬНАЯ ТЕХНИКА, РАДИОТЕХНИКА И СВЯЗЬ

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

ЭЛЕКТРОТЕХНИКА

Editorial board

Contents

ELECTRONICS, MEASUREMENT TECHNOLOGY, RADIO ENGINEERING AND COMMUNICATIONS

CONTROL, COMPUTER SCIENCE, AND INFORMATICS

ELECTRICAL ENGINEERING

ЭЛЕКТРОНИКА,
ИЗМЕРИТЕЛЬНАЯ ТЕХНИКА,
РАДИОТЕХНИКА И СВЯЗЬ

УДК 629.7.052

В.Л. Гулько, А.А. Мещеряков

Использование ортогонально эллиптически поляризованных сигналов в бортовых СВЧ двухканальных радиомаячных системах навигации

Исследуется возможность определения пеленга и угла крена подвижного объекта по ортогонально эллиптически поляризованным сигналам радиомаяка, излучаемым одновременно из двух пространственно разнесенных точек с известными координатами. Пеленг и крен определяются на борту подвижного объекта СВЧ двухканальной приемной системой на основе амплитудно-фазовой обработки результирующих векторных сигналов, принятых в линейном поляризационном базисе.

Ключевые слова: радиомаяк, ортогонально эллиптически поляризованные сигналы, амплитудно-фазовая обработка, линейный поляризационный базис, пеленг, крен, подвижный объект.
doi: 10.21293/1818-0442-2018-21-2-7-11

Используемые на практике радиомаячные системы навигации (РМС) для получения информации о пеленге подвижного объекта (ПО) традиционно используют амплитудные, частотные или временные характеристики принимаемых на борту ПО сигналов радиомаяка [1–3], а для измерения крена используются дорогостоящие автономные инерциальные средства навигации [4–6]. Поляризационные же характеристики сигналов радиомаяка как «носителя» навигационной информации практически не используются [7–9]. В работах [10–13] для оценки пеленга и крена ПО исследовались частные случаи использования ортогонально-линейных [10, 11] или ортогонально круговых [12, 13] сигналов радиомаяка. Пеленг и крен ПО оценивались на выходе СВЧ двухканальной приемной системы по результатам амплитудно-фазовой обработки результирующих векторных сигналов, принятых в линейном [10] или круговом [11, 13] поляризационных базисах. Выбор поляризационных базисов, в которых представляются излучаемые и принимаемые на борту ПО результирующие векторные сигналы, определяется физическим смыслом решаемой технической задачи.

Постановка задачи

Цель данной работы – исследовать наиболее общий случай использования ортогонально эллиптически поляризованных сигналов радиомаяка для оценки пеленга и угла крена ПО.

Поляризационный метод определения пеленга и угла крена ПО

Предположим, что радиомаяк одновременно излучает из двух пространственно разнесенных в горизонтальной плоскости на расстоянии d точек ортогонально эллиптические поляризованные электромагнитные волны с равными амплитудами, начальными фазами, длинами волн и равными углами эллиптичности. Используем представление плоской однородной эллиптически поляризованной электромагнитной волны вектором Джонса [14, 15]. Тогда результирующая волна на направлении α может быть представлена в линейном поляризационном базисе (ЛПБ) в векторной форме (опуская временную зависимость) в виде

$$\mathbf{E_P} = \frac{1}{\sqrt{2}}\left\{\begin{bmatrix}\cos\varepsilon\\ j\sin\varepsilon\end{bmatrix} + \begin{bmatrix}j\sin\varepsilon\\ \cos\varepsilon\end{bmatrix}\cdot e^{j\Delta\varphi}\right\}, \qquad (1)$$

где $\Delta\varphi = \frac{2\pi d}{\lambda}\sin\alpha$ – разность фаз между ортогонально эллиптически поляризованными волнами в точке приема на ПО; λ – длина волны; ε – угол эллиптичности излучаемых ортогонально поляризованных электромагнитных волн.

Из (1) следует, что пеленг α, определяемый как угол между перпендикуляром к середине базы d и направлением на ПО, может быть найден как

$$\alpha = \arcsin\frac{\lambda}{2\pi d}\cdot(\Delta\varphi). \qquad (2)$$

Наличие множителя $1/\sqrt{2}$ в выражении (1) объясняется принятой для удобства единичной интенсивностью результирующей волны $\mathbf{E}_\text{р}$.

Предположим, что ПО имеет в общем случае крен γ, определяемый как угол между правой поперечной осью ПО и горизонтальной плоскостью [1]. Предположим также, что прием результирующей волны (1) на борту ПО осуществляется приемной антенной в ЛПБ и в её СВЧ-тракт установлен линейный поляризационный разделитель (ЛПР), орты собственной системы координат которого совпадают с вертикальной и поперечной строительными осями ПО. Выбранная ориентация ортов ЛПР позволяет в ЛПБ разделить принятую результирующую волну (1) на две ортогонально линейно поляризованные составляющие $\mathbf{E}_1$ и $\mathbf{E}_2$ ориентированные вдоль поперечной и вертикальной строительными осями ПО соответственно.

Установим связь амплитуд A_1 и A_2, а также фаз Ψ_1 и Ψ_2 составляющих $\mathbf{E}_1$ и $\mathbf{E}_2$ на выходах ЛПР с пеленгом α и углом крена γ ПО.

Для описания взаимодействия результирующей волны (1) с элементами СВЧ-тракта приемной антенны воспользуемся известным формализмом векторов и матриц Джонса [14]. Тогда составляющие $\mathbf{E}_1$ и $\mathbf{E}_2$ на выходах ЛПР (опуская временную зависимость) в ЛПБ в векторной форме можно найти с помощью преобразований вида

$$\mathbf{E}_1 = [\Pi_1][R(\pm\gamma)]\mathbf{E}_\text{p}; \quad (3)$$

$$\mathbf{E}_2 = [\Pi_2][R(\pm\gamma)]\mathbf{E}_\text{p}, \quad (4)$$

где $[R(\pm\gamma)] = \begin{bmatrix} \cos\gamma & \mp\sin\gamma \\ \pm\sin\gamma & \cos\gamma \end{bmatrix}$ – оператор поворота на угол крена $\pm\gamma$; $+\gamma$ – правая поперечная ось ПО ниже горизонтальной плоскости; $-\gamma$ – правая поперечная ось ПО выше горизонтальной плоскости; $[\Pi_1] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ – оператор Джонса первого плеча ЛПР (переход с круглого волновода на прямоугольный с горизонтальной собственной поляризацией, совпадающей с правой поперечной осью ПО), записанный в собственной системе координат; $[\Pi_2] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ – оператор Джонса второго плеча ЛПР (переход с круглого волновода на прямоугольный с вертикальной собственной поляризацией, совпадающей с вертикальной осью ПО), записанный в собственной системе координат.

Проделав в (3) и (4) необходимые вычисления, получим векторы Джонса $\mathbf{E}_1$ и $\mathbf{E}_2$ на выходах ЛПР для углов крена $\pm\gamma$ в виде

$$\mathbf{E}_1(\pm\gamma) = \frac{1}{\sqrt{2}}\left\{\begin{bmatrix} A(\pm\gamma) + jB(\pm\gamma) \\ 0 \end{bmatrix}\right\}; \quad (5)$$

$$\mathbf{E}_2(\pm\gamma) = \frac{1}{\sqrt{2}}\left\{\begin{bmatrix} 0 \\ C(\pm\gamma) + jD(\pm\gamma) \end{bmatrix}\right\}, \quad (6)$$

где

$$A(\pm\gamma) = \cos\gamma\cos\varepsilon - \sin\varepsilon\cos\gamma\sin\Delta\varphi \mp \mp\sin\gamma\cos\varepsilon\cos\Delta\varphi; \quad (7)$$

$$B(\pm\gamma) = \sin\varepsilon\cos\gamma\cos\Delta\varphi \mp \sin\gamma\sin\varepsilon \mp \mp\sin\gamma\cos\varepsilon\sin\Delta\varphi; \quad (8)$$

$$C(\pm\gamma) = \pm\sin\gamma\cos\varepsilon + \cos\gamma\cos\varepsilon\cos\Delta\varphi \mp \mp\sin\varepsilon\sin\gamma\sin\Delta\varphi; \quad (9)$$

$$D(\pm\gamma) = \cos\gamma\sin\varepsilon \pm \sin\varepsilon\sin\gamma\cos\Delta\varphi + +\cos\gamma\cos\varepsilon\sin\Delta\varphi. \quad (10)$$

С учетом (5)–(10) сигналы на входах двухканального приемника будут иметь вид

$$\dot{E}_1(\pm\gamma) = \frac{1}{\sqrt{2}}\{A(\pm\gamma) + jB(\pm\gamma)\}; \quad (11)$$

$$\dot{E}_2(\pm\gamma) = \frac{1}{\sqrt{2}}\{C(\pm\gamma) + jD(\pm\gamma)\}. \quad (12)$$

Комплексные элементы (11) и (12) представляют собой проекции в общем случае эллиптически поляризованной результирующей волны (1) на орты ЛПБ.

Найдем амплитуды A_1, A_2 и фазы Ψ_1, Ψ_2 сигналов (11) и (12) на выходах двухканального приемника, имеющего, например, линейную амплитудную характеристику и линейный детектор, и установим их связь с навигационными элементами α и γ:

$$A_1(\pm\gamma) = \frac{1}{\sqrt{2}}\sqrt{1 \mp \sin 2\gamma\cos\Delta\varphi - \sin 2\varepsilon\cos 2\gamma\sin\Delta\varphi}; \quad (13)$$

$$\Psi_1(\pm\gamma) = \operatorname{arctg}\frac{B(\pm\gamma)}{A(\pm\gamma)}; \quad (14)$$

$$A_2(\pm\gamma) = \frac{1}{\sqrt{2}}\sqrt{1 \pm \sin 2\gamma\cos\Delta\varphi + \sin 2\varepsilon\cos 2\gamma\sin\Delta\varphi}; \quad (15)$$

$$\Psi_2(\pm\gamma) = \operatorname{arctg}\frac{D(\pm\gamma)}{C(\pm\gamma)}. \quad (16)$$

Найдем отношение амплитуд A_2/A_1 и разность фаз $\Delta\Psi(\pm\gamma) = \Psi_2(\pm\gamma) - \Psi_1(\pm\gamma)$ сигналов (11) и (12) на выходе приемника для углов крена $\pm\gamma$:

$$\frac{A_2}{A_1}(\pm\gamma) = \frac{\sqrt{1 \pm \sin 2\gamma\cos\Delta\varphi + \sin 2\varepsilon\cos 2\gamma\sin\Delta\varphi}}{\sqrt{1 \mp \sin 2\gamma\cos\Delta\varphi - \sin 2\varepsilon\cos 2\gamma\sin\Delta\varphi}} \quad (17)$$

и

$$\Delta\Psi(\pm\gamma) = \operatorname{arctg}\frac{D(\pm\gamma)}{C(\pm\gamma)} - \operatorname{arctg}\frac{B(\pm\gamma)}{A(\pm\gamma)} \pm n\pi, \quad (18)$$

где $n = 0, 1, 2, \ldots$.

В (14), (16) и (18) обозначения A, B, C и D определяются соответственно выражениями (7)–(10).

Обсуждение результатов исследования

Из анализа (17) и (18) следует, что в общем случае, отношение амплитуд A_1/A_2 и разность фаз $\Delta\Psi$ составляющих $\mathbf{E}_1$ и $\mathbf{E}_2$ зависят как от угла эллиптичности ε излучаемых электромагнитных волн, так и от навигационных элементов α и γ ПО.

В частных случаях, если, например, радиомаяк излучает ортогонально линейно поляризованные волны, тогда, подставляя $\varepsilon = 0°$ в (17) и (18), с учетом (7)–(10) получим

$$\frac{A_2}{A_1}(\pm\gamma) = \frac{\sqrt{1 \pm \sin 2\gamma\cos\Delta\varphi}}{\sqrt{1 \mp \sin 2\gamma\cos\Delta\varphi}} \quad (19)$$

и

$$\Delta\Psi(\pm\gamma) = \pm\operatorname{arctg}\left\{\frac{1}{\cos 2\gamma}\operatorname{tg}\Delta\varphi\right\} \pm n\pi. \quad (20)$$

Из (19), (20) следует, что для однозначной оценки α или γ требуется априорная информация об одном из них, что полностью согласуется с результатами частных исследований, полученных в [10].

В другом частном случае, если радиомаяк излучает ортогонально поляризованные по кругу электромагнитные волны, то, подставляя $\varepsilon=\frac{\pi}{4}$ в (17) и (18), с учетом (7)–(10) получим

$$\frac{A_2}{A_1}(\pm\gamma)=\frac{\sqrt{1+\sin(\Delta\varphi\pm 2\gamma)}}{\sqrt{1-\sin(\Delta\varphi\pm 2\gamma)}} \qquad (21)$$

и

$$\Delta\Psi(\pm\gamma)=0^\circ . \qquad (22)$$

Преобразуя (21), получим

$$\frac{A_2}{A_1}(\pm\gamma)=\left|\operatorname{ctg}\left(\frac{\pi}{4}-\frac{\Delta\varphi}{2}\pm\gamma\right)\right| . \qquad (23)$$

Из анализа (22) и (23) следует, что информация о пеленге α и угле крена γ содержится в амплитудных соотношениях синфазных ортогонально линейно поляризованных составляющих $\mathbf{E}_1$ и $\mathbf{E}_2$ на выходах ЛПР и для однозначной их оценки также требуется априорная информация об одном из них.

Предположим, что приемная бортовая антенна и её СВЧ-элементы располагаются на гиростабилизированной платформе [4, 5]. Тогда подставляя в (23) $\gamma=0^\circ$, получим

$$\Delta\varphi=\pm\left(\frac{\pi}{2}-2\operatorname{arcctg}\frac{A_2}{A_1}\right)\pm n\pi . \qquad (24)$$

Подставляя (24) в (2), получим выражение для расчета пеленга α ПО в виде

$$\alpha=\pm\arcsin\left[\frac{\lambda}{\pi d}\left(\frac{\pi}{4}-\operatorname{arcctg}\frac{A_2}{A_1}\right)\right]\pm n\pi . \qquad (25)$$

Из (25) следует, что если отношение амплитуд $A_2/A_1=1$, то $\alpha=0^\circ$, если $A_2/A_1<1$, то $\alpha<0^\circ$, и если $A_2/A_1>1$, то $\alpha>0^\circ$.

В другом случае, если, например, ПО двигается вдоль равносигнального направления, совпадающего с перпендикуляром к середине баз *d*, образованной источниками излучения ортогонально поляризованных по кругу электромагнитных волн, тогда, подставляя в (23) $\Delta\varphi=0^\circ$, получим

$$\frac{A_2}{A_1}(\pm\gamma)=\left|\operatorname{ctg}(45\pm\gamma)\right| . \qquad (26)$$

Откуда следует, что крен γ ПО будет равен

$$\gamma[\text{рад}]=\pm\left(\frac{\pi}{4}-\operatorname{arcctg}\frac{A_2}{A_1}\right) . \qquad (27)$$

Из (27) следует, что если отношение амплитуд $A_2/A_1=1$, то $\gamma=0^\circ$, если $A_2/A_1<1$, то $\gamma<0^\circ$, и если $A_2/A_1>1$, то $\gamma>0^\circ$.

Заключение

По результатам исследований можно сформулировать следующие выводы:

1. Если радиомаяк излучает ортогонально эллиптически поляризованные сигналы и прием результирующих векторных сигналов на борту осуществляется в ЛПБ, то одновременно и независимо оценить пеленг и крен ПО не представляется возможным.

2. Практическое использование ортогонально эллиптически поляризованных сигналов радиомаяка в анализируемой навигационной задаче не целесообразно, так как требуется априорная информация об одном из рассматриваемых навигационных элементов.

Работа выполнена в рамках проекта по госзаданию Минобрнауки № 8.7348.2017/8.9.

Литература

1. Ярлыков М.С. Статистическая теория радионавигации. – М.: Радио и связь, 1985. – 344 с.

2. Сосновский А.А. Авиационная радионавигация: справочник / А.А. Сосновский, И.А. Хаймович, Э.А. Лутин, И.Б. Максимов. – М.: Транспорт, 1990. – 264 с.

3. Ширман Я.Д. Радиоэлектронные системы: основы построения и теория: справочник / Я.Д. Ширман, С.Т. Багдасарян, А.С. Маляренко и др. – М.: Радиотехника, 2007. – 512 с.

4. Пельпор Д.С. Гироскопические системы ориентации и стабилизации. – М.: Машиностроение, 1982. – 165 с.

5. Смирнов Е.Л. Гироскопические навигационные системы. – СПб.: Эльмор, 2004. – 400 с.

6. Алешин Б.С., Афонин А.А., Веремеенко К.К. и др. Ориентация и навигация подвижных объектов: современные информационные технологии / под ред. Б.С. Алёшина, К.К. Веремеенко, А.И. Черноморского. – М.: Физматлит, 2006. – 424 с.

7. Гусев К.Г. Поляризационная модуляция / К.Г. Гусев, А.Д. Филатов, А.П. Сополев. – М.: Сов. радио, 1974. – 288 с.

8. Богородский В.В. Поляризация рассеянного и собственного радиоизлучения земных покровов / В.В. Богородский, Д.Б. Канарейкин, А.И. Козлов. – Л.: Гидрометеоиздат, 1981. – 279 с.

9. Козлов А.И. Поляризация радиоволн. Поляризационная структура радиолокационных сигналов / А.И. Козлов, А.И. Логвин, В.А. Сарычев. – М.: Радиотехника, 2005. – 704 с.

10. Гулько В.Л. Использование ортогонально линейно поляризованных сигналов в бортовых СВЧ двухканальных радиомаячных системах навигации / В.Л. Гулько, А.А. Мещеряков // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2017. – Т. 20, № 1. – С. 14–17.

11. Гулько В.Л. Поляризационный метод определения пеленга и угла крена подвижного объекта в двухканальных радиомаячных системах навигации / В.Л. Гулько, А.А. Мещеряков // Изв. вузов. Физика. – 2017. – Т. 60, № 6. – С. 44–49.

12. Гулько В.Л. Использование ортогонально поляризационных по кругу сигналов радиомаяка для определения пеленга подвижного объекта бортовой СВЧ двухканальной приемной системой / В.Л. Гулько, А.А. Мещеряков // Сб. тр. XXIII Междунар. науч.-техн. конф. «Радиолокация, навигация, связь». – Воронеж, 2017. – Т. 3. – С. 822–826.

13. Гулько В.Л. Поляризационно-фазовый метод определения пеленга и угла крена подвижного объекта по ортогонально поляризованным по кругу сигналам радиомаяка / В.Л. Гулько, А.А.Мещеряков // Сб. тр. XXIV Междунар. науч.-техн. конф. «Радиолокация, навигация, связь». – Воронеж, 2018. – Т. 3. - С. 251–255.

14. Аззам Р.М.А. Эллипсометрия и поляризованный свет / Р.М.А. Аззам, Н. Башара. – М.: Мир, 1981. – 583 с.

15. Татаринов В.Н. Введение в современную теорию поляризации радиолокационных сигналов / В.Н. Татаринов, С.В. Татаринов, Л.П. Лигтхарт. – Томск: Изд-во Том. ун-та, 2006. – 379 с.

Гулько Владимир Леонидович
Канд. техн. наук, доцент каф. радиотехнических систем (РТС) Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7 (383-2) 41-34-55
Эл. почта: gulkovl@sibmail.com

Мещеряков Александр Алексеевич
Канд. техн. наук, доцент, доцент каф. РТС ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID 0000-0001-9566-7905
Тел.: +7 (383-2) 41-34-55
Эл. почта: msch@rts.tusur.ru

Gulko V.L., Mescheryakov A.A.
Use of orthogonal linearly polarized signals on board dual-channel UHF radio beacon navigation systems

The possibility of using orthogonally elliptically polarized signals of the beacon having two spaced radiation points for determining bearing and roll angle of a mobile object is examined.
The bearing and roll angle can be identified by results of analysis of amplitudes and phases in the linear polarization basis of simultaneously received vector signals by aboard mobile unit with UWF two-channel receiver.
Keywords: beacon, movable object, orthogonally elliptically polarized signals, Jones vector, amplitude-phase processing, bearing, roll angle, linear polarization basis.
doi: 10.21293/1818-0442-2018-21-2-7-11

References

1. Yarlykov M.S. *Statisticheskaya teoriya radionavigacii* [Statistical theory of radio navigation]. Moskow, Radio I svyaz', 1985. 344 p.

2. Sosnovskij A.A., Hajmovich I.A., Lutin EH.A., Maksimov I.B. *Aviacionnaya radionavigaciya: spravochnik* [Aviation radionavigation: Reference book.]. Moskow, Transport, 1990. 264 p.

3. Shirman Ya.D., Bagdasaryan S.T., Malyarenko A.S. i dr. *Radioehlektronnye sistemy: osnovy postroeniya i teoriya: spravochnik* [Radioelectronic Systems: Fundamentals of Construction and Theory: Reference Book.]. Moskow, Radiotekhnika, 2007. 512 p.

4. Pel'por D.S. *Giroskopicheskie sistemy orientacii i stabilizacii* [Gyroscopic systems of orientation and stabilization]. Moskow, Mashinostroenie, 1982. 165 p.

5. Smirnov E.L. *Giroskopicheskie navigacionnye sistemy* [Gyroscopic Navigation Systems]. Sankt-Peterburg, Ehl'mor, 2004. 400 p.

6. Aleshin B.S., Afonin A.A., Veremeenko K.K., Koshelev B.V. i dr. *Orientaciya i navigaciya podvizhnyh ob"ektov: sovremennye informacionnye tekhnologii* [Orientation and navigation of mobile objects: modern information technologies]. Pod red. B.S. Alyoshina, K.K. Veremeenko, A.I. Chernomorskogo. Moskow, Fizmatlit, 2006. 424 p.

7. Gusev K.G., Filatov A.D., Sopolev A.P. *Polyarizacionnaya modulyaciya* [Polarization modulation]. Moskow, Sov. radio, 1974. 288 p.

8. Bogorodskij V.V., Kanarejkin D.B., Kozlov A.I.. *Polyarizaciya rasseyannogo i sobstvennogo radioizlucheniya zemnyh pokrovov* [Polarization of scattered and intrinsic radio emission of terrestrial coverings]. Leningrad: Gidrometeoizdat, 1981. 279 p.

9. Kozlov A.I., Logvin A.I., Sarychev V.A. *Polyarizaciya radiovoln. Polyarizacionnaya struktura radiolokacionnyh signalov* [Polarization of radio waves. Polarization structure of radar signals]. Moskwa: Radiotekhnika, 2005, 704 p.

10. Gulko V.L., Mescheryakov A.A. Use of orthogonal linearly polarized signals in a dual channel board UHF radio beacon landing navigation systems. *Proceedings of TUSUR University*, 2017, vol. 20, no. 1, pp. 14–17 (In Russ.).

11. Gulko V.L., Mescheryakov A.A. Polarization Method of Determining the Bearing and the Roll Angle of a Mobile Object with Two channel Radio Beacon Navigation Systems. *Izv. Vuzov «Fizika»*, 2017, vol. 60, no. 6, pp. 44–49 (In Russ.).

12. Gulko V.L., Mescheryakov A.A. Ispol'zovanie ortogonal'no polyarizovannyh po krugu signalov radiomayaka dlya opredeleniya pelenga podvizhnogo ob"ekta bortovoj SVCH dvuhkanal'noj priemnoj sistemoj [The use of orthogonal circularly polarized beacon signals to determine the bearing of the mobile unit board UHF dual-channel receiver system]. *Sbornik trudov XXIII Mezhdunarodnoj nauchno-tekhnicheskoj konferencii «Radiolokaciya, navigaciya, svyaz'»* [Proceedings of the XXIII International Scientific and Technical Conference «Radiolocation, navigation, communication»]. Voronezh, 2017, vol. 3, pp. 822–826.

13. Gulko V.L., Mescheryakov A.A. Polyarizacionno-fazovyj metod opredeleniya pelenga i ugla krena podvizhnogo ob"ekta po ortogonal'no polyarizovannym po krugu signalam radiomayaka [Polarization-phase method for determining bearing and roll angle of a mobile object along orthogonally circularly polarized beacon signals] *Sbornik trudov XXIV Mezhdunarodnoj nauchno-tekhnicheskoj konferencii «Radiolokaciya, navigaciya, svyaz'»* [Proceedings of the XXIV International Scientific and Technical Conference «Radiolocation, navigation, communication»]. Voronezh, 2018, vol. 3, pp. 251–255.

14. Azzam P.M.A., Bashara H. *Ellipsometriya i polyarizovannyj svet* [Ellipsometry and Polarized Light]. Moskow, MIR, 1981. 583 p.

15. Tatarinov V.N., Tatarinov S.V., Ligtkhart L.P. Vvedenie v sovremennuyu teoriyu polyarizacii radiolokatsionnykh signalov. [Introduction to the modern theory of polarization of radar signals]. Tomsk, Izdatelstvo Tomskogo universiteta, 2006. 379 p.

Vladimir L. Gulko
Doctor of Engineering Sciences, Assistant Professor,
Department of Radio Engineering Systems, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-34-55
Email: gulkovl@sibmail.com

Alexander A. Mescheryakov
Doctor of Engineering Sciences, Assistant Professor,
Department of Radio Engineering Systems, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenina prosp., Tomsk, Russia, 634050
ORCID 0000-0001-9566-7905
Phone: +7 (382-2) 41-34-55
Email: msch@rts.tusur.ru

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 004.056.5

А.Г. Втюрина, В.Л. Елисеев, А.Е. Жиляев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский

Реализация средства криптографической защиты информации, использующего квантовое распределение ключей

Рассматриваются основные принципы построения комплексов защиты информации, допускающих автоматическое распространение и использование квантовых ключей. Рассматриваются неотъемлемые составные части, необходимые для функционирования такого комплекса в целом и аппаратуры распределения квантовых ключей в частности. В том числе обоснован выбор схемы аутентификации служебного канала квантовой аппаратуры, обоснован выбор квантового генератора случайных чисел и получен алгоритм его работы. Указаны проблемы совмещения шифраторов и квантовой аппаратуры и выявлены требования к логическому интерфейсу их взаимодействия. Также представлены результаты анализа влияния служебного трафика квантовой аппаратуры на нагруженность защищенного канала между шифраторами.

Ключевые слова: криптография, квантовое распределение ключей, квантовый генератор случайных чисел, аутентификация.

doi: 10.21293/1818-0442-2018-21-2-15-21

В современном мире наблюдается значительный рост скорости и объемов информации, передаваемой по каналам связи. В связи с продолжающимся переходом на электронные формы взаимодействия в России возрастают требования к обеспечению защиты информации. При этом необходимость обеспечения конкурентоспособности российской экономики, присутствия российских товаров и услуг на мировых рынках требует интеграции в международную сеть Интернет. Адекватной защитой от возрастающих рисков несанкционированного доступа к критически важной информации является использование шифрования. Однако в связи с отмечавшимся ранее ростом скорости передачи данных появляется проблема быстрой выработки нагрузки на ключ и необходимости частой смены ключа шифрования.

Другим риском является создание эффективного квантового компьютера, что потенциально снижает стойкость асимметричных криптографических алгоритмов и алгоритмов выработки симметричного ключа, основанных на задачах факторизации и дискретного логарифмирования, в связи с возможностью применения квантового алгоритма Шора [1].

Одним из возможных решений поставленных проблем является применение квантового распределения ключей (КРК) как средства доставки симметричных ключей абонентам [2]. Однако необходимо обеспечить тесную взаимосвязь шифраторов и аппаратуры квантового распределения ключей для синхронной смены ключей шифрования и безопасной бесперебойной поставки данных ключей от квантовой аппаратуры. Более того, так как параметры оптоволокна, в котором реализуется квантовый канал связи (ККС), постоянно изменяются в зависимости от условий окружающей среды и это влияет на распространение лазерных импульсов в квантовом канале связи, то при квантовом распределении ключей в условиях рабочей эксплуатации необходима своевременная подстройка параметров аппаратной части аппаратуры КРК, что возможно только в автоматическом режиме.

Компания «ИнфоТеКС» совместно с лабораторией квантовых оптических технологий МГУ в рамках проекта Минобрнауки РФ (проект 03.G25.31.0254) разрабатывает комплекс квантовой криптографической аппаратуры защиты информации (ККА ЗИ) ViPNet Quandor (рис. 1), в котором учтено решение описанных выше проблем и который будет обеспечивать передачу информации по сетям связи общего пользования, используя квантовый принцип распределения симметричных ключей шифрования [3]. Данный ККА ЗИ структурно состоит из двух взаимосвязанных составных частей:

– автоматической аппаратуры квантового распределения ключей (АА КРК);

– квантово-криптографического шифратора (ККШ).

Пользовательские данные из доверенной среды передачи (ДСП) передаются в зашифрованном виде между сопряженными ККШ в сети связи общего пользования.

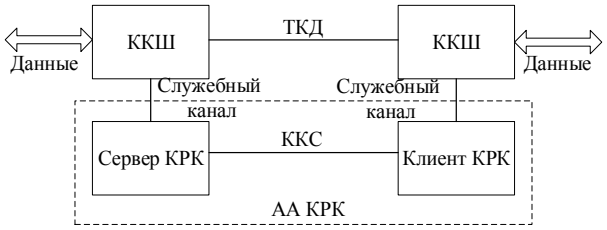


Рис. 1. Общая схема ККА ЗИ ViPNet Quandor

Для организации транспортного канала данных (ТКД) с использованием квантовых ключей необходимо наличие двух сопряженных составных частей АА КРК: сервера КРК и клиента КРК, а также двух ККШ. При этом на одной стороне располагается один ККШ и сервер КРК, а на другой стороне – другой ККШ и клиент КРК. Два ККШ соединяются ТКД, а сервер КРК и клиент КРК – квантовым каналом связи. Составные части АА КРК и ККШ на каждой из сторон ТКД связаны друг с другом служебным каналом, который позволяет ККШ получать

квантовые ключи (КК) и осуществлять операции по запросу АА КРК. Плановые характеристики разрабатываемого комплекса: скорость передачи данных в ТКД – 10 Гбит/с, при этом обеспечение конфиденциальности информации по ГОСТ Р 34.12–2015, а скорость выработки квантовых ключей не менее 256 бит в минуту.

Существенные составляющие АА КРК

Рассмотрим неотъемлемые компоненты АА КРК и общие принципы их взаимодействия.

Работа любой АА КРК определяется используемым протоколом квантового распределения ключей (протокол КРК). Обязательными этапами в любом протоколе КРК являются:

1. Предварительная настройка квантового канала связи.

2. Кодирование ключевой информации в одиночные фотоны и передача данных фотонов через квантовый канал связи. Неотъемлемой частью АА КРК является генератор случайных чисел, необходимый для выработки ключевой информации для кодирования фотонов.

3. Постобработка полученной ключевой информации (в том числе исправление ошибок в принятой и переданной последовательностях, усиление секретности очищенных последовательностей) с использованием классического канала. При этом неотъемлемой частью любой АА КРК является построение классического аутентифицированного канала для передачи служебного трафика по постобработке полученной ключевой информации.

Физическими законами обеспечивается неперехватываемость информации, передаваемой в квантовом канале связи. Можно выделить несколько типов кодирования ключевой информации в фотоны. Так, известный протокол BB84 использует поляризационное кодирование [4], что непременно повлечет использование специализированного оптоволокна, сохраняющего поляризацию. Иное оптическое волокно не сохраняет состояние поляризации, поэтому при прохождении через линию связи поляризация квазиоднофотонных состояний неконтролируемым способом изменяется. Хотя эти изменения достаточно медленные, все равно необходима активная стабилизация поляризации. Попытки реализовать такие системы были, но не получили дальнейшего развития из-за сложности стабилизации.

Поэтому в проекте выбрано фазовое кодирование, при котором биты исходной ключевой информации кодируются в относительную фазу двух когерентных разделенных во времени квазиоднофотонных состояний. В таких системах КРК при детектировании информационных квантовых состояний используется интерферометр Маха–Цандера, на котором «сбивается» пара пространственно разнесенных квазиоднофотонных когерентных состояний с различной относительной фазой [5]. Пространственное разнесение состояний производилось на таком же интерферометре Маха–Цандера.

Для получения стабильной интерференционной картины важно, чтобы относительная разность длин плеч интерферометров была одинаковой. Основные способы балансировки предполагают прерывание передачи ключей в режиме квазиоднофотонных состояний, перевод системы в классический режим и посылки одинаковых состояний для того, чтобы сбалансировать интерферометр [6]. Смена режима работы лазера и прерывание передачи негативно скажутся на времени выработки квантового ключа. Также данный метод балансировки требует дополнительной передачи служебных команд через классический аутентифицированный канал.

В целях ускорения выработки квантовых ключей целесообразно сократить число переключений режимов работы лазера. Для этих целей возможно применение альтернативного способа балансировки, не требующего дополнительного трафика в служебном канале, основанного на внесении дополнительной контролируемой фазы в одно из плеч интерферометра принимающей стороны, так как замечено, что отклонение видности интерференционной картины от идеальной однозначно связано с регистрируемой разностью числа нулей и единиц в просеянном ключе, т.е. в совпадающих базисах. Поэтому можно осуществлять балансировку только в квазиоднофотонном режиме, используя разность числа нулей и единиц в просеянном ключе как сигнал ошибки Q в качестве сигнала обратной связи. Это сокращает время балансировки и, кроме того, не требует дополнительного обмена по открытому каналу связи. Поскольку видность интерференционной картины определяется относительной разностью длин плеч интерферометров в сервере КРК и клиенте КРК, то достаточно регулировать только один из интерферометров.

Согласно результатам экспериментов [7] время разбалансировки интерферометров на величину, дающую чувствительный вклад в ошибку ключа, иногда оказывается сравнимо со временем его генерации. Это означает, что регулировка фазы должна производиться чаще, чем вырабатывается сигнал ошибки (просеянный ключ).

Таким образом, чтобы обеспечить равенство длин плеч интерферометров без постоянного их измерения, необходимо постоянно изменять фазу, интерполируя эту подстройку фазы между редкими моментами измерения разности длин плеч. То есть необходимо определить усредненную за некоторое время скорость изменения фазы и в промежутках между моментами регулирования изменять фазу с этой скоростью.

Особенности аутентификации при квантовом распределении ключей

Как обозначалось ранее, неотъемлемой частью АА КРК является построение классического аутентифицированного канала для передачи служебного трафика.

Обычно для аутентификации первой сессии выработки первичных квантовых ключей должны использоваться предварительно распределенные симметричные ключи. При накоплении достаточного количе-

ства квантовых ключей аутентификация продолжается на этих квантовых ключах, полученных от АА КРК.

Существует два основных подхода к аутентификации классического канала в системах КРК. Возможно применение либо теоретико-информационно стойкой, либо вычислительно стойкой аутентификации. Применение теоретико-информационно стойкой аутентификации, несмотря на более высокий уровень стойкости, связано с рядом существенных проблем.

Ключевой проблемой теоретико-информационно стойкой аутентификации является необходимость использования новых различных ключей аутентификации для каждого аутентифицируемого сообщения [8]. При этом ключ на аутентификацию последующей сессии выработки квантовых ключей принято отрезать от текущего общего квантового ключа, выработанного в результате протокола КРК. Таким образом, в зависимости от объемов трафика, который необходимо аутентифицировать, возможна ситуация, при которой большая часть выработанного квантового ключа будет отрезана на аутентификацию канала для последующей серии.

В качестве теоретико-информационной стойкой аутентификации принято применять функции универсального хэширования [9]. Характеристики наиболее перспективных классов функций универсального хэширования приведены в [10]. Нижняя оценка для длины ключа аутентификации таких функций – двоичный логарифм от длины сообщения. Так, для аутентификации хэш-функциями на базе кодов Рида–Соломона, обладающей одной из минимальных длин необходимого ключа аутентификации, для аутентификации 3,5 Мбит трафика, переданного в ходе работы протокола КРК, разработанного в рамках проекта, необходимо 236 бит ключа аутентификации при ожидаемой производительности данного протокола 256 бит ключа. Следовательно, почти весь вырабатываемый ключ будет отводиться на аутентификацию следующей сессии выработки, что малоцелесообразно.

Таким образом, для квантовых криптографических систем, обладающих небольшой скоростью генерации ключей из-за высокого уровня стойкости вырабатываемых КК, применение теоретико-информационной аутентификации оказывается невозможным. Для таких систем остается применение вычислительно стойкой аутентификации. При этом в отличие от первого подхода на одном ключе аутентификации допустимо аутентифицировать несколько сообщений.

Необходимость и базовые принципы квантового генератора случайных чисел

Неотъемлемой частью АА КРК является генератор случайных чисел (ГСЧ) для получения случайных последовательностей. Для обеспечения секретности вырабатываемых квантовых ключей необходимо использование случайных чисел, полученных исключительно с физических генераторов [11]. При этом необходимо использовать именно квантовые генераторы случайных чисел (КГСЧ). Результаты измерений над квантовой системой, приготовленной каждый раз в одном и том же состоянии, носят принципиально случайный характер. Поэтому истинная случайность имеет место только в квантовой области.

Наиболее целесообразным способом получения первичной случайности можно считать способ, основанный на принципе фотодетектирования [12]. Финальная случайная последовательность нулей и единиц возникает в результате измерений над квантовой системой и последующей обработки результатов этих измерений. Для грамотного исполнения КГСЧ необходимо утвердить следующие важные этапы работы КГСЧ:

1. Выбрать способ фотодетектирования, который бы контролируемым образом обеспечивал независимость отдельных актов регистрации и приводил к пуассоновской статистике фотоотсчетов.
2. Выбрать такую группировку фотоотсчетов в отдельные блоки, которая бы обеспечивала извлечение всей случайности, которая содержится в процессе регистрации квантовых состояний.
3. Выбрать такой способ постобработки, который бы гарантировал получение идеально случайной последовательности, а не близкой к идеальной.

Фотодетектирование по своей природе является квантовым процессом, поэтому оно используется многими авторами при разработке КГСЧ. При фотодетектировании возникает распределение Ферми–Дирака [13] при «размещении» фотоотсчетов по временным интервалам.

Получение истинно случайной последовательности из последовательности фотоотсчетов означает отображение последовательностей фотоотсчетов длиной в n тактов с m отсчетами в истинно случайные блоки нулей и единиц длиной l, зависящей от n и m: $\{*,\_\}^{n_m} \to \{0,1\}^l$, $(1<n)$. Последовательность разбивается на ходу на блоки длиной n, содержащие одинаковое число тактов. В каждом блоке может быть m фотоотсчетов (*), $0 \le m \le n$. Всего типов таких блоков существует $2n$. Вероятность последовательности с m отсчетами (*) и n–m-пропусками (_) имеет вид $(1-p(*))^{n-m}\, p(*)^m$. При этом полное число равновероятных последовательностей (последовательностей, содержащих одинаковое число тактов с отсчетами (*) и пустых тактов (_)) одного класса равно C_n^m.

Согласно [14] необходимо пронумеровать все равновероятные последовательности из одного класса, а затем извлечь блок случайных нулей и единиц из двоичного номера последовательности в данном классе. При прямом способе нумерации сама последовательность является адресом номера в данном классе. Однако в этом случае размер адресной таблицы будет экспоненциально велик. Например, при длине обрабатываемого блока в 64 такта размер адресной таблицы составит $2^{64} \approx 10^{19}$, что практически нереализуемо. Поэтому предлагается использо-

вать методы арифметического кодирования, а именно способ нумерации последовательностей фотоотсчетов, требующий лишь полиномиальных ресурсов по длине последовательности и позволяющий обрабатывать последовательности практически любой длины [15].

Пусть в последовательности имеется K отсчетов (*). Тогда есть взаимное однозначное соответствие между последовательностью фотоотсчетов (i_1, i_2, …, i_n) и ее номером:

$$\mathrm{Num}(i_1,i_2,...,i_n)(0\le \mathrm{Num}(i_1,i_2,...,i_n)\le C_n^K-1):$$

$$\mathrm{Num}(i_1,i_2,...,i_n)=C^1_{j_1-1}+C^2_{j_2-1}+...+C^k_{j_k-1},$$

$$C^1_{j_1-1}=0,\quad j<l. \qquad (1)$$

В формуле (1) индексом j_k обозначен номер позиции.

В результате разработки АА КРК был получен следующий алгоритм работы КГСЧ:

1. Биномиальные коэффициенты вычисляются заранее и помещаются в таблицу размером $n\times n$ в память вычислительного устройства, например, системы на модуле, содержащей FPGA (рис. 2).

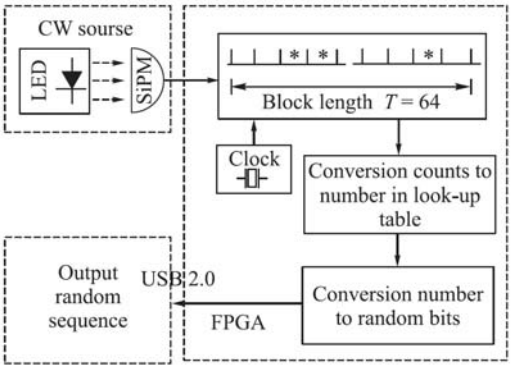


Рис. 2. Блок-схема функционирования КГСЧ

2. При появлении первого отсчета в позиции j_1 выбирается биномиальный коэффициент на пересечении первой строки j_1 и первого столбца матрицы. При появлении второго отсчета выбирается коэффициент в матрице на пересечении j_2 строки и второго столбца матрицы. В итоге получается номер последовательности $\mathrm{Num}(i_1,i_2,...,i_n)$.

3. Номера последовательностей находятся в пределах $0<\mathrm{Num}<N_k-1$, причем бинарное представление числа последовательности в классе $N_k=\sum_{i=0}^{i_{\max}}2^{k_i}$. Необходимо рекурсивно выдать блок случайных нулей и единиц. Если номер текущей последовательности Num находится в интервале $2^{k0}+2^{k1}+...+2^{k_{i-1}}\le \mathrm{Num}\le 2^{k0}+2^{k1}+...+2^{k_{i-1}}+2^{k_i}-1$, причем $i\le i_{\max}$, тогда выходной случайной последовательностью будет k_i младших разрядов бинарного представления Num. Число номеров последовательностей в этом диапазоне равно 2^{k_i}.

Замечательно, что использование подобного способа экстракции случайной последовательности дает истинно случайную последовательность. Единственным условием становится пуассоновский характер последовательности фотоотсчетов, что может быть достигнуто точностью практической реализации КГСЧ.

Как видно из схемы, представленной на рис. 2, КГСЧ состоит из трех элементов:

– генератора случайных импульсов (источник излучения LED, матрица SiPM);

– блока обработки на основе вычислительного устройства (FPGA), в котором реализованы алгоритмы КГСЧ-группировки фотоотсчетов, постобработки полученной последовательности и выдачи их потребителю;

– интерфейса для подключения внешнего потребителя получаемой последовательности случайных чисел (Output random sequence).

Интерфейс взаимодействия ККШ и АА КРК

Для практической реализации КККА ЗИ с использованием КРК немаловажным аспектом является грамотное согласование АА КРК и ККШ, в которые будут передаваться квантовые ключи.

Протокол их взаимодействия необходимо разрабатывать универсальным, чтобы не создавать жесткой привязки шифраторов к серверу КРК или клиенту КРК.

Самодостаточная квантовая аппаратура, которая самостоятельно строит для себя классический аутентифицированный канал, вызывает ряд проблем при практическом использовании, а именно необходимость маршрутизации отдельного канала служебного трафика и необходимость обеспечения защиты передачи квантовых ключей в шифраторы, что ведет к созданию и контролю сложных криптографических преобразований в квантовой аппаратуре. Поэтому целесообразно строить данный канал непосредственно внутри комплекса защиты информации, т.е. через шифратор.

Таким образом, можем выделить минимально необходимый состав трафика, проходящего между АА КРК и ККШ, а также обозначить требования, которые необходимо обеспечить при прохождении данного трафика.

1. В канале между АА КРК и ККШ передаются полученные готовые квантовые ключи. Криптографические ключи, в том числе и КК, должны передаваться только по защищенным каналам. В случае с передачей квантовых ключей защита должна осуществляться с помощью шифрования. Следовательно, стоит учитывать необходимость выделения ключей для шифрования квантовых ключей при передаче, что несомненно вызовет существенные изменения в общей ключевой системе комплекса. Более того, для бесперебойной работы шифраторов следует передавать ключи в приоритетном порядке.

2. Вторым важным типом трафика является служебный трафик АА КРК, которым обменивается аппаратура при постобработке переданной ключевой

последовательности. Протоколы КРК накладывают только требование аутентификации на данный трафик, поэтому шифровать служебный трафик не обязательно. Важно, чтобы ККШ по возможности без задержек передавал служебный трафик по каналу и дальше в АА КРК. С точки зрения интерфейса между АА КРК и ККШ данный трафик – данные, которые необходимо оперативно передать без изменений и какой-либо обработки.

3. Стоит учитывать, что создание комплекса защиты информации, а не применение отдельных шифратора и квантовой аппаратуры позволяет наладить тесное взаимодействие устройств, что в свою очередь выльется в появление сервисного трафика между ККШ и АА КРК. Таким образом, АА КРК и ККШ способны отслеживать работоспособность друг друга и, более того, оценивать возможность возобновления работоспособности в зависимости от типов ошибки.

Деградация канала ТКД

Стоит отметить, что в связи с появлением дополнительного для ККШ трафика, а именно служебного трафика АА КРК, важной частью разработки комплекса является согласованное использование транспортного канала полезной нагрузкой и служебным трафиком АА КРК. В рамках проекта была оценена деградация ТКД при различных ограничениях полосы пропускания служебного трафика.

Были проведены исследовательские испытания по выявлению величины падения скорости передачи данных в ТКД из-за добавления служебного трафика АА КРК. На рис. 3 представлен график зависимости падения скорости передачи данных в ТКД в виде деградации ДСП от длины квантового канала связи (ККС).

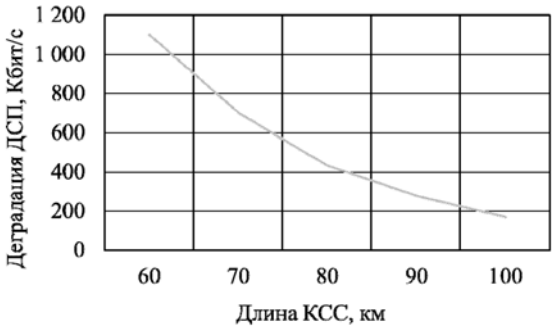


Рис. 3. График зависимости падения скорости передачи в ДСП

Из графика видно, что наибольшее падение скорости передачи данных в ДСП наблюдается при длине ККС 60 км, при которой объем данных, передаваемых по каналу служебной связи, максимальный для постобработки переданной ключевой информации. Тем не менее максимальная величина падения скорости передачи полезных данных в ДСП составляет – 1,1 Мбит/с при скорости ТКД 10 Гбит/с, что составляет 0,011% от скорости ТКД.

По результатам анализа исследовательских испытаний следует, что падение скорости передачи данных в ДСП составляет 0,011%. Таким образом, при использовании КРК для защиты высокоскоростных каналов передачи можно не ограничивать скорость служебного трафика, обеспечивая оперативную доставку необходимых данных для АА КРК при сохранении скорости передачи полезных пользовательских данных.

Заключение

В данной статье описаны структура и состав ККА ЗИ ViPNet Quandor, разрабатываемого ОАО «ИнфоТеКС» совместно с МГУ им. М.В. Ломоносова. Обоснован выбор фазового кодирования в используемом протоколе КРК, описан реализуемый способ стабилизации интерференционной картины. Показано, что скорость генерации квантовых ключей должна быть достаточно высокой для применения теоретико-информационно стойкой аутентификации. Также рассмотрено устройство используемого КГСЧ и представлен алгоритм его работы, составленный в процессе разработки АА КРК. Обозначены требования для трафика между АА КРК и ККШ. Отмечено, что для защиты высокоскоростных каналов передачи данных можно не ограничивать скорость служебного трафика.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (проект 03.G25.31.0254).

Литература

1. Shor P. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134. – doi: 10.1109/SFCS.1994.365700

2. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.

3. Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата. – М.: Юрайт, 2017. – 321 с.

4. Bennett C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennett, G. Brassard // Proceedings of International Conference on Computers, Systems & Signal Processing. – IEEE, 1984. – PP. 175–179.

5. Балыгин К.А. Активная стабилизация оптической части в волоконной квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2016. – Т. 103, вып. 6. – С. 469–474.

6. Молотков С.Н. О секретности волоконных систем квантовой криптографии без контроля интенсивности квазиоднофотонных когерентных состояний // Письма в ЖЭТФ. – 2015. – Т. 101, вып. 8. – С. 579–585.

7. Управление распределенной интерференцией в однопроходной системе квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2017. – Т. 106, № 2. –С. 108–114.

8. Quantum Key Distribution [Электронный ресурс] // ETSI. – Режим доступа: http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution, свободный (дата обращения: 24.07.18).

9. Abidin A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions // Dissertation. – Division of Information Coding, Linkoping University, Linkoping, Swede, 2013.

10. Zhilyaev A.E. On the question of the authentication tag length based on Reed-Solomon codes / A.E. Zhilyaev, E.B. Gurova // Proceedings of Moscow Workshop on Electronic and Networking Technologies. – IEEE, 2018. –

doi: 10.1109/MWENT.2018.8337293. – URL: https://ieeexplore.ieee.org/document/8337293/ (дата обращения: 24.07.18).

11. Quantum Safe Cryptography and Security [Электронный ресурс] // ETSI. – Режим доступа: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, свободный (дата обращения: 24.07.18).

12. Молотков С.Н. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов / С.Н. Молотков, К.А. Балыгин, А.Н. Климов, В.И. Зайцев, С.П. Кулик // Письма в ЖЭТФ. – 2017. – Т. 106, № 7. – С. 470–476.

13. Ландау Л.Д. Статистическая физика / Л.Д. Ландау, Е.М. Лифшиц. – М.: Физматлит, 2002. – 1995. – Т. 5, ч. 1. – 616 с.

14. Молотков С.Н. О предельных характеристиках квантовых генераторов случайных чисел при различных группировках фотоотсчетов // Письма в ЖЭТФ. – 2017. – Т. 105, № 6. – С. 374–380.

15. Бабкин В.Ф. Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости // Проблемы передачи информации. – 1971. – Т. 7, №13. – С. 288–294.

Втюрина Анна Георгиевна
Инженер физического ф-та МГУ им. М.В. Ломоносова
1, Ленинские горы, стр. 2, г. Москва, Россия, 119991
Тел.: +7-904-333-24-56
Эл. почта: ataniru@gmail.com

Елисеев Владимир Леонидович
Канд. техн. наук, руководитель Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 70-59
Эл. почта: EliseevVL@infotecs.ru

Жиляев Андрей Евгеньевич
Исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7-903-960-05-27, доб. 42-64
Эл. почта: Andrey.zhilyaev@infotecs.ru

Николаева Анастасия Сергеевна
Исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 45-11
Эл. почта: EliseevVL@infotecs.ru

Сергеев Владимир Николаевич
Вед. исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 44-95
Эл. почта: Vladimir.Sergeev@infotecs.ru

Уривский Алексей Викторович
Канд. физ.-мат. наук, зам. генерального директора по науке и инновациям ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 52-49
Эл. почта: Urivskiy@infotecs.ru

Vtyurina A.G., Eliseev V. L., Zhilyaev A.E.,
Nikolaeva A.S., Sergeev V.N., Urivskiy A.V.

On the principal decisions of the practical implementation of the cryptographic devices with quantum key distribution

This article is considering the basic principles of building information security complexes, which allow automatic distribution and usage of quantum keys. Required parts of such complex are described which are needed for the operation of complex as a whole and for quantum key distribution in particular. The authentication scheme for quantum protocol is chosen. The choice of quantum random number generator is justified and algorithm for such generator is developed. The problems of combining encryptors with quantum key distribution devices are indicated and requirements for the logical interface of their interaction are revealed. In addition, authors present results of the analysis of quantum devices' traffic influence on the load of protected channel between encryptors.

Keywords: cryptography, quantum key distribution, quantum random number generator, authentication.
doi: 10.21293/1818-0442-2018-21-2-15-21

References

1. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Publ., 1994, P. 124–134, doi: 10.1109/SFCS.1994.365700.

2. Nillsen M., Chang I. *Quantovie vichisleniya I quantovaya informaciya* [Quantum computing and quantum information]. Moscow, Mir Publ., 2006. 824 p.

3. Nesterov S.A. *Informatsionnaya bezopasnost. Uchebnik i praktikum dlya akademicheskogo bakalavriata* [Information security. Textbook and workbook for bachelor students], Moscow, URAIT Publ., 2017. 321 p.

4. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of International Conference on Computers, Systems & Signal Processing. IEEE Publ., 1984, pp. 175–179.

5. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. Active stabilization of the optical part in fiber optic quantum cryptography. *Jetp Lett.*, 2016, vol. 103, no. 6, pp. 420–424 (In Russ.).

6. Molotkov S.N. On the security of fiber optic quantum cryptography systems without the control of the intensity of quasi-single-photon coherent states. *Jetp Lett*., 2015, vol. 101, no. 8, pp. 579–585 (In Russ.).

7. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. Control of distributed interference in the one-way quantum cryptography system. *Jetp Lett.*, 2017, vol. 106, no. 2, pp. 120–126 (In Russ.).

8. Quantum Key Distribution. ETSI Publ.. Available at: http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution (accessed 24 July 2018)

9. Abidin A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions, Dissertation, Division of Information Coding, Linkoping University, Linkoping, Sweden, 2013.

10. Zhilyaev A.E., Gurova E.B. On the question of the authentication tag length based on Reed-Solomon / Proceedings of Moscow Workshop on Electronic and Networking Technologies, IEEE Publ., 2018, doi: 10.1109/MWENT.2018.8337293. Available at: https://ieeexplore.ieee.org/document/8337293/ (accessed: 24.07.18).

11. Quantum Safe Cryptography and Security. ETSI Publ.. Available at: http://www.etsi.org/images/files/ETSI WhitePapers/QuantumSafeWhitepaper.pdf (accessed 24 July 2018).

12. Balygin K.A., Zaitsev V.I., Klimov A.N. et al. Implementation of a quantum random number generator based on the optimal clustering of photocounts. *Jetp Lett*., 2017, vol. 106, no. 7, pp. 470–476 (In Russ.).

13. Landau L.D., Lifshitz E.M. *Statistical Physics*, *Vol. V, No. 1*, FIZMATLIT Publ., 2002, 616 p. (In Russ.).

14. Molotkov S.N. On the limiting characteristics of quantum random number generators at various clusterings of photocounts. *Jetp Lett.*, 2017, vol. 105, no. 6, pp. 395–401 (In Russ.).

15. Babkin V.F., A Universal Encoding Method with Nonexponential Work Expenditure for a Source of Independent Messages, *Problems Inform. Transmission.,* 1971, vol. 7, no. 4, pp. 288–294.

Anna G. Vtyurina
Engineer, Faculty of Physics,
M.V. Lomonosov State University, Moscow
1, Leninskie Gory, Bld. 2, Moscow, Russia, 119991
Phone: +7-904-333-24-56
Email: ataniru@gmail.com

Vladimir L. Eliseev
Ph.D., Chief of Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 70-59
Email: EliseevVL@infotecs.ru

Andrey E. Zhilyaev
Researcher, Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7-903-960-05-27, add. 42-64
Email: Andrey.zhilyaev@infotecs.ru

Anastasia S. Nikolaeva
Researcher, Research and Development Center,
JSC «InfoTeCS», B.Sc. MIPT (SU)
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 45-11
Email: Anastasia.Nikolaeva@infotecs.ru

Vladimir N. Sergeev
Lead Researcher, Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 44-95
Email: Vladimir.Sergeev@infotecs.ru

Alexey V. Urivskiy
Ph.D., Deputy Director General for Science and Innovation,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 52-49
Email: Urivskiy@infotecs.ru

УДК 004.021

Е.А. Толоманенко

Дифференциальный анализ трех раундов шифра «Кузнечик»

«Кузнечик» – это новый симметричный алгоритм шифрования, принятый в качестве стандарта шифрования ГОСТ Р 34.12–2015, построенный по принципу SP-сети. До сих пор нет публикаций о дифференциальных свойствах алгоритма «Кузнечик». В данной работе исследованы и описаны свойства основных операций и предложен метод дифференциального анализа трех раундов алгоритма шифрования «Кузнечик». В результате исследования дифференциальных свойств нелинейной функции S и линейной функции L было установлено, что возможна ситуация, когда один ненулевой байт разности в результате функции L разворачивается в 16 ненулевых байтов, проходит через блок замены S и затем сворачивается снова в один ненулевой байт. Разработанная схема позволяет затрагивать активный S-блок минимальное количество раз. Таким образом, общая сложность анализа, включая поиск правильных пар текстов и поиск битов секретного ключа шифрования составляет $2^{-108} + 6*2^{-120}$ зашифрований.

Ключевые слова: криптография, блочный шифр, SP-сеть, криптоанализ, дифференциальный криптоанализ, шифр «Кузнечик», ГОСТ Р 34.12–2015.
doi: 10.21293/1818-0442-2018-21-2-22-26

Алгоритм шифрования «Кузнечик» представляет собой часть стандарта шифрования ГОСТ Р 34.12–2015, официально вступившего в силу 01.01.2016, поэтому исследование его надежности на сегодняшний день является актуальной задачей. Описание алгоритма шифрования «Кузнечик» как части нового принятого стандарта шифрования содержится в документе Технического комитета по стандартизации ТК 26 «Криптографическая защита информации» в ГОСТ Р 34.12–2015 [1]. Есть несколько статей, посвященных различным способам реализации алгоритма «Кузнечик», в том числе и с использованием специальных таблиц предвычислений [2]. Метод дифференциального криптоанализа был впервые предложен Эли Бихамом и Ади Шамиром, которые применили его к анализу алгоритма шифрования DES [3, 4]. Также криптоанализ был рассмотрен в работах [5–7]. На данный момент в открытой печати не фигурируют публикации, содержащие информацию о дифференциальных свойствах и о итоговых количественных оценках сложности дифференциального криптоанализа алгоритма шифрования «Кузнечик» и предлагающие применение данного метода криптоанализа к некоторому сокращенному количеству раундов шифра «Кузнечик».

В данной работе предложен метод построения трехраундового дифференциала для алгоритма шифрования «Кузнечик». Разработанная схема анализа основана на использовании дифференциальных свойств преобразований S и L алгоритма «Кузнечик» и предназначена для того, чтобы можно было определить правильную пару текстов для дальнейшего анализа, целью которого является определение секретного ключа шифрования. Схема разработана таким образом, чтобы затрагивать активные нелинейные компоненты (S-блоки) минимальное количество раз. В результате для предложенной схемы вероятность нахождения правильных пар текстов составляет 2^{-108} зашифрований. Также был разработан алгоритм нахождения секретного ключа, сложность которого составляет $6*2^{-120}$ зашифрований с использованием шифра «Кузнечик». Таким образом, общая сложность анализа, включая поиск правильных пар текстов и поиск битов секретного ключа шифрования, составляет $2^{-108} + 6*2^{-120}$ зашифрований. Сложность предложенной схемы является достаточно высокой в сравнении с возможностями современных вычислительных средств, но гораздо более низкой, чем сложность компрометации ключа методом полного перебора.

Описание алгоритма шифрования «Кузнечик»

Кузнечик – это симметричный блочный шифр с длиной мастер-ключа, равной 256 бит, и длиной блока – 128 бит. Шифр построен по принципу SP-сети, что позволяет выполнить преобразование всего входного блока целиком, а не только его части.

Шифрование реализуется с использованием 9 раундов и поочередным применением трех преобразований: XOR-блока данных с раундовым ключом, с помощью блока замены (S) и линейное преобразование (L). Десять раундовых ключей вырабатываются из 256-битного мастер-ключа.

Расшифрование осуществляется наоборот, снизу вверх, с помощью преобразований, обратных к тем, которые применялись при зашифровании.

Более подробно с процессами зашифрования и расшифрования, их программной реализацией, а также с применяемыми в алгоритме «Кузнечик» преобразованиями можно ознакомиться в [8–11].

Разработка алгоритма для дифференциального криптоанализа шифра «Кузнечик»

Общий метод дифференциального криптоанализа симметричных блочных шифров описан в [12].

Для применения метода дифференциального криптоанализа применительно к шифру «Кузнечик» необходимо пару открытых текстов X и X', объединенную дифференциалом ΔX, отправить на вход алгоритма. На выходе получим пару текстов Y и Y', соответствующую входным текстам и объединенную дифференциалом ΔY. Значение раундового

ключа не влияет на дифференциалы, так как при выполнении операции XOR его биты будут взаимно уничтожены – $X \oplus K_i \oplus X' \oplus K_i$.

Анализ алгоритма подразумевает создание таблицы вероятностей для блока замены *S*. В строках таблицы обозначены значения ΔA, являющиеся входом в блок подстановок, а в столбцах – значения ΔC, получаемые на выходе из блока подстановок, соответствующие ΔA. Ячейки на пересечении показывают, сколько пар дифференциалов $\Delta A/\Delta C$ имеют данные входные и выходные значения. Таблица отражает значение вероятности, с которой при конкретном дифференциале ΔA, поданном на вход блока *S*, на выходе будет получено конкретное значение ΔC. Алгоритм получения дифференциальных характеристик *S*-блоков замены описан в работе [13]. Малая часть полученной таблицы со значениями вероятностей содержится в таблице.

Фрагмент таблицы со значениями вероятностей, построенной для блока замены *S*

ΔC/ΔA	0	1	2	…	3e	3f	…	fe	ff
0	256/ 256	0/256	0/256	…	0/256	0/256	…	0/256	0/256
1	0/256	0/256	2/256	…	2/256	4/256	…	0/256	2/256
…	…	…	…	…	…	…	…	…	…
ff	0/256	2/256	2/256	…	0/256	4/256	…	0/256	0/256

В результате криптоанализа должен быть скомпрометирован раундовый ключ. Процесс компрометации в данной ситуации подразумевает, что для конкретного значения ΔA соответствующие ΔC имеют разную вероятность быть полученными. Таблица свидетельствует о том, что в данном случае вероятность может быть равна 2/256, 4/256, 6/256 и 8/256, а также может быть равной нулю. Пара дифференциалов ΔA и ΔC позволяет предположить значения $A \oplus K_i$ и $A' \oplus K_i$. При известных A и A' это позволяет определить K_i [14].

На сегодняшний день в открытой печати нет информации о дифференциальных свойствах алгоритма шифрования «Кузнечик». Существующий метод дифференциального криптоанализа применялся к различным известным шифрам [15], а схема применения данного метода криптоанализа к шифру «Кузнечик», аналогов которой не существует, была разработана и описана в данной работе. В результате исследования свойств функций *S* и *L* было установлено, что возможна ситуация, когда 1 байт в результате функции *L* разворачивается на 16 байт, проходит через блок замены *S* и затем сворачивается в 1 байт. Разработанная схема позволяет затрагивать *S*-блок минимальное количество раз. Разработанный метод анализа для трех раундов шифрования изображен на рис. 1. На основании данной схемы был разработан алгоритм.

Первый этап соответствует первому раунду:

1. Случайно сгенерированный текст X и парный ему текст X' отличаются лишь значением ΔA, Эти значения подаются на вход.

2. После уничтожения ключей в результате использования блока замены *S* данный байт меняется на другой по таблице вероятностей

3. Далее преобразование *L* раскладывает данный байт на 16 байт.

Второй этап соответствует второму раунду:

1. После уничтожения ключа преобразование *S* изменит каждый из 16 байтов на другой в соответствии с таблицей.

2. После преобразования *L* во 2-м раунде 16 байт наиболее вероятных значений преобразуются снова в 1 байт.

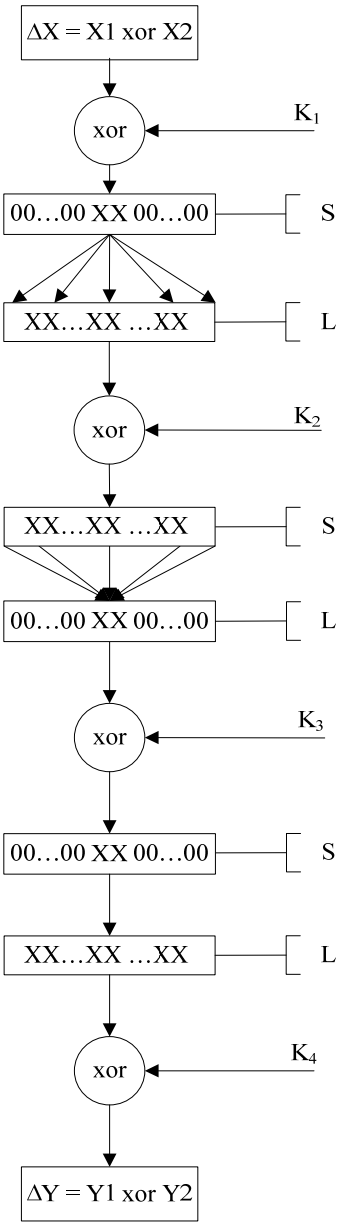


Рис. 1. Схема дифференциального анализа трех раундов шифрования

Третий этап соответствует третьему раунду:

1. Преобразованное на втором этапе значение после уничтожения ключа меняется на другое по таблице вероятности

2. В итоге преобразование L раскладывает этот 1 байт на 16, и на выходе будет получен результат по итогам трех раундов шифрования.

Таким образом, для рассматриваемой схемы анализа получается всего 18 активных S-блоков вместо 33, как было рассмотрено ранее.

Даже если предположить, что можно подобрать значения дифференциалов, которые будут соответствовать рис. 1, с минимальными значениями вероятностей для каждого из активных S-блоков $2/256 = 1/2^7$, получится трехраундовый дифференциал с вероятностью в $(1/2^7)^{18} = 1/2^{126}$, что меньше, чем ранее предположенное значение $1/2^{165}$. Нужно отметить, что удалось получить трехраундовую характеристику, вероятность появления которой равна $1/2^{108}$, что означает, что при использовании активных S-блоков были задействованы не самые минимальные вероятности.

Алгоритм нахождения правильных пар текстов для трехраундовой характеристики

Алгоритм нахождения правильных пар тестов для проведения анализа не может быть прямо реализован из-за маленькой вероятности получения правильных пар текстов. Мощности обычного персонального компьютера для этого недостаточно. Поэтому для осуществления проверки работоспособности предложенного метода был разработан способ «от обратного». Применение данного способа подразумевает, что будут подобраны такие правильные пары текстов, которые при конкретных значениях раундовых секретных ключей будут формировать необходимые значения дифференциалов.

На основе данного способа был разработан алгоритм нахождения правильных пар текстов. Данный алгоритм, найденные значения и проверка его работоспособности подробно описаны в работе [14].

Всего было найдено 13 пар значений $\Delta A/\Delta C$. Например, для ΔA=f3ab8c55c199996f0c5a4f2381976846 найдено ΔC=51ac91f0df24701900ad86a256131163, а для ΔA=1a76bc71665284b01a3e595982599369 найдено ΔC=ba5a9d5e6d2b64310ac6b9cb72dc5a7a1.

После нахождения всех байтов исходных текстов, составляющих данные дифференциалы, можно сделать вывод, что общее число всех вариантов значений X и X': P=2*2*4*4*2*2*2*2*2*2*2*2*2*4*2*2 = = 524288.

Из найденных значений $\Delta A/\Delta C$ легко можно определить значения дифференциалов на входе и выходе 3-раундового алгоритма «Кузнечик» $\Delta X/\Delta Y$, а также вероятность их появления.

Нахождение конкретных текстов на входе и выходе трехраундового алгоритма было выполнено с помощью прямых и обратных преобразований над найденными значениями во втором и третьем раунде.

Алгоритм компрометации секретного ключа на основе найденных правильных пар текстов

Метод дифференциального криптоанализа, как правило, заключается в компрометации раундовых ключей с целью расшифрования информации. Описать технологию криптоанализа с помощью найденных ранее правильных пар текстов можно следующим образом.

В рассмотренных 3 раундах алгоритма шифрования используется 4 раундовых ключа (см. рис. 1). Необходимо обратить внимание на то, что в алгоритме «Кузнечик» первыми двумя раундовыми ключами являются левая и правая части 256-битного мастер-ключа, разделенного напополам. На этом факте основан разработанный мной алгоритм, который подразумевает поиск первого ключа K1, после него – K2, с помощью которых затем можно выработать остальные ключи – K3 и K4. Предложенный алгоритм состоит из таких этапов, как:

1. Проведение обратных операций $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$ и $L_{\text{inv}}(\Delta A)$ для получения входа и выхода преобразования S первого раунда соответственно.

2. На вход алгоритма (см. рис. 1) подается ранее подобранная пара текстов X и X', которая при сложении с числом, получившимся в результате операции $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$, дает значение ключа K1.

3. Получившееся значение $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$ состоит из одного байта и его вероятность равна 6 по таблице, содержащей значения вероятностей. Это говорит о том, что будет 6 возможных значений одного байта ключа K1. Таким образом, количество всех возможных вариантов 128-битного ключа K1 будет равно $2^{120}\times 6$.

4. Производится поиск правильного ключа K1, подразумевающий следующие операции:

Подаются на вход 2 подобранных текста X и X', складываются с первым возможным ключом K1. Полученные значения проходят преобразования S и L первого раунда. Результат складывается со значениями A и A', объединенными дифференциалом ΔA, поступающими на вход преобразования S второго раунда. Данные преобразования позволяют найти одно из возможных значений ключа K2. Ключи K1 и K2 объединяются в 256-битный мастер-ключ и из него вырабатываются ключи K3 и K4. Далее два возможных шифртекста Y и Y', полученных в результате применения алгоритма нахождения правильных пар текстов, складываются с ключом K4. Полученные значения претерпевают преобразования L_{inv} и S_{inv} третьего раунда, складываются с ключом K3 и затем проходят преобразование L_{inv} второго раунда.

Результаты преобразования L_{inv} второго раунда сравниваются со значениями, составляющими дифференциал ΔC. Если значения равны, то ключи сохраняются как вероятно правильные. Если значения не равны, то алгоритм повторяется заново.

Фактически опробование ключей сводится к выполнению всех операций трехраундового зашифрования. Поэтому сложность алгоритма нахождения ключей будет задействовать максимум $2^{120}\times 6$ зашифрований. При данном условии будут скомпрометированы все 4 ключа с гораздо меньшей сложностью, чем при условии полного перебора, сложность которого равна 2^{256}.

Общая сложность дифференциального криптоанализа трех раундов алгоритма шифрования «Кузнечик» может быть оценена как $2^{120}\times6+2^{108}$ зашифрований.

Выводы

В результате работы над данным проектом впервые были исследованы и получены дифференциальные свойства алгоритма шифрования «Кузнечик». На основе проведенных исследований была выявлена связь между преобразованиями *S* и *L*, которая позволила разработать алгоритм дифференциального криптоанализа трех раундов шифра «Кузнечик», ранее никем не предложенный в открытых литературных источниках.

На основе предложенной схемы трехраундового дифференциала были разработаны алгоритм нахождения правильных пар текстов для анализа шифра и алгоритм нахождения секретного ключа с гораздо меньшей сложностью, чем сложность при поиске ключа полным перебором. Разработанные алгоритмы позволяют оценить общую сложность проведения анализа, которая составляет $2^{108} + 6*2^{120}$. Результаты работы использованы при выполнении исследовательских работ по гранту РФФИ №17-07-00654-а «Разработка и исследование последовательных и параллельных алгоритмов анализа современных симметричных шифров с использованием технологий MPI, NVIDIA CUDA, SageMath».

Литература

1. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12–2015 [Электронный ресурс]. – Режим доступа: http://tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf, свободный (дата обращения: 04.04.2018).

2. Ishchukova E.A. Fast Implementation and Cryptanalysis of GOST R 34.12-2015 Block Ciphers / E.A. Ishchukova, L.K. Babenko, M.V. Anikeev // 9th International Conference on Security of Information and Networks SIN 2016. – Newark, Nj: 20–22 July 2016. – P. 104–111. – URL: https://dl.acm.org/citation.cfm?doid=2947626.2947657

3. Biham E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology 1991. – Vol. 4, No. 1. – PP. 3–72. – URL: http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Biham-DC.pdf

4. Biham E. Differential cryptanalysis of the full 16-round DES / E. Biham, A. Shamir // Advances in cryptology, proceedings of CRYPTO'92 1992. – Vol 740. – PP. 487–496. (URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.215&rep=rep1&type=pdf)

5. Biham E. Differential Cryptanalysis in Stream Ciphers / E. Biham, O. Dunkelman // Cryptology ePrint Archive, Report 2007/218 2007. – URL: https://eprint.iacr.org/2007/218.pdf

6. Biham E. Differential Cryptanalysis of Hash Functions / E. Biham, A. Shamir // Differential Cryptanalysis of The Data Encryption Standard, Springer 1993. – P. 133–148. – URL: https://link.springer.com/chapter/10.1007/978-1-4613-9314-6_8

7. Бабенко Л.К. Применение методов криптоанализа для исследования стойкости современных блочных шифров / Л.К. Бабенко, Е.А. Мишустина (Ищукова) // Тезисы докл. X Всерос. науч. конф. «Проблемы информационной безопасности в системе высшей школы». – М.: МИФИ, 2003. – URL: http://cyberrus.com/wp-content/uploads/2015/05/vkb_10_02.pdf

8. Кузнечик (шифр) [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Кузнечик_(шифр), свободный (дата обращения: 04.04.2018).

9. Толоманенко Е.А. Программная реализация шифра «Кузнечик» // Матер. IX Междунар. студ. электрон. науч. конф. «Студенческий научный форум». – 2017. Актуальные проблемы информационной безопасности. – URL: https://www.scienceforum.ru/2017/pdf/36883.pdf

10. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002. – 648 с. – URL: https://htrd.su/wiki/_media/zhurnal/2012/03/23/todo_prikladnaja_kriptografija/cryptoshn.pdf

11. В ГОСТе сидел «Кузнечик» [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/266359/, свободный (дата обращения: 04.04.2018).

12. Дифференциальный криптоанализ [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Дифференциаль-ный_криптоанализ, свободный (дата обращения: 04.04.2018).

13. Ищукова Е.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147–89 / Е.А. Ищукова, И.А. Калмыков // Инженерный вестник Дона. – 2015. – №4. – URL: https://cyberleninka.ru/article/n/differentsialnye-svoystva-s-blokov-zameny-dlya-algoritma-gost-28147-89).

14. Бабенко Л.К. Дифференциальный анализ шифра «Кузнечик» / Л.К. Бабенко, Е.А. Ищукова, Е.А. Толоманенко // Изв. ЮФУ. Технические науки. – Таганрог: Изд-во ЮФУ, 2017. – №5. – С. 25–37. – URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2017/5/3.pdf

15. Бабенко Л.К. Анализ современных криптографических систем с помощью метода дифференциального криптоанализа / Л.К. Бабенко, Е.А. Ищукова // Актуальные аспекты защиты информации в Южном федеральном университете. – Таганрог: ТТИ ЮФУ, 2011. – С. 102–181.

Толоманенко Екатерина Алексеевна
Аспирантка 1-го года обучения
каф. безопасности информационных технологий (БИТ),
Инженерно-технологической академии
Южного федерального университета (ИТА ЮФУ)
Чехова ул., д. 2, г. Таганрог, Россия, 347928
Тел.: +7 (863-4) 37-19-05, +7-908-504-73-92
Эл. почта: kat.tea@mail.ru

Tolomanenko E.A.

Differential analysis of three rounds of cipher «Kuznyechik»

«Kuznyechik» is a new symmetric encryption algorithm, adopted as an encryption standard GOST R 34.12–2015, built on the principle of SP-network. There are still no publications on the differential properties of the algorithm «Kuznyechik». In this paper, the properties of the main operations are researched and described, and a method of differential analysis of three rounds of the algorithm of encryption «Kuznyechik» is proposed. In the issue of the investigation of the differential properties of the nonlinear function *S* and linear function *L*, it was established that a 1 non-zero byte of the difference as a result of the function *L* can be expanded into 16 non-zero bytes, passes through the replacement block *S*, and then folded again into 1 nonzero byte. The developed scheme allows to

affect the active *S*-unit a minimum number of times. Thus, the overall complexity of the analysis, including searching for the correct pairs of texts and searching for bits of the secret encryption key is $2^{108} + 6 * 2^{120}$ encryptions.

Keywords: cryptography, block cipher, SP-network, cryptanalysis, differential cryptanalysis, cipher «Kuznyechik», GOST R 34.12-2015.

doi: 10.21293/1818-0442-2018-21-2-22-26

References

1. Cryptographic protection of information. Block ciphers. GOST R 34.12–2015. Available at: http://tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf (accessed: 04 April 2018).

2. Ishchukova E.A., Babenko L.K., Anikeev M.V. Fast Implementation and Cryptanalysis of GOST R 34.12–2015 Block Ciphers. *9th International Conference on Security of Information and Networks SIN 2016.* Newark, Nj, 2016. pp. 104–111. URL: https://dl.acm.org/citation.cfm?doid=2947626.2947657

3. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 1991, vol. 4, no. 1, pp. 3–72. URL: http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Biham-DC.pdf

4 Biham E., Shamir A. Differential cryptanalysis of the full 16-round DES. *Advances in cryptology*. Proc. of CRYPTO'92 conference? 1992? vol. 740, pp. 487–496? URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.215&rep=rep1&type=pdf

5. Biham E., Dunkelman O. Differential Cryptanalysis in Stream Ciphers. *Cryptology ePrint Archive*, Report 2007/218 2007. – URL: https://eprint.iacr.org/2007/218.pdf

6. Biham E., Shamir A. Differential Cryptanalysis of Hash Functions. Differential Cryptanalysis of The Data Encryption Standard. *Springer,* 1993, pp. 133–148. URL: https://link.springer.com/chapter/10.1007/978-1-4613-9314-6_8

7. Babenko L.K., Ishchukova E.A. Primenenie metodov kriptoanaliza dlya issledovania stoikosti sovremennikh blochnikh shifrov [The use of cryptanalysis methods to study the persistence of modern block ciphers]. Problemi informacionnoy bezopasnosti v sisteme vishchey shkoli. Tezisi dokladov X Vserossiyskoy nauchnoy conferencii [*The problems of information security in the system of higher education.* Proc. of the tenth AllRussian scientific conference]. Moscow, MIFI, 2003. URL: http://cyberrus.com/wp-content/uploads/2015/05/vkb_10_02.pdf

8. Kuznyechik (cipher). Available at: https://ru.wikipedia.org/wiki/Кузнечик_(шифр) (accessed: 04 April 2018).

9. Tolomanenko E. A. Programnaya realizaciya shifra Kuznyechik [Software implementation of the cipher Kuznyechik]. Studencheskiy nauchniy forum. Materiali IX mezhdunarodnoy studencheskoy elektronnoy nauchnoy konferentsii. [*Student Science Forum*. Proc. of ninth International Student Electronic Scientific Conference]. 2017. URL: https://www.scienceforum.ru/2017/pdf/36883.pdf

10. Schneier B. *Prikladnaya kriptografiya: Protocoli, algoritmy, iskhodnyye teksty na yazyke Ci* [Applied cryptography: Protocols, algorithms, C source code]. Moscow, TRIUMPH, 2002. 648 p. URL: https://htrd.su/wiki/_media/ zhurnal/2012/03/23/todo_prikladnaja_kriptografija/cryptoshn.pdf

11. In the GOST there was a «Kuznyechik». Available at: https://habrahabr.ru/post/266359/ (accessed: 04 April 2018).

12. Differential cryptanalysis. Available at: https://ru.wikipedia.org/wiki/Дифференциальный_криптоанализ (accessed: 04 April 2018).

13. Ishchukova E.A., Kalmikov I.A. Differential properties of S-replacement blocks for the algorithm GOST 28147-89. *The engineer's messenger of the Don*, 2015, no 4. – URL: https://cyberleninka.ru/article/n/differentsialnye-svoystva-s-blokov-zameny-dlya-algoritma-gost-28147-89

14. Babenko L.K., Ishchukova E.A., Tolomanenko E.A. Differential analysis of cipher Kuznyechik. *News of SFedU. Technical science*. Taganrog, Publishing house SFedU, 2017, no. 5, pp. 25–37. URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2017/5/3.pdf

15. Babenko L.K., Ishchukova E.A. *Analiz sovremennykh kriptograficheskikh sistem s pomoshch'yu metoda differentsial'nogo kriptoanaliza* [Analysis of modern cryptographic systems using differential cryptanalysis]. Topical aspects of information security in the Southern Federal University, 2011, Taganrog, TTI SFedU, pp. 102–181.

Ekaterina A. Tolomanenko
PhD student,
Department of Security of Information Technologies
Engineering and Technology Academy
of the Southern Federal University
2, Chekhova st., Taganrog, Russia, 347928
Phone: +7 (863-4) 37-19-05, +7-908-504-73-92
Email: kat.tea@mail.ru

УДК 621.396.41

Д.А. Антипов

Анализ утечек информации на основе побочных электромагнитных излучений

Приведён систематизированный обзор исследований, посвященных каналу утечки информации через побочное электромагнитное излучение. По результатам обзора сделаны выводы об актуальности исследований в части снижения угроз утечки информации через побочное электромагнитное излучение. В частности, показано, что перспективным направлением является изучение направленности излучения. Выявлено преобладание программных способов устранения утечек над аппаратными, а также недостаток реализаций аппаратных решений.
Ключевые слова: защита информации, ПЭМИ, ОТСС, генераторы электромагнитного шума, съём информации, мягкий ПЭМИН.
doi: 10.21293/1818-0442-2018-21-2-27-32

Создание надежных систем обеспечения информационной безопасности является ключевым аспектом при проектировании комплексных систем безопасности [1, 2]. Это подтверждает необходимость общесистемного подхода при анализе рисков и оценке угроз безопасности, а также выявлении технических каналов утечки информации и обеспечения их надёжной защиты [3].

Канал утечки информации через побочное электромагнитное излучение (ПЭМИ) является одним из самых актуальных технических каналов утечки [4]. При обработке информации с помощью основных технических средств (ОТСС) неизбежно возникает ПЭМИ, несущее в себе информативный сигнал [5, 6].

Работа по защите канала утечки информации осуществляется на основе нормативных документов регуляторов, а также федеральных законов. В них описаны не только требования к информационным системам и их составляющим, но и методики оценки защищённости информации.

Основное направление исследований, посвящённых источникам ПЭМИ, излучающим информационный сигнал при использовании автоматизированных рабочих мест (АРМ), являются уязвимости экранов, жестких дисков и USB-устройств. Другие источники также изучаются, однако на практике уровень излучения от них мал, и утечка не реализуется.

Канал утечки информации традиционно делится на 3 составляющие (рис. 1):

1. Источник сигнала, под которым понимается любое радиоэлектронное устройство. Чаще рассматриваются источники, реализация угроз от которых экспериментально подтверждена.
2. Среда передачи (воздух, проводящие материалы и линии связи).
3. Устройство съёма информации, которое, как правило, включает блок обработки информации.

Области научных исследований можно условно разделить на 4 большие категории:

1. Исследования, связанные с обработкой сигнала, происходящей после съёма информации. Знания о структуре принимаемого сигнала упрощают процедуру его восстановления.
2. Исследования, связанные с источником ПЭМИ. В них речь идёт о переосмыслении характеристик и физики ПЭМИ от известных источников, а также о способах снижения уровня излучения.
3. Средства защиты информации, активные – генераторы электромагнитного шума и пассивные – экранирующие материалы. Основной темой исследования здесь выступают анализ излучения генераторов шума и решения по оптимизации их параметров.
4. Моделирование канала утечки. В этих работах показывается несостоятельность существующей классической модели канала утечки, а также предлагаются модели и способы оценки защищённости. Кроме того, рассматриваются потенциальные новые проявления канала утечки.

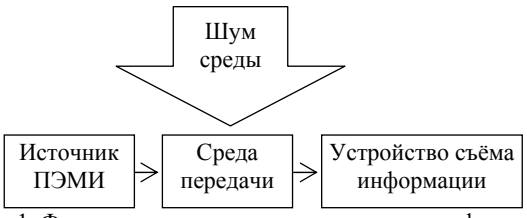


Рис. 1. Функциональная схема канала утечки информации

Обработка сигнала

В статье [7] говорится о том, что реализация утечки от монитора является более вероятной, чем это принято считать. Информативный сигнал восстанавливается с помощью статистической обработки на основе знаний о форме и периодичности сигнала. Проведённый эксперимент показал возможность реализации угрозы утечки на расстоянии 46 м от источника излучения.

Так как передача информации по шине USB тоже является дискретным случайным процессом с точки зрения съёма информации, а характеристики фронтов известны заранее, то можно использовать математический аппарат для восстановления информативного сигнала из смеси «сигнал+шум» [8]. В результате исследования авторы представили модель, которая позволила повысить возможность восстановления информативного сигнала на 3–6 дБ в зависимости от типа присутствующих помех.

Способ оценки защищённости предложен в работе [9]. Этот способ основан на расчёте информационной ёмкости канала, которая рассчитывается на основе проведённых измерений. Полученная ёмкость канала сравнивается с его пропускной способностью, которая рассчитывается на основе характеристик устройства. Если ёмкость канала утечки информации больше рассчитанной пропускной способности, можно говорить о риске реализации утечки.

Подход [10] также заслуживает внимания. Автор [10] руководствуется формулой Шеннона–Хартли, позволяющей оценить пропускную способность канала передачи данных. Учитывая соотношение «сигнал/шум», производится её пересчёт, что выражается в максимальном разрешении изображения, которое способен перехватить злоумышленник. Уменьшение разрешения экрана при работе способно повысить защищённость, так как его будет сложнее восстановить. Однако автор [10] не учитывает особенности сигналов и шума, а также отсутствуют экспериментальные подтверждения приведённым рассуждениям, что затрудняет оценку их достоверности.

Средства защиты информации

В работе [11] описана техническая реализация режекторного фильтра, позволяющего генератору электромагнитного шума (ГЭШ) осуществлять селективное зашумление. Такое решение позволяет создать «окно» в спектре ГЭШ, в котором может работать гражданское устройство, не испытывая на себе действие генератора. Кроме того, разработанное устройство обладает возможностью подстройки частоты режекции в пределах 10–20 МГц.

В работах [12, 13] расширяется этот подход. Однако из-за технических трудностей диапазон частот, на которые может быть настроен этот режекторный фильтр, имеет ограничения по ширине и не может лежать в области высоких частот. Это делает такой подход неприменимым на практике, ведь большинство информационных сигналов лежат в полосе от 100 МГц и выше.

Работа [14] посвящена изучению эффективности применения структурных помех. Автор утверждает, что имитирующая помеха позволяет снизить общий уровень излучаемой мощности без потерь в защищённости. Также предложена модель оценки эффективности таких помех.

Работа [15] посвящена проблемам маскирования ПЭМИ. К проблемам построения адаптивных ГЭШ автор [15] походит иначе. Суть его исследований в возможности генерирования шумоподобной помехи, используя как несущую квазигармонический сигнал, модулируя его низкочастотным сигналом. На определённой частоте имеется возможность установить помеху, которая будет обладать лучшими характеристиками зашумления по сравнению с привычным шумом от ГЭШ.

Один из основных недостатков ГЭШ, существующих в настоящее время и широко обсуждаемый сообществом, – это недостаточная полоса зашумления. В работе [16] рассматриваются современные интерфейсы передачи изображения. Видовая информация, или информация, перехватываемая с экрана АРМ, обладает наибольшей информативностью для злоумышленника. Согласно полученным результатам в работе [16], частоты первой гармоники некоторых цифровых интерфейсов передачи изображения могут выходить за 2 ГГц, что оставляет возможность для реализации уязвимости из-за технических характеристик некоторых ГЭШ.

В работе [17] автор представляет оценку эффективности маскирования сигнала подобным ему шумом. Сигнал ПЭМИ сначала записывается, а затем излучается в пространство как шумоподобная помеха. Из-за высокой схожести этих сигналов друг с другом задача по их различению и выделению информативного сигнала усложняется. Оценке возможности этого восстановления и посвящена работа [17].

В работе [18] также обращается внимание на возможность повысить защищённость, манипулируя формой шумового сигнала путём создания помехи компенсационного типа. Реализованная селекция приёма ПЭМИ в устройствах снятия информации делает ГЭШ неэффективными из-за различий между структурой информационного сигнала и шума. Предлагается реализовывать защиту в виде ретрансляторов, устанавливаемых непосредственно в близости устройства, излучающего ПЭМИ. Принимая ПЭМИ, обрабатывая его и излучая компенсационный шум, можно добиться высокого уровня защиты при минимально возможном уровне излучаемой мощности. Для развязки приёмного и передающего трактов у ретранслятора рекомендуется применять направленные антенны, которые ориентируются в сторону предполагаемого размещения устройства съёма информации.

В работе [19] авторы отмечают недостатки активных средств защиты информации, такие как вредность высокого уровня излучения для здоровья. Электромагнитный шум является демаскирующим признаком работы ГЭШ, что привлекает интерес злоумышленников к объекту. Кроме того, активный метод защиты информации (ЗИ) не обеспечивает гарантированную защиту от перехвата информации. Сам перехват, по мнению авторов [19], можно совершить с помощью доступного лабораторного оборудования, такого как анализатор спектра, антенна и средство обработки цифровых сигналов.

Моделирование канала утечки

Авторы [20] строят модель функционирования канала утечки информации. Рассматривается структура технического канала, в которой показывается набор элементов, участвующих в нём. Такая модель позволяет оценивать защищённость системы на этапе планирования мероприятий по её защите. Кроме того, результаты работы являются базой для дальнейших исследований составных элементов канала утечки.

В работе [21] выдвинуто предложение по коррекции расчёта коэффициента затухания. Показано,

что при правильной оценке коэффициента ослабления можно получить результаты, отличающиеся от классического подхода. Для расстояния от точки излучения в 30 и 50 см – 30 и 34 дБ соответственно.

Также обсуждается и тестовый режим работы средства вычислительной техники [22]. По мнению автора [22], эта тема приобретает актуальность в связи с переходом от аналоговых сигналов к цифровым. Цифровой сигнал обладает особыми характеристиками. Это связано с кодированием информации, а также с различной структурой протоколов обмена информации.

В работе [23] показывается возможность реализации оптического канала утечки информации от индикационных светодиодов таких устройств, как жёсткие диски, сетевые карты и др. Этот канал авторы называют «optical TEMPEST» и экспериментально доказывают возможность перехвата информативного оптического излучения. Хотя канал и не обладает электромагнитной природой распространения, он имеет право быть отнесённым к группе каналов утечки, связанной с побочным излучением. В данном случае излучение является оптическим.

Источники сигнала

Вариация программного способа защиты видовой информации предлагается в [24]. Так как цифровой сигнал монитора состоит из блоков данных, кодирующих цвет каждого пикселя по формату RGB, то авторы [24] предлагают оставить информационным только один цветовой канал, а на других двух генерировать шум. Пользователь может настроить у монитора фильтр цветовых каналов, чтобы его не отвлекал их шум от работы. Рассматриваются различные способы манипуляции уровнем сигнала цветовых каналов, а также делается вывод о продуктивности такого способа обеспечения информационной безопасности.

Угроза утечки информации по шине данных USB распространяется даже на линии, по которым не передаётся информативный сигнал, демонстрируется в работе [25]. Из-за близости разъёмов USB в одном USB-хабе информативный сигнал одних разъёмов может наводиться на линии других незадействованных разъёмов.

Перехват информации от жёсткого диска, согласно исследованию [26], затруднён из-за слабого уровня сигнала. Это происходит, даже если используются специальные последовательности сигналов для максимизации амплитуд сигналов. Автор утверждает, что для защиты информации от жестких дисков можно обойтись пассивными мерами: экранированием и заземлением АРМ. Хотя некоторые исследования показывают [27], что канал утечки реализуем.

Большой вклад в исследование сигналов принадлежит Markus G. Kuhn. Основная часть его работ [28–31] посвящена перехвату сигнала от мониторов. Ранние его публикации описывают перехват сигнала мониторов с электронно-лучевыми трубками (ЭЛТ), но в поздних работах возможность перехвата сигнала опытно доказана и для ЖК-мониторов. Суть его исследований – в оценке угрозы перехвата информации, исследования частотных характеристик ПЭМИ, а также способах снизить риски реализации этого канала перехвата информации.

Оценивается угроза перехвата по распространению электромагнитных волн и по излучаемой энергии. Согласно [28], можно снизить угрозу, расширив контролируемую зону так, чтобы сигнал от монитора снизился до невозможности его восстановления. Можно влиять на уровень излучаемой энергии, управляя информацией, выводимой на экран. Специальным способом окрашивая пиксели, можно сгладить пики излучения, что затруднит восстановление цифрового сигнала.

В работе [32] отмечается, что недостаточное внимание уделено источникам ПЭМИ, находящимся внутри устройства. Большинство исследований направлено на изучение работы соединительных интерфейсов. Было получено информативное ПЭМИ от блока лазерного принтера. Это стало возможным благодаря доработке этого блока, повышающей уровень побочного излучения. Фактически ПЭМИ может быть снято, но вероятность реализации такой угрозы крайне мала ввиду сложности выполнения.

Автор [33] рассматривает применимость пассивных средств защиты, анализируя возможность применения специальных экранирующих тканей. Обладающие высокими показателями экранирования, они могут использоваться вместе с ГЭШ. При этом предполагается, что ГЭШ будут работать на частотах до 1 ГГц, а распространение сигналов более высоких частот будут останавливаться тканями. Как показывают опыты [33], на частотах ниже 1 ГГц ткани не обеспечивают требуемую величину экранирования из-за своих физических свойств.

В работе [34] предложен схожий пассивный метод защиты. Он заключается во внедрении в резиновые материалы односторонних углеродных (карбоновых) нанотрубок. Такой материал обеспечивает поглощение 90% мощности сигнала в СВЧ-частотах.

Правильный выбор материалов для изготовления кабелей может значительно снизить излучаемый уровень шума в диапазоне 2–150 кГц. В работе [35] исследуются характеристики нанокристаллического феррита и его способность повышать электромагнитную совместимость с другими источниками сигналов этого диапазона частот.

Исследования [36] посвящены видовому каналу утечки информации. В работе [36] рассмотрена возможность восстановления изображения монитора по отражению от прочих поверхностей – зрачка глаза, бытовых предметов.

Выделяется также Soft TEMPEST, или «мягкое» ПЭМИ. Основная особенность данной вариации канала утечки в том, что на АРМ устанавливается специальное ПО для усиления ПЭМИ путём обращения к диску, при этом обращение производится именно к той информации, которая представляет ценность для злоумышленника. Soft TEMPEST также включает в себя и ПО, которое осложняет либо предотвращает

утечку. Изменяя отображаемые шрифты на экране, можно сделать ПЭМИ более стойкими к перехвату.

Заключение

Проведенный анализ исследований позволяет сделать следующие выводы:

1. Некоторые проблемы обеспечения защиты информации, возникающие из-за высокого уровня ПЭМИ от устройств в составе ОТСС, могут быть решены программным способом. Такой подход предпочтителен использованию активных средств защиты, так как является пассивным и не требует дополнительного оборудования. Пассивная защита от утечки через ПЭМИ разгружает радиодиапазон по сравнению с активными средствами постановки помехи.

2. Подходы к оптимизации работы активных средств защиты показывают свою эффективность в модели, но зачастую не имеют подтверждённой технической реализации.

3. Модель канала утечки, изложенная в нормативных документах регуляторов, обладает рядом недостатков, влияющих на точность оценки защищённости информации от утечки. Рассматривая источники излучения как систему радиоэлектронных устройств, можно точнее оценивать степень воздействия каждого элемента на защищённость информации.

4. Из-за перехода от аналоговой техники к цифровой происходит переоценка распространения сигналов. Ей подвергаются все характеристики сигнала, влияющие на возможность перехвата и восстановления информации. Однако недостаточно внимания уделяется направленности излучения информации. Работа [12] показывает, что использование информации о направленности расширяет возможности обеспечения защиты информации.

Учитывая внедряемость и практическую значимость результатов, можно выделить перспективные направления исследования:

- Программное изменение функционирования устройств, в том числе протоколов обмена информацией, что позволяет снизить уровень ПЭМИ.
- Разработка материалов, снижающих излучаемый уровень ПЭМИ.
- Глубокий анализ канала утечки, где каждый элемент рассматривается в системе с другими, а именно влияние элементов друг на друга. Благодаря системному подходу открываются новые аспекты канала утечки, представляющие угрозу защищённости информации.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУРа на 2017–2019 гг. (проект № 2.8172.2017/8.9).

Литература

1. Шелупанов А.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / А.А. Шелупанов, С.А. Лопарев // Вопросы защиты информации. – 2003. – С. 2–5.

2. Шелупанов А.А., Системный анализ в защите информации / А.А. Шелупанов, А.А. Шумский. – М: Гелиос, 2005. – 224 с.

3. Лось В.П. Основы информационной безопасности / В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов, Е.Б. Белов. – М.: Горячая линия – Телеком, 2006. – 544 с.

4. Мещеряков Р.В. Технические средства и методы защиты информации. – 7-е. изд. – М.: Горячая линия – Телеком, 2012. – 442 с.

5. Шелупанов А.А. Технические средства и методы защиты информации / А.А. Шелупанов, Р.В. Мещеряков, С.В. Скрыль, А.П. Зайцев. – М.: ООО «Изд-во Машиностроение», 2009. – 508 с.

6. Тимченко С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Тимченко, А.А. Шелупанов, С.В. Прищеп // Безопасность информационных технологий. – 2007. – С. 15–21.

7. Ugur Sarac Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system /. Ugur Sarac, Isin Erer Furkan Elibol // EUSIPCO 2012. – Buharest, august 2012. – PP. 1767–1771.

8. Соколов Р.И. Исследование системы синхронизации при восстановлении сигналов ПЭМИ USB-клавиатуры в условиях индустриального шума / Р.И. Соколов, Д.В. Астрецов // Изв. Самар. нНауч. центра Российской академии наук. – 2016. – № 18, вып. 2-3.– С. 881–885.

9. Tanaka H. Evaluation of information leakage via electromagnetic emanation and effectiveness of Tempest // Ieice Trans. Inf. & Syst. – № E91-D, Is. 5. – May 2008. – PP. 1439–1447.

10. Жалковский И.В. Определение энергетического критерия оценки защищённости информации от утечки по каналу побочных электромагнитных излучений // Докл. Белорус. гос. ун-та информатики и радиоэлектроники. – 2015, вып. 3 (89). – С. 107–111.

11. Урбанович П.В. Средство формирования шумовой электромагнитной помехи / П.В. Урбанович, Н.Т. Югов, А.А. Шелупанов // Научный вестник Новосиб. гос. техн. ун-та. – 2012. – С. 121–126.

12. Шелупанов А.А. Определение режимов для формирования полос частот средств активной защиты / А.А. Шелупанов, Н.Т. Югов, П.В. Урбанович // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 78–81.

13. Урбанович П.В. Генератор шума с подстройкой диапазонов // Доклады ТУСУРа. – 2008. – № 2 (18), ч. 1. – С. 9–11.

14. Егин А.В. Применение структурных и шумовых помех для защиты информации от утечки по каналу побочных электромагнитных излучений / А.В. Егин, С.А. Святкин, А.В. Паршуткин // Вопросы оборонной техники. Сер. 16: Технические средства противодействия терроризму. – 2016. – С. 27–34.

15. Землянухин П.А. Многоканальный адаптивнй генератор шума для маскирования ПЭМИН // Изв. ЮФУ. Технические науки. – 2016. – Сент. – С. 82–93.

16. Слободчиков А.А. Побочные электромагнитные излучения интерфейсов LVDS, DVI, HDMI // Безопасность информационного пространства / Сб. матер. XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. – Курган – 2016. – Дек.– С. 239–242.

17. Петров И.С. оценка энергетической эффективности метода формирования маскирующих помех путём записи/воспроизведения сигналов ПЭМИ от СВТ // Технологический ин-т ФГОУ ВПО «Южный федеральный университет». – Таганрог, 2010. – Вып. 14. – С. 171–175.

18. Богаченков К.Н. Особенности создания помех компенсационного типа для решения задач защиты

информации от утечки по техническим каналам / К.Н. Богаченков, П.А. Маслаков, В.В. Вознюк // Труды военно-космической академии им. А.Ф. Можайского. – 2015. – Вып. 646. – С. 83–92.

19. Семенов А.В. Утечка информации по каналам ПЭМИ и способы их защиты / А.В. Семенов, Н.В. Киреева // Международный журнал прикладных и фундаметальных исследований. – 2016. – Вып. 8-4. – С. 499–504.

20. Авсентьев А.О. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации / А.О. Авсентьев, А.Г. Вальде, О.С. Авсентьев // Вестник Воронеж. ин-та МВД России. – 2017. – С. 22–31.

21. Катруша А.Н. Оценка уровней побочных электромагнитных излучений на основе измерений в ближней зоне технического средства // Новая наука: от идеи к результату. – 2016. – С. 100–102.

22. Рыженко С.В. К вопросу о побочных электромагнитных излучениях современных интерфейсов средств вычислительной техники // Актуальные проблемы обес-печения информационной безопасности. – 2017. – С. 170–176.

23. David A. Umphress, Joe Loughry Information leakage from optical emanations // ACM Transactions on Information and System security. – August 2002. – № 5, Is. 3. – PP. 262–289.

24. Мищенко Д.А. Защита информации от утечки через побочные электромагнитные излучения видеосистемы компьютера / Д.А. Мищенко, Д.И. Железнов // Науч.-практ. электрон. журнал. Аллея науки. – 2017. – Вып. 10.

25. Daniel Genkin, Yuval Yarom, Damith Ranasinghe Yang Su USB Snooping Made easy: Crosstalk Leakage Attacks on USB Hubs // Матер. конф. «26th USENIX Security Symposium». – Vancouver, BC, Canada, 2017. – PP. 1145–1161.

26. Мельшиян М.А. Исследование возможности перехвата побочных электромагнитных излучений жестких дисков // Электрон. науч. журнал. – Июнь 2016. – Вып. № 5 (8). – С. 112–114.

27. Баюшкин С.С. Исследование возможности перехвата побочных электромагнитных излучений HDD ПЭВМ / С.С. Баюшкин, И.Ю. Назаров // Технологии XXI века: проблемы и персепктивы развития: сб. ст. Междунар. науч.-практ. конф. – Июнь 2017. – Пенза. – Вып. 2, ч. 2. – С. 22–26.

28. Markus G. Kuhn. Compromising emanations: eavesdropping risks of computer displays / University of Cambridge. – Cambridge: Technical Report UCAM-CL-TR-577, 2003.

29. Markus G. Kuhn Electromagnetic Eavesdropping Risks of Flat-Panel Displays // 4th Workshop on Privacy Enhancing Technologies. – Toronto, Canada, 2004. – PP. 88–107.

30. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays // Proceedings 2002 IEEE Symposium on Security and Privacy, Berkley, California, 12–15 May 2002. IEEE Computer Society. – Berkeley, California, USA. – May 2002. – PP. 3–18.

31. Markus G. Kuhn Security Limits for Compromising Emanations // CHES 2005. – 2005, Edinburgh, UK. – P. 265–279.

32. Дириенко Е.В. Исследование возможности получения информации с печатающего блока лазерного принтера по каналу ПЭМИ / Е.В. Дириенко, А.А. Голяков // Безопасность информационных технологий. – 2015. – С. 25–32.

33. Петигин А.Ф. Применение радиоэкранирующих тканей для защиты информации от утечки за счёт побочных электромагнитных излучений // REDS: Телекоммуникационные устройства и системы. – 2015. – №5, вып. 4. – С. 428–431.

34. Masahiro Horibe, Seisuke Ata, Takeo Yamadab, Kenji Hatab Yuto Kato Stretchable electromagnetic-interference shielding materials made of a long single-walled carbon-nanotube-elastomer composite // The Royal Society of Chemistry. – Feb. 2017. – PP. 10841–10847.

35. Jorge Victoria, Antonio Alcarria Adrian Suarez Characterization of Different Cable Ferrite Materials to Reduce the Electromagnetic Noise in the 2–150 kHz Frequency Range // MDPI. – Jan. 2018. – PP. 1–20.

36. Markus Durmuth, Dominique Unruh Michael Backes. Compromising reflections or how to read LCD monitors around the corner // 2008 IEEE Symposium on Security and Privacy. – Saarbrucken, Germany, 2008. – PP. 158–169.

Антипов Денис Александрович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-983-345-93-68
Эл. почта: antipodp@gmail.com, antipodya@yandex.ru

Antipov D.A.

Analysis of information leaks based on spurious electromagnetic emissions

This systematic review of the research devoted to the channel of information leakage through secondary electromagnetic radiation is given. Based on the results of the survey, conclusions were drawn about the relevance of research in reducing the risks of information leakage through spurious electromagnetic radiation. In particular, it has been shown that the direction of radiation is a promising direction. The predominance of software methods for eliminating leaks over hardware was identified, as well as a lack of hardware implementations.
doi: 10.21293/1818-0442-2018-21-2-27-32

References

1. Shelupanov A.A., Loparev S.A. *Analiz instrumental'nyh sredstv ocenki riskov utechki informacii v komp'yuternoj seti predpriyatiya* [Analysis of tools for assessing the risks of information leakage in an enterprise computer network]. Questions of information protection, 2003, pp. 2–5.

2. Shelupanov A.A., Shumsky A.A. *Sistemnyj analiz v zashchite informacii* [System analysis in the protection of information]. Moscow: Helios, 2005, 224 p.

3. Los V.P., Meshcheryakov R.V., Shelupanov A.A., Belov E.B. *Osnovy informacionnoj bezopasnosti* [Information security basics]. Moscow: Hot line – Telecom, 2006, 544 p.

4. Meshcheryakov R.V., Shelupanov A.A., Zaitsev A.P. *Tekhnicheskie sredstva i metody zashchity informacii* [Technical means and methods of information protection]. 7th edition, Moscow: Hot line – Telecom, 2012, 442 p.

5. Shelupanov A.A., Meshcheryakov R.V., Skryl S.V., Zaitsev A.P. *Tekhnicheskie sredstva i metody zashchity informacii* [Technical means and methods of information protection]. Moscow: OOO «Izdatelstvo Mashinostroenie», 2009, 508 p.

6. Timchenko S.V., Shelupanov A.A., Prishchep S.V. Approaches and criteria for assessing the risks of information security. *The safety of information technology*, 2007, pp. 15–21.

7. Ugur Sarac, Isin Erer, Furkan Elibol, Realistic eavesdropping attacks. *EUSIPCO 2012*, Buharest, august 2012, pp. 1767–1771.

8. Sokolov R.I, Astretsov D.V. Investigation of the synchronization system during recovery of the USB keyboard signals in the conditions of industrial noise. *Izvestiya of Samara Scientific Center*, Russian Academy of Sciences, no. 18, iss. 2-3, 2016, pp. 881–885.

9. Tanaka H. Evaluation of information leakage via electromagnetic emanation and effectiveness of Tempest. *IEICE TRANS. INF. & SYST*, no. E91-D., iss. 5, May 2008, pp. 1439–1447.

10. Zhalkovsky I.V. Determination of the energy criterion for estimating the security of information from leakage through the channel of spurious electromagnetic radiation. *Reports of the Belarusian State University of Informatics and Radioelectronics*. vol. 3 (89), 2015, pp. 107–111.

11. Urbanovich P.V., Yugov N.T., Shelupanov A.A. Means of formation of noise electromagnetic interference. *Scientific Bulletin of Novosibirsk State Technical University*, 2012, pp. 121–126.

12. Shelupanov A.A., Yugov N.T., Urbanovich P.V. Determination of regimes for the formation of frequency bands of active protection means. *Reports of TUSUR*, No. 1 (21), part 1, June 2010, pp. 78–81.

13. Urbanovich P.V. The noise generator with tuning of ranges. *Proceedings of TUSUR University*, No. 2 (18), part 1, June 2008, pp. 9–11.

14. Egin A.V., Sviatkin S.A., Parshutkin A.V. Application of structural and noise interference to protect information from leakage through the channel of spurious electromagnetic radiation. *Questions of defensive technology*. Series 16: Technical Countermeasures to Terrorism, 2016, pp. 27–34.

15. Zemlyanukhin P.A. Multichannel adaptive noise generator for masking PEMIN. *Izvestiya SFU. Technical science*, September 2016, pp. 82–93.

16. Slobodchikov A.A. Side-by-side electromagnetic emissions of LVDS, DVI, and HDMI interfaces. *Information Space Security. Collected materials of the XV All-Russian scientific-practical conference of students, graduate students and young scientists*, Kurgan, December 2016, pp. 239–242.

17. Petrov I.S. Estimating the energy efficiency of the method of forming masking interference by recording / reproducing PEMI signals from SVT. *Technological Institute of the Federal State Educational Institution of Higher Professional Education «Southern Federal University»*. Taganrog, no. 14, 2010, pp. 171–175.

18. Bogatchenkov K.N., Maslakov P.A., Voznyuk V.V. Features of creation of jamming of the compensating type for solving problems of information protection from leakage through technical channels. *Proceedings of the Military Space Academy,* no. 646, 2015, pp. 83–92.

19. Semenov A.V. Kireeva N.V. The leakage of information through the PEMI channels and ways to protect them. *International Journal of Applied and Fundamental Research*, no. 8-4, 2016, pp. 499–504.

20. Avsentiev A.O., Valde A.G., Avsentiev O.S. Investigation of the conditions for the emergence of technical information leakage channels for secondary electromagnetic radiation at information objects. *Vestnik Voronezhskogo Institute of the Ministry of Internal Affairs of Russia,* 2017, pp. 22–31.

21. Katrusha A.N., Estimation of the levels of spurious electromagnetic radiation based on measurements in the near zone of a technical device. *New Science: From Idea to Result,* 2016, pp. 100–102.

22. Ryzhenko S.V. To the question of secondary electromagnetic radiation of modern interfaces of computer facilities. *Actual problems of information security,* 2017, pp. 170–176.

23. David A. Umphress, Joe Loughry. Information leakage from optical emanations. *ACM Transactions on Information and System security*. No 5., Iss. 3, august 2002, pp. 262–289.

24. Mishchenko D.A., Zheleznov D.I. Protection of information from leakage through secondary electromagnetic radiation of the computer's video system. *Scientific and practical electronic journal Science Alley*, no. 10, 2017.

25. Daniel Genkin, Yuval Yarom, Damith Ranasinghe Yang Su USB Snooping Easily: attacks on crosstalk leakage on USB hubs. *Proceedings of the conference «26th Symposium on USENIX Security»*. Vancouver, British Columbia, Canada, 2017, pp. 1145–1161.

26. Mel'shiyan M.A. Investigation of the possibility of interception of spurious electromagnetic radiation of hard disks. *Electronic scientific journal*, No. 5 (8), June 2016, pp. 112–114.

27. Bayushkin S.S., Nazarov I.Y. Investigation of the possibility of interception of secondary electromagnetic radiations HDD. *Technologies of the XXI century: problems and development perspectives. Collection of articles of the International Scientific and Practical Conference*, Penza, Vol 2, p. 2, June 2017, pp. 22–26.

28. Markus G. Kuhn. Compromising emanations: eavesdropping risks of computer displays. University of Cambridge, Cambridge, *Technical Report UCAM-CL-TR-577*, 2003.

29. Markus G. Kuhn. Electromagnetic Eavesdropping Risks of Flat-Panel Displays, *4th Workshop on Privacy Enhancing Technologies*, Toronto, Canada, 2004, pp. 88–107.

30. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays. *Proceedings 2002 IEEE Symposium on Security and Privacy*, Berkley, California, 12–15 May 2002, IEEE Computer Society, Berkeley, California, USA, May 2002, pp. 3–18.

31. Markus G. Kuhn. Security Limits for Compromising Emanations. *CHES 2005*, Edinburgh, UK, 2005, pp. 265–279.

32. Dirienko E.V., Golyakov A.A. Investigation of the possibility of obtaining information from a printing unit of a laser printer via the PEMI channel. *IT Security*, 2015, pp. 25–32.

33. Petigin A.F. The use of radio-shielding fabrics to protect information from a spike due to spurious electromagnetic radiations. *REDS: Telecommunication Devices and Systems*, no. 5, iss. 4, 2015, pp. 428–431.

34. Masahiro Horibe, Seisuke Ata, Takeo Yamadab, Kenji Hatab Yuto Kato. Stretchable electromagnetic-interference shielding materials made of a long single-walled carbon-nanotube-elastomer composite. *The Royal Society of Chemistry*, Feb. 2017, pp. 10841–10847.

35. Jorge Victoria, Antonio Alcarria, Adrian Suarez. Characterization of Different Cable Ferrite Materials to Reduce the Electromagnetic Noise in the 2–150 kHz Frequency Range. *MDPI*, Jan. 2018, pp. 1–20.

36. Markus Durmuth, Dominique Unruh Michael Backes. Compromising reflections or how to read LCD monitors around the corner. *2008 IEEE Symposium on Security and Privacy,* Saarbrucken, Germany, 2008, pp. 158–169.

Denis A. Antipov
Post-graduate student. Integrated Information Security of Electronic Computing Systems, Tomsk University of Control Systems and Radioelectronics (TUSUR)
Lenina av., 40, Tomsk, Russia, 634050
Tel.: +7-983-345-93-68
Email: antipodp@gmail.com, antipodya@yandex.ru

УДК 621.396.41

Д.А. Антипов, А.А. Шелупанов

Исследование направленности побочного электромагнитного излучения от персонального компьютера

Исследуется распространение побочного электромагнитного излучения от устройств в составе персонального компьютера. В ходе работы проведены эксперименты, демонстрирующие неравномерные характеристики диаграммы направленности излучения. Приведены расчётные соотношения, позволяющие оценить влияние неравномерности распространения на защищённость информации. Сделан вывод о том, что величина колебаний уровня сигнала, в зависимости от направления излучения, оказывает влияние на защищённость информации.
Ключевые слова: побочное электромагнитное излучение, защита информации, диаграмма направленности, монитор, USB-накопитель.
doi: 10.21293/1818-0442-2018-21-2-33-37

Источником побочного электромагнитного излучения (ПЭМИ) в электронных устройствах являются проводники с протекающим по ним током. Из-за формы и топологии проводников, они могут становиться случайными антеннами, распространяющими электромагнитное излучение (ЭМИ) в пространство [1–7]. На распространение ЭМИ оказывает влияние техническое исполнение электронного устройства [2]. Например, металлический корпус способен действовать как экран, снижая уровень ЭМИ.

Проводники в устройстве являются антеннами, расположенными случайным образом относительно друг друга. Излучение антенн интерферирует между собой. Предполагается, что из-за их несогласованного расположения распределение излучения близко к равномерному. Целью данной работы является исследование распределения ЭМИ от устройств в составе персонального компьютера.

Построение измерительного стенда и расчёт дальности распространения ЭМИ

Для проведения экспериментов, был построен измерительный стенд. Характеристики элементов стенда и процедура съёма уровней сигнала соответствуют методике специальных исследований побочных электромагнитных излучений

Измерительный стенд включает в себя:

- широкополосный спектральный анализатор R&S FSC-3;
- антенну дипольную активную «АИ5-0»;
- автоматизированное рабочее место (АРМ), состоящее из системного блока, монитора, клавиатуры и мыши;
- поворотный стол.

На рис. 1 представлено его схематичное изображение.

Эксперименты направлены на исследование излучения монитора, а также USB-накопителей, подключённых к системному блоку. Основной целью ставится снятие диаграмм направленности (ДН) излучения и их анализ. Задачей является проверка предположения, что ДН – равномерна. Если она не равномерна, то необходимо оценить неравномерность, сравнив уровни сигнала.

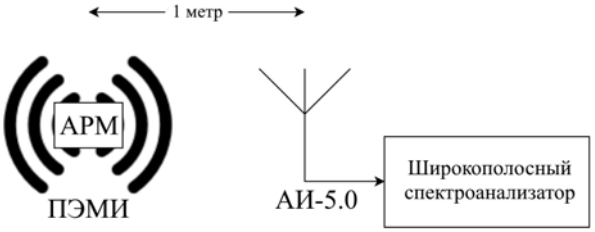


Рис. 1. Схема измерительного стенда

Снимая уровень напряжённости и поворачивая стол с шагом 10, получаем ДН. Уровень напряжённости усредняется по 3 последним измерениям.

Измеренные уровни сигналов «сигнал+шум» и «шум» [8] позволяют выделить напряжённость сигнала [9–11]. После алгебраического вычитания сигналов возможно пересчитать результат в дБмкВ [12]. Воспользуемся выражением

$$U_{\text{с}} = 20 \times \lg \sqrt{10^{(U_{\text{с+ш}}/10)} - 10^{(U_{\text{ш}}/10)}}\,, \qquad (1)$$

где $U_{\text{с+ш}}$ – значение напряжённости смеси «сигнал+шум»; $U_{\text{ш}}$ – значение напряжённости шума; $U_{\text{с}}$ – значение напряжённости сигнала.

Таким образом, показатель защищённости $П$ определяется как

$$П = U_{\text{с}} - U_{\text{ш}}\,. \qquad (2)$$

При расчёте коэффициента затухания $K_{\text{п}}$ используются измеренные величины напряжённости между точками измерения

$$K_{\text{п}} = \frac{20 \times \lg(U_{1\text{изм}}/U_{2\text{изм}})}{l}\,, \qquad (3)$$

где l – расстояние между точками измерения.

После расчёта показателя защищённости и коэффициента затухания рассчитывается возможная длина пробега сигнала:

$$R_i = \frac{П}{K_{\text{п}}}\,. \qquad (4)$$

Исследование направленности излучения монитора

Опорная частота информативного сигнала, излучаемого монитором, определяется на основе раз-

решения экрана и частоты обновления изображения [13]. При анализе внутреннего устройства LCD-монитора, было замечено его сходство с антенной решёткой: проводники располагаются плоской двумерной матрицей [14]. Однако расстояние между соседними проводниками, по которым проходит ток, не постоянно, так как не все пиксели работают одновременно. Более того, пиксель формируют субпиксели, работающие в зависимости от выводимого на экран изображения.

На основе этих особенностей выдвинуто предположение, что ДН излучения от монитора будет схожа с ДН антенной решётки (рис. 5). Однако основной лепесток ДН будет менее выражен из-за представленных выше особенностей функционирования монитора.

В ходе исследования были изучены 3 монитора различных марок: BenQ BL902M, LG 24MP65HQ-P, Samsung EX2020X. Каждый из мониторов обладал уникальной ДН, но в данной работе представлены ДН, имеющие самые выраженные неравномерности. Чем больше разница уровней сигнала по разным направлениям излучения, тем больше вероятность реализации утечки информации, так как присутствует возможность неправильной оценки распространения ПЭМИ, сделанной экспертом.

Были сняты ДН мониторов, лежащие в плоскостях *X*0*Y* и *Y*0*Z*, как представлено на рис. 2. Диаграммы дальности распространения подобны ДН в шкале мкВ/м.

Результаты измерений представлены на рис. 3 и 4. Горизонтальная ДН (см. рис. 3) подтвердила предположения о её схожести с ДН антенной решётки (см. рис. 5). На рис. 3 направление 0° соответствует оси *X* (см. рис. 2). У ДН есть участки более высокого уровня излучения (от 320 до 60°). В этом диапазоне уровень сигнала меняется в пределах 17–27 мкВ/м, тогда как на остальной части диаграммы (от 60 до 320°) уровень сигнала изменяется в узком диапазоне 11–16 мкВ/м. Шум остаётся на уровне 3–4 мкВ/м. Дальность распространения лежит в пределах 3,2–6,6 м. Это означает, что в направлении наибольшего уровня излучения сигнал «пробегает» более чем в два раза большее расстояние по сравнению с наименьшим.

У вертикальной ДН (см. рис. 4) направление 0° соответствует оси *Z* (см. рис. 2). На вертикальной ДН колебания уровень сигнала меняется в пределах 6–12 мкВ/м. Несмотря на то, что они менее выражены по сравнению с горизонтальной ДН, неравномерность распространения ЭМИ присутствует. Максимальный уровень сигнала излучается в диапазоне 10–140° и изменяется в пределах 10–12 мкВ/м.

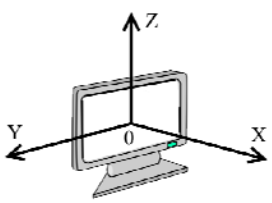


Рис. 2. Обозначение ориентации монитора при описании ДН

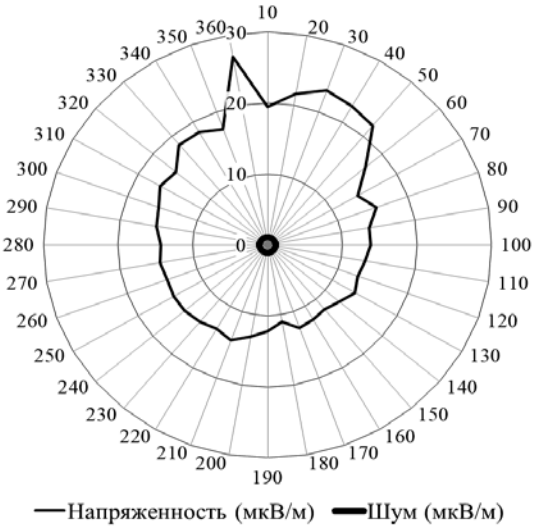


Рис. 3. Горизонтальная ДН для монитора BenQ BL902M, подключенного по DVI-интерфейсу

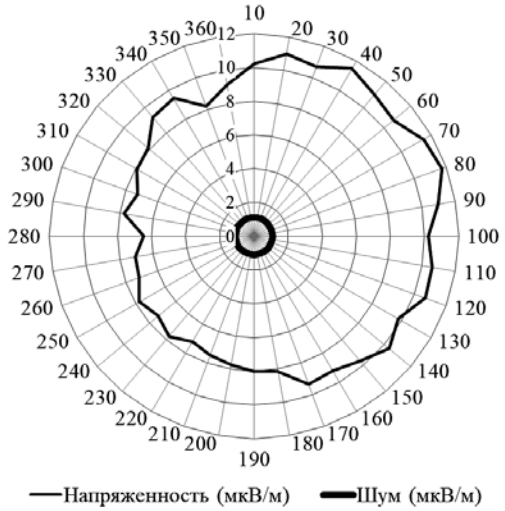


Рис. 4. Вертикальная ДН для монитора BenQ BL902M, подключенного по DVI-интерфейсу

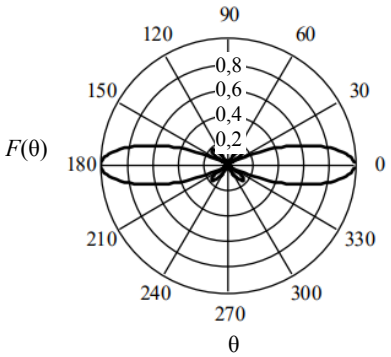


Рис. 5. Нормированная амплитудная ДН решетки из 4 полуволновых линейных симметричных электрических вибраторов

Исследование влияния расположения кабеля видеоинтерфейса на диаграмму направленности излучения монитора

По соединительному кабелю видеоинтерфейса передаётся информация для вывода на экран. Так как он является проводником, предполагается, что уровень ПЭМИ от него будет сопоставим с излуче-

нием монитора. Если кабель расположен вдоль прямой линии, ДН излучения от него будет подобна ДН штыревой антенны [15] (рис. 6).

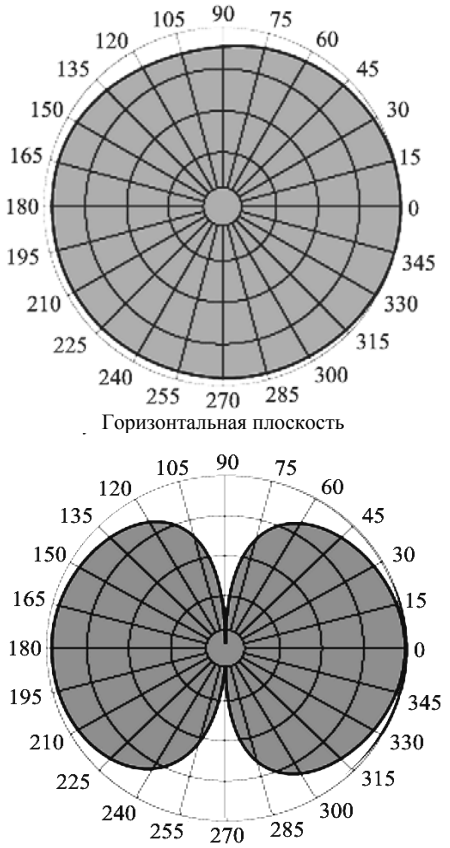


Рис. 6. Горизонтальная и вертикальная ДН штыревой антенны

Эксперимент проводится с целью выявить влияние соединительного видеокабеля на распространение ПЭМИ.

Было проведено два цикла измерений. В первом цикле положение кабеля сохранялось таким образом, чтобы не оказывать влияния на снимаемые уровни излучения. Оно соответствовало оси *X* (см. рис. 2). На этой же оси располагалась и измерительная антенна.

Во втором цикле измерений кабель был размещён коллинеарно оси *Y*, чтобы обеспечивать максимальный уровень влияния на уровень принимаемого сигнала.

Все измерения проводились с монитором LG 24MP65HQ-P. В обоих циклах измерений использовались VGA- и DVI-интерфейсы. В работе представлены ДН для VGA-интерфейса.

Результаты измерений представлены на рис. 7. Полученные ДН показывают, что уровни принятого сигнала возрастают при максимальном воздействии кабеля по сравнению с минимальным. В среднем, уровень возрастает в 2 раза, при этом есть участки, где возрастание ниже среднего (от 10 до 140°), и участки (от 210 до 220°), где сигнал возрастает более чем в 2,6 раза.

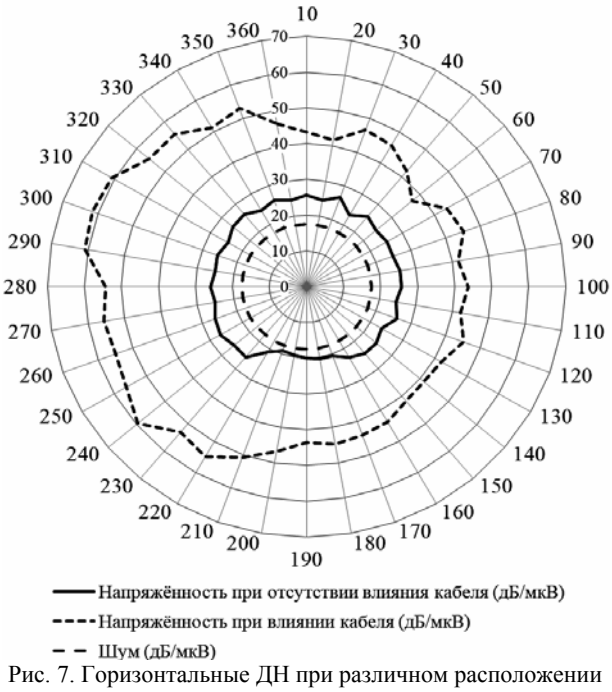


Рис. 7. Горизонтальные ДН при различном расположении соединительного видеокабеля

Исследование направленности излучения от USB-накопителей

В экспериментах исследовались USB-накопители, хранящие память по технологии flash. Интерфейс обмена данными у накопителей – USB 2.0. USB-flash-накопители миниатюрны. Плотность расположения элементов высока по сравнению с другими технологиями хранения информации. Предположительно ДН излучения от накопителей стремится к равномерной из-за большого количества разнонаправленных случайных антенн.

Сигнал измерялся на частоте работы шины данных USB 2.0 – 54 МГц. Запускалась цикличная запись на носитель для получения тестового сигнала. Положение USB-накопителя при съёме ДН соответствовало точке 0, совпадающей с центром поворотного стола. Таким образом, расстояние от накопителя до измерительной антенны не менялось на протяжении всего эксперимента. Горизонтальная ДН соответствует плоскости *X*0*Y*, а вертикальная – плоскости *Y*0*Z*.

В исследованиях использовались 3 накопителя разных фирм-изготовителей. Все накопители показали различную неравномерность ДН. Результаты съёма ДН для одного из них как обладающие большим количеством всплесков, представлены на рис. 8 и 9. Горизонтальная ДН близка к равномерной. На горизонтальной ДН направление 0° соответствует оси *X*. Колебания уровня сигнала лежат в пределах 10–13 мкВ/м. Значимых аномалий не выявлено.

На вертикальной ДН направление 0° соответствует оси *Z*. Присутствуют «провалы» в диаграмме в направлениях 60–80, 150–170, 250–270°. Причинами таких «провалов» являются экранирующие свойства системного блока, а также внутреннее устройство

накопителя. Учитывая «провалы» в ДН, дальность распространения колеблется в диапазоне 0,5–15,8 м.

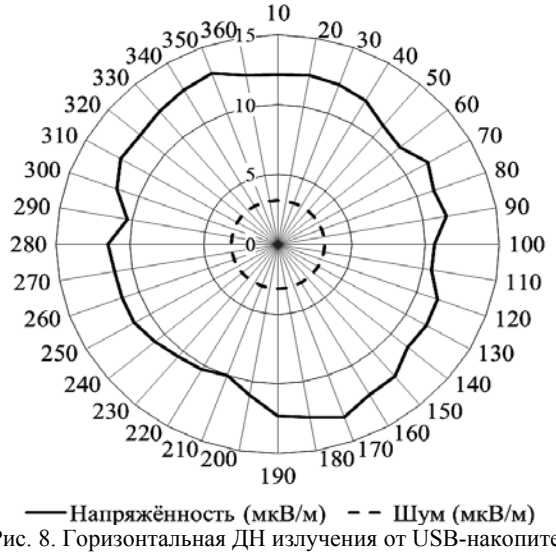


Рис. 8. Горизонтальная ДН излучения от USB-накопителя

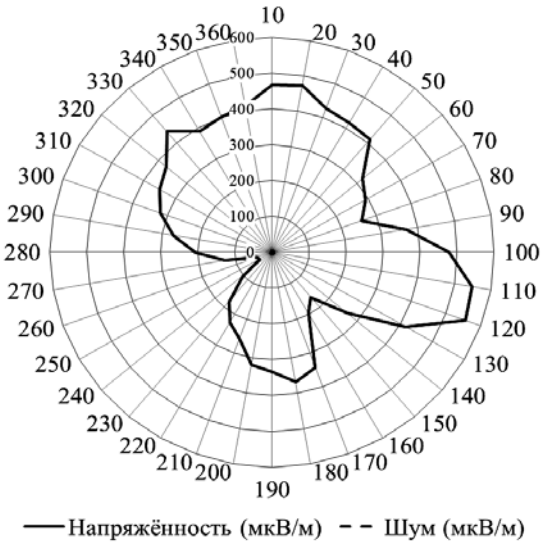


Рис. 9. Вертикальная ДН излучения от USB-накопителя

Заключение

В работе представлены и проанализированы результаты экспериментов по снятию диаграмм направленности ПЭМИ от монитора и USB-накопителя. Проведённый анализ показал, что распространение ПЭМИ обладает неравномерными характеристиками. Предположения о форме ДН частично подтверждены.

ДН для различных устройств разных марок уникальны. Неравномерность ДН объясняется внутренним расположением элементов, материалом и формой корпуса, его экранирующими свойствами. Из-за большого количества причин, влияющих на формирование ДН, спрогнозировать её не представляется возможным. Однако ДН является устойчивой во времени характеристикой устройства, поэтому можно делать выводы о распространении ПЭМИ на основе полученных ранее измерений. Тем не менее на ДН оказывает влияние и помещение, в котором функционирует устройство, что склонно видоизменять ДН.

Выполнена оценка дальности распространения сигнала. Результаты экспериментов показали, что колебания в дальности распространения в зависимости от направления излучения сравнимы с размерами помещений, в которых происходит обработка информации. Из-за непредсказуемости этих колебаний появляется угроза неправильной оценки защищённости информации от утечки по ПЭМИ.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУРа на 2017–2019 гг. (проект № 2.8172.2017/8.9).

Литература

1. Ружников В.А. Основы теории антенн и распространения радиоволн / М.Ю. Сподобаев, Ю.М. Сподобаев, В.П. Кубанов / под ред. В.П. Кубанова. – Самара: ОФОРТ, 2016. – 257 с.

2. Авсентьев А.О. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации / А.О. Авсентьев, А.Г. Вальде, О.С. Авсентьев // Вестник Воронежского института МВД России. – 2017. – С. 22–31.

3. Петров Б.М. Электродинамика и распространение радиоволн. – 2-е. изд. – М.: Телеком, 2007. – 558 с.

4. Харлов Н.Н. Электромагнитная совместимость в электроэнергетике. – Томск: ТПУ, 2007. – 207 с.

5. Семенов А.В. Утечка информации по каналам ПЭМИ и способы их защиты / А.В. Семенов, Н.В. Киреева // Международный журнал прикладных и фундаметальных исследований. – 2016. – Вып. 8-4.– С. 499–504.

6. Шелупанов А.А. Оценка ПЭМИ электронных устройств / А.А. Шелупанов, А.П. Зайцев // Доклады ТУСУР. – 2008. – № 2 (18), ч. 1. – С. 12–17.

7. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера / А.А. Хорев // Доклады ТУСУР. – 2014. – № 2(32). – С. 207–213.

8. Жалковский И.В. Определение энергетического критерия оценки защищённости информации от утечки по каналу побочных электромагнитных излучений // Докл. Белорус. гос. ун-та информатики и радиоэлектроники. – 2015. – Вып. 3 (89). – С. 107–111.

9. Шелупанов А.А. Системный анализ в защите информации / А.А. Шелупанов, А.А. Шумский. – М.: Гелиос, 2005. – 224 с.

10. Мещеряков Р.В. Технические средства и методы защиты информации / Р. В. Мещеряков, А.А. Шелупанов, А.П. Зайцев. –7-е изд. – М: Горячая линия – Телеком, 2012. – 442 с.

11. Шелупанов А.А. Технические средства и методы защиты информации / А.А. Шелупанов, Р.В. Мещеряков, С.В. Скрыль, А.П. Зайцев. – М.: Машиностроение, 2009. – 508 с.

12. Лось В.П. Основы информационной безопасности / В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов, Е.Б. Белов. – М.: Горячая линия – Телеком, 2006. – 544 с.

13. Markus G. Kuhn. Electromagnetic Eavesdropping Risks of Flat-Panel Displays // 4th Workshop on Privacy Enhancing Technologies. – Toronto, Canada, 2004. – PP. 88–107.

14. Кубанов В.П. Направленные свойства антенных решёток. – Самара: ПГУТИ, 2011. – 56 с.

15. Панасюк Ю.Н. Основы теории антенн / Ю.Н. Панасюк, А.А. Иванков, А.П. Пудовкин. – Тамбов: ГОУ ВПО ТГТУ, 2011. – 94 с.

Антипов Денис Александрович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Томского университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д.40, г. Томск, Россия, 634050
Тел.: +7-983-345-93-68
Эл. почта: antipodp@gmail.com, antipodya@yandex.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, ректор ТУСУР
Ленина пр-т., д.40, г. Томск, Россия, 634050
Тел.: (382-2) 51-05-30
Эл. почта: rector@tusur.ru

Antipov D.A., Shelupanov A.A.

Research of the direction of secondary electromagnetic radiation from a personal computer

The work is devoted to the research of the propagation of secondary electromagnetic radiation from devices in a personal computer. In the course of the work, experiments were performed demonstrating non-uniform characteristics of the radiation pattern. The calculations are given that allow one to assess the influence of uneven distribution on the security of information. It is concluded that the magnitude of the signal level fluctuations, depending on the direction of the radiation, affects the security of information.

Keywords: spurious electromagnetic radiation, information protection, radiation pattern, monitor, usb-drive.
doi: 10.21293/1818-0442-2018-21-2-33-37

References

1. Ruzhnikov V.A., Spodobaev M.Yu., Spodobaev Yu.M., Kubanov V.P. *Fundamentalnie osnovi teorii antenn i rasprostraneniya radiovoln* [Fundamentals of the theory of antennas and the propagation of radio waves]. The Russian Federation, ed. Kubanov V.P., Samara: OFORT, 2016., 257 p.

2. Avsentiev A.O., Valde A.G., Osnt'ev O.S. Investigation of the conditions for the emergence of technical information leakage channels for secondary electromagnetic radiation at information objects. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2017, pp. 22–31.

3. Petrov B.M. *Electrodinamika i rasprostranenie radiovoln* [Electrodynamics and propagation of radio waves]. Russia, Moscow Telecom, 2007, 558 p.

4. Kharlov N.N. *Electromgnitnaya sovmestimost v electroenergetike* [Electromagnetic compatibility in the electric power industry]. Tomsk: TPU, 2007, 207 p.

5. Semenov A.V., Kireeva N.V. The leakage of information through PEMI channels and ways to protect them. *Journal of Applied and Fundamental Research*. vol. 8-4, 2016, pp. 499–504.

6. Shelupanov A.A., Zaitsev A.P. Evaluation of PEMI electronic devices. *Reports of TUSUR*, 2008, no. 2 (18), part 1, pp. 12–17.

7. Khorev A.A. Evaluation of opportunities for detecting secondary electromagnetic emissions of the computer's video system. *Reports of TUSUR*, 2014, no. 2 (32), pp. 207–213.

8. Zhalkovsky I.V. Determination of the energy criterion for estimating the security of information from leakage through the channel of spurious electromagnetic radiation. *Reports of the Belarusian State University and Radioelectronics*. Vol. 3 (89), 2015, pp. 107–111.

9. Shelupanov A.A., Shumsky A.A *Sistemnii analiz v zashite informacii* [System analysis in the protection of information]. Moscow Helios, 2005, 224 p.

10. Meshcheryakov R.V., Shelupanov A.A., Zaitsev A.P. *Tekhnicheskie sredstva i metodi zashiti informacii* [Technical means and methods of information protection] 7th, Moscow: Hot line – Telecom, 2012, 442 p.

11. Shelupanov A.A., Meshcheryakov R.V., Skryl S.V., Zaitsev A.P. *Tekhnicheskie sredstva i metodi zashiti informacii* [Technical means and methods of information protection] Moscow: Mashinostroenie, 2009, 508 p.

12. Los V.P., Meshcheryakov R.V., Shelupanov A.A., *Belov E.B. Osnovi infomacionnoi bezopasnosti* [Fundamentals of Information Security], Moscow: Hotline – Telecom, 2006, 544 p.

13. Markus G. Kuhn Electromagnetic Eavesdropping Risks of Flat-Panel Displays // *4th Workshop on Privacy Enhancing Technologies*, Toronto, Canada, 2004, pp. 88–107.

14. Kubanov V.P. *Napravlennie svoistva antennih reshetok* [Directional properties of antenna arrays] Russian Federation, Samara: PGUTI, 2011, 56 p.

15. Panasyuk Yu.N., Ivankov A.A., Pudovkin A.P. *Osnovi teorii antenn* [Fundamentals of the theory of antennas] Tambov: GOU VPO TSTU, 2011, 94 p.

Denis A. Antipov
Post-graduate student. Integrated Information Security of Electronic Computing Systems, Tomsk University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone.: +7-983-345-93-68
Email: antipodp@gmail.com, antipodya@yandex.ru

Alexander A. Shelupanov
Doctor of Technical Sciences, Professor, Rector TUSUR
40, Lenina pr., Tomsk, Russia, 634050
Phone.: (382-2) 51-05-30

УДК 004.056

В.А. Трушин, А.В. Иванов

Возможности снижения интегрального уровня помехи в средствах активной защиты речевой информации (состояние и перспективы)

Рассматриваются основные подходы к снижению интегрального уровня шума от средств активной защиты речевой информации. Приведены результаты выбора оптимального спектра шумовой помехи. Описаны возможные подходы по применению метода автоматического регулирования уровня помехи, который, помимо снижения уровня паразитного шума, может предотвратить утечку информации за счет возникновения эффекта форсирования речи. Сформированы первоначальные правила формирования помех с коммутацией частотных полос, эффективность данного метода подтверждена экспериментально. Исследованы подходы к формированию речевой помехи из слогов, слов, связных текстов. Получены результаты по влиянию речевого материала и голосов дикторов на эффективность речевой помехи.

Ключевые слова: защита речевой информации, паразитный шум, спектр помехи, коммутация частотных полос, речевая помеха.
doi: 10.21293/1818-0442-2018-21-2-38-42

Для защиты речевой информации от утечки по техническим каналам широко применяются активные средства защиты – генераторы акустического и виброакустического шума. В настоящее время такие генераторы построены, в основном, с использованием в качестве задающего белого шума с нормальным законом распределения вероятности значений. При этом огибающая этого шума в частотной области может соответствовать белому, розовому, речеподобному и др. Естественно, что встает вопрос о выборе оптимальной помехи, т.е. такой, которая при обеспечении требуемого показателя защищенности (в общем случае это коэффициент словесной разборчивости речи W) давала бы минимальное значение интегрального уровня помехи, т.е. обеспечивающее минимальный дискомфорт при проведении переговоров. При этом применяемые в средствах защиты помехи можно условно разделить на две большие группы: шумовые и речеподобные.

В настоящее время известны следующие подходы к решению задачи снижения интегрального уровня шума.

Шумовая помеха с оптимальной спектральной огибающей

Проведенные исследования, в частности [1–3], показали (рис. 1), что шумоподобные помехи с различными огибающими спектра имеют серьезные отличия по их эффективности, т.е. для обеспечения одного и того же значения W требуют разные уровни интегрального отношения сигнал/шум. При этом наиболее эффективной из рассмотренных (белый, розовый, коричневый, речеподобный) является шумовая речеподобная помеха, т.е. имеющие огибающую, подобную спектру речи.

В работе [4] говорится о возможности создания оптимизированной по спектру шумовой помехи, зависящей от требуемого значения W (рис. 2).

Однако в работах [5–7] показано, что оптимальной является формантоподобная помеха, т.е. имеющая огибающую, соответствующую спектру формант (рис. 3).

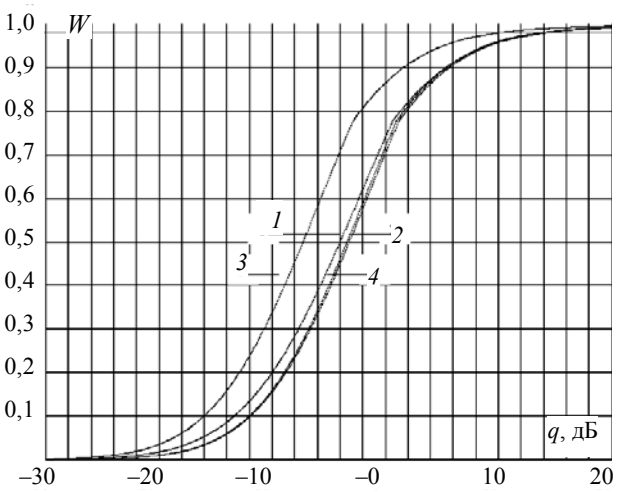


Рис. 1. Зависимость словесной разборчивости W от интегрального отношения сигнал / шум q:
1 – белый шум; *2* – розовый шум; *3* – шум со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот; *4* – шумовая речеподобная помеха

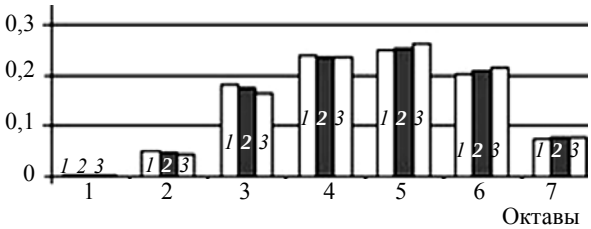


Рис. 2. Распределение мощности помеховых сигналов по семи октавным полосам:
1 – $P_W = 0{,}1$; *2* – $P_W = 0{,}2$; *3* – $P_W = 0{,}4$

Автоматическое регулирование уровня помехи

Принцип данного подхода заключается в регулировании интегрального уровня помехи (его увеличении или уменьшении) в зависимости от интегрального уровня речи в защищаемом помещении. Для этого необходим канал обратной связи, определяющий интегральный уровень речи в данный момент времени, который может быть реализован раз-

личными способами, например: установкой микрофона в месте расположения вибродатчика (возможно, в нескольких местах для раздельного регулирования уровня шума в контрольных точках), измерением интегрального уровня «сигнал плюс помеха» и «помеха» с последующим нахождением уровня сигнала или в моменты специального кратковременного отключения помехи, установкой микрофона обратной связи вблизи источника речевой информации и др. При этом согласно распределению вероятностей уровней речи [8] вероятность того, что уровень речи будет меньше ее среднего интегрального значения, составляет 0,8 [8].

Данный подход реализуется в генераторах «Заслон-2М», «Кедр» и др.

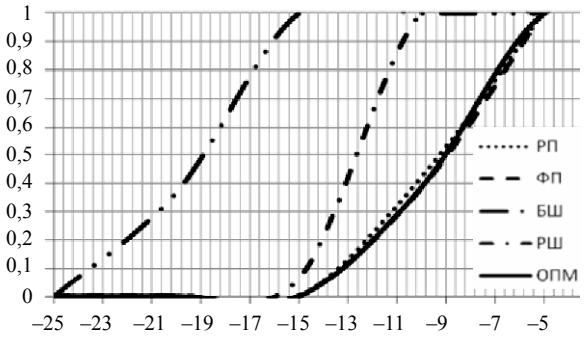


Рис. 3. Зависимость словесной разборчивости W от интегрального отношения сигнал/шум q:
РП – речеподобная помеха; ФП – формантоподобная помеха; БШ – белый шум; РШ – розовый шум; ОПМ – оптимальная помеха по методике

Формирование речеподобной помехи из речевых сигналов

В отличие от шумовой помехи, имеющей огибающую спектра, соответствующую спектру речи, реальная речеподобная помеха имеет «тонкую» структуру речевого сигнала и во временной области.

Имеющиеся на рынке активных средств защиты речевой информации генераторы речеподобных помех, такие как «Барон», «Шаман», «Бубен», «Druid» и др., используют различные алгоритмы формирования речеподобной (РП) помехи. Так, в «Бароне» она формируется от 3 внешних радиостанций с использованием дополнительного фонемного клонера из голосов говорящих. В «Факире» применяется выбор фрагментов сигнала по псевдослучайной последовательности. В генераторе «Druid» используется реверберационная помеха из голосов участников переговоров. Такие различающиеся РП-помехи не позволяют унифицировать (нормировать) алгоритм создания РП-помехи. К сожалению, разработчики этих генераторов не раскрывают алгоритмы формирования РП-помехи, ограничиваясь общими фразами. Вместе с тем появились попытки создания единого подхода на основе существующих баз элементов речи с последующей случайной выборкой этих элементов с озвучиванием на звукосинтезаторе. Так, в работе [13] рассмотрен алгоритм формирования РП-помехи из случайной последовательности звуков русской речи, реализованной на основе специально разработанного программного обеспечения и с использованием артикуляционных таблиц [14]. Получены весьма впечатляющие результаты (таблица).

Результаты оценки словесной разборчивости методом артикуляционных испытаний

Номер аудитора	Отношение сигнал/шум q, дБ					
	–5	0	5	10	15	20
	Словесная разборчивость W, %					
1	5	0	45	65	70	75
2	0	0	10	40	65	80
3	0	0	0	0	40	55
4	0	0	0	20	45	60
5	0	0	0	15	55	70
$W_{\text{сред}}$	1	0	11	28	55	70

О возможности снижения интегрального уровня помехи за счет коммутации частотных полос

Наряду с вышеизложенными подходами, возможным вариантом снижения уровня паразитного шума является коммутация частотных полос, в которых в отдельный момент времени на участников переговоров воздействует не широкополосная помеха, а шум в нескольких частотных полосах, коммутируемых по определенному алгоритму и с заданной скоростью.

Для того чтобы определиться с правилами формирования подобных помех, были решены следующие задачи:

– выбор разбиения частотного диапазона;

– выбор количества полос (суммарной ширины частотного диапазона), в которых в отдельный момент времени присутствует маскирующая помеха;

– выбор времени переключения частотных полос.

При выборе разбиения частотного диапазона сразу был исключен вариант разбиения на октавные / третьоктавные полосы. Причина в том, что при данных подходах ширина полосы различная и присутствуют широкие полосы, что приводит к невозможности равномерно во времени распределить мощность помехи. Например, при октавном разбиение включение 7-й полосы (5600–11200 Гц) приводит к существенному скачку в мощности излучаемого сигнала (на слух подобное чередование будет происходить со щелчками, которые только усиливают раздражающее воздействие на участников переговоров), так как данная полоса фактически перекрывает половину всего речевого диапазона, при этом ее вклад в разборчивость речи ниже, чем у области средних частот, следовательно, данный подход явно неэффективен.

Было принято решение разбивать весь диапазона на полосы равной ширины. За основу взяли минимальную ширину равноартикуляционных полос, равную 150 Гц. В результате весь диапазон разделяется на 40 полос.

Экспериментально была определена наиболее эффективная ширина суммарного частотного диапазона (количества частотных полос), в котором в от-

дельный момент времени присутствует помеха. Необходимо было найти «золотую середину», потому как очевидно, что чем шире данный диапазон, тем ниже будет уровень разборчивости речи, но выше будет и уровень паразитного шума, воздействующий на участников переговоров. Было определено, что оптимальным является значение 2850 Гц (19 полос по 150 Гц).

Что касается алгоритма коммутации данных частотных полос, то первоначально был проработан подход, основывающийся на весовых коэффициентах (вкладах частотных полос в суммарную разборчивость).

Таким образом, график встречаемости каждой из полос выглядит следующим образом (рис. 4):

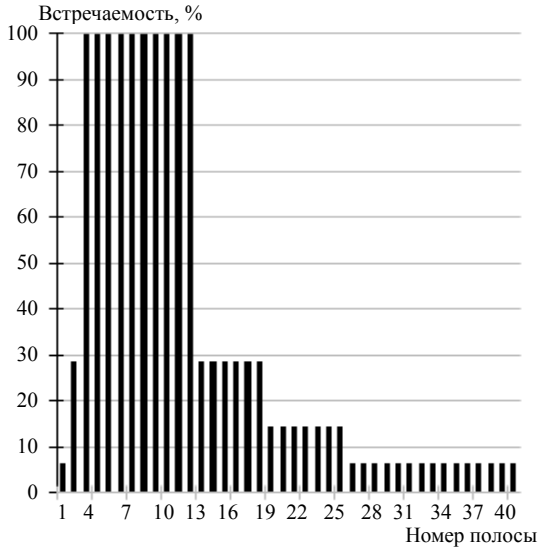


Рис. 4. Встречаемость каждой полосы в шуме с распределением по весовым коэффициентам

На следующем этапе проводилось экспериментальное обоснование выбора времени переключения частотных полос. Исходя из того, что длительность звуков русской речи различна и находится в пределах от 20 до 260 мс, были выбраны следующие варианты времени чередования частотных полос: 100, 50, 10 и 1 мс. Наилучший результат показал вариант с чередованием диапазонов частотных полос через 10 и 1 мс. «Выигрыш» в интегральном уровне, воздействующем в отдельный момент времени, по сравнению с широкополосной помехой (белым шумом) составил 3,3 дБ.

Основываясь на известных положениях психоакустики [9–12], указывающих, что наибольший маскирующий эффект вносят низкочастотные сигналы, был исследован вариант встречаемости частотных полос с преобладанием низкочастотной области (рис. 5).

Результаты подтвердили эти положения, и «выигрыш» по сравнению с широкополосной помехой составил 5,1 дБ. Данный факт также ставит под сомнение корректность применения формантного распределения (весовых коэффициентов) при оценке защищенности речевой информации.

На заключительном этапе был произведен анализ влияния огибающей спектра помехи: был поставлен эксперимент с формантоподобной помехой вместо белого шума. В результате получилось добиться дополнительного выигрыша в 1 дБ.

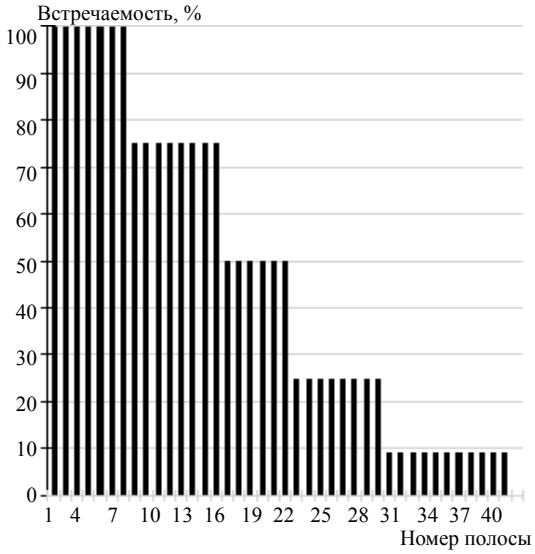


Рис. 5. Встречаемость каждой полосы в шуме с преобладанием низкочастотной области

Таким образом, были определены правила формирования помех с коммутацией частотных полос, позволившие снизить уровень шума на 6 дБ.

О возможности создания унифицированного подхода к реализации речеподобной помехи

Авторами были проведены исследования возможности создания «унифицированных» подходов реализации РП-помехи на базе слоговых и словесных таблиц из [14], а также на основе связных текстов из произведений русских классиков.

Основные параметры эксперимента:

– алгоритм случайной выборки RNGCryptoServiceProvider на языке C#;

– программный звукосинтезатор Vocalizer;

– программа обработки звуковых файлов Adobe Audition 3.0;

– число «дикторов» – 3 + один живой голос;

– число аудиторов – 4.

Основные выводы эксперимента:

– спектры РП-помехи, полученной из таблиц слогов и слов, практически не различаются;

– ближе всего к спектру реальной русской речи – РП-помеха типа «речевой хор» из трех голосов (2 мужских, 1 женский);

– наилучшими маскирующими свойствами обладает РП-помеха «речевой хор», причем из голосов участников переговоров.

На рис. 6 приведен пример результатов артикуляционных испытаний. Очевидно, что данные результаты предварительные; требуется увеличение количества аудиторов и корректная обработка результатов в соответствии с [15]. Вместе с тем полученные результаты показывают перспективность создания средств активной защиты речевой инфор-

мации на основе РП-помех, реализованных с использованием слогов, слов связных текстов.

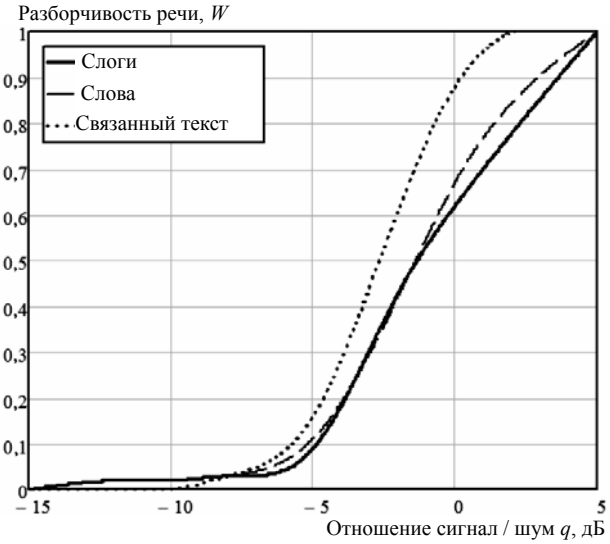


Рис. 6 Зависимости разборчивости речи от отношения сигнал / шум «речевого хора» из слогов, слов и связных текстов

Заключение

В работе рассмотрены основные подходы к снижению интегрального уровня помехи в средствах активной защиты речевой информации при сохранении требуемого показателя защищенности.

В вопросе выбора спектра шумовой помехи приведены основные результаты, показывающие, что оптимальной является формантоподобная помеха.

Отмечен вариант применения автоматической регулировки уровня помехи, зависящего напрямую от уровня защищаемого сигнала либо применяемого только в случае превышения уровнем речи установленных средних значений (эффект форсирования речи).

Предложено применение коммутации частотных полос шумовой помехи. Экспериментально подтверждено, что суммарный диапазон частот, который подвергается зашумлению в отдельный момент времени, составляет 2850 Гц. Время чередования частотных полос должно составлять 1–10 мс. Рассмотренные варианты алгоритмов коммутации частотных полос показали лучшую эффективность в случае помехи с преобладанием в низкочастотный области. В результате удалось снизить уровень шумовой помехи на 6 дБ.

Проведены некоторые результаты предварительных исследований в области формирования речеподобной помехи из слоговых и словесных таблиц, а также связных текстов. Установлено, что РП-помеха типа «речевой хор» обладает наилучшей эффективностью. Отмечены целесообразность и перспективность продолжения исследований.

Благодарности

Авторы выражают искреннюю признательность д.т.н., профессору Авдееву Владимиру Борисовичу за полезную дискуссию по возможности создания генераторов РП-помех с «унифицированным» алгоритмом функционирования, что послужило стимулом к проведению данных исследований.

Литература

1. Хорев А.А. Оценка эффективности систем виброакустической маскировки / А.А. Хорев, Ю.К. Макаров // Вопросы защиты информации. – 2001. – № 1. – С. 21–28.

2. Хорев А.А. Контроль защищённости речевой информации от её утечки по техническим каналам // Специальная техника. – 2014. – № 4. – С. 45–53.

3. Дидковский В.С. Акустическая экспертиза каналов речевой коммуникации / В.С. Дидковский, М.Л. Дидковский, А.Н. Продеус. – Киев: Имекс-ЛТД, 2008. – 420 с.

4. Григорьев С.В. Оптимизированная по спектру шумовая помеха / С.В. Григорьев, С.А. Колычев // Защита информации: Инсайд. – 2003. – № 4. – С. 52–57.

5. Трушин В.А. К вопросу об оценке разборчивости речи // Проблемы информационной безопасности государства, общества, личности: матер. Девятой Всерос. науч.-техн. конф. – Томск: ТУСУР, 2007. – С. 115–119.

6. Иванов А.В. О модели речевого сигнала при оценке защищенности речевой информации от утечки по техническим каналам / А.В. Иванов, В.А. Трушин // Доклады ТУСУР. – 2014. – № 2 (32). – С. 87–90.

7. Иванов А.В. Реализация оптимальной помехи при защите речевой информации от утечки по акустическим и виброакустическим каналам / А.В. Иванов, И.Л. Рева, В.А. Трушин // Науч. вестник НГТУ. – 2011. – № 4. – С. 151–154.

8. Иванов А.В. О выборе модели тестового сигнала при оценке защищенности речевой информации от утечки по техническим каналам / А.В. Иванов, В.А. Трушин, В.Е. Хиценко // Труды СПИИРАН. – 2015. – Вып. №3 (90). – С. 122–133.

9. Алдошина И.А. Музыкальная акустика: учебник / И.А. Алдошина, Р. Притц. – СПб.: Композитор, 2006. – 720 с.

10. Fastl H. Psychoacoustics. Facts and Models / H. Fastl, E. Zwicker. – Springer-Verlag, 2007. – 471 p.

11. Howard D.M. Acoustics and Psychoacoustics / D.M. Howard, J. Angus. – Taylor & Francis, 2009. – 488 p.

12. Everest F.A. Master Handbook of Acoustics. – NJ, USA: Mc Graw Hill, 2001. – 616 p.

13. Хорев А.А. Способ и алгоритм формирования речеподобной помехи / А.А. Хорев, Н.В. Царев // Вестник ВГУ. Сер.: Системный анализ и информационные технологии. – 2017. – №1. – С. 57–67.

14. ГОСТ 16600–72. Межгосударственный стандарт. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений. – М.: Стандарт-Информ, 2007. – 74 с.

15. ГОСТ Р50840–95. Передача речи по трактам связи. Методы оценки качества, разборчивости, узнаваемости. – М., 1995. – 230 с.

Трушин Виктор Александрович
Канд. техн. наук, доцент каф. защиты информации
Новосибирского государственного технического университета (НГТУ)
Карла Маркса пр-т., д. 20, г. Новосибирск, Россия, 630073
Тел.: +7 (383-3) 46-08-53
Эл. почта: rastr89@mail.ru

Иванов Андрей Валерьевич
Канд. техн. наук, и.о. зав. каф. защиты информации НГТУ
Карла Маркса пр-т., д. 20, г. Новосибирск, Россия, 630073
ORCID 0000-0003-2002-8572
Тел.: +7 (383-3) 46-08-53
Эл. почта: andrej.ivanov@corp.nstu.ru

Trushin V.A., Ivanov A.V.

Possibilities and outlooks of integral noise level decrease in voice information active protection means

In the paper, the approaches to integral noise level decrease in voice information active protection means are reviewed. Results of the optimal noise spectrum choice are given. Some approaches to use of automated noise level adjustment method, which helps to decrease parasitic noise level and to prevent information leakage because of speech forcing effect, are described. Simple rules of generation of frequency bands switching noise are developed; efficiency of the method is experimentally proved. Approaches to generation of speech noise from syllables, words, and connected texts are investigated. Results of influence of speech on speech noise efficiency are obtained.

Keywords: voice information protection, parasitic noise, noise spectrum, frequency bands switching, speech noise.
doi: 10.21293/1818-0442-2018-21-2-38-42

References

1. Khorev A.A., Makarov Yu.K. Estimation of the effectiveness of vibro-bush camouflage systems. *Questions of information protection*, 2001, no. 1, pp. 21–28 (In Russ.).

2. Khorev A.A. Control over the protection of voice information from its leakage through technical channels. *Special equipment*, 2014, no. 4, pp. 45–53 (In Russ.).

3. Grigoryev S.V., Kolychev S.A. Spectrum-optimized noise interference. *Protection of the information: Inside,* 2003, No. 4, pp. 52–57. (In Russ.).

4. Didkovskiy V.S. Didkovskiy M.L., Prodeus A.N. *Akusticheskaja jekspertiza kanalov rechevoj kommunikacii. Monografija* [Acoustic speech communication channel expertise. Monograph]. Kiev, Imeks-LTD publ., 2008. 420 p. (In Russ.).

5. Grigoryev SV, Kolychev SA Spectrum-optimized noise interference. *Protection of information: Inside*, 2003, no. 4, pp. 52–57. (In Russ.).

6. Trushin V.A. To the question of assessing the intelligibility of speech. *Problems of Information Security of the State, Society, Person.* Materials of the Ninth All-Russian Scientific and Technical Conference. Tomsk, TUSUR publ., 2007, pp. 115–119 (In Russ.).

7. Ivanov A.V., Reva I.L., Trushin V.A. Implementation optimum speech interference protection of information against leakage of acoustic and vibroacoustic channels. *Scientific Bulletin NSTU*, 2011, no. 4, pp. 151–154 (In Russ.).

8. Ivanov A.V., Trushin V.A., Khitsenko V.E. On the choice of the test signal model in assessing the protection of voice information from leakage through technical channels. *Proceedings of SPIIRAS*, 2015, No. 3 (90), pp. 122–133 (In Russ.).

9. Aldoshina I.A., Pritz R. *Musical acoustics.* Textbook. St. Petersburg. Composer, 2006. 720 p. (In Russ.).

10. Fastl H., Zwicker. E. *Psychoacoustics. Facts and Models*. Springer-Verlag, 2007. 471 p.

11. Howard D.M., Angus J. *Acoustics and Psychoacoustics*. Taylor & Francis, 2009. 488 p.

12. Everest F.A. *Master Handbook of Acoustics*. NJ, USA, Mc Graw Hill, 2001. 616 p.

13. Khorev A.A., Tsarev N.V. Method and algorithm of formation of re-chep-like interference. *Vestnik VSU, series: system analysis and information technologies*, 2017, no.1, pp. 57–67 (In Russ.).

14. GOST 16600–72. *Interstate standard. The transmission of speech through the radiotelephone communications. Requirements for intelligibility of speech and methods of articulatory measurements*. M.: Standard Inform, 2007, 74 p. (In Russ.).

15. GOST P50840–95 *Transmission of speech through communication paths. Methods for assessing quality, intelligibility, recognizability*. M., 1995, 230 p. (In Russ.).

Victor A. Trushin
Ph. D., assistant professor of the Information Security
Department of Novosibirsk State Technical University (NSTU)
K. Marksa pr., 20, st. Novosibirsk, Russia, 630073
Phone: +7 (383-3) 46-08-53
Email: rastr89@mail.ru

Andrey V. Ivanov
Ph. D., head of the Information Security Department
of Novosibirsk State Technical University (NSTU)
K. Marksa pr., 20, st. Novosibirsk, Russia, 630073
ORCID 0000-0003-2002-8572
Phone: +7 (383-3) 46-08-53
Email: andrej.ivanov@corp.nstu.ru

УДК 621.396.41

О.С. Кустова, Е.А. Шешенева, А.М. Калашников

О корректировке показателей словесной разборчивости речи при оценке защищенности помещения

Защищаемые помещения, в которых циркулирует конфиденциальная информация, требуют оценки их защищенности. Для оценки защищенности помещений по акустическому и виброакустическому каналу могут использоваться соответствующие методики. Имеется стандартная методика ФСТЭК, которая обладает как достоинствами, так и недостатками. В связи с этим цель данной работы – корректировка значений словесной разборчивости, полученных при помощи системы «Шепот» с учетом дополнений стандартной методики.

В представляемой статье приведены результаты анализа достоинств и недостатков методики оценки словесной разборчивости, рассмотрены дополнения этой методики. Для корректировки значения словесной разборчивости при вычислении значения словесной разборчивости с учетом дополнений и усовершенствований, рекомендуемых в публикациях современных авторов, в работе предлагается:

− рассмотрение влияния технических средств акустической разведки (ТСАР), а именно узконаправленных микрофонов и средств шумовой очистки;

− минимизация методической погрешности за счет линеаризации зависимости уровня ощущений от коэффициента восприятия и линеаризации словесной разборчивости от формантной.

Для анализа полученных данных в представляемой статье произведены расчеты значения словесной разборчивости с использованием иного формантного метода.

Ключевые слова: узконаправленные микрофоны; словесная разборчивость; утечка речевой информации; технические средства акустической разведки.

doi: 10.21293/1818-0442-2018-21-2-43-47

Для определения возможности негласного получения речевой конфиденциальной информации и актуальности применения средств защиты могут использоваться различные методы, основанные на оценке интегрального критерия – разборчивости речи, а также на определениях формантной теории. Существующие методы изначально разрабатывались для оценки качества линий связи, и именно поэтому требуется адаптация таких методов и их корректировка для задач оценки защищенности речевой информации. Самыми популярными в нашей стране методами оценки защищенности речевой информации являются версии Н.Б Покровского., М.А. Сапожкова, Ю.С. Быкова.

В настоящее время для оценки защищенности речевой информации используется методика, основой которой является метод Н.Б. Покровского [1].

Наряду с известными достоинствами указанный метод обладает существенными недостатками:

− в нем не рассматриваются варианты возможного перехвата информации при помощи узконаправленных микрофонов и возможность прослушивания речи с использованием технических средств шумовой очистки (фильтров);

− методическая погрешность оценки словесной разборчивости значительна, поскольку в методе Н.Б. Покровского не учтена зависимость от частоты при определении коэффициента восприятия речи.

Коэффициент восприятия речи, входящий в расчет словесной разборчивости, представляет собой вероятное относительное количество формантных составляющих речи, которые будут иметь уровни интенсивности выше порогового значения [2]. Коэффициент восприятия от уровня ощущений $P(Q)$ определяется по специальному графику. Зависимости коэффициента восприятия от уровня ощущений формант не являются симметричными и должны зависеть от частоты. В методе Н.Б. Покровского условие зависимости коэффициента восприятия от уровня ощущений формант пренебрегается, что ведет к большим погрешностям вычислений.

Учитывая то, что методика имеет погрешности и изначально не была создана для определения защищенности акустической информации, в наше время активно ведутся работы по ее усовершенствованию.

Основываясь на достоинствах формантных и модуляционных методов, был предложен новый формантно-модуляционный метод. Он объединяет в себе достоинства обоих методов. Также позволяет учитывать реверберационную помеху. Описание данного метода дается в работах А.Н. Продеуса [15].

На основании формантно-модуляционного метода А.Н. Продеуса в работе [15] было предложено усовершенствование метода Н.Б. Покровского, которое позволяло учитывать реверберационную помеху, считая шумом энергию отраженного звука, приходящего после 50 мс.

Однако если производится оценка меблированного помещения, то такая помеха может не учитываться, так как время реверберации меньше 0,85 с незаметно для слуха и большого влияния на расчеты эта величина не окажет. Учитывая то, что примерное время реверберации для меблированных помещений не превышает 0,6 с, данная модификация метода не будет рассматриваться в данной работе. Авторы работы [3] для задач информационной безопасности представляют усовершенствованную методику, в ко-

торой предлагают линеаризацию функций коэффициента восприятия от уровня ощущений формант и линеаризацию словесной разборчивости от формантной. При определении относительного уровня сигнал / шум рассматривается возможность того, что перехват речевой информации может происходить с применением микрофонов, коэффициент направленного действия (КНД) которых позволяет учесть использование различных микрофонов при перехвате информации.

Для корректировки значения словесной разборчивости с помощью рассмотренных рекомендаций и дополнений в представляемой методике необходимо определить следующие параметры:

1. L_{ci} – спектральный уровень акустического сигнала в пяти октавных полосах со среднегеометрическими частотами 250–4000 Гц, дБ.
2. $L_{ші,}$ – уровень шумов и помех, дБ.
3. КНД$_i$ – коэффициент направленного действия узконаправленного микрофона, дБ.
4. КОШ$_i$ – коэффициент очистки шума, дБ.
5. Q_i – относительный уровень сигнал/шум, дБ.
6. p_i – коэффициент восприятия формант.
7. R – формантную разборчивость.

Для определения КНД таких типов микрофонов, как микрофонная решетка, трубчатый щелевой микрофон, рефлекторный (параболический) микрофон, в настоящей работе использованы соответственно формулы из публикаций [4, 5] (табл. 1):

$$R(\theta,\varphi)=R_1(\theta,\varphi)\times \times\frac{\sin\left[\frac{Nx\pi dx}{\lambda}\cos\varphi\sin\theta\right]\sin\left[\frac{Ny\pi dy}{\lambda}\sin\varphi\sin\theta\right]}{Nx\sin\left[\frac{\pi dx}{\lambda}\cos\varphi\sin\theta\right]Ny\sin\left[\frac{\pi dy}{\lambda}\sin\varphi\sin\theta\right]}, \quad (1)$$

$$R(\theta)=\frac{\sin\left(\frac{\pi L}{\lambda}\left[1-\cos(\theta)\right]\right)}{\frac{\pi L}{\lambda}\left[1-\cos(\theta)\right]}; \quad (2)$$

$$R(\theta)=\frac{2J_1\left(\frac{2\pi\rho_0}{\lambda}\sin\theta\right)}{\frac{2\pi\rho_0}{\lambda}\sin\theta}. \quad (3)$$

Таблица 1

Характеристики узконаправленных микрофонов

Рефлекторный микрофон	
Диаметр отражателя, м	0,6
Дальность перехвата разговоров, м	100
Трубчатый микрофон	
Частотный диапазон, Гц	200–15 000
Максимальный коэффициент усиления, дБ	50
Микрофонная решетка	
Апертура, D, м	0,4
Частотный диапазон, Гц	316–15 000

Для трех типов микрофонов рассчитаны значения коэффициентов направленного действия (табл. 2) [6, 7].

Таблица 2

Значения коэффициентов направленного действия узконаправленных микрофонов

Тип микрофона	Октавные полосы, Гц				
	250	500	1000	2000	4000
Рефлекторный	3,2	9,3	15,2	21,3	27,3
Трубчатый	6,7	9,6	12,5	15,5	18,5
Микрофонная решетка	1,6	7,5	13,6	16,6	25,0

Основная энергия речевого (акустического) сигнала сосредоточена в диапазоне частот 300–4000 Гц [4]. Из представленных узконаправленных микрофонов трубчатый щелевой микрофон в данном диапазоне имеет наихудшие направленные свойства, (рис. 1). Поэтому является целесообразным применение фильтров шумовой очистки.

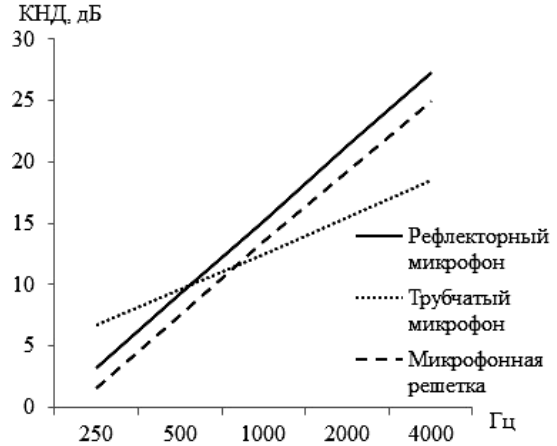


Рис. 1. Значения КНД в пяти октавных полосах со среднегеометрическими частотами 250–4000 Гц

Чтобы учесть влияние таких микрофонов и средств шумовой очистки, воспользуемся формулой из работы [5]:

$$Q_i=q_i-\Delta A_i=L_{ci}-L_{шi}-\Delta A_i+\Theta КНД_i+m\text{КОШ}_i. \quad (4)$$

Для определения коэффициента восприятия формант и словесной разборчивости предлагается использование линейной зависимости уровня ощущений от коэффициента восприятия $P(Q)$, как и в зарубежном методе articulation index AI [13, 14]. Таким образом, для минимизации значения методической погрешности предлагается использование формул из работы [3]:

$$P_i(Q_i)=0{,}05Q_i+1{,}25. \quad (5)$$

Зависимость словесной разборчивости от формантной определяется согласно следующему равенству:

$$W(R)=6R. \quad (6)$$

Экспериментальная часть работы заключалась в модельном проведении инструментального контроля защищаемого помещения от утечки речевой информации использованием автоматизированной системы «Шепот» [8]. Для проведения измерений в аудитории были выбраны две контрольные точки однородной (КТ 1) и неоднородной ограждающей поверхностей (КТ 2). Результаты измерений были от-

корректированы в соответствии с рассмотренными выше дополнениями (табл. 3–5).

Таблица 3

Результаты эксперимента по определению словесной разборчивости с учетом дополнений и влияния рефлекторного микрофона

Параметр	Октавные полосы, Гц				
	250	500	1000	2000	4000
ТС	64,7	67,0	70,5	71,0	65,4
С+Ш	38,7	38,6	30,4	29,0	24,3
Ш	24,8	24,2	20,2	16,1	16,5
$\otimes$	0	0	0	0	0,9
L_{c2i}	38,7	38,6	30,4	29,0	23,4
Z_i	26	28,4	40,1	42	42
L_{ci}	40	37,6	20,9	14	11
q_i	15,2	13,4	0,7	–2,1	–5,5
Q_i (без ТСАР)	–2,8	–0,6	–8,3	–8,1	–10,5
Q_i (с ТСАР)	0,09	8,7	6,9	13,2	17,7
P_i	0,99	0,99	0,99	0,99	0,99
R_i	0,029	0,118	0,198	0,297	0,257
R	0,8997				
W	0,999				

Таблица 4

Результаты эксперимента по определению словесной разборчивости с учетом дополнений и влияния трубчатого микрофона и средств шумоочистки

Параметр	Октавные полосы, Гц				
	250	500	1000	2000	4000
ТС	64,7	67,0	70,5	71,0	65,4
С+Ш	38,7	38,6	30,4	29,0	24,3
Ш	24,8	24,2	20,2	16,1	16,5
$\otimes$	0	0	0	0	0,9
L_{c2i}	38,7	38,6	30,4	29,0	23,4
Z_i	26	28,4	40,1	42	42
L_{ci}	40	37,6	20,9	14	11
q_i	15,2	13,4	0,7	–2,1	–5,5
Q_i (без ТСАР)	–2,8	–0,6	–8,3	–8,1	–10,5
Q_i (с ТСАР)	10,9	16	10,2	10,4	9,6
p_i	0,99	0,99	0,99	0,99	0,99
R_i	0,0297	0,1188	0,198	0,297	0,2574
R	0,889				
W	0,999				

Таблица 5

Результаты эксперимента по определению словесной разборчивости с учетом дополнений и влияния микрофонной решетки

Параметр	Октавные полосы, Гц				
	250	500	1000	2000	4000
ТС	64,7	67,0	70,5	71,0	65,4
С+Ш	38,7	38,6	30,4	29,0	24,3
Ш	24,8	24,2	20,2	16,1	16,5
$\otimes$	0	0	0	0	0,9
L_{c2i}	38,7	38,6	30,4	29,0	23,4
Z_i	26	28,4	40,1	42	42
L_{ci}	40	37,6	20,9	14	11
q_i	15,2	13,4	0,7	–2,1	–5,5
Q_i (без ТСАР)	–2,8	–0,6	–8,3	–8,1	–10,5
Q_i (с ТСАР)	–1,5	6,9	5,3	8,5	15,9
P_i	0,99	0,99	0,99	0,99	0,99
R_i	0,029	0,118	0,198	0,297	0,257
R	0,8997				
W	0,999				

Анализ полученных результатов обработки проведенных измерений в контрольной точке КТ 1 позволил сделать вывод о недостаточной защите помещения от утечки речевой информации. Видно, что значения отношений сигнал / шум и словесной разборчивости превышают нормированные как при расчете по методике ФСТЭК, так и по представляемой методике с учетом дополнений [9].

Методическая погрешность минимизируется на интервале отношений сигнал / шум от –20 до –5 дБ, т.е. отношение сигнал / шум на среднегеометрической частоте 4000 Гц попадает в данный интервал. Методическая погрешность экспериментальных данных минимизируется только на частоте 4000 Гц. Значение словесной разборчивости получается завышенным.

Полагаем, что в настоящих условиях при осуществлении перехвата речевой информации с использованием любого из рассмотренных выше микрофонов может быть получена справка подробного содержания ведущихся конфиденциальных переговоров, т.е. имеет канал утечки речевой информации.

Для анализа полученных данных произведен расчет значения словесной разборчивости с использованием формантного метода AI, [13, 14] (табл. 6).

$$P_{AI}(\Delta L)=\begin{cases}0, & \Delta L \le 0\,\text{дБ},\\ \dfrac{\Delta L}{30}, & 0 \le \Delta L \le 30\,\text{дБ},\\ 1, & \Delta L > 30\,\text{дБ}.\end{cases} \qquad (7)$$

$$\Delta L = Q + 12. \qquad (8)$$

Таблица 6

Результаты расчета словесной разборчивости методом AI

Параметр	Октавные полосы, Гц					
	250	500	1000	2000	4000	8000
ТС	64,7	67,0	70,5	71,0	65,4	64,7
С+Ш	38,7	38,6	30,4	29,0	24,3	22,1
Ш	24,8	24,2	20,2	16,1	16,5	18,5
Q	–2,8	–0,6	–8,3	–8,1	–10,5	–16,1
$\otimes L$	9,2	11,4	3,7	3,9	1,5	–4,1
$P_{AI}(\otimes L)$	0,31	0,38	0,123	0,13	0,05	0
AI	0,999					
W	0,981					

Анализ полученных результатов позволил сделать вывод о том, что защищенность речевой информации минимальна, и утечка такой информации может быть актуальной и без применения специальных ТСАР.

Следовательно, на основании расчетов можно говорить о том, что корректировка значений словесной разборчивости с помощью предлагаемых дополнений не противоречит результатам, полученным с использованием оценки защищенности речевой информации по методу AI [10, 11].

Погрешность результатов не превышает 5%. При этом авторы настоящей работы отмечают, что полученное максимальное значение абсолютной погрешности равно 7%, а относительной погрешности –

35%. Эти результаты справедливы для интервала отношений сигнал / шум от –20 до –5 дБ. На таком интервале данный метод точнее базового метода благодаря тому, что В.А. Трушин, И.Л. Рева и А.В. Иванов в работе [3] предлагают уменьшение методической погрешности при оценке защищенности речевой информации значительной степени секретности (рис. 2). Однако в расчетах, представленных выше, отношение сигнал / шум, в большей степени не входит в указанный интервал.

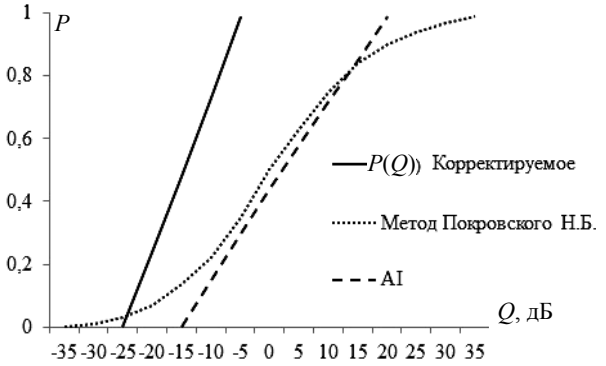


Рис. 2. Сравнение зависимостей коэффициентов восприятия формант *P* от относительного уровня интенсивности формант *Q*

Выводы

На основании вышеизложенного можно сделать следующие выводы:

1. Значения, полученные с помощью предложенных дополнений, позволяют оценить возможность утечки информации по акустическим и виброакустическим каналам при уменьшении методической погрешности метода оценки для отношения сигнал / шум от – 20 до – 5 дБ и при условии, что используются дополнительные ТСАР и различные средства шумовой очистки. Однако если при исследовании отношения сигнал / шум не войдут в представленный выше интервал, использование дополнений этого метода не будет достаточно удобным, поскольку значения будут завышены и не позволят получить точные значения словесной разборчивости.

2. Значения словесной разборчивости, которые были получены в ходе выполнения работы, достаточно велики, $W = 0{,}999$, что позволяет сделать вывод о том, что утечка речевой информации актуальна. При этом отношения сигнал / шум в большей степени не входят в диапазон от –20 до –5 дБ, и можно говорить, что полученные значения завышены. Однако погрешность при расчете с учетом предложенных дополнений в контрольной точке КТ 1 составляет 5%. Таким образом, можно утверждать, что хотя полученные значения завышены, защищенность помещения недостаточна и имеется возможность утечки речевой информации по техническим каналам.

3. Рассмотренные дополнения методики ФСТЭК не противоречат данным, полученным с помощью методики AI [12], и могут использоваться для оценки защищенности речевой информации.

Литература

1. Сапожков М.А. Акустика: справочник. – 2-е изд., перераб. и доп. – М.: Радио и связь, 1989. – 336 с.

2. Железняк В.К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В.К. Железняк, Ю.К. Макаров, А.А. Хорев // Специальная техника. – 2000. – № 4(5). – С. 2–11.

3. Трушин В.А. Усовершенствование методики оценки разборчивости речи в задачах защиты информации / В.А. Трушин, И.Л. Рева, А.В. Иванов // Ползуновский вестник. – 2012. – № 3-2. – С. 238–241.

4. Трушин В.А. Реализация оптимальной помехи при защите речевой информации от утечки по акустическому и виброакустическому каналам / В.А. Трушин, И.Л. Рева, А.В. Иванов // Научный вестник НГТУ. – 2011. – № 4. – С. 140–145.

5. Сагдеев К.М. Методика оценки технической защищенности информации в выделенных помещениях / К. М. Сагдеев, В.И. Петренко // Известия ЮФУ. Технические науки. – 2012. – № 12(137). – С. 109–121.

6. Олейников А.Н. Сравнительная характеристика параметров узконаправленных микрофонов. / А.Н. Олейников, А.О. Войтенко // Радиотехника Всеукр. межвед. науч.-техн. сб. – Харьков, 2013. – Вып. 173. – С. 172–179.

7. Хорев А.А. Средства акустической разведки: направленные микрофоны и лазерные акустические системы разведки // Спецтехника и связь. – 2008. – № 3(3). – С. 34–43.

8. Зайцев А.П. Технические средства и методы защиты информации: учеб. для вузов / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2013. – 442 с.

9. Меньшаков Ю.К. Защита объектов и информатизации от технических средств разведки / Рос. гос. гуманит. ун-т. – М., 2002. – 399 с.

10. Козлачков С.Б. Методические аспекты оценки защищенности речевой информации // Спецтехника и связь. – 2001. – № 2(6). – С. 44–47.

11. Паршин К.А., Анашкин П.А. Сравнительный анализ методик оценки защищенности речевой информации от утечки по прямым акустическим каналам при аттестации выделенных помещений / К.А. Паршин, П.А. Анашкин // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 5(15). – С. 13–26.

12. Рева И.Л. Сравнительный анализ объективных методов оценки разборчивости речи // Сборник научных трудов НГТУ. – 2010. – № 1(59). – С. 91–102.

13. Kryter K.D. Methods for the calculation and use of the articulation index // J. Acoust. Soc. Am. – 1962. – Vol. 34. – С. 1689–1697.

14. Fletcher H., Galt F. Perception of Speech and its Relation to Telephony // The Journal Acoustical Society of America. – 1950. – Vol. 22, No. 2. – PP. 89–151.

15. Продеус А.Н. О некоторых особенностях развития объективных методов измерений разборчивости речи // Науч.-техн. журнал. Тематический вып.: Электроника и нанотехнологии. – Киев: НТУ КПИ, 2010. – № 2(55). – С. 217–223.

Кустова Ольга Сергеевна
Магистрантка Омского гос. техн. ун-та (ОмГТУ)
Мира пр-т, д. 11, г. Омск, Россия, 644050
Тел.: +7-923-684-25-08
Эл. почта: kustova.olga.1994@yandex.ru

Шешенева Елизавета Анатольевна
Магистрантка ОмГТУ
Мира пр-т, д. 11, г. Омск, Россия, 644050
Тел.: +7-965-974-06-29
Эл. почта: yelizavetashesheneva@gmail.com

Калашников Алексей Михайлович
Студент ОмГТУ
Мира пр-т, д. 11, г. Омск, Россия, 644050
Тел.: +7-913-154-00-70
Эл. почта: betalaex@gmail.com

Kustova O.S., Shesheneva E.A., Kalashnikov A.M.

Correction of wordy legibility's value to evaluate the security of the premises

The protected premises, in which confidential information circulates, requires an assessment of their security. To assess the security of premises on the acoustic and vibro-acoustic channel may include appropriate techniques. There is a standard methodology of the Federal Service for Technical and Export Control, which has both advantages and disadvantages. In this regard, the purpose of this work is to correct the values of verbal intelligibility, with the help of the «Whisper» system, taking into account the additions of the standard methodology.
In the presented article the resulted results of the analysis of merits and demerits of a technique of an estimation of verbal intelligibility, additions of this technique are considered. To correct the values of verbal intelligibility in calculating the values of verbal intelligibility, taking into account the additions and improvements recommended in the publications of modern authors, we propose:
– consideration of the influence of technical means of acoustic reconnaissance, namely narrowly focused microphones and noise cleaning means;
– minimization of methodical error due to linearization of the dependence of the sensation level on perception and linearization of verbal intelligibility from the formant.
To analyze the data in the presented article, the calculations of the value of verbal intelligibility using another formant method are performed.
Keywords: shotgun microphone; wordy legibility; voice information leak; technical devices of acoustic reconnaissance.
doi: 10.21293/1818-0442-2018-21-2-43-47

References

1. Sapozhkov M.A. *Akustika: spravochnik* [Acoustics*:* reference book]. Moskva, Radio i svjaz' Publ., 1989. no. 2, 336 p.

2. Zheleznyak V.K, Makarov Yu.K., Horev A.A. Methodical approaches to assessing the effectiveness of protection of speech information. *Special equipment*. 2000, no. 4 (5), pp. 2–11 (In Russ.).

3. Trushin V.A., Reva I.L., Ivanov A.V Improvement of the methodology for assessing speech intelligibility in information security tasks. *Polzunovskii vestnik.* 2012, no. 3-2, pp. 238–241 (In Russ.).

4. Trushin V.A., Reva I.L., Ivanov A.V. Realization of the optimal interference in protecting voice information from leakage through acoustic and vibro-acoustic channels. *Nauchnyy vestnik NGTU*, 2011, № 4, pp. 140–145 (In Russ.).

5. Sagdeev K.M., Petrenko V.I. Methodology for assessing the technical security of information in dedicated rooms. *News of the SFU. Technical science*, 2012, no. 12 (137), pp. 109–121 (In Russ.).

6. Oleinikov A.N. Comparative characteristics of the parameters of narrowly directed microphones. *Radio engineering: All-Ukrainian interdepartmental scientific and technical collection,* Kharkiv, 2014, Issue 177, pp. 161–171 (In Russ.).

7. Horev A.A. Acoustical reconnaissance means: directional microphones and laser acoustic reconnaissance systems. *Special equipment and communications.* 2008, no. 3(3), pp. 34–43 (In Rus)

8. Zajcev A.P. Meshherjakov R.V., Shelupanov A.A. *Tehnicheskie sredstva i metody zashhity informacii.* [Technical means and methods of information security.] Moskva, Gorjachaja linija, Telekom Publ., 2013. 442 p.

9. Menshakov Ju.K. *Zashita objektov i informatizacii ot tehnicheskih sredstv razvedki.* [Protection of objects and information from technical means of reconnaissance.] Moskva, Rossijskiy gosudarstvennyj gumanitarnyj universitet Publ., 2002, 399 p.

10. Kozlachkov S.B. Methodical aspects of assessing the security of voice information. *Special equipment and communications.* 2001, no. 2(6), pp. 44–47 (In Russ.).

11. Parshin K.A., Anashkin P.A. Comparative analysis of methods for assessing the security of voice information from leakage through direct acoustic channels in the certification of allocated premises. *Herald UFD, Information security*, 2015, no. 5(15), pp. 13–26 (In Russ.).

12. Reva I.L. Comparative analysis of objective methods for assessing speech intelligibility. *Collection of scientific works of NSTU*. Novosibirsk, NSTU, 2010, no. 1(59), pp. 91–102 (In Russ.).

13. Kryter K.D. Methods for the calculation and use of the articulation index. *J. Acoust. Soc. Am.* 1962? vol. 34. pp. 1689–1697.

14. Fletcher H., Galt F. Perception of Speech and its Relation to Telephony. *The Journal Acoustical Soicety of Amerika.* 1950, vol. 22, no. 2, pp. 89–151.

15. Prodeus A. N. About features of the development of objective methods of measuring speech intelligibility. *Scientific and Technical Journal. Thematic issue Electronics and nanotechnology.* Kiev, NTU KPI, pp. 217–223 (In Russ.)

Olga S. Kustova
Master of Science Omsk State Technical University (OmSTU)
Mira pr., 11, Omsk, Russia, 644050
Phone.: +7-923-684-25-08
Email: kustova.olga.1994@yandex.ru

Elizaveta A. Shesheneva
Master of Science, OmSTU
Mira pr., 11, Omsk, Russia, 644050
Phone.: +7-965-974-06-29
Email: yelizavetashesheneva@gmail.com

Alexey M. Kalashnikov
Student of OmSTU
Mira pr., 11, Omsk, Russia, 644050
Phone.: +7-913-154-00-70
Email: betalaex@gmail.com

УДК 004.934.2

И.А. Гураков, Е.Ю. Костюченко, Д.И. Новохрестова, М.П. Силич

Алгоритм выделения формант и поиска выровненных фрагментов при подготовке к проведению фоноскопической экспертизы

Одним из методов, используемых при проведении фоноскопических экспертиз, является метод формантного выравнивания. В его рамках сперва выделяются фрагменты, содержащие идентичную фонетическую информацию, в их рамках находятся участки с совпадающими частотами первой и второй формант (выровненные участки), которые используются в дальнейшем в рамках экспертизы. В рамках данной работы предложен и реализован алгоритм выделения формантных частот и поиска на их основе кандидатов на роль выравненных участков. Это позволяет сократить время проведения экспертизы за счет сокращения объема используемой для ручного анализа информации.

Ключевые слова: форманта, формантное выравнивание, фоноскопическая экспертиза.
doi: 10.21293/1818-0442-2018-21-2-48-53

В криминалистике часто возникает потребность установления личности человека по имеющейся звукозаписи. С этой целью было разработано несколько методик идентификации лиц на основании физических параметров звучащей речи с применением ЭВМ [1–6]. Однако большинство этих методик требует наличия специализированного оборудования, позволяющего непосредственно обрабатывать звуковые сигналы [7]. При этом исследование звукозаписи перцептивными методами все равно является обязательным.

Известные в настоящее время методы использования результатов спектрального анализа речевых сигналов [8] можно классифицировать по типу выделяемых и сравниваемых признаков:

1) сравнение интегральных признаков усредненного спектра мощности, кросскорреляционного спектра, спектров более высокого порядка, среднего спектра отдельных фрагментов фонограмм для относительно длительного (около 10 с) суммарного звучания исследуемых голосов;

2) сравнение формантного спектра фонетически одинаковых звуков и звукосочетаний в сопоставимом контексте (ударные гласные, гласные равной степени редукции и т.д.). Иногда такой подход принято называть формантным микроанализом;

3) сравнение формантного спектра подобных артикуляторных событий:

– для мгновенных спектральных срезов;

– для динамических структур формант внутри звука, слога, слова;

4) сравнение специфики спектрально-формантных структур, реализующих одинаковые артикуляторные динамические явления;

5) сравнение спектрально-гармонических характеристик ларингального тембра голоса для просодически подобных событий;

6) сравнение спектров и их динамики внутри периода основного тона голоса для сопоставимых фаз смыкания / размыкания голосовых складок для сопоставимых речевых фрагментов [9].

В [10] в качестве признаков использовались частота основного тона, три формантные частоты на переходных и стационарных участках гласных, параметры огибающей спектра фрикативных, а также общая длительность слова и относительные длительности сегментов речи. Явным недостатком этого подхода является то, что просодические характеристики обладают малой различающей способностью и легко поддаются имитации.

В [11] наиболее важным фактором индивидуальности голоса считается частота основного тона, за ней – формантные частоты, размер флюктуаций частоты основного тона и наклон спектра. Однако, как и в [10], несмотря на устойчивость этих признаков, они легко поддаются имитации и имеют малую различительную способность.

В [12] наиболее важным фактором считаются формантные частоты, в частности, четвертая форманта, которая практически не зависит от типа фонемы и характеризует тракт [13].

Имеющиеся работы позволяют говорить о наличии недостатков как в самих используемых подходах, так и в аспектах их автоматизации.

Цель данной работы – автоматизация выделения формантных частот и поиска на их основе кандидатов на роль выровненных участков. Это позволяет сократить время проведения экспертизы за счет сокращения объема используемой для ручного анализа информации. Ручной этап анализа полностью устранить не представляется возможным, поскольку в конечном итоге при проведении фоноскопической экспертизы принимает решение и несет за него соответствующую ответственность именно эксперт.

Выделение формант

Типовая последовательность действий при выделении формант:

– просматривается спектрограмма и проводится поиск участков речевого спектра с ярко выраженной формантной картиной при наличии четвертой и более высоких формант. Обычно минимальной единицей рассмотрения является слог. На звукозаписи должен звучать голос только одного диктора [14];

– уяснение типичного поведения формант данного диктора для однотипных артикуляторных событий;

– выбор опорного фрагмента фонограммы, на котором прослеживается траектория четырех или более формант и выбранные спектральные максимумы однозначно интерпретируются как форманты, т.е. соответствуют теоретическому представлению, а все исчезновения формант или появление «лишних» формант можно разумно интерпретировать. Фрагмент выбирается с учетом типичного поведения формант данного диктора в данной артикуляторной ситуации;

– по выбранному фрагменту строится спектр и выбираются выраженные максимумы мощности в диапазонах, соответствующих стандартным диапазонам расположения формант.

Проблемы выделения формант:

1. Форманты постоянно меняют свое положение в процессе звучания слога. Если рассматривается не чистая гласная, а гласная в составе некоторого слога, то согласные, расположенные по обе стороны от нее, будут оказывать влияние на расположение формант, и с течением времени это влияние будет меняться. В результате, в одном слоге первые четыре форманты могут принимать теоретически бесконечное количество комбинаций. Можно выбирать только слоги, на спектрограммах которых можно выделить участок, на котором все форманты не изменяют свое положение, но такие случаи встречаются довольно редко, и нет никаких гарантий, что эти частоты действительно будут повторяться в других артикуляторно подобных ситуациях для того же диктора, поскольку положение формант зависит не только от характеристик речевого тракта и фонемы, но и от интонации [15] и психического состояния диктора, которые могут меняться в процессе разговора. Этот факт заметно снижает шанс корректной верификации диктора по коротким аудиозаписям (3–6 с) (рис. 1).

2. Появление «лишних» формант в одном или нескольких диапазонах спектра – очень частое явление. Стандартная методика предлагает не рассматривать такие случаи, однако факт того, что у конкретного диктора, в конкретной артикуляторной ситуации, в конкретной области спектра возникает «лишняя» форманта, также можно использовать при идентификации (рис. 2).

3. Проблему выбора диапазона также нельзя оставлять в стороне. Согласно методике, диапазон выбирается на основе типичного поведения формант для подобных артикуляторных событий, однако в обычной речи такие события не всегда встречаются часто, особенно для коротких аудиозаписей. В ударных слогах гласная может звучать до 120 мс, а диапазон, из которого выделяются форманты, обычно берут не более 30 мс. Следовательно, нужно определить правила выбора диапазона в случае, когда недостаточно подобных артикуляторных событий для выявления типичных закономерностей движения формант, либо перейти от рассмотрения одного выровненного участка артикуляторного события исследуемой аудиозаписи к множеству участков одного артикуляторного события.

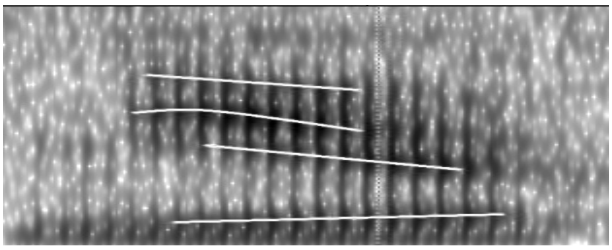


Рис. 1. Пример движения формант на примере спектрограммы слога «няк», зависимость частоты от времени

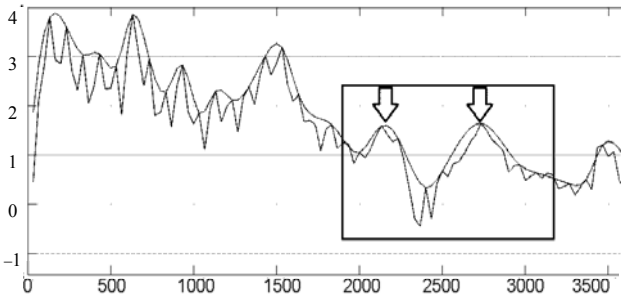


Рис. 2. Пример «лишней» форманты:
ось абсцисс – частота, Гц, ординат – уровень

После анализа выделенных недостатков была сформулирована задача автоматизированного выделения формант.

Решение задачи автоматизированного выделения формант состоит в разработке метода и алгоритмов, использование которых позволит выделять список комбинаций первых четырех формант из звукозаписи с минимальным участием специалиста для контроля процесса.

Главные отличия новой методики от стандартной:

– в каждой исследуемой записи рассматривается не один 30 мс интервал, а множество таких интервалов с некоторым шагом внутри области звучания гласной. В результате каждому слогу будет соответствовать не один, а множество комбинаций формант;

– «лишние» форманты, которые в традиционной методике не рассматриваются, в новом методе были интерпретированы как два варианта одной форманты. Если такая форманта встречается в процессе анализа, то создается две комбинации формант как с одним вариантом, так и с другим. В результате на один интервал, в теории, может приходиться до 16 комбинаций формант.

Автоматизация выделения формант

Поиск формант состоит из двух этапов. В рамках первого проводится проверка предположения о наличии формант в анализируемом диапазоне частот. На втором этапе проводятся непосредственно измерения частот формант. Алгоритмы, позволяющие автоматизировать эти этапы, представлены на рис. 3 и 4.

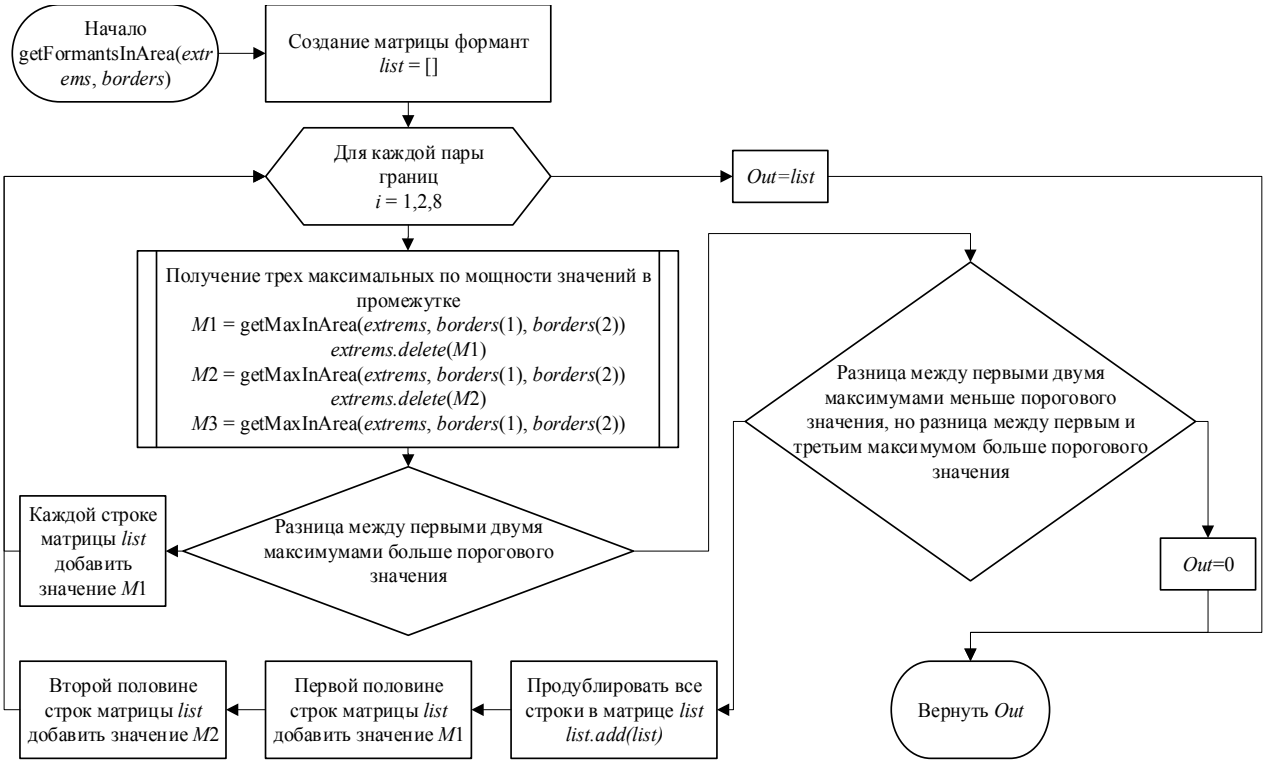


Рис. 3. Блок-схема алгоритма принятия решения о наличии или отсутствии формант в заданном диапазоне частот

Поиск выровненных фрагментов

После этапа выделения формант проводится поиск выровненных участков, на которых частоты первой и второй формант совпадают. Реализованное программное обеспечение позволяет как непосредственно находить по измеренным ранее формантным частотам такие участки, так и фильтровать только те из них, на которых наблюдается совпадение третьей и четвертой формант. Наличие таких участков на идентичных с фонетической точки зрения фрагментах речевого сигнала является аргументом в пользу утверждения о совпадении дикторов на соответствующих анализируемых фрагментах. Точность совпадения формант является регулируемым параметром и задается пользователем. Программа написана на языке Matlab 2018a. В единственной таблице перечислены все найденные комбинации формант для каждого шага. В левой части формы указываются границы диапазонов частот, в которых программа будет искать каждую из формант. В программе можно осуществлять контроль корректности найденных формант. Для этого предусмотрены функции просмотра спектра, соответствующего конкретному набору формант, и просмотра положения промежутка длительностью 30 мс, которому соответствует этот спектр. Если, по мнению проверяющего, набор формант не подходит данному спектру, он может удалить соответствующую строку таблицы при помощи кнопки «Delete Row». После того как данные будут проверены, их можно экспортировать в файл с расширением «.xlsx», нажав кнопку «Export To Exl».

Разработан модуль, позволяющий сравнивать между собой списки формант двух выбранных аудиозаписей и выводить список выровненных и совпавших участков.

В данном модуле для каждой аудиозаписи выбираются границы диапазонов частот, в которых будут искаться форманты, выбираются файлы, которые будут сравниваться, и разбросы для каждой форманты, в пределах которых будет производиться заключение о совпадении или несовпадении формант. Этот разброс необходим по причине неустойчивого положения формант, в особенности третьей и четвертой, которые даже у одного и того же диктора в одинаковых слогах далеко не всегда принимают одинаковые значения. При выборе разброса нужно учитывать, что разница между формантами всегда будет кратна 33,(3) Гц, это связано с тем, что берутся промежутки длиной в 30 мс, а значит, независимо от частоты дискретизации, шаг частоты в спектре будет равен 33.(3). Процесс сравнения аудиозаписей запустится после нажатия клавиши «Start».

Результатом работы данной программы являются два списка: список выровненных участков и список совпавших комбинаций формант. О степени схожести артикуляционных трактов дикторов можно судить по количеству выровненных и совпавших участков, а не по одному срезу, как предлагает традиционная методика.

Анализ получаемых с помощью программы результатов

В ходе работы было сделано по 20 записей для 6 гласных в составе однотипного слога для 2 дикторов. Для каждого слога было составлено распределение, всего 240 распределений.

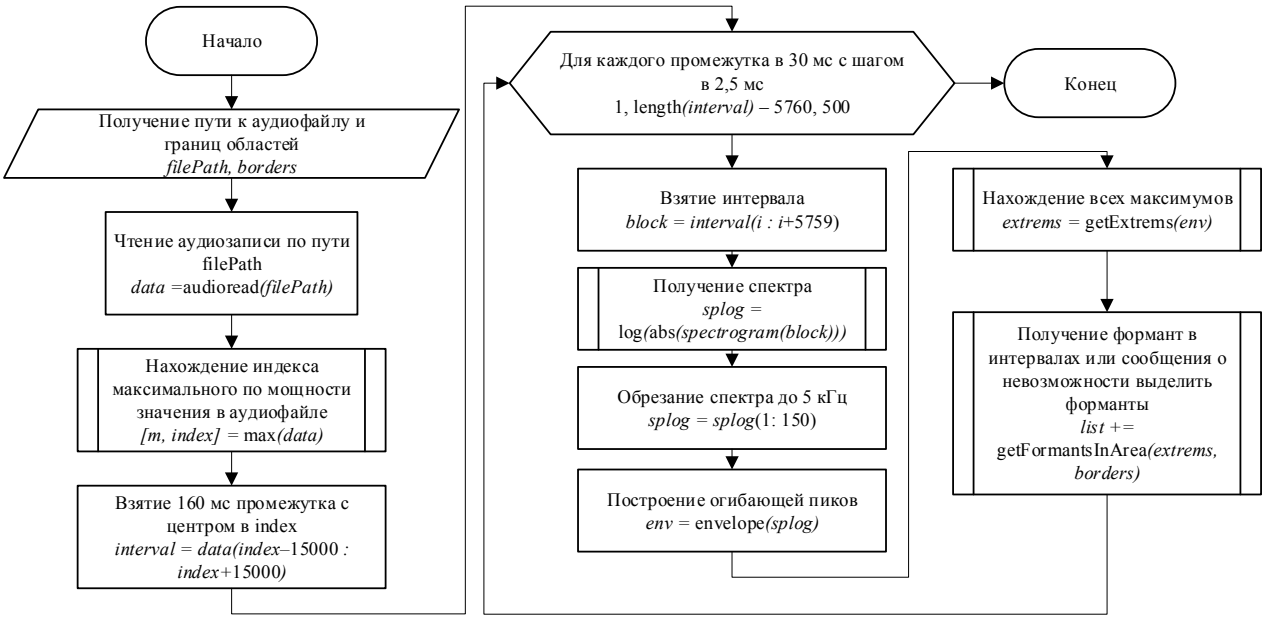


Рис. 4. Блок-схема алгоритма выделения формант

В дальнейшем они будут использоваться для обучения нейронной сети с целью еще большей автоматизации процесса. Небольшой размер базы объясняется предварительным тестированием программы, а не получением полноценного распределения формант. Были подсчитаны количества выровненных участков и совпавших формант для каждой из гласных. Пример результатов для звука «ы» (слог «нык») представлен в таблице.

Как видно из результатов сравнения, среднее количество выровненных участков и среднее количество совпавших комбинаций формант при сравнении записей в рамках одного диктора, как правило, многократно превышают эти параметры при сравнении разных дикторов. По количеству пар записей без выровненных участков и количеству пар записей без совпавших комбинаций формант также можно заметить, что при сравнении записей в рамках одного диктора эти значения заметно меньше, чем при сравнении разных дикторов.

Отдельное внимание стоит уделить парам записей, между которыми не было найдено совпадений. Стоит напомнить, что распределение, получаемое с каждой записи, обладает приличной избыточностью за счет «лишних» формант, а значит, что при корректно определенных диапазонах частот тот интервал, с которого традиционная методика предлагает выделять форманты, однозначно будет входить в эти распределения. Тот факт, что сравнение некоторых записей одного диктора показывает отсутствие совпавших пар формант, говорит о том, что традиционная методика также будет показывать отрицательный результат на этих парах записей.

Также стоит обратить внимание на огромную разницу между количеством выровненных участков и количеством совпавших пар формант. Традиционная методика утверждает, что высокие форманты полностью определяются нижними, но, учитывая результаты эксперимента, становится очевидно, что одному набору первых двух формант одного диктора всегда соответствует множество вариантов третьей и четвертой формант. Возвращаясь к традиционной методике. После того как найден участок на исследуемой записи и осуществляется поиск выровненных участков, на одной записи может быть найдено множество выровненных участков, однако только 1–2 из них могут действительно соответствовать полному набору формант. Следовательно, у специалиста, который будет проводить анализ, есть высокий шанс ошибиться и сделать неверный вывод о схожести артикуляторных трактов дикторов в данных двух записях.

Результаты сравнения дикторов по слогу «нык»

	1-й и 1-й диктор	1-й и 2-й дикторы	2-й и 2-й диктор
Среднее количество выровненных участков	46,94737	4,0975	25,14211
Среднее количество совпавших комбинаций формант	4,068421	0,2875	4,710526
Максимальное количество выровненных участков	260	68	224
Максимальное количество совпавших участков	28	7	21
Количество пар записей без выровненных участков	14	228	36
Количество пар записей без совпавших комбинаций	148	381	126

Заключение

В результате анализа источников и проведения ряда экспериментов была выявлена актуальность разработки автоматизированной системы выделения формант и, как продолжение этой системы, автома-

тизированной системы сравнения артикуляционных трактов дикторов на основе двух аудиозаписей. Были исследованы современные методы полуавтоматической верификации дикторов. В частности, был проанализирован метод формантного выравнивания, были выделены слабые места традиционной методики, которые учитывались при разработке нового алгоритма. Предложен новый метод верификации диктора на основе выровненных фрагментов, но с использованием множества опорных фрагментов из одной звукозаписи.

Был описан алгоритм новой методики и выполнена программная реализация на основе описанного алгоритма. Проведено первоначальное тестирование разработанных алгоритмов.

Были проанализированы полученные результаты. Сделан первичный вывод о работоспособности метода, а также подтверждены некоторые слабые места традиционной методики.

Получаемые значения частот формант могут быть использованы при проведении фоноскопической экспертизы. Кроме того, эти значения могут использоваться при изучении динамики характеристик речевого сигнала в процессе речевой реабилитации при оперативном лечении онкологических заболеваний органов речеобразующего тракта.

Работа выполнена при поддержке Российского научного фонда, проект «Восстановление речевой функции с использованием технических методов и математического моделирования у больных раком полости рта и ротоглотки после хирургического лечения», № 1615-00038.

Литература

1. Рахманенко И.А. Программный комплекс для идентификации диктора по голосу с применением параллельных вычислений на центральном и графическом процессорах // Доклады ТУСУР. – 2017. – Т. 20, № 1. – С. 70–74.

2. Rakhmanenko I. Text-independent speaker verification using convolutional deep belief network and gaussian mixture model / I. Rakhmanenko, R. Meshcheryakov // CEUR Workshop Proceedings. Secure Information Technologies 2017 (BIT 2017). – Moscow, Russia, 06–07 December 2017. – 2017. – PP. 118–121.

3. Qing Q. Speech authentication and content recovery scheme for security communication and storage / Q. Qing, W. Hongxia, S. Xingming et al. // Telecommunication Systems. – 2017. – Vol. 67, No. 4. – PP. 635–649.

4. Qiuyu Z. An efficient speech perceptual hashing authentication algorithm based on DWT and symmetric ternary string / Z. Qiuyu, X. Pengfei, H. Yibo, D. Ruihong, Y. Zhongping // International Journal of Information and Communication Technology. – 2017. – Vol. 12, No. 1-2. – PP. 31–50.

5. Felker N. Voice input for authentication / N. Felker, S. Chen, S. Mishra // Technical Disclosure Commons. Defensive Publications Series. – 2018. – Vol. 1128. – URL: https://www.tdcommons.org/cgi/viewcontent.cgi?article=2191&context=dpubs_series (дата обращения: 01.06.2018).

6. Hundal J.K. Some feature extraction techniques for voice based authentication system / J.K. Hundal, S.T. Hamde // 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). – 2017. – PP. 419–421. – URL: http://dx.doi.org/10.1109/ICPCSI.2017.8392328 (дата обращения: 01.06.2018).

7. Экспертиза видео- и звукозаписей [Электронный ресурс]. – Режим доступа: http://www.sudexpert.ru/possib/video.php (дата обращения: 25.04.2018).

8. Wu C. Text-independent speech emotion recognition using frequency adaptive features / C. Wu, C. Huang, H. Chen // Multimedia Tools and Applications. – 2018. – PP. 1–11

9. Коваль С.Л. Сборник научно-методических рекомендаций по выполнению криминалистических экспертиз звукозаписей речи. – СПб.: Центр речевых технологий. – 2000. – 174 с.

10. Sorokin V.N. Speaker verification using the spectral and time parameters of voice signal / V.N. Sorokin, A.I. Tsyplikhin // Journal of Communications Technology and Electronics. – 2010. – Vol. 10, No. 2. – PP. 87–104.

11. Multidimensional representation of personal quality of vowels and its acoustical correlates / H. Matsumoto, S. Hiki, T. Sone, T. Nimura // IEEE Trans. – 1973. – Vol. 21, No. 5. – PP. 428–436.

12. Lavner Y. The effects of acoustic modifications on the identification of familiar voices speaking isolated vowels / Y. Lavner, I. Gath, J. Rosenhouse // Speech Communication. – 2000. – Vol. 30, No. 1. – PP. 9–26.

13. Acoustic roles of the laryngeal cavity in vocal tract resonance / H. Takemoto, S. Adachi, T. Kitamura, P. Mokhtari, K. Honda // The Journal of the Acoustical Society of America. – 2006. – Vol. 120, No. 4. – PP. 28–38.

14. Vainio L. The Influence of Number Magnitude on Vocal Responses / L. Vainio, T. Mustonen, M. Vainio // Journal of Motor Behavior. – 2018. – PP. 1–12.

15. Variability of articulator positions and formants across nine English vowels / D.H. Whalen, W. Chen, M.K. Tiede, H. Nam // Journal of Phonetics. – 2018. – Vol. 68. – PP. 1–14.

Гураков Иван Алексеевич
Студент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр., д. 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-34-26
Эл. почта: gia@fb.tusur.ru

Костюченко Евгений Юрьевич
Канд. техн. наук, доцент каф. КИБЭВС ТУСУР
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-34-26
Эл. почта: key@keva.tusur.ru

Новохрестова Дарья Игоревна
Техник лаб. медико-биологических исследований (ЛМБИ) ТУСУР
Ленина пр., д. 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-29 (внутр. 29-66)
Эл. почта: ndi@fb.tusur.ru

Силич Мария Петровна
Профессор кафедры автоматизации обработки информации (АОИ) ТУСУР
Ленина пр., д. 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-91 (внутр. 20-11)
Эл. почта: smp@muma.tusur.ru

Gurakov I.A., Kostyuchenko E.Y.,
Novokhrestova D.I., Silich M.P.

Algorithm for formants calculation and searching of aligned fragments in preparation for phonoscopic examination

One of the methods used in conducting phonoscopic examinations is the method of formant alignment. Within this framework, fragments containing identical phonetic information are first identified, in their frames there are sections with coinciding frequencies of the first and second formants (aligned areas), which are used later in the phonoscopic examination. During this work, an algorithm for allocating the formant frequencies and searching on their basis candidates for the role of aligned areas has been proposed and implemented. This allows you to shorten the time of the phonoscopic examination due to the reduction of information used for manual analysis.

Keywords: formant, formant alignment, phonoscopic examination.
doi: 10.21293/1818-0442-2018-21-2-48-53

References

1. Rakhmanenko I.A. Software system for speaker verification using parallel CPU and GPU computing. Proceedings of TUSUR University, 2017, vol. 20, no. 1, pp. 70–74 (In Russ.).

2. Rakhmanenko I., Meshcheryakov R. Text-independent speaker verification using convolutional deep belief network and gaussian mixture model. *CEUR Workshop Proceedings. Secure Information Technologies 2017 (BIT 2017), Moscow, Russia, 06–07 December 2017*, pp. 118–121.

3. Qing Q., Hongxia W., Xingming S., Yunhe C., Huan W., Canghong S. Speech authentication and content recovery scheme for security communication and storage. *Telecommunication Systems*, 2017, vol. 67, no. 4, pp. 635–649.

4. Qiuyu Z., Pengfei X., Yibo H., Ruihong D., Zhongping Y. An efficient speech perceptual hashing authentication algorithm based on DWT and symmetric ternary string. *International Journal of Information and Communication Technology,* 2017, vol. 12, no. 1-2, pp. 31–50.

5. Felker N., Chen S., Mishra S. Voice input for authentication. *Technical Disclosure Commons. Defensive Publications Series*, 2018, vol. 1128. Available at: https://www.tdcommons.org/cgi/viewcontent.cgi?article=2191&context=dpubs_series (accessed: 1 June 2018).

6. Hundal J.K., Hamde S.T. Some feature extraction techniques for voice based authentication system. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 2017, pp. 419–421. Available at: http://dx.doi.org/10.1109/ICPCSI.2017.8392328 (accessed: 1 June 2018).

7. *Ehkspertiza video- i zvukozapisej* [Examination of video and sound recordings] Available at: http://www.sudexpert.ru/possib/video.php (accessed: 25 April 2014).

8. Wu C. Text-independent speech emotion recognition using frequency adaptive features / C. Wu, C. Huang, H. Chen // Multimedia Tools and Applications, 2018, pp. 1–11.

9. Koval S.L. *Sbornik nauchno-metodicheskih rekomendacij po vypolneniyu kriminalisticheskih ehks-pertiz zvukozapisej rechi* [Collection of scientific and methodical recommendations on the performance of forensic examinations of sound recordings of speech]. Saint-Petersburg.: Center of speech technologies. 2000, 174 c. (in Russ.).

10. Sorokin V.N. Speaker verification using the spectral and time parameters of voice signal / V.N. Sorokin, A.I. Tsyplikhin // Journal of Communications Technology and Electronics, 2010, vol. 10, no. 2, pp. 87–104.

11. Multidimensional representation of personal quality of vowels and its acoustical correlates/ H. Matsumoto, S. Hiki, T. Sone, T. Nimura // IEEE Trans. 1973, vol. 21, no. 5, pp. 428–436.

12. Lavner Y. The effects of acoustic modifications on the identification of familiar voices speaking isolated vowels / Y. Lavner, I. Gath, J. Rosenhouse // Speech Communication. – 2000, vol. 30, no. 1, pp. 9–26.

13. Acoustic roles of the laryngeal cavity in vocal tract resonance / H. Takemoto, S. Adachi, T. Kitamura, P. Mokhtari, K. Honda // The Journal of the Acoustical Society of America, 2006, vol. 120, no. 4, pp. 28–38.

14. Vainio L. The Influence of Number Magnitude on Vocal Responses / L. Vainio, T. Mustonen, M. Vainio // Journal of Motor Behavior, 2018, pp. 1–12.

15. Variability of articulator positions and formants across nine English vowels / D.H. Whalen, W. Chen, M.K. Tiede, H. Nam // Journal of Phonetics, 2018, vol. 68, pp. 1–14.

Ivan A. Gurakov
Student, Department of Complex Information Security,
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 41-34-26
Email: gia@fb.tusur.ru

Evgeny Y. Kostyuchenko
Ph.D., associate professor,
Department of Complex Information Security, TUSUR
40, Lenina pr., Tomsk, Russia, 634050
ORCID: 0000-0001-8000-2716
Phone: +7 (382-2) 41-34-26
Email: key@keva.tusur.ru

Daria I. Novokhrestova
Technician, Laboratory of Medic-Biologigal Researches,
TUSUR
40, Lenina prosp., Tomsk, Russia, 634050
ORCID: 0000-0002-4931-1681
Phone: +7 (382-2) 70-15-29 (main 29-66)
Email: ndi@fb.tusur.ru

Maria P. Silich
Department of Data Processing Automation, TUSUR
40, Lenina prosp., Tomsk, Russia, 634050
ORCID: 0000-0002-4931-1681
Phone: +7 (382-2) 70-15-29 (main 29-66)
Email: ndi@fb.tusur.ru

УДК 528.873

М.Ю. Катаев, А.В. Богомолов

Особенности кластеризации многоспектральных изображений спутникового прибора Landsat

Исследуются особенности тематической обработки данных дистанционного зондированияЗемли, полученных в различных диапазонах оптического спектра с помощью прибора Landsat-8. Кластеризация данных многоспектральной съемки, основанная на измерениях в первых каналах спутникового прибора (пространственное разрешение 30 м), не позволяет с высокой точностью выделять типы поверхности за счет неоднородности их смешивания. Изучение проблемы выделения однородных участков по различным признакам и является предметом данной статьи. Приведены результаты обработки реальных данных спутниковых измерений. Полученные результаты показывают хорошую согласованность кластеризованных данных с известным мировым аналогом GlobeLand30.

Ключевые слова: дистанционное зондирование, обработка спутниковых изображений, многоспектральный, кластеризация.
doi: 10.21293/1818-0442-2018-21-2-54-59

В последнее десятилетие мониторинговые методы дистанционного зондирования Земли (ДЗЗ) из космоса являются одними из важнейших подходов к исследованию параметров атмосферы и поверхности Земли [1, 2]. Особую значимость имеют направления, связанные с изучением поверхности Земли, позволяющие изучать природные и техногенные объекты, а также, изменения, которые связаны с объектами. Для огромных территорий России единственно возможными для контроля экологического состояния, решения производственных и научных задач и др. являются данные мониторинга ДЗЗ. Получаемые спутниковые данные проходят несколько этапов обработки: предварительную, тематическую и анализ [1].

На этапе предварительной обработки разработано множество методов, которые привязаны к каждому спутнику отдельно, так как учитывают индивидуальные характеристики орбиты и измерительного прибора. Методы тематической обработки являются более унифицированными и разбиты на группы, связанные с размерностью измерений (пространство, время, спектральный канал). Одним из наиболее развитых подходов тематической обработки является формирование попиксельных изображений, где каждое изображение связано с характеристиками спектральных каналов, и их совместный анализ. Анализ возможен независимо для каждого изображения или их функциональных преобразований (индексов) [1].

Важным направлением исследований является выделение типов поверхности на спутниковом снимке и изучение свойств выделенных классов. Для спутниковых снимков с низким пространственным разрешением (более 100 м) выделение классов проходит более успешно, чем для среднего (10–50 м). Это связано с тем, что в первом случае за счет осреднения различных типов поверхности, попадающих в пиксель, классы являются более однородными, чем для второго случая. Однако более высокое пространственное разрешение позволяет получить дополнительные возможности при изучении пространственно-временных изменений типов поверхности.

Постановка задачи

При тематической обработке данных среднего пространственного разрешения типично проводят выделение однородных участков по спектральным или иным признакам. Процедура выделения таких участков связана с кластеризацией (сегментацией) спутниковых изображений [3–8]. Проблемой выделения однородных участков по различным признакам является обнаружение неперекрывающихся классов. Однако выполнение этого условия для реальных спутниковых данных весьма проблематично, поскольку для естественных ландшафтов сказывается рельеф (наклон поверхности относительно точки освещения Солнцем и наблюдением), а также типы поверхности, попадающие в пиксель с разной площадью. Нельзя забывать и про влияние состояния атмосферы (освещенность, замутнённость, наличие дымки, облачности и т.д.). Эти аспекты, а также их естественные суточные и сезонные изменения делают задачу кластеризации весьма сложной.

Кластеризация спутниковых изображений заключается в разбиении изображения на непересекающиеся пространственные области на основе близости их спектральных, индексных (например, вегетационных, водных и др.), пространственных или пространственно-временных характеристик (например, текстурных).

В настоящее время известны и широко используются на практике методы кластеризации, позволяющие разбивать спутниковые изображения на классы, соответствующие различным типам поверхности (лес, вода, город, поле и др.). Существует достаточно много подходов к кластеризации: иерархические или неиерархические методы, четкие или нечеткие, масштабируемые или немасштабируемые, с выбором числа и типа кластеров или нет, последовательные или параллельные,

отличающиеся по выбору меры расстояния (Евклидово, городские кварталы, Чебышева, степенное и др.), метрики (односвязные, полносвязные, взвешенные и др.) и др. При решении практических задач существуют особенности, которые необходимо учитывать при выполнении процедуры кластеризации. Выбор метода кластеризации из множества подходов связан с их эффективностью при решении конкретной задачи. При этом необходимо учитывать проблему выбора метода, меры расстояния, числа кластеров, формы кластеров, их пересечения и др.

В случае кластерного анализа спутниковых изображений отсутствуют априорные сведения о количестве классов (типов поверхности), спектральных и пространственных характеристик (возможного наличия в пикселе нескольких типов поверхности). Известные программные продукты, такие как Multispec [https://engineering.purdue.edu/~biehl/MultiSpec/], ERDAS Imagine [www.mapinfo.ru/product/erdas], ENVI [HarrisGeospatial.com], ArcGIS [https://www.arcgis.com/], решают задачи кластеризации для спутниковых приборов различного пространственного разрешения, учитывают особенности для исследуемой территории Земли (определяются типы поверхности, углы освещения Солнцем, состояние атмосферы и др.). Однако для получения качественного результата требуется значительный вклад ручного труда и знаний пользователя. Наиболее распространенный подход к кластеризации мультиспектральных спутниковых изображений в отсутствие обучающей выборки основан на применении алгоритмов, использующих пространство спектральных признаков изображения (спектральных каналов).

Изучая опыт практический реализации различных авторов [2–16], нами выбран алгоритм кластеризации k-средних. Число кластеров нами было ограничено и задано 12, учитывая опыт построения баз данных типов поверхности. Целью является изучение различных аспектов кластеризации для понимания процессов, необходимых для разработки автоматизированной процедуры кластеризации.

Спутниковый прибор Landsat-8

Использование измеренных изображений прибором Landsat [https://landsat.usgs.gov/] в научных и производственных целях начинает свой отсчёт с 1970 г. Этому способствует несколько причин: 1) близкие по числу и спектральным свойствам характеристики спектральных каналов приборов, 2) достаточно высокое пространственное разрешение (30 м в видимом и ближнем инфракрасном спектральном диапазоне) и 3) наличие панхроматического канала (15 м). Спектральные каналы приборов Landsat позволяют выделять разнообразные типы поверхности, в том числе и наземную растительность. Однако результаты анализа литературных источников говорят, что имеются некоторые отличия между различными исследованиями одной и той же территории. Поэтому важным элементом для исследований остается вопрос точности выделения типов поверхности.

Кластеризация спутниковых изображений

Особенностью многоспектральной спутниковой измерительной техники Landsat является возможность наблюдать поверхность Земли в любое время суток, используя каналы видимого, ближнего ИК или ИК диапазона спектра. Основой измерений является спектральная яркость типов поверхности, попадающих в пиксель, которая определяется коэффициентами отражения типов поверхности и их площадью в пикселе. Автоматическое распознавание типов поверхности на спутниковом изображении необходимо для составления разнообразных карт, включающих в себя информацию о растительности, почвах, водных объектах, городах и др.

Сравнивая карты за различные промежутки времени, удаётся выявлять изменения формы, площади и свойств типов поверхности за счёт естественных или антропогенных процессов. На первом этапе тематической обработки спутниковых изображений выполняется кластеризация изображения, т.е. выделение отдельных участков, характеризующихся однородностью внутри участка и существенными отличиями между участками. На втором этапе обработки выделенные участки подлежат классификации или определению типа поверхности (лес, вода, город или др.).

Для решения задач кластеризации необходимо выбрать множество признаков, характеризующих изображение, что определяет набор методов исследования. Одним из наборов признаков могут быть измеренные значения спектральной яркости в каждом выбранном канале. Эти значения могут быть усреднены на некоторой выбранной области (например, области, состоящей из 3×3 пикселей, что ведет к понижению пространственного разрешения). Если используется попиксельный подход, то каждый кластер состоит из пикселей, представленных на изображении. На основе спектральных каналов можно рассчитать тот или иной индекс, например вегетационный, который и будет являться изображением, подлежащим анализу. Можно использовать не только спектральные, но и пространственные характеристики, используя, например, текстурные или морфологические характеристики, и др.

Важным направлением является переход из пространства спектральных признаков в пространство цветовых признаков, например RGB. В этом случае можно использовать классические подходы обработки изображений. Поэтому, поиск условий для автоматизации процесса кластеризации является важным.

Анализ результатов кластеризации

Нами выполняются работы по анализу пространственно-временных данных спутникового прибора MODIS, пространственное разрешение

пикселя которого составляет 250, 500 м [17, 18]. В некоторых научных и практических задачах возникает необходимость более детального рассмотрения процессов изменения типов поверхности, и для этих целей применяют данные прибора Landsat.

В данной работе для целей кластеризации рассматривается алгоритм k-средних (k-means), суть которого связана с разбиением всех пикселей на кластеры таким образом, чтобы минимизировать сумму расстояний от каждого пикселя до соответствующих им центров кластеров. Параметрами кластера могут быть: значения RGB-каналов синтезированного изображения, значения спектральных каналов или индексов (например, вегетационный индекс). Множество пикселей изображения делится на k кластеров, сама кластеризация выполняется за счёт смещения центров для поиска из устойчивого положения. В качестве спутниковых данных нами были выбраны спутниковые изображения Landsat-8. Разбиение на кластеры проводится на основе расстояний между пикселями изображения, на которое потом накладывается определенное ограничение, разделяющее кластеры между собой. Примерами функций, определяющими расстояние, могут быть эвклидово расстояние (1), или Чебышевская мера (2), представленные формулами:

$$D(i,k)=\sqrt{\sum_{i=1}^{N}(I(i,j)-I(j,k))^2}\,, \qquad (1)$$

$$D(i,k)=\max_{1,\dots N}\left|(I(i,j)-I(j,k))\right|, \qquad (2)$$

где i – индекс текущего наблюдения, k – индекс кластера, N – количество признаков цветового пространства ($N = 3$) и $\mathbf{I} = \{R, G, B\}$ – вектор в выбранном цветовом пространстве.

На рис. 1 показан результат кластеризации синтезированного спутникового изображения ($R = 4$, канал Landsat-8, $G = 3$, $B = 2$) для территории, расположенной рядом с г. Томском, полученный в июне 2016 г., на основе выражения (1). Число обнаруженных классов равно 12. Из рис. 1 видно, что имеются однородные области, связанные с водой – река Томь, участками города, сельскохозяйственными и заливными полями, лесом. В большей своей части пиксели того или иного участка соответствуют определенным типам поверхности, однако имеется много артефактов. Например, на поверхности воды обнаруживаются пиксели, характеристики которых совпадают с пикселями, расположенными на поверхности Земли. Это всё приводит к выводу, что помимо цветовых признаков необходимо использовать спектральные.

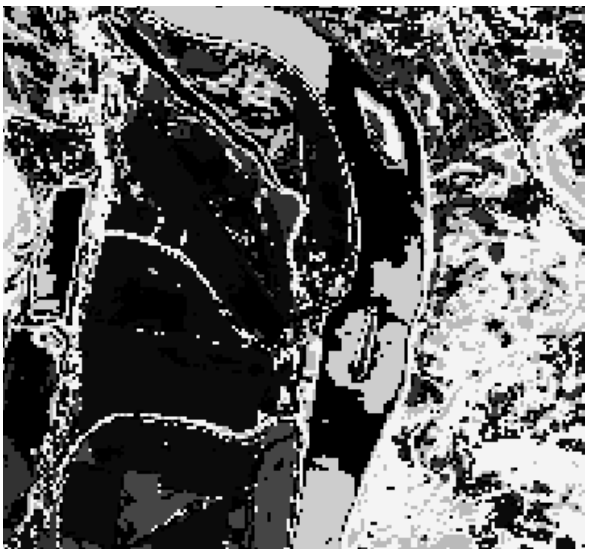
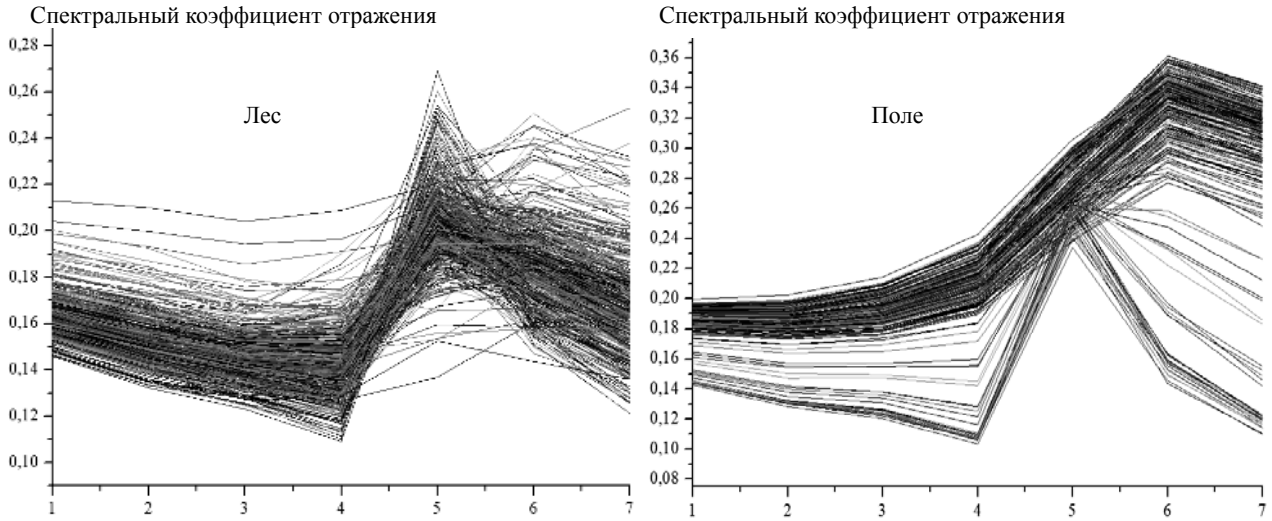


Рис. 1. Пример кластеризации синтезированного спутникового изображения для спектральных каналов 4-3-2

На рис. 2 представлены спектральные кривые коэффициентов отражения в первых семи каналах прибора Landsat-8.



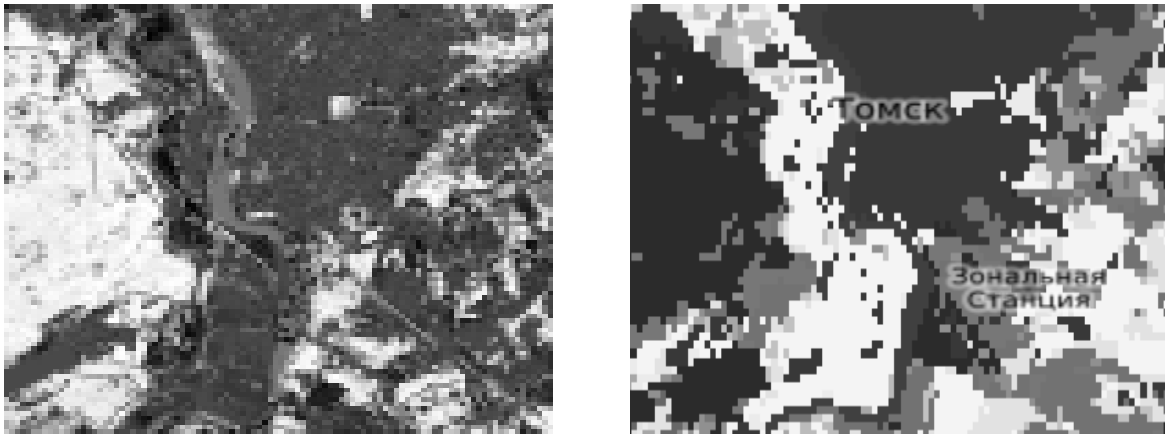
а *б*

Рис. 2. Значения спектрального коэффициента отражения для каждого из семи спектральных каналов Landsat-8 для области 15×15 пикселей (450×450 м) для леса – *а* и поля – *б*

Нами были выбраны однородные участки по типам поверхности размером 15×15 пикселей и для каждого из них выбраны значения спектральных коэффициентов отражения. Хорошо видно, что вариации значений спектральных кривых для всех пикселей весьма значительны, а также явно просматриваются разные типы поверхности в выбранной области. Это говорит о том, что в части пикселей присутствует несколько типов поверхностей с разной площадью, что изменяет типичное для определенного типа поверхности распределение значений (см. рис. 2). Например, на рис. 2, *а* в области класса поля в нескольких пикселях присутствуют деревья (нижняя часть рисунка), хотя большая часть пикселей принадлежит классу поля.

Учитывая специфику распределения значений коэффициентов отражения, нами выделены средние значения коэффициентов отражения для нескольких классов: поле, вода, город, лес и др. Далее проведена кластеризация согласно заданному количеству и типу классов.

Результат приведен на рис. 3, *а*. Сравнение полученных нами результатов кластеризации и глобальной базы данных типов поверхности GlobeLand30 [http://www.global-landcover.com] по данным Landsat-8 показано на рис. 3. Из рис. 3 видно, что в глобальной базе данных проводилось существенное увеличение пространственного разрешения для достижения однородности областей (увеличение площади одного из типов поверхности по отношению к другому). В выполненных нами расчётах такого осреднения не сделано, что приводит к появлению множества мелких областей с одним из выделенных типов поверхности. Обнаружено, что в отражении воды р. Томи присутствуют участки с разной глубиной, и это приводит к появлению не одного, а нескольких типов водной поверхности. Поэтому наличие точных значений участков глубины, полученных, например, с помощью эхолота, позволит провести калибровку спутниковых данных водной поверхности.



а *б*

Рис. 3. Сравнение полученных результатов кластеризации – *а*
и данных глобальной базы данных типов поверхности GlobeLand30 – *б*, по данным Landsat-8

В целом полученные на рис. 3 данные показывают хорошее согласие по основным типам поверхности, которые выделены нами и которые присутствуют в известной глобальной базе данных поверхности GlobeLand30.

Заключение

В работе рассмотрены основные особенности, возникающие в задаче многоспектральной кластеризации спутниковых изображений. Выполнен обзор методов кластеризации. Указаны условия, по которым спутниковые изображения среднего пространственного разрешения (10–50 м) можно кластеризовать. Выбран широко известный метод кластеризации – k-средних с эвклидовой метрикой, который хорошо работает при обработке данных большого объема. Полученные результаты показывают на хорошую согласованность кластеризованных данных в работе с известным мировым аналогом GlobeLand30.

Работа выполнена в центре космического мониторинга ТУСУРа и в рамках государственного задания Министерства образования и науки РФ, проект № 8.8184.2017/8.9 «Методология создания систем энергогенерирующих и энергопреобразующих устройств для наземных и бортовых комплексов наземного, космического и подводного базирования».

Литература

1. Бондур В.Г. Основы аэрокосмического мониторинга окружающей среды: курс лекций. – М.: МИИГАиК, 2008. – 546 с.

2. Бондур В.Г. Современные подходы к обработке больших потоков гиперспектральной и многоспектральной аэрокосмической информации // Исследование Земли из космоса. – 2014. – № 1. – С. 4–16.

3. Burnett C. Multi-scale segmentation/object relationship modelling methodology for landscape analysis / C. Burnett, T.A. Dlaschke // Ecological Modelling. – 2003. – Vol. 168, No. 3. – PP. 233–249.

4. Chen G. Object-based change detection / G. Chen, G.J. Hay, L.M.T. Carvalho, M.A. Wulder // International Journal of Remote Sensing. – 2012. – Vol. 33, No. 14. – PP. 4434–4457.

5. Haralick R.M. Textural features for image classification / R.M. Haralick, K. Shanmugam, I. Dinstein // IEEE Transactions on Systems, Man and Cybernetics. – 1973. – Vol. 3, No. 6. – PP. 610–621.

6. Сидорова В.С. Оценка качества классификации многоспектральных изображений гистограммным методом // Автометрия. – 2007. – Т. 43, № 1. – С. 37–43.

7. Halkidi M. On clustering validation techniques / M. Halkidi, Y. Batistakis, M. Vazirgiannis // Journal of Intelligent Information Systems. – 2001. – No. 17. – PP. 107– 132.

8. Chen C.H. The Handbook of Pattern Recognition and Computer Vision / C.H. Chen, L.F. Pau, P.S.P. Wang. – Singapore: World Scientific Publishing Co, 1998. – 1004 p.

9. Magnussen S. Contextual classification of Landsat TM images to forest inventory cover types / S. Magnussen,P. Boudewyn, M. Wulder // Int. J. Remote Sens. – 2004. – No. 25. – PP. 2421–2440.

10. Duda T. Unsupervised classification of satellite imagery: choosing a good algorithm /T. Duda, M.J. Canty // Int. J. Remote Sens. – 2002. – No. 23. – PP. 2193–2212.

11. Li C. Comparison of classification algorithms and training sample sizes in urban land classification with Landsat Thematic Mapper imagery / C. Li, J. Wang, L. Wang, L. Hu, P. Gong // Remote Sens. – 2014. – No. 6. – PP. 964–983.

12. Li M. A review of remote sensing image classification techniques: The role of spatio-contextual information / M. Li, S.Y. Zang, B. Zhang, S.S. Li, C.S. Wu // Eur. J. Remote Sens. – 2014. – No. 47. – PP. 389–411

13. Асмус В.В. Контролируемая классификация данных дистанционного зондирования Земли / В.В. Асмус, А.А. Бучнев, В.П. Пяткин // Автометрия. – 2008. – № 4. – С. 60–67.

14. Книжников Ю.Ф. Аэрокосмические методы географических исследований / Ю.Ф. Книжников, В.И. Кравцова, О.В. Тутубалина. – М.: Академия, 2004. – 336 с.

15. Лурье И.К. Теория и практика цифровой обработки изображений. Дистанционное зондирование и географические информационные системы / И.К. Лурье, А.Г. Косиков. – М.: Научный мир, 2003. – 168 с.

16. Yonggang L. PHA: A fast potential-based hierarchical agglomerative clustering method / L. Yonggang // Patt. Recogn. – 2013. – Vol. 46, No. 5. – PP. 1227–1239.

17. Xu R., Wunsch D. I. Survey of clustering algorithms // IEEE Trans. Neural Networks. – 2005. – Vol. 16, No. 3. – PP. 645–678.

18. Катаев М.Ю. Обнаружение экологических изменений природной среды по данным спутниковых измерений / М.Ю. Катаев, А.А. Бекеров // Оптика атмосферы и океана. – 2014. – Т. 27, № 7. – С. 652–656.

19. Катаев М.Ю. Интернет-информационная система накопления, обработки и анализа спутниковых данных MODIS / М.Ю. Катаев, А.А. Бекеров, А.К. Лукьянов // Доклады ТУСУР. – 2015. – Т. 35, № 1. – С. 93–99.

Катаев Михаил Юрьевич
Д-р техн. наук, профессор каф. автоматизированных систем управления систем (АСУ)
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: (382-2) 70-15-36
Эл. почта: kmy@asu.tusur.ru

Богомолов Александр Владимирович
Магистрант 2-го курса каф. АСУ ТУСУР
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-951-587-04-08
Эл. почта: alex1.bogomolov@gmail.com

Kataev M.Yu., Bogomolov A.V.

Features of clustering the multispectral satellite Landsat images

In the article, features of thematic processing of Earth remote sensing data obtained in different ranges of the optical spectrum using the Landsat-8 instrument are studied. The clustering of multispectral survey data, based on measurements in the first channels of a satellite instrument, with a resolution of 30 m, does not allow the high-precision determination of surface types due to heterogeneity of their mixing. The study of these aspects is the subject of this article. The results of real data processing of satellite measurements are presented.

Keywords: remote sensing, satellite image processing, multispectral, clustering.
doi: 10.21293/1818-0442-2018-21-2-54-59

References

1. Bondur V.G. *Osnovy aerokosmicheskogo monitoringa okruzhayushchey sredy. Kurslektsiy* [Fundamentals of airspace environment monitoring. Lecture course]. Moscow, MIIGAiK Publ., 2008. 546 p. (In Russ.)

2. Burnett C., Dlaschke T.A Multi-scale segmentation/object relationship modelling methodology for landscape analysis. *Ecological Modelling*, 2003, vol. 168, no. 3, pp. 233–249.

3. Chen G., Hay G.J., Carvalho L.M.T., Wulder M.A. Object-based change detection. *International Journal of Remote Sensing*, 2012, vol. 33, no. 14, pp. 4434–4457.

4. Bondur V.G. Modern approaches to the processing of huge hyperspectral and multispectral airspace data flow. *Issledovanie Zemli iz kosmosa*, 2014, no. 1, pp. 4–16 (In Russ.).

5. Haralick R.M., Shanmugam K., Dinstein I. Textural features for image classification.*IEEE Trans. Syst. Man and Cybernetics*, 1973, vol. 3, no. 6, pp. 610–621.

6. Sidorova V.S. Evaluation of the quality of classification of multispectral images by the histogram method. *Avtometriya*. 2007, vol. 43, no. 1, pp. 37–43 (In Russ.).

7. Halkidi M., Batistakis Y. and Vazirgiannis M. On clustering validation techniques.*Journal of Intelligent* Information Systems, 2001, no. 17, pp. 107–132.

8. Chen C.H., Pau L.F., Wang P.S.P. The Handbook of Pattern Recognition and Computer Vision.World Scientific Publishing Co, 1998. 1004 p.

9. Magnussen S., Boudewyn P., Wulder M. Contextual classification of Landsat TM images to forest inventory cover types. *Int. J. Remote Sens*, 2004, no. 25, pp. 2421–2440.

10. Duda T., Canty M.J. Unsupervised classification of satellite imagery: choosing a good algorithm. *Int. J. Remote Sens*, 2002, no. 23, pp. 2193–2212.

11. Li C., Wang J., Wang L., Hu L., Gong P. Comparison of classification algorithms and training sample sizes in urban land classification with Landsat Thematic Mapper imagery. *Remote Sens*, 2014, no. 6, pp. 964–983.

12. Li M., Zang S.Y., Zhang B., Li S.S., Wu C.S. A review of remote sensing image classification techniques: The

role of spatio-contextual information. *Eur. J. Remote Sens*, 2014, no. 47, pp. 389–411.

13. Asmus V.V., Buchnev A.A., Pyatkin V.P. Controlled classification of remote sensing data of the Earth, *Avtometriya*, 2008, no. 4, pp. 60–67.

14. Knizhnikov Yu.F., Kravtsova V.I., Tutubalin O.V. Aerospace methods of geographical research. Moscow, Academy, 2004. 336 c.

15. Lurie I.K. *Theory and practice of digital image processing. Remote sensing and geographic information systems* / I.K. Lurie, A. G. Kosikov. Moscow, The scientific world, 2003. 168 p.

16. Yonggang L. PHA: A fast potential-based hierarchical agglomerative clustering method. *Patt. Recogn,* 2013, vol. 46, no. 5, pp. 1227–1239.

17. Xu R., Wunsch D.I. Survey of clustering algorithms. *IEEE Trans. Neural Networks,* 2005, vol. 16, no. 3, pp. 645–678.

18. Kataev M.Yu. Obnaruzhenie ekologicheskih izmeneniy prirodnoi sredy po dannym sputnikovyh izmerenij. *Optika atmosfery i okeana*, 2014, vol. 27, no. 7, pp. 652–656 (In Russ.)

19. Kataev M.Yu., Bekerov A.A., Lukyanov A.K. Internet information system for the accumulation, processing and analysis of satellite data MODIS. *Proceedings of TUSUR University*, 2015, vol. 35, no. 1, pp. 93–99 (In Russ.)

Mikhail Yu. Kataev
Doctor of Engineering Sciences, professor,
Department of Control Systems, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-36
Email: kmy@asu.tusur.ru

Alexander V. Bogomolov
Master student, Department of Control Systems, TUSUR
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7-951-587-04-08
Email: alex1.bogomolov@gmail.com

УДК 004.89

Т.В. Левашова, М.П. Пашкин

Модель определения предпочтительной конфигурации продукта

Предложен подход к определению конфигурации продукта, являющейся для заказчика предпочтительной. В подходе использованы методы выбора на основе специфических для заказчика функций ценности и весовой значимости. Критерии выбора определяются на основании онтологической модели конфигурируемого продукта и результатов, полученных в ходе профилирования заказчика на предмет принятия им решений в процессе конфигурирования или приобретения различных продуктов. Для описания предпочтений заказчика используются отношения предпочтения, принятые в моделях принятия решений. Подход иллюстрируется на примере задачи определения предпочтительной конфигурации продукта оператора сотовой связи.
Ключевые слова: персонализированное конфигурирование продукта, предпочтительная конфигурация, онтологическая модель продукта, отношения предпочтения, продукт оператора сотовой связи.
doi: 10.21293/1818-0442-2018-21-2-60-67

Конфигурирование продукта – это процесс модификации продукта в соответствии с требованиями заказчика. Неформально конфигурирование может быть определено как особый вид проектирования, при котором создаваемый объект (продукт) собирается из различных компонентов, которые могут быть объединены в продукте таким образом, что продукт будет соответствовать заданным ограничениям. Решением задачи конфигурирования является набор компонентов, составляющих продукт, и при необходимости отношений между этими компонентами. Это решение называется конфигурацией продукта. Для создания конфигурации продукта используются различные механизмы конфигурирования, например, правил [1], удовлетворения ограничений [2–4], нейронных сетей [5], создания серийных программных продуктов [6, 7], концептуального моделирования [8–11] и др. Эти механизмы, как правило, предлагают в качестве решения несколько альтернативных конфигураций, из которых должна быть выбрана одна.

В основе теории принятия решений лежит предположение о том, что человек, поставленный перед проблемой выбора альтернативы, руководствуется своими предпочтениями [12–14]. Целью данной работы является автоматическое определение конфигурации, которая является предпочтительной для заказчика. Предпосылкой к разработке рассматриваемого в работе подхода служит ранее разработанный онтологический подход к конфигурированию нематериальных продуктов [15]. В результате онтологического подхода формировалось множество альтернативных конфигураций продукта, которое предлагалось заказчику на рассмотрение для выбора наиболее привлекательной с его точки зрения конфигурации.

В основе механизма конфигурирования в онтологическом подходе лежит концептуальное моделирование продукта средствами онтологий. Онтологическая модель представляет компоненты, образующие продукт, и их свойства, включая отношения между компонентами.

Подходы к выбору предпочтительной конфигурации используют генетические алгоритмы [16–18], механизмы управления вариабельными конфигурациями [19], теорию полезности [20, 21], методы выбора на основе специфических для пользователя функций ценности и весовой значимости [22, 23] и др.

Для определения предпочтительной конфигурации в данной работе используются методы выбора на основе специфических для заказчика функций ценности и весовой значимости. Изначально эти методы ориентировались на экспертов, которые попарно сравнивали альтернативы по заданным критериям, что является достаточно трудоемким процессом. Подход, предлагаемый в данной работе, для определения критериев заказчика использует результаты, полученные в ходе профилирования этого заказчика по итогам принятия им решений в процессе конфигурирования или приобретения различных продуктов. Для описания предпочтений заказчика используются отношения предпочтения [24], применяемые в моделях принятия решений. Эти отношения достаточно широко применяются в теории потребительского выбора [25, 26].

В онтологическом подходе к конфигурированию нематериальных продуктов рассматривалась задача конфигурирования продукта оператора сотовой связи [15]. Здесь этот пример будет продолжен, и будет определена конфигурация продукта оператора сотовой связи, являющаяся для абонента (заказчика) предпочтительной.

Обращение к проблемной области «мобильная связь» для демонстрации подхода представляется своевременным в силу современных требований со стороны цифровой экономики к телекоммуникационным технологиям. В соответствии с этими требованиями необходимо перейти к цифровому преобразованию операционной модели телекоммуникационного рынка и внедрению методов углубленной аналитики больших массивов данных [27].

Персонализированное конфигурирование продукта

Общая схема подхода к персонализированному конфигурированию продукта представлена на рис. 1. Исходная информация поступает из онтологической модели продукта (или онтологии продукта) и профиля заказчика.

Рис. 1. Общая схема подхода к персонализированному конфигурированию продукта

Онтологическая модель описывает продукт через его компоненты, их характеристики (свойства) и отношения между компонентами. Эта модель дает полное представление о продукте, обо всех компонентах, которые может содержать этот продукт, их характеристиках и условиях, при которых компоненты могут быть включены в продукт.

Профиль заказчика является источником информации об ограничениях, накладываемых на создаваемую конфигурацию со стороны заказчика, но не связанных с его предпочтениями. В частности, при конфигурировании продукта оператора сотовой связи [15] таким ограничением была конфигурация мобильного устройства, к которому клиент хотел подключить новую услугу.

Результатом онтологического конфигурирования является множество возможных конфигураций продукта. Все конфигурации имеют онтологическое представление, т.е. каждая конфигурация – это онтологическая модель предлагаемого продукта.

Для того чтобы определить, какие характеристики продукта представляют интерес для заказчика, между критериями заказчика, представленными в его профиле, и характеристиками продукта, представленными в онтологии, устанавливаются отображения. В общем случае профиль заказчика содержит все критерии, которыми заказчик пользовался для оценки конфигурируемых или приобретаемых продуктов за всю историю профилирования. Отображения устанавливаются только для тех критериев, которые могут быть использованы для оценки конкретного конфигурируемого продукта. На текущий момент установка отображений осуществляется экспертами. Так как каждая конфигурация создана из онтологии продукта и по сути сама является онтологией, отображения позволяют выделить в каждой конфигурации характеристики, соответствующие критериям заказчика.

Множество возможных конфигураций ранжируется в соответствии с предпочтениями заказчика. Предпочтения включают в себя критерии оценки продукта, являющиеся для заказчика приоритетными, и дополнительные ограничения в виде отношений сравнимости (максимальный, минимальный, лучше, хуже, меньше, больше, равно и т.п.). Приоритетные критерии определяются на основании анализа истории выбора заказчиком конфигураций продуктов. Например, если заказчик всегда выбирает самую дешевую из предложенных конфигураций, то приоритетным критерием заказчика является цена, а ограничением – минимальная (цена).

Если приоритетный критерий один, то ранжирование осуществляется по этому критерию в соответствии с отношениями сравнимости. Если приоритетных критериев несколько, то ранжирование конфигураций осуществляется на основании весового предпочтения. Вес является функцией от частоты использования рассматриваемого критерия при выборе заказчиком различных конфигураций, «важности» данного критерия по сравнению с другими критериями и количества продуктов, рассмотренных заказчиком за всю историю профилирования.

Определение предпочтительной конфигурации продукта: подход

Целью подхода к определению предпочтительной конфигурации является получение ранжированного списка альтернативных конфигураций, в котором конфигурация, соответствующая предпочтениям заказчика, является крайним элементом (первым или последним).

Определение предпочтительной конфигурации начинается с определения критериев, на основании которых заказчик оценивает продукты. Для выявления критериев заказчика используется его профиль [28, 29]. Использование профиля заказчика вместо взаимодействия с заказчиком в процессе конфигурирования обусловлено рядом причин:

– выбор критериев и определение предпочтений в диалоге с заказчиком не всегда возможны или вызывают затруднения, например в случае удаленного конфигурирования;

– построение всех отображений в процессе диалога с заказчиком требует значительных временных затрат;

– цифровая экономика ориентируется на использование методов углубленной аналитики больших массивов данных.

Технология профилирования предлагает различные методы для выявления предпочтений заказчиков. Например, аналитическая обработка запросов заказчиков относительно интересующих их продуктов и характеристик; анализ отзывов заказчиков, отправленных ими продавцу продукта в форме обратной связи; анализ обсуждений заказчиками продуктов в социальных сетях и на форумах; анализ решений заказчика при покупке продукта и др. Данная работа ориентируется на выявление предпочтений заказчика посредством анализа решений, которые

были приняты заказчиком при конфигурировании или приобретении различных продуктов.

Для описания предпочтений заказчика предлагается использовать отношения предпочтения, принятые в теории потребительского выбора [25, 26]. В соответствии с этой теорией оценка предпочтений производится на множествах с одинаковыми наборами критериев, но с разными значениями в каждом множестве.

В рассматриваемом здесь подходе предлагается сравнивать множества, в которых встречается хотя бы один критерий из множества критериев заказчика (C), с таким же критерием в других множествах. Множество, которое сравнивается с множеством C, является пересечением двух множеств. Таким образом, сравниваются множества $C_k = C$ и $C_m = C \cap X$, где X – множество, содержащее критерии из множества C. Слабое предпочтение выражается как $c \geq (C_k, C_m)$ и обозначает, что на паре множеств C_k и C_m для заказчика критерий c является предпочтительным. Строгое предпочтение критерия определяется по результатам сравнения множеств, в которых есть рассматриваемый критерий и для которых определены отношения слабого предпочтения. Критерий c считается строго предпочтительным $c > C$ тогда и только тогда, когда $c \geq (C_k, C_m)$ для всех пар (C_k, C_m). Предложенный подход позволяет выявить предпочитаемые заказчиком критерии в результате анализа принятых им решений при приобретении или конфигурировании различных продуктов, для оценки которых могут применяться одинаковые критерии. Например, критерии надежности, стоимости и др. могут быть применены к любым видам продуктов, критерий «удобство использования» – к интерфейсу, методическим рекомендациям, некоторым видам услуг и т.п., но этот критерий неприменим к продукту как произведению искусства.

Между критериями, которые заказчик использует для оценки продукта, и характеристиками продукта, представленными в онтологии, устанавливаются отображения. Необходимость установки отображений вызвана тем, что словари профиля заказчика и онтологии, как правило, отличаются, т.е. критерии, представленные в профиле заказчика, могут не совпадать с названиями характеристик продукта в онтологии. Отображения позволяют определить критерии заказчика в терминах проблемной области.

Для установки отображений предлагается использовать алгоритм, приведенный на рис. 2.

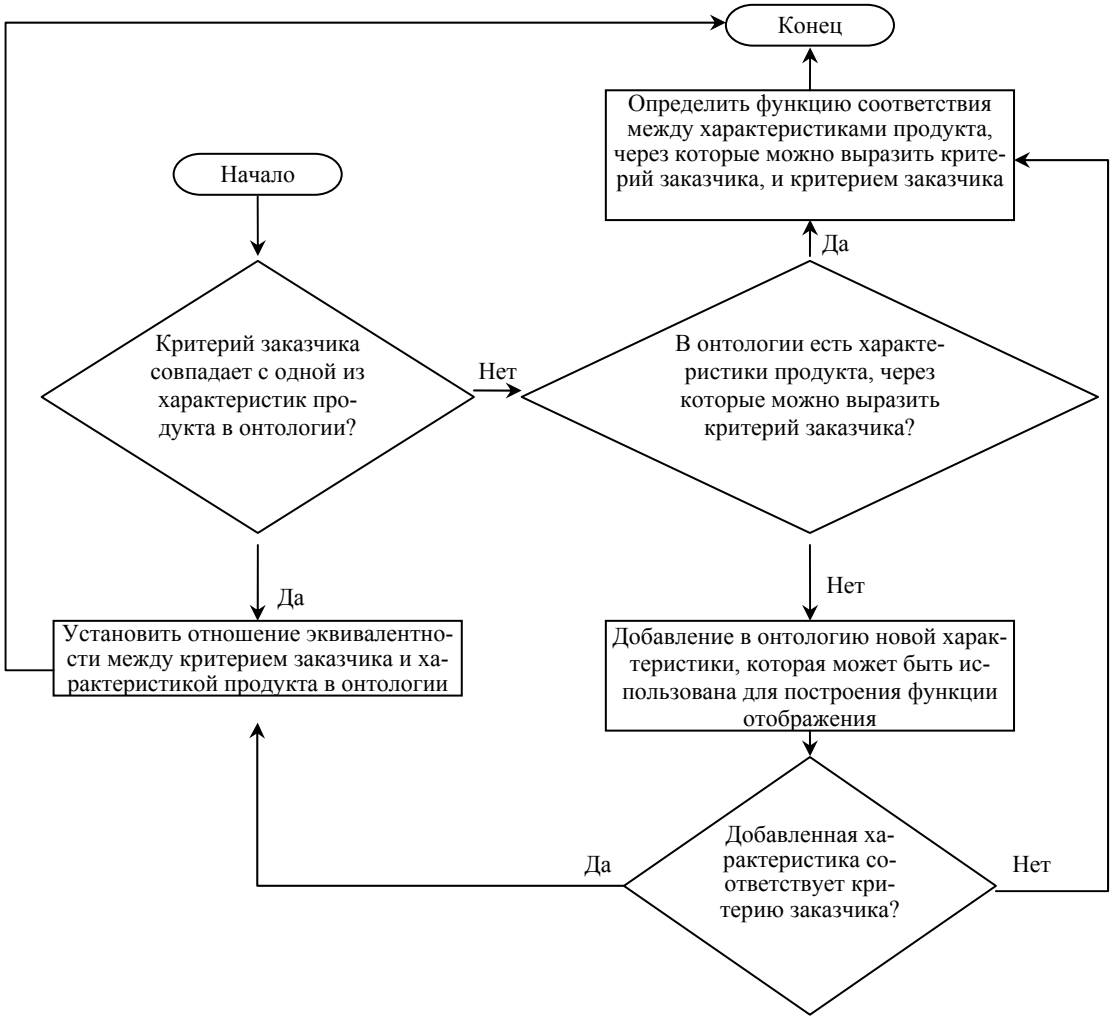


Рис. 2. Алгоритм установки отображений между критериями заказчика и онтологией продукта

В соответствии с этим алгоритмом вначале осуществляется анализ характеристик продукта, представленных в онтологии, на предмет возможности их использования в качестве критериев заказчика. Если в онтологии продукта (OP) представлена характеристика p_{p}, точно соответствующая критерию заказчика p_{c}, то отображение между этими критерием и характеристикой моделируется при помощи отношения эквивалентности: OP : p_{p} = VC : p_{c}, где VC – это словарь заказчика.

Например, если заказчик выбрал критерием стоимость конфигурации продукта, а в онтологии этот продукт характеризуется ценой, то между понятиями «стоимость» и «цена» устанавливается отношение эквивалентности: OP : цена = VC : стоимость.

Если точного соответствия не существует, то следующим шагом является попытка выразить критерий заказчика p_{c} как функцию от характеристик продукта, которые представлены в онтологии. Если в онтологии есть характеристики продукта, которые могут быть использованы для выражения критерия заказчика, то отображение между критерием и характеристиками имеет вид OP : $p_k \wedge$ OP: p_m = VC : p_{c}, где p_k и p_m – характеристики продукта в онтологии, которые могут быть использованы для выражения критерия заказчика.

Например, если заказчик выбрал критерием качество конфигурируемого продукта, а в онтологии эта характеристика явно не представлена, но известно, что на качество рассматриваемого заказчиком продукта влияют такие характеристики как доступность и универсальность, то отображение между интересующим заказчика критерием и онтологией выглядит как OP : доступность $\wedge$ OP : универсальность = VC : качество.

Если в онтологии продукта не существует характеристик для выражения критерия заказчика, то в онтологию добавляется новая характеристика, которая либо точно соответствует критерию заказчика, либо может быть использована в совокупности с представленными характеристиками для построения отображения.

После установки отображений для критериев, получивших отображения в виде, отличном от отношений эквивалентности, строятся агрегирующие функции, которые позволяют определить значение критерия пользователя по множеству значений характеристик. Результатом установки всех отображений является множество отображений (M): $M : C \to P$, где P – множество характеристик продукта в онтологии OP.

После анализа всех решений заказчика при конфигурировании или приобретении им различных продуктов имеем непересекающиеся множества, в каждом из которых один из критериев приоритетный.

В случае единственного множества (выявлен только один приоритетный критерий) ранжирование альтернативных конфигураций осуществляется по этому критерию в соответствии с отношениями сравнимости.

В случае нескольких приоритетных критериев ранжировать альтернативные конфигурации предлагается на основании весового предпочтения.

Вес предпочтения в i-м множестве (w_i) предложено определять как

$$w_i = \frac{\|X\|_{\max} \cdot N_X}{N_S},$$

где $\|X\|_{\max}$ – максимальная мощность множества X; N_X – количество множеств X; N_S – количество продуктов, для которых приняты решения.

Если после определения весов появились критерии, имеющие одинаковый вес (равнозначные критерии), то для каждого критерия формируется самостоятельный список конфигураций, ранжированный по этому критерию. Если аналитическое сравнение таких списков вызывает трудности со стороны заказчика или специалиста по конфигурированию, то для получения одного списка можно использовать, например, метод справедливого компромисса [30, 31] или другие методы многокритериального выбора [32]. В рамках данной работы вопрос оценки продукта по равнозначным критериям не рассматривается.

Выбор предпочтительной конфигурации продукта оператора сотовой связи

В работе используется пример конфигурирования продукта оператора сотовой связи (ОСС), который был рассмотрен в предыдущей статье [15]. Требованием заказчика (абонента для проблемной области «мобильная связь») в этом примере являлось подключение на его номер услуги определения местоположения абонента с мобильных устройств. Задача конфигурирования заключалась в создании конфигурации продукта ОСС, расширяющей существующую конфигурацию новым компонентом.

Онтологическая модель продуктов ОСС, используемая в рассматриваемом примере, приведена на рис. 3, где показана только часть онтологии, релевантная для рассматриваемого примера. Для представления онтологии используются средства модели OWL (Web Ontology Language) [33]. На рисунке незатененные прямоугольники соответствуют классам, затененные – индивидам (экземплярам классов). Отношения (родовидовые и «использует») представлены бинарными предикатами, свойства одного аргумента представлены унарными предикатами.

Как видно из рисунка, услуга определения местоположения является платной. Эта услуга характеризуется стоимостью. ОСС предлагает два варианта реализации запрашиваемой услуги: «Локатор» и «Спутник». «Локатор» определяет местоположение абонента при регистрации в сети. «Спутник» определяет местоположение абонента по GPS / ГЛОНАСС. Пользование услугой возможно, если на устройстве абонента установлено приложение «Smart Positioning», разработанное для операционной системы Android версий 4.4 и выше.

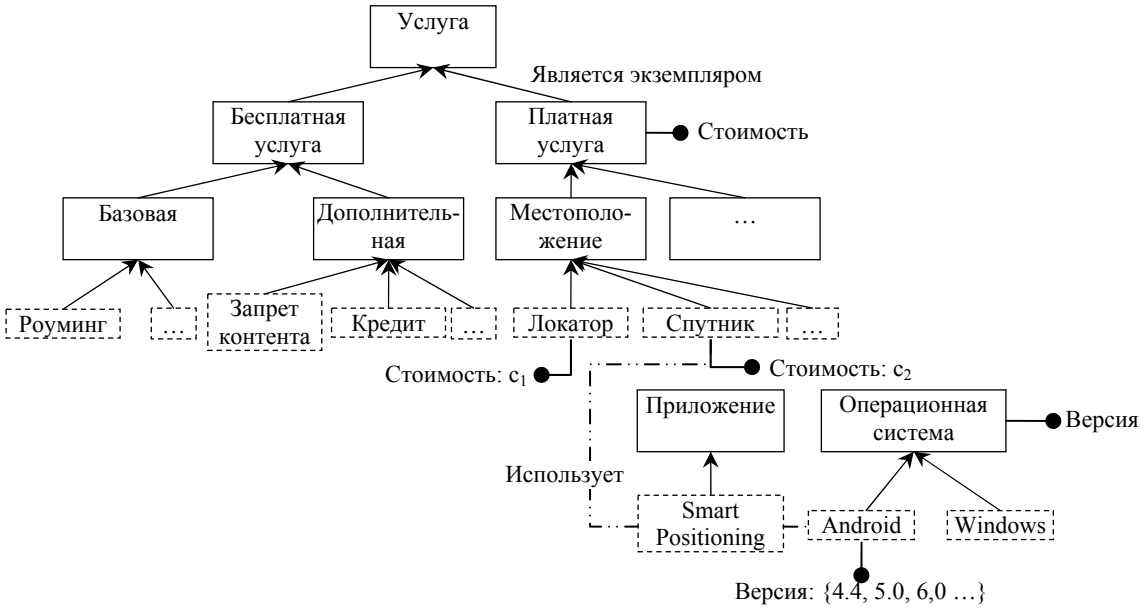


Рис. 3. Онтология продукта «услуги ОСС» (пример)

Из приведенной онтологии продукта «услуги ОСС» можно получить две альтернативные конфигурации требуемого продукта (таблица) (для краткости родовидовые отношения «являться экземпляром» в таблице не показаны).

Возможные конфигурации продукта «услуга определения местоположения»

Класс	Свойство	Область значений свойства
Конфигурация$_1$		
Платная услуга	Стоимость	
Местоположение	Стоимость	
Локатор		c_1
Стоимость конфигурации 1		c_1
Конфигурация$_2$		
Платная услуга	Стоимость	
Местоположение	Стоимость	
Спутник	Стоимость	c_2
Спутник	Использует	Приложение
Smart Positioning	Использует	Операционная система
Android	Версия	4.4 и выше
Стоимость конфигурации 2		c_2

Компоненты, входящие в первую конфигурацию, характеризуются только стоимостью. В общем случае стоимость конфигурации не является простой суммой стоимости ее компонентов. Здесь, для простоты функция расчета конфигураций не рассматривается и считается, что стоимость конфигурации складывается из стоимости компонентов. Вторая конфигурация характеризуется видом приложения, видом операционной системы, версией операционной системы и стоимостью.

Определены следующие отображения между профилем заказчика (VC) и онтологией продукта (OP):

1) VC:цена = OP:Стоимость;

2) VC:ОС = OP:Операционная система.

Оба отображения представлены отношениями эквивалентности.

Для класса приложение отображений не установлено, так как в профиле заказчика отсутствуют критерии, которые могли бы быть связаны с этой характеристикой.

Анализ профиля заказчика показал, что операционная система является единственным строго предпочтительным критерием. Дополнительное ограничение заказчика заключается в том, что он всегда выбирает приложения, работающие под системой Android. Это ограничение в виде отношения сравнимости выглядит следующим образом: Операционная система = Android. После ранжирования по этому отношению получаем, что в рассматриваемом примере предпочтительной конфигурацией является вторая.

Заключение

В работе описан подход к определению конфигурации продукта, которая является для заказчика предпочтительной. Подход предполагает использование онтологической модели продукта. Эта модель лежит в основе ранее разработанного онтологического подхода к конфигурированию нематериальных продуктов. В рассмотренном в данной работе подходе онтологическая модель продукта используется для определения соответствий между критериями предпочтений заказчика и характеристиками конфигурируемого продукта, что позволяет выразить критерии заказчика в терминах проблемной области и соответственно приблизиться к представлению заказчика о продукте, если этот заказчик не является специалистом в данной области.

Для описания предпочтений заказчика предложено использовать отношения предпочтения, применяемые в моделях принятия решений и теории потребительского выбора. Выявление предпочтений заказчика осуществляется по результатам профилирования этого заказчика на предмет принятия им решений в процессе конфигурирования или приобретения им различных продуктов. Использование

профиля заказчика, во-первых, позволяет отказаться от трудоемкого процесса сравнения экспертами различных наборов продуктов, как это делается в теории потребительского выбора; во-вторых, предоставляет историю выбора заказчиком продуктов для расчета весовых коэффициентов критериев при возникновении проблемы многокритериального выбора; в-третьих, опирается на использование результатов анализа больших объемов данных, что является одним из ключевых требований со стороны цифровой экономики.

Критериями эффективности работы предложенных моделей персонализированного конфигурирования продукта, определения предпочтений заказчика и ранжирования альтернативных конфигураций продукта являются степень удовлетворенности заказчика и время, затрачиваемое на обслуживание заказчика. Модели позволяют повысить степень удовлетворенности заказчика и сократить время обслуживания.

Предложенный подход находится на этапе разработки. На текущий момент имеются следующие ограничения и недоработки. Установка отображений между словарем заказчика и онтологией продукта производится экспертами. В дальнейшем планируется автоматизировать эту процедуру. В частности, за счет использования механизмов отображения онтологий. Также в части установки отображений в данной работе рассмотрены только отображения между эквивалентными понятиями. В перспективе планируется разработать типовые функции, позволяющие строить отображения, являющиеся функциями нескольких понятий. Для проверки подхода на жизнеспособность и с целью получения представления о необходимости возможной доработки требуется тестирование подхода на больших наборах реальных данных.

Работа выполнена при финансовой поддержке РФФИ (гранты №№ 16-07-00375, 17-07-00247, 17-07-00248) и бюджетной темы № 0073-2018-0002.

Литература

1. Expert systems for configuration at Digital: XCON and beyond / V.E. Barker, D.E. O'Connor, J. Bachant, E. Soloway // Communications of the ACM. – 1989. – Vol. 32, No. 3. – PP. 298–318. – Doi: 10.1145/62065.62067.

2. Mittal S. Dynamic constraint satisfaction problems / S. Mittal, F. Frayman // Proceedings of the eighth National conference on Artificial intelligence. – AAAI, 1990. – Vol. 1. – PP. 25–32.

3. Xie H. Modelling and solving engineering product configuration problems by constraint satisfaction / H. Xie, P. Henderson, M. Kernahan // International Journal of Production Research. – 2005. – Vol. 43, No. 20. – PP. 4455–4469.

4. Wang L. Constraint satisfaction approach on product configuration with cost estimation / L. Wang, W.K. Ng, B. Song // Next-Generation Applied Intelligence. – Berlin etc.: Springer, 2009. – PP 731–740. – (Lecture Notes in Computer Science; Vol. 5579).

5. Wubneh A. Feature transformation from configuration of open-loop mechanisms into linkages with a case study / A. Wubneh, C.K. Au, Y.-S. Ma // Semantic Modeling and Interoperability in Product and Process Engineering / Ed. Y.-S. Ma. – London: Springer-Verlag, 2013. – PP. 275–302.

6. Bosch J. Design and use of software architectures: adopting and evolving a product-line approach. – New York: Addison-Wesley, 2000. – 354 p.

7. Automated analysis in feature modelling and product configuration / D. Benavides, A. Felfernig, J.A. Galindo, F. Reinfrank // Safe and Secure Software Reuse. – Berlin etc.: Springer, 2013. – PP. 160–175. – (Lecture Notes in Computer Science; Vol. 7925).

8. Towards a general ontology of configuration / T. Soininen, J. Tiihonen, T. Männistö, R. Sulonen // Artificial Intelligence for Engineering Design, Analysis and Manufacturing. – 1998. – Vol. 12, No. 4. – PP. 357–372. – Doi: 10.1017/S0890060498124083

9. Felfernig A. Conceptual modeling for configuration of mass-customizable products / A. Felfernig, G. Friedrich, D. Jannach // Artificial Intelligence in Engineering. – 2001. – Vol. 15, No. 2. – PP. 165–176.

10. Yang D. Development of a product configuration system with an ontology-based approach / D. Yang, M. Dong, R. Miao // Computer-Aided Design. – 2008. – Vol. 40, Is. 8. – PP. 863–878. – Doi: 10.1016/j.cad.2008.05.004

11. Lee H. Product configuration strategy based on product family similarity // International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering. – 2013. – Vol. 7, No. 8. – PP. 1709–1713.

12. Ларичев О.И. Объективные модели и субъективные решения. – М.: Наука, 1987. – 144 с.

13. Петровский А.Б. Теория принятия решений: университетский учебник. – М.: Академия, 2009. – 400 с.

14. Осипов Г.С. Многокритериальный выбор альтернатив на основе нечеткого отношения предпочтения // Развитие современной науки: теоретические и прикладные аспекты. – 2016. – № 1. – С. 24–27.

15. Левашова Т.В. Онтологический подход к конфигурированию продуктов операторов сотовой связи для абонентов / Т.В. Левашова, М.П. Пашкин // Научный вестник НГТУ (Новосибирск). – 2016. – Вып. 63, № 2. – С. 99–114.

16. Yeh J.-Y. Parallel genetic algorithms for product configuration management on PC cluster systems / J.-Y. Yeh, T.-H. Wu, J. Chang // The International Journal of Advanced Manufacturing Technology. – 2007. – Vol. 31, Is. 11–12. – PP. 1233–1242.

17. Che Z.-H. Using hybrid genetic algorithms for multi-period product configuration change planning // International Journal of Innovative Computing, Information & Control. – 2010. – Vol. 6, No. 6. – PP. 2781–2785.

18. Dou R. Multi-stage interactive genetic algorithm for collaborative product customization / R. Dou, C. Zong, G. Nan // Knowledge Based Systems. –2016. – Vol. 92. – PP. 43–54.

19. Schuh G. Identifying preferable product variants using similarity analysis / G. Schuh, M. Riesener, S. Rudolf // Procedia CIRP. – 2014. – Vol. 20. – PP. 38–43.

20. Luce R.D. Games and decisions: introduction and critical surveys / R.D. Luce, R. Howard. – New York: Wiley, 1957. – 740 p.

21. Keeney R.L. Designing win-win financial loan products for consumers and businesses / R.L. Keeney, R.M. Oliver // Journal of the Operational Research Society. – 2005. – Vol. 56. – PP. 1030–1040.

22. Usability guidelines for product recommenders based on example critiquing research / P. Pu, B. Faltings, L. Chen, J. Zhang, P. Viappiani // Recommender systems handbook / Eds. F. Ricci, L. Rokach, B. Shapira, P.B. Kantor. Boston: Springer, 2011. – PP. 511–545.

23. A configuration-based recommender system for supporting e-commerce decisions / M. Scholz, V. Dorner, G. Schryen, A. Benlian // European Journal of Operational Research. – 2017. – Vol. 259, Is. 1. – PP. 205–215.

24. Шрейдер Ю.А. Равенство, сходство, порядок. – М.: Наука, 1971. – 256 с.

25. Вэриан Х.Р. Микроэкономика. Промежуточный уровень. Современный подход: учеб. для вузов: пер. с англ.; под ред. Н.Л. Фроловой. – М.: ЮНИТИ, 1997. – 767 с.

26. Чеканский А.Н. Микроэкономика: промежуточный уровень / А.Н. Чеканский, Н.Л. Фролова: учеб. – М.: ИНФРА, 2005. – 684 с.

27. Цифровая Россия: новая реальность / А. Аптекман, В. Калабин, В. Клинцов, Е. Кузнецова, В. Кулагин, И. Ясеновец: отчет. – Digital McKinsey. – 2017. – 134 с.

28. Silverman D. The adviser, Who Knows the Client Best, Wins [Electronic resource]: White Paper. – Capital Preferences Ltd. – 2017. Patent Pending. – Режим доступа: https://www.onefpa.org/Membership/Documents/CapitalPreferences_whitepaper-Advisers-who-know-client-wins_Feb2017.pdf, свободный (дата обращения: 05.03.2018).

29. Рудская Е.Н. Профилирование цифрового клиента: новые форматы интеллектуального анализа данных / Е.Н. Рудская, Ю.Ю. Полтавская // Молодой учёный. – 2015. – № 21. – С. 464–471.

30. Батищев Д.И. Методы оптимального проектирования: учеб. пособие для вузов. – М.: Радио и связь, 1984. – 248 с.

31. Многокритериальные модели формирования и выбора вариантов систем / Ю.А. Дубов, С.И. Травкин, В.Н. Якимец. – М.: Наука, 1986. – 296 с.

32. Сафронов В.В. Сравнительная оценка методов «жесткого» ранжирования, справедливого компромисса и равномерной оптимальности в задаче гипервекторного ранжирования систем // Информационно-управляющие системы. – 2011. – Вып. 52, № 3. – С. 2–8.

33. OWL Web Ontology Language Overview / Eds. D.L. McGuinness, F. van Harmelen [Electronic resource]: W3C Recommendation. – 10 Feb. 2004. – Режим доступа: https://www.w3.org/TR/owl-features/, свободный (дата обращения: 11.03.2018).

Левашова Татьяна Викторовна
Канд. техн. наук, с.н. с. лаб. интегрированных систем автоматизации Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)
14-я линия, д. 39, г. Санкт-Петербург, Россия, 199178
Тел.: (812-3) 28-80-71, +7-911-708-10-14
Эл. почта: tatiana.levashova@iias.spb.su

Пашкин Михаил Павлович
Канд. техн. наук, с.н.с. лаб. интегрированных систем автоматизации СПИИРАН
14-я линия, д. 39, г. Санкт-Петербург, Россия, 199178
Тел.: (812-3) 28-80-71
Эл. почта: michaelpashkin@mail.ru

Levashova T., Pashkin M.

Model for definition of preferred product configuration

The paper proposes an approach to define a product configuration preferred by the customer. The approach uses methods of choice that are based on customer-specific value functions and weight significance. The choice criteria are revealed based on the product ontology model and the results obtained by the customer profiling. These results provide information about the customer decisions in the processes of configuring or purchasing various products. Preference hypothesis accepted in decision making models are used to describe the customer preferences. The approach applicability is illustrated by the problem of a preferred configuration definition for a mobile operator product.

Keywords: customized product configuration, preferred configuration, ontology product model, preference hypothesis, mobile operator product.
doi: 10.21293/1818-0442-2018-21-2-60-67

References

1. Barker V.E. O'Connor D.E., Bachant J. Expert systems for configuration at Digital: XCON and beyond. *Communications of the ACM,* 1989, vol. 32, no. 3, pp. 298–318. doi: 10.1145/62065.62067.

2. Mittal S., Frayman F. Dynamic constraint satisfaction problems. *Proceedings of the eighth National conference on Artificial intelligence*, AAAI, 1990, vol. 1, pp. 25–32.

3. Xie H. Henderson P., Kernahan M. Modelling and solving engineering product configuration problems by constraint satisfaction. *International Journal of Production Research*, 2005, vol. 43, no. 20, pp. 4455–4469.

4. Wang L., Ng W.K., Song B. Constraint satisfaction approach on product configuration with cost estimation. *Next-Generation Applied Intelligence*, 2009. Lecture Notes in Computer Science, vol. 5579, Springer, Berlin, Heidelberg, pp. 731–740.

5. Wubneh A., Au C.K., Ma Y.-S. Feature transformation from configuration of open-loop mechanisms into linkages with a case study. *Semantic Modeling and Interoperability in Product and Process Engineering*; ed. by Y.-S. Ma. London, Springer-Verlag, 2013, pp. 275–302.

6. Bosch J. *Design and use of software architectures: adopting and evolving a product-line approach*. New York, Addison-Wesley, 2000, 354 p.

7. Benavides D., Felfernig A., Galindo J.A., Reinfrank F. Automated analysis in feature modelling and product configuration. *Safe and Secure Software Reuse*, 2013. Lecture Notes in Computer Science, vol. 7925. Berlin London Heidelberg, Springer, pp. 160–175.

8. Soininen T., Tiihonen J., Männistö T., Sulonen R. Towards a general ontology of configuration. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*, 1998, vol. 12, no. 4, pp. 357–372. doi: 10.1017/S0890060498124083.

9. Felfernig A., Friedrich G., Jannach D. Conceptual modeling for configuration of mass-customizable products. *Artificial Intelligence in Engineering*, 2001, vol. 15, no. 2, pp. 165–176.

10. Yang D., Dong M., Miao R. Development of a product configuration system with an ontology-based approach. *Computer-Aided Design*, 2008, Vol. 40, Is. 8, pp. 863 –878. doi: 10.1016/j.cad.2008.05.004.

11. Lee H. Product configuration strategy based on product family similarity. *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, 2013, vol. 7, no. 8, pp. 1709–1713.

12. Larichev O.I. *Ob"ektivnye modeli i sub"ektivnye resheniya* [Objective models and subjective decisions]. Moscow, Nauka Publ., 1987, 144 p. (In Russ).

13. Petrovskij A.B. *Teorija prinjatija reshenij* [Decision making theory]: university textbook. Moscow, Academia Publ., 2009, 400 p. (In Russ).

14. Osipov G.S. Mnogokriterial'nyj vybor al'ternativ na osnove nechetkogo otnoshenija predpochtenija [Multi-criteria choice of alternatives based on a fuzzy preference relation]. *Razvitie sovremennoj nauki: teoreticheskie i prikladnye aspekty* [*Development of modern science: theoretical and applied aspects*], 2016, no 1, pp. 24–27. (In Russ).

15. Levashova T.V., Pashkin M.P. [Ontology-based approach to configuring of mobile operator products]. [*Scientific Bulletin of NSTU*] (Novosibirsk), 2016, vol. 63, no 2, pp. 99–114. (In Russ).

16. Yeh J.-Y., Wu T.-H., Chang J. Parallel genetic algorithms for product configuration management on PC cluster systems. *The International Journal of Advanced Manufacturing Technology*, 2007, vol. 31, is. 11–12, pp. 1233–1242.

17. Che Z.-H. Using hybrid genetic algorithms for multi-period product configuration change planning. *International Journal of Innovative Computing, Information & Control*, 2010, vol. 6, no. 6, pp. 2781–2785.

18. Dou R., Zong C., Nan G. Multi-stage interactive genetic algorithm for collaborative product customization. *Knowledge Based Systems*, 2016, vol. 92, pp. 43–54.

19. Schuh G., Riesener M., Rudolf S. Identifying preferable product variants using similarity analysis. *Procedia CIRP*, 2014, vol. 20, pp. 38–43.

20. Luce R.D., Howard R. *Games and decisions: introduction and critical surveys*. New York, Wiley, 1957, 740 p.

21. Keeney R.L., Oliver R.M. Designing win-win financial loan products for consumers and businesses. *Journal of the Operational Research Society*, 2005, vol. 56, pp. 1030–1040.

22. Pu P., Faltings B., Chen L., Zhang J., Viappiani P. Usability guidelines for product recommenders based on example critiquing research. *Recommender systems handbook*, eds. by F. Ricci, L. Rokach, B. Shapira, P.B. Kantor. Boston, Springer, 2011, pp. 511–545.

23. Scholz M., Dorner V., Schryen G., Benlian A. A configuration-based recommender system for supporting e-commerce decisions. *European Journal of Operational Research*, 2017, vol. 259, is. 1, pp. 205–215.

24. Shreider Yu.A. *Ravenstvo, shodstvo, porjadok* [Equality, similarity, order]. Moscow, Nauka Publ., 1971, 256 p. (In Russ).

25. Varian H.R. *Intermediate microeconomics: a modern approach*. New York, London, W. W. Norton & Company, 1996 (Russ ed.: N.L. Frolova. Moscow, UNITI Publ., 1997, 767 p.)

26. Chekanskij A.N., Frolova N.L. *Mikroekonomika: promezhutochnyj uroven* [Intermediate microeconomics]: textbook. Moscow, INFRA Publ., 2005, 684 p. (In Russ).

27. Aptekman A., Kalabin V., Klintsov V., Kuznetsova E., Kulagin V., Jasenovets I. Tsifrovaja Rossija: novaja real'nost' [Digital Russia: the new reality]: report. Digital McKinsey, 2017, 134 p. (In Russ).

28. Silverman D. The adviser who knows the client best, wins [Electronic resource]: White Paper. Capital Preferences Ltd., 2017. Patent Pending. Available at: https://www.onefpa.org/Membership/Documents/CapitalPreferences whitepaper-Advisers-who-know-client-wins_Feb2017.pdf (accessed: 5 March 2018).

29. Rudskaja E.N., Poltavskaja Yu.Yu. Profiling of digital client: new formats for intelligent data analysis / E.N. Rudskaja. *Molodoj uchjonyj* [*Young Scientist*], 2015, no. 21, pp. 464–471 (In Russ).

30. Batischev D.I. *Metody optimal'nogo proektirovanija* [Methods of optimal design]: tutorial for universities, Moscow, Radio i svyaz' Publ., 1984, 248 p. (In Russ).

31. Dubov Yu.A., Travkin S.I., Jakimets V.N. *Mnogokriterial'nye modeli formirovanija i vybora variantov sistem* [Multi-criteria models for formation and selection of system variants], Moscow, Nauka Publ., 1986, 296 p. (In Russ).

32. Safronov V.V. A comparative assessment of the «rigid» ranking method, of the fair compromise, and the uniform optimality methods in the hyper-vector ranking of systems tasks. *Information and Control Systems*, 2011, vol. 52, No 3, pp. 2–8. (In Russ).

33. OWL Web Ontology Language Overview; eds. D.L. McGuinness, F. van Harmelen [Electronic resource]: W3C Recommendation. 10 Feb 2004. Available at: https://www.w3.org/TR/owl-features/ (accessed: 11 March 2018).

Tatiana V. Levashova
PhD, Laboratory of computer aided system
Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14th line, St. Petersburg, Russia, 199178
Phone: (812-3) 28-80-71, +7-911-708-10-14
Email: tatiana.levashova@iias.spb.su

Michael P. Pashkin
PhD, Laboratory of computer aided system SPIIRAS
39, 14th line, St. Petersburg, Russia, 199178
Phone: (812-3) 28-80-71
Email: michaelpashkin@mail.ru

УДК 004.8

А.А. Тарамов, Н.Г. Шилов

Рекомендующие системы для информационной поддержки водителя: анализ состояния исследований

Представлен обзор, анализ и систематизация научных работ в области использования рекомендующих систем для информационной поддержки водителя. Показана актуальность данной темы исследований. Выполнена классификация публикаций по четырем тематическим блокам. Определены ключевые характеристики систем информационной поддержки водителей, на основе которых выполнено сравнение работ, наиболее близко относящихся к теме. В качестве наиболее перспективного направления исследований в этой области предложено объединение сервисов и технологий для реализации рекомендующей системы в рассматриваемой области.
Ключевые слова: информационная поддержка водителя, рекомендующая система, аналитический обзор, систематизация, сервис-ориентированная архитектура.
doi: 10.21293/1818-0442-2018-21-2-68-74

Одной из перспективных областей применения информационных технологий является информационная поддержка водителя. Количество частных автотранспортных средств за последнее время существенно увеличилось и продолжает неуклонно расти. Это явилось причиной значимых проблем вне зависимости от географической локализации. Например, в крупных городах все чаще можно увидеть нескончаемые пробки, а на поиск парковочного места может потребоваться значительное время.

Помимо проблем и угроз современный мир также предоставляет и большое количество возможностей. Благодаря глобализации границы стали более открытыми, и число туристов растет год от года [1]. К сожалению, люди все еще вынуждены тратить свое время на поиск оптимальных маршрутов и определение приоритетов, по сути решая сложные математические задачи, которые едва ли должны их касаться. Неверный расчет может привести к нежелательным последствиям, например, к срыву поездки или трате существенного количества времени в пробках [2]. Что касается ежедневных задач, вроде поездки в офис на рабочее место или же турне по магазинам, то ситуация ничем не лучше – погода может преподнести неожиданный сюрприз в самый неподходящий момент, дороги закрыться на ремонт, а времени на обдумывание ситуации, тем более за рулем, практически не бывает.

Таким образом, поскольку автомобильное движение является весьма динамичным и непредсказуемым процессом, возлагающим на водителя огромную ответственность как за себя, так и за окружающих, предоставление точной контекстно зависимой информации подчас бывает жизненно важным фактором.

Учитывая перечисленные факты, становится очевидным, что для эффективного решения данной задачи необходимы новые технологии, способные обеспечивать информационную поддержку водителя в режиме реального времени. Интегрированная реализация таких технологий называется «системой информационной поддержки водителя». В большинстве случаев данные системы включают в себя несколько различных технологий, окончательный состав которых определяется общим назначением системы. Типичными примерами таких технологий являются предоставление рекомендаций, методы анализа состояния водителя, алгоритмы построения маршрута.

Последние, исходя из названия, используются для автомобильной навигации методом нахождения кратчайшего пути между заданными точками с учетом определенных ограничений. Системы анализа состояния водителя могут отслеживать различные показатели находящегося за рулём человека – начиная от физиологических данных и заканчивая степью его рассеянности и анализом эмоций [3]. Технологии предоставления рекомендаций, лежащие в основе рекомендующих систем, используются для предоставления пользователям ранжированного согласно некоторым критериям списка сущностей, коими могут быть сервисы, продукты, географические локации, которые соответствуют предпочтениям конкретного пользователя [2]. Их можно встретить повсеместно на просторах сети Интернет, в сервисах, где ведется учет пользовательских предпочтений. Однако этим их применение не ограничивается, и сегодня они широко распространены, в том числе в сфере информационной поддержки водителя [1].

Эффективная информационная поддержка водителя достигается благодаря обработке контекстной информации и анализу персонализированных пользовательских данных, выполняемому с помощью технологий рекомендующих систем, что позволяет составлять целостную картину текущей ситуации и даже прогнозировать предстоящие события. Данный тип систем представляется предпочтительным ввиду наличия ограничений на возможное взаимодействие водителя с системой во время движения [4].

Таким образом, данная статья посвящена обзору, анализу и систематизации существующих на текущий момент методологических и технологических решений в области информационной поддержки водителя. Рассматриваются решения, относящиеся к предоставлению информации о маршруте, а также

сопутствующей информации с точки зрения ее обработки для персонализированного контекстно-зависимого предоставления пользователю. Авторы не рассматривают вопросы, связанные с анализом работы узлов автомобиля или состояния пользователя.

Анализ публикаций в области информационной поддержки водителя

Поиск публикаций осуществлялся в системах доступа к научным публикациям ScienceDirect (http://www.sciencedirect.com/) и Springer (http://www.springer.com/gp/computer-science/). На основе выбранных ключевых слов были отобраны 28 публикаций со средним возрастом 2,5 года.

Проведя соответствующие наблюдения, можно заметить, что количество литературы, по крайней мере согласно текущей выборке, неуклонно растет, что подтверждает актуальность рассматриваемой темы (рис. 1).

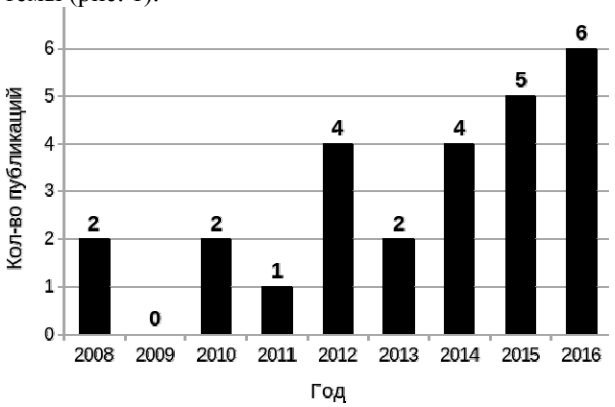


Рис. 1. Количество найденных публикаций в области информационной поддержки водителя

Несмотря на схожую тематику представленных работ, список проблем, покрываемых ими, крайне неоднороден – одни статьи сфокусированы на сугубо теоретической проблематике, без касательства к вероятной практической области применения (например, работы, оценивающие эффективность разных математических моделей, используемых для создания рекомендаций [5–8]), иные же, наоборот, посвящены решению весьма прикладных задач, возникающих в ходе проектирования конкретного технического решения (например, MOVE [4], где описывается проблема восприятия водителем информации, представленной в различных текстово-графических формах). Подобное многообразие отражает сложность и глубину исследуемой темы. Изучив все материалы, были определены пять основных проблемных областей, затронутых в рассматриваемых статьях и релевантных для настоящего исследования:

– Информационная поддержка водителя: практические способы предоставления информации водителю.

– Рекомендующая система: описание готовой системы формирования рекомендаций и предоставления этих рекомендаций конечному пользователю.

– Учет контекста: использование контекстной информации для информационной поддержки водителя (в том числе формирования рекомендаций).

– Алгоритмы рекомендующих систем: описание математического базиса, используемого для создания алгоритма формирования рекомендаций.

– Описание платформы: платформа, используемая в системе информационной поддержки водителя.

В табл. 1 приведено соответствие выбранных публикаций рассматриваемой проблематике. На ее основании можно сделать вывод о том, что следующие статьи недостаточно соответствуют предметной области данного обзора, поскольку не содержат ни одного полного тематического совпадения с выделенными категориями:

• Vehicle to Vehicle GeoNetworking using Wireless Sensor Networks [27].

• User resistance to acceptance of In-Vehicle Infotainment (IVI) [26].

Таблица 1

Тематика публикаций

Публикация	Информационная поддержка водителя	Рекомендующая система	Учет контекста	Алгоритмы рекомендующих систем	Описание платформы
[1]	✔	✔	✔	✔	✔
[2]	✔	✔	✔		✔
[3]	✔	✔			
[4]	✔	±	✔		✔
[5]		✔	✔	✔	✔
[6]		✔	✔	✔	
[7]		✔	✔	✔	
[8]			✔	✔	
[9]	✔	±	✔		✔
[10]	✔	✔	✔		✔
[11]		✔	✔	✔	✔
[12]		✔	✔	✔	
[13]	✔	✔	✔		
[14]	✔	✔	✔		✔
[15]		✔	✔	✔	✔
[16]			✔	✔	
[17]	✔	±	±		
[18]	✔	±	±		✔
[19]	✔	✔	✔	✔	
[20]	±	±	±		✔
[21]	✔	✔	✔	✔	
[22]		✔	✔	✔	
[23]		✔	✔	✔	
[24]		✔	✔	✔	
[25]		✔		✔	
[26]		±			
[27]			±		±
[28]	✔	✔	✔		✔

Остальные из перечисленных статей представляют существенный интерес для исследования. Тем не менее выделение каких-либо общих критериев для их анализа и сравнения представляется весьма трудной задачей, так как спектр рассматриваемых вопросов крайне широк. По этой причине статьи были разбиты на тематические блоки, в рамках которых проводилось сравнение (табл. 2).

Первый блок (описание рекомендующей системы для водителя) включает в себя статьи, затрагивающие тему создания систем информационной

поддержки водителя или описания уже существующих. В них может присутствовать как демонстрация алгоритмического ядра системы, так и конфигурации технического характера, вкупе с анализом результативности по отношению к существующим альтернативам.

Второй блок (программные структуры рекомендующих систем) объединяет статьи, посвященные обзору какой-либо платформы, предоставляющей ряд функциональных решений в области рекомендующих технологий. Такие платформы отличаются от одиночных алгоритмов большей комплексностью, тесной интеграцией между составными частями и более обширным списком охватываемых проблем.

В третьем блоке (алгоритмы рекомендующих систем) содержатся статьи, описывающие всевозможные рекомендующие алгоритмы, отдельно от систем поддержки водителя, чье применение возможно также и в других областях. Эти статьи позволяют взглянуть на проблему создания рекомендаций и анализа предпочтений пользователя, абстрагируясь от автомобильной тематики, позволяя тем самым привнести туда что-то новое.

Последний блок (создание рекомендующих систем) содержит статьи, в которых изложены не столько конкретные варианты реализаций систем и их алгоритмов, сколько описания самого процесса создания таких систем и агрегации любого другого опыта подобного рода.

Таблица 2

Классификация публикаций по предметной области исследования

Наименование тематического блока	Публикации, входящие в тематический блок
1. Описание рекомендующей системы для водителя	[1–4, 10, 14, 19, 21, 28]
2. Программные структуры рекомендующих систем	[5, 15, 22]
3. Алгоритмы рекомендующих систем	[6–8, 11, 12, 16, 23–25]
4. Создание рекомендующих систем	[9, 13, 20]

Обсуждение результатов анализа

Данный раздел состоит из определения ключевых характеристик рассматриваемых систем поддержки водителей, последующего их сравнения и определения перспективных областей будущих разработок.

Сравнение решений

Очевидно, что наиболее близкими по смыслу к рассматриваемому вопросу являются публикации первого блока, посвященные описанию рекомендующих систем для водителей. В результате их систематического обзора было выделено несколько отличительных аспектов, которые определяют их функциональную основу и являются общими для систем поддержки водителей:

1. Платформа: программная структура или набор инструментов и интерфейсов, на основе которых построена система.

2. Связь между компонентами: способ передачи информации и соответствующие интерфейсы, которые позволяют частям системы взаимодействовать друг с другом.

3. Используемые модели и алгоритмы: математические модели и алгоритмы, отражающие принципы функционирования системы и представляющие ее программную часть.

4. Анализ предпочтений пользователя: подходы к учету предпочтений пользователя, влияющих на релевантность представленных и обработанных данных для конкретного человека, также определяют уровень настройки системы.

5. Анализ контекстной информации: если предыдущий аспект отвечает за способность системы адаптироваться к определенному пользователю, данный аспект обеспечивает адаптируемость системы к изменениям условий окружающей среды, что позволяет предоставлять информацию, актуальную для текущего местоположения, времени и других обстоятельств.

6. Архитектура: выбранный способ реализации аппаратного и программного обеспечения, который определяет принципы построения и функционирования ключевых элементов системы и их взаимодействие.

Сравнение решений на основе выбранных аспектов представлено в табл. 3, где используются следующие условные обозначения: «–» – данная функция не поддерживается, «?» – соответствующая информация недоступна.

Анализ результатов

Как видно из таблицы, различные исследования сосредоточены на разных, зачастую весьма узких разделах выбранных вопросов. Некоторые из них сосредоточены на использовании любых новых, возможно, неожиданных для данной области алгоритмов, некоторые стремятся получить максимальный результат от взаимодействия независимых сервисов, основанных на принципах сервис-ориентированной архитектуры, другие используют преимущества все более популярной концепции краудсорсинга.

Таким образом, можно сделать вывод о том, что нет однозначно оптимального решения, которое может быть заявлено как «золотой стандарт» [9]. В то же время почти каждая из рассмотренных публикаций предлагает новые возможности, потенциал которых еще полностью не раскрыт. В сочетании со значительной востребованностью систем навигации и рекомендаций в отдельности можно утверждать, что успешная их комбинация на основе предложенных в рассматриваемых работах концепций и технологий станет настоящим прорывом в вопросе интеллектуальной поддержки водителей.

Однако, как отмечалось выше, разработка такого решения вряд ли будет ограничена выбором одной технологии, поскольку каждая имеет свои преимущества и недостатки, которые часто трудно устранить. Например, коллаборативная фильтрация в большинстве случаев справляется с интеллектуаль-

ным анализом предпочтений пользователей, но когда дело доходит до конкретных случаев с заранее определенным контекстом, эффективность этой технологии быстро падает даже при совместном использовании с различными методами коррекции [3, 5–7, 11, 12].

Выбор алгоритма поиска на основе муравьиных колоний является обоснованным для быстрого, ресурсосберегающего поиска кратчайших путей, но в значительной степени зависит от отзывов пользователей и количества участвующих агентов в системе и, следовательно, абсолютно бесполезен в областях с низкой аудиторией [19]. То же самое касается практически любых искусственных нейронных сетей, которые нуждаются в обучении [7]: некоторые гибридные решения, рассмотренные в данной статье, являются достаточно эффективными в преодолении части проблем, но при этом создают новые проблемы, хотя и менее значительные.

В некоторых исследованиях было решено отказаться от внутренних расчетов и сбора данных в пользу сторонних сервисов, в то время как другие сосредоточены на сборе показаний только со своих собственных сенсоров, создавая таким образом полностью автономную систему.

Таким образом, главной проблемой на данный момент является не отсутствие технологий и решений как таковых – на самом их зачастую даже больше, чем требуется. Реальная проблема заключается в отсутствии интероперабельности из-за недостаточной однородности их интерфейсов [11]. Этот факт был также затронут в [10], где было высказано мнение о том, что достойным решением является использование сервис-ориентированной архитектуры. Этот метод требует множества независимых, унифицированных и, следовательно, взаимозаменяемых сервисов, которые составляют функциональные блоки единой системы. Такой подход обеспечивает максимальную гибкость системы и меньшую зависимость от некоторых ее элементов, что позволяет адаптировать окончательную конфигурацию к конкретной задаче.

Таблица 3

Сравнение рассмотренных решений

Публикация	Платформа	Связь между компонентами	Используемые модели и алгоритмы	Анализ предпочтений пользователя	Анализ контекстной информации	Архитектура
[3]	DVE	CAN, TCP/IP	–	Явные требования, данные с сенсоров	Автомобильные сенсоры, камеры	Встроенная система
[1]	–	TCP/IP	Нечеткая оценка путей	Объекты интереса, ограничивающие отношения, предпочтения V2V*, явные требования	V2V, характеристики маршрута, история маршрутов, собранная посредством V2V	V2V, взаимодействие с точками доступа (hot-spots)
[2]	REJA	TCP/IP	Коллаборативная фильтрация	Коллаборативная фильтрация	GPS, фильтрация знаний с учетом местоположения	Трехуровневая архитектура клиент-сервер
[4]	MOVE	–	Картографическое обобщение (5 шагов)	–	На основе текущего местоположения, подход «Zoom in Context»	–
[10]	Transport ML	XML via TCP/IP, TMLDocuments	–	?	На основе связанных сервисов	Сервис-ориентированная архитектура
[14]	PostGIS, расширение PgRouting	HTTP, JSON	Коллаборативная фильтрация, краудсорсинг	?	Данные акселерометра и других сенсоров	Архитектура клиент-сервер
[19]	SACO	?	Оптимизация на основе муравьиных колоний, оценка семантических расстояний	Онтология предметной области	?	?
[21]	–	–	Байесовские сети	Явные предпочтения объектов интереса, история действий пользователя	Онтология пользователя, сенсоры автомобиля	Встроенная система
[28]	?	TCP/IP	Коллаборативная фильтрация	Состояние водителя, определяемое сенсорами	Сервисы, зависящие от местоположения (LBS)	Встроенная система, сервис-ориентированная архитектура для внешних модулей

Заключение

В статье представлен обзор литературы на тему интеллектуальной поддержки водителей и смежных областей исследований. Судя по количеству найденных статей и динамике их роста, можно сделать вывод о том, что этот вопрос активно развивается благодаря усилиям научного сообщества и находит поддержку среди заинтересованных сторон.

Несмотря на весьма разные подходы к разработке систем поддержки водителей, которые были описаны в рассмотренных публикациях, а также разнообразие решаемых задач, авторы постарались организовать вышеупомянутые публикации и рассмотреть их в рамках единой парадигмы.

На основании выполненного анализа можно сделать вывод о том, что проблема разработки системы интеллектуальной поддержки водителей является весьма актуальной. В то же время в ходе настоящей работы наиболее перспективным направлением исследований в этой области предложено объединение сервисов и технологий для реализации решения поставленной проблемы на основе сервис-ориентированной архитектуры.

Работа выполнена при финансовой поддержке РФФИ (проекты № 18-07-01201 и 18-07-01203) и бюджетной темы № 0073-2018-0002.

Литература

1. A real-time personalized route recommendation system for self-drive tourists based on vehicle to vehicle communication / L. Liu, J. Xu, S.S. Liao, H. Chen // Expert Systems with Applications. – 2014. – Vol. 41, No. 7. – PP. 3409–3417.

2. A mobile 3D-GIS hybrid recommender system for tourism / J.M. Noguera, M.J. Barranco, R.J. Segura, L. Martínez // Information Sciences. – 2012. – Vol. 215. – PP. 37–52.

3. Driver–Vehicle–Environment monitoring for on-board driver support systems: Lessons learned from design and implementation / A. Amditis, K. Pagle, S. Joshi, E. Bekiaris // Applied Ergonomics. – 2010. – Vol. 41, No. 2. – PP. 225–235.

4. Lee J. Iterative design of MOVE: A situationally appropriate vehicle navigation system / J. Lee, J. Forlizzi, S.E. Hudson // International Journal of Human-Computer Studies. – 2008. – Vol. 66, No. 3. – PP. 198–215.

5. Panigrahi S. A Hybrid Distributed Collaborative Filtering Recommender Engine Using Apache Spark / S. Panigrahi, R.K. Lenka, A.A. Stitipragyan // Procedia Computer Science. – 2016. – Vol. 83. – PP. 1000–1006.

6. Kothari A.A. A Novel Approach Towards Context Based Recommendations Using Support Vector Machine Methodology / A.A. Kothari, W.D. Patel // Procedia Computer Science. – 2015. – Vol. 57. – PP. 1171–1178.

7. Elahi M. A survey of active learning in collaborative filtering recommender systems / M. Elahi, F. Ricci, N. Rubens // Computer Science Review. – 2016. – Vol. 20. – PP. 29–50.

8. Baltrunas L. Experimental evaluation of context-dependent collaborative filtering using item splitting / L. Baltrunas, F. Ricci // User Modeling and User-Adapted Interaction. – 2014. – Vol. 24, No. 1–2. – PP. 7–34.

9. Tideman M. A new scenario based approach for designing driver support systems applied to the design of a lane change support system / M. Tideman, M.C. van der Voort, B. van Arem // Transportation Research Part C: Emerging Technologies. – 2010. – Vol. 18, No. 2. – PP. 247–258.

10. Ait-Cheik-Bihi W. A Platform for Interactive Location-Based Services / W. Ait-Cheik-Bihi, M. Bakhouya, A. Nait-Sidi-Moh, J. Gaber, M. Wack // Procedia Computer Science. – 2011. – Vol. 5. – PP. 697–704.

11. Yeung K.F. A proactive personalised mobile recommendation system using analytic hierarchy process and Bayesian network / K.F. Yeung, Y. Yang, D. Ndzi // Journal of Internet Services and Applications. – 2012. – Vol. 3, No. 2. – PP. 195–214.

12. Champiri Z.D. A systematic review of scholar context-aware recommender systems / Z.D. Champiri, S.R. Shahamiri, S.S.B. Salim // Expert Systems with Applications. – 2015. – Vol. 42, No. 3. – PP. 1743–1758.

13. Fastrez P. Designing and evaluating driver support systems with the user in mind / P. Fastrez, J.-B. Haué // International Journal of Human-Computer Studies. – 2008. – Vol. 66, No. 3. – PP. 125–131.

14. Predic B. Enhancing driver situational awareness through crowd intelligence / B. Predic, D. Stojanovic // Expert Systems with Applications. – 2015. – Vol. 42, No. 11. – PP. 4892–4909.

15. Hussein T. Hybreed: A software framework for developing context-aware hybrid recommender systems / T. Hussein, T. Linder, W. Gaulke, J. Ziegler // User Modeling and User-Adapted Interaction. – 2014. – Vol. 24, No. 1–2. – PP. 121–174.

16. Panniello U. Incorporating context into recommender systems: an empirical comparison of context-based approaches / U. Panniello, M. Gorgoglione // Electronic Commerce Research. – 2012. – Vol. 12, No. 1. – PP. 1–30.

17. Borràs J. Intelligent tourism recommender systems: A survey / J. Borràs, A. Moreno, A. Valls // Expert Systems with Applications. – 2014. – Vol. 41, No. 16. – PP. 7370–7389.

18. Fors C. Interface design of eco-driving support systems – Truck drivers' preferences and behavioural compliance / C. Fors, K. Kircher, C. Ahlström // Transportation Research Part C: Emerging Technologies. – 2015. – Vol. 58. – PP. 706–720.

19. Mocholi J.A. Learning semantically-annotated routes for context-aware recommendations on map navigation systems / J.A. Mocholi, J. Jaen, K. Krynicki, A. Catala, A. Picón, A. Cadenas // Applied Soft Computing Journal. – 2012. – Vol. 12, No. 9. – PP. 3088–3098.

20. Gavalas D. Mobile recommender systems in tourism / D. Gavalas, C. Konstantopoulos, K. Mastakas, G. Pantziou // Journal of Network and Computer Applications. – 2014. – Vol. 39. – PP. 319–333.

21. Lüddecke D. Modeling context-aware and intention-aware in-car infotainment systems / D. Lüddecke, C. Seidl, J. Schneider, I. Schaefer // Software & Systems Modeling. – 2016. – PP. 1–15 [Электронный ресурс]. – Режим доступа: http://www.ssl.stu.neva.ru/psw/crypto.html, требуется подписка (дата обращения: 28.07.2017).

22. Rodríguez-Hernández M. del C. Pull-based recommendations in mobile environments / M. del C. Rodríguez-Hernández, S. Ilarri // Computer Standards & Interfaces. – 2016. – Vol. 44. – PP. 185–204.

23. Bobadilla J. Recommender systems survey / J. Bobadilla, F. Ortega, A. Hernando, A. Gutiérrez // Knowledge-Based Systems. – 2013. – Vol. 46. – PP. 109–132.

24. Unger M. Towards latent context-aware recommendation systems / M. Unger, A. Bar, B. Shapira, L. Rokach // Knowledge-Based Systems. – 2016. – Vol. 104. – PP. 165–178.

25. Kurashima T. Travel route recommendation using geotagged photos / T. Kurashima, T. Iwata, G. Irie, K. Fujimura // Knowledge and Information Systems. – 2013. – Vol. 37, No. 1. – PP. 37–60.

26. Kim J. User resistance to acceptance of In-Vehicle Infotainment (IVI) systems / J. Kim, S. Kim, C. Nam // Telecommunications Policy. – 2016. – Vol. 40, No. 9. – PP. 919–930.

27. Anaya J.J. Vehicle to Vehicle GeoNetworking using Wireless Sensor Networks / J.J. Anaya, E. Talavera, F. Jiménez, F. Serradilla, J.E. Naranjo // Ad Hoc Networks. – 2015. – Vol. 27. – PP. 133–146.

28. Árnason J.I. Volvo intelligent news: A context aware multi modal proactive recommender system for in-vehicle use / J.I. Árnason, J. Jepsen, A. Koudal, M.R. Schmidt, S. Serafin // Pervasive and Mobile Computing. – 2014. – Vol. 14. – PP. 95–111.

Тарамов Андрей Александрович
Студент каф. информационных систем
Университета ИТМО
Кронверкский пр-т., д. 49, г. Санкт-Петербург, 197101
Тел.: +7 (812) 328-80-71
Эл. почта: tar-aa-spb@yandex.ru

Шилов Николай Германович
Канд. техн. наук, доцент, с.н.с. лаб.
интегрированных систем автоматизации СПИИРАН
14-я линия, д. 39, г. Санкт-Петербург, 199178
Тел.: +7 (812-3) 28-80-71
Эл. почта: nick@iias.spb.su

Taramov A.A., Shilov N.G.
Recommender Systems for Driver Information Support: State-of-the-Art Review

The article presents a review, analysis and systematization of scientific works in the area of recommender system application to driver information support. The relevance of this research topic is shown. The classification of publications on four thematic blocks is proposed. The key characteristics of driver information support systems are identified and used as the basis for comparison of works most closely related to the topic. The integration of services and technologies for implementation of a recommender system in the considered domain is proposed as a promising research direction.
Keywords: driver information support, recommender system, state-of-the-art review, systematization, service-oriented architecture.
doi: 10.21293/1818-0442-2018-21-2-68-74

References

1. Liu L., Xu J., Liao S.S., Chen H. A real-time personalized route recommendation system for self-drive tourists based on vehicle to vehicle communication. *Expert Systems with Applications*, 2014, vol. 41, no. 7, pp. 3409–3417.

2. Noguera J.M., Barranco M.J., Segura R.J., Martínez L. A mobile 3D-GIS hybrid recommender system for tourism. *Information Sciences*, 2012, vol. 215, pp. 37–52.

3. Amditis A., Pagle K., Joshi S., Bekiaris E. Driver-Vehicle-Environment monitoring for on-board driver support systems: Lessons learned from design and implementation. *Applied Ergonomics*, 2010, vol. 41, no. 2, pp. 225–235.

4. Lee J., Forlizzi J., Hudson S.E., Lee J. Iterative design of MOVE: A situationally appropriate vehicle navigation system. *International Journal of Human-Computer Studies*, 2008, vol. 66, no. 3, pp. 198–215.

5. Panigrahi S., Lenka R.K., Stitipragyan A.A. A Hybrid Distributed Collaborative Filtering Recommender Engine Using Apache Spark. *Procedia Computer Science*, 2016, vol. 83, pp. 1000–1006.

6. Kothari A.A., Patel W.D. A Novel Approach Towards Context Based Recommendations Using Support Vector Machine Methodology. *Procedia Computer Science*, 2015, vol. 57, pp. 1171–1178.

7. Elahi M., Ricci F., Rubens N. A survey of active learning in collaborative filtering recommender systems. *Computer Science Review*, 2016, vol. 20, pp 29–50.

8. Baltrunas L., Ricci F. Experimental evaluation of context-dependent collaborative filtering using item splitting. *User Modeling and User-Adapted Interaction*, 2014, vol. 24, no. 1, pp. 7–34.

9. Tideman M.,van der Voort M.C., van Arem B. A new scenario based approach for designing driver support systems applied to the design of a lane change support system. *Transportation Research Part C: Emerging Technologies*, 2010, vol. 18, no. 2, pp. 247–258.

10. Ait-Cheik-Bihi W., Bakhouya M., Nait-Sidi-Moh A., Gaber J., Wack M. A Platform for Interactive Location-Based Services. *Procedia Computer Science*, 2011, vol. 5, pp. 697–704.

11. Yeung K.F., Yang Y., Ndzi D. A proactive personalised mobile recommendation system using analytic hierarchy process and Bayesian network. *Journal of Internet Services and Applications*, 2012, vol. 3, no. 2, pp. 195–214.

12. Champiri Z.D., Shahamiri S.R., Salim S.S.B. A systematic review of scholar context-aware recommender systems. *Expert Systems with Applications*, 2015, vol. 42, no. 3, pp. 1743–1758.

13. Fastrez P., Haué J.-B. Designing and evaluating driver support systems with the user in mind. *International Journal of Human-Computer Studies*, 2008, vol. 66, no. 3, pp. 125–131.

14. Predic B., Stojanovic D. Enhancing driver situational awareness through crowd intelligence. *Expert Systems with Applications*, 2015, vol. 42, no. 11, pp. 4892–4909.

15. Hussein T., Linder T., Gaulke W., Ziegler J. Hybreed: A software framework for developing context-aware hybrid recommender systems. *User Modeling and User-Adapted Interaction*, 2014, vol. 24, no. 1–2, pp. 121–174.

16. Panniello U, Gorgoglione M. Incorporating context into recommender systems: an empirical comparison of context-based approaches. *Electronic Commerce Research*, 2012. vol. 12, no. 1, pp. 1–30.

17. Borràs J., Moreno A., Valls A. Intelligent tourism recommender systems: A survey. *Expert Systems with Applications*, 2014, vol. 41, no. 16, pp. 7370–7389.

18. Fors C., Kircher K., Ahlström C. Interface design of eco-driving support systems – Truck drivers' preferences and behavioural compliance. *Transportation Research Part C: Emerging Technologies*, 2015, vol. 58, pp. 706–720.

19. Mocholi J.A., Jaen J., Krynicki K., Catala A., Picón A., Cadenas A. Learning semantically-annotated routes for context-aware recommendations on map navigation systems. *Applied Soft Computing Journal*, 2012, vol. 12, no. 9, pp. 3088–3098.

20. Gavalas D., Konstantopoulos C., Mastakas K., Pantziou G. Mobile recommender systems in tourism. *Journal of Network and Computer Applications*, 2014, vol. 39, pp. 319–333.

21. Lüddecke D., Seidl C., Schneider J., Schaefer I. Modeling context-aware and intention-aware in-car infotain-

ment systems. *Software & Systems Modeling*, 2016, pp. 1–15. Available at: http://www.ssl.stu.neva.ru/psw/crypto.html (accessed: 28.07.2017).

22. Rodríguez-Hernández M. del C., Ilarri S. Pull-based recommendations in mobile environments. *Computer Standards & Interfaces*, 2016, vol. 44, pp. 185–204.

23. Bobadilla J., Ortega F., Hernando A., Gutiérrez A. Recommender systems survey. *Knowledge-Based Systems*, 2013, vol. 46, pp. 109–132.

24. Unger M., Bar A., Shapira B., Rokach L. Towards latent context-aware recommendation systems. *Knowledge-Based Systems*, 2016, vol. 104, pp. 165–178.

25. Kurashima T., Iwata T., Irie G., Fujimura K. Travel route recommendation using geotagged photos. *Knowledge and Information Systems*, 2013, vol. 37, no. 1, pp. 37–60.

26. Kim J., Kim S., Nam V. User resistance to acceptance of In-Vehicle Infotainment (IVI) systems. *Telecommunications Policy*, 2016, vol. 40, no. 9, pp. 919–930.

27. Anaya J.J., Talavera E., Jiménez F., Serradilla F., Naranjo J.E. Vehicle to Vehicle GeoNetworking using Wireless Sensor Networks. *Ad Hoc Networks*, 2015, vol. 27, pp. 133–146.

28. Árnason J.I., Jepsen J., Koudal A., Schmidt M.R., Serafin S. Volvo intelligent news: A context aware multi modal proactive recommender system for in-vehicle use. *Pervasive and Mobile Computing*, 2014, vol. 14, pp. 95–111.

Andrei A. Taramov
Master Student
Department of Information Systems
ITMO University
Kronverksky pr., 49, St. Petersburg, Russia, 197101
Phone: +7 (812-3) 28-80-71
Email: tar-aa-spb@yandex.ru

Nikolay G. Shilov
Doctor of Engineering Sciences, Senior Researcher
Computer-Aided Integrated Systems Laboratory SPIIRAS
14 Line, 39, St. Petersburg, Russia, 199178
0000-0002-9264-9127
Phone: +7 (812-3) 28-80-71
Email: nick@iias.spb.su

УДК 519.683.8, 004.4’236

В.М. Дмитриев, Т.В. Ганджа, А.С. Букреев

Моделирование сценариев управления динамическими объектами на основе графического языка X-Robot

С ростом числа функций динамических объектов усложняются алгоритмы, на основе которых функционируют их устройства управления. Также увеличиваются программы, написанные на низкоуровневых языках программирования контроллеров, что усложняет процесс их отладки. Актуальность разработки новых средств формирования и моделирования сценариев функционирования контроллеров обусловлена необходимостью учёта многих наблюдаемых переменных и использования ряда управляющих воздействий, а также нетривиальностью алгоритмов функционирования контроллеров.

Рассматриваются принципы моделирования сценариев управления динамическими объектами с использованием графических нотаций языка X-Robot. Помимо традиционного текстового представления программы, называемой сценарием, для данного языка предложена и разработана графическая интерпретация, ставящая для каждой его команды определенный компонент. Графическое формирование сценариев осуществляется в среде компьютерного моделирования МАРС на логическом уровне многоуровневой компьютерной модели, на объектном уровне которой располагается модель управляемого динамического объекта с включенными в нее моделями исполнительных и измерительных устройств. Это открывает возможности формирования сценариев управления в графической форме и их предварительной отладки на модели динамического объекта. На визуальном уровне многоуровневой компьютерной модели располагаются управляющие компоненты, с помощью которых пользователь имеет возможность воздействовать на модель объекта и модель сценария, а также компоненты-визуализаторы, осуществляющие отображение для пользователя данных для визуализации, которыми могут быть как значения наблюдаемых переменных объекта, так и их обобщенные параметры-функционалы. В настоящее время разработанный графический язык моделирования сценариев адаптирован к контроллеру X-Mega, но ведутся исследования по его развитию и применению к управляющим контроллерам других типов.

Ключевые слова: компонент, контроллер, сценарий, динамический объект, многоуровневая компьютерная модель.

doi: 10.21293/1818-0442-2018-21-2-75-82

В настоящее время при реализации устройств управления получили широкое распространение различные контроллеры: X-Mega [1, 2], Arduino [3] и т.п. Их функционирование основано на сценариях, которые формируются на различных языках программирования. Большинство из них являются или приближены к языкам программирования для логических контроллеров. К большинству из существующих контроллеров созданы программно-инструментальные средства программирования и формирования сценариев в текстовой или графической форме [4]. Зачастую отладка и настройка устройств управления с использованием реального объекта затруднены или невозможны вследствие различных причин. К ним относятся сложность технической реализации исполнительных и измерительных устройств, необходимость расчета или подбора значений их параметров, безопасность использования объекта управления, а также большие финансовые затраты для постановки реальных экспериментов.

Большинство языков программирования контроллеров согласуются с международным стандартом IEC 61131 [5], включающим в себя три графических и два текстовых языка. Графические языки базируются на различных графических платформах: язык LD является программной реализацией электрических схем на базе электромагнитных реле. Язык FD представляет сценарий функционирования контроллера в виде некоторой подпрограммы, а язык SFC основан на базе математического аппарата сетей Петри [6]. Текстовые языки аналогичны известным языкам программирования: сценарии функционирования контроллеров, написанные на язык ST, напоминают программы языка Паскаль, а сценарии языка IL подобны программам, написанным на языке Ассемблер.

Для программирования контроллеров с использованием обозначенных языков используются системы CodeSys [7, 8] и ISaGRAF [9]. Автоматизируя все необходимые функции по разработке сценария, прошивки его в контроллер с последующим тестированием и отладкой разработанного кода, данные системы не включают в свой состав средств моделирования управляемых технических объектов. Это не позволяет осуществлять предварительную отладку разработанного сценария на модели объекта, а предполагают работать напрямую с реальным объектом. Использование моделей управляемых объектов направлено на существенное облегчение разработки и отладки сценариев функционирования контроллеров.

Для решения данных проблем в работе предлагается использовать графический язык формирования сценариев управляющих контроллеров X-Robot [10], а также встроенный в среду многоуровневого компьютерного моделирования МАРС [11] модуль графического моделирования сценариев [12]. Язык X-Robot имеет текстовую нотацию, приближенную к низкоуровневому языку Ассемблер, которая не позволяет интегрировать сценарий с моделью объекта, представленной в среде моделирования МАРС. Для

решения проблемы в работе предлагается графическая интерпретация языка X-Robot, позволяющая интегрировать разрабатываемый сценарий с моделью управляемого объекта. Она позволяет разрабатывать сценарии в компонентной форме и осуществлять их предварительную отладку на компьютерных моделях объектов управления, исследуя при этом наблюдаемые характеристики модели управляемого объекта и варьируя различные её параметры, а также управляющие и возмущающие воздействия.

Модуль моделирования сценариев лежит в основе разработки курса лабораторных работ по дисциплине «Основы проектирования систем и средств управления», являющейся базовой профилирующей дисциплиной при подготовке бакалавров по направлению «Системный анализ и управление».

Сценарий языка управления динамическими объектами X-Robot

Поведение динамического объекта описывается сценарием на языке X-Robot [10]. Он разбит на блоки, определяющие отдельные процессы, выполняющиеся параллельно. Каждый процесс имеет собственную локальную ячейку памяти – аккумулятор, собственный таймер и регистр состояния для условного ветвления. К атрибутам процесса относятся флаги ожидания, которые при запуске сценария сбрасываются для всех процессов. Каждый процесс представляет собой безусловный цикл с опционной секцией предварительной настройки, расположенной в начале процесса. За ней идет его рабочая секция, после выполнения последней инструкции которой осуществляется безусловный переход на первую инструкцию рабочей секции. Перед этим производится попытка переключиться на следующий процесс.

При первом запуске сценария последовательно запускаются все процессы, начиная с первого. Если в тексте выполняемого процесса встречается инструкция ожидания или любого изменения порядка выполнения инструкций, выполняется попытка переключения на следующий процесс. Если его нет, то снова выполняется первый процесс. Инструкции ожидания взводят флаг ожидания процесса. Он перестает обрабатываться диспетчером и не занимает процессорного времени контроллера.

В настоящее время существует два способа формирования сценариев языка X-Robot: текстовый, когда сценарий формируется в любом текстовом редакторе в виде инструкций с их разделением на процессы, и графический, при котором каждой инструкции языка ставится в соответствие компонент, реализующий его в рамках модуля моделирования сценариев среды многоуровневого компьютерного моделирования.

Многоуровневая структура компьютерной модели в модуле моделирования сценариев

Модуль моделирования сценариев в формате языка X-Robot реализован в рамках среды многоуровневого компьютерного моделирования МАРС [13]. Его основными задачами являются:

– моделирование и анализ поведения объекта управления при формировании и выполнении различных команд управления;

– формирование сценариев функционирования управляющих контроллеров и отладка их параллельных потоков на компьютерных моделях объектов управления;

– интерпретация сформированного графического сценария в код с последующим программированием контроллера;

– отладка поведения модели объекта с использованием виртуальных приборов, разработанных в системе виртуальных инструментов и приборов [14, 15].

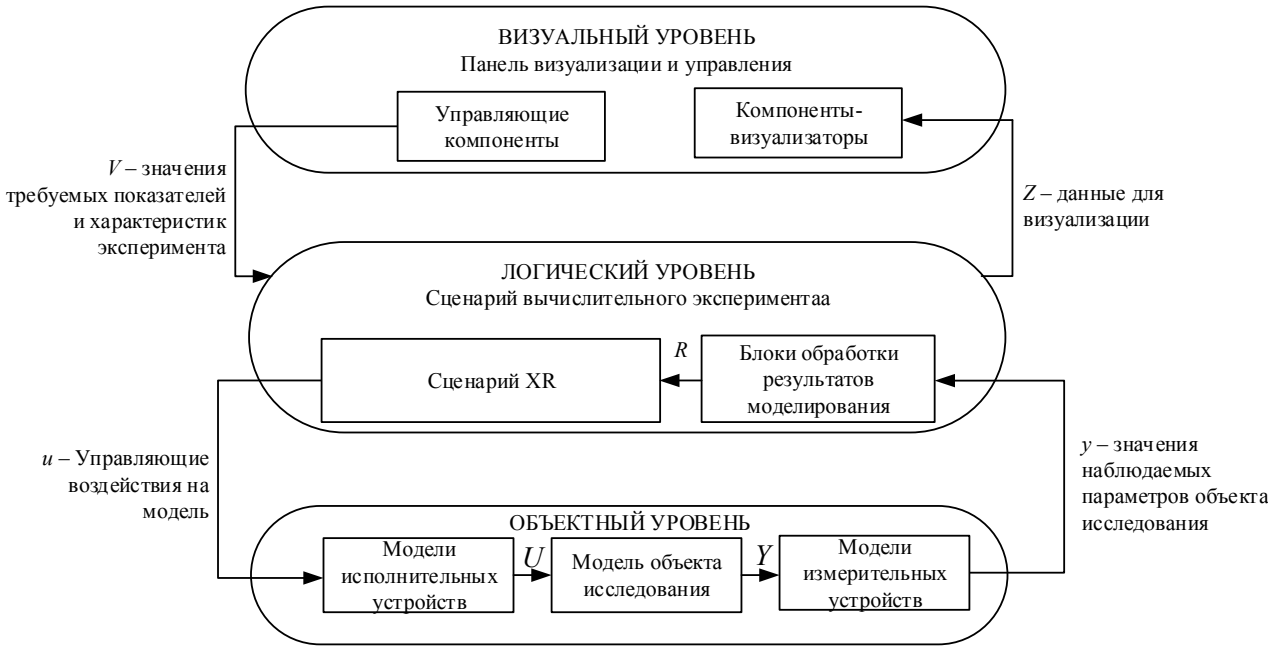


Рис. 1. Структура многоуровневой компьютерной модели для формирования и отладки графических сценариев

Компьютерная модель, предназначенная для формирования и отладки сценариев управления, представлена многоуровневой компьютерной моделью [16] (рис. 1), на трех уровнях которой располагаются взаимосвязанные модели:

– на объектном уровне расположена компьютерная модель объекта управления с подключенными к ней моделями измерительных и исполнительных устройств. Они формируются на основе метода компонентных цепей [17] и в общем случае представляют собой системы алгебро-дифференциальных уравнений. Формирование общей модели в виде системы алгебро-дифференциальных уравнений, линеаризация нелинейных и алгебраизация дифференциальных уравнений с последующим решением системы линейных алгебраических уравнений на каждом шаге анализа по времени производится универсальным вычислительным ядром [18]. С помощью моделей измерительных устройств, имеющих свои графические отображения одновременно на многоуровневой компьютерной модели осуществляется передача значений наблюдаемых переменных объекта управления y с объектного уровня на логический;

– на логическом уровне формируется функциональная модель устройства управления в виде параллельных потоков сценария, взаимосвязанного с моделью объекта управления. Функционирование сценария осуществляется алгоритмом передачи сообщений [19];

– на визуальном уровне располагаются средства визуализации результатов моделирования и работы сценария управления, а также средства интерактивного управления задающими воздействиями [20, 21].

Формируемый на логическом уровне многоуровневой компьютерной модели сценарий функционирования управляющего контроллера в формате графического представления нотаций языка X-Robot на основе значений наблюдаемых переменных объекта управления y осуществляет выработку управляющих воздействий на модель исполнительных устройств u. С формальной точки зрения сценарий управления может быть представлен моделью

$$U = F_{SC}(y),$$

где F_{SC} – функция сценария, заданная в явной форме в виде набора последовательно соединенных элементарных инструкций (команд) языка управления механизмами X-Robot.

Классификация компонентов графического сценария

Компонент, отображающий одну из инструкций (команд) языка X-Robot, представлен на рис. 2 и содержит следующие связи:

1) входные информационные связи $X1$ и $X2$, по которым в компонент передаются значения вступающих в операцию операндов;

2) управляющие связи $U1$ и $U2$, причем $U1$ предназначена для приема сигнала начала выполнения операции, а $U2$ – для передачи управляющего сигнала следующему компоненту;

3) выходная информационная связь Y, по которой передается результат выполнения операции.

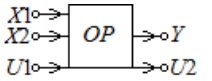


Рис. 2. Обобщенный компонент операции языка X-Robot

В ряде компонентов, описывающих операции ветвления, имеется одна входная управляющая связь $U1$ и одна входная информационная связь $X1$. На основе анализа поступающего по ней значения переменной осуществляется ветвление сценария по одной из выходных управляющих связей: $U2$, $U3$, …, Un. Некоторые компоненты могут иметь только управляющие сигналы.

Рассмотрим основные классы компонентов, из которых осуществляется формирование графических сценариев.

Компоненты начала и окончания процессов и подпрограмм предназначены для обозначения определенных блоков сценария, а также позволяют отделить блок инициализации от основного потока, циклически выполняющегося при работе сценария. Каждый компонент данного класса включает только одну входную $U1$ и одну выходную $U2$ управляющие связи. В данный класс компонентов входят компоненты, обозначающие начало (Begin Process) и конец процесса (End Process), начала цикла процесса (Begin), а также компоненты, при выполнении которых производится безусловный переход на начало процесса как с выполнением блока инициализации (INT), так и без выполнения этого блока (RST).

Класс компонентов взаимодействия сценария с датчиками и исполнителями содержит 8 команд считывания информации с датчиков ($In0$, …, $In7$), а также 8 команд передачи команд исполнителям ($Ex0$, …, $Ex7$). Каждый датчик и исполнитель задаются своим номером от 0 до 255. По входной управляющей связи $U1$ осуществляется передача команды на выполнение, управляющая связь $U2$ предназначена для передачи другим компонентам сигнала о завершении выполнения команды.

Класс компонентов команд ожидания предназначен для остановки некоторого процесса до выполнения определенного события или достижения определенного времени. Обобщенный компонент этого класса представлен на рис. 3.

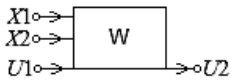


Рис. 3. Обобщённый вид компонентов ожидания

Ожидание начинается с момента времени, когда поступает сообщение на управляющую связь $U1$. В момент наступления ожидаемого события осуществляется передача сообщения по управляющей связи $U2$. По информационным связям $X1$ и $X2$ в компонент при отладке сценария поступают данные, характеризующие значения определенных переменных или текущего времени. К данному классу относятся

компоненты: ожидания заданного промежутка времени (WT), ожидания сообщения (WM), ожидания равенства переменных $X1 = X2$ (WD), ожидания неравенства переменных $X1 \neq X2$ (WND), ожидания больше $X1 > X2$ (WDH), ожидания меньше $X1 < X2$ (WDL). Последовательное соединение данных компонентов в группы представляет собой структуру «ИЛИ». Для их включения в схему «И» используется компонент, обозначающий команду BAND языка X-Robot.

Класс компонентов работы с подпрограммами содержит команды, позволяющие представить один из процессов сценария в виде подпрограммы и вызвать его из другого процесса. Для этого компонентами представлены следующие команды:

– команда вызова подпрограммы (CALL) – устанавливается в процесс, который должен вызвать другой процесс;

– команда ожидания вызова подпрограммы (WR) – устанавливается в процесс-подпрограмму, которая должна выполниться по соответствующей команде CALL.

Класс компонентов арифметических и побитовых операций включает в себя компоненты, для выполнения основных бинарных арифметических и побитовых операций. К ним относятся: присваивание переменной некоторого значения (MOV); суммирование (ADD), вычитание (SUB), побитовое И (AND), побитовое ИЛИ (OR), побитовое исключающее ИЛИ (XOR), команда перестановки байтов (SWAP) и команды побитового сдвига влево (LSL) и вправо (LSR).

Каждая из этих команд выполняется при поступлении на управляющий вход $U1$ компонента (см. рис. 2) сигнала о выполнении над последними полученными значениями операндов $X1$ и $X2$.

Все переменные являются глобальными, и их значения одинаковы для всех потоков сценария. При этом у каждого из процессов есть одна локальная переменная, называемая *аккумулятором*, значение которой для каждого из процессов свое.

Класс компонентов изменения порядка выполнения процесса предназначен для осуществления изменения последовательного порядка выполнения команд процесса, ветвления, циклов и т.п. К этому классу относятся следующие компоненты:

– Компонент «Сравнение» (CMP) при получении сообщений о выполнении по управляющей связи $U1$ осуществляет сравнение последних значений переменных, поступивших по информационным связям $X1$ и $X2$, и на выходную информационную связь Y передает 0, если $X1 = X2$, 1, если $X1 > X2$, и 2, когда $X1 < X2$.

– Компонент «Ветвление» (CASE), имеющий несколько выходных управляющих связей ($U2$, $U3$, …, Un), производит анализ значения, поступившего по информационной связи $X1$, в соответствии с которым посылает сообщение по одной из выходных управляющих связей.

– Компонент «Выбор по сравнению» (CASES) по своей входной информационной связи $X1$ осуществляет прием значения результата операций сравнения и перенаправление выполнения сценария по одной из ветвей, каждая из которых соответствует ситуациям «Меньше», «Равно» или «Больше».

– Компонент «Возврат из структуры сравнения» (RETS) устанавливается в одну из ветвей, образуемых компонентом «Выбор по сравнению». При получении сообщения по входной управляющей связи данный компонент осуществляет безусловный переход на начало команды CASES, в структуре которой он установлен.

– Компонент «Конец структуры выбора» (ENDC) устанавливается в конец каждой ветви сценария, образованной структурами компонентов CASE и CASES.

Таким образом, описаны все классы компонентов, предназначенных для формирования сценариев функционирования управляющих контроллеров на графическом языке X-Robot.

Сценарий управления дискретным объектом

Светофор, организующий регулирование дорожным движением, является дискретным устройством. Модель светофора, содержащая три фонаря, соответственно красного $L1$, жёлтого $L2$ и зелёного цвета $L3$, загорание которых осуществляется с помощью ключей $S1$, $S2$ и $S3$, реализована на объектном уровне многоуровневой компьютерной модели и представлена на рис. 4. Регулировочным резистором $R1$ осуществляется регулировка интенсивности свечения фонарей в зависимости от времени суток, погодных условий и других факторов.

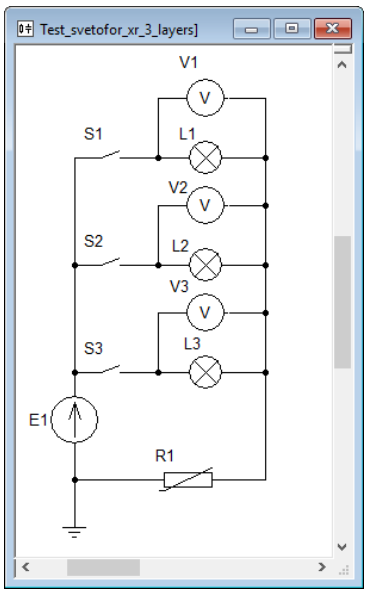


Рис. 4. Компьютерная модель светофора на объектном уровне многоуровневой компьютерной модели

Пусть фонарём красного цвета управляет исполнитель с номером $08, фонарём жёлтого цвета – исполнитель $09, а фонарём зелёного цвета – исполнитель $0a. Каждый из них зажигает определенный фонарь с помощью команды Ex3 подачей максимально возможного значения $7FFF = 32767. Фонарь погасает подачей с помощью команды Ex3 значения 0.

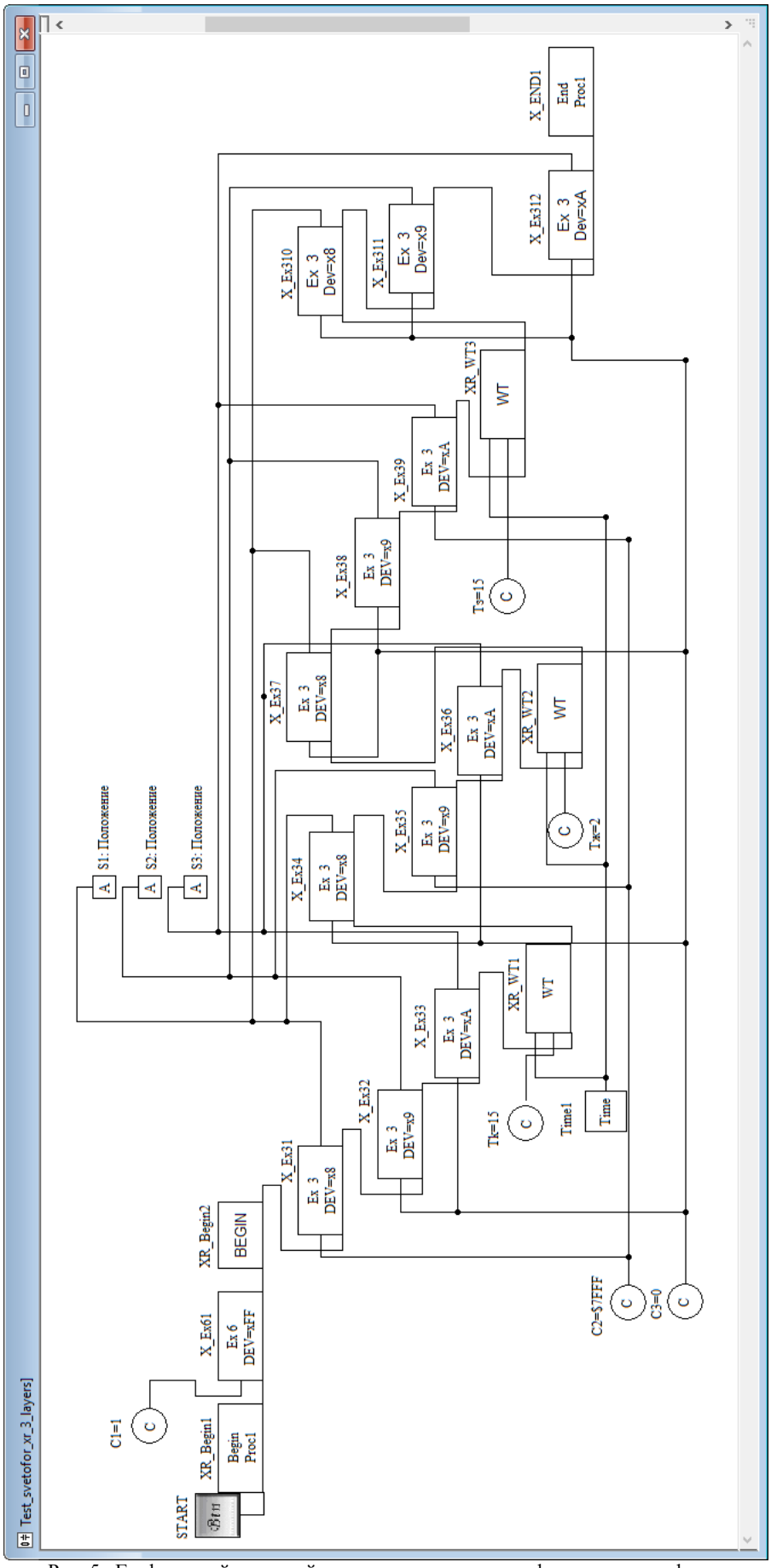


Рис. 5. Графический сценарий управления состоянием фонарями светофора

Инициализация описанных исполнителей, осуществляющих изменение состояний ключей, производится командой Ex6, выполненной для исполнителя инициализации $ff = 255 с аргументом 1. В этом случае осуществляется инициализация ШИМ-генераторов. Блок инициализации ограничивается от основного цикла процесса компонентом XR_Begin2. С помощью компонентов XR_WT1, XR_WT2 и XR_WT3 производится задержка процесса на определённое время, которое должен гореть соответствующий фонарь светофора.

Графическая форма сценария управления состоянием светофора представлена на рис. 5. На основе представленного сценария будет сформирован код для программирования контроллера, осуществляющего управление состоянием светофора.

Заключение

Модуль моделирования сценариев, реализованный в рамках среды многоуровневого компьютерного моделирования, открывает возможности формирования графических сценариев управления динамическими объектами с их отладкой на компьютерных моделях объектов с включенными в них моделями исполнительных и измерительных устройств. Совокупность графического сценария и модели объекта управления также позволяют производить выбор значений параметров компонентов, удовлетворяющих соответствующим критериям качества управления. Применение разработанных программно-инструментальных средств в процессе обучения направлено на автоматизацию проведения практических и лабораторных занятий, в ходе которых студенты и школьники старших классов приобретают первоначальные знания и умения программирования контроллеров. Данные разработки также будут интересны центрам научно-технического творчества молодёжи, деятельность которых направлена на разработку управляемых динамических объектов.

Работа выполнена при финансовой поддержке Минобрнауки в рамках проекта RFMEFI57717X0266.

Литература

1. Гумеров Р.И. Практикум по микропроцессорам. Часть первая: Микроконтроллеры AVR: руководство. – Казань: КГУ, 2009. – 37 с.

2. Евстифеев А.В. Микроконтроллеры AVR семейств Tiny и Mega фирмы ATMEL. – 3-е изд. – М.: Изд. дом «Додэка-XXI», 2006. – 560 с.

3. Петин В.А. Проекты с использованием контроллера Arduino. – СПб.: БХВ-Петербург, 2014. – 400 с.

4. Деменков Н.П. Языки программирования промышленных контроллеров: учеб. пособие / под ред. К.А. Пупкова. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 172 с.

5. IEC 61131-3:2013 | IEC Webstore | water automation, water management, smart city [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/publication/4552, свободный (дата обращения: 08.05.2018).

6. Мараховский В.Б. Моделирование параллельных процессов. Сети Петри. Курс для системных архитекторов, программистов, системных аналитиков, проектировщиков сложных систем управления / В.Б. Мараховский, Л.Я. Розенблюм, А.В. Яковлев. – СПб.: Профессиональная литература, АйТи-Подготовка, 2014. – 400 с.

7. Петров И.В. Программируемые контроллеры. Стандартные языки и приёмы прикладного программирования / под ред. В.П. Дьяконова. – М.: СОЛОН-Пресс, 2004. – 256 с.

8. Home – CODESYS [Электронный ресурс]. – Режим доступа: https://www.codesys.com/, свободный (дата обращения: 03.05.2018).

9. ISaGRAF – leading IEC 61131 and IEC 61499 software [Электронный ресурс]. – Режим доступа: http://www.isagraf.com/index.htm, свободный (дата обращения: 03.05.2018).

10. Мальцев Ю.И. Язык управления механизмами X-Robot // Электронные средства и системы управления. – Томск: ТУСУР, 2013. – № 2. – С. 114–118.

11. МАРС – среда моделирования технических устройств и систем / В.М. Дмитриев, А.В. Шутенков, Т.Н. Зайченко, Т.В. Ганджа. – Томск: В-Спектр, 2011. – 278 с.

12. Дмитриев В.М. Среда моделирования сценариев для прототипирования контроллеров / В.М. Дмитриев, Т.В. Ганджа, А.С. Букреев // Научная сессия ТУСУР–2017: матер. Междунар. науч.-техн. конф. студентов, аспирантов и молодых ученых, посвященной 55-летию ТУСУРа, Томск: 10–12 мая 2017 г.: в 8 ч. – Томск: В-Спектр, 2017. – Ч. 4. – С. 107–110.

13. Среда многоуровневого компьютерного моделирования химико-технологических систем / В.М. Дмитриев, Т.В. Ганджа. – Томск: Изд-во Том. ун-та, 2017. – 332 с.

14. СВИП – система виртуальных инструментов и приборов / В.М. Дмитриев, Т.В. Ганджа, В.В. Ганджа, Ю.И. Мальцев. – Томск: В-Спектр, 2014. – 216 с.

15. Дмитриев В.М. Система визуализации и управления вычислительным экспериментом в среде многоуровневого моделирования МАРС / В.М. Дмитриев, Т.В. Ганджа, Т.Ю. Коротина // Доклады ТУСУР. – 2010. – № 1 (21), ч. 2. – С. 149–155.

16. Дмитриев В.М. Принцип формирования многоуровневых компьютерных моделей SCADA-систем для управления сложными технологическими объектами / В.М. Дмитриев, Т.В. Ганджа // Информатика и системы управления. – 2013. – № 2 (36). – С. 24–35.

17. Автоматизация моделирования промышленных роботов / В.М. Дмитриев, Л.А. Арайс, А.В. Шутенков. – М.: Машиностроение, 1995. – 304 с.

18. Дмитриев В.М. Архитектура универсального вычислительного ядра для реализации виртуальных лабораторий / В.М. Дмитриев, А.В. Шутенков, Т.В. Ганджа // Приборы и системы. Управление. Контроль. Диагностика. – 2004. – № 2. – С. 24–28.

19. Григорьева Т.Е. Дискретно-событийное моделирование в СМ МАРС для курса «Системы массового обслуживания» // Доклады ТУСУР. – 2014. – № 1 (31). – С. 152–155.

20. Дмитриев В.М. Компьютерное моделирование визуальных интерфейсов виртуальных инструментов и приборов / В.М. Дмитриев, Т.В. Ганджа, В.В. Ганджа, А.С. Панов // Научная визуализация. – 2016. – Т. 8, № 3. – С. 111–131.

21. Дмитриев В.М. Система виртуальных инструментов и приборов для автоматизации учебных и научных экспериментов / В.М. Дмитриев, Т.В. Ганджа, С.А. Панов // Программные продукты и системы / Sortware & System. – 2016. – Т. 29, № 3. – С. 154–162.

Дмитриев Вячеслав Михайлович
Профессор кафедры компьютерных систем
в управлении и проектировании (КСУП) ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-913-867-01-56
Эл. почта: dmitriewvm@gmail.com

Ганджа Тарас Викторович
Доцент каф. КСУП ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID: 0000-0002-4996-8114
Тел.: +7-913-846-11-77
Эл. почта: gandgatv@gmail.com

Букреев Александр Сергеевич
Аспирант каф. КСУП ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-960-978-86-68
Эл. почта: alexander.eleventh@gmail.com

Dmritriev V.M., Gandzha T.V., Bukreev A.S.

Modeling scenarios to control dynamic objects based on the graphical language X-Robot

As the number of function of dynamic object increases, the algorithm that controls devices becomes more complex. Also, programs written in low-level programming languages of controllers are increasing, that complicates the process of their debugging. The urgency of the development of new means for the formation and modeling of controller operation scenarios is due to the need to take into account many observable variables and the use of a number of control action, but also determined by the non trivial character of the algorithms to operate controllers.

The article discusses the principles of modeling scenarios to control dynamic objects with the use of graphical notations of X-Robot language. In addition to the traditional text representation of a program called a script, a graphic interpretation has been proposed and developed for this language, setting a certain component for its commands. Graphical scenario formation is carried out in the environment of computer simulation MARS at the logical level of a multi-level computer model, at the object level of which the models of a controlled dynamic object are located with the models of executive and measuring devices included in it. This opens up the possibility of forming control scenarios in a graphical form and their preliminary debugging on the model of a dynamic object. At the visual level of the multi-level computer model, control components are located, through which the user has the opportunity to influence the model of the object and the scenario model, as well as the visualization components that display the visualization data for the user, which can be either the values of the observed object variables, or and their generalized parameter-functionals. At present, the developed graphical language for modeling scenarios is adapted to the X-Mega controller, but studies are underway to develop it and apply it to other types of controllers.

Keywords: component, controller, scenario, dynamic object, multilevel computer model
doi: 10.21293/1818-0442-2018-21-2-75-82

References

1. Gumerov R.I. *Praktikum po nicroprocessoram. Chast' pervaja: microcontrollery AVR. Rukovodstvo.* [Workshop on microprocessors. Part one: microcontrollers AVR. Management]. Kazan': KGU, 2009. 37 p.

2. Evstifeev A.V. *Microcontrollery AVR semeystva Tiny I Mega firmy ATMEL* [Microcontrollers AVR families Tiny and Mega firm ATMEL]. 3-e izd. M.: Izdatel'skiy dom «Dodeka-XXI», 2006. 560 p.

3. Petin V.A. *Proecty s ispol'zovaniem kontrollera Arduino* [Projects using the Arduino controller]. BHV-Peterburg, 2014. 400 p.

4. Demenkov N.P. *Jazyki programmirovaniya promyshlennyh controllerov: Uchebnoe posobie* [Programming languages for industrial controllers: Tutorial]. Pod red. K.A. Pupkova. M.: Izd-vo MGTU im. N.E. Baumana publ., 2004. 172 p.

5. IEC 61131-3:2013 | IEC Webstore | water automation, water management, smart city. Available at: https://webstore.iec.ch/publication/4552 (accessed: 08 May 2018).

6. Marahovskiy V.B., Rozenblyum, A.V. Yakovlev. *Modelirovanie parallel'nyh processov. Seti Petri. Kurs dlja sistemnyh arhitektorov, programmistov, sistemnyh analitikov, proektirovschikov sloghnyh sistem* [Simulation of parallel processes. Petri net. Course for system architects, programmers, system analystsm designers of complex control systems]. SPb.: Professional'naja literatura, IT-Podgotovka publ., 2014. 400 p. (In Russ.).

7. Petrov I.V. *Programmiruemye kontrollery. Standartnye jazyki i prioemy prikladnogo programmirovanija* [Programmable controllers. Standart languages and application programming techniques]. Pod. red. V.P. Djakonova. M.: SOLON-Press, 2004. 256 p. (In Russ.).

8. Home – CODESYS. Available at https://www.codesys.com/ (accessed: 03 May 2018).

9. ISaGRAF – leading IEC 61131 and IEC 61499 software. Available at http://www.isagraf.com/index.htm (accesses: 03.05.2018).

10. Maltsev Yu.I. *Yasyk upravlenia mehanizmami X-Robot* [Language to control of mechanisms X-Robot] // Elektronnye sredstva i systemy upravlenija. Tomsk, Tomsk state university of control system and radioelectroniks. 2013, no. 2, pp. 114–118.

11. Dmitriev V.M., Shutenkov A.V., Zaychenko T.N., Gandzha T.V. *MARS – sreda modelirovanija technicheskih ustroystv i system* [MARS – modeling environment of technical devices and systems]. Tomsk, V-Spectr, 2011. 278 p. (In Russ).

12. Dmitriev V.M., Gandzha T.V., Bukreev A.S. Sreda modelirovanija scenariev dlja prototipirovanija kontrollerov [Scenario modeling environment for prototyping controllers]. Nauchnaja sessija TUSUR-2017. Materialy Mejdunarodnoy nauchno-technicheskoy konferenzii studentov, aspirantov i molodiy uchenih, posvjaschemmoy 55-letiju TUSURa [*Scientific session of TUSUR-2017: materials of the International scientific and technical conference of students, graduate students and young scientists dedicated to the 55th annicersary of TUSUR*], Tomsk. 10–12 May 2017: in 8 parts. Tomsk.: V-Spectr publ., 2017, part 4, pp. 107–110.

13. Dmitriev V.M., Gandzha T.V. *Sreda mnogourovnevogo komputernogo modelirovanija himiko-tehnologicheskiy system* [Multilevel computer modeling of chemical-technological systems]. Tomsk, Izd-vo Tom. un-ta, 2017, 332 pp.

14. Dmitriev V.M., Gandzha T.V., Gandzha V.V., Maltsev Yu.I. *SVIP – sistema virtual'nyh instrumentov i priborov* [SVIP – system of virtual instruments and devices]. Tomsk, V-Spectr, 2014, 216 p.

15. Dmitriev V.M., Gandzha T.V., Korotina T.Y. System for visualization and control of computational experi-

ments in the environment of multilevel modeling. *Reports of TUSUR,* 2010, no. 1 (21), part. 2, pp. 149–155.

16. Dmitriev V.M. Gandzha T.V. Principe of formation of multilevel computer models of SCADA-systems for the control of complex technological objects. *Informatics and control systems*, 2013, no. 2 (36), pp. 24–35.

17. Dmitriev V.M. Shutenkov A.V. Arays L.A. *Avtomatizatiya modelirovaniya promyshlennyh robotov* [Automation of simulation of industrial robots]. M.: Mashinostroenie, 1995. 304 p. (In Russ.).

18. Dmitriev V.M., Shutenkov A.V., Gandzha T.V. The architecture of a universal computing kernel for the implementation of virtual laboratories. *Instruments and systems. Management. Conrol, Diagnostic*, 2004, no. 2, pp. 24–28.

19. Grigorieva T.E. Discrete-event modeling in the simulate environment MARS. *Proceedings of TUSUR University,* 2014, no. 1 (31), pp. 152–155.

20. Dmitriev V.M., Gandzha T.V., Gamdzha V.V., Panov S.A. Computer simulate of the visual interface in virtual instruments and devices. *Scientific Visualization*, 2016, vol. 8, no. 3, pp. 111–131.

21. Dmitriev V.M., Gandzha T.V., S.A. Panov. System of virtual instruments and devices for automation of education and scientific experiments. *Software & System*, 2016, vol. 29, no. 3, pp. 154–162.

Vjacheslav M. Dmritriev
Doctor of Engineering Sciences, professor,
Department of Computer Control and Design Systems,
Tomsk State University of Control Systems
and Radioelectronics
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7-913-867-01-56
Email: dmitriewvm@gmail.com

Taras V. Gandzha
Doctor of Engineering Sciences, Assistant Professor,
Department of Computer Control and Design Systems,
Tomsk State University of Control Systems
and Radioelectronics
40, Lenina pr., Tomsk, Russia, 634050
ORCID 0000-0003-4996-8114
Phone: +7-913-846-11-77
Email: gandgatv@gmail.com

Alexandr A. Bukreev
PhD student Department of Computer Control and Design Systems, Tomsk State University of Control Systems
and Radioelectronics
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7-960-978 86-68
Email: alexander.eleventh@gmail.com

УДК 65.012.123

М.Ю. Катаев, Н.В. Лосева, Л.А. Булышева

Структура информационной рекомендательной системы поддержки принятия решений при оказании услуг государственным учреждением

Рассматривается построение информационной рекомендательной системы для целей поддержки принятия решений государственным учреждением при оказании услуг. В процессе оказания услуг возникает масса ситуаций, которые заставляют руководящий состав искать соответствующие решения. Возникающие ситуации связаны с изменениями внутренней или внешней среды учреждения, что создает большое множество возможных вариантов при поиске решения. В настоящий момент поддержки принятия решений не существует, и руководитель принимает решения относительно его знаний и опыта. Учет цифровой формы описания текущих процессов учреждения позволяет строить различного рода информационные системы. Современной формой развития информационных систем являются рекомендательные системы. В работе предлагается анализировать цифровые показатели процессов оказания услуг и на этой основе построить рекомендательную систему поддержки принятия решений руководителя государственного учреждения.

Ключевые слова: информационная система, поддержка принятия решений, рекомендательная система.
doi: 10.21293/1818-0442-2018-21-2-83-87

Успешная деятельность организации зависит от формы управления, качества и скорости принимаемых решений. В этом плане перешедшая к нам из прошлого функциональная система управления не отвечает существующим реалиям, поскольку не позволяет эффективно внедрять информационные системы [1]. Последнему факту мешает вертикальная структура управления (разделение задач сверху, отсутствие видимости общего результата конкретным исполнителем), которая является эффективной лишь при определенных обстоятельствах (талант руководителя, подбор кадров и др.). В современных условиях более гибкой и удобной является процессно-ориентированная форма управления предприятием, основанная на бизнес-процессах [2]. При этом бизнес-процессы предприятия можно постоянно модифицировать, получая заданный уровень оптимизации.

Внедрение в организации процессного подхода в управлении позволяет повысить эффективность процессов деятельности и контроля, так как позволяет оценивать, управлять и контролировать каждый отдельный элемент процесса (подпроцессы или функции). Совершенствование методов управления является одной из основных задач, от решения которой зависят качество и эффективность деятельности учреждения. С появлением новых поколений цифровой техники и информационных систем неизбежно растет и усложняется интенсивность обмена информацией между подразделениями организации, в связи с чем большую актуальность приобретает проблема создания методов описания, анализа и исследования потоков информации, обусловленных функционированием бизнес-процессов, для целей управления. Возникающие потоки информации необходимо не только измерять, обрабатывать, но и скорейшим образом анализировать для решения насущных задач предприятия.

В настоящее время имеется множество приложений, основанных на процессном подходе и решающих задачи документооборота и ведения хозяйственной деятельности, однако для решения задач управленческого уровня подобных систем практически нет. Одной из причин такого дефицита является качественная сторона управленческой деятельности.

Особое внимание в последнее время уделяется цифровой форме деятельности государственных учреждений при оказании разнообразных услуг. Для этих целей разработана программа «Цифровая экономика Российской Федерации», которая была утверждена распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р. Нами предлагается ввести в процесс управления количественные данные, а именно временные показатели бизнес-процессов, и на этой основе построить новый тип информационной рекомендательной системы.

Постановка задачи

В настоящее время основные векторы развития российской экономики представлены в концепции «Цифровая экономика». Однако в этих документах не указаны способы реализации, типы моделей цифрового представления различных элементов экономики. Одним из векторов развития является управленческая деятельность, которая должна более опираться не на субъективные выводы и решения, пусть и основанные на знаниях, а на информационные модели и количественное представление деятельности. В настоящее время существуют подходы и информационные системы управления организациями, которые опираются на концепции управления результативностью бизнеса (CPM, Corporate Performance Management). Однако постепенный перевод организаций на количественное описание процесса деятельности привел к значительному росту объемов информации на оперативном уровне. Это обстоятельство, в свою очередь, привело к тому, что процесс управления на более высоких уровнях (тактическом и стратегическом) стал информационно разорван. Возникла проблема управления в режиме реального времени

(RTE, Real Time Enterprise). Другая проблема связана с тем, что возникла сложность усвоения потока информации для принятия правильных управленческих решений.

Описание деятельности в виде бизнес-процессов заставляет предприятия переходить от старой функциональной формы управления к новой – процессно-ориентированной. Именно для организаций, перешедших на процессный уровень управления, концепции CPM являются наиболее эффективными. Описание деятельности в виде бизнес-процессов позволяет более строго организовать переход к цифровой форме управления.

Традиционно непрерывный цикл управления основывается на четырех элементах: анализ, моделирование, планирование и мониторинг. Под понятием «мониторинг» будем понимать систематизированный сбор и первичную обработку поступившей информации. Применение мониторинга в целях управления необходимо для решения производственных и экономических задач, а также для улучшения процесса принятия решений. Мониторинг позволяет связать различные уровни управления и производственные процессы в целях достижения определенного (заданного) уровня качества результатов производства. Проведение мониторинга подразумевает высокий уровень информатизации деятельности организации (накопление, анализ, моделирование, планирование). Моделирование и планирование текущего процесса деятельности организации возможно лишь при наличии большого количества данных, полученных с помощью системы мониторинга. На основе анализа этих данных возможно построение разнообразных моделей деятельности организации [3–6].

Существует ряд математических подходов описания процессов деятельности: имитационные модели, событийно управляемые процессы, метод Монте-Карло, метод диаграмм активности, семантическая модель и др. Однако на практике эти модели достаточно сложно использовать, так как они являются вероятностными, требуют значительных вычислительных ресурсов, наличия на предприятии соответствующих специалистов, а также понимания и трансформации полученных результатов.

Отметим, что для эффективной деятельности организации роль аналитических подходов к оценке деятельности и получения своевременных, точных управленческих решений весьма высока. В процессе управления даже при цифровой форме представления результатов деятельности нельзя исключать опыт руководителя. Поэтому зачастую возникает дисбаланс между объемом имеющейся информации и субъективизмом, знаниями и опытом руководителя. Имеющиеся в настоящее время информационные системы из класса CRM (Customer Relationship Management, управление отношениями с заказчиками), ERP-систем (Enterprise Resource Planning, управление корпоративными ресурсами) или MRP-систем (Materials Requirements Planning, планирование материалов для производства) позволяют осуществить сбор, интеграцию, анализ разнообразных данных. Однако возникающий объем данных затрудняет понимание текущей информации, удлиняет процесс формирования решений. Поэтому возникает насущная необходимость в поиске решений, позволяющих руководителям получать некоторые рекомендации, связанные с принятием тех или иных решений.

Государственные услуги

Деятельность Правительства Российской Федерации и федеральных органов исполнительной власти направлена на разработку правил предоставления гражданам и организациям государственных услуг (результатов исполнения государственных функций). Немаловажным фактором является оптимизация процесса оказания государственных услуг, связанная, в большей мере, со снижением потерь времени при взаимодействии граждан и организаций с органами исполнительной власти. Процесс оказания государственных услуг регулирует Федеральный закон № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 г. Этот закон описывает общие требования к предоставлению государственных и муниципальных услуг, административные регламенты, организацию предоставления государственных и муниципальных услуг в многофункциональных центрах и использование информационно-телекоммуникационных технологий при предоставлении государственных и муниципальных услуг. Оптимизация процесса оказания услуг связана с анализом результатов их мониторинга для государственных учреждений, реализуемого в форме опросов, интервью или анкетирования получателей государственных услуг. Такой вид мониторинга является внешним по отношению к государственному учреждению, предоставляющему услугу. Внутренние аспекты мониторинга процесса предоставления услуг, необходимые для оптимизации и решения конкретных текущих задач, решаются непосредственно руководителем.

Рекомендательные системы

В литературе рекомендательные системы (РС) определяются как информационные системы, разрабатываемые для автоматизации процесса поддержки принятия решений. В настоящее время такие системы в основном используются для оценки интереса пользователей сети Интернет к определенному продукту или сервису. Основой для РС является информация, которую пользователи оставляют при использовании различных онлайн-сервисов (частота посещения сайта, выбор того или иного продукта и др.) [7–10].

Рекомендательные системы стали развиваться достаточно давно и первое время опирались на информацию, которая собиралась в базу данных из различных источников. С развитием возможностей Интернета рекомендательные системы стали неотъемлемой частью крупных компаний Google, Netflix, Amazon и др. Подходы, используемые для оценки интереса потребителей, основываются на фильтрации содержания (content-based information filtering) или коллаборативной фильтрации (collaborative filtering).

В первом случае в информационной системе (как правило, интернет-сайт), где имеется информация о пользователях, изучается зависимость характеристик пользователя (возраст, пол и др.) от его потребительских предпочтений. Во втором случае изучается и классифицируется информация о перечне покупок, оценках продуктов, которые сделал ранее пользователь. Реже применяются на практике подходы: интеллектуальные (knowledge-based), при которых оценка вычисляется на основе формализованных знаний (онтологии), и гибридные (hybrid prediction) методы, в основе которых лежат комбинации ранее представленных подходов.

Основной целью РС является нахождение такой оценки событий из анализа предшествующих предпочтений различных групп пользователей, которая позволила бы определить прогнозное значение. Для целей прогнозирования применяются различные группы методов: 1) расчет функции полезности и исследование ее поведения в зависимости от времени дня, времени года, характеристик групп пользователей и др., 2) построение эмпирических зависимостей и исследование их поведения. В результате пользователь получает в качестве рекомендации, например, своевременное извещение о наличии того или иного продукта, времени скидок и др. Возможно применение и таких подходов, как Байесовский классификатор, методы искусственного интеллекта (кластеризация, деревья решений, искусственные нейронные сети и др.). Однако результат для пользователя будет аналогичен.

Типовая структура информационной системы для реализации рекомендательных систем представлена на рис. 1.

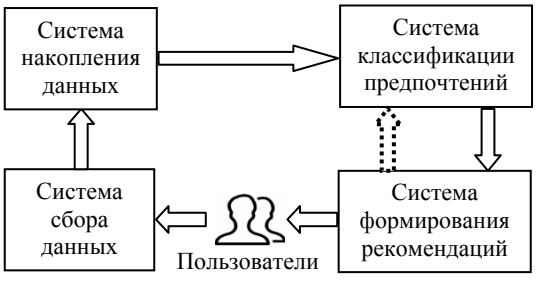


Рис. 1. Типовая структура информационной системы рекомендательных систем

Описание разрабатываемой информационной рекомендательной системы

Основные требования к информационным технологиям в области оказания государственных услуг изложены в Федеральной целевой программе «Электронная Россия (2002–2020)» [http://base.garant.ru/184120/]. Цель этой программы связана с формированием инфраструктуры электронного правительства для повышения оперативности и качества взаимодействия государства и граждан. Электронное правительство представляет собой комплекс технологически связанных между собой государственных информационных систем, обеспечивающих возможности взаимодействия с государством 24 часа в день, в режиме самообслуживания. Результатом действия этой программы стали интернет-порталы министерств и субъектов РФ, а также Единый портал государственных услуг (ЕПГУ) [https://www.gosuslugi.ru].

Математическая модель деятельности государственного учреждения, оказывающего услуги, опирается на функции тактического уровня, так как детальная информация, возникающая на оперативном уровне, приводит к значительному количеству случайных данных. В основу описания поведения бизнес-процесса во времени положена аддитивная временная модель [11, 12]. Модель бизнес-процесса при оказании услуг в государственном учреждении может быть представлена набором параметров:

$$BP = < T, I >, \quad (1)$$

где T – заданное, регламентное время выполнения того или иного бизнес-процесса BP; I – множество информации, необходимой для реализации бизнес-процесса.

Время, затрачиваемое клиентом на получение услуги, является одной из главных составляющих качества работы государственного учреждения. Однако это время не поддается автоматизированной фиксации и последующему анализу. Поэтому основой оценки качества получаемой клиентом услуги, возможной для автоматизированной фиксации, является время работы специалиста в специализированных информационных системах. Таким образом, время, которое фиксируется в информационной системе при оказании услуги (тип услуги, начало и конец бизнес-процесса), можно использовать в целях анализа и последующего принятия управленческих решений.

Временную модель процесса оказания услуги в государственном учреждении можно представить с точки зрения анализа рабочего времени отдельного специалиста:

$$T(k) = \sum_{l=1}^{L} t_{\text{отд}}(l,k) + \sum_{p=1}^{P} t_{\text{пор}}(p,k) + \sum_{i=1}^{N}\sum_{j=1}^{M} t_{\text{бп}}(i,j,k), \quad (2)$$

где $t_{\text{отд}}(l,\ k)$ – время работы k-го специалиста, не связанное с выполнением бизнес-процесса; ($l = 1, L$) – число отрезков в течение рабочего времени; $t_{\text{пор}}(p,\ k)$ – время на исполнение k-м специалистом поручений от руководства типа ($p = 1,\ P$); $t_{\text{бп}}(i,\ j,\ k)$ – время оказания i-му клиенту ($i = 1, N$) j-й госу-дарственной услуги ($j = 1, M$) k-м специалистом.

Выражение (2) позволяет максимально полно учесть все отдельные подпроцессы, возникающее в течение рабочего времени при оказании услуг в государственном учреждении.

На рис. 2 представлена структура рекомендательной системы, которая позволяет на основе данных процесса деятельности организации [см. выражение (2)] формировать рекомендательные решения для лица, принимающего решения тактического уровня.

Именно особенность, связанная с измерением времени оказания услуги (бизнес-процесса), позволя-

ет оценить отклонения от некоторого заданного (регламентного) времени выполнения бизнес-процесса в зависимости от возможных воздействий внешней и внутренней среды или квалификации специалиста [13–15]. Контроль этих отклонений позволяет оценить работу как отдельного специалиста, так и подразделения в целом. Единичные случаи сбоя (отклонений, превышающих заданную величину), конечно, не должны вызывать опасений у руководящего состава, в то же время регулярно повторяющиеся случаи сбоя требуют более пристального внимания. В настоящее время контроль таких ситуаций не осуществляется.

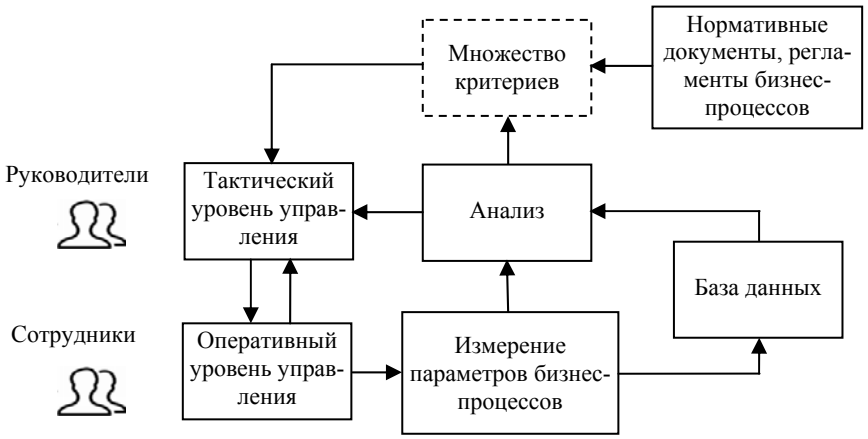


Рис. 2. Структура рекомендательной системы

Учитывая этот факт, нами предлагается рекомендательная система, структура которой показана на рис. 2. На оперативном уровне происходит измерение времени начала и завершения того или иного бизнес-процесса в течение рабочего времени (например, 8.30–17.30). Располагая такой информацией, можно провести анализ с помощью простых критериев (например, отклонение от регламентного времени, суммарное время поручений, не связанных с бизнес-процессами, и суммарное время, непосредственно затраченное на бизнес-процессы), которые позволяют оценить знак и величину отклонений времени выполнения бизнес-процесса данного типа от заданного. Такие измерения регулярно заносятся в базу данных. На основе критериев, которые ранжируют полученные отклонения по величине, типу, знаку, полученная информация соотносится с показателями, которые определяются на основе нормативных документов и регламентов бизнес-процессов. В итоге описанных действий получается набор типовых решений для выбранных ситуаций.

Заключение

В работе представлено описание нового, развивающегося направления «Рекомендательные системы». Показывается, что идею подходов, которые реализуются в этом направлении, можно переориентировать на задачи управления в информационных системах поддержки принятия решений в государственных учреждениях. Предложена структура информационной рекомендательной системы, которая призвана автоматизировать процесс подготовки принятия решений. Данный подход хорошо сочетается с основными направлениями «Цифровой экономики». Важной особенностью предлагаемой структуры является возможность постоянного дополнения системы новыми знаниями и совершенствования ранее используемых знаний. Поэтому данное направление позволяет, в итоге, перейти к построению полноценной информационно-аналитической системы управления организацией.

Литература

1. Белов В.С. Информационно-аналитические системы. Основы проектирования и применения. – М.: Моск. гос. ун-т экономики, статистики и информатики, 2005. – 111 с.

2. Пейн Э. Руководство по CRM: путь к совершенствованию менеджмента клиентов. – М.: Гревцов Паблишер, 2007. – 255 с.

3. Шуремов Е.Л. Информационные системы управления предприятиями / Е.Л. Шуремов, Д.В. Чистов, Г.В. Лямова. – М.: Бухгалтерский учет, 2006. – 109 с.

4. Репин В.В. Процессный подход к управлению / В.В. Репин, В.Г. Елиферов. – М.: РИА «Стандарты и качество», 2004. – 408 с.

5. Романов В.П. Интеллектуальные информационные системы в экономике. – М.: Экзамен, 2003. – 494 с.

6. О'Лири Д. ERP-системы: выбор, внедрение, эксплуатация. Современное планирование и управление ресурсами предприятия. – М.: Вершина, 2004. – 272 с.

7. Deshpande M. Item-Based Top-N Recommendation Algorithms. / M. Deshpande, G. Karypis // ACM Trans. Information Systems. – 2004. – Vol. 22, No. 1. – PP. 143–177

8. Desrosiers C. Comprehensive survey of neighborhood-based recommendation methods / C. Desrosiers, G.A. Karypis // Recommender systems handbook. – Springer, 2011. – PP. 107–144.

9. Adomavicius G. Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions / G. Adomavicius, A. Tuzhilin // IEEE Transactions on Knowledge and Data Engineering. – 2005. – Vol. 17, No. 6. – PP. 734–749

10. Дьяконов А.Г. Алгоритмы для рекомендательной системы: технология LENKOR / А.Г. Дьяконов // Бизнес-Информатика. – 2012. – Т. 1, № 19. – С. 32–39.

11. Катаев М.Ю. Модель оценки эффективности тактического планирования на предприятии с процессно-ориентированным подходом к управлению / М.Ю. Катаев, А.А. Емельяненко // Управление экономическими системами. – 2013. – № 58. – С. 31–42.

12. Катаев М.Ю. Влияние внешней и внутренней среды на принятие решений государственного учреждения / М.Ю. Катаев, L.A. Bulysheva, Li Da Xu, Н.В. Лосева // 22-я Междунар. науч.-практ. конф., 10–11 октября 2016. – Томск: В-Спектр. – 2016. – С. 50–54.

13. Дмитриев О.Н. Системный анализ в управлении / О.Н. Дмитриев. – М.: Гном и Д, 2002. – 182 с.

14. Медведев В.П. Основы менеджмента. – М.: Дека, 2002. – 840 с.

15. Боронина Л.Н. Основы управления проектами / Л.Н. Боронина, З.В. Сенук. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 112 с.

Катаев Михаил Юрьевич
Д-р техн. наук, профессор каф. автоматизированных систем управления (АСУ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
профессор Юргинского технологического института, филиала Национального исследовательского Томского политехнического университета
Тел.: (382-2) 70-15-36, +7-960-975-27-85
Эл. почта: kmy@asu.tusur.ru

Лосева Наталья Валерьевна
Специалист Фонда социального страхования, г. Томск
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: (382-2) 70-15-36
Эл. почта: lonat@bk.com

Булышева Лариса Андреевна
Канд. техн. наук, доцент каф. информационных технологий и принятия решений Олд Доминион Университета, США
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: (382-2) 70-15-36
Эл. почта: lbulyshe@odu.edu

Kataev M.Yu., Loseva N.V., Bulysheva L.A.

Structure of an information recommendation system to support decision-making of the state institution

The article deals with the construction of an information advisory system for the purposes of supporting the decision-making of a government agency when providing services. In the process of providing public services, a lot of situations arise that force the management to seek appropriate solutions. Some of the emerging situations are repeated, although with a variety of conditions, which creates a large number of possible options when searching for the right solution. To solve this problem, it becomes possible to use the ideas of information advisory systems.

Keywords: information system, decision support, recommendation system.
doi: 10.21293/1818-0442-2018-21-2-83-87

References

1. Belov V.S. *Informational and analytical systems. Basics of design and application*. Moscow: Moscow State University of Economics, Statistics and Informatics, 2005, 111 p. (in Russ.).

2. Payne E. *A Guide to CRM: a way to improve the management of clients*. Moscow, Grevtsov Pablisher, 2007. 255 p. (in Russ.).

3. Shurimov E.L. *Information systems for enterprise management* / E.L. Shuremov, D.V. Chistov, G.V. Lyamova. Moscow, Accounting, 2006. 109 p.

4. Repin V.V. *Process approach to management* / V.V. Repin, V.G. Elifera. Moscow, RIA «Standards and Quality», 2004. 408 p. (in Russ.)

5. Romanov V.P. *Intellectual information systems in the economy*. Moscow, Examination, 2003. 494 p. (in Russ.)

6. O'Leary D. ERP-systems: choice, implementation, exploitation. Modern planning and management of enterprise resources. Moscow, Vershina, 2004. 272 p. (in Russ.)

7. Deshpande M. Item-Based Top-N Recommendation Algorithms. / M. Deshpande, G. Karypis // *ACM Trans. Information Systems*, 2004, vol.22, no. 1, pp. 143–177.

8. Desrosiers C. *Comprehensive survey of neighborhoodbased recommendation methods*. C. Desrosiers, G.A. Karypis // Recommender systems handbook, Springer, 2011, pp. 107–144.

9. Adomavicius G. Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions / G. Adomavicius, A. Tuzhilin // *IEEE Transactions on Knowledge and Data Engineering*, 2005, vol. 17, no. 6, pp. 734–749.

10. Dyakonov A.G. «Algorithms for the recommendation system: LENKOR technology» / A.G. Dyakonov // *Business-Informatics*, 2012, vol. 1, no. 19, pp. 32–39 (in Russ.).

11. Kataev M.Yu. Model for assessing the effectiveness of tactical planning in an enterprise with a process-oriented approach to management / M.Yu. Kataev, A.A. Emelianenko. // *Management of economic systems*, 2013, no. 58, pp. 31–42 (in Russ.)

12. Kataev M.Yu. *The influence of the external and internal environment on the decision-making of the state institution* / M.Yu. Kataev, L.A. Bulysheva, Li Da Xu, N.V. Loseva // 22 International Scientific and Practical Conference, October 10–11, 2016, Tomsk, V-Spectrum, 2016, pp. 50–54. (in Russ.)

13. Dmitriev O.N. *System analysis in management* / O.N. Dmitriev. Moscow, Publishing house «Gnome and D», 2002. 182 p. (in Russ.).

14. Medvedev V.P. *Fundamentals of management*. Moscow, Deca, 2002. 840 p. (in Russ.).

15. Boronina L.N. *Fundamentals of Project Management* / L.N. Boronina, Z.V. Senuk. Ekaterinburg, Publishing house Ural. University, 2015, 112 p. (in Russ.).

Mikhail Yu. Kataev
Doctor of Engineering Sciences, Professor of the Department. Automated Control Systems (ACS) of the Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Professor of the Yurginsky Technological Institute, a branch of the National Research Tomsk Polytechnic University
Phone: (382-2) 70-15-36, +7-960-975-27-85
Email: kmy@asu.tusur.ru

Natalya V. Loseva
Specialist of the social insurance fund, Tomsk
40, Lenina pr., Tomsk, Russia, 634050
Phone: (382-2) 70-15-36
Email: lonat@bk.com

Larisa A. Bulysheva
Candidate of Engineering Sciences, Associate Professor, Chair of Information Technologies and Decision Making Old Dominion University, USA
40, Lenina pr., Tomsk, Russia, 634050
Phone: (382-2) 70-15-36
Email: lbulyshe@odu.edu

УДК 004.056:519.1

О.С. Авсентьев, Д.А. Гудков

Исследование характеристик акустооптического канала утечки речевой информации в условиях реализации механизмов защиты

Определяются динамические характеристики реализации процессов передачи речевой информации от источника к ее получателю, а также перехвата этой информации злоумышленником по акустооптическому каналу утечки. Формализуются вероятности корректности согласования данных характеристик на каждом этапе смены материального носителя информационного речевого сигнала в условиях использования средств защиты информации от утечки по каналам рассматриваемого типа.

Ключевые слова: речевая информация, акустооптический канал утечки речевой информации, лазерные акустические локационные системы, электрические характеристики канала связи, условия согласования характеристик сигналов и канала связи, корректность согласования, вероятность утечки речевой информации.
doi: 10.21293/1818-0442-2018-21-2-88-94

Деятельность правоохранительных органов по всем направлениям [1] предусматривает использование информации в различных формах ее представления. В процессе осуществления возложенных на органы внутренних дел (ОВД) задач, широко используется речевая информация (РИ). Это обусловлено естественностью процессов приема и передачи РИ для человека, а также рядом важных для решаемых задач свойств информации, характерных для данной формы ее представления: оперативностью, аутентичностью, разборчивостью, своевременностью и др. [2].

Информационный обмен в данном случае может осуществляться в различных условиях:

– в помещениях, выделенных для проведения конфиденциальных переговоров (выделенных помещениях (ВП));

– в служебных кабинетах, в которых расположены различные технические средства и системы, как предназначенные для обработки конфиденциальной информации, например терминалы и периферийные устройства инфокоммуникационных систем (ИКС), так и не предназначенные для этих целей (различного рода вспомогательные технические средства и системы (ВТСС) [3].

Исполнение поставленных задач перед ОВД сопряжено с передачей, получением, обработкой и хранением информации ограниченного доступа. Для этих целей также используется речевая форма представления такого рода информации. Это определяет высокий интерес со стороны злоумышленников к ее перехвату с объектов рассматриваемого типа.

Одним из наиболее эффективных путей перехвата такой информации является перехват по техническим каналам утечки информации (ТКУИ) [4]. Для их реализации применяются различные технические средства разведки (ТСР).

Согласно [4], одним из основных принципов ведения технической разведки (ТР) является скрытность, которая обеспечивается путем маскировки разведывательной аппаратуры, а также за счет увеличения дальности ее использования.

Одним из способов реализации этого принципа злоумышленниками при перехвате РИ является применение лазерных микрофонов в структуре лазерных акустических локационных систем (ЛАЛС). Условия их применения рассмотрены в [4–6].

Данная работа посвящена исследованию основных параметров канала передачи РИ и канала ее перехвата с использованием ЛАЛС а также условий влияющих на параметры возникающего при этом акустооптического канала (АОК) утечки.

Структурно-логическое представление информационных процессов по передаче и перехвату речевой информации

Рассмотрим информационные процессы (ИПр) по передаче РИ на объектах рассматриваемого типа, а также процессы ее перехвата (ПрПИ) при помощи ЛАЛС, представленные на рис. 1.

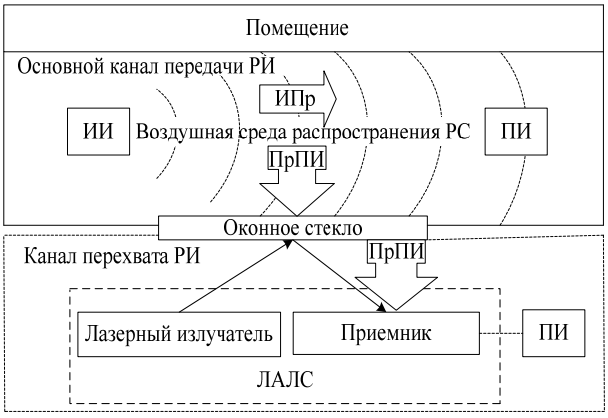


Рис. 1. Обобщенная структура процессов передачи и перехвата речевого сигнала

Основной канал передачи РИ включает источник РИ (ИИ), среду распространения и получателя РИ (ПИ).

ИИ может быть человек или устройство, воспроизводящее ранее записанную речь. В качестве материального носителя РИ выступают акустические колебания упругой среды, которые могут быть охарактеризованы множеством сигнальных (выходных) характеристик $S = \{s_x, x = 1, 2, \ldots, X\}$. В насто-

ящей работе рассмотрим следующие из них [7]: s_1 – громкость звука, зависящая от амплитуды звуковой волны (A_c); s_2 – диапазон звуковых частот (Δf_c); s_3 – время передачи речевого сигнала (РС) (Δt_c); s_o – обобщенная характеристика сигнала, определяемая как его объем (V_c).

ПИ может быть человек или звукозаписывающее устройство, которые могут быть охарактеризованы множеством входных (линейных) характеристик $R = \{r_x, x = 1, 2, \ldots, X\}$. В настоящей работе рассмотрим следующие из них [4]: r_1 – чувствительность ($\mu_{пр}$); r_2 – полоса пропускания по частоте ($\Delta f_{пр}$); r_3 – время приема РС ($\Delta t_{пр}$); r_o – обобщенная характеристика канала связи, определяемая как его емкость (пропускная способность) ($V_{кс}$).

Средой распространения звуковых колебаний между ИИ и ПИ в рассматриваемом случае является воздух. Будем считать, что характеристики РС, передаваемого по основному каналу, определяются типом ИИ, конструктивными особенностями помещения и при проектировании объекта.

В процессе распространения звуковые колебания воздействуют на различные ограждающие конструкции, в том числе стекла в оконных рамах, или другие отражающие поверхности (ОП). В результате такого рода воздействий возникают вибрации ОП, обуславливающие образование побочных информационных РС, а реализация ПрПИ осуществляется при помощи ЛАЛС. Эти вибрации модулируют лазерное узконаправленное излучение, которое после отражения принимается злоумышленником при помощи оптического разведывательного приемника. ПИ в канале перехвата РИ может быть человек или звукозаписывающее устройство, обладающие аналогичными характеристиками, что и ПИ основного канала передачи РИ.

Образованный таким образом АОК является составным, включающим акустический, вибрационный и оптический участки. При этом осуществляется изменение материального носителя информации: акустические колебания преобразуются в механические колебания ОП, в свою очередь, выступающей в качестве датчика информационного сигнала для ЛАЛС, где материальным носителем перехватываемой РИ являются электромагнитные колебания оптического диапазона волн.

Для обеспечения качественного информационного обмена по основному каналу передачи РИ требуется согласование между сигнальными характеристиками ИИ и линейными характеристиками ПИ [6, 7].

РС представляет собой сложный акустический сигнал, частотный диапазон которого Δf_c находится в пределах 50–12000 Гц. Основная часть энергии такого сигнала сосредоточена в области частот от 300 до 4000 Гц. Данная полоса частот считается достаточной для обеспечения приемлемой для ПИ разборчивости речи с возможностью идентификации говорящего [9, 10].

Для комфортного восприятия РС получателем информации требуется обеспечить достаточный уровень громкости речи. При этом характеристика громкости, в качестве которой рассматривается амплитуда акустических колебаний A_c определяется звуковым давлением N, создаваемым ИИ, и выражается в децибелах (дБ).

$$N = 20\lg(P/P_0), \qquad (1)$$

где P – формируемое звуковое давление; P_0 – статическое давление, при отсутствии звуковых колебаний.

Диапазон значений звукового давления N в нормальных условиях речевого обмена может изменяться от 35 до 85 дБ [9]. При значениях амплитуды РС A_c ниже минимального уровня затрудняется его восприятие ПИ. При уровне A_c выше максимального у ПИ возникает дискомфорт от излишней громкости. Средний уровень звукового давления составляет 55–75 дБ при расположении ИИ на расстоянии 1 м от ПИ [11].

Зависимость между энергетическими и частотными параметрами РС имеет сложный характер [12]. В диапазоне частот от 500 до 7000 Гц энергия частотных составляющих уменьшается примерно на 10 дБ на октаву. Поскольку под октавой понимается интервал частот, в котором соотношение между верхней и нижней частотами составляет два к одному, можно отметить более существенное уменьшение энергии речевого сигнала в низкочастотной области, чем в высокочастотной [3].

Важным свойством речи является разборчивость, под которой понимается относительное количество (в процентах) правильно понятых человеком или перехваченных (зарегистрированных) средством разведки слов или фрагментов сообщения. Данное свойство определяет достоверность принимаемой получателем РИ.

Значения весовых коэффициентов октавных частотных полос для определения разборчивости речи представлены в таблице. Из приведенных значений следует, что первая, вторая и седьмая октавные полосы являются малоинформативными. Основной вклад в разборчивость речи вносят полосы с третьей по шестую [13].

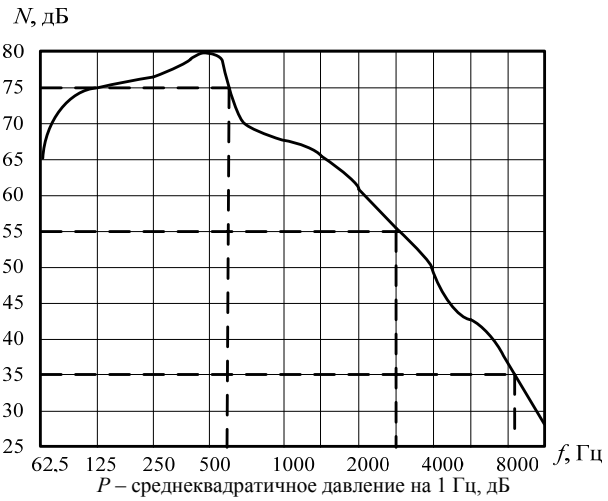
Характеристики октавных полос частотного диапазона речи

Номер полосы	Частотные границы полосы, Гц	Среднегеометрическое значение частотной полосы, Гц	Весовой коэффициент полосы
1	90…180	125	0,01
2	180…355	250	0,03
3	355…710	500	0,12
4	710…1400	1000	0,20
5	1400…2800	2000	0,30
6	2800…5600	4000	0,26
7	5600…11200	8000	0,07

Среднегеометрическое значение частотной полосы – это среднее значение частоты РС, равное квадратному корню из произведения значений нижней и верхней частотной границ полосы, используемое для удобства исследования характеристик РС.

Весовой коэффициент характеризует энергетический вклад конкретной полосы частот в формирование РС. Из таблицы следует, что диапазон частот от 355 до 5600 Гц является наиболее информативным.

Усредненный за длительный промежуток времени спектр мощности речи, измеренной на расстоянии 30 см от ИИ, представлен на рис. 2 [12]. Из этого рисунка видно, что энергетический максимум звукового давления находится в пределах 500 Гц, что соответствует частоте основного тона ИИ [14, 15].



P – среднеквадратичное давление на 1 Гц, дБ

Рис. 2. Усредненный за длительный промежуток времени спектр мощности речи, измеренной на расстоянии 30 см от ИИ

Рассмотрим взаимосвязи параметров РС с информационными параметрами ИИ и электрическими параметрами каналов передачи или перехвата РИ. Для этих целей по аналогии с [16] рассматриваемые на рис. 1 информационные процессы представим в виде, показанном на рис. 3.

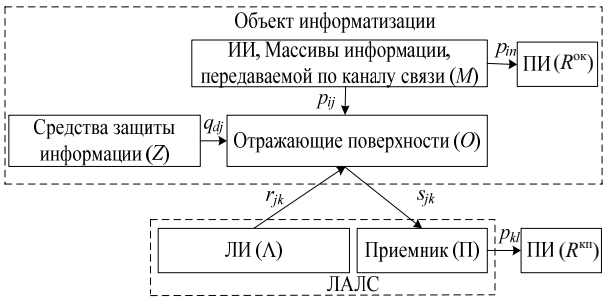


Рис. 3. Обобщённая предметно-функциональная структура взаимосвязей информационных и электрических параметров РС, АОК и СЗИ

На рис. 3 используются следующие обозначения:

$M = \{м_i,\ i = 1, 2, \ldots, I\}$ – массивы информации, передаваемой по основному каналу связи; i и I – номер массива информации и их количество соответственно;

$O = \{o_j,\ j = 1, 2, \ldots, J\}$ – ОП, преобразующие акустические колебания воздушной среды в механические колебания этой поверхности, j и J – номер ОП и их количество соответственно;

$Z = \{z_d,\ d = 1, 2, \ldots, D\}$ – средства защиты информации (СЗИ), используемые для подавления АОК; d и D – номер СЗИ и их количество соответственно;

$R^{ок} = \{ r_n^{ок},\ n = 1, 2, \ldots, N\}$ – получатели речевой информации в основном канале; n и N – номер ПИ и их количество соответственно;

$R^{кп} = \{ r_l^{кп},\ l = 1, 2, \ldots, L\}$ – получатели речевой информации в АОК (канале перехвата); l и L – номер ПИ и их количество соответственно;

ЛИ – лазерный излучатель;

$\Lambda = \{\lambda_k,\ k = 1, 2, \ldots, K\}$ – множество видов ЛИ ЛАЛС, используемых для облучения ОП; k и K – номер и количество ЛИ соответственно;

$\Pi = \{\pi_k,\ k = 1, 2, \ldots, K\}$ – множество видов приемников отраженного лазерного луча; k и K – номер и количество приемников, соответственно;

p_{in} – вероятность реализации ИПр между i-м ИИ и n-м ПИ в основном канале;

p_{ij} – вероятность реализации ПрПИ на акустовибрационном участке АОК между i-м ИИ и j-й ОП;

r_{jk} – вероятность облучения k-м ЛИ ЛАЛС j-й ОП;

s_{jk} – вероятность реализации ПрПИ между j-й ОП и k-м ЛИ ЛАЛС (модуляции) и образования вибрационно-оптического участка АОК, содержащего информационный РС;

q_{dj} – вероятность воздействия d-го СЗИ на j-ю ОП в целях подавления АОК;

p_{kl} – вероятность восприятия перехваченного РС l-м ПИ в АОК от k-го приемника ЛАЛС.

В качестве условий, определяющих взаимосвязи элементов структуры, представленной на рис. 3, будем полагать справедливыми следующие:

1) одна и та же ЛАЛС может использоваться злоумышленником для перехвата РС с различных ОП;

2) одно и то же СЗИ может использоваться для подавления побочного информационного РС в нескольких ОП.

Обозначим $P_{АОК}$ и $P_{АОК}^{ЗИ}$ – вероятности утечки РИ по АОК в условиях отсутствия механизмов защиты и в условиях их реализации соответственно.

Как ОК, так и КП могут быть представлены в виде некоторых траекторий преобразований РС, состоящих в изменении вида его материального носителя. При этом в каждой из этих траекторий могут быть выделены передающие, приемные и преобразующие элементы [17, 18]. По аналогии с [17, 18] следует отметить взаимосвязи расположенных рядом элементов в рассматриваемых траекториях. Изменение вида материального носителя приводит к некоторым искажениям соответствующих сигналов.

Одним из основных условий минимизации этих искажений является обеспечение согласования входных характеристик последующего элемента с выходными характеристиками предыдущего элемента рассматриваемой траектории. При этом степень согласованности рассматриваемых характеристик определим как корректность их согласования, а

для ее оценки будем использовать соответствующую вероятность [17, 18].

Так, для согласования выходных характеристик ИИ с входными характеристиками ПИ в основном канале требуется одновременное выполнение следующих условий:

$$A_{\text{с}}^{\text{ИИ}} \triangleq \mu_{\text{пр}}^{\text{ПИ}}, \text{ при } A_{\text{с}}^{\text{ИИ}} > \mu_{\text{пр}}^{\text{ПИ}}; \quad (2)$$

$$\Delta f_{\text{с}}^{\text{ИИ}} \triangleq \Delta f_{\text{пр}}^{\text{ПИ}}, \text{ при } \Delta f_{\text{с}}^{\text{ИИ}} \le \Delta f_{\text{пр}}^{\text{ПИ}}; \quad (3)$$

$$\Delta t_{\text{с}}^{\text{ИИ}} \triangleq \Delta t_{\text{пр}}^{\text{ПИ}}, \text{ при } \Delta t_{\text{с}}^{\text{ИИ}} \le \Delta t_{\text{пр}}^{\text{ПИ}}; \quad (4)$$

$$V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ПИ}}, \text{ при } V_{\text{с}}^{\text{ИИ}} \le V_{\text{кс}}^{\text{ПИ}}, \quad (5)$$

где $A_{\text{с}}^{\text{ИИ}}$ – характеристика s_1 ИИ; $\mu_{\text{пр}}^{\text{ПИ}}$ – характеристика r_1 ПИ; $\Delta f_{\text{с}}^{\text{ИИ}}$ – характеристика s_2 ИИ; $\Delta f_{\text{пр}}^{\text{ПИ}}$ – характеристика r_2 законного ПИ; $\Delta t_{\text{с}}^{\text{ИИ}}$ – характеристика s_3 ИИ; $\Delta t_{\text{пр}}^{\text{ПИ}}$ – характеристика r_3 законного ПИ; $V_{\text{с}}^{\text{ИИ}} = A_{\text{с}}^{\text{ИИ}} \cdot \Delta f_{\text{с}}^{\text{ИИ}} \cdot \Delta t_{\text{с}}^{\text{ИИ}}$ – характеристика $s_{\text{о}}$ ИИ; $V_{\text{кс}}^{\text{ПИ}} = \mu_{\text{пр}}^{\text{ПИ}}\ \Delta f_{\text{пр}}^{\text{ПИ}}\ \Delta t_{\text{пр}}^{\text{ПИ}}$ – характеристика $r_{\text{о}}$ законного ПИ; $\triangleq$ – знак согласования рассматриваемых характеристик.

Вероятность корректности согласования обобщенных характеристик $V_{\text{с}}^{\text{ИИ}}$ и $V_{\text{кс}}^{\text{ПИ}}$ может быть использована как показатель качества основного канала передачи речевой информации p_{in} (см. рис. 3).

$$p(V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ПИ}}) = p_{in} = |1 - V_{\text{с}}^{\text{ИИ}} / V_{\text{кс}}^{\text{ПИ}}|. \quad (6)$$

Применяя обозначения, используемые на рис. 3, запишем условия (2)–(5) в виде

$$м_{is_1}^{\text{ок}} \triangleq r_{nr_1}^{\text{ок}}, \text{ при } м_{is_1}^{\text{ок}} > r_{nr_1}^{\text{ок}}, \quad (7)$$

$$м_{is_2}^{\text{ок}} \triangleq r_{nr_2}^{\text{ок}}, \text{ при } м_{is_2}^{\text{ок}} \le r_{nr_2}^{\text{ок}}, \quad (8)$$

$$м_{is_3}^{\text{ок}} \triangleq r_{nr_3}^{\text{ок}}, \text{ при } м_{is_3}^{\text{ок}} \le r_{nr_3}^{\text{ок}}, \quad (9)$$

$$V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ПИ}} \text{ при} = V_{\text{с}}^{\text{ИИ}} \le V_{\text{кс}}^{\text{ПИ}}, \quad (10)$$

$$p(V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ПИ}}) = p_{in} \to 1, \quad (11)$$

где $м_{is_1}^{\text{ок}} = A_{\text{с}}^{\text{ИИ}}$ – характеристика s_1 ИИ; $r_{nr_1}^{\text{ок}} = \mu_{\text{пр}}^{\text{ПИ}}$ – характеристика r_1 законного ПИ; $м_{is_2}^{\text{ок}} = \Delta f_{\text{с}}^{\text{ИИ}}$ – характеристика s_2 ИИ; $r_{nr_2}^{\text{ок}} = \Delta f_{\text{с}}^{\text{ИИ}}$ – характеристика r_2 законного ПИ; $м_{is_3}^{\text{ок}} = \Delta t_{\text{с}}^{\text{ИИ}}$ – характеристика s_3 ИИ; $r_{nr_3}^{\text{ок}} = \Delta t_{\text{пр}}^{\text{ПИ}}$ – характеристика r_3 законного ПИ.

Будем считать, что в ОК обеспечение согласованности рассматриваемых характеристик стремится к 1 в соответствии с требованиями законных пользователей.

Аналогично условиям (7)–(10) в канале перехвата информации запишем условия обеспечения согласования выходных характеристик ИИ с входными характеристиками ОП:

$$м_{is_1}^{\text{кп}} \triangleq o_{jr_1}^{\text{кп}}, \text{ при } м_{is_1}^{\text{кп}} > o_{jr_1}^{\text{кп}}; \quad (12)$$

$$м_{is_2}^{\text{кп}} \triangleq o_{jr_2}^{\text{кп}}, \text{ при } м_{is_2}^{\text{кп}} \le o_{jr_2}^{\text{кп}}; \quad (13)$$

$$м_{is_3}^{\text{кп}} \triangleq o_{jr_3}^{\text{кп}}, \text{ при } м_{is_3}^{\text{кп}} \le o_{jr_3}^{\text{кп}}; \quad (14)$$

$$V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ОП}}, \text{ при } V_{\text{с}}^{\text{ИИ}} \le V_{\text{кс}}^{\text{ОП}}, \quad (15)$$

где $м_{is_1}^{\text{кп}} = A_{\text{с}}^{\text{ИИ}}$ – характеристика s_1 ИИ; $o_{jr_1}^{\text{кп}} = \mu_{\text{пр}}^{\text{ОП}}$ – характеристика r_1 ОП; $м_{is_2}^{\text{кп}} = \Delta f_{\text{с}}^{\text{ИИ}}$ – характеристика s_2 ИИ; $o_{jr_2}^{\text{кп}} = \Delta f_{\text{пр}}^{\text{ОП}}$ – характеристика r_2 ОП; $м_{is_3}^{\text{кп}} = \Delta t_{\text{с}}^{\text{ИИ}}$ – характеристика s_3 ИИ; $o_{jr_3}^{\text{кп}} = \Delta t_{\text{пр}}^{\text{ОП}}$ – характеристика r_3 ОП; $V_{\text{с}}^{\text{ИИ}} = м_{is_1}^{\text{кп}} \cdot м_{is_2}^{\text{кп}} \cdot м_{is_3}^{\text{кп}}$ – характеристика $s_{\text{о}}$ ИИ; $V_{\text{кс}}^{\text{ОП}} = o_{jr_1}^{\text{кп}}\ o_{jr_2}^{\text{кп}}\ o_{jr_3}^{\text{кп}}$ – характеристика $r_{\text{о}}$ ОП в канале перехвата.

Вероятность корректности согласования обобщенных характеристик $V_{\text{с}}^{\text{ИИ}}$ и $V_{\text{кс}}^{\text{ОП}}$ может быть использована как показатель качества акустовибрационного участка АОК перехвата РИ:

$$p(V_{\text{с}}^{\text{ИИ}} \triangleq V_{\text{кс}}^{\text{ОП}}) = p_{ij} = |1 - V_{\text{с}}^{\text{ИИ}} / V_{\text{кс}}^{\text{ПИ}}|. \quad (16)$$

Условия согласования входных и выходных характеристик рассматриваемых элементов в основном канале учитываются на этапе проектирования, при этом в канале перехвата информации данные условия могут не выполняться либо выполняться лишь частично, что приводит к снижению качества перехватываемой информации [18, 19].

В этих условиях следует отметить противоположность целей законного получателя информации и злоумышленника. Целью злоумышленника в канале перехвата информации является обеспечение максимального качества перехватываемой информации за счет согласования входных характеристик ОП и выходных характеристик лазерного излучателя (ЛИ):

$$o_{jr1} \triangleq \lambda_{ks1}, \text{ при } o_{jr1} < \lambda_{ks1}, \quad (17)$$

$$o_{jr2} \triangleq \lambda_{ks2}, \text{ при } o_{jr2} \ge \lambda_{ks2}, \quad (18)$$

$$o_{jr3} \triangleq \lambda_{ks3}, \text{ при } o_{jr3} \ge \lambda_{ks3}, \quad (19)$$

$$V_{\text{с}}^{\text{ОП}} \triangleq V_{\text{кс}}^{\text{ЛИ}}, \text{ при } V_{\text{с}}^{\text{ОП}} \le V_{\text{кс}}^{\text{ЛИ}}, \quad (20)$$

где $o_{jr1} = \mu_{\text{пр}}^{\text{ОП}}$ – характеристика r_1 ОП; $\lambda_{ks1} = A_{\text{с}}^{\text{ЛИ}}$ – характеристика s_1 ЛИ; $o_{jr2} = \Delta f_{\text{пр}}^{\text{ОП}}$ – характеристика r_2 ОП; $\lambda_{k2} = \Delta f_{\text{с}}^{\text{ЛИ}}$ – характеристика s_2 ЛИ; $o_{jr3} = \Delta t_{\text{пр}}^{\text{ОП}}$ – характеристика r_3 ОП; $\lambda_{ks3} = \Delta t_{\text{с}}^{\text{ЛИ}}$ – характеристика s_3 ЛИ; $V_{\text{с}}^{\text{ОП}} = o_{jr1} \cdot o_{jr2} \cdot o_{jr3}$ – характеристика $r_{\text{о}}$ ОП; $V_{\text{кс}}^{\text{ЛИ}} = \lambda_{ks1}\ \lambda_{ks2}\ \lambda_{ks3}$ – характеристика $s_{\text{о}}$ ЛИ в канале перехвата.

Вероятность корректности согласования обобщенных характеристик $V_{\text{с}}^{\text{ОП}}$ и $V_{\text{кс}}^{\text{ЛИ}}$ может быть использована как показатель r_{jk}, характеризующий качество облучения ОП лазерным лучом:

$$p(V_{\text{с}}^{\text{ОП}} \triangleq V_{\text{кс}}^{\text{ЛИ}}) = s_{jk} = |1 - V_{\text{с}}^{\text{ОП}} / V_{\text{кс}}^{\text{ЛИ}}|. \quad (21)$$

Целью законных пользователей является обеспечение требуемого уровня защищенности РИ от утечки в канале перехвата рассматриваемого типа. Это может быть достигнуто за счет нарушения условий (16)–(19):

$$o_{jr1} \hat{\neq} \lambda_{ks1}, \quad (22)$$

$$o_{jr2} \hat{\neq} \lambda_{ks2}. \quad (23)$$

$$o_{jr3} \hat{\neq} \lambda_{ks3}, \quad (24)$$

$$V_{\text{с}}^{\text{ОП}} \hat{\neq} V_{\text{кс}}^{\text{ЛИ}}. \quad (25)$$

Для этого используются СЗИ, воздействующие на ОП.

Заключительным этапом в канале перехвата является использование злоумышленником перехваченного информационного РС от приемника ЛАЛС:

$$\pi_{ks1} \hat{=} r_{n\text{1}}^{\text{кп}}, \text{ при } \pi_{ks1} > r_{n\text{1}}^{\text{кп}}, \quad (26)$$

$$\pi_{ks2} \hat{=} r_{nr_2}^{\text{кп}}, \text{ при } \pi_{ks2} \le r_{nr_2}^{\text{кп}}, \quad (27)$$

$$\pi_{ks3} \hat{=} r_{nr_3}^{\text{кп}}, \text{ при } \pi_{ks3} \le r_{nr_3}^{\text{кп}}, \quad (28)$$

$$V_{\text{с}}^{\text{П}} \hat{=} V_{\text{кс}}^{\text{ПИ}}, \text{ при } V_{\text{с}}^{\text{ЛИ}} \le V_{\text{кс}}^{\text{ЛИ}}, \quad (29)$$

где $\pi_{ks1} = A_{\text{с}}^{\text{ЛИ}}$ – характеристика s_1 приемника ЛАЛС; $r_{n\text{1}}^{\text{кп}} = \mu_{\text{пр}}^{\text{ОП}}$ – характеристика r_1 ПИ в канале перехвата; $\lambda_{k2} = \Delta f_{\text{с}}^{\text{ЛИ}}$ – характеристика s_2 приемника ЛАЛС; $r_{nr_2}^{\text{кп}} = \Delta f_{\text{пр}}^{\text{ОП}}$ – характеристика r_2 ПИ в канале перехвата; $\lambda_{ks3} = \Delta t_{\text{с}}^{\text{ЛИ}}$ – характеристика s_3 приемника ЛАЛС; $r_{nr_3}^{\text{кп}} = \Delta t_{\text{пр}}^{\text{ОП}}$ – характеристика r_3 ПИ в канале перехвата; $V_{\text{с}}^{\text{П}} = \pi_{ks1} \cdot \pi_{ks2} \cdot \pi_{ks3}$ – характеристика $s_{\text{о}}$ ОП; $V_{\text{кс}}^{\text{ПИ}} = r_{n\text{1}}^{\text{кп}} \; r_{nr_2}^{\text{кп}} \; r_{nr_3}^{\text{кп}}$ – характеристика $r_{\text{о}}$ ПИ в канале перехвата.

Вероятность корректности согласования обобщенных характеристик $V_{\text{с}}^{\text{П}}$ и $V_{\text{кс}}^{\text{ПИ}}$ может быть использована как показатель p_{kl}, характеризующий качество восприятия перехваченного РС l-м ПИ в АОК от k-го приемника ЛАЛС:

$$p(V_{\text{с}}^{\text{ОП}} \hat{=} V_{\text{кс}}^{\text{ЛИ}}) = p_{kl} = |1 - V_{\text{с}}^{\text{П}} / V_{\text{кс}}^{\text{ПИ}}|. \quad (30)$$

Вероятность утечки по АОК $P_{\text{АОК}}$ определим как произведение вероятностей каждого участка перехвата РС по АОК:

$$P_{\text{АОК}} = p_{ij} \, s_{jk} \, p_{kl}. \quad (31)$$

Вероятность s_{jk} будем рассматривать как условную вероятность от r_{jk}. При этом поскольку вероятности r_{jk} и s_{jk} взаимосвязаны за счет общей ЛАЛС и одной и той же ОП, то

$$s_{jk} / r_{jk} = r_{jk}. \quad (32)$$

Тогда выражение (31) для условий отсутствия СЗИ запишем в виде

$$P_{\text{АОК}} = p_{ij} \, r_{jk} \, p_{kl}. \quad (33)$$

Применение механизмов защиты позволяет представить вероятности в следующем виде:

$$p_{ij}^{\text{ЗИ}} = p_{ij} / q_{dj}, \quad (34)$$

$$r_{jk}^{\text{ЗИ}} = r_{jk} / q_{dj}. \quad (35)$$

С учетом наличия взаимосвязей по аналогии с выражением (32) запишем:

$$p_{ij}^{\text{ЗИ}} = q_{dj}, \quad (36)$$

$$r_{jk}^{\text{ЗИ}} = q_{dj}. \quad (37)$$

Тогда вероятность утечки РИ по АОК в условиях реализации механизмов защиты запишем в виде

$$P_{\text{АОК}} = q_{dj} \, q_{dj} \, p_{kl} = q_{dj}^2 \; p_{kl}. \quad (38)$$

Заключение

На практике параметры выражений (17)–(25) оцениваются как в процессе проектирования, разработки и развертывания защищенного ОИ путем реализации организационных и технических мероприятий пассивного и активного характера [4, 5], так и в процессе мероприятий по защите информации и дальнейшей аттестации ОИ по требованиям к защищенности информации путем противодействия применению злоумышленником различных средств технической разведки.

При этом определение вероятностей, представленных на рис. 3, осуществляется для конкретных ОИ путем моделирования соответствующих информационных процессов и является предметом дальнейших исследований авторов.

Литература

1. О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (в ред. от 7 марта 2018 г.) // Собрание законодательства Российской Федерации. – 2011. – № 7. – 900 с.

2. Авсентьев А.О., Мишина Н.О., Гудков. Д.А. Особенности использования речевой информации в деятельности органов внутренних дел // Охрана, безопасность, связь. – 2017. – № 1-2. – С. 20–26.

3. Авсентьев О.С., Мишина Н.О. Условия образования технических каналов утечки речевой информации в деятельности правоохранительных органов // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2017. – № 3-3. – С. 220–228.

4. Меньшаков Ю.К. Теоретические основы технических разведок: учеб. пособие / под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

5. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации: учеб. для вузов – 7-е изд., испр. – М.: Горячая линия – Телеком, 2012. – 442 с.

6. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2015. – 586 с.

7. Теория электрической связи: конспект лекций / под общ. ред. В.А. Григорьева. – СПб.: НИУ ИТМО, 2012. – 148 с.

8. Авсентьев О.С., Гудков Д.А. Особенности каналов утечки речевой информации в деятельности органов внутренних дел // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. матер. Всерос. науч.-практ. конф. – 2016. – С. 108–111.

9. Бондарко Л.В., Вербицкая Л.А., Гордина М.В. Основы общей фонетики: учеб. пособие. – СПб.: Изд-во С.-Петерб. ун-та, 1991. – 152 с.

10. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь! – М.: НОУ ШО «Баярд», 2004. – 432 с.

11. ГОСТ Р ИСО 24504–2015. Уровни звукового давления речевых сообщений для продукции и систем оповещения.

12. Джеймс Л. Фланаган. Анализ, синтез и восприятие речи / пер. с англ. под ред. А.А. Пирогова. – М.: Связь, 1968. – 396 с.

13. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. – № 5. – С. 46−56.

14. Голубинский А.Н. Расчёт частоты основного тона речевого сигнала на основе полигармонической математической модели // Вестник Воронеж. ин-та МВД России. – 2009. – № 1. – С. 81–90.

15. Ахмад Х.М. Введение в цифровую обработку речевых сигналов: учеб. пособие / Х.М. Ахмад, В.Ф. Жирков. – Владимир: Изд-во Владимир. гос. ун-та, 2007. – 192 с.

16. Авсентьев О.С., Авсентьев А.О., Вальде А.Г. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации // Вестник Воронеж. ин-та МВД России. – 2017. – № 3. – С. 22–31.

17. Авсентьев О.С., Меньших В.В., Авсентьев А.О. Моделирование и оптимизация процессов передачи и защиты информации в каналах связи // Специальная техника. – 2015. – №5. – С. 47–50.

18. Авсентьев О.С., Меньших В.В., Авсентьев А.О. Модель оптимизации процесса передачи информации по каналам связи в условиях угроз ее безопасности // Телекоммуникации. – 2016. – №1. – С. 28—32.

19. Авсентьев О.С., Авсентьев А.О., Вальде А.Г. Математическая модель защиты информации от утечки по электромагнитным каналам // Вестник Воронеж. ин-та МВД России. – 2016. – № 3. – С. 42–50.

Авсентьев Олег Сергеевич
Д-р техн. наук, профессор каф. информационной безопасности Воронежского института МВД России
Патриотов пр., д. 53, г. Воронеж, Россия, 394065
Тел.: +7-(473-2) 00-52-36
Эл. почта: osaos@mail.ru

Гудков Данила Андреевич
Адъюнкт каф. информационной безопасности Воронежского института МВД России
Патриотов пр., д. 53, г. Воронеж, Россия, 394065
Тел.: +7-(473-2) 00-52-36
Эл. почта: guddan@mail.ru

Avsentiev O.S., Gudkov D.A.

Study of characteristics of the acousto-optic channel of speech information leakage in the conditions of implementation of protection mechanisms

The dynamic characteristics of the processes of speech information transmission from the source to its recipient, as well as the interception of this information by an attacker through the acousto-optical leakage channel are determined. The authors formalized the probability of correctness of matching these characteristics at each stage of the change of the material carrier of the information speech signal when using the means of information protection from leakage through channels of the considered type.

Keywords: speech information, acousto-optical channel of speech information leakage, laser acoustic location system, electrical characteristics of the communication channel, matching conditions of signal characteristics, communication channel, correctness of matching, possibility of speech information leakage.
doi: 10.21293/1818-0442-2018-21-2-88-94

References

1. About the police: Federal law of 7 February 2011 г. № 3-FL (as amended on March 7, 2018). Collected legislation of the Russian Federation, 2011, no. 7, St. 900. (In Russ.).

2. Avsentiev A.O., Mishina N.O., Gudkov D.A. Features of the use of speech information in the activities of the internal Affairs bodies. Security, safety, communication, 2017, № 1-2, pp. 20–26. (In Russ.).

3. Avsentiev O.S., Mishina N.O. Conditions of formation of technical channels of speech information leakage in the activities of law enforcement agencies. Public security, rule of law in the III Millennium, 2017, no. 3-3, pp. 220–228. (In Russ.).

4. Menshakov U.K. *Teoreticheskie osnovy tehnitcheskih razvedok* [The theoretical basis of technical intelligence]. Proc. Benefit, under the editorship. U.N. Lavruhina. Moscow, Publishing house MSTU im. N.E. Baumana, 2008, 536 p. (In Russ.).

5. Zaitsev A.P., Mesheryakov R.V., Shelupanov A.A. *Tehnitcheskie sredstva i metody zacshity informatsii* [Technical means and methods of information protection]. Textbook for high schools, 7th ed., the Rev. Moscow, Goryatchaya liniya, Telecom, 2012, 442 p. (In Russ.).

6. Buzov G.A. *Zaschita informatsii ogranichennogo dostupa ot utechki po tehnitcheskim kanalam* [Protection of restricted information from leakage through technical channels]. Moscow, Goryatchaya liniya, Telecom, 2015, 586 p. (In Russ.).

7. *Teoriya elektricheskoi svyazi: konspekt lektsiy* [Theory of electrical communication: lecture notes]. Under the General editorship of V.A. Grigoriev, SPb, NIU ITMO, 2012, 148 p. (In Russ.).

8. Avsentiev O.S., Gudkov D.A. Features of channels of leakage of speech information in activity of law-enforcement bodies. Actual questions of operation of systems of protection and the protected telecommunication systems. The collection of materials of the all-Russian scientific and practical conference. 2016, pp. 108–111. (In Russ.).

9. Bondarko L.V., Verbitskaya L.A., Gordina M.V. *Osnovy obshey fonetiki* [Basics of General phonetics]. Studies. Benefit, SPb, Publishing house S.-Peterburg un-ty, 1991, 152 p. (In Russ.).

10. Halyapin D.B. *Zaschita informatsii. Vas podslushivayut? Zashishaites!* [Information protection. Are you eavesdropping? Defend yourself!]. Moscow, NOU SHO «Bayard», 2004, 432 p. (In Russ.).

11. GOST R ISO 24504-2015. Sound pressure levels of voice messages for products and warning systems. (In Russ.).

12. James L. Flanagan. *Analiz, sintez I vospriyatie rechi* [Analysis, synthesis and speech perception]. Translation from English edited by A.A. Pirogov, Moscow, Publishing House «Svyaz», 1968, 396 p. (In Russ.).

13. Horev A.A., Makarov U.K.. To assess the effectiveness of protection of acoustic (speech) information. *Special equipment*, Moscow, 2000, no. 5, pp. 46−56 (In Russ.).

14. Golubinskkiy A.N. Calculation of the basic tone frequency of a speech signal based on a polyharmonic mathematical model. *Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia*, 2009, № 1, pp. 81–90 (In Russ.).

15. Ahmad H.M. *Vvedenie v tsifrovuyu obrabotku rechevyh signalov* [Introduction to digital speech processing]. Studies. Benefit, H.M. Ahmad, V.F. Zhirkov, Vlad. state un-

ty, Vladimir, Publishing house Vladimir. state un-ty, 2007, 192 p. (In Russ.).

16. Avsentiev O.S., Avsentiev A.O., Valde A.G. Research of conditions of emergence of technical channels of information leakage on side electromagnetic radiation at objects of in-formatting. *Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia,* 2017, no. 3, pp. 22–31 (In Russ.).

17. Avsentiev O.S., Men'shikh V.V., Avsentiev A.O. Modeling and optimization of information transmission and protection processes in communication channels. *Special equipment,* 2015, no. 5, pp. 47–50 (In Russ.).

18. Avsentiev O.S., Men'shikh V.V., Avsentiev A.O. Model of optimization of information transmission through communication channels in the conditions of threats to its security. *Telecommunication,* 2016, no. 1, pp. 28—32 (In Russ.).

19. Avsentiev O.S., Avsentiev A.O., Valde A.G. Mathematical model of information protection from leakage through electromagnetic channels. *Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia*, 2016, no. 3, pp. 42–50 (In Russ.).

Oleg S. Avsentiev
Dr. techn. sciences, professor of the Department
of information security of the Voronezh Institute
of the Ministry of internal Affairs of Russia
53, Patriots pr., Voronezh, Russia, 394065
Phone: +7-(473-2) 00-52-36
Email: osaos@mail.ru

Danila A. Gudkov
Adjunct of the Department of information security
of the Voronezh Institute of the Ministry
of internal Affairs of Russia
53, Patriots pr., Voronezh, Russia, 394065
Phone: +7-(473-2) 00-52-36
Email: guddan@mail.ru

УДК 519.863

Е.Б. Грибанова

Методы решения обратных задач экономического анализа с помощью минимизации приращений аргументов

Предложен метод решения обратных задач экономического анализа при минимальном изменении аргументов. Его реализация является более простой по сравнению с методами решения нелинейных оптимизационных задач. Рассмотрена аддитивная, мультипликативная и кратная модель. В качестве примера приведена задача формирования рейтинга группы онлайновой социальной сети.

Ключевые слова: обратные вычисления, оптимизация, квадратичное программирование, рейтинг.
doi: 10.21293/1818-0442-2018-21-2-95-99

При принятии решений в области экономики специалист сталкивается с прямыми и обратными задачами. Под решением задач с помощью обратных вычислений [1–3] понимают нахождение приращений аргументов функции на основе следующей информации:

- начальные значения аргументов (x_1, x_2) и функции (y);
- новое значение функции ($y \pm \Delta y$);
- коэффициенты относительной важности аргументов (α, β);
- направление изменений аргументов (+,–).

Таким образом, может быть сформирована система уравнений:

$$\begin{cases} y \pm \Delta y = f(x_1 \pm \Delta x_1(\alpha), x_2 \pm \Delta x_2(\beta)); \\ \dfrac{\Delta x_1}{\Delta x_2} = \dfrac{\alpha}{\beta}; \\ \alpha + \beta = 1. \end{cases} \quad (1)$$

Решением системы будут величины Δx_1 и Δx_2, обеспечивающие значение результирующего показателя, равное $y \pm \Delta y$.

Полученные значения могут быть использованы для определения направлений изменения показателей деятельности исследуемого объекта для достижения заданной цели. Примеры решения задач такого рода рассмотрены в статьях [4–7]. В работе [8] метод обратных вычислений был использован совместно с лагранжевым анализом конечных изменений, что позволило выявить факторы, оказавшие наибольшее влияние на результат. При наличии ограничений на величины аргументов могут быть использованы итерационные алгоритмы, в том числе с применением элементов случайного поиска [3, 9].

Результат решения системы (1) определяется значениями коэффициентов относительной важности и направлением изменений показателей, которые устанавливаются исследователем. Привязка к мнению эксперта имеет свои положительные стороны: может быть рассмотрено несколько возможных вариантов решения задачи, коэффициенты могут быть установлены с учётом реальной возможности направления изменения аргументов и их взаимозависимости. Полученное решение впоследствии может быть скорректировано с учетом дополнительных условий. Так, например, в работе [10] рассматривается получение решения в соответствии с «золотыми» пропорциями показателей. Однако иногда возникает необходимость получить результат без привлечения экспертной информации. К такому случаю можно отнести нахождение решения, максимально близкого к исходному, т.е. при минимальном изменении значений аргументов.

В данной работе рассмотрено решение задач с помощью обратных вычислений в случае минимального приращения аргументов (без привлечения экспертной информации). Модификация классической схемы решения (1) при этом выражается в изменении величины соотношения значений приращений аргументов, которая будет определяться теперь угловым коэффициентом линии уровня, определяемого новым значением функции. Далее будет рассмотрено решение задачи в случае аддитивной, кратной и мультипликативной зависимости.

Аддитивная модель

Рассмотрим задачу с аддитивной зависимостью (например, суммарные затраты равны сумме постоянных и переменных затрат [1]):

$$y = x_1 + x_2 .$$

Пусть начальные условия задачи: $y^0 = 5$, $x_1^0 = 2$, $x_2^0 = 3$. Необходимо определить такие значения x_1^1, x_2^1, при которых y^1 равно 10. Построим две линии уровня 5 и 10 соответственно (рис. 1), представляющие собой параллельные прямые. Точка А соответствует начальному условию задачи. Точки линии $x_2 = 10 - x_1$ обеспечат значение результирующей величины, равное 10. Точки *B* и *C* соответствуют случаям, когда искомое значение функции будет получено только за счет изменения x_2 и x_1 соответственно. Точки линии $x_2 = 10 - x_1$, принадлежащие отрезку *BC*, будут получены при увеличении аргументов функции (x_1 , x_2), расположенные левее точки *B* – при уменьшении аргумента x_1 и увеличении x_2 (x_1^- , x_2^+), а точки правее *C* – при увеличении x_1 и уменьшении x_2 (x_1^+ , x_2^-).

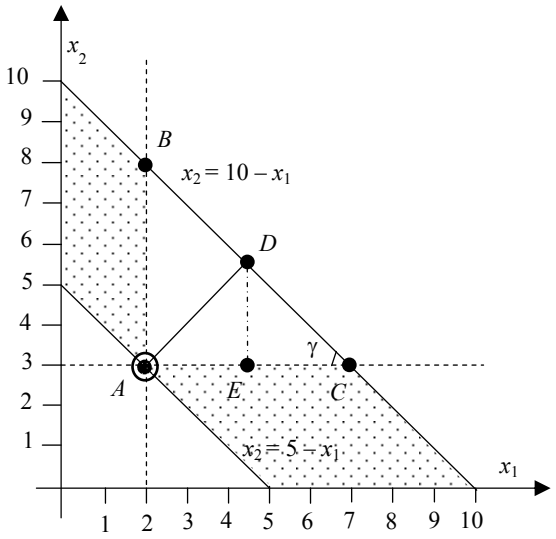


Рис. 1. Линии уровня 5 и 10

Кратчайшее расстояние из точки A до прямой $x_2 = 10 - x_1$ представляет собой длину перпендикуляра AD. Таким образом, при переходе из точки A в точку D изменение аргументов будет наименьшим. Изменение первого аргумента (Δx_1) равно длине отрезка AE, изменение второго аргумента (Δx_2) – отрезка DE ($AD^2 = AE^2 + DE^2$).

Задача оптимизации при этом может быть представлена в виде задачи квадратичного программирования [11–12]:

$$f(\Delta x_1, \Delta x_2) = \Delta x_1^2 + \Delta x_2^2 \to \min,$$
$$2 + \Delta x_1 + 3 + \Delta x_2 = 10.$$

Для решения данной задачи могут быть использованы методы нелинейной оптимизации: множителей Лагранжа, метод штрафов [13, 14]. В результате будут получены следующие значения приращений: $\Delta x_1 = 2{,}5$, $\Delta x_2 = 2{,}5$. Таким образом, новые величины аргументов:

$$x_1^1 = 2 + 2{,}5 = 4{,}5;$$
$$x_2^1 = 3 + 2{,}5 = 5{,}5.$$

Из рис. 1 можно увидеть, что угол ADE равен углу ECD. Поскольку тангенс угла равен угловому коэффициенту, то

$$\frac{AE}{DE} = -\rho,$$

где ρ – коэффициент угла наклона прямой.

Для рассматриваемого примера $\rho = -1$. Следовательно, для определения значений приращений с наименьшим изменением необходимо решить систему:

$$\begin{cases} \dfrac{\Delta x_1}{\Delta x_2} = 1; \\ 2 + \Delta x_1 + 3 + \Delta x_2 = 10. \end{cases}$$

Подставляя во второе уравнение $\Delta x_1 = \Delta x_2$, получим

$$2 + \Delta x_2 + 3 + \Delta x_2 = 10;$$
$$\Delta x_2 = 2{,}5;$$
$$\Delta x_1 = 2{,}5.$$

Рассмотрим случай при большем числе аргументов. Пусть функция имеет вид

$$y = c_1 x_1 + c_2 x_2 + \ldots c_n x_n,$$

где c – константы.

Тогда определение аргументов с наименьшим приращением будет выполнено путем решения системы:

$$\begin{cases} \dfrac{\Delta x_i}{\Delta x_k} = \dfrac{c_i}{c_k}, i = 1 \ldots n,\ i \neq k; \\ c_1(x_1^0 + \Delta x_1) + c_2(x_2^0 + \Delta x_2) + \ldots c_n(x_n^0 + \Delta x_n) = y^1, \end{cases}$$

где k – номер аргумента, который принимается за базовый.

Кратная модель

При кратной зависимости модель имеет следующий вид (например, рентабельность определяется как отношение прибыли к затратам):

$$y = \frac{x_2}{x_1}.$$

Пусть начальные значения равны: $y^0 = 2$, $x_1^0 = 5$, $x_2^0 = 10$. Необходимо определить значения x_1^1, x_2^1, при которых значение функции равно 4.

Задача квадратичного программирования имеет вид

$$f(\Delta x_1, \Delta x_2) = \Delta x_1^2 + \Delta x_2^2 \to \min;$$
$$\frac{(10 + \Delta x_2)}{(5 + \Delta x_1)} = 4.$$

Решение задачи: $\Delta x_1 = -2{,}353$, $\Delta x_2 = 0{,}588$, $x_1^1 = 2{,}647$, $x_2^1 = 10{,}588$.

На рис. 2 представлены линии уровня 2 и 4.

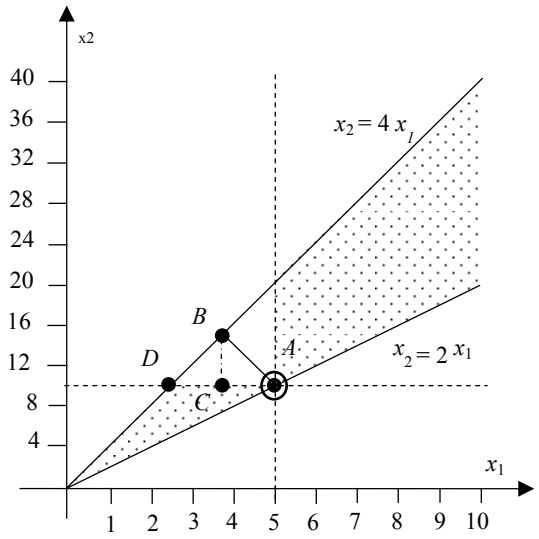


Рис. 2. Линии уровня 2 и 4

Начальные значения аргументов образуют точку A. Наименьшее расстояние из этой точки до пря-

мой $x_2 = 4x_1$ – это длина перпендикуляра AB. Высота BC образует два подобных треугольника. Следовательно, справедливо соотношение

$$\frac{AC}{BC} = -4 .$$

Тогда система будет иметь вид

$$\begin{cases} \dfrac{\Delta x_1}{\Delta x_2} = -4; \\ \dfrac{10 + \Delta x_2}{5 + \Delta x_1} = 4. \end{cases}$$

Решение системы: $\Delta x_1 = -2{,}353$, $\Delta x_2 = 0{,}588$.

Мультипликативная модель

Наконец, рассмотрим мультипликативную зависимость (например, выручка от продажи товара равна произведению цены и количества):

$$y = x_1 \cdot x_2 .$$

Примем начальные условия задачи: $y^0 = 10$, $x_1^0 = 5$, $x_2^0 = 2$. Необходимо определить значения x_1^1, x_2^1, при которых y^1 равно 20.

Задача квадратичного программирования:

$$f(\Delta x_1, \Delta x_2) = \Delta x_1^2 + \Delta x_2^2 \to \min,$$
$$(5 + \Delta x_1)(2 + \Delta x_2) = 20.$$

Решение задачи: $\Delta x_1 = 0{,}837$, $\Delta x_2 = 1{,}426$, $x_1^1 = 5{,}837$, $x_2^1 = 3{,}426$.

Рассмотрим линии уровня 10 и 20 (рис. 3). Точка А соответствует начальным значениям аргументов. Определение точки графика $x_2 = 20/x_1$ таким образом, чтобы изменения аргументов были минимальны, может быть выполнено с использованием уравнения касательной:

$$k = f'(x_0)(x - x_0) + f(x_0) ,$$

где x_0 – точка функции $f(x)$, к которой строится касательная.

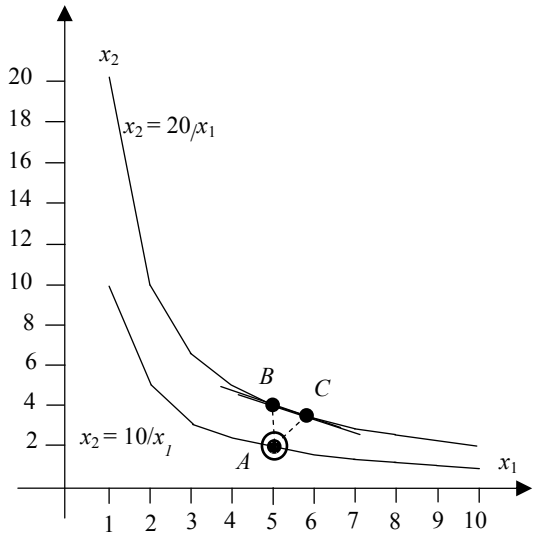


Рис. 3. Кривые уровня 10 и 20

Уравнение касательной к точке B будет иметь вид

$$x_2 = \frac{-20}{5^2}(x_1 - 5) + \frac{20}{5} = -0{,}8x_1 + 8 .$$

Поиск наименьших изменений аргументов для перехода в точку на прямой может быть выполнен с помощью решения системы уравнения:

$$\begin{cases} \dfrac{\Delta x_1}{\Delta x_2} = \dfrac{y^1}{\left(x_1^0\right)^2} = 0{,}8; \\ 0{,}8(5 + \Delta x_1) + (2 + \Delta x_2) = 8. \end{cases}$$

Отношение приращений аргументов будет равно угловому коэффициенту в уравнении касательной (со знаком «минус»). Решение системы: $\Delta x_1 = 0{,}976$, $\Delta x_2 = 1{,}22$, $x_1^1 = 5{,}976$, $x_2^1 = 3{,}22$.

Далее необходимо построить уравнение касательной к новой точке ($x_1^1 = 5{,}976$, $x_2^1 = 3{,}22$) и выполнить поиск новой точки с минимальным изменением аргументов.

Таким образом, алгоритм нахождения решения в случае мультипликативной модели включает следующие шаги:

1. Установка начальных значений:

$$i = 0,\ x_1(i) = x_1^0,\ x_2(i) = x_2^0 .$$

2. Построение уравнения касательной к точке $x_1(i)$ функции $x_2 = \dfrac{y^1}{x_1}$.

3. Поиск точки $x_1(i+1)$, $x_2(i+1)$ на касательной, до которой расстояние от исходной точки x_1^0, x_2^0 будет минимальным.

4. Проверка выполнения условия останова: если изменение положения точки меньше заданной точности ε ($\delta = \sqrt{(x_1(i+1) - x_1(i))^2 + (x_2(i+1) - x_2(i))^2} < \varepsilon$), то алгоритм завершается, иначе осуществляется переход на шаг 2 ($i = i + 1$).

В таблице представлены результаты выполнения итераций для рассматриваемого примера ($\varepsilon = 0{,}003$).

Результаты выполнения итераций

i	$x_1(i)$	$x_2(i)$	$-f'(x_1(i))$	δ
0	5	2	0,8	–
1	5,976	3,22	0,56	1
2	5,807	3,441	0,593	0,278
3	5,844	3,423	0,586	0,041
4	5,835	3,425	0,587	0,009
5	5,838	3,428	0,587	0,004
6	5,837	3,426	–	0,002

Пример формирования рейтинговой оценки

В качестве примера рассмотрим также задачу формирования рейтинга группы онлайновой соци-

альной сети. Интегральная оценка вычисляется по формуле:

$$R_j = 0{,}701x_{1j} + 0{,}24x_{2j} + 0{,}059x_{3j},$$

где x_{1j} – нормированное значение числа подписчиков j-й группы; x_{2j} – нормированное значение показателя популярности j-й группы; x_{3j} – нормированное значение показателя активности j-й группы.

Для выбранной группы значения нормированных величин равны: $x_1^0 = 0{,}313$, $x_2^0 = 0{,}004$, $x_3^0 = 0{,}029$. Тогда интегральная оценка составит:

$$R = 0{,}701 \cdot 0{,}313 + 0{,}24 \cdot 0{,}004 + 0{,}059 \cdot 0{,}029 = 0{,}222.$$

Пусть необходимо определить такие новые значения x, которые обеспечат значение рейтинговой оценки, равное 0,3, при минимальном изменении аргументов.

Система уравнений имеет вид:

$$\begin{cases} \dfrac{\Delta x_1}{\Delta x_2} = \dfrac{c_1}{c_2} = \dfrac{0{,}701}{0{,}24}; \\ \dfrac{\Delta x_3}{\Delta x_2} = \dfrac{c_3}{c_2} = \dfrac{0{,}059}{0{,}24}; \\ 0{,}701(0{,}313 + \Delta x_1) + 0{,}24(0{,}004 + \Delta x_2) + \\ +0{,}059(0{,}029 + \Delta x_3) = 0{,}3. \end{cases}$$

Решение системы: $\Delta x_1 = 0{,}099$, $\Delta x_2 = 0{,}034$, $\Delta x_3 = 0{,}008$. Таким образом,

$$x_1^1 = 0{,}313 + 0{,}099 = 0{,}412;$$

$$x_2^1 = 0{,}004 + 0{,}034 = 0{,}038;$$

$$x_3^1 = 0{,}029 + 0{,}008 = 0{,}037.$$

Заключение

В статье рассмотрено решение обратных задач экономического анализа с помощью обратных вычислений путем минимизации приращений аргументов. Модификация классической схемы решения заключается в использовании в качестве отношения коэффициентов относительной важности углового коэффициента линии установленного уровня. Представлена графическая интерпретация используемых соотношений. По сравнению с решением оптимизационных задач нелинейного программирования представленный подход является более простым в компьютерной реализации: решение задачи сводится к решению системы алгебраических уравнений. Рассмотрен случай аддитивной, кратной и мультипликативной зависимости между аргументами. Также в статье представлен пример формирования рейтинговой оценки с заданным значением интегрального показателя. Результаты вычислений совпали с результатами, полученными путем решения задачи нелинейного программирования с использованием оптимизационных методов.

С помощью представленных методов может быть получено решение обратных задач при отсутствии экспертных оценок о важности аргументов функции и направлении изменения показателей и минимальном изменении исходных данных.

Также рассмотренный подход может быть использован для решения отдельных задач квадратичного программирования с одним ограничением [15].

Литература

1. Одинцов Б.Е. Обратные вычисления в формировании экономических решений. – М.: Финансы и статистика, 2004. – 256 с.

2. Дик В.В. Методология формирования решений в экономических системах и инструментальные среды их поддержки. – М.: Финансы и статистика, 2001. – 300 с.

3. Одинцов Б.Е. Итерационный метод оптимизации управления предприятиями средствами обратных вычислений / Б.Е. Одинцов, А.Н. Романов // Вестник Финансового ун-та. – 2014. – № 2. – С. 60–73.

4. Виштак О.В. Использование технологии обратных вычислений при мониторинге качества дополнительного образования в вузе / О.В. Виштак, И.А. Штырова // Вестник Астрахан. гос. техн. ун-та. – 2014. – № 2. – С. 67–73.

5. Бармина Е.А. Мониторинг качества коммерческой организации. Структурирование показателей. Применение когнитивных карт / Е.А. Бармина, И.Ю. Квятковская // Вестник Астрахан. гос. техн. ун-та. – 2010. – № 2. – С. 15–20.

6. Мартьянова А.В. Управление эффективностью банка на базе обратных вычислений // Вестник магистратуры. – 2015. – №6(45). – С. 77–79.

7. Одинцов Б.Е. Когнитивные древовидные структуры в управлении слабоформализованными социально-экономическими процессами // Информатизация образования и науки. – 2017. – № 2. – С. 46–56.

8. Блюмин С.Л. // Обратные задачи в лагранжевом анализе конечных изменений / С.Л. Блюмин, Г.С. Боровкова, А.С. Сысоев // Современные проблемы горно-металлургического комплекса. Наука и производство: матер. Тринадцатой Всерос. науч.-практ. конф. – Старый Оскол, 2016. – Т. 2. – С. 6–10.

9. Грибанова Е.Б. Стохастические алгоритмы решения обратных задач с ограничениями // Доклады ТУСУР. – 2016. – № 4. – С. 112–116.

10. Одинцов Б.Е. Управление с учетом «золотых» пропорций плановых показателей // Управленческие науки в современном мире. – 2016. – № 1. – С. 43–47.

11. Грибанова Е.Б. Методы решения обратных задач экономического анализа // Корпоративные финансы. – 2016. – № 1. – С. 119–130.

12. Сініцький М. Є. До питання розв'язку обернених задач економічного спрямування // Науковий вісник Національної академії статистики, обліку та аудиту. – 2018. – № 1. – С. 195–202.

13. Мицель А.А. Методы оптимизации: учеб. пособие / А.А. Мицель, А.А. Шелестов. – Томск: Изд-во ТУСУРа, 2004. – 256 с.

14. Карманов В.Г. Математическое программирование: учеб. пособие. – М.: Наука, 1989. – 263 с.

15. Грибанова Е.Б. Решение задачи оптимизации закупок с помощью обратных вычислений // Экономический анализ: теория и практика. – 2018. – № 3. – С. 586–596.

Грибанова Екатерина Борисовна
Канд. техн. наук, доцент каф. автоматизированных систем управления (АСУ) Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-36
Эл. почта: katag@yandex.ru

Gribanova E.B.

Methods for solving inverse problems of economic analysis by minimizing argument increments

The article describes the method of solving inverse problems of economic analysis by minimizing the increments of arguments. A simpler solution was obtained in comparison with the use of optimization methods of nonlinear programming. Additive, multiplicative and multiple models are considered. The task of rating formation is given as an example.

Keywords: inverse computations, optimization, quadratic programming, rating.
doi: 10.21293/1818-0442-2018-21-2-95-99

References

1. Odincov B.E. Obratnye vychislenija v formirovanii jeko-nomicheskih reshenij [Inverse computations in forming of economic decisions]. Moscow, Finansy i statistika Publ., 2004. 256 p.

2. Dik V.V. Metodologija formirovanija reshenij v jekonomicheskih sistemah i instrumental'nye sredy ih podderzhki [Methodology of decision-making in economic systems and instrumental environment of their support]. Moscow, Finansy i statistika Publ., 2001, 300 p.

3. Odintsov B.E., Romanov A.N. An iterative method of optimization of enterprise management by means of inverse calcalations. *The bulletin of the financial university*, 2014, no. 2, pp. 60–73. (In Russ.).

4. Vishtak O.V., Shtyrova I.A. The use of technology of inverse calculations when monitoring the quality of additional education at the University. *The bulletin of Astrakhan state technical university*, 2014, no. 2, pp. 67–73.

5. Barmina E.A., Kvjatkovskaja I.Ju. Quality monitoring of a commercial organization. The structuring of indicators. Application of cognitive maps. *The bulletin of Astrakhan state technical university*, 2010, no. 2, pp. 15–20.

6. Mart'janova A.V. The performance management of the bank using the inverse calculation. *Bulletin of the magistracy*, 2015, no. 6, pp. 77–79.

7. Odincov B.E. Cognitive tree structures in the management of weakly formalized socio-economic processes. *Informatization of education and science*, 2017, no. 2, pp. 46–56.

8. Bljumin S.L., Borovkova G.S., Sysoev A.S. Obratnye zadachi v lagranzhevom analize konechnyh izmene-nij [The inverse problem in Lagrangian analysis of the final changes]. Sovremennye problemy gorno-metallurgicheskogo kompleksa. Nauka i proizvodstvo. Materialy trinadcatoj Vserossijskoj nauchno-prakticheskoj konferencii [Modern problems of mining and metallurgical complex. Science and production. Proc. of the thirteenth All-Russian scientific-practical conference]. Staryj Oskol, 2016, vol. II, pp. 6–10.

9. Gribanova E.B. Stochastic algorithms for solving the economic analysis inverse problems with constraints. *Proceedings of TUSUR University,* 2016, no. 4, pp. 112–116.

10. Odintsov B.E. Management taking into account the «golden» proportions of the planned indicators. *Managerial sciences in the modern world*, 2016, no. 1, pp. 43–47.

11. Gribanova E.B. Methods for solving inverse problems of economic analysis. *Corporate Finance*, 2016, no. 1, pp. 119–130.

12. Sinic'kij M. Є. To the solution of inverse problems of economic direction. *Scientific Bulletin of National Academy of statistics, accounting and audit*, 2018, no. 1–2, pp. 195–202.

13. Micel' A.A., Shelestov A.A. Metody optimizacii: uchebnoe posobie [Optimization method]. Tomsk, TUSUR Publ., 2004, 256 p.

14. Karmanov V.G. Matematicheskoe programmirovanie: uchebnoe posobie [Mathematical programming]. Moscow, Nauka Publ., 1989, 263 p.

15. Gribanova E.B. Solving the procurement optimization problem by means of inverse computation. *Economic analysis: theory and practice*, 2018, no. 3, pp. 586–596.

Ekaterina B. Gribanova
Candidate of Engineering Sciences, Assistant Professor, Department of Automated Control System, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-36
Email: katag@yandex.ru

ЭЛЕКТРОТЕХНИКА

УДК 621.316.722.1

Н.Н. Цебенко, А.В. Иванов, В.А. Пчельников,
А.А. Правикова, В.М. Рулевский, А.В. Фёдоров

Сравнение вариантов реализации модуля контроля и управления литий-ионных аккумуляторных батарей

Проведено сравнение двух вариантов реализации модуля контроля и управления, предназначенного для работы в составе литий-ионной аккумуляторной батареи.
Ключевые слова: контроль параметров, измерение напряжения, литий-ионная аккумуляторная батарея.
doi: 10.21293/1818-0442-2018-21-2-103-107

В настоящее время литий-ионные аккумуляторные батареи (ЛИАБ) благодаря своим преимуществам широко применяются как в гражданской, так и в военной технике. Основные достоинства ЛИАБ – это высокая удельная емкость и большое количество рабочих циклов. Например, серийно выпускаются ЛИАБ с емкостью до 300 А·ч, а опытные образцы с емкостью 1000 А·ч. Однако, эксплуатация батареи, состоящей из последовательно соединенных элементов на основе Li-ion, имеет ряд особенностей, основная из которых – возможность перегрева в процессе эксплуатации [1].

Аккумуляторная батарея (АБ) состоит из аккумуляторных элементов (АЭ), которые стараются подобрать с достаточно близкими техническими параметрами при изготовлении АБ, а именно токи саморазряда при хранении, скорость деградации материалов электродов, внутреннее сопротивление при зарядно-разрядном цикле и т.д. В силу вышесказанного значения напряжений на элементах аккумуляторной батареи должны быть как можно ближе друг к другу (например, от 3,782 до 3,785 В), однако их заряд возможен с определенной точностью.

АБ на основе литий-ионных аккумуляторных элементов (ЛИАЭ) в силу особенностей электрохимических процессов, протекающих в них, имеют повышенные требования к контролю их параметров в процессе эксплуатации. Неидентичность характеристик ЛИАЭ, необходимых для обеспечения высоких эксплуатационных характеристик АБ, ставит задачу либо повышения требований к технологическому процессу изготовления ЛИАЭ, что ведёт к резкому удорожанию изделий, либо введения в состав ЛИАБ модуля контроля параметров АБ и управления режимом заряда-разряда (МКУ), задачей, которой является контроль напряжения на элементах АБ и выполнение процедуры балансировки в процессе эксплуатации [2].

В процессе эксплуатации батареи, состоящей из соединенных последовательно АЭ, все эти факторы приводят к образованию так называемого «окна» (*DU*), которое равно разности напряжений самого заряженного (U_{max}) и самого разряженного (U_{min}) аккумулятора (рис. 1), т.е. примерно равные напряжения начинают различаться значительно. При увеличении «окна» емкость батареи будет снижаться, так как максимально и минимально допустимые величины напряжений на одном из аккумуляторов будут достигаться раньше, чем полный заряд или разряд всей батареи. В результате расширение «окна» приводит к снижению емкости до недопустимо малой величины.

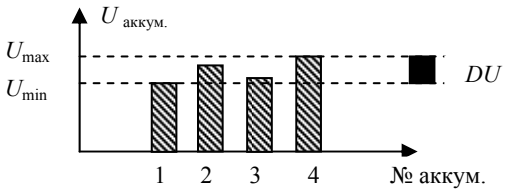


Рис. 1. «Окно» разбаланса, снижающее емкость

В настоящее время в состав аккумуляторных батарей с целью повышения их надежности и продления срока службы вводится электронный блок со схемой контроля параметров аккумуляторов и управления режимом заряда-разряда. Общепринятое название этого блока – модуль контроля и управления (МКУ). В силу особенностей работы литий-ионных аккумуляторов наличие МКУ обязательно, так как при его отсутствии при любых нештатных ситуациях или даже при технологическом разбросе параметров отдельных аккумуляторов в батарее может привести к её перегреву и, даже выходу из строя [3].

Использование МКУ обеспечивает повышение надежности и продление срока эксплуатации АБ за счет выравнивания напряжений на последовательно соединенных аккумуляторных элементах и позволяет использовать АБ с максимальной отдачей по емкости. Данное решение позволяет добиться следующего: повысить безопасность при эксплуатации ЛИАБ, увеличить эффективность зарядно-разрядного цикла, обеспечить выдачу параметров о состоянии батареи в вышестоящие системы или оператору, что значительно повышает эксплуатационные характеристики АБ. Модули контроля и управления могут быть реализованы на различной элементной базе, например на основе специализированных интегральных микросхем, что позволяет получить малые габариты, либо на элементной базе общего назначения, что ведет к увеличению габаритов, но при этом позволяет расширять функциональные возможности [4, 5].

Функциональные требования, предъявляемые к МКУ:

– связь с бортовой центральной вычислительной машиной (БЦВМ);

– контроль напряжений ЛИАЭ и ЛИАБ;

– контроль температуры ЛИАБ;

– балансировка (нивелирование разности напряжения на отдельных ЛИАЭ ЛИАБ);

– анализ текущего состояния параметров ЛИАБ и формирование сигналов запрета / разрешения для управления процессами безопасного заряда / разряда батареи [6, 7].

Дополнительными требованиями, характерными для изделий военной и космической техники, являются надёжность и, в частности, сохранение работоспособности при отказе одного или нескольких радиоэлектронных компонентов (РЭК). Для выполнения требований по отказоустойчивости, надежности и безопасности необходимо дублирование подсистем изделия [8].

Таким образом, исходя из приведённого выше перечня требований к МКУ, можно выделить несколько основных подсистем, которые при проектировании в силу их функциональных особенностей также будут выполнены отдельным модулем [9, 10]. В частности, такими подсистемами могут быть:

– контроль напряжения – модуль измерения напряжения (МИН);

– контроль температуры – модуль измерения сопротивления (МИС);

– балансировка – модуль коммутации балансировочных резисторов (МКБР);

– связь с центральной вычислительной машиной – модуль контроллера (МК).

К изделиям космического назначения часто предъявляется противоречивое требование высокой надежности и минимальной массы. Основным способом повышения надежности является резервирование. Применение резервирования обычно связано с увеличением массы, объема, стоимости изготовления. Для получения оптимальных массогабаритных показателей применяются различные способы резервирования: нагруженный, ненагруженный, облегченный резерв. В зависимости от конкретных условий резервироваться могут системы, модули или отдельные элементы [11].

Для измерительных модулей, кроме требований погрешности измерения, также появляется требование оценки достоверности измерений. Данное требование, при условии парирования неисправности любого РЭК в тракте измерения, можно обеспечить выполнением устройства контроля по мажоритарной схеме [12].

Структура преобразования информации по мажоритарной схеме в общем случае приведена на рис. 2. Такая схема применяется в системах с нагруженным резервом, где 1, 2, …, n – одинаковые устройства преобразования информации, работающие параллельно (n – общее число элементов); О – мажоритарный орган [13]; X_1, X_2, X_n – измеряемые величины; Y_1, Y_2, Y_n – сигналы от устройств 1, 2, 3; Y – выдаваемый во внешнюю цепь сигнал, равный большинству сигналов от измерителей.

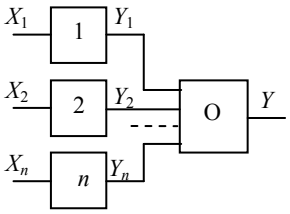


Рис. 2. Схема мажоритарного резервирования в общем виде

Данный вариант резервирования принято называть методом «голосования большинством». Очевидным является то, что для его корректной работы число обрабатываемых параллельных измерительных цепей должно быть не менее трех.

На рис. 3, вариант 1, приведен частный случай реализации указанного метода, где A_1 – контроллер МКУ на базе микропроцессорного устройства; B_1, B_2 и B_3 – идентичные каналы измерения напряжений ЛИАЭ и ЛИАБ.

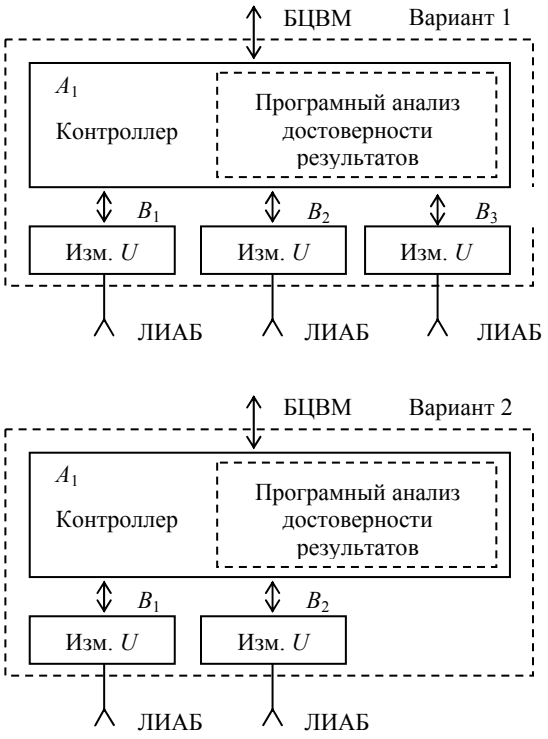


Рис. 3. Варианты реализации системы измерения напряжения

В данном случае анализ достоверности результатов измерений напряжений ЛИАБ по трём массивам выполняется реализацией программного мажоритара одноимённых параметров. Истинным значением принимается:

– среднее значение трёх измеренных значений при условии, что их три попарные разности не превышают величины, принятой за допуск;

– среднее значение двух измеренных значений наиболее близких друг другу, при условии, что одна из трёх попарных разностей превышает величину, принятую за допуск;

– среднее значение двух измеренных значений, наиболее близких друг другу, при условии, что две из трёх попарных разностей превышает величину, принятую за допуск;

– прочее принимается как неисправность подсистемы измерения напряжения.

Таким образом, при принятии решения достоверности результата измерения используются три аппаратных канала измерения, три массива измеренных значений, дополнительный критерий допуска, мера, обусловленная собственной погрешностью каналов измерения, и контроллер с ПО в качестве мажоритарного элемента.

Так как для изделий космического применения лимитирующим фактором является масса, то целесообразно оптимизировать способ резервирования. Учитывая тот факт, что объектом контроля является ЛИАБ, характеристики которой заранее и достаточно точно известны, то можно проводить проверку достоверности измерений, основываясь на свойствах ЛИАБ.

В качестве дополнительных критериев оценки достоверности результатов измерения можно использовать следующие свойства ЛИАБ:

– сумма напряжений всех ЛИАЭ равна полному напряжению ЛИАБ (с учётом погрешности измерения и падений напряжений на токопроводящих соединителях ЛИАЭ одной ЛИАБ);

– напряжения ЛИАЭ находятся в определённом диапазоне;

– полное напряжение ЛИАБ находится в определённом диапазоне;

– при наличии тока заряда или разряда падение напряжения на внутреннем сопротивлении ЛИАЭ вносит равные погрешности как в измеряемые напряжения ЛИАЭ, так и в измеряемое напряжение ЛИАБ, и его можно не учитывать.

Исходя из вышеприведённого, подсистему контроля напряжений ЛИАЭ и ЛИАБ можно реализовать в виде, приведённом на рис. 1, вариант 2, с использованием двух каналов измерения (B_1, B_2).

Соответственно подсистема измерения напряжения МКУ может быть выполнена двухканальной, состоящей из основного и резервного каналов. Причём каждый канал выполняет как поэлементный контроль напряжений, так и контроль напряжения всей ЛИАБ. Результат измерений подвергается анализу на соответствие приведённым выше особенностям ЛИАБ, на основании чего принимается решение о исправности каналов. По умолчанию МКУ в качестве результата измерения предоставляет данные по основному каналу измерения.

Таким образом, при принятии решения достоверности результата измерения используются два аппаратных канала измерения, два массива измеренных значений, дополнительный критерий на основе свойств ЛИАБ и контроллер с ПО в качестве устройства принятия решения.

Сравнение различных способов реализации системы измерения напряжения представлено в таблице.

Различные способы реализации системы измерения напряжения

№ п/п	МКУ (мажоритар)	МКУ (на основе свойств ЛИАБ)
1	Три канала измерения напряжений ЛИАЭ и ЛИАБ	Два канала измерения напряжений ЛИАЭ и ЛИАБ
2	Контроллер (программный анализ достоверности результата измерений – мажоритар)	Контроллер (программный анализ достоверности результата измерений – на основе свойств ЛИАБ)

Проведем сравнение надежности двух способов реализации подсистемы измерения напряжения. Понятие резервирования будем определять согласно [14].

Вариант 1. Мажоритарное резервирование (с дробной кратностью, при которой два и более однотипных элементов резервируются одним и более резервными элементами) [15].

Вероятность безотказной работы мажоритарной системы при условии, что все элементы имеют одинаковую надежность [14], находится по формуле

$$P_1(t)=\sum_{i=0}^{m} C_n^i \cdot Q^i(t)\cdot P^{n-i}(t)= \\ =P^3(t)+3\cdot(1-P(t))\cdot P^2(t)=3\cdot P^2(t)-2\cdot P^3(t), \quad (1)$$

где m – количество резервных элементов; n – общее число элементов; C_n^i – биномиальный коэффициент из n по i; $P(t)$ – вероятность безотказной работы i-го элемента; $Q(t)$ – вероятность отказа i-го элемента

Вариант 2. Нагруженный резерв.

Вероятность безотказной работы системы с постоянно включенным резервом при условии, что все элементы имеют одинаковую надежность [3], находится по формуле

$$P_2(t)=1-(1-P(t))^{m+1}=1-(1-P(t))^2=2\cdot P(t)-P^2(t),$$

где m – количество резервных элементов; $P(t)$ – вероятность безотказной работы i-го элемента.

Рассчитаем отношение вероятностей безотказной работы (Δ_P) первого варианта относительно второго: следовательно, $P_1 < P_2$.

$$\Delta_P=\frac{P_1}{P_2}=\frac{2P\cdot(P-1{,}5)}{P-2}<1 \quad \text{при} \quad 0<P<1.$$

Проведем сравнение массы двух способов реализации подсистемы измерения напряжения. Оценку будем производить на конкретном примере. На рис. 4 приведен пример реализации подсистемы измерения напряжения по варианту 1, соответственно при реализации по варианту 2 система будет содержать на один элемент ИЗ меньше. В обоих вариантах $И_i$ – измеритель, а ПП – обязательная для их нормального функционирования подсистема питания. Ориентировочные размеры на рис. 4 указаны в миллиметрах.

Для данного сравнения сделаем следующие допущения: измерители и подсистема питания имеют одинаковую удельную массу, масса пропорциональна площади, занимаемой на печатной плате, подсис-

тема питания остается неизменной. Из рисунка видно, что площадь, занимаемая подсистемой питания, составляет около 35% от площади, занимаемой измерителем. Таким образом, масса варианта 1 будет равна

$$M_1 = 3M_0 + 0{,}35M_0 .$$

Масса варианта 2 будет равна:

$$M_2 = 2M_0 + 0{,}35M_0 ,$$

где M_0 – масса измерителя.

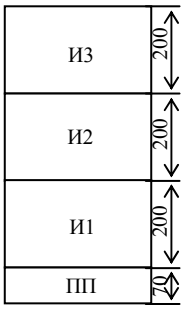


Рис. 4. Компоновка подсистемы измерения по варианту 1

Определим выигрыш по массе при втором способе реализации, для чего рассчитаем отношение масс (Δ_M) варианта 2 относительно варианта 1:

$$\Delta_M = \frac{M_2}{M_1} = \frac{2{,}35M_0}{3{,}35M_0} = 0{,}7 .$$

Таким образом, выигрыш в массе составляет 30%.

Вывод. Реализация подсистемы измерения на основе свойств ЛИАБ в сравнении с мажоритарным способом будет иметь следующие преимущества: содержит меньшее количество элементов, обладает большей надежностью и обеспечивает выигрыш по массе 30%.

Литература

1. Рыкованов А. Система баланса Li-ion аккумуляторных батарей // Силовая электроника. – 2009. – №1. – С. 52–55.

2. Хромов А. В. Литий-ионные аккумуляторные батареи низкоорбитальных космических аппаратов // Вопросы электромеханики. – М., 2016. – Т. 152. – С. 20–28.

3. Hannana M.A., Lipub M.S.H., Hussainb A., Mohamedb A. A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: Challenges and recommendations// Renewable and Sustainable Energy Reviews. – October 2017. – Vol. 78. – PP. 834–854.

4. Варламов Д.О., Яблочкин С.И., Еременко В.Г. Устройство выравнивания напряжения на ячейках Li-Ion аккумуляторной батареи и его моделирование в программе P-Spice // Матер. междунар. науч.-техн. конф. ААИ «Автомобиле- и тракторостроение в России: приоритеты развития и подготовка кадров», посвященной 145-летию МГТУ «МАМИ». – М., 2012. – С. 9–14.

5. Moore S., Schneider P. A Review of Cell Equalization Methods for Lithium Ion and Lithium Polymer Battery Systems // SAE Technical Paper 2001-01-0959. – 2001.

6. Ouyang Q., Chen J. Optimal Cell-to-Cell Balancing Topology Design for Serially Connected Lithium-Ion Battery Packs // IEEE transactions on sustainable energy. – 2018. – Vol. 1. – PP. 350–360.

7. Ouyang Q., Chen J., Zheng J., Hong Y. SOC Estimation-Based Quasi-Sliding Mode Control for Cell Balancing in Lithium-Ion Battery Packs // IEEE transactions on industrial electronics. – 2018. – Vol. 4. – PP. 3427–3436.

8. Белоножко П.П. Космическая роботехника. Современное состояние, перспективные задачи, тенденции развития. Аналитический обзор // Наука и образование / МГТУ им. Н. Э. Баумана. – М., 2016. – С. 110–153.

9. Dong-Hua Zhang, Guo-Rong Zhu, Shao-Jia He et al. Balancing Control Strategy for Li-Ion Batteries String Based on Dynamic Balanced Point// Energies. – 2015. – Vol. 8. – PP. 1830–1847.

10. Yusof M.S., Toha S.F., Kamisan N.A. et al. Battery Cell Balancing Optimisation for Battery Management System // International Conference on Mechanical, Automotive and Aerospace Engineering. – 2016.

11. Цебенко Н.Н., Иванов А.В., Ракитин Г.А. и др. Модуль контроля и управления для литий-ионных аккумуляторных батарей // Актуальные вопросы проектирования автоматических космических аппаратов для фундаментальных и прикладных научных исследований. – Вып. 2. – Химки, 2017. – С. 484–491.

12. Половко А.М. Основы теории надежности: практикум / А.М. Половко, С.В. Гуров. – СПб.: БХВ-Петербург, 2006. – 560 с.

13. Иыуду К.А. Надежность, контроль и диагностика вычислительных машин и систем: учеб. пособие для вузов по спец. «Вычислительные машины комплексы, системы и сети». – М.: Высш. шк., 1989. – 216 с.

14. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения.

15. Денисенко В. Аппаратное резервирование в промышленной автоматизации. – Ч. 1 // Современные технологии автоматизации. – 2008. – № 2. – С. 90–99.

Цебенко Николай Николаевич
Зав. лаб. НИИ автоматики и электромеханики
(НИИ АЭМ) ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 55-61-96 доб. 13-06
Эл. почта: tnn@niiaem.tomsk.ru

Иванов Александр Валериевич
Вед. инж. НИИ АЭМ ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 56-37-46
Эл. почта: ivanovnii@sibmail.com;

Пчельников Виктор Алексеевич
Зам. директора по НР НИИ АЭМ ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 56-00-59
Эл. почта: pchelnikov@niiaem.tomsk.ru

Правикова Александра Александровна
Мл. науч. сотр. НИИ АЭМ ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 55-61-96
Эл. почта: bezruchenko@niiaem.tomsk.ru

Рулевский Виктор Михайлович
Канд. техн. наук, директор НИИ АЭМ ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 55-61-96
Эл. почта: rulevsky@niiaem.tomsk.ru

Фёдоров Александр Владимирович
Зав. лаб. НИИ АЭМ ТУСУРа
Белинского ул., 53, г. Томск, Россия, 634034
Тел.: +7 (382-2) 55-56-80
Эл. почта: fedorov@niiaem.tomsk.ru

Tsebenko N.N., Ivanov A.V., Pcelnikov V.A.,
Pravikova A.A., Rulevskiy V.M., Fedorov A.V.

Comparison of the implementation options of the module for monitoring and controlling lithium-ion batteries

The article compares two versions of the monitoring and control module, intended for operation as a part of a lithium-ion battery.

Keywords: parameter control, voltage measurement, lithium-ion rechargeable battery.
doi: 10.21293/1818-0442-2018-21-2-103-107

References

1. Rykovanov A. Sistema balansa Li-ion akkumulyatornykh batarey. [Balancing system for Li-ion rechargeable batteries] *Silovaya elektronika*, vol. 1, 2009, pp. 52–55 (In Russ.).

2. Khromov A.V. Lithium-ion batteries of low-orbit spacecraft. [Litiy-ionnye akkumulyatornye batarei nizkoorbitalnykh kosmicheskikh apparatov] *Voprosy elektromekhaniki*, 2016, vol. 152, pp. 20–28 (In Russ.).

3. Hannana M.A., Lipub M.S.H., Hussainb A., Mohamedb A. A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: Challenges and recommendations. *Renewable and Sustainable Energy Reviews,* October 2017, vol. 78, pp. 834–854.

4. Varlamov D.O., Yablochkin S.I., Eremenko V.G. Ustroystvo vyravnivaniya napryazheniya na yacheykakh Li-Ion akkumulyatornoy batarei i ego modelirovanie v programme P-Spice. [Device for voltage equalization on cells of Li-Ion battery and its simulation in P-Spice program] *Avtomobile i traktorostroenie v Rossii: prioritety razvitiya i podgotovka kadrov: materialy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii AAI, posvyashchennoy 145-letiyu MGTU «MAMI»*, 2012, pp. 9–14 (In Russ.).

5. Moore S., Schneider P. A Review of Cell Equalization Methods for Lithium Ion and Lithium Polymer Battery Systems. *SAE Technical Paper* 2001-01-0959, 2001.

6. Ouyang Q., Chen J. Optimal Cell-to-Cell Balancing Topology Design for Serially Connected Lithium-Ion Battery Packs. *IEEE transactions on sustainable energy*, 2018, vol. 1, pp. 350–360.

7. Ouyang Q., Chen J., Zheng J., Hong Y. SOC Estimation-Based Quasi-Sliding Mode Control for Cell Balancing in Lithium-Ion Battery Packs. *IEEE transactions on industrial electronics*, 2018, vol. 4, pp. 3427–3436.

8. Belonozhko P.P. Kosmicheskaya robotekhnika. Sovremennoe sostoyanie, perspektivnye zadachi, tendentsii razvitiya. Analiticheskii obzor. [Space robotics. Current state, long-term tasks, development trends. Analytical review] *Nauka i* obrazovanie*. MGTU im. N. E. Baumana*, Moscow, 2016, pp. 110–153 (In Russ.).

9. Dong-Hua Zhang, Guo-Rong Zhu, Shao-Jia He, Shi Qiu, Yan Ma, Qin-Mu Wu, Wei Chen. Balancing Control Strategy for Li-Ion Batteries String Based on Dynamic Balanced Point, *Energies*, 2015, vol. 8, pp. 1830–1847.

10. Yusof M.S., Toha S.F., Kamisan N.A., Hashim W.N., Abdullah A. Battery Cell Balancing Optimisation for Battery Management System. *International Conference on Mechanical, Automotive and Aerospace Engineering*, 2016.

11. Tsebenko N.N., Ivanov A.V., Rakitin G.A., Rulevskii V.M., Fedorov A.V. Modul kontrolya i upravleniya dlya litii-ionnykh akkumulyatornykh batarei. [Control and management module for lithium-ion batteries] *Aktualnye voprosy proektirovaniya avtomaticheskikh kosmicheskikh apparatov dlya fundamentalnykh i prikladnykh nauchnykh issledovanii*, Khimki, 2017, vol. 2, pp. 484–491 (In Russ.).

12. Polovko A.M. *Osnovy teorii nadezhnosti. Praktikum* [Fundamentals of the reliability theory]. A.M. Polovko, S.V. Gurov, SPb.: BKhV-Peterburg, 2006 (In Russ.).

13 Iyudu K. A. *Nadezhnost, kontrol i diagnostika vychislitelnykh mashin i sistem: Ucheb. posobie dlya vuzov po spets. «Vychislitelnye mashiny kompleksy, sistemy i seti».* [Reliability, control and diagnostics of computers and systems]. M.: Vyssh. shk., 1989 (In Russ.).

14. GOST 27.002-89. *Nadezhnost v tekhnike. Osnovnye ponyatiya. Terminy i opredeleniya.* [Reliability in techniques. Basic concepts. Terms and Definitions] (In Russ.).

15. Denisenko V. Apparatnoe rezervirovanie v promyshlennoi avtomatizatsii. Vol. 1 [Hardware redundancy in industrial automation] *Sovremennye tekhnologii avtomatizatsii*, 2008, vol. 2, pp. 90–99.

Nikolai N. Tsebenko
Head of laboratory, NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone: +7 (382-2) 55-61-96 dob. 1306
Email: tnn@niiaem.tomsk.ru

Aleksandr V. Ivanov
Lead Engineer, NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone: +7 (382-2) 56-37-46
Email: ivanovnii@sibmail.com

Viktor A. Pchelnikov
Vice director NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone: +7 (382-2) 56-00-59
Email: pchelnikov@niiaem.tomsk.ru

Aleksandra A. Pravikova
Junior researcher, NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone.: +7 (382-2) 55-61-96
Email: bezruchenko@niiaem.tomsk.ru

Viktor M. Rulevskii
PhD, Director, NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone: +7 (382-2) 55-61-96
Email: rulevsky@niiaem.tomsk.ru

Aleksandr V. Fedorov
Head of laboratory, NII AEM TUSUR
53, Belinskogo st., Tomsk, Russia, 634034
Phone: +7 (382-2) 55-56-80
Email: fedorov@niiaem.tomsk.ru

УДК 621.314

А.В. Осипов, И.С. Шемолин, А.А. Лопатин, Р.А. Латыпов

Двунаправленный вольтодобавочный преобразователь с мягким переключением для систем электропитания

Рассмотрен двунаправленный вольтодобавочный преобразователь с активным выпрямителем для заряда-разряда аккумулятора систем электропитания космических аппаратов. Рассмотрены коммутационные процессы, показано, что в вольтодобавочном преобразователе за счет двуполярного тока сглаживающего дросселя формируется интервал рекуперации, обеспечивающий предварительный разряд паразитных емкостей транзисторов инвертора и их включение при нуле напряжения, т.е. в режиме ZVS. Установлено, что из-за уменьшения амплитуды пульсаций тока дросселя мягкая коммутация обеспечивается в узком диапазоне регулирования, что не является удовлетворительным. Показано, что диапазон мягкой коммутации может быть существенно расширен за счет подстройки частоты преобразования по условию появления интервала рекуперации. Проведены расчеты, определено, что при единичном коэффициенте трансформации и при отсутствии завышения индукции трансформатора предельный диапазон ZVS может достигать 80% от максимального. Рассмотрен режим заряда аккумулятора, показано, что большое значение отрицательного тока дросселя приводит к коммутационным выбросам напряжения при выключении транзисторов выпрямителя, устранить которые можно включением дополнительных снабберных конденсаторов. Проведена экспериментальная проверка полученных результатов, сделаны выводы, обсуждены полученные результаты.

Ключевые слова: система электропитания, вольтодобавочный преобразователь, мягкая коммутация.
doi: 10.21293/1818-0442-2018-21-2-108-117

Современные системы электропитания (СЭП) непременно содержат аккумуляторную батарею (АБ), обеспечивающую питание нагрузки постоянным напряжением при отсутствии энергии основного источника. В СЭП космических аппаратов силовой преобразователь, преобразующий энергию АБ, как правило, выполняется на основе схемы непосредственного повышающего преобразователя с дополнительным каскадом ограничения выходного тока. Увеличение мощности систем электропитания повышает требования к энергетическим характеристикам преобразователя, важнейшей из которых является КПД. В этой связи вольтодобавочные преобразователи более эффективны, так как высокочастотному преобразованию подвергается лишь часть потока энергии входного источника.

Анализ таких преобразователей наиболее полно проведен в работах [1–4]. Однако жесткое переключение транзисторов, сопровождаемое большими динамическими потерями, требует формирования режимов работы, обеспечивающих включение транзисторов при нуле напряжения (режим ZVS). Мягкое переключение может быть достигнуто применением демпфирующих цепей, как активных, так и пассивных [5]. Однако передача энергии коммутации транзисторов в нагрузку лишь вызывает дополнительные потери. Другим вариантом является применение резонансных преобразователей, ток которых изменяется по синусоидальному закону [6–7], что создает условия для мягкого включения. Однако наличие дополнительных реактивных элементов, образующих резонансный контур, увеличивает массу преобразователя.

Учитывая, что реализация мягкой коммутации, как правило, связана с обеспечением отрицательного тока транзистора при его включении, авторы стремятся создать эти условия с минимальными затратами, максимально используя электромагнитные элементы, уже присутствующие в схеме преобразователя. Возможно использование энергии намагничивания силового трансформатора для включения при нулевом напряжении [8], применение коммутирующего дросселя в двухтактном повышающем преобразователе [9], а также формирование интервалов рекуперации тока самого сглаживающего дросселя [10], в последнем случае необходим активный выпрямитель. Последний способ представляется наиболее эффективным, так как вообще не требует дополнительных элементов, хотя большая переменная составляющая тока и вызывает дополнительные потери.

Таким образом, целью настоящей работы является исследование характеристик вольтодобавочного преобразователя с активным выпрямителем в режиме двуполярного тока сглаживающего дросселя и определение условий мягкого включения транзисторов.

Вольтодобавочный преобразователь в режиме двуполярного тока сглаживающего дросселя

Рассматриваемый преобразователь состоит из инвертора и активного выпрямителя, соединенных по вольтодобавочной топологии и образующих высокочастотное звено, преобразующее часть потока энергии, необходимую для формирования требуемого выходного напряжения [11, 12] (рис. 1). При таком построении преобразователя выходное напряжение является суммой входного напряжения и добавленного регулируемого напряжения высокочастотного звена. Для реализации режима ограничения выходного тока при перегрузках или коротком замыкании в структуру преобразователя вводится дополнительный каскад, не показанный на рис. 1.

Регулирование напряжения преобразователя основано на фазовом сдвиге управляющих импуль-

сов транзисторов регулируемой стойки инвертора *VT*3, *VT*4 относительно нерегулируемой *VT*1, *VT*2, при этом управление транзисторами выпрямителя формируется логическим сложением управляющих импульсов диагоналей инвертора. Формирование такого управления приводит к появлению на такте управления двух интервалов – интервала вольтодобавки, при котором на вход *LC*-фильтра поступает напряжение $2U_{АБ}$, и интервала непосредственного соединения (закоротки) АБ с *LC*-фильтром.

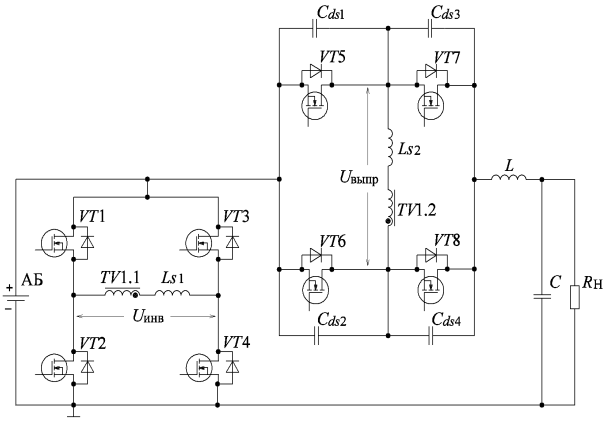


Рис. 1. Двунаправленный вольтодобавочный преобразователь

Реализация выпрямителя на активных ключах позволяет исключить режим прерывистого тока и линеаризовать регулировочную характеристику во всем диапазоне изменения нагрузки

$$U_{вых} = U_{АБ} \cdot \left(1 + \frac{\gamma}{K_{тр}}\right).$$

При стабилизации выходного напряжения и $K_{тр}$=1, что применимо для большинства АБ, можно связать напряжение АБ с длительностью импульсов выходного напряжения инвертора

$$\sigma U_{АБ} = \frac{U_{АБ}}{U_{вых}} = \frac{1}{1+\gamma}. \qquad (1)$$

Работа преобразователя в режиме однополярного тока дросселя и его характеристики подробно рассмотрены в [11]. Однако в режиме двуполярного тока дросселя коммутационные процессы имеют ряд особенностей, так как появляется интервал отрицательного значения тока дросселя. Исследованы коммутационные процессы в преобразователе. Диаграммы работы представлены на рис. 2, для каждого интервала, указанного на диаграммах, приведены контуры протекания тока, показанные на рис. 3.

На интервале вольтодобавки (t_0 – t_1) открыты транзисторы инвертора *VT*1, *VT*4 и транзисторы выпрямителя *VT*6, *VT*7, что обеспечивает вольтодобавку к входному напряжению и рост тока сглаживающего дросселя (см. рис. 3, *а*). В момент времени t_1 выключается транзистор *VT*1, что приводит к окончанию интервала вольтодобавки. Подробно интервал t_1 – t_2 показан на рис. 2, *б*. После выключения транзистора *VT*1 ток трансформатора I_{TV} продолжает протекать в прежнем направлении за счет наличия индуктивности рассеяния трансформатора *Ls*1. Происходит перезаряд паразитных емкостей транзисторов регулируемой стойки инвертора, после чего отпирается обратный диод транзистора *VT*2. При нулевом напряжении инвертора $U_{инв} = 0$, напряжение выпрямителя $U_{выпр}$ сохраняет потенциал за счет *Ls*2. Поэтому ток трансформатора I_{TV}, продолжая протекать в прежнем направлении (в нагрузку), уменьшается. Появление разности между током дросселя и током трансформатора приводит к протеканию разрядного тока через снабберные конденсаторы *Cds*1, *Cds*4:

$$I_{VT7} + I_{Cds4} = I_L,$$
$$I_{VT7} - I_{Cds4} = I_{TV},$$

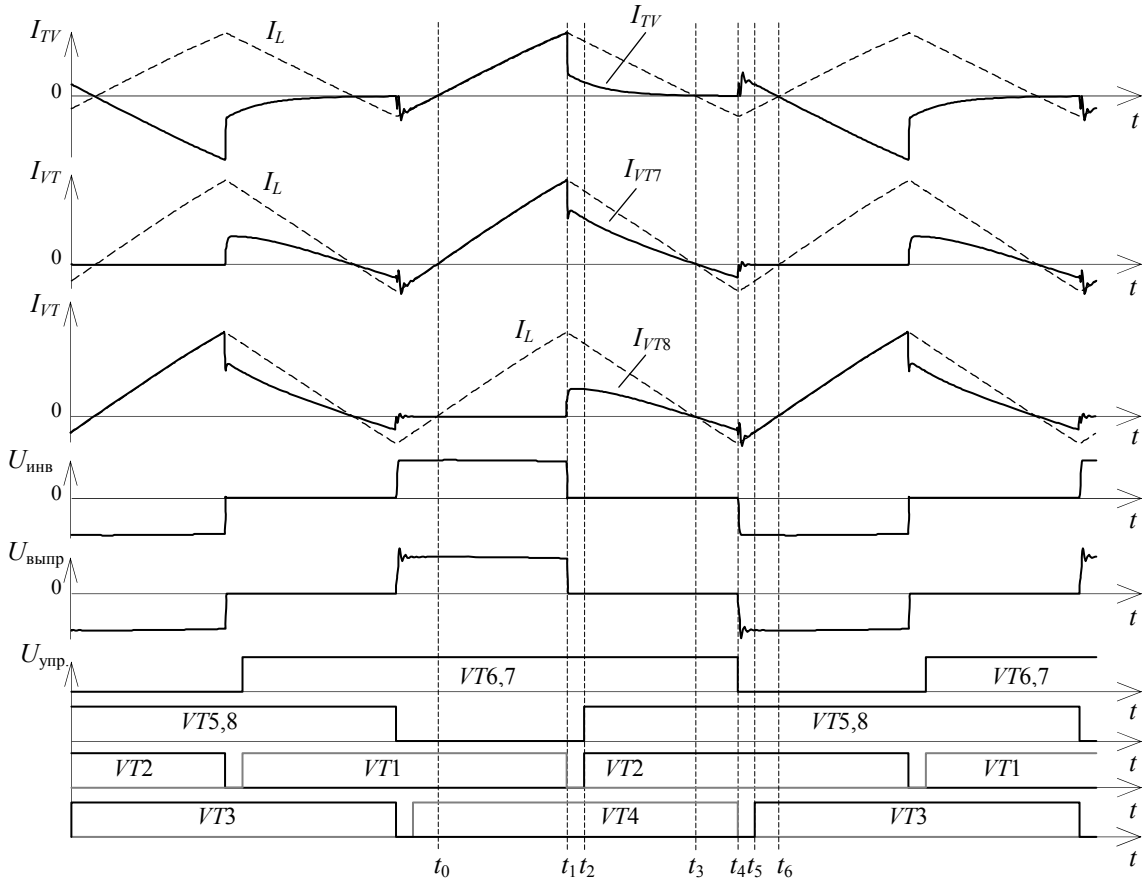
т.е. происходит перераспределение тока дросселя между транзистором *VT*7 и *Cds*4. Энергия конденсаторов *Cds*2, *Cds*4 и энергия *Ls*2 передается в нагрузку. После полного разряда конденсаторов открываются обратные диоды транзисторов *VT*5, *VT*8 и напряжение выпрямителя становится равным нулю $U_{выпр} = 0$. Пропадает условие уменьшения тока трансформатора, и оставшийся ток трансформатора медленно спадает за счет активных потерь (см. рис. 2, *а*):

$$I_{VT7} + I_{VT8} = I_L,$$
$$I_{VT7} - I_{VT8} = I_{TV}.$$

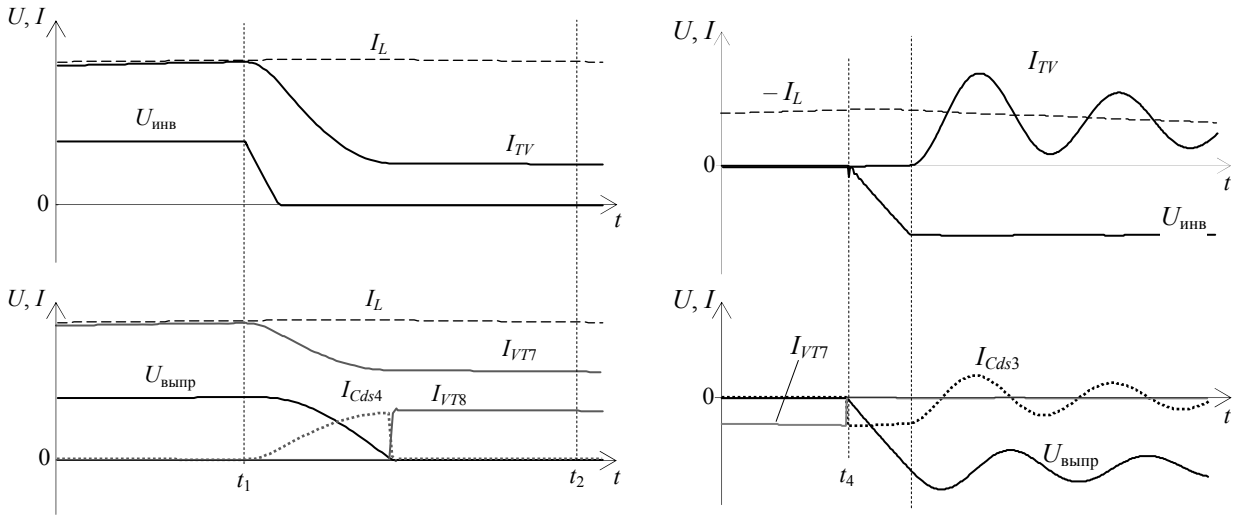
т.е. ток трансформатора некоторое время продолжает протекать в прежнем направлении, создавая разницу между токами транзисторов *VT*7 и *VT*8, после чего ток дросселя делится поровну между транзисторами $I_{VT7} = I_{VT8} = I_L/2$ (см. рис. 2, *а*). Процесс разряда конденсаторов *Cds*1, *Cds*4 должен закончиться на интервале коммутационной паузы до момента t_2, тогда включение транзисторов выпрямителя *VT*5, *VT*8 будет происходить при нуле напряжения, т.е. при ZVS.

После разряда снабберных конденсаторов преобразователь переходит в состояние закоротки (см. рис. 3, *в*). Обмотки трансформатора закорачиваются, и на вход *LC* фильтра подается входное напряжение, за счет чего ток сглаживающего дросселя уменьшается. В момент времени t_3 ток сглаживающего дросселя меняет направление и преобразователь переходит в состояние рекуперации энергии (см. рис. 3, *г*). Транзисторы инвертора *VT*2, *VT*4 по-прежнему открыты, но ток I_{TV} по ним уже не протекает. В момент времени t_4 происходит одновременное запирание транзистора инвертора *VT*4 и транзисторов выпрямителя *VT*6, *VT*7. Процесс выключения *VT*6, *VT*7 демпфируется снабберными конденсаторами *Cds*2, *Cds*3. Это приводит к росту тока трансформатора и отпиранию этим током обратного диода транзистора *VT*3 (см. рис. 3, *д*), что гарантирует его мягкое включение в момент t_5 (см. рис. 3, *е*). Важно, что для мягкого включения *VT*3 условие отрицательного тока дросселя является необходимым (положительный ток дросселя просто откроет обратные диоды выключаемых транзисторов выпрямителя). Более подробно момент t_4 рассмотрен на рис. 2, *в*.

Выключение транзисторов *VT*6, *VT*7 приводит к непосредственной коммутации дросселя с трансформатором, имеющим индуктивность рассеяния *Ls*2. Разница токов дросселя и трансформатора (на момент коммутации $I_{TV} = 0$) делает необходимым включение параллельно транзисторам выпрямителя снабберных конденсаторов, обеспечивающих протекание тока дросселя в момент коммутации. Ток транзистора *VT*7 полностью перехватывается конденсатором *Cds*3, обеспечивая уменьшение потерь при выключении, напряжение выпрямителя $U_{выпр}$ начинает расти. Соответственно растет и напряжение инвертора $U_{инв}$, происходит перезаряд паразитных емкостей нерегулируемой стойки инвертора *VT*3, *VT*4 (на диаграммах рис. 2, *в* ток перезаряда незначителен, поэтому $I_{TV} = 0$).



а – полный период работы при γ = 0,5



б – момент включения транзисторов выпрямителя

в – момент выключения транзисторов выпрямителя

Рис. 2. Диаграммы работы вольтодобавочного преобразователя в режиме двуполярного тока сглаживающего дросселя

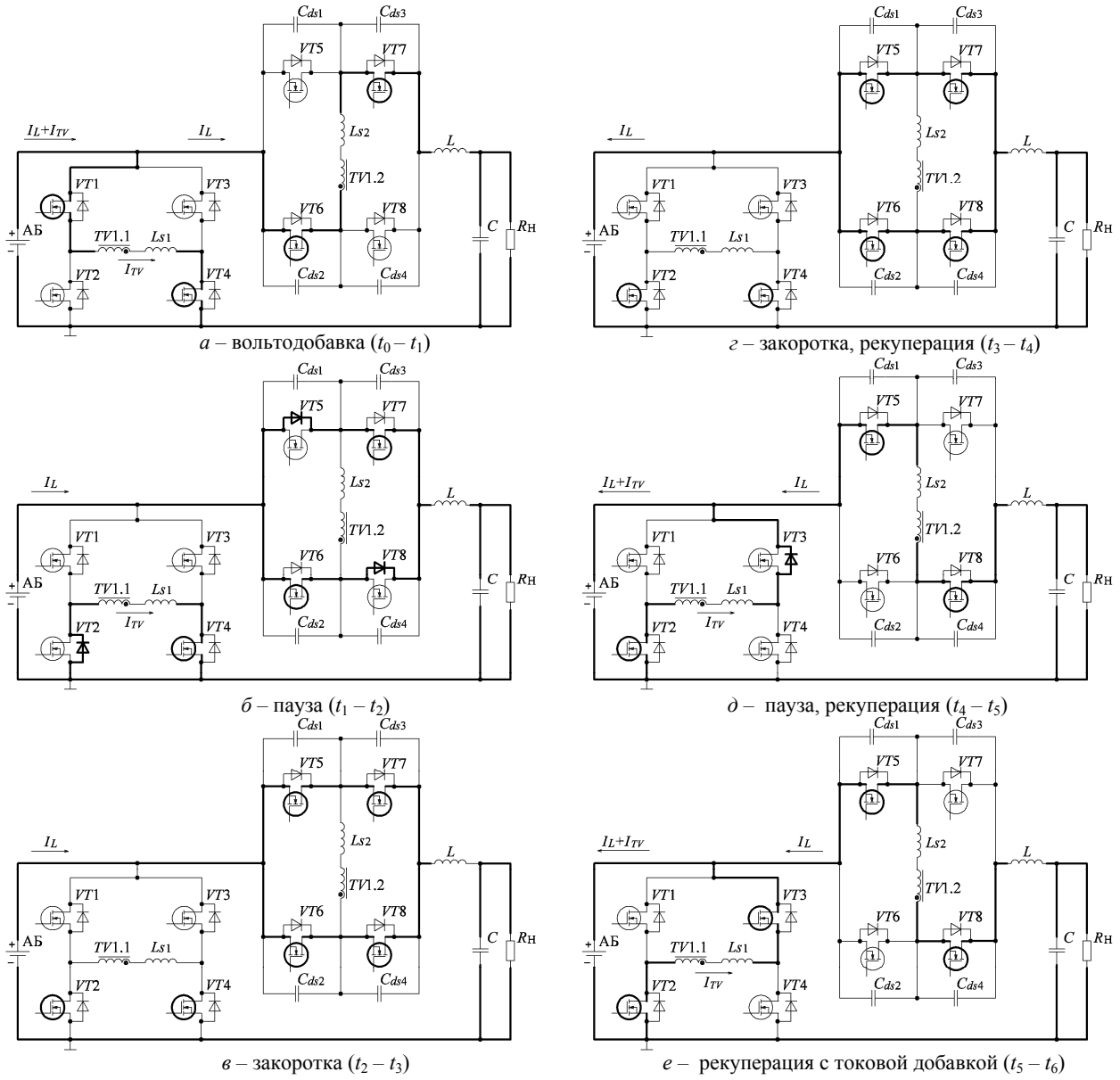


Рис. 3. Контуры протекания тока в вольтодобавочном преобразователе в режиме двуполярного тока сглаживающего дросселя

После достижения напряжением инвертора входного напряжения $U_{инв} = U_{АБ}$ открывается обратный диод транзистора *VT*3 и начинается рост тока рекуперации через трансформатор. Учитывая наличие индуктивности рассеяния трансформатора, рост его тока вызывает перенапряжение на транзисторах выпрямителя, определяемое величиной емкости конденсаторов *Cds*2, *Cds*3. Далее инициируется затухающий колебательный процесс между *Ls*2 и конденсаторами *Cds*2, *Cds*3, который происходит при открытом обратном диоде транзистора *VT*3 и не мешает его мягкому включению.

Начиная с момента времени t_4, преобразователь находится в режиме рекуперации с токовой добавкой, (так как $I_{АБ}=I_L+I_{TV}$), выпрямитель на этом интервале работает как инвертор тока. Это приводит к увеличению напряжения на входе *LC* фильтра, под действием которого отрицательный ток дросселя начинает спадать, включение *VT*3 в момент t_5 не меняет контуров протекания тока. В момент времени t_6 ток дросселя меняет направление на положительное и преобразователь переходит в режим вольтодобавки, далее процессы повторяются.

Таким образом, коммутационные процессы в инверторе и выпрямителе различны, так как первый является преобразователем напряжения, а второй – преобразователем тока, что требует включения снабберных конденсаторов. Интервал отрицательного тока дросселя позволяет обеспечить мягкое включение транзисторов нерегулируемой стойки инвертора *VT*3, *VT*4. В результате включение всех транзисторов преобразователя происходит в нуле напряжения при открытом обратном диоде, т.е. в режиме ZVS.

Вольтодобавочный преобразователь при изменении нагрузки и в режиме заряда аккумулятора

Уменьшение нагрузки преобразователя приводит к уменьшению постоянной составляющей тока дросселя и как следствие увеличению интервала рекуперации. В предельном случае на холостом ходу постоянная составляющая тока дросселя равна нулю, а интервалы прямой передачи энергии $t_{пп}$ и рекуперации энергии $t_{рек}$ равны $t_{пп}=t_{рек}$, также, как и равны интервалы вольтодобавки $t_{вд}$ и токовой добавки $t_{тд}$, т.е. $t_{вд}=t_{тд}$ (рис. 4). Соответственно активная составляющая мощности отсутствует.

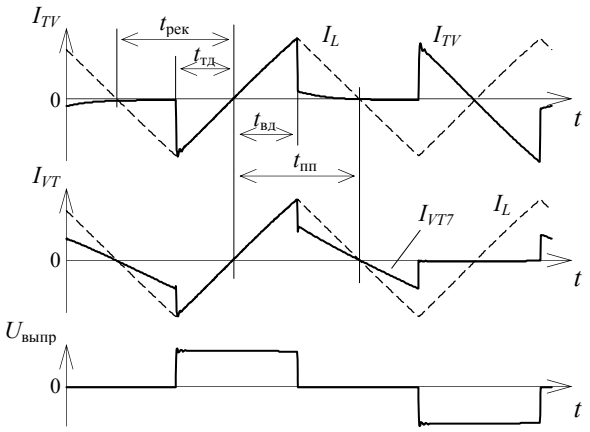


Рис. 4. Диаграммы работы вольтодобавочного преобразователя на холостом ходу при γ = 0,5

При избытке энергии солнечной батареи питание нагрузки осуществляется преобразователем солнечной энергии, появление напряжения внешнего источника на выходе двунаправленного преобразователя создает условия для его перехода в режим заряда АБ, диаграммы работы показаны на рис. 5. Управление преобразователем в режиме заряда ничем не отличается от режима разряда, изменяются только длительности интервалов. В режиме заряда интервал рекуперации превышает интервал прямой передачи $t_{рек} > t_{пп}$, что и определяет отрицательное направление передачи энергии. Соответственно интервал токовой добавки $t_{тд}$ также превышает интервал вольтодобавки $t_{вд}$, так как длительности интервалов связаны соотношением

$$\gamma = \frac{t_{тд}}{t_{рек}} = \frac{t_{вд}}{t_{пп}}.$$

На интервале токовой добавки $t_{тд}$ ток АБ является суммой тока дросселя и тока выпрямителя, а на интервале закорачивания $(t_{рек} - t_{тд})$ ток АБ равен току дросселя, поэтому при $K_{тр}$=1 зарядный ток можно выразить соотношением

$$I_{АБ} = I_L\left(1+\gamma\right).$$

Можно сказать, что в режиме заряда АБ выпрямитель вольтодобавочного преобразователя выполняет функцию инвертора тока, а инвертор – функцию выпрямителя [11]. При этом инвертор тока осуществляет высокочастотное преобразование тока дросселя, который суммируется в общем узле со своим исходным значением, т.е. осуществляется токовая добавка.

Коммутационные процессы в режиме заряда АБ аналогичны процессам в режиме разряда, однако значение отрицательного тока выходного дросселя в этом случае существенно больше (соответственно больше энергия, накапливаемая в индуктивности рассеяния), что вызывает более энергоемкий колебательный процесс (рис. 5).

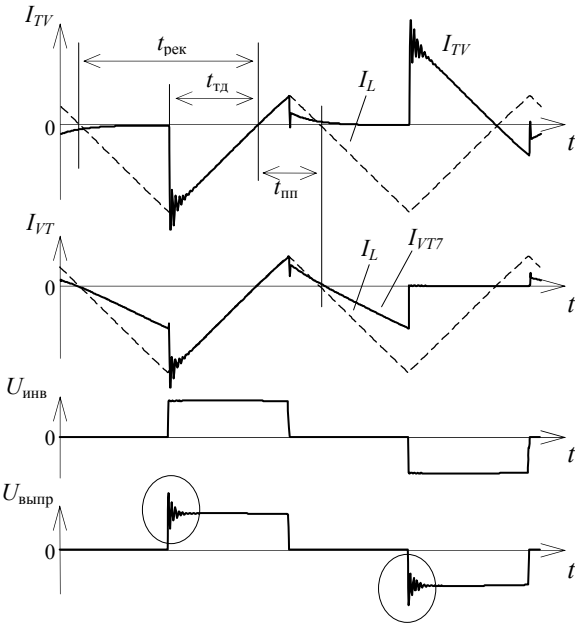


Рис. 5. Диаграммы работы преобразователя в режиме заряда АБ при γ = 0,5; Ls = 100 нГн; C_{ds} = 2нФ

Определение диапазона мягкого переключения в вольтодобавочном преобразователе

Условием мягкого включения транзисторов преобразователя является наличие пульсаций тока дросселя, превышающих ток нагрузки. Однако амплитуда пульсаций тока дросселя зависит от длительности импульсов напряжения инвертора γ, что не позволяет получить мягкое включение транзисторов во всем диапазоне. При $K_{тр}$ = 1 амплитуда пульсаций тока дросселя определяется выражением

$$\Delta I_L = \frac{U_{вых}}{2fL}\cdot\frac{\gamma\left(1-\gamma\right)}{1+\gamma}, \qquad (2)$$

где f – частота пульсаций тока дросселя, равная удвоенной частоте работы инвертора. По отношению к току нагрузки

$$\Delta I_L^{*} = \frac{\Delta I_L}{I_н} = \frac{1}{\sigma}\cdot\frac{\pi\gamma\left(1-\gamma\right)}{1+\gamma},$$

где $\sigma = \omega L/R$ – коэффициент, определяющий отношение реактивного сопротивления дросселя к сопротивлению нагрузки. Условие мягкой коммутации можно записать как

$$\Delta I_L^* > 1 \quad \text{или} \quad \sigma < \frac{\pi\gamma(1-\gamma)}{1+\gamma}.$$

Зависимости относительной амплитуды пульсаций тока дросселя от длительности импульсов напряжения γ при разных σ показаны на рис. 6. Видно, что мягкое включение можно обеспечить лишь в узком диапазоне регулирования, зависящем от σ. Значение коэффициента $\sigma_0 = 0{,}54$ определяет пограничный режим, когда мягкая коммутация возможна в одной точке (см. рис. 6). Расширения диапазона ZVS можно достичь уменьшением коэффициента σ (т.е. уменьшением индуктивности дросселя), что неизбежно приводит к существенному увеличению отрицательного тока и дополнительным статическим потерям.

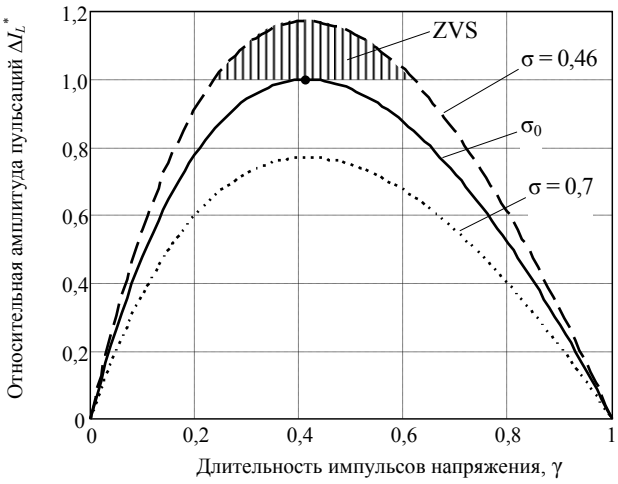


Рис. 6. Относительная величина пульсаций при различных коэффициентах индуктивности

Таким образом, для расширения диапазона мягкого включения и исключения больших отрицательных токов нужно адаптивно менять σ в зависимости от γ, что может быть реализовано, например, путем подстройки рабочей частоты. Частотная подстройка по условию обеспечения мягкой коммутации, т.е. равенства амплитуд переменной и постоянной составляющих тока дросселя, может быть получена по условию $\Delta I_L^* = 1$, из которого можно получить значение подстраиваемой частоты:

$$\omega_{ZVS}^* = \frac{\omega}{\omega_{max}} = \frac{1}{\sigma_0} \cdot \frac{\pi\gamma(1-\gamma)}{1+\gamma}.$$

Графически зависимость показана на рис. 7, видно, что величина частотной постройки существенна и определяется требуемым диапазоном регулирования напряжения. На краях диапазона регулирования частота стремится к нулю, поэтому в любом случае диапазон ZVS меньше полного диапазона регулирования.

Следует отметить, что при уменьшении частоты увеличивается амплитуда индукции трансформатора, что на первый взгляд может вызвать рост его габаритов. Однако амплитуда рабочей индукции трансформатора определяется не только частотой, но и длительностью импульсов напряжения γ, которая является переменной величиной:

$$B \sim U_{АБ} \cdot \gamma T.$$

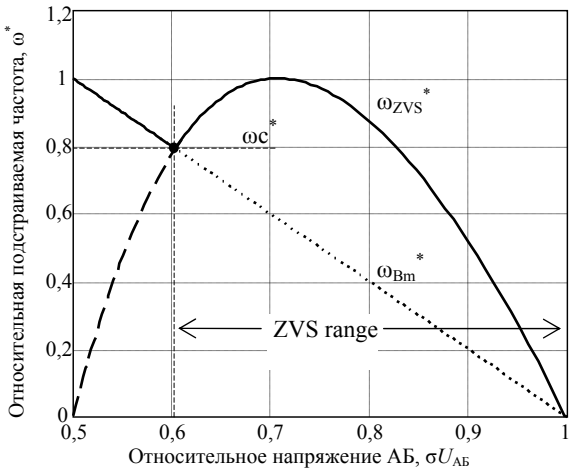


Рис. 7. Режим частотной подстройки с ограничением индукции трансформатора

По отношению к максимальному значению индукции при γ = 1 индукцию трансформатора на фиксированной частоте можно представить выражением

$$B^* = \frac{2\gamma}{1+\gamma},$$

а при частотной подстройке

$$B^* = \frac{2\gamma}{1+\gamma} \cdot \frac{1}{\omega_{ZVS}^*(\gamma)}.$$

Данное соотношение позволяет получить предельные зависимости частотной подстройки ω_{Bm} при условии отсутствия завышения индукции $B^* = 1$, ограничивающие нижний порог подстройки частоты:

$$\omega_{Bm}^* = 2(1-\sigma U).$$

Используя эту ограничительную зависимость совместно с функцией частотной подстройки ω_{ZVS}, можно определить диапазон мягкого переключения, достижимый без завышения индукции трансформатора.

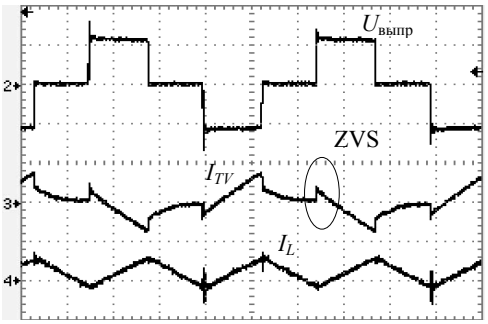
Можно увидеть, что диапазон регулирования преобразователя состоит из участков мягкого и жесткого включения транзисторов, с частотой сопряжения ωc^*, ограничивающей нижнюю границу диапазона мягкого переключения. Верхняя граница диапазона ZVS ограничена допустимым диапазоном частотной подстройки.

В режиме заряда АБ амплитуда пульсаций $\Delta I_L(\gamma)$ также определяется выражением (2), однако при определении диапазона ZVS соотносится к току заряда АБ, который существенно меньше тока разряда, поэтому в режиме заряда АБ диапазон ZVS будет шире, т.е. режим разряда АБ с позиций обеспечения ZVS является наихудшим.

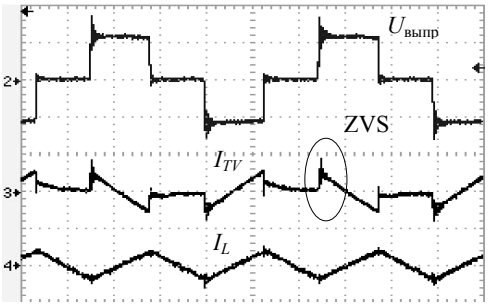
Результаты эксперимента двунаправленного вольтодобавочного преобразователя

Для экспериментальной проверки полученных результатов был спроектирован макет исследуемого

вольтодобавочного преобразователя, состоящего из мостовых преобразователей на транзисторах IRFP4868, трансформатора с коэффициентом трансформации $K_{тр} = 1$, выполненного на магнитопроводе ELP 38/8/25 (феррит N87). Измерения показали наличие у трансформатора индуктивности рассеяния $Ls = 83$ нГн. Дроссель индуктивностью $L = 8$ мкГн на магнитопроводе E32/6/20 с зазором $g = 0{,}5$ мм (феррит N87) и выходной конденсатор, состоящий из 5 конденсаторов К73-11-160В-5,6 мкФ, общей емкостью $C = 28$ мкФ. Работа преобразователя представлена осциллограммами тока дросселя, тока трансформатора, напряжения выпрямителя при напряжении аккумулятора $U_{АБ} = 55$ В на нагрузке $R_н = 12$ Ом и на холостом ходу (рис. 8).



а – $R_н = 12{,}5$ Ом

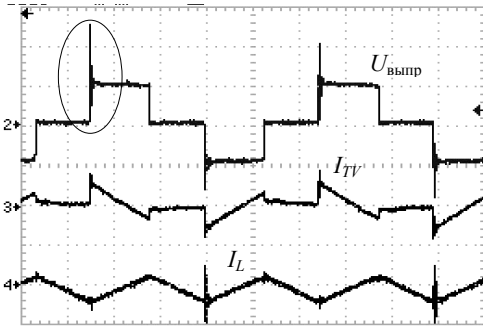


б – холостой ход

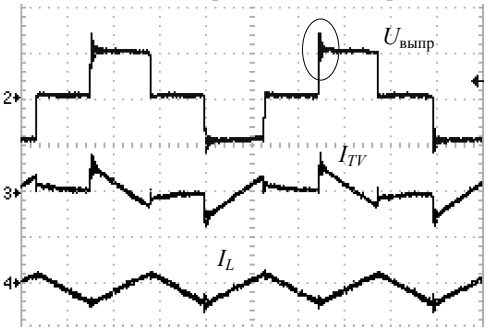
Рис. 8. Осциллограммы токов дросселя (20 А/дел) и трансформатора (16 А/дел) и напряжения выпрямителя (50 В/дел) вольтодобавочного преобразователя в режиме разряда АБ на частоте 40 кГц (5 мкс/дел)

Осциллограммы показывают наличие интервала рекуперации тока трансформатора, свидетельствующего об отрицательном токе включения транзисторов отстающей стойки инвертора, т.е. об их включении в режиме ZVS.

В режиме заряда АБ осциллограммы показаны на рис. 9 при $U_{АБ} = 50$ В. Без дополнительных снабберных конденсаторов напряжение выпрямителя имеет существенные коммутационные выбросы в момент выключения транзисторов (см. рис. 9, *а*), с амплитудой, превышающей напряжение АБ. Собственной емкости транзисторов IRFP4868 явно недостаточно для их демпфирования. При включении дополнительных конденсаторов параллельно транзисторам выпрямителя $Cds = 4{,}7$ нФ коммутационные выбросы значительно уменьшаются (см. рис. 9, *б*). При этом коммутационные выбросы напряжения при включении транзисторов выпрямителя отсутствуют.

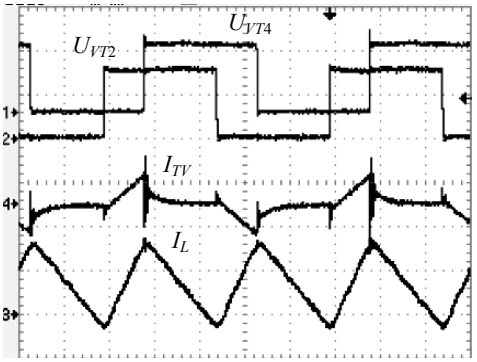


а – без снабберных конденсаторов

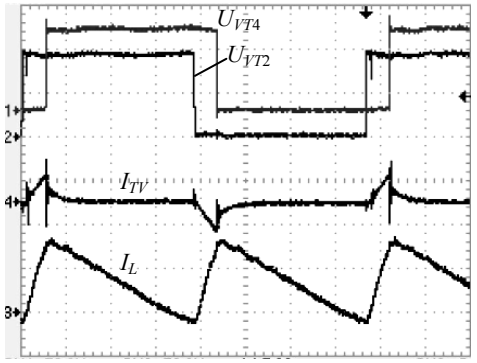


б – $Cds = 4{,}7$ нФ

Рис. 9. Осциллограммы токов дросселя (20 А/дел), трансформатора (16 А/дел), напряжения выпрямителя (50 В/дел) вольтодобавочного преобразователя в режиме заряда АБ на частоте 40 кГц (5 мкс/дел)



а – $U_{АБ} = 75$ В; $\gamma = 0{,}37$; $f = 40$ кГц



б – $U_{АБ} = 90$ В; $\gamma = 0{,}12$; $f = 26$ кГц

Рис. 10. Осциллограммы токов дросселя (15 А/дел) и трансформатора (32 А/дел) и напряжений на транзисторах (50 В/дел) вольтодобавочного преобразователя при стабилизации напряжения $U_{вых} = 100$ В (5 мкс/дел)

Проведена экспериментальная проверка режима частотной подстройки при стабилизации выходного напряжения на уровне $U_{вых} = 100$ В, осциллограммы

при разных $U_{АБ}$ представлены на рис. 10. Увеличение напряжения на АБ приводит к уменьшению γ, при этом амплитуда пульсаций тока дросселя стабилизируется подстройкой частоты. Значение частоты $f = 26$ кГц, соответствующее $U_{АБ} = 90$ В (см. рис. 10, *б*), примерно соответствует характеристике рис. 7, если учесть нестабильность длительности интервала рекуперации.

В целом экспериментальные результаты подтверждают сделанные в работе выводы, в частности, показывают мягкое включение транзисторов.

Заключение

Представленный вольтодобавочный преобразователь с активным выпрямителем, благодаря интервалу отрицательного тока дросселя обладает мягким включением транзисторов как инвертора, так и выпрямителя, что позволяет увеличить частоту преобразования и энергетические характеристики в целом. При этом режимы коммутации в инверторе и выпрямителе различны, так как первый является преобразователем напряжения, а второй – преобразователем тока. Существенное влияние на коммутационные процессы оказывает индуктивность рассеяния трансформатора, вызывающая перегрузки транзисторов выпрямителя при их выключении, особенно ярко это выражено в режиме заряда АБ при больших значениях отрицательного тока дросселя (см. рис. 9, *а*). Включение снабберных конденсаторов параллельно транзисторам выпрямителя шунтирует коммутационный ток и уменьшает выбросы напряжения (см. рис. 9, *б*). Следует заметить, что аналогичный эффект имеет включение одного конденсатора параллельно вторичной обмотке трансформатора.

Мягкое включение транзисторов инвертора в рассматриваемом преобразователе достигается при пульсациях тока слаживающего дросселя, превышающих ток нагрузки, поэтому зависимость амплитуды пульсаций от γ сужает диапазон мягкой коммутации. Применение частотной подстройки по условию возникновения отрицательного тока включения транзисторов позволяет существенно расширить диапазон мягкого включения без завышения индукции в трансформаторе. При этом верхняя граница диапазона ZVS ограничена допустимым диапазоном частотной подстройки, которая может изменяться в несколько раз в зависимости от напряжения АБ, что не всегда может быть приемлемым. Поэтому из практических соображений рекомендуется ограничить верхнюю границу диапазона значением $\sigma U_{АБ} = 0{,}9$ (см. рис. 10, *б*).

Работа выполнена в рамках реализации Постановления Правительства РФ № 218 от 09.04.2010 г. и договора между АО «ИСС» и Минобрнауки РФ от 01.12.2015 г. № 02. G25.31.0182.

Литература

1. Arthur G. Birchenough. The Series Connected Buck Boost Regulator Concept for High Efficiency Light Weight DC Voltage Regulation. – Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20030093550.pdf. (accessed: 6.04.2018).

2. Maksimovic D. The Series Connected Buck Boost Regulator Concept for High Efficiency Light Weight DC Voltage Regulation / D. Maksimovic, B. Jacobson // IEEE Transactions on Power Electronics. – 2012. – Vol. 27, No. 7. – PP. 3266–3276.

3. Park K.B. Nonisolated high step-up stacked converter based on boost-integrated isolated converter / K.B. Park, G.W. Moon, M.J. Youn // IEEE Transactions on Power Electronics. – 2011. – Vol. 26, No. 2. – PP. 577–587.

4. Li W. Review of nonisolated high-step-up DC/DC converters in photovoltaic grid-connected applications / W. Li, X. He // IEEE Transactions on Power Electronics. – 2011. – Vol. 58, No. 4. – PP. 1239–1250.

5. Improved zero-current-transition converters for high-power applications / H. Mao, F.C.Y. Lee, X. Zhou, H. Dai, M. Cosan, D. Boroyevich // IEEE Transactions on Industry Applications. – 1997. – Vol. 33, No. 5. – PP. 1220–1232.

6. Minimum current operation of bidirectional dual-bridge series resonant DC/DC converters / L. Corradini, D. Seltzer, D. Bloomquist, R. Zane, D. Maksimovic, B. Jacobson // IEEE Transactions on Power Electronics. – 2012. – Vol. 27, No. 7. – PP. 3266–3276.

7. Вольтодобавочный последовательный резонансный преобразователь с изменяемой структурой для систем электропитания / А.В. Осипов, Е.В. Ярославцев, Е.Ю. Буркин, В.В. Свиридов // Изв. Том. политех. ун-та. Инжиниринг георесурсов. – 2018. – Т. 329, № 2. – С. 27–37.

8. Казанцев Ю.М. Уменьшение потерь в двухтактных импульсных преобразователях напряжения / Ю.М. Казанцев, А.Ф. Лекарев // Электронные и электромеханические системы и устройства: сб. науч. трудов НПЦ «Полюс». Томск: Изд-во Томского НЦТИ, 1997. – С. 73–79.

9. Двухфазный повышающий преобразователь с мягкой коммутацией транзисторов и особенности его динамических свойств / Р.К. Диксон, Ю.Н. Дементьев, Г.Я. Михальченко, С.Г. Михальченко, С.М. Семенов // Изв. Том. политехн. ун-та. Инжиниринг георесурсов. – 2014. – Т. 324, № 4. – С. 96–101.

10.Waffler S. A novel low-loss modulation strategy for high-power bidirectional buck + boost converters / S. Waffler, J.W. Kolar // IEEE Transactions on Power Electronics. – 2009. Vol. 24, No. 6. – PP. 1589–1599.

11. Двунаправленный вольтодобавочный преобразователь с активным выпрямителем для заряда-разряда аккумулятора в системах электропитания / А.В. Осипов, И.С. Шемолин, В.Н. Школьный, Р.А. Латыпов // Доклады ТУСУРа. – 2018. – № 1. – С. 119–126.

12. Кобзев А.В. Энергетическая электроника: учеб. пособие / А.В. Кобзев, Б.И. Коновалов, В.Д. Семенов. – Томск: Томский межвузовский центр дистанционного образования, ТУСУР. – 2010. – 164 с.

Осипов Александр Владимирович
Канд. техн. наук, ст. науч. сотр.
НИИ космических технологий (НИИ КТ)
Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-903-914-09-67
Эл. почта: ossan@mail.ru

Шемолин Илья Сергеевич
Магистрант каф. промышленной электроники,
инженер НИИ КТ ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-906-948-91-55
Эл. почта: ilya.shemolin@mail.ru

Лопатин Александр Александрович
Канд. техн. наук, нач. сектора разработки силовой
бортовой аппаратуры АО «Информационные
спутниковые системы» им. акад. М.Ф. Решетнева
Ленина ул., д. 52, г. Железногорск, Россия, 662972
Тел.: +7 (391-9) 73-67-03
Эл. почта: lopatin@iss-reshetnev.ru

Латыпов Раимджан Акмальханович
Инженер-конструктор сектора разработки силовой
бортовой аппаратуры АО «Информационные
спутниковые системы» им. акад. М.Ф. Решетнева
Ленина ул., д. 52, г. Железногорск, Россия, 662972
Тел.: +7-904-896-99-51
Эл. почта: raimdzhan.latypov@gmail.com

Osipov A.V., Shemolin I.S., Lopatin A.A., Latypov R.A.
Bidirectional booster converter with soft-switching for power supply systems

The paper considers a bi-directional booster converter with an active rectifier for charge-discharge of a battery of power systems of space vehicles. Switching processes are considered, it is shown that in the booster converter due to the bipolar current of the smoothing-inductor the recovery interval is formed, which ensures drain-source capacitances pre-dump of the transistors of the inverter, which results in the inclusion at zero voltage. The battery charge mode is considered, it is shown that a large value of the negative current of the throttle leads to commutation voltage surges when the rectifier transistors are turned off, which can be eliminated by increasing the drain-source capacitances of rectifier transistors. The soft switching range can be significantly extended by adjusting the conversion frequency by the condition that the regeneration interval appears. It is shown that, in the absence of overstating the transformer induction, the limiting range of the ZVS reaches 80% of the maximum. An experimental verification of the results obtained is made, conclusions are drawn, and the results obtained are discussed.
Keywords: power supply system, booster converter, soft switching.
doi: 10.21293/1818-0442-2018-21-2-108-117

References

1. Arthur G. Birchenough. The Series Connected Buck Boost Regulator Concept for High Efficiency Light Weight DC Voltage Regulation. – Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20030093550.pdf. (accessed: 06 April 2018).

2. Maksimovic D., Jacobson B. The Series Connected Buck Boost Regulator Concept for High Efficiency Light Weight DC Voltage Regulation. *IEEE Transactions on Power Electronics*, 2012, vol. 27, no. 7, pp. 3266–3276.

3. Park K.B., Moon G.W., Youn M.J. Nonisolated high step-up stacked converter based on boost-integrated isolated converter. *IEEE Transactions on Power Electronics*. 2011, vol. 26, no. 2, pp. 577–587.

4. Li W., He X. Review of nonisolated high-step-up DC/DC converters in photovoltaic grid-connected applications. *IEEE Transactions on Power Electronics*. 2011, vol. 58, no. 4, pp. 1239–1250.

5. Mao H., Lee F.C.Y., Zhou X., Dai H., Cosan M., Boroyevich D. Improved zero-current-transition converters for high-power applications. *IEEE Transactions on Industry Applications*. 1997, vol. 33, no. 5, pp. 1220–1232.

6. Corradini L., Seltzer D., Bloomquist D., Zane R., Maksimovic D., Jacobson B. Minimum current operation of bidirectional dual-bridge series resonant DC/DC converters. *IEEE Transactions on Power Electronics*. 2012, vol. 27, no. 7, pp. 3266–3276.

7. Osipov A.V., Yaroslavtsev E.V., Burkin E.Yu., Sviridov V.V. Vol'todobavochnyi posledovatel'nyi rezonansnyi preobrazovatel' s izmenyaemoi strukturoi dlya sistem elektropitaniya [Booster series resonant transformer with variable structure for power supply system's]. *Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov* [Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering], 2018, vol. 329, no 2, pp. 27–37 (In Russ.).

8. Kazantsev Yu.M., Lekarev A.F. Umen'shenie poter' v dvukhtaktnykh impul'snykh preobrazovatelyakh napryazheniya [Reduction of losses in push-pull voltage transducers of voltage]. *Elektronnye i elektromekhanicheskie sistemy i ustroistva: sb. nauch. trudov NPTs «Polyus»* [Electronic and electromechanical systems and devices: sat. sci. proceedings of the NPC «Polus»]. Tomsk, Tomsk NCTI Publ., 1997, pp. 73–79 (In Russ.).

9. Dixon R.K., Dement'ev Yu.N., Mikhal'chenko G.Ya., Mikhal'chenko S.G., Semenov S.M. Dvukhfaznyi povyshayushchii preobrazova-tel' s myagkoi kommutatsiei tranzistorov i osobennosti ego dinamicheskikh svoistv [Two-phase boost-converter with soft switching of transistors and features of its dynamic properties]. *Izvestiya Tomskogo politekhnicheskogo universiteta* [Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering], 2014, vol. 324, no. 4, pp. 96–101 (In Russ.).

10. Waffler S., Kolar J.W. A novel low-loss modulation strategy for high-power bidirectional buck + boost converters. *IEEE Transactions on Power Electronics*, 2009, vol. 24, no. 6, pp. 1589–1599.

11. Osipov A.V., Shemolin I.S., Shkolnyi V.N, Latypov R.A. Dvunapravlennyi vol'todobavochnyi preobrazovatel' s aktivnym vypryamitelem dlya zaryada-razryada akkumulyatora v sistemakh elektropitaniya [Bidirectional booster converter with an active rectifier for charge-discharge of a battery in power systems]. *Doklady TUSUR* [Proceedings of TUSUR University], 2018, no 1, pp. 119–126 (In Russ.).

12. Kobzev A.V, Konovalov B.I, Semenov V.D. *Energeticheskaya elektronika. Uchebnoe posobie* [Energy Electronics: A Tutorial]. Tomsk, Tomskii mezhvuzovskii tsentr distantsionnogo obrazovaniya [Tomsk Interuniversity Center for Distance Education], 2010. 164 p. (In Russ.).

Alexander V. Osipov
Doctor of Engineering Sciences, Senior science fellow
Research Institute of Space Technology Tomsk State
University of Control Systems and Radioelectronics (TUSUR)
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7-903-914-09-67
Email: ossan@mail.ru

Shemolin Ilya Sergeevich
Master student, Department of Industrial Electronics, TUSUR
40, Lenina pr., Tomsk, Russia, 634050
Phone: +7-906-948-91-55
Email: ilya.shemolin@mail.ru

Lopatin Aleksandr Aleksandrovich
Doctor of Engineering Sciences, Head of Design Section
Power Supply and Conversion Equipment JSC «Information
Satellite Systems» named after Academician M.F. Reshetnev
52, Lenina st., Zheleznogorsk, Russia, 662972
Phone: +7 (391-9) 73-67-03
Email: lopatin@iss-reshetnev.ru

Latipov Raimjan Akmalkhanovich
PhD student, Engineer-designer of Design Section Power
Supply and Conversion Equipment JSC «Information
Satellite Systems» named after Academician M.F. Reshetnev
52, Lenina str., Zheleznogorsk, Russia, 662972
Phone: +7-904-896-99-51
Email: raimdzhan.latypov@gmail.com

Требования к подготовке рукописей статей,

представляемых для публикации в журнале «Доклады Томского государственного университета систем управления и радиоэлектроники»

1. Электронный вариант статьи должен быть представлен в виде файла, названного по-русски фамилией первого автора, на дискете или диске в формате Word 2003. Предпочтительнее представить его по электронной почте.

2. Оригинал на бумажном носителе должен полностью соответствовать электронному варианту.

3. Статья должна иметь (в порядке следования): УДК; И.О. Фамилии авторов; заглавие; аннотация (не реферат); ключевые слова; основной текст статьи; список библиографий под подзаголовком «Литература»; сведения об авторах; далее на английском языке: Фамилии авторов И.О., заглавие статьи, аннотацию, ключевые слова. Сведения об авторах включают в себя фамилию, имя, отчество, ученую степень, ученое звание, должность, место работы, телефон, электронный адрес.

4. Текст статьи должен быть размещен в две колонки без принудительных переносов через один интервал шрифтом Times New Roman 10 кегля на одной стороне листа белой писчей бумаги формата А4, без помарок и вставок. Для облегчения форматирования прилагается **шаблон статьи**, который размещен на сайте: **journal.tusur.ru.** Размер статьи со всеми атрибутами должен быть, как правило, не более пяти страниц.

5. Одни и те же символы в тексте, формулах, таблицах и рисунках должны быть единообразными по написанию. Русские и греческие символы набираются прямым шрифтом, а латинские – курсивом, кроме слов, их сокращений, имен функций, программ, фирм и химических формул.

6. Формулы должны быть набраны в формульном редакторе (Equation, MathType) программы Word. Русские буквы, греческие символы, математические знаки (+, –, ×, ∈, =, скобки, …) и цифры всегда набираются прямым не жирным шрифтом, а переменные (и кривые), обозначенные латинскими буквами или цифрами – курсивом, кроме слов, их сокращений, имен функций, программ, фирм и химических формул (const, input; $\sin x(t_1)$; U_{in}; $I_{\text{вх}}$; T_z; β_2; H_2O, Adobe Acrobat, Cisco и т.д.); векторные величины – жирным, прямо (не курсив) – $\mathbf{A}_1$, $\mathbf{M}(f)$, $\boldsymbol{\beta}$. Шаблоны для набора формул необходимо взять из шаблона статьи.

7. Все употребляемые обозначения и сокращения должны быть пояснены.

8. Единицы измерения физических величин должны соответствовать Международной системе единиц (СИ) и написаны по-русски через пробел (x, ГГц; 20 ГГц; T, град; 7 °С). Десятичные числа пишутся через запятую (не точку).

9. Таблицы и рисунки должны иметь тематические заголовки (не повторяющие фразы-ссылки на них в тексте). (Рис. 1. Название рисунка; Таблица 1. Название таблицы). Большие блоки расшифровки условных обозначений лучше приводить в тексте. Подписи и надписи – Times New Roman, 9 пт, не жирным, не курсивом, переменные – также как и в тексте. На все рисунки и таблицы должны быть ссылки в тексте (… на рис. 3, … в табл. 2).

10. Рисунки и фотографии должны быть **черно-белыми**, четкими, контрастными, аккуратными, сгруппированными. Графики – не жирно, сетка – четко. Единицы измерения – на русском. Десятичная запятая (не точка). Рисунки могут быть выполнены в программах CorelDraw, Illustrator, Word, Visio и должны давать возможность внесения исправлений.

11. Иллюстрации, должны быть разрешением не менее 600 dpi. Масштаб изображения – 8 или 16,7 см по ширине (при условии читаемости всех надписей, выполненных шрифтом Times New Roman 9 кегля).

12. На все источники, указанные в списке литературы, должны быть ссылки по тексту (нумерация в порядке упоминания, например, [1, 2], [5–7]). Описание источников должно соответствовать ГОСТ 7.1–2003 и ГОСТ Р 7.0.5–2008 и содержать всю необходимую для идентификации источника информацию, а именно: *для непериодических изданий* – фамилию и инициалы автора, полное название работы, место издания, название издательства, год издания, количество страниц; *для периодических изданий* – фамилию, инициалы автора, полное название работы, название журнала, год выпуска, том, номер, номера страниц (см. примеры оформления библиографий).

Бумажный вариант рукописи статьи должен быть подписан авторами и (для сторонних авторов) иметь сопроводительное письмо на бланке организации.

Плата за публикацию рукописей не взимается.

Материальные претензии авторов, связанные с распространением материалов их статей после опубликования, не принимаются.

Авторы несут полную ответственность за содержание статей и за последствия, связанные с их публикацией.

Контактная информация

Адрес: 634050, Томск, пр. Ленина, 40, 414-ГК.

Эл. почта: vnmas@tusur.ru. Тел.: +7 (382-2) 51-21-21

9 771818 044708 02007