МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Вестник СибГУТИ Том 18, № 2, 2024

Выпускается ежеквартально, выходит с 2007 г.

Учредитель –
федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»

Адрес редакции и издателя

630102, г. Новосибирск, ул. Кирова, д. 86 e-mail: vestnik@sibguti.ru

Информация о журнале доступна в сети Internet по адресу https://vestnik.sibsutis.ru.

Журнал включён в Перечень ВАК российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук.

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия, свидетельство о регистрации ПИ № ФС77-25835 от 29.09.2006. ISSN 1998-6920. Подписной индекс в каталоге «Урал-Пресс» – 82519.

Дата выхода в свет 01.07.2024. Отпускная (редакционная) цена 750 руб.
Отпечатано в типографии Альфа по адресу: 630015, г. Новосибирск, ул. Шишкина, д. 3.
Бумага офсетная, формат А4. Тираж 300 экз.

СОДЕРЖАНИЕ

DOI: 10.55648/1998-6920-2024-18-2-3-12 УДК 621.3.049.779

Широкополосный приёмник мгновенного измерения частоты*

П. И. Пузырёв, А. Н. Ляшук, С. А. Завьялов

Омский государственный технический университет

Аннотация: В данной работе предложена структура широкополосного приёмника мгновенного измерения частоты, состоящего из аналоговых корреляторов и цифрового блока вычисления оценки частоты. Особенностью данной структуры является использование всего двух аналого-цифровых преобразователей, вне зависимости от ширины рабочего диапазона частот. Расширение частотного диапазона достигается за счет применения каналов с компараторами, причем каждый канал с компаратором увеличивает ширину рабочего частотного диапазона вдвое. Приведен порядок расчета основных характеристик приёмника мгновенного измерения частоты: время задержки и количество каналов с компараторами. Приведены результаты моделирования, показывающие сравнение среднеквадратичного отклонения оценки частоты с известной широкополосной структурой, представленной в литературе, и предлагаемой структурой.

Ключевые слова: мгновенное измерение частоты, МИЧ-приёмник, линия задержки, компаратор, автокорреляционный дискриминатор, АЦП.

Для цитирования: Пузырёв П. И., Ляшук А. Н., Завьялов С. А. Широкополосный приёмник мгновенного измерения частоты // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 3–12. https://doi.org/10.55648/1998-6920-2024-18-2-3-12.

Статья поступила в редакцию 29.11.2023;
принята к публикации 09.12.2023.

1. Введение

Приёмники мгновенного измерения частоты (МИЧ-приёмники) широко используются при решении задач обнаружения и идентификации источника радиоволн в станциях предупреждения об облучении, средствах радиоэлектронной борьбы и радиоастрономии. Классический МИЧ-приёмник представляет собой автокорреляционный приёмник, на выходе которого сигнал пропорционален разности фаз между прямым и задержанным сигналами (рис. 1). История применения подобных МИЧ-приёмников насчитывает уже более 60 лет [1–2]. К достоинствам такой структуры относятся высокая чувствительность и простота реализации. К недостаткам же относится небольшая рабочая полоса частот (обычно не более 2 ГГц). Проблема узкополосности решается за счет распараллеливания каналов [3], однако это приводит

* Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в рамках федерального проекта «Подготовка кадров и научного фундамента для электронной промышленности» государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации». Соглашение о предоставлении субсидии № 075-02-2024-1533.

к увеличению габаритов, энергопотреблению и сложности сопряжения с модулем цифровой обработки сигналов.

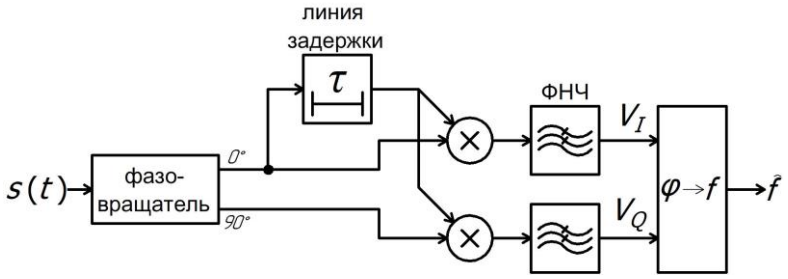


Рис. 1. Классический автокорреляционный приёмник мгновенного измерения частоты

На габариты отдельного МИЧ-приёмника в первую очередь влияет размер линии задержки, которая представляет собой длинную линию. Учитывая тот факт, что задерживать сигнал нужно на время от нескольких сотен пикосекунд до единиц наносекунд [4–12], исполнение МИЧ-приёмника в интегральном виде, даже в виде гибридной микросхемы, становится нетривиальной задачей. Таким образом, рассмотрение новых структур, которые по сложности, массогабаритным параметрам и энергопотреблению незначительно проигрывают классической структуре, сохраняют высокую помехоустойчивость, но обеспечивают значительно б*о*льшую рабочую полосу частот (10 ГГц и более), является актуальной задачей.

2. Постановка задачи

Рассмотрим работу автокорреляционного МИЧ-приёмника, структурная схема которого представлена на рис. 1 [7], при подаче на вход гармонического сигнала

$$s(t) = A\cos(2\pi ft),$$

где A – амплитуда сигнала, f – частота сигнала в Гц.

Тогда квадратурные составляющие будут описываться выражениями

$$\begin{aligned} V_I(f) &= \frac{A^2}{2}\cos(2\pi f\tau), \\ V_Q(f) &= \frac{A^2}{2}\sin(2\pi f\tau), \end{aligned} \tag{1}$$

где τ – время задержки.

Нахождение оценки частоты сигнала $\hat{f}(f)$ заключается в последовательном вычислении фазового сдвига φ, вызванного линией задержки, с последующим масштабированием

$$\varphi(f) = \operatorname{atan2}\left[V_I(f), V_Q(f)\right], \tag{2}$$

$$\hat{f}(f) = \frac{\hat{\varphi}(f)}{2\pi\tau} + \frac{n}{\tau}, \tag{3}$$

где $n \in \mathbb{N}$ обозначает номер диапазона неоднозначности в дискриминационной характеристике (рис. 2). Как видно из рис. 2, рабочий частотный диапазон ограничивается величиной $B_W = 1/\tau$. При этом в силу периодичности дискриминационной характеристики возникает неоднозначность определения частоты: два сигнала с частотами f и $f+B_W$ будут неотличимы.

Таким образом, для расширения рабочего частотного диапазона МИЧ-приёмника, представленного на рис. 1, требуется уменьшение времени задержки τ. Однако, как показано в [8], время задержки также определяет точность определение частоты – чем меньше τ, тем выше СКО оценки частоты. Оценочные значения СКО оценки частоты для автокорреляционных МИЧ-приёмников приведены в [8], [12], [13].

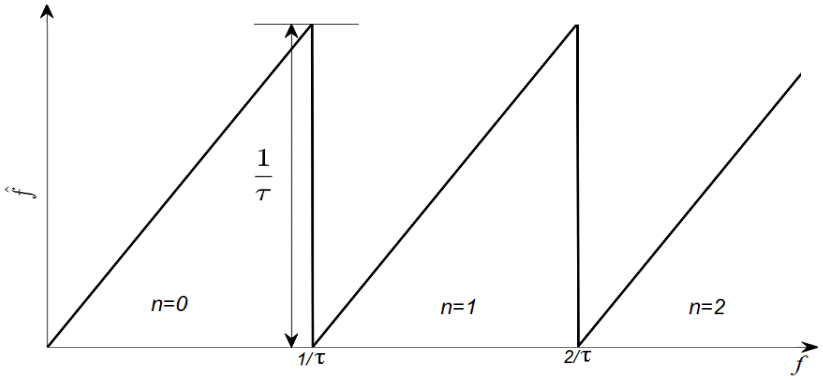


Рис. 2. Дискриминационная характеристика МИЧ-приёмника

Одним из путей решения проблемы компромисса «точность – диапазон частот» является использование структуры МИЧ-приёмника с двумя квадратурными каналами с задержками на τ_1 и τ_2 (рис. 3). В такой структуре рабочий частотный диапазон B_W определяется разностью $\Delta\tau = \tau_1 - \tau_2$, но при этом СКО оценки частоты определяется τ_1 и τ_2 в отдельности [8].

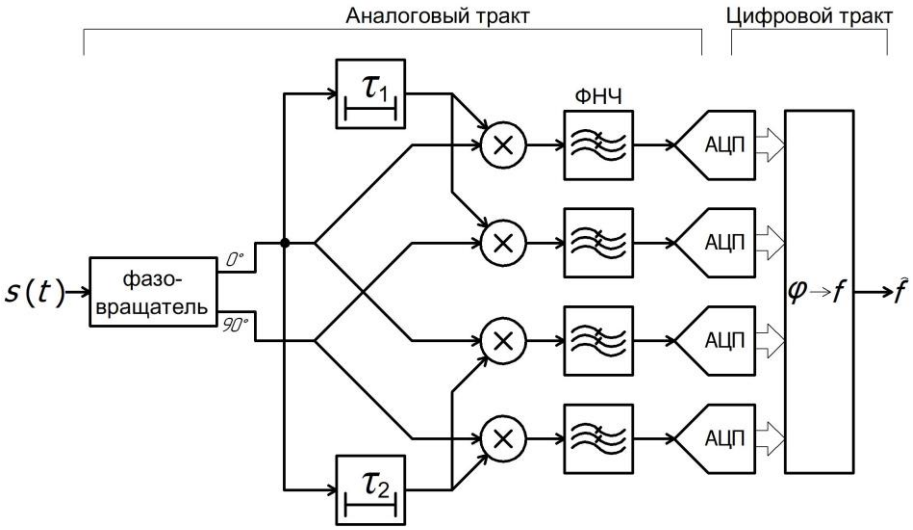


Рис. 3. МИЧ-приёмник с двумя квадратурными каналами

$$B_W = \frac{1}{\Delta\tau} = \frac{1}{\tau_2 - \tau_1}. \qquad (4)$$

В данной структуре также показано разделение, какую часть обработки сигналов целесообразно выполнять в аналоговом виде, а какую – в цифровом.

Недостатком структуры МИЧ-приёмника рис. 3 является необходимость использования четырёх аналого-цифровых преобразователей, по сравнению со структурой на рис. 1, где требуется два АЦП. Учитывая необходимость использования быстродействующих АЦП с частотами преобразования более 100 МГц для оценки частоты коротких радиоимпульсов менее 50 нс (требования к современным системам предупреждения об облучении), сложность реализации может стать ограничительным фактором. Особенно остро проблема встает при реализации многоканальных систем. В данной работе ставится задача уменьшить сложность реализации МИЧ-приёмника за счет уменьшения количества АЦП до двух с сохранением широкополосности и точности определения частоты путем использования новой структуры МИЧ-приёмника, а также разработать алгоритм расчета параметров основных узлов.

3. Описание предлагаемой структуры МИЧ-приёмника

Предлагаемая структура МИЧ-приёмника (рис. 4) базируется на комбинации структур классического МИЧ-приёмника (рис. 1) и МИЧ-приёмника с двоично взвешенными автокорреляционными дискриминаторами [9–11], основным преимуществом которого является использование компараторов вместо АЦП. Недостатком же МИЧ-приёмника с двоично взвешенными дискриминаторами является низкая разрешающая способность Δf, которая зависит от количества каналов k:

$$\Delta f = \frac{B_W}{2^k}. \tag{5}$$

В предлагаемой структуре МИЧ-приёмника точность оценки частоты определяется квадратурными каналами V_I и V_Q (тонкая оценка частоты $\hat{f}_0$), а рабочий частотой диапазон определяется каналами d_1, d_2 … d_k (грубая оценка частоты).

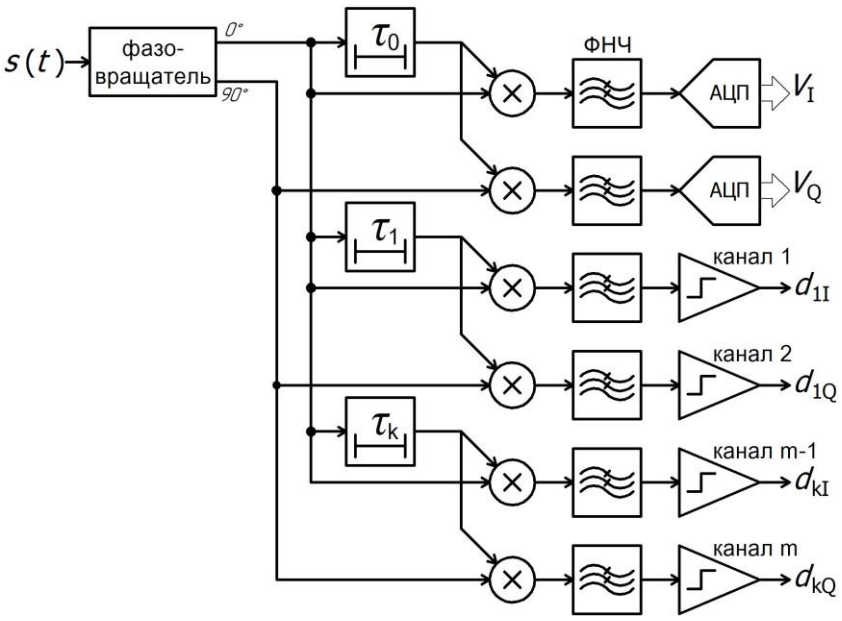


Рис. 4. Предлагаемая структура МИЧ-приёмника

Приведем порядок определения необходимого количества каналов исходя из заданного СКО, отношения сигнал/шум и рабочего частотного диапазона B_W:

1. Определить по графикам, представленным на рис. 5, задержку τ_0 для достижения требуемого СКО оценки частоты при заданном отношении сигнал/шум. Данные графики получены численным моделированием для структуры, изображенной на рис. 1, при входной аддитивной смеси гармонического сигнала и белого гауссовского шума.

2. Определить ширину диапазона неоднозначности для нулевого канала $B_0 = 1/\tau_0$.

Если $B_0 \geq B_W$, то структура сводится к классическому МИЧ-приёмнику без дополнительных каналов с компараторами (рис. 1). Если $B_0 < B_W$, то количество каналов с компараторами m определяется согласно выражению:

$$m = \left\lceil \log_2 \left(\frac{B_W}{B_0} \right) \right\rceil, \tag{6}$$

где $\lceil\ \rceil$ обозначает округление вверх.

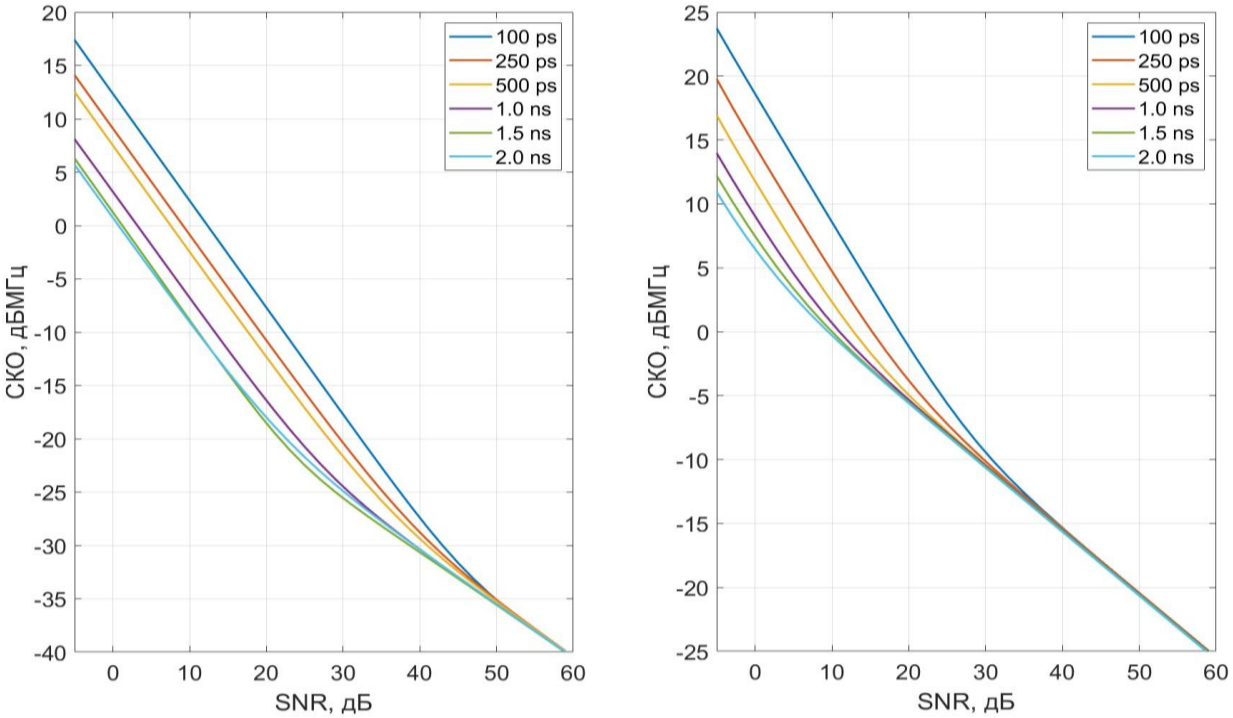


Рис. 5. Зависимость СКО оценки частоты от отношения сигнал/шум на входе МИЧ приёмника: (а) для ФНЧ 10 МГц; (б) для ФНЧ 100 МГц

Задержки τ_k определяются через рекуррентное выражение:

$$\tau_k = G_k \frac{\tau_{k-1}}{4}, \quad G_k \geq 1, \tag{7}$$

где G_k – коэффициент увеличения, который необходим для предотвращения ситуации, когда два или более компараторов переключаются на одной частоте (рис. 6) в пределах рабочего диапазона частот B_W. Если два компаратора на расчетной дискриминационной характеристике будут переключаться на одной частоте, то при изготовлении МИЧ-приёмника из-за ухода параметров задержек τ_k или под воздействием шумов положения фронтов переключения компараторов неизбежно сместятся друг относительно друга. Это приведет к тому, что в окрестностях данной частоты МИЧ-приёмник будет давать ошибку, равную $1/\tau_k$.

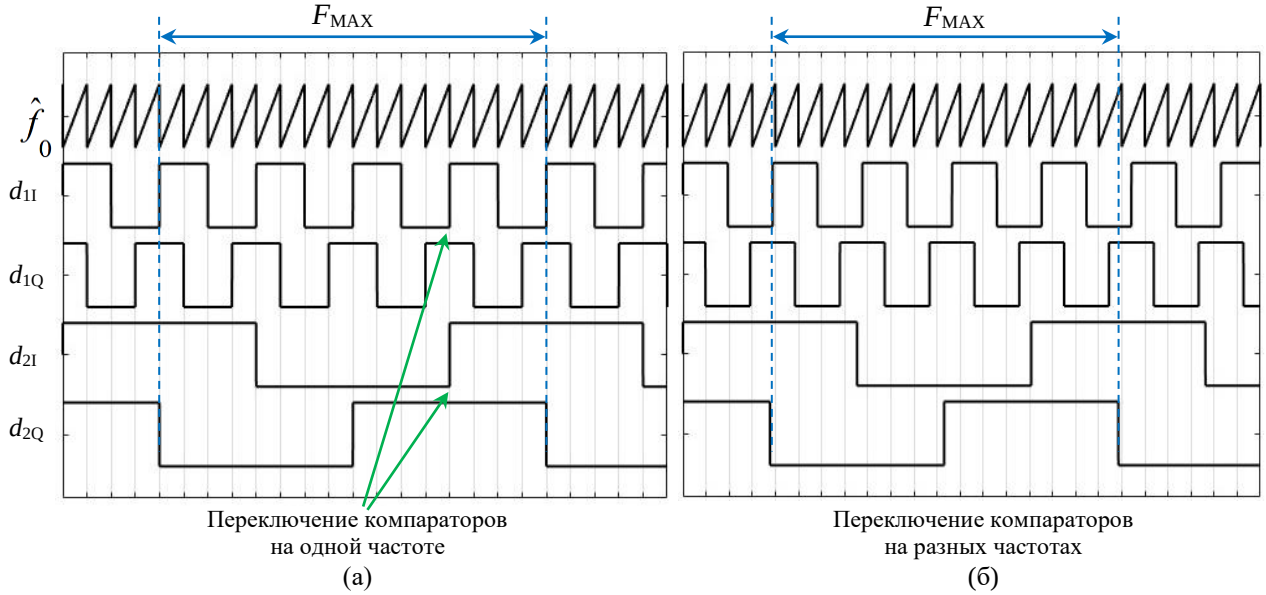


Рис. 6. Дискриминационная характеристика: (а) $G = 1$; (б) $G = 1.03$

Выбор коэффициентов увеличения G_k должен производиться исходя из двух условий:

1) отсутствие переключения компараторов на одной частоте в пределах B_W;

2) обеспечение максимального диапазона частот F_{MAX} (интервал частот, в котором оценка частоты вычисляется без неопределенностей) большего, чем рабочий диапазон частот, т.е. $F_{MAX} \geq B_W$.

Оценка частоты для случая $G_k = 1$ определяется выражениями:

$$\hat{f}_0 = \frac{\text{atan2}(V_I, V_Q) + \pi}{2\pi\tau_0}, \tag{8}$$

$$\hat{f} = \hat{f}_0 + \frac{p_1}{\tau_0} + \frac{p_2}{\tau_1} + ... + \frac{p_k}{\tau_{k-1}}, \tag{9}$$

$$p_k = \begin{cases} 0, & d_{Qk} > 0 \text{ and } d_{Ik} > 0 \\ 1, & d_{Qk} > 0 \text{ and } d_{Ik} \leq 0 \\ 2, & d_{Qk} \leq 0 \text{ and } d_{Ik} \leq 0 \\ 3, & d_{Qk} \leq 0 \text{ and } d_{Ik} > 0 \end{cases}. \tag{10}$$

Для случая, когда $G_k \neq 1$, вывод выражений для определения оценки частоты является нетривиальной задачей, т.к. на каждом поддиапазоне необходимо учитывать смещение всех характеристик d_k. Однако с практической точки зрения нет необходимости в аналитическом вычислении оценки частоты, поскольку, помимо коэффициентов G_k, на смещение d_k, V_I и V_Q оказывает влияние также непостоянство в частоте характеристик основных узлов МИЧ приёмника: задержки, фазовращателя, смесителя и т.п.

Решением данной проблемы является реализация вычислителя оценки частоты на основе таблицы соответствия (Lookup Table, LUT), в которую записываются значения реальных измерений изготовленного МИЧ-приёмника (рис. 7). Таблица соответствия представляет собой память, адрес для которой формируется из значений $\hat{f}_0$ (младшие N бит) и d_k (старшие m бит). В ячейки памяти с адресами [d_k, $\hat{f}_0$] записывается цифровой код частоты, соответствующий частоте сигнала с поверенного источника, подключаемого ко входу МИЧ-приёмника.

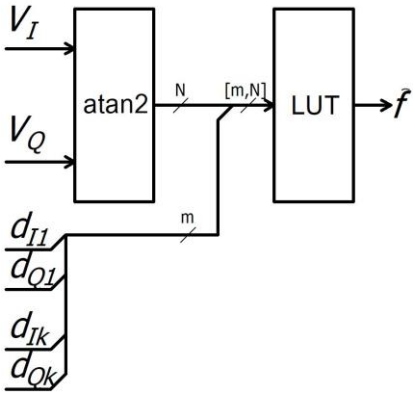


Рис. 7. Вычисление оценки частоты в цифровом тракте МИЧ-приёмника

На рис. 8 представлены сравнительные графики зависимости СКО оценки частоты для предлагаемой структуры МИЧ-приёмника, а также структуры с двумя квадратурными каналами с задержками на τ_1 и τ_2 (рис. 3). Из графиков видно, что предлагаемая структура МИЧ-приёмника показывает небольшое ухудшение СКО оценки частоты по сравнению со схемой [8]: разница 2.2 дБ для τ = 100 пс; 1.5 дБ для τ = 500 пс; 1.7 дБ для τ = 1 нс; 1.3 дБ для τ = 2 нс.

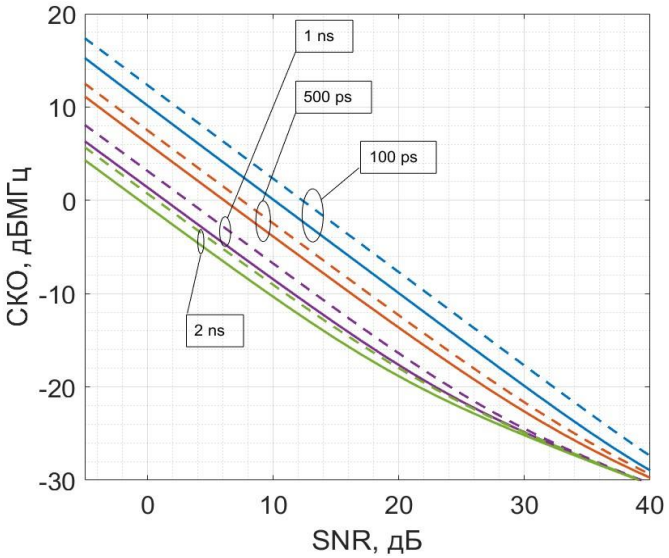


Рис. 8. Сравнение СКО оценки частоты предлагаемой структуры (пунктир) и структуры с двумя квадратурными каналами (сплошные)

4. Заключение

Предложенная структура МИЧ-приёмника обладает рядом преимуществ, таких как снижение сложности реализации за счет использования всего двух быстродействующих АЦП при одновременном сохранении широкополосности. Увеличение рабочего частотного диапазона в 4 раза достигается за счет добавления одной линии задержки и двух цепочек из перемножителей (фазовых детекторов), ФНЧ и компараторов. При этом все линии задержек в предлагаемой структуре конструктивно могут быть исполнены как одна линия задержки с ответвлениями, что позволяет еще уменьшить массогабаритные параметры МИЧ-приёмника.

Приведена последовательность расчета основных параметров приёмника, таких как время задержки и количество каналов с компараторами. Предложено использовать расширяющий коэффициент при расчете линии задержки, что позволяет снизить влияние технологического разброса параметров МИЧ-приёмника на ошибку измерения частоты за счет разнесения частот переключения компараторов.

С помощью математического моделирования установлено, что предложенная схема обеспечивает небольшое ухудшение СКО оценки частоты (1.5 – 2 дБ) по сравнению со структурой с двумя квадратурными каналами [8]. Однако при этом сокращение быстродействующих АЦП позволяет сэкономить габаритные параметры, что важно при реализации в интегральном виде, а также уменьшить энергопотребление и количество интерфейсных линий, что также является ограничительным фактором при реализации в интегральном виде.

Литература

1. *Thornton M. J.* Ultra-broadband frequency discriminator designs for IFM receivers // IEE Colloquium on Multi-Octave Active and Passive Components and Antennas. London, UK. 1989. P. 13/1–13/4.
2. *East P. W.* Fifty years of instantaneous frequency measurement // Radar, Sonar & Navigation. 2011. V. 6, № 2. P. 112–122.
3. *Keshani S., Masoumi N., Rahimpour H., Safavi-Naeini S.* Digital Processing for Accurate Frequency Extraction in IFM Receivers // IEEE Transactions on Instrumentation and Measurement. V. 69, № 9. P. 6092–6100.

4. *Lam D., Buckley B. W., Lonappan C. K., Madni A., M. Jalali B.* Ultra-wideband instantaneous frequency estimation // IEEE Instrumentation & Measurement Magazine. April 2015. V. 18, № 2. P. 26–30.
5. *Goavec A., Vauché R., Gaubert J., Hameau F., Zarudniev M., Mercier E.* Instantaneous frequency measurement for IR-UWB signal in CMOS 130 nm // Proc. IEEE International Conference on Electronics, Circuits and Systems (ICECS), Monte Carlo, Monaco, 2016. P. 157–160.
6. *Mahlooji S., Mohammadi K.* Very High Resolution Digital Instantaneous Frequency Measurement Receiver // Proc. International Conference on Signal Processing Systems, Singapore, 2009. P. 177–181.
7. *Егоров Н., Кочемасов В.* Мгновенное измерение частоты: методы и средства // Электроника, наука, технология, бизнес. 2017. № 5 (00165). С. 136–141.
8. *Kvachev M. A., Puzyrev P. I., Semenov K. V.* Research of Instantaneous Frequency Measurement Receiver // Proc. Dynamics of Systems, Mechanisms and Machines (Dynamics), Omsk, Russia, 2020, P. 1–5.
9. *Rahimpour H., Masoumi N.* High-Resolution Frequency Discriminator for Instantaneous Frequency Measurement Subsystem // IEEE Transactions on Instrumentation and Measurement. 2018. V. 67, № 10. P. 2373–2381.
10. *Rahimpour H., Masoumi N.* Design and Implementation of a High-Sensitivity and Compact-Size IFM Receiver // IEEE Transactions on Instrumentation and Measurement. July 2019. V. 68, № 7. P. 2602–2609.
11. *Rahimpour H., Masoumi N., Keshani S., Safavi-Naeini S.* A High Frequency Resolution Successive-Band Shifted Filters Architecture for a 15-bit IFM Receiver // IEEE Transactions on Microwave Theory and Techniques. May 2019. V. 67, № 5. P. 2028–2035.
12. *Pandolfi C., Fitini E., Gabrielli G., Megna E., Zaccaron A.* Comparison of analog IFM and digital frequency measurement receivers for electronic warfare // Proc. 7th European Radar Conference, Paris, France, 2010. P. 232–235.
13. *Василенко В. Э., Дикарев Б. Д., Зикий А. Н., Сальный И. А.* Экспериментальное исследование приёмника мгновенного измерения частоты // Известия ЮФУ. Технические науки. 2008. № 3. С. 168–171.

Пузырев Павел Иванович
к.т.н., доцент кафедры радиотехнических устройств и систем диагностики, Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, д. 11), e-mail: pipuzyrev@omgtu.ru, ORCID: 0000-0003-0694-9973.

Ляшук Алексей Николаевич
к.т.н., доцент кафедры радиотехнических устройств и систем диагностики, Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, д. 11), e-mail: pribor78@mail.ru, ORCID: 0000-0002-6394-9390.

Завьялов Сергей Анатольевич
к.т.н., доцент кафедры радиотехнических устройств и систем диагностики, Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, д. 11), e-mail: zavyalov62@mail.ru, ORCID: 0000-0001-5114-2074.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Broadband Instantaneous Frequency Measurement Receiver

Pavel I. Puzyrev, Aleksey N. Lyashuk, Sergey. A. Zavyalov

Omsk State Technical University (OmSTU)

Abstract: This paper proposes a structure of a broadband instantaneous frequency measurement receiver consisting of an analog correlator and a digital frequency estimation calculation unit. A feature of this structure is the use of only two ADCs regardless of the width of the operating frequency range. Expansion of the frequency range is achieved through the use of channels with comparators, and each channel with a comparator doubles the width of the operating frequency range. The procedure for calculating the main characteristics of a IFM receiver is given: delay time and the number of channels with comparators. Simulation results are presented showing a comparison of the standard deviation of the frequency estimation for the known broadband structure presented in the literature and the proposed structure.

Keywords: instantaneous frequency measurement, IMF receiver, delay line, comparator, auto-correlation discriminator, ADC.

For citation: Puzyrev P. I., Lyashuk A. N. Zavyalov S. A. Broadband instantaneous frequency measurement receiver (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 3-12. https://doi.org/10.55648/1998-6920-2024-18-2-3-12.

The article was submitted: 29.11.2023; accepted for publication 09.12.2023.

References

1. Thornton M. J. Ultra-broadband frequency discriminator designs for IFM receivers. *IEE Colloquium on Multi-Octave Active and Passive Components and Antennas*, 1989, pp. 13/1-13/4.
2. East P. W. Fifty years of instantaneous frequency measurement. *Radar, Sonar & Navigation*, 2011, vol. 6, no. 2, pp. 112-122.
3. Keshani S., Masoumi N., Rahimpour H., Safavi-Naeini S. Digital Processing for Accurate Frequency Extraction in IFM Receivers. *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 9, pp. 6092-6100.
4. Lam D., Buckley B. W., Lonappan C. K., Madni A., M. Jalali B. Ultra-wideband instantaneous frequency estimation. *IEEE Instrumentation & Measurement Magazine*, 2015, vol. 18, no. 2. pp. 26-30.
5. Goavec A., Vauche R., Gaubert J., Hameau F., Zarudniev M., Mercier E. Instantaneous frequency measurement for IR-UWB signal in CMOS 130 nm. *2016 IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2016, pp. 157-160.
6. Mahlooji S., Mohammadi K. Very High Resolution Digital Instantaneous Frequency Measurement Receiver. *2009 International Conference on Signal Processing Systems*, 2009, pp. 177-181.
7. Egorov N., Kochemasov V. Mgnovennoe izmerenie chastoti, metodi i sredstva [Instantaneous frequency measurement: methods and tools]. *Elektronika, nauka, tehnologiya, biznes*, 2017, iss. 5, pp. 136-141.
8. Kvachev M. A., Puzyrev P. I., Semenov K. V. Research of Instantaneous Frequency Measurement Receiver. *2020 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, 2020, pp. 1-5.
9. Rahimpour H., Masoumi N. High-Resolution Frequency Discriminator for Instantaneous Frequency Measurement Subsystem. *IEEE Transactions on Instrumentation and Measurement*, 2018, vol. 67, no. 10, pp. 2373-2381.
10. Rahimpour H., Masoumi N. Design and Implementation of a High-Sensitivity and Compact-Size IFM Receiver. *IEEE Transactions on Instrumentation and Measurement*, 2019, vol. 68, no. 7, pp. 2602-2609.

11. Rahimpour H., Masoumi N., Keshani S., Safavi-Naeini S. A High Frequency Resolution Successive-Band Shifted Filters Architecture for a 15-bit IFM Receiver. *IEEE Transactions on Microwave Theory and Techniques*, 2019, vol. 67, no. 5, pp. 2028-2035.
12. Pandolfi C., Fitini E., Gabrielli G., Megna E., Zaccaron A. Comparison of analog IFM and digital frequency measurement receivers for electronic warfare. *The 7th European Radar Conference*, 2010, pp. 232-235.
13. Vasilenko V. E., Dikarev B. D., Zikii A. N., Salnii I. A. Eksperimentalnoe issledovanie priemnika mgnovennogo izmereniya chastoti [Experimental research of instantaneous frequency measurement receiver]. *Izvestiya YuFU. Tehnicheskie nauki*, 2008, no. 3. pp. 168-171.

Pavel I. Puzyrev

Cand. of Sci. (Engineering), Associate Professor of Radio Engineering devices and Diagnostic Systems Department, Omsk State Technical University (OmSTU, Russia, 644050, Omsk, Mira Ave. 11), e-mail: pipuzyrev@omgtu.ru, ORCID: 0000-0003-0694-9973, ResearcherID: E-8041-2014.

Aleksey N. Lyashuk

Cand. of Sci. (Engineering), Associate Professor of Radio Engineering devices and Diagnostic Systems Department, Omsk State Technical University, e-mail: pribor78@mail.ru, ORCID: 0000-0002-6394-9390, ResearcherID: R-2812-2016.

Sergey A. Zavyalov

Cand. of Sci. (Engineering), Associate Professor of Radio Engineering devices and Diagnostic Systems Department, Omsk State Technical University, e-mail: zavyalov62@mail.ru, ORCID: 0000-0001-5114-2074, ResearcherID: E-8661-2014.

DOI: 10.55648/1998-6920-2024-18-2-13-31 УДК 621.396.41

Анализ проблемы развертывания при планировании покрытия сети 5G

И. В. Алиев, В. И. Носов

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: Глобальный спрос на услуги мобильного Интернета с более высокой пропускной способностью стимулирует постоянную эволюцию технологий сотовой связи. Сегодня сотовые сети насыщены частотами ниже 3 ГГц. Для обеспечения требуемого увеличения скорости передачи данных требуется бо́льшая пропускная способность в более высокочастотном диапазоне. Из-за растущих требований к пропускной способности мобильные сети 5-го поколения (5G) нацелены на диапазон частот от 3 до 6 ГГц (FR1). Также для сетей 5G планируется использование частот в диапазоне 24–29 ГГц. Несмотря на ожидаемое широкое использование диапазона частот от 3 до 6 ГГц, имеется мало эмпирических данных о потерях в тракте и опыте планирования сетей мобильной радиосвязи. В данной работе разработана методика определения зоны покрытия базовой станции сети 5G при учёте большинства параметров аппаратуры и сигналов для разных моделей распространения сигнала. Получено выражение для определения скорости передачи данных в аппаратуре 5G-NR в режиме TDD. Представлены результаты расчётов зоны покрытия на примере города Новосибирска для частоты 4.8 ГГц. Проанализирована проблема развертывания при планировании покрытия сети 5G .

Ключевые слова: методика определения покрытия сети 5G, определение скорости передачи данных в сети 5G, модель распространения Лонгли–Райса, модель 3GPP 5G-NR.

Для цитирования: Алиев И. В., Носов В. И. Анализ проблемы развертывания при планировании покрытия сети 5G // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 13–31. https://doi.org/10.55648/1998-6920-2024-18-2-13-31.

Статья поступила в редакцию 20.07.2023;
переработанный вариант – 14.12.2023;
принята к публикации 17.12.2023.

1. Введение

Увеличение скорости передачи данных в сотовой сети, удовлетворение потребности растущего спроса на передачу данных, обеспечение необходимым качеством услуг большего количества устройств являются основными задачами при разработке новых поколений сотовой связи. В сетях сотовой связи следующего (пятого) поколения 5G предполагается использование самых разнородных устройств, так называемых устройств Интернета вещей (IoT), увеличение пропускной способности до 20 Гбит/с в нисходящей линии и до 10 Гбит/с в обратном направлении, увеличение количества абонентов в 10–100 раз. Постоянно растущий спрос на передачу данных приведет к острой нехватке доступных полос частот в нижних участках спектра и к росту стоимости радиочастотного спектра. Дефицит проявляется особенно остро в нижних участках частотного спектра до 6 ГГц. Из-за проблем с нехваткой более привлекательного частотного спектра в нижних диапазонах в сетях пятого поколения

рассматривается возможность использования высоких (десятки гигагерц) частот, где возможно применение широких полос частот.

Сеть 5G потребует очень высокого уровня доступности сети (99.999 %) и очень высокой надежности сети (99.99 %), что потребует 100 % покрытия сети [1]. Поэтому оптимальное планирование покрытия сети будет ключевым фактором для обеспечения всех требований сети 5G и предоставления пользователям необходимых услуг. Это позволит выполнить все ключевые показатели эффективности сети 5G.

В то время как диапазон 3.5 ГГц был принят в некоторых частях мира для использования в недавно развернутых сетях 5G NR, для развертывания сетей 5G на территории РФ выбраны диапазоны частот 4.4–4.9 ГГц и 24.25–24.65 ГГц. Поскольку большинство существующих приложений мобильной связи используют частоты ниже 3 ГГц, имеется мало эмпирических данных о потерях в тракте и опыте планирования сетей мобильной радиосвязи для диапазона частот от 3 до 6 ГГц. Соответственно, целью данной работы является определение максимальной дальности связи на частотах диапазона 4.8 ГГц, на которых обеспечиваются все ключевые показатели эффективности сети 5G.

Согласно [2] при использовании модели распространения Лонгли–Райса дальность связи от абонентского терминала (АТ) к базовой станции (БС) в сети 5G составила 27.47 км.

В данной работе разработана методика определения зоны покрытия базовой станции сети 5G при учёте большинства параметров аппаратуры и сигналов с использованием моделей распространения сигнала Лонгли–Райса и рекомендации 3GPP 5G-NR. Представлены результаты расчётов зоны покрытия на примере города Новосибирска для частоты 4.8 ГГц. По полученным результатам произведена сравнительная оценка дальности связи для системы 5G с учетом требуемых запасов на различные условия приёма сигналов. Получено выражение для определения скорости передачи данных в аппаратуре 5G-NR в режиме TDD. Проанализирована проблема развертывания при планировании покрытия сети 5G.

2. Модели распространения радиоволн

В системах связи с подвижными объектами установление соединения по радиоканалу между БС и АТ осуществляется при непрерывном изменении условий радиосвязи. Поэтому произвести точный расчет дальности связи не представляется возможным и приходится оперировать вероятностными величинами. Электромагнитное поле в точке приема является результатом взаимодействия прямой волны и волн, отраженных от поверхности земли, неоднородностей рельефа местности, строений. Кроме того, уровень сигнала в точке приема зависит от условий рефракции земной волны при меняющейся атмосфере, а также от дифракции на местных предметах.

Для описания поведения излучаемого сигнала между передатчиком и приёмником в математической форме используются модели распространения радиоволн. Модели распространения радиоволн используются для определения максимальной дальности связи между передатчиком и приёмником на основе максимально допустимых потерь между ними.

Существуют детерминированные (модель Логли – Райса, метод трассировки лучей, метод изображения), эмпирические (модель Окамура–Хата, 3GPP TR 38.901 5G-NR, COST231 – Уолфиша–Икегами) и стандартизированные модели распространения для планирования радиосетей [4]. Детерминированные модели являются вычислительно сложными, требуют высокой степени детального описания и калибровки среды, способны обеспечить точные результаты. Между тем эмпирические и стандартизированные модели основаны на экспериментальных измерениях и широко применяются для прогнозирования средних потерь на пути распространения как функции расстояния, частоты и некоторых других специфичных параметров. Специфичные параметры, используемые в эмпирических и стандартизованных моделях, зависят от окружающей среды и инфраструктуры. Эмпирические и стандартизированные модели требуют всего несколько параметров для обеспечения приемлемой точности

прогнозирования. Такие модели были оптимизированы для оценки потерь на пути распространения (PL – path loss) при использовании частот диапазона до 2 ГГц, поскольку большинство приложений мобильной связи используют данные частоты. В дальнейшем использование данных моделей было оптимизировано для частот до 2.5 ГГц. На частотах выше 3 ГГц для описания поведения излучаемого сигнала между передатчиком и приёмником возможно использование моделей распространения согласно рекомендациям 3GPP TR 38.901 5G-NR, ITU-R.525-2 и Лонгли–Райса.

Так как недооценка потерь на пути распространения может привести к образованию теневых зон в покрытии, переоценка потерь также нежелательна, поскольку это приводит к серьезным проблемам с межсотовой интерференцией. Для точного прогнозирования существующие модели должны быть оптимизированы для условий, в которых они будут использоваться, и при необходимости скорректированы [5].

При распространении в реальных условиях зачастую сложно соблюдать прямую видимость между приёмником и передатчиком. Кроме того, проникновение сигналов с улицы в помещение зависит от материалов здания и сильно варьируется даже в пределах одной и той же зоны покрытия сотовой связи. В плотной городской застройке на пути распространения радиочастотного сигнала существует много поглощающих и отражающих препятствий (например: здания, автомобили, деревья и т.д.). Потери на пути распространения, включающие потери проникновения в здания, вычисляются согласно рекомендации 3GPP TR 38.913 [6]:

$$PL_{\Sigma} = PL_b + PL_{tw} + PL_{in}, \text{ дБ}, \quad (1)$$

$$L_{\text{Бетон}} = 5 + 4 \cdot f, \text{ дБ}, \quad (2)$$

$$L_{\text{Древесина}} = 4.85 + 0.12 \cdot f, \text{ дБ}, \quad (3)$$

$$L_{\text{Стекло}} = 2 + 0.2 \cdot f, \text{ дБ}, \quad (4)$$

где PL_{Σ} – суммарные потери на пути распространения; PL_b – основные потери в свободном пространстве на пути распространения; PL_{tw} – потери проникновения в здание через внешнюю стену; PL_{in} – потери внутри здания, зависящие от глубины проникновения в здание; f – частота, ГГц.

В табл. 1 приведены модели потерь на пути распространения для условий LOS (наличие прямой видимости) и NLOS (отсутствие прямой видимости) согласно рекомендации 3GPP TR 38.901 5G-NR (соответствует рекомендации МСЭ ITU-R.252-2 [8]) «Исследование модели канала для частот от 0.5 до 100 ГГц» для сценария UMa (Urban Macrocell) [6].

В табл. 1 расстояние до точки разрыва d_{BP} согласно рекомендации 3GPP TR 38.901 определяется как:

$$d_{BP} = 4h_{БС}h_{AT}f / c, \quad (5)$$

где f – частота радиоволны, Гц; $h_{БС}$, h_{AT} – высоты антенн БС и АТ, м; c – скорость света, м/с.

Таблица 1. Модели потерь на пути распространения
согласно рекомендации 3GPP TR 38.901 5G-NR

Сценарий	Условия	Потери [дБ], f_c [ГГц], d [м]	Теневые замирания (shadow fading) [дБ]	Высота антенны (значения по умолчанию)
UMa	LOS	$PL_{UMa-LOS} = \begin{cases} PL_1 \ 10м \le d_{2D} \le d_{BP} \\ PL_2 \ \ d_{BP} \le d_{2D} \le 5км \end{cases}$ $PL_1 = 28.0 + 22\log_{10}(d_{3D}) + 20\log_{10}(f_c)$ $PL_2 = 28.0 + 40\log_{10}(d_{3D}) + 20\log_{10}(f_c) -$ $-9\log_{10}\left((d_{BP})^2 + (h_{БС} - h_{AT})^2\right)$	$\sigma_{SF} = 4$	1.5 м ≤ h_{AT} ≤ 22.5 м $h_{БС}$ = 25 м
	NLOS	$PL_{UMa-NLOS} = \max\left(PL_{UMa-LOS}, PL'_{UMa-NLOS}\right)$ для 10м ≤ d_{2D} ≤ 5 км $PL'_{UMa-NLOS} = 13.54 + 39.08\log_{10}(d_{3D}) +$ $+20\log_{10}(f_c) - 0.6(h_{AT} - 1.5)$	$\sigma_{SF} = 6$	1.5 м ≤ h_{AT} ≤ 22.5 м $h_{БС}$ = 25 м
		Опционально $PL = 32.4 + 20\log_{10}(f_c) + 30\log_{10}(d_{3D})$.	$\sigma_{SF} = 7.8$	

Определение расстояния между приёмником БС и приёмником АТ в модели потерь на пути распространения согласно рекомендации 3GPP TR 38.901 5G-NR приведено на рис. 1.

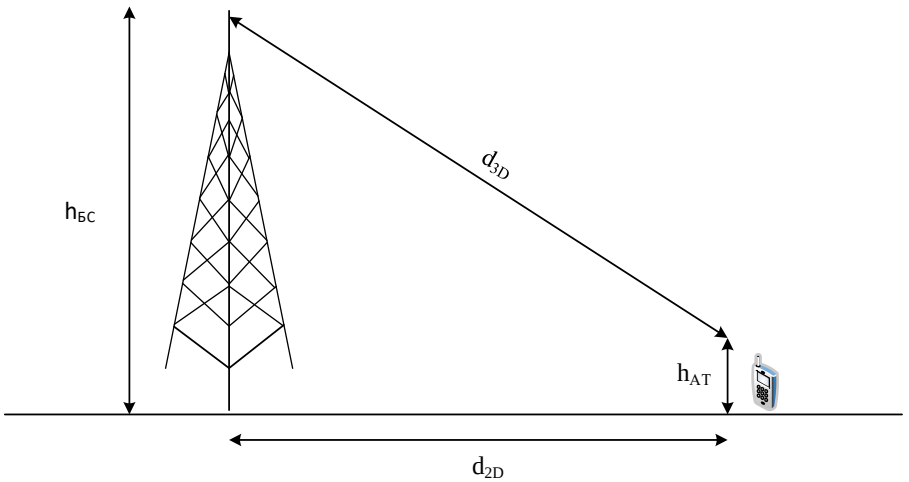


Рис. 1. Определение расстояния между БС и АТ согласно рекомендации 3GPP TR 38.901 5G-NR

Модель Лонгли–Райса (Irregular Terrain Model (ITM)) [9] оценивает потери в тракте распространения радиосигнала от передатчика до приёмника с учётом рельефа местности, включая здания. Данная модель действует в диапазоне частот от 20 МГц до 20 ГГц и обеспечивает оценку потерь в тракте, сочетая физические и эмпирические данные.

Согласно модели Лонгли–Райса, результирующее ослабление PL_0 радиосигнала можно выразить как:

$$PL_0 = PL_{ref} + PL_{fs} + PL_{var}, \qquad (6)$$

где PL_{ref} – ослабление дифракцией и рассеянием радиоволны; PL_{fs} – ослабление свободного пространства; PL_{var} – ослабление изменчивостью условий распространения.

Ослабление радиоволны при распространении в свободном пространстве можно выразить как:

$$PL_{fs} = 20\log\left(4\pi df / c\right), \tag{7}$$

где d – расстояние между передатчиком и приёмником, м.

Входные параметры местности для города Новосибирска [9], характеризующие трассу распространения радиосигнала, использованные в модели Лонгли–Райса, представлены в табл. 2.

Таблица 2. Входные параметры местности

Параметр	Значение
Климат региона	умеренный
Коэффициент рефракции N_0	301
Относительная диэлектрическая проницаемость почвы ε	15
Проводимость почвы σ, См	0.05

Открытая карта улиц OSM (OpenStreetMap – картографический проект по созданию свободной и бесплатной географической карты мира) (рис. 2) и данные рельефа местности (карты SRTM3, Shuttle Radar Topography Mission) для города Новосибирска использованы для определения ослабления сигнала между передатчиком и приёмником.

3. Бюджет радиочастотного канала

Потери на пути распространения определяются как суммарные потери между антенными портами АТ и антенными портами БС и включают в себя усиление антенн, потери в тракте, затенение, потери в здании и т.д.

Рис. 2. Пример OSM-карты для города Новосибирска

Максимально допустимые потери (МДП) – это предельное значение потерь в канале связи, при котором услуга может быть предоставлена, которое, следовательно, определяет зону покрытия услуги. МДП в DL [10]:

$$L_{МДП\ DL} = P_{RAD\ BS\ TX} - P_{SENS\ AT\ RX}, \quad (8)$$

где $P_{RAD\ BS\ TX}$ – эквивалентный уровень излучаемой мощности передающего устройства базовой станции, дБм; $P_{SENS\ AT\ RX}$ – чувствительность приёмника абонентского терминала, дБм.

МДП в UL:

$$L_{МДП\ UL} = P_{RAD\ AT\ TX} - P_{SENS\ BS\ RX}. \quad (9)$$

Предлагаемый шаблон расчета МДП согласно рекомендации 3GPP TR 38.913 приведен в табл. 3.

Таблица 3. Шаблон расчета максимально допустимых потерь

Параметр	Значение
Передатчик	
(1) Уровень излучаемой мощности передатчика, (дБм)	
Приёмник	
(2) Плотность теплового шума (дБм/Гц)	
(3) Коэффициент шума приёмника (дБ)	
(5) Занимаемая полоса частот канала (Гц)	
(6) Уровень мощности теплового шума (2) + (3) + 10 log(5) (дБм)	
(7) Требуемое значение SNR (дБ)	
(8) Чувствительность приёмника (6) + (7) (дБм)	
(9) МДП (1) – (8) (дБ)	

В результате расчёта бюджета канала (рис. 3) определяется уровень мощности сигнала на входе приёмника, который сравнивается с чувствительностью приёмника, чтобы проверить, является ли канал работоспособным.

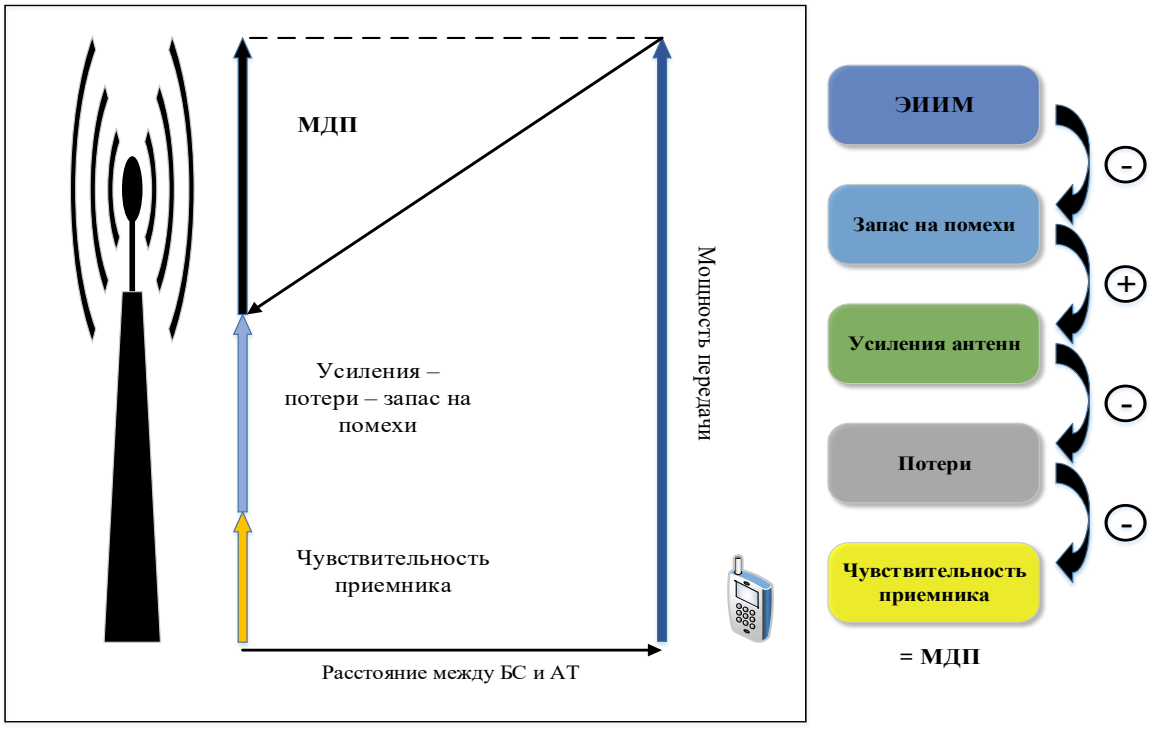


Рис. 3. Принцип расчета энергетического бюджета

Чувствительность приёмника в основном зависит от требований к пропускной способности, поскольку значение SNR напрямую связано с тем, какой пропускной способности мы хотим достичь на границе соты, а для этого важно определить и рассчитать радиус соты.

Предложено выражение для определения скорости передачи данных R_{data} в аппаратуре 5G NR при работе в режиме временного дуплекса TDD:

$$R_{data}\left(Mbps\right)=10^{-6}\cdot K_{par\ subch}\cdot\gamma_{mod}\cdot R_c\cdot BW_{RB}\left(\mu\right)\cdot N_{RB}\cdot\frac{N_{OFDM\ in\ CH}}{N_{OFDM\ in\ SLOT}}\cdot\left(1-OH\right), \quad (10)$$

где $K_{par\ subch}$ – количество параллельных подканалов MIMO, ед; $\gamma_{mod} = \log_2 M_{mod}$ – спектральная эффективность M_{mod} позиционной модуляции, (бит/с)/Гц; R_c – скорость кода, ед; $BW_{RB}(\mu)$ – полоса частот, занимаемая одним ресурсным блоком, Гц; μ – нумерология ед; N_{RB} – количество ресурсных блоков, ед; $N_{OFDM\ in\ CH}$ – количество OFDM-символов в канале DL или UL, ед; $N_{OFDM\ in\ SLOT}$ – количество OFDM-символов в слоте, ед; OH – определяет долю служебной информации, для частотного диапазона FR1 принимает значения 0.14 для канала DL и 0.08 для UL.

Максимально допустимые потери на пути распространения, полученные в табл. 3, с учетом различных видов запаса M_Σ определяются как:

$$L_{МДП} = P_t - L_t + G_t - P_{rsens} - L_r + G_r - M_\Sigma, \text{ дБ}, \quad (11)$$

где P_t – уровень мощности сигнала на выходе передатчика, дБм; $P_{r\ sens}$ – чувствительность приёмника, дБм; G_t, G_r – коэффициенты усиления передающей и приёмной антенн дБи; L_{tf}, L_{rf} – потери в антенно-фидерных трактах передатчика и приёмника, дБ.

Для расчетов зоны покрытия используются основные технические характеристики средств связи, приведенные в табл. 1. Данные, приведенные в табл. 4, соответствуют базовой станции NR Medium Range BS (среднего радиуса действия) [11], [12].

Таблица 4. Характеристики приемопередающей аппаратуры

Параметр	Базовая станция (БС)	Абонентский терминал (АТ)
Уровень мощности передатчика, дБм	38	23
Коэффициент шума приёмника, дБ	7	5
Коэффициент усиления антенны, дБи	21	0
Высота антенны, м	30	1.5

Согласно рекомендации 3GPP 38.213 формат слота включает символы нисходящего канала (D), символы восходящего канала (U) и гибкие символы (F). Рекомендация 3GPP 38.213 определяет 55 форматов слотов для обычного циклического префикса. В табл. 5 приведены некоторые форматы слотов.

Таблица 5. Форматы слотов для обычного циклического префикса

Формат	**Номер символа в слоте**													
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
26	D	D	F	F	F	F	F	F	F	F	F	U	U	U
27	D	D	D	F	F	F	F	F	F	F	F	U	U	U
28	D	D	D	D	D	D	D	D	D	D	D	D	F	U

Расчет энергетического бюджета (табл. 6) выполнен для системы 5G с временным дуплексом, работающим в диапазоне 4800 МГц. Для системы с временным дуплексом выбран

вариант конфигурации кадра формата 27 согласно 3GPP 38.213 [13], системная полоса – 40 МГц.

Таблица 6. Энергетический бюджет для условий плотной городской застройки

TDD, полоса 40 МГц (конфигурация кадра – формат 27 согласно 3GPP 38.213)			
	Параметр	DL	UL
$K_{par\ subch}$	Количество параллельных подканалов MIMO	4	4
$N_{OFDM\ in\ CH}$/ $N_{OFDM\ in\ SLOT}$	Отношение числа OFDM-символов в канале к общему числу OFDM-символов в слоте	9/14 = 0.643	4/14 = 0.286
Передатчик			
P_t	Выходной уровень мощности передатчика, дБм	38.0	23.0
G_t	Коэффициент усиления антенны передатчика, дБи	21	12
L_{tf}	Потери в фидерном тракте передатчика, дБ	1	0
P_{RAD}	ЭИИМ, дБм	58	35
Приёмник			
Δf_{subch}	Расстояние между поднесущими, кГц	30	
N_{RB}	Число используемых ресурсных блоков	8	6
BW_{RB}	Полоса частот ресурсного блока, кГц	360	
M_{mod}	Позиционность модуляции	64QAM	16QAM
R_c	Скорость кодирования	910/1024	658/1024
SNR	Требуемое отношение сигнал/шум, дБ	21	9
R_{data}	Скорость передачи данных на краю соты на абонента, Мбит/с (формула (10))	31.7	
R_{data}	Скорость передачи данных на краю соты от абонента, Мбит/с (формула (10))		5.85
N_0	Спектральная плотность уровня мощности теплового шума (дБм/Гц)	-174	
L_N	Коэффициент шума приёмника, дБ	7	5
P_N	Уровень мощности теплового шума, дБм $P_N = N_0 + L_N + 10\log(BW)$	-102.406	-105.656
$P_{r\ sens}$	Чувствительность приёмника, дБм $P_{r\ sens} = P_N + \mathrm{SNR}$	-81.41	-96.656
G_r	Коэффициент усиления антенны приёмника, дБи	12	21
L_{rf}	Потери в фидерном тракте приёмника, дБ	0	1
Прочие запасы/выигрыши			
M_{int}	Запас на помехи, дБ	6	3.8
M_{build}	Запас на проникновение в помещение, дБ	20	
$M_{foliage}$	Запас на проникновение на открытой местности, дБ	7.5	
M_{shade}	Запас на затенение, дБ	7.8	
$L_{МДП}$	Максимально допустимые потери с запасами, дБ	117.61	116.356

После определения необходимой информации о технических характеристиках используемых средств связи можно определить максимально допустимые потери пути распространения согласно моделям потери распространения радиоволн. Максимально допустимые потери пути распространения на трассе для частот диапазона 4.8 ГГц в нисходящей и восходящей линиях составляют 117.61 и 116.356 дБ соответственно.

После определения величины максимальных допустимых потерь на пути распространения, используя выражения для модели потерь на пути распространения 3GPP TR 38.901 5G-NR (табл. 1), можно определить границу зоны обслуживания для заданного частотного диапазона (рис. 4, 5, 6 и 7).

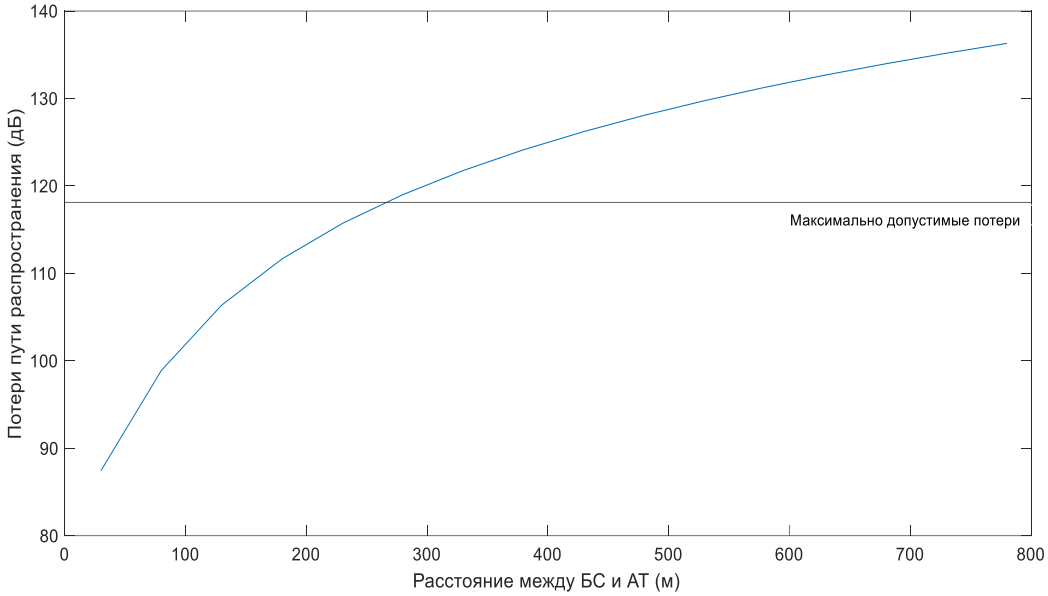


Рис. 4. Ослабление сигнала на входе приёмника АТ в условиях NLOS согласно модели потерь на пути распространения 3GPP TR 38.901 5G-NR

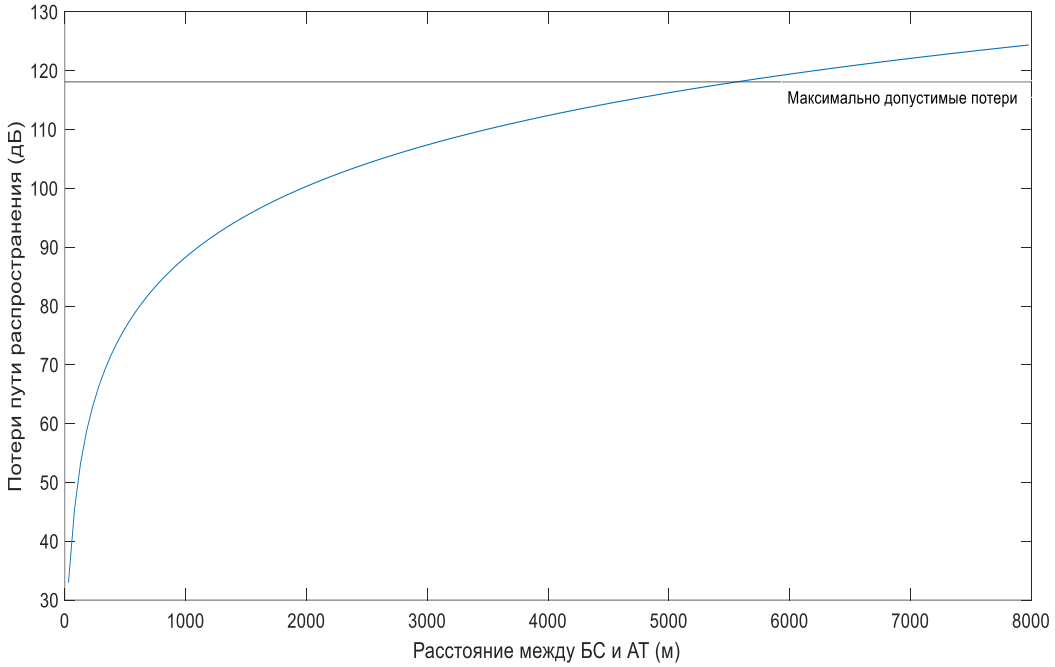


Рис. 5. Ослабление сигнала на входе приёмника АТ в условиях LOS согласно модели потерь пути TR 38.901 5G-NR

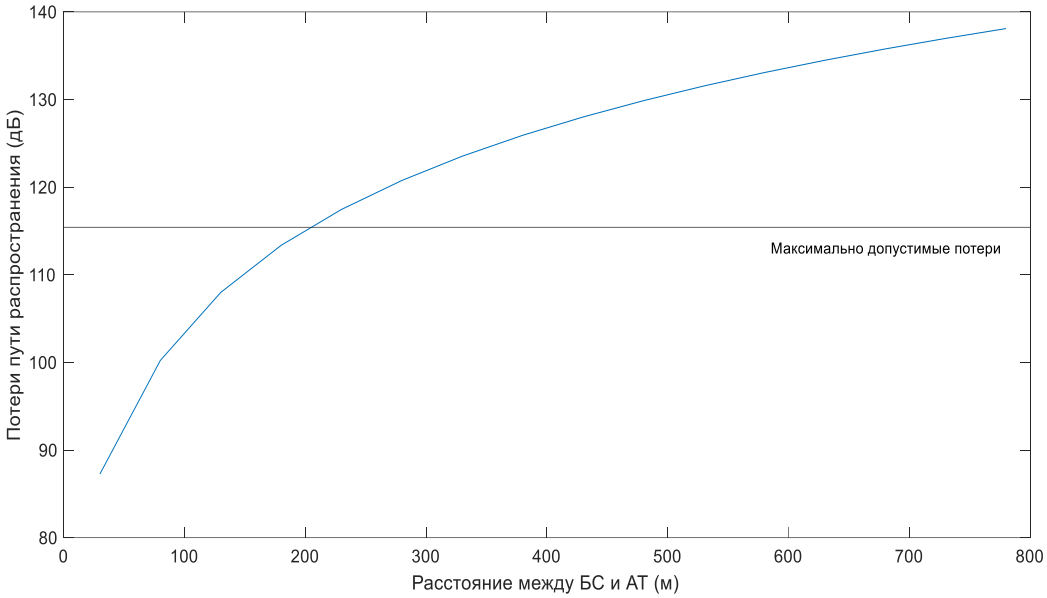


Рис. 6. Ослабление сигнала на входе приёмника БС в условиях NLOS согласно модели потерь пути 3GPP TR 38.901 5G-NR

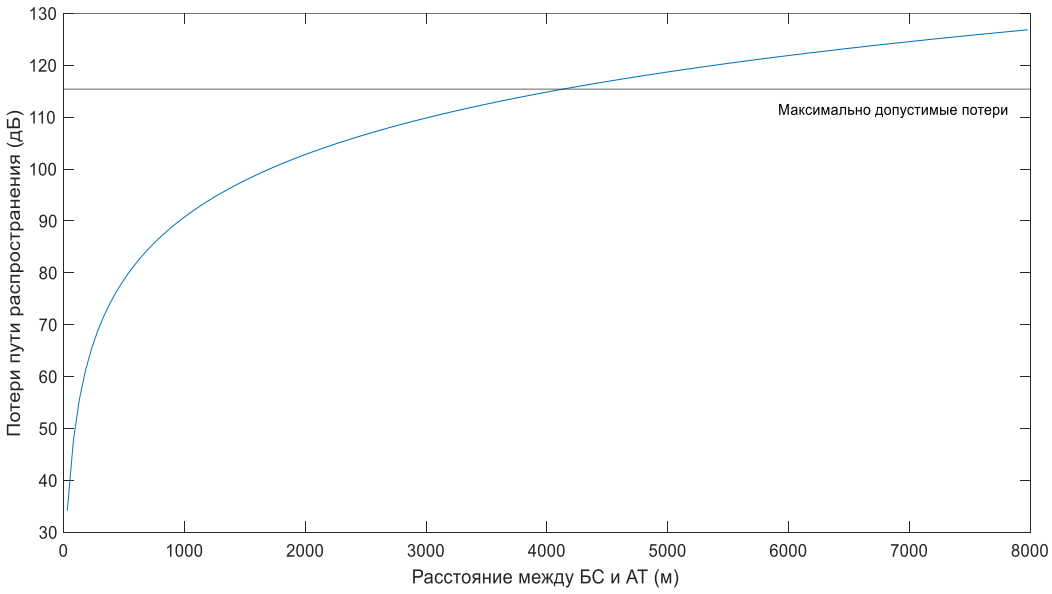


Рис. 7. Ослабление сигнала на входе приёмника БС в условиях LOS согласно модели потерь пути TR 38.901 5G-NR

Модель Лонгли–Райса определяет потери в тракте, связанные с потерями в свободном пространстве, дифракцией на рельефе и препятствиях, отражением от земли, атмосферной рефракцией и тропосферным рассеянием. Данная модель обеспечивает оценку потерь в тракте, сочетая физические и эмпирические данные. На рис. 8, 9, 10 приведены результаты расчета ослабления сигнала согласно модели Лонгли–Райса в условиях плотной городской застройки.

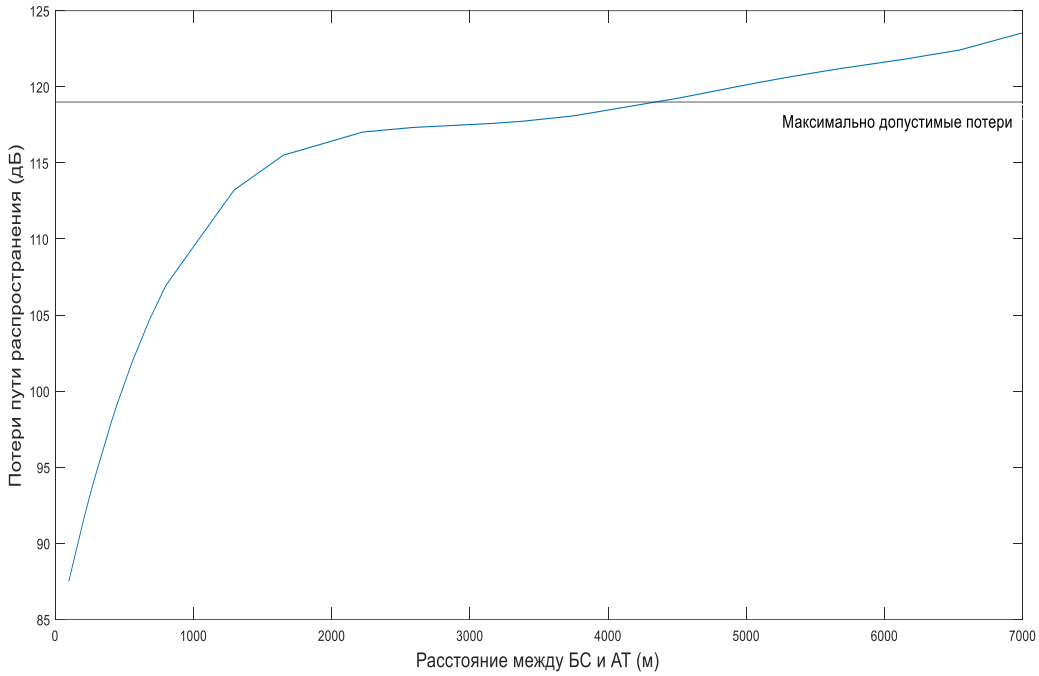


Рис. 8. Ослабление сигнала на входе приёмника АТ в условиях LOS согласно модели Лонгли–Райса

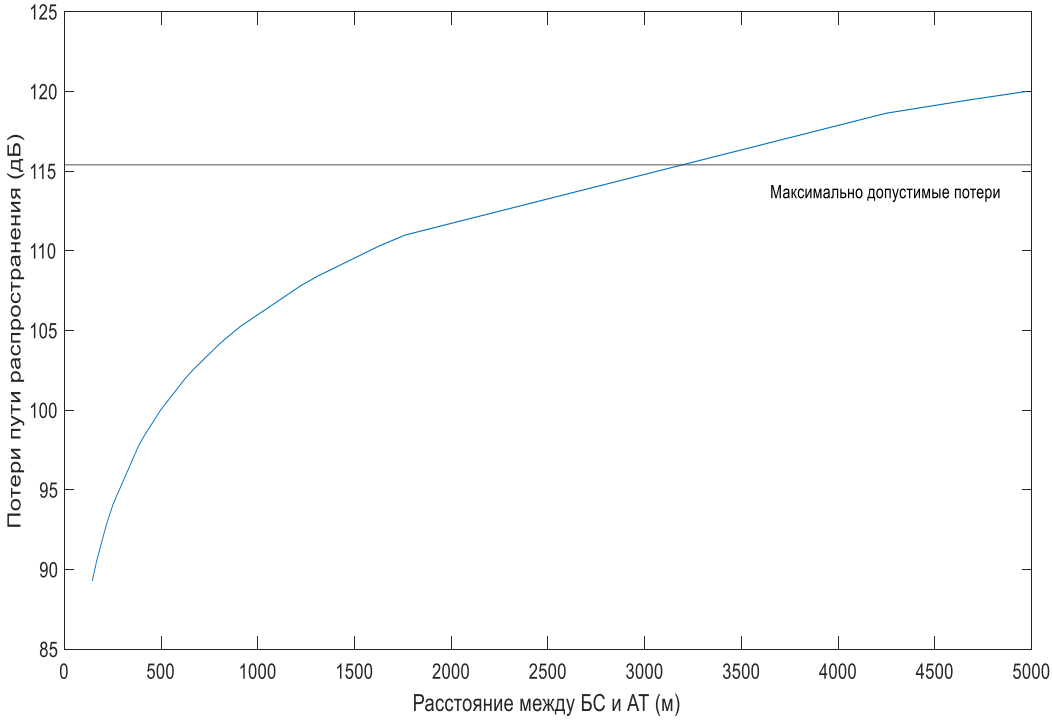


Рис. 9. Ослабление сигнала на входе приёмника БС в условиях LOS согласно модели Лонгли–Райса

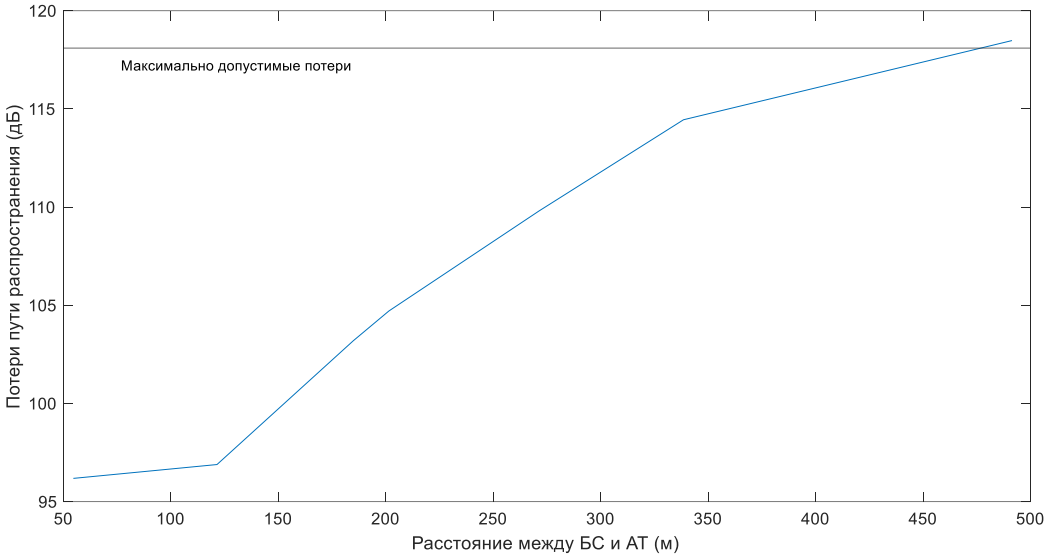


Рис. 10. Ослабления сигнала в условиях NLOS согласно модели Лонгли–Райса

По результатам моделирования с использованием модели Лонгли–Райса в условиях прямой видимости дальность связи на частотах диапазона 4.8 ГГц может составлять до 4.3 км в нисходящей линии и до 3.2 км в восходящей линии. В подавляющем большинстве случаев прямая видимость между БС и АТ отсутствует, т.к. распространение радиосигнала происходит в плотной городской застройке, также учитывается неравномерность рельефа местности, и ослабление сигнала превышает максимально допустимые потери пути распространения. В ситуациях многолучевости, переотражения лучей от различных объектов в условиях отсутствия прямой видимости NLOS максимальная дальность согласно модели Лонгли–Райса может составлять до 450 м. Для обеспечения прямой видимости между приёмником БС и приёмником АТ в условиях плотной городской застройки требуется более плотное расположение БС.

В табл. 7 приведены примерные границы зоны обслуживания и максимальная дальность связи между БС и АТ согласно моделям распространения 3GPP TR 38.901 и Лонгли–Райса для частот диапазона 4.8 ГГц при сценарии UMa LOS и NLOS.

Таблица 7. Максимальная дальность связи между БС и АТ согласно моделям потерь пути распространения согласно рекомендациям 3GPP TR 38.901 и Лонгли–Райса для частот диапазона 4.8 ГГц при сценарии UMa LOS и NLOS

		Максимальная дальность связи от БС к АТ, м	Максимальная дальность связи от АТ к БС, м
	Условия видимости	$f_s = 4.8$ ГГц	
3GPP 5G-NR UMa	NLOS	260	
	LOS	5700	4200
Лонгли–Райса		4300	3200

В результате проведённых расчётов по разработанной методике с учётом городской застройки для условия наличия прямой видимости дальность связи, определенная по двум рассмотренным моделям, составила около 5 км.

Также в результате проведённых расчётов без учёта карты городской застройки в условиях отсутствия помех (без учета запасов) и для условия наличия прямой видимости дальность связи, определенная по модели Лонгли–Райса, составила 26.5 км (рис. 11).

Согласно [2] при использовании модели Лонгли–Райса дальность связи в условиях прямой видимости без учёта городской застройки составила 27 км.

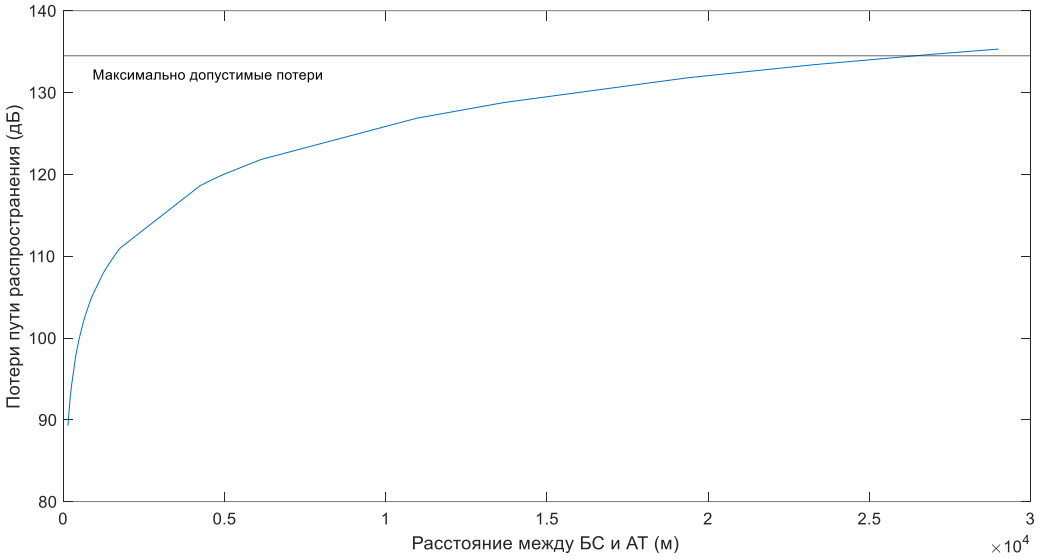


Рис. 11. Ослабление сигнала согласно модели Лонгли–Райса
без учета карты городской застройки и без учета помех

Таким образом, можно утверждать, что результаты определения дальности связи, полученные с использованием предложенной методики, практически совпадают с результатами, полученными другими авторами.

4. Анализ проблемы развертывания при планировании покрытия сети 5G

Ключевая особенность сетей сотовой связи заключается в том, что общая зона покрытия делится на ячейки (соты), определяющиеся зонами покрытия отдельных базовых станций. Соты частично перекрываются и вместе образуют сеть. Зона покрытия сотовой сети (рис. 12) – область, в которой каждая БС покрывает определенную географическую область и предоставляет услуги всем абонентским терминалам, находящимся в этой области. Эта область называется ячейкой. Ячейка состоит из всех географических точек, где данная БС обеспечивает необходимый уровень приемного сигнала.

В условиях плотных городских застроек общая зона покрытия сетей мобильной связи состоит из двух основных уровней, сосуществующих на одной территории [12]:

1. Уровень покрытия: состоит из открытых (outdoor) БС, которые обеспечивают широкое покрытие, поддержку мобильности и используются совместно многими АТ.

2. Уровень точек доступа: состоит в основном из внутренних (indoor) БС, которые обеспечивают высокую пропускную способность в небольших локальных зонах для нескольких АТ.

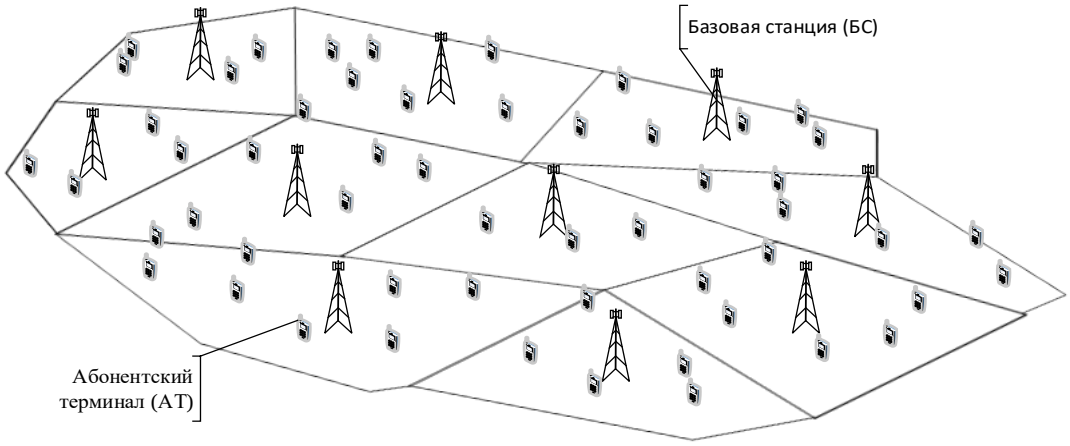


Рис. 12. Зона покрытия сотовой сети

Зоны покрытия соты – область вокруг базовой станции, где пользователь может успешно соединиться с БС и получать услуги приемлемого качества. Радиус соты определяет максимальную границу покрытия соты, и пользователь не будет устанавливать соединения за границей соты. Рассчитав радиус соты, мы можем оценить количество сотовых сайтов, необходимых для покрытия зоны развертывания. При планировании зоны покрытия для исключения внесотовых помех, помех от БС, расположенных в соседних сотах, между БС, расположенными в соседних сотах, должно поддерживаться определенное минимальное расстояние, называемое межсотовым расстоянием (ISD – Inter-Site Distance). Если минимальное расстояние ISD не соблюдается, пользователи могут получать более одного доминирующего сигнала от соседних сотовых станций, что называется внесотовой интерференцией, которая может значительно ухудшить производительность сети.

Более низкие частоты обладают хорошей проникающей способностью и способны обеспечить качественное обслуживание с точки зрения расстояния распространения и надёжности при малых затратах. С другой стороны, очень широкие полосы пропускания могут быть использованы только в более высоких диапазонах частот, где возможно достижение пиковых скоростей. Однако с увеличением частоты сигнала увеличиваются потери распространения, уменьшается эффективное расстояние передачи информации, следовательно, потребуется более плотное расположение БС.

Для улучшения пропускной способности и уровня покрытия особенно важно увеличить спектральную эффективность, поскольку плотность установки БС и использование дополнительной полосы пропускания на более высоких частотах ухудшат поддержку мобильности и покрытие.

Спектральная эффективность канала (бит/с/Гц) – это количество битов информации, которое можно передать по каналу передачи за единицу времени на единицу радиочастотного спектра.

Пропускная способность канала, или предельная скорость передачи информации, определяется теоремой Шеннона:

$$C \le K \cdot W \cdot \log_2 \left(1 + SNR\right), \text{ бит/с}, \tag{12}$$

где K – число пространственно ортогональных пользователей; W – полоса пропускания канала; SNR – отношение сигнал/шум.

В зависимости от применяемых схем кодирования/декодирования за счёт изменения требуемого значения SNR в канале передачи между приёмником и передатчиком можно достичь разных значений пропускной способности.

При использовании технологии MIMO передача и приём с пространственным разнесением может увеличить суммарную пропускную способность более чем на порядок за счет одновременного обслуживания K пространственно ортогональных пользователей.

Дефицит свободных частот в нижних участках спектра приводит к необходимости использования частот в более высоких диапазонах спектра. Путем использования массива антенн на высоких частотах можно компенсировать увеличивающиеся потери распространения.

Уровень мощности принимаемого сигнала P_r на входе приёмника АТ при коэффициенте усиления его антенны определяется как:

$$P_r = P_t + G_t + G_r - L_0 . \tag{13}$$

Коэффициент усиления антенны равен:

$$G_t = G_r = 10 \cdot \log_{10}(4 \cdot \pi \cdot S_a / \lambda^2), \tag{14}$$

где λ – длина волны; S_a – апертура антенной решетки.

Затухание в свободном пространстве равно:

$$L_0 = 10 \cdot \log_{10}\left(4 \cdot \pi \cdot d / \lambda\right)^2 . \tag{15}$$

С учётом уравнений (14) и (15) уровень мощности принимаемого сигнала P_r (14) будет равен

$$P_r = P_t + 2 \cdot 10 \cdot \log_{10}\left(S_a / \left(4 \cdot \pi \cdot d^2\right)\right) - L_0 . \tag{16}$$

Из уравнения (16) следует, что для рассматриваемых условий уровень мощности принимаемого сигнала на входе приёмника не зависит от длины волны, так как в соответствии с уравнением (14) с увеличением частоты рост затухания сигнала в среде распространения L_0 компенсируется ростом коэффициента усиления антенной решётки.

Количество антенн на массив с фиксированной апертурой при расстоянии между антеннами, равном $d = \lambda/2$, равно:

$$S_a = \left(M_x \cdot d_x\right) \cdot \left(M_y \cdot d_y\right) = \left(M_x \cdot M_y\right) \cdot \frac{\lambda^2}{4}, \tag{17}$$

где M_x, M_y – количество антенн в строке (горизонтальная плоскость) и столбце (вертикальная плоскость) плоской прямоугольной антенной решётки.

Необходимо отметить, что ширина диаграммы направленности в горизонтальной плоскости зависит от количества антенн M_x, а ширина диаграммы направленности в вертикальной плоскости зависит от количества антенн M_y. Если через M_Σ обозначить общее количество антенн в антенной решётке

$$M_\Sigma = M_x \cdot M_y , \tag{18}$$

то общее количество антенн в антенной решётке будет равно

$$M_\Sigma = 4 \cdot S_a / \lambda^2 . \tag{19}$$

Это означает, что освоение более высоких диапазонов частот приведет к увеличению общеего количества антенн, т.к. количество антенн на массив с фиксированной апертурой обратно пропорционально квадрату длины волны.

Плотность антенн D_a есть отношение M_Σ к площади зоны обслуживания $S_з$:

$$D_a = M_\Sigma / S_з = M_\Sigma \Big/ \left(\pi \cdot R_з^2\right). \tag{20}$$

Из (20) следует, что при одинаковой энергетической эффективности в сети сотовой связи можно применять либо соты с большим радиусом зоны обслуживания (макросоты) и большим массивом антенн, либо большое количество сот с малым радиусом зон обслуживания (микросоты) и с небольшим количеством антенн в каждой соте.

В свободном пространстве с равномерным распределением пользователей U количество ортогональных каналов K_U, генерируемых M-MIMO, равно числу антенн массива $K_U = M_\Sigma$, поэтому плотность пользователей равна плотности антенн:

$$D_U = K_U / S_з = M_\Sigma / S_з. \tag{21}$$

Это означает, что для обеспечения такой же плотности пользователей мы можем либо использовать одну большую макроячейку, оборудованную большим числом антенн, либо много маленьких микроячеек, оборудованных небольшим количеством антенн каждая.

В соответствии с (12) и (21) пропускная способность этих двух вариантов построения сети будет одинаковой, так как обслуживаемая ими площадь одинаковая:

$$C_{macro} \le K_{U\ macro} \cdot W \cdot \log_2\left(1 + SNR\right), \tag{22}$$

$$C_{micro} \le \sum_{i=1}^{N} K_{U\ i\ micro} \cdot W \cdot \log_2\left(1 + SNR\right), \tag{23}$$

5. Заключение

В данной работе разработана методика определения зоны покрытия базовой станции сети 5G при учёте большинства параметров аппаратуры и сигналов для разных моделей распространения. Учитывается количество параллельных подканалов системы MIMO, число которых определяется рангом матрицы $K \le \min\{M, N\}$, где M, N – количество антенн на передающей и приёмных сторонах соответственно. В режиме временного разделения дуплекса TDD определяется отношение числа OFDM-символов в канале DL или UL к общему числу OFDM-символов в слоте. Также определяется коэффициент усиления плоской многоэлементной антенной решётки. При расчётах учитываются запасы на помехи, на проникновение сигнала в помещение, на затенение.

В результате проведённых расчётов по предложенной методике определены границы зоны обслуживания в сети 5G с использованием моделей распространения 3GPP TR 38.901 и Лонгли–Райса для частот диапазона 4.8 ГГц при сценарии UMa LOS и NLOS.

Дальность связи, определенная по двум рассмотренным моделям, с учётом городской застройки для условия наличия прямой видимости составила около 5 км. Дальность связи при использовании модели 3GPP TR 38.901 в условиях отсутствия прямой видимости не превышает 260 м, а при использовании модели Лонгли–Райса, которая учитывает переотражение лучей от различных объектов, дальность может составлять до 450 м.

Также в результате проведённых расчётов без учёта карты городской застройки и без учета запасов для условия наличия прямой видимости дальность связи, определенная по модели Лонгли–Райса, составила 26.5 км.

Получено выражение для определения скорости передачи данных в аппаратуре 5G-NR в режиме TDD. Это выражение учитывает ранг матрицы MIMO, спектральную эффективность M позиционной модуляции, $\gamma_{mod} = \log_2 M_{mod}$, (бит/с)/Гц; полосу частот, занимаемую одним ресурсным блоком, количество OFDM-символов в канале DL или UL, количество OFDM-символов в слоте.

Проанализирована проблема развертывания при планировании покрытия сети 5G. Показано, что при обеспечении одинаковой пропускной способности возможны два равноценных варианта построения сетей при использовании либо одной большой макроячейки, оборудованной большим числом антенн, либо многих маленьких микроячеек, оборудованных небольшим количеством антенн каждая.

Литература

1. *Ahamed M. M., Faruque S.* 5G Network Coverage Planning and Analysis of the Deployment Challenges // Sensors. 2021. P. 6608.
2. *Мовчан А. К., Рогожников Е. В., Дмитриев Э. М., Новичков С. А., Лаконцев Д. В.* Расчет ослабления сигнала сетей сотовой связи 5G для частот диапазона FR1 // Доклады ТУСУР. 2022. Т. 23, № 1. С. 17 – 23.
3. *Sarkar T. K., Wicks M. C., Salazar-Palma M., Bonneau R. J.* Smart Antennas. A survey of various propagation models for mobile communication. P. 239–307.
4. Data sheet 3GPP TR 38.901 V17.0.0 Release 17. URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.901 (дата обращения: 28.04.2023).
5. [IMT-2020.EVAL], Guidelines for Evaluation of Radio Interface Technologies for IMT-2020. 2017. URL: https://www.itu.int/md/R15-SG05-C-0057 (дата обращения: 04.08.2022).
6. *Hufford G. A., Longley A. G., Kissick W. A.* A guide to the use of the ITS irregular terrain model in the area prediction mode / US Department of Commerce, National Telecommunications and Information Administration. NTIA REPORT 82-100, 1982. 73 p.
7. Data sheet 3GPP TR 38.913 version 17.0.0 Release 17 URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.913 (дата обращения: 15.03.2023).
8. *Proakis J. G., Salehi M.* Digital Communications, 5th ed.; McGraw-Hill Education: New York, NY, USA, 2007. P. 1170.
9. Data sheet 3GPP TS 38.104 version 17.4.0 Release 17 URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.104 (дата обращения: 15.03.2023).
10. Data sheet 3GPP TS 38.101 version 17.4.0 Release 17 URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.101-1 (дата обращения: 15.03.2023).
11. Data sheet 3GPP TS 38.213 version 17.1.0 Release 17 URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.213 (дата обращения: 15.03.2023).
12. *Bjornson E., Hoydis J., and Sanguinetti L.* Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency // Foundations and Trends in Signal Processing. 2017. V. 11, № 3–4. P. 154–655. DOI: 10.1561/2000000093.

Алиев Исфандиёр Вакосович

аспирант кафедры цифрового телерадиовещания и систем радиосвязи, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), тел. +7 383 2698 254, e-mail: aliev_i_v@mail.ru, ORCID ID: 0009-0007-0300-0494.

Носов Владимир Иванович

д.т.н., профессор кафедры цифрового телерадиовещания и систем радиосвязи, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), тел. +7 383 2698 254, e-mail: nvi@sibguti.ru, ORCID ID: 0000-0003-2671-4258.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия, как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи*

Analysis of the Deployment Problem when Planning 5G Network Coverage

Isfandier V. Aliev, Vladimir I. Nosov

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: Global demand for higher bandwidth mobile Internet services stimulates the constant evolution of cellular technologies. Today, cellular networks are saturated with frequencies below 3 GHz. To achieve the required increase in data rates, more bandwidth is required in the higher frequency range. Due to increasing bandwidth requirements, 5th generation (5G) mobile networks are targeting the frequency range of 3 to 6 GHz (FR1). It is also planned to use frequencies in the 24-29 GHz range for 5G networks. Despite the expected widespread use of the frequency range from 3 to 6 GHz, there is little empirical data on path losses and experience in mobile radio network planning. In this paper, a methodology has been developed for determining the coverage area of the 5G network base station taking into account most equipment and signal parameters for different signal propagation models. An expression has been obtained to determine the data transfer rate in 5G-NR equipment in TDD mode. Calculations results of the coverage area are presented using the example for the city of Novosibirsk for a frequency of 4.8 GHz. The deployment problem when planning 5G network coverage is analyzed.

Keywords: methodology for determining 5G network coverage; determination of data transfer speed in the 5G network; Longley-Rice and 3GPP 5G-NR propagation models.

For citation: Aliev I. V., Nosov V. I. Analysis of the deployment problem when planning 5G network coverage (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 13-31. https://doi.org/10.55648/1998-6920-2024-18-2-13-31.

The article was submitted: 20.07.2023;
revised version: 14.12.2023;
accepted for publication 17.12.2023.

References

1. Ahamed, M.M.; Faruque, S. *5G Network Coverage Planning and Analysis of the Deployment Challenges*. Sensors 2021, 21, 6608.
2. Movchan A. K., Rogozhnikov E. V., Dmitriev E. M., Novichkov S. A., Lakontsev D. V. Raschet oslableniya signala setei sotovoi svyazi 5G dlya chastot diapazona FR1 [Calculation of signal attenuation of 5G cellular networks for frequencies in the FR1 range]. *Dokladi TUSUR*, 2022, vol. 23, no. 1, pp. 17-23.
3. Tapan K. Sarkar, Michael C. Wicks, Magdalena Salazar-Palma, Robert J. Bonneau. A survey of various propagation models for mobile communication. *Smart Antennas*, Wiley-IEEE Press, 2003, pp. 239-307.
4. Data sheet 3GPP TR 38.901 V17.0.0 Release 17 available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.901 (accessed: 28.04.2023).
5. [IMT-2020.EVAL], *Guidelines for Evaluation of Radio Interface Technologies for IMT-2020*. 2017. available at: https://www.itu.int/md/R15-SG05-C-0057 (accessed: 04.08.2022).
6. Hufford G. A., Longley A. G., Kissick W. A. *A guide to the use of the ITS irregular terrain model in the area prediction mode*. US Department of Commerce, National Telecommunications and Information Administration, NTIA REPORT 82-100, 1982. 73 p.
7. Data sheet 3GPP TR 38.913 version 17.0.0 Release 17 available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.913 (accessed: 15.03.2023).
8. Proakis J. G.; Salehi M. *Digital Communications*. 5th ed., McGraw-Hill Education: New York, NY, USA, 2007, p. 1170.
9. Data sheet 3GPP TS 38.104 version 17.4.0 Release 17 available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.104 (accessed: 15.03.2023).
10. Data sheet 3GPP TS 38.101 version 17.4.0 Release 17 available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.101-1 (accessed: 15.03.2023).
11. Data sheet 3GPP TS 38.213 version 17.1.0 Release 17 available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.213 (accessed: 15.03.2023).
12. Emil Bjornson, Jakob Hoydis and Luca Sanguinetti, Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency. *Foundations and Trends in Signal Processing*, 2017, vol. 11, iss. 3-4, pp. 154-655. DOI: 10.1561/2000000093.

Isfandiyor V. Aliev

Postgraduate of the Department of Digital Broadcasting and Radio Communication Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 254, e-mail: aliev_i_v@mail.ru, ORCID ID: 0009-0007-0300-0494.

Vladimir I. Nosov

Dr. of Sci. (Engineering), Professor; Professor of the Department of Digital Broadcasting and Radio Communication Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 254, e-mail: nvi@sibguti.ru, ORCID ID: 0000-0003-2671-4258.

DOI: 10.55648/1998-6920-2024-18-2-32-42 УДК 621.394

Анализ иерархической системы управления сетями связи при ограниченной надежности элементов системы

В. И. Мейкшан, Ю. С. Лизнева, Е. В. Ростова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: При анализе иерархической системы управления сетями связи используется математический аппарат теории сетей массового обслуживания. Особенность и научная новизна построенной модели заключается в том, что учитывается ограниченная надежность элементов системы. Представленные результаты численных расчётов демонстрируют влияние коэффициента готовности элементов системы управления на показатели, характеризующие время реакции системы при поступлении запросов, связанных с процессами технического обслуживания и эксплуатации сетевых объектов.

Ключевые слова: сети связи, система управления, очереди заявок, приоритеты, среднее время реакции.

Для цитирования: Мейкшан В. И., Лизнева Ю. С., Ростова Е. В. Анализ иерархической системы управления сетями связи при ограниченной надежности элементов системы // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 32–42. https://doi.org/10.55648/1998-6920-2024-18-2-32-42.

Статья поступила в редакцию 24.11.2023;
принята к публикации 24.12.2023.

1. Введение

В сфере управления современными сетями связи фактическим стандартом является широко распространенная концепция TMN (Telecommunications Network Management), ей посвящена специальная серия Рекомендаций М.3000 Сектора телекоммуникаций Международного союза электросвязи (МСЭ-Т). В пирамиде TMN функции управления распределяются по следующим уровням [1, 2]:

- каждый элемент сети (Network Element – NE) снабжается собственным агентом для выполнения базовых функций непосредственного управления конкретным объектом;
- подсистема EMS (Element Management System) осуществляет управление некоторой группой сетевых элементов, образующих отдельный фрагмент (домен) сети;
- подсистема NMS (Network Management System) относится к самому верхнему уровню и обеспечивает функции интегрированного управления в масштабе всей сети оператора связи.

Со временем многие основополагающие принципы, заложенные в идеологию построения TMN, благополучно мигрировали в сугубо технологические модели, определяющие состав, архитектуру и функциональность реальной системы эксплуатационной поддержки (Operation Support System – OSS). В частности, обозначенный подход, предполагающий разделение от-

дельных элементов интегрированной системы управления по функциональным уровням, сохраняется и в концепции NGOSS, которая направлена на формирование универсальной методологии разработки, внедрения и развития систем OSS операторов связи [3, 4].

При наличии сложной структуры системы управления сетью связи (СУСС) эффективная работа СУСС во многом зависит от совместного влияния большого числа факторов. По этой причине задачи анализа качества функционирования СУСС постоянно привлекают к себе внимание отечественных и зарубежных авторов. Применительно к многоуровневой архитектуре СУСС, построенной в полном соответствии с концепцией TMN, наибольший интерес представляют исследования, в которых моделируются процессы взаимодействия сразу нескольких уровней иерархии СУСС [5–7].

Особого внимания заслуживает работа [7], где предлагается комплексная модель СУСС в классе сетей массового обслуживания (СеМО). Настоящая статья посвящена развитию этой модели на случай, когда элементы исследуемой СУСС могут выходить из строя, т.е. имеют ограниченную надежность.

2. Функциональная модель СУСС

Общая топология сети очередей, с помощью которой моделируется работа исследуемой системы, представлена на рис. 1 в укрупненном виде (т.е. на уровне «макроузлов», соответствующих типовым функциональным модулям СУСС).

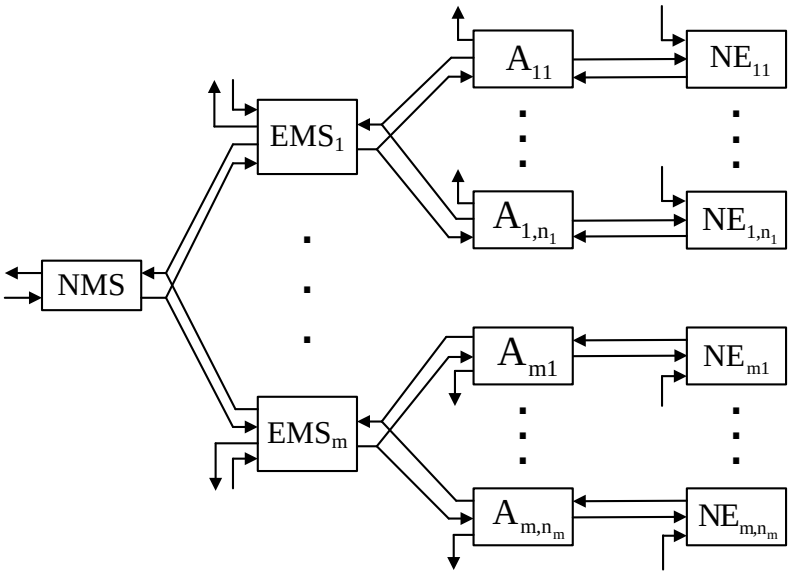


Рис. 1. Модель системы OSS в виде сети СМО

Внутренняя структура отдельных «макроузлов» детализируется на рис. 2, где обозначены следующие элементы СеМО:

- входная (*NI*) и выходная (*NO*) очереди подсистемы NMS;
- входная (EI_i) и выходная (EO_i) очереди подсистемы EMS_i, которая установлена в одном из региональных центров управления (РЦУСС) и охватывает i-й фрагмент (домен) сети связи ($i = \overline{1,m}$);
- входная (AI_{ij}) и выходная (AO_{ij}) очереди в составе агента A_{ij}, который подчиняется подсистеме EMS_i ($i = \overline{1,m}$; $j = \overline{1,n_i}$);

▪ QE_{ij} – очередь заявок к процессору эксплуатации и технического обслуживания (Operation and Maintenance Processor – OMP) для элемента сети NE_{ij}, который управляется агентом A_{ij} ($i=\overline{1,m}$; $j=\overline{1,n_i}$).

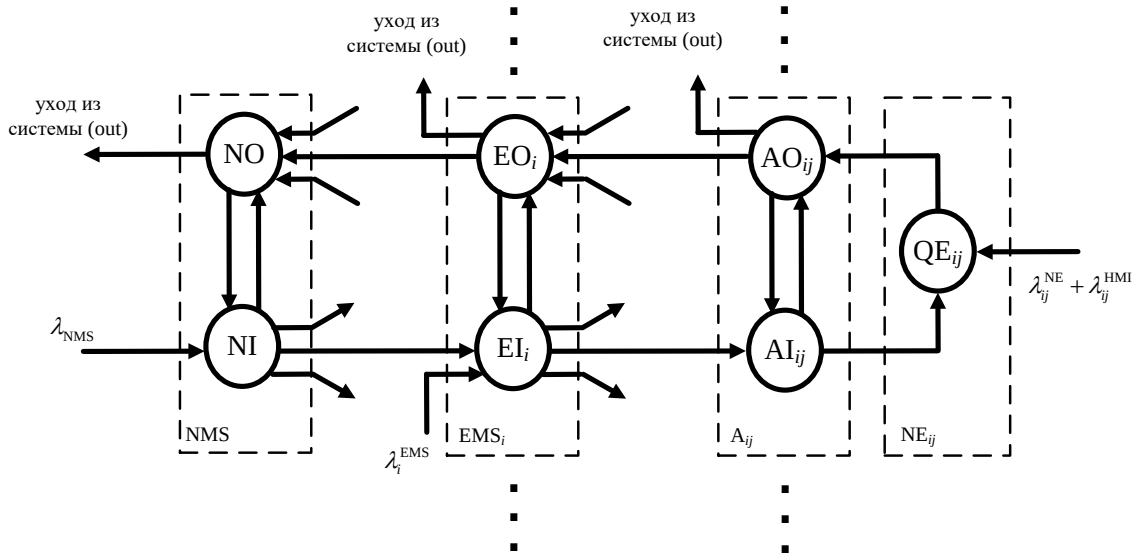


Рис. 2. Внутренняя структура «макроузлов»

Наличие входных и выходных очередей обусловлено стандартной схемой взаимодействия «менеджер – агент» [1]. Входные очереди преимущественно имеют дело с командами (директивами), поступающими от менеджера к агенту, а выходные очереди связаны с формированием ответной реакции на эти команды.

3. Построение математической модели СУСС

Распределение потоков заявок между элементами СеМО принято описывать с помощью маршрутной матрицы $\Theta = ||\theta(i, j)||$, в которой элемент $\theta(i, j)$ определяет вероятность того, что заявки после обслуживания в очереди i переходят в очередь j. Для рассматриваемой СеМО (рис. 2) ненулевые элементы маршрутной матрицы представлены в табл. 1.

Таблица 1 Маршрутная матрица для исследуемой СеМО

Элементы маршрутной матрицы ($i=\overline{1,m}$; $j=\overline{1,n_i}$)	Пояснения
$\theta(NO, \text{out}) = P_{NO}$	После пребывания в очереди *NO* заявки с вероятностью P_{NO} уходят из СеМО, а с дополнительной вероятностью $P'_{NO}=1-P_{NO}$ возникают внутренние заявки, т.е. заявки возвращаются во входную очередь *NI* для повторной обработки.
$\theta(NO, \text{NI}) = P'_{NO}$	
$\theta(NI, EI_i) = P_i^{EI}$	После обработки в NMS заявки из очереди *NI* с вероятностью P_i^{EI} направляются в подсистему EMS$_i$, а с вероятностью P_0^{EI} обслуженная заявка из очереди *NI* замыкается в пределах NMS, т.е. переходит в очередь *NO*.
$\theta(NI, NO) = P_0^{EI}$	
$\theta(EO_i, \text{out}) = P_i^{ex}$	После обслуживания в очереди EO_i заявка с вероятностью P_i^{ex} покидает СеМО.

$\theta(EO_i, NO) = P_i^{EO}$	Заявка, которая прошла обслуживание в очереди EO_i, с вероятностью P_i^{EO} направляется в очередь NO.
$\theta(EO_i, EO_i) = 1 - P_i^{EO} - P_i^{ex}$	С вероятностью $1 - P_i^{EO} - P_i^{ex}$ обслуженные заявки из очереди EO_i становятся внутренними заявками, т.е. направляются на повторное обслуживание.
$\theta(EI_i, A_{ij}) = P_{ij}^{AI}$	Обслуженная заявка из очереди EI_i с вероятностью P_{ij}^{AI} посылается агенту A_{ij}, а с вероятностью P_{i0}^{AI} поступает для дальнейшей обработки в очередь EO_i.
$\theta(EI_i, EO_i) = P_{i0}^{AI}$	
$\theta(AO_{ij}, EO_i) = P_{ij}^{F}$	После анализа внутренних и внешних уведомлений, которые накапливаются в очереди AO_{ij} агента A_{ij}, в очередь EO_i подсистемы EMS_i передается только часть обработанных уведомлений, определяемая вероятностью P_{ij}^{F} .
$\theta(AO_{ij}, \text{out}) = 1 - P_{ij}^{F}$	
$\theta(AI_{ij}, QE_{ij}) = P_{ij}^{NE}$	Результаты обработки команды (директивы), принятой агентом A_{ij}, с вероятностью P_{ij}^{NE} получает объект управления, т.е. сетевой элемент NE_{ij}, а с дополнительной вероятностью $1 - P_{ij}^{NE}$ обработка команды завершается посылкой внутреннего уведомления в выходную очередь AO_{ij} этого агента.
$\theta(AI_{ij}, AO_{ij}) = 1 - P_{ij}^{NE}$	
$\theta(QE_{ij}, AO_{ij}) = 1$	Процессор ОМР после обработки каждой заявки отправляет соответствующее уведомление в очередь AO_{ij}.

Маршрутную матрицу часто называют дискретной топологической характеристикой СеМО [8], и при анализе сети очередей она играет ключевую роль. В частности, с учетом ненулевых элементов маршрутной матрицы из таблицы 1 несложно записать следующую систему линейных алгебраических уравнений (СЛАУ), которые выражают условия глобального равновесия для СеМО в целом:

$$\left.\begin{aligned}
\lambda_{NI} &= \lambda_{NMS} + P'_{NO}\lambda_{NO} \\
\lambda_{NO} &= P_0^{EI}\lambda_{NI} + \sum_{i=1}^{m} P_i^{EO}\lambda_i^{EO} \\
\lambda_i^{EI} &= \lambda_i^{EMS} + P_i^{EI}\lambda_{NI} + (1 - P_i^{EO} - P_i^{ex})\lambda_i^{EO} \\
\lambda_i^{EO} &= P_{i0}^{AI}\lambda_i^{EI} + \sum_{j=1}^{n_i} P_{ij}^{F}\lambda_{ij}^{AO} \\
\lambda_{ij}^{AI} &= P_{ij}^{AI}\lambda_i^{EI} \\
\lambda_{ij}^{AO} &= \lambda_{ij}^{QE} + (1 - P_{ij}^{NE})\lambda_{ij}^{AI} \\
\lambda_{ij}^{QE} &= \lambda_{ij}^{NE} + \lambda_{ij}^{HMI} + P_{ij}^{NE}\lambda_{ij}^{AI}
\end{aligned}\right\} \qquad (1)$$

В дополнение к параметрам из табл. 1 в этой СЛАУ присутствуют интенсивности λ_{NMS}, λ_i^{EMS}, λ_{ij}^{NE} и λ_{ij}^{HMI}, которые характеризуют потоки заявок от внешних источников, относящихся к разным уровням рассматриваемой СУСС (рис. 2).

Дальнейшие действия включают в себя:

1) решение полученной СЛАУ, что позволяет найти для каждой очереди в составе рассматриваемой СеМО полную интенсивность входного потока заявок;

2) независимый анализ отдельных СМО, что соответствует хорошо известному принципу декомпозиции, который широко применяется для исследования сложных систем, описываемых с помощью сети очередей [9, 10].

Сформулированный подход более подробно проиллюстрируем на примере полностью однородной структуры СУСС, т.е. $n_i = n = const$ при всех $i = \overline{1,m}$. Также предполагается, что все однотипные структурные элементы системы имеют одинаковые значения функциональных параметров: $P_i^{EI} = P_{EI}$, $P_i^{EO} = P_{EO}$, $P_i^{ex} = P_{ex}$, $P_{ij}^{AI} = P_{AI}$, $P_{ij}^{AO} = P_{AO}$, $P_{ij}^{F} = P_F$, $P_{ij}^{NE} = P_{NE}$, $\lambda_i^{EMS} = \lambda_{EMS}$, $\lambda_{ij}^{NE} = \lambda_{NE}$, $\lambda_{ij}^{HMI} = \lambda_{HMI}$ при любых $i = \overline{1,m}$ и $j = \overline{1,n}$.

В этом случае систему уравнений (1) можно записать в матричной форме: $\mathbf{GX} = \mathbf{B}$, где

$$\mathbf{G} = \begin{Vmatrix} 1 & -P'_{NO} & 0 & 0 & 0 & 0 & 0 \\ -P_0^{EI} & 1 & 0 & -mP_{EO} & 0 & 0 & 0 \\ -P_{EI} & 0 & 1 & -(1-P_{EO}-P_{ex}) & 0 & 0 & 0 \\ 0 & 0 & -P_0^{AI} & 1 & 0 & -nP_F & 0 \\ 0 & 0 & -P_{AI} & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -(1-P_{NE}) & 1 & -1 \\ 0 & 0 & 0 & 0 & -P_{NE} & 0 & 1 \end{Vmatrix},$$

$$\mathbf{X} = \begin{Vmatrix} \lambda_{NI} \\ \lambda_{NO} \\ \lambda_{EI} \\ \lambda_{EO} \\ \lambda_{AI} \\ \lambda_{AO} \\ \lambda_{QE} \end{Vmatrix}, \qquad \mathbf{B} = \begin{Vmatrix} \lambda_{NMS} \\ 0 \\ \lambda_{EMS} \\ 0 \\ 0 \\ 0 \\ \lambda_{NE} + \lambda_{HMI} \end{Vmatrix}.$$

Отсюда легко получить численное решение СЛАУ методом обратной матицы:

$$\mathbf{X} = \mathbf{G}^{-1}\mathbf{B}. \qquad (2)$$

4. Локальные характеристики процесса функционирования СУСС

Принцип декомпозиции открывает широкие возможности для анализа СеМО с применением многочисленных теоретических результатов в классе однолинейных СМО. В частности, при самых простых предположениях относительно процесса обслуживания поступающих заявок отдельным элементом СеМО может использоваться модель СМО типа $M/M/1/\infty$, как это сделано в работе [7]. Более сложная ситуация, когда поступающие в СУСС внешние запросы неоднородны по важности для задач управления сетью связи и требуется применять дисциплины приоритетного обслуживания, исследована в работах [11, 12].

Влияние отказов, возникающих в элементах СУСС, на степень ухудшения качества функционирования исследуемой системы можно оценить с помощью теоретических результатов, представленных в [13]. Здесь построена модель однолинейной СМО с бесконечным входным буфером при условии, что поступающие заявки образуют простейший поток с интенсивностью λ и имеют длительность обслуживания, которая распределена по экспоненциальному закону с параметром μ. Дополнительно вводится фактор ограниченной надежности

обслуживающего устройства, причем это может проявляться как в свободном состоянии, так и при занятом устройстве.

В рассматриваемом случае принимаются во внимание следующие показатели надежности: коэффициент готовности $k_{\text{г}}$ и средняя длительность простоя $\tau_{\text{п}}$. Среднее значение полного времени, в течение которого заявка пребывает в СМО (включая дообслуживание, возникающее после устранения отказа в обслуживающем устройстве), определяется из соотношения

$$w = T_{\text{д}} = \frac{1}{\mu_{\text{э}} - \lambda}\left(1 + \mu_{\text{э}} k_{\text{п}} \tau_{\text{п}}\right), \tag{3}$$

где $\mu_{\text{э}} = k_{\text{г}}\mu;\ k_{\text{п}} = 1 - k_{\text{г}}$. После применения формулы (2) становятся известными значения компонентов вектор-столбца $\boldsymbol{X}$, и тогда с помощью соотношения (3) можно вычислить указанную характеристику w_k для любой k-й очереди в составе рассматриваемой СеМО, т.е. при $k \in \{NI,\ NO,\ EI,\ EO,\ AI,\ AO,\ QE\}$.

5. Оценка комплексных показателей качества функционирования СУСС

Оперативность исследуемой СУСС проявляется как скорость ее реакции в процессе человеко-машинного взаимодействия и характеризуется средней длительностью интервала времени от момента ввода в систему внешнего запроса (или команды управления) до момента получения оператором ответного сообщения (или уведомления о выполнении команды). Оценка указанного показателя связана с вычислением среднего времени пребывания заявки в пределах рассматриваемой СеМО. При этом простое суммирование значений, найденных с помощью выражения (3), не является допустимым, поскольку разные заявки отличаются своими маршрутами движения по сети, причем нельзя утверждать, что любая заявка обязательно попадает в каждую очередь всего один раз.

Суммарная интенсивность (λ_{total}) общего потока заявок, входящих в систему, равна сумме интенсивностей внешних потоков для отдельных очередей:

$$\lambda_{total} = \lambda_{NMS} + m(\lambda_{EMS} + n\lambda_{EOM}), \tag{4}$$

где $\lambda_{EOM} = \lambda_{NE} + \lambda_{HMI}$ – средняя интенсивность внешних обращений к одному процессору ОМР.

Тогда согласно формуле Литтла среднее значение общего времени нахождения произвольной внешней заявки в пределах рассматриваемой СУСС рассчитывается как

$$W_{total} = \frac{L_{total}}{\lambda_{total}} = \frac{\sum\limits_{k} \lambda_k w_k}{\lambda_{NMS} + m(\lambda_{EMS} + n\lambda_{EOM})}. \tag{5}$$

Также представляет интерес оценка скорости реакции исследуемой системы TMN по отношению к отдельным потокам внешних заявок. Для примера рассмотрим заявки, приходящие во входную очередь *NI* подсистемы NMS, которая выполняет поддержку функций главного центра управления сетью связи (ГЦУСС). Обработка команд управления, поступающих от персонала ГЦУСС, последовательно осуществляется на разных уровнях анализируемой системы TMN с участием подсистем NMS и EMS, а также агента и средств технического обслуживания сетевого элемента (NE). С учетом возможных траекторий (маршрутов) перемещения заявок по отдельным фазам обслуживания можем получить среднее значение времени реакции:

$$W_{NMS} = w_{NI} + w_{NO} + (1 - P_0^{EI})\left[w_{EI} + w_{EO} + (1 - P_0^{AI})(w_{AI} + w_{AO} + P_{NE} w_{QE}) \right].$$

6. Результаты численных расчетов

Контрольные расчеты проведены для случая однородной структуры СУСС при $m = n = 5$. Параметры системы, которые в ходе расчетов оставались неизменными, принимали следующие значения [7]:

– интенсивности внешних заявок: $\lambda_{NE} = \lambda_{HMI} = 0.105$; $\lambda_{EMS} = 0.07$;

– вероятности распределения заявок:

$P_{NO} = 0.99$; $P_0^{EI} = P_0^{AI} = 0.1$; $P_{EI} = (1 - P_0^{EI}) / m = 0.18$; $P_{EO} = P_{NE} = 0.5$; $P_{ex} = 0.49$; $P_{AI} = (1 - P_0^{AI}) / n = 0.18$; $P_F = 0.9$;

– интенсивности обслуживания заявок:

$\mu_{NI} = \mu_{NO} = \mu_{EI} = \mu_{EO} = 2.85$; $\mu_{AI} = 4.1$; $\mu_{AO} = 2.15$; $\mu_{QE} = 7.3$.

Рассмотрим случай, когда коэффициент готовности на первом уровне системы управления, т.е. на уровне управления всей сетью (NMS), имеет значение $k_г = 0.996$ (линия Trace1a на рис. 3) и $k_г = 0.992$ (линия Trace1b на рис. 3), а значение коэффициента готовности на остальных уровнях (уровень EMS, уровень агентов, уровень АТМ-коммутаторов) будет равным 1.

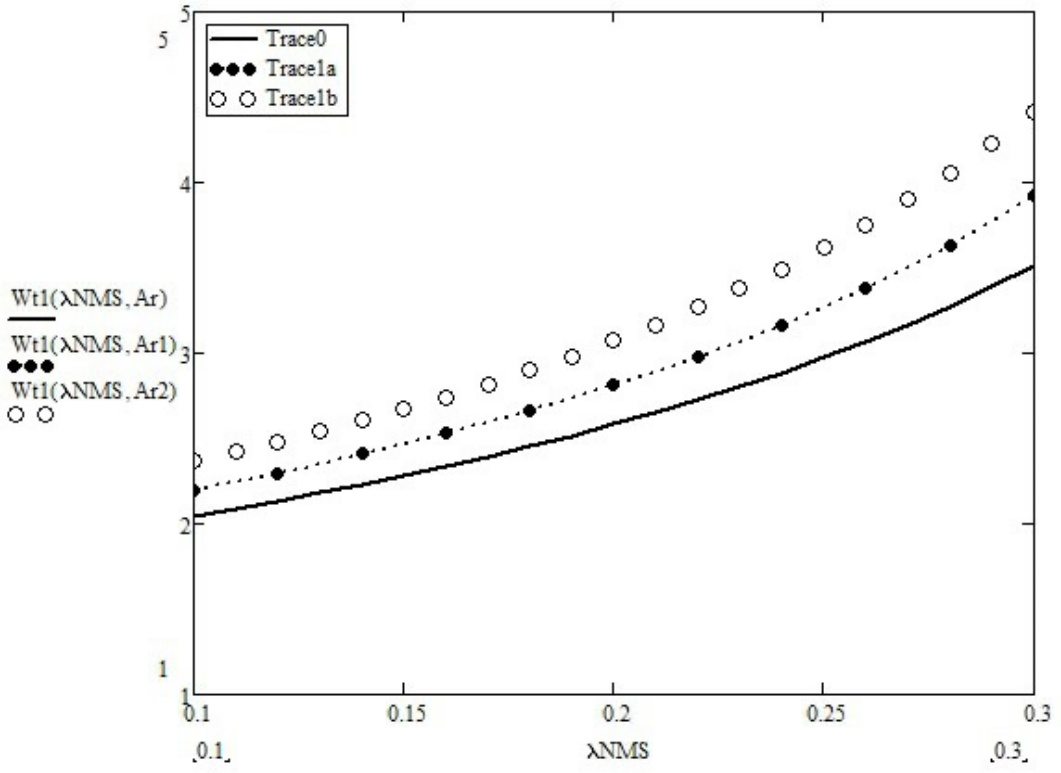


Рис. 3. Зависимость среднего времени реакции СУСС от интенсивности поступающих запросов

Анализ рис. 3 показал, что коэффициент готовности элементов системы, занимающихся обработкой поступающих запросов, значительно влияет на конечные задержки в системе. Так, линия Trace0 построена для идеально надежной системы, т.е. у всех её элементов $k_г = 1$. При уменьшении коэффициента готовности до 0.992 в системе наблюдается рост времени нахождения заявки в очереди. При этом с увеличением интенсивности запросов λ_{NMS} рост времени нахождения заявки в очереди изменяется нелинейно. Так, при $\lambda_{NMS} = 0.1$ время задержки увеличивается на 15 %, а при $\lambda_{NMS} = 0.3$ – на 25 %.

Если значение коэффициента готовности на других уровнях, т.е. на уровне EMS, уровне агента и уровне коммутатора, будет иметь значение меньше единицы, то по рис. 4 можно сделать вывод, что система почти близка к идеальной, а время реакции системы практически не отличается.

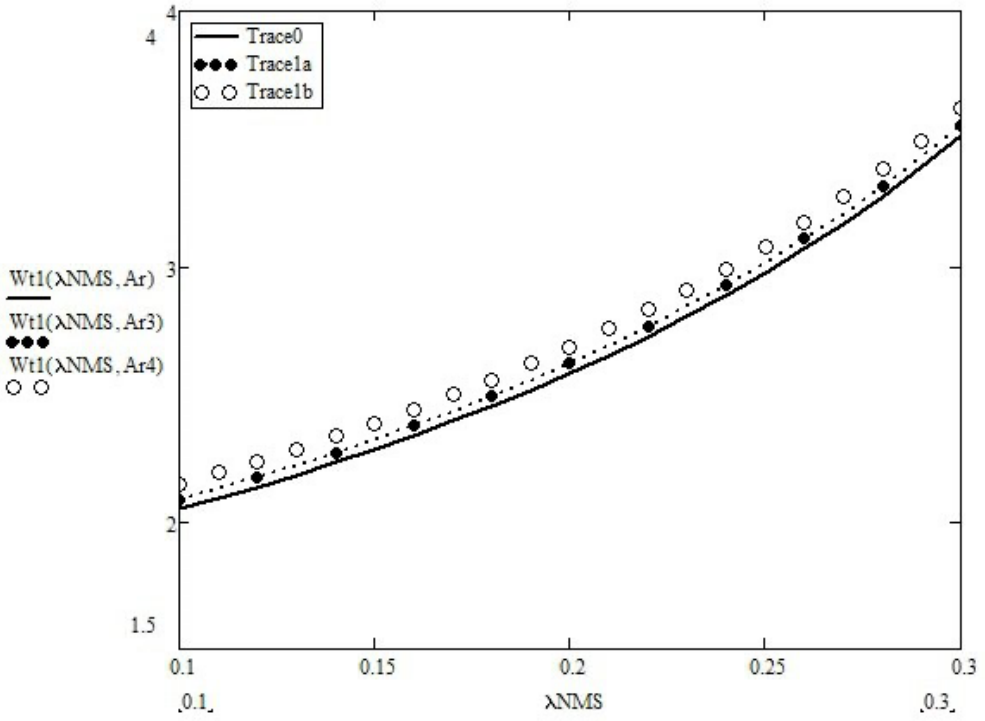


Рис. 4. Зависимость среднего времени реакции СУСС от интенсивности поступающих запросов

При дальнейших изменениях коэффициента готовности для различных элементов системы, за исключением NMS, получаются практически аналогичные результаты. Это связано с тем, что в условиях практически идеальной надежности главенствующей системы сложно пронаблюдать какие-либо тенденции при ухудшении надежности связующих и оконечных элементов.

На основании проведенных расчетов можно сделать вывод, что даже при незначительном понижении коэффициента готовности элементов системы NMS относительно идеальной надежности время задержки обслуживания поступающих заявок заметно растет.

7. Заключение

Основным результатом проведенного исследования является построение математической модели иерархической системы управления сетью связи. Модель использует аппарат сетей массового обслуживания, что обеспечивает наибольшее соответствие особенностям изучаемого объекта, при этом учитываются отказы, возникающие в элементах системы управления.

На основании проведенных расчетов показано влияние элементов СУСС на качество функционирования исследуемой системы.

Литература

1. *Гребешков А. Ю.* Стандарты и технологии управления сетями связи. М.: Эко-Трендз, 2003. 288 с.
2. *Дымарский Я. С., Крутякова Н. П., Яновский Г. Г.* Управление сетями связи: принципы, протоколы, прикладные задачи. М.: ИТЦ «Мобильные коммуникации», 2003. 384 с.
3. *Райли Д., Кринер М.* NGOSS: Построение эффективных систем поддержки и эксплуатации сетей для оператора связи. М.: Альпина Бизнес Букс, 2007. 192 с.
4. *Самуйлов К. Е., Чукарин А. В., Яркина Н. В.* Бизнес-процессы и информационные технологии в управлении телекоммуникационными компаниями. М.: Альпина Паблишерз, 2009. 442 с.
5. *Костин А. А.* Модель системы интегрированного управления телекоммуникационными сетями и услугами // Электросвязь. 2002. № 10. С. 22–26.
6. *Мочалов В. П.* Теоретические основы разработки и анализ вероятностно-временных характеристик распределенных систем управления телекоммуникационными сетями и услугами. М.: ФИЗМАТЛИТ, 2006. 365 с.
7. *Hwang Y. H., Chung S. W., Lee G.-H., Kim Y. I.* A Performance Analysis of TMN Systems Using Models of Networks of Queues, Jackson's Theorem, and Simulation // ETRI Journal. October 2002. V. 24, № 5. P. 381–390.
8. *Башарин Г. П., Бочаров П. П., Коган Я. А.* Анализ очередей в вычислительных сетях. Теория и методы расчета. М.: Наука. Гл. ред. физ.-мат. лит., 1989. 336 с.
9. *Kühn P.* Analysis of Complex Queuing Networks by Decomposition // Congress book, 8th International Teletraffic Congress, Melbourne. 1976. V. 1. P. 236/1–236/8.
10. *Kuehn P.* Approximate Analysis of General Queuing Networks by Decomposition // IEEE Trans. on Commun. 1979. V. 27, № 1, P. 113–126.
11. *Мейкшан В. И.* Анализ приоритетных дисциплин обслуживания в иерархической системе управления сетями связи // Вестник СибГУТИ. 2013. № 4. С. 21–34.
12. *Мейкшан В. И.* К вопросу анализа дисциплины приоритетного обслуживания при многоуровневом управлении сетями связи // Доклады Академии наук высшей школы РФ. 2016. № 1 (30). С. 73–83.
13. *Захаров Г. П.* Методы исследования сетей передачи данных. М.: Радио и связь, 1982. 208 с.

Мейкшан Владимир Иванович

д.т.н., профессор кафедры инфокоммуникационных систем и сетей, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 242, e-mail: meikshanvi@gmail.com, ORCID ID: 0000-0001-9834-5346.

Лизнева Юлия Сергеевна

к.т.н., доцент кафедры инфокоммуникационных систем и сетей, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 242, e-mail: ktm5r@rambler.ru, ORCID ID: 0000-0001-9746-7413.

Ростова Елена Владимировна

старший преподаватель кафедры инфокоммуникационных систем и сетей, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 242, e-mail: rostova@sibguti.ru, ORCID ID: 0009-0007-9293-7106.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Analysis of Hierarchical Communication Network Management System with Limited Reliability of System Elements

Vladimir I. Mejkshan, Yulia S. Lizneva, Elena V. Rostova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The mathematical apparatus of the queuing networks theory is used when analyzing the hierarchical control system of communication networks. The peculiarity and scientific novelty of the constructed model lies in the fact that the limited reliability of the system elements is taken into account. The presented results of numerical calculations demonstrate the influence of the availability coefficient of the control system elements on the indicators characterizing the time of the system's reaction upon requests related to the maintenance and operation of network facilities.

Keywords: communication networks, control system, request queues, priorities, average response time.

For citation: Mejkshan V. I., Lizneva Yu. S., Rostova E. V. Analysis of a hierarchical communication network management system with limited reliability of system elements (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 32-42. https://doi.org/10.55648/1998-6920-2024-18-2-32-42.

The article was submitted: 24.11.2023;
accepted for publication 24.12.2023.

References

1. Grebeshkov A. Yu. *Standarty i tekhnologii upravleniya setyami svyazi* [Communication network management standards and technologies]. Moscow, Eko-Trendz, 2003, 288 p.
2. Dymarskij YA. S., Krutyakova N. P., Yanovskij G. G. *Upravlenie setyami svyazi: principy, protokoly, prikladnye zadachi* [Communication network management: principles, protocols, applications]. Moscow, ITC «Mobil'nye kommunikacii», 2003, 384 p.
3. Rajli D., Kriner M. NGOSS: *Postroenie effektivnyh sistem podderzhki i ekspluatacii setej dlya operatora svyazi* [NGOSS: Building effective network support and operation systems for telecom operators]. Moscow, Al'pina Biznes Buks, 2007, 192 p.
4. Samujlov K. E., Chukarin A. V., Yarkina N. V. *Biznes-processy i informacionnye tekhnologii v upravlenii telekommunikacionnymi kompaniyami* [Business processes and information technologies in the management of telecommunications companies]. Moscow, Al'pina Publisherz, 2009, 442 p.
5. Kostin A.A. Model' sistemy integrirovannogo upravleniya telekommunikacionnymi setyami i uslugami [Model of an integrated management system for telecommunication networks and services]. *Elektrosvyaz'*, no. 10, 2002, pp. 22-26.
6. Mochalov V. P. *Teoreticheskie osnovy razrabotki i analiz veroyatnostno-vremennyh harakteristik raspredelennyh sistem upravleniya telekommunikacionnymi setyami i uslugami* [Theoretical foundations for the development and analysis of probabilistic-time characteristics of distributed control systems for telecommunication networks and services]. Moscow, FIZMATLIT, 2006, 365p.

7. Hwang Y. H., Chung S. W., Lee G.-H., Kim Y. I. A Performance Analysis of TMN Systems Using Models of Networks of Queues, Jackson's Theorem, and Simulation. *ETRI Journal*, vol. 24, no. 5, October 2002, pp.381-390.
8. Basharin G.P., Bocharov P.P., Kogan Ya.A. *Analiz ocheredej v vychislitel'nyh setyah. Teoriya i metody* rascheta [Analysis of queues in computer networks. Theory and calculation methods]. Moscow, Nauka, Gl. red. fiz.-mat. lit., 1989, 336 p.
9. Kühn P. Analysis of Complex Queuing Networks by Decomposition. Congress book, 8th International Teletraffic Congress, Melbourne, 1976, vol. 1, pp. 236/1–236/8.
10. Kuehn P. Approximate Analysis of General Queuing Networks by Decomposition. IEEE Trans. on Commun., 1979, vol. 27, no. 1, pp. 113–126.
11. Mejkshan V. I. *Analiz prioritetnyh disciplin obsluzhivaniya v ierarhicheskoj sisteme upravleniya setyami svyazi* [Analysis of priority service disciplines in a hierarchical communication network management system]. Vestnik SibGUTI, 2013, no. 4, pp. 21-34.
12. Mejkshan V. I. K voprosu analiza discipliny prioritetnogo obsluzhivaniya pri mnogourovnevom upravlenii setyami svyazi [On the issue of analyzing the priority service discipline in multi-level management of communication networks]. *Doklady Akademii nauk vysshej shkoly RF*, 2016, no.1 (30), pp. 73-83.
13. Zaharov G.P. *Metody issledovaniya setej peredachi dannyh* [Methods for studying data networks], Moscow, Radio i svyaz', 1982, 208 p.

Vladimir I. Mejkshan

Dr. of Sci. (Engineering), Professor; Professor of the Department of Infocommunication Systems and Networks, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 242, e-mail: meikshanvi@gmail.com, ORCID ID: 0000-0001-9834-5346.

Yulia S. Lizneva

PhD (Engineering), Associate Professor; Associate Professor of the Department of Infocommunication Systems and Networks, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 242, e-mail: ktm5r@rambler.ru, ORCID ID: 0000-0001-9746-7413.

Elena V. Rostova

Senior lecturer of the Department of Infocommunication Systems and Networks, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 242, e-mail: rostova@sibguti.ru, ORCID ID: 0009-0007-9293-7106.

DOI: 10.55648/1998-6920-2024-18-2-43-56 УДК 004.056.53

Подход к оценке защищенности речевой акустической информации с применением нейронных сетей

Н. А. Волков, А. В. Иванов

Самарский государственный технический университет (СамГТУ)

Аннотация: В работе рассматривается методика оценки защищенности речевой акустической информации при подготовке помещений для проведения закрытых переговоров. Авторами предложена структурная схема этапов создания интеллектуальной системы, в которой с учетом недостатков существующих подходов используются методы распознавания, основанные на сверточных нейронных сетях. Описывается процесс формирования обучающего набора данных в формате аудиозаписей с наложенными шумами с различными отношениями сигнал/шум. Рассматриваются возможности аудиоредактора Adobe Audition и библиотек Python для формирования наборов данных. Предлагается классифицировать спектрограммы либо мел-частотные кепстральные коэффициенты аудиозаписей с помощью нейронной сети по процентам разборчивости речи с целью автоматизации процесса оценки защищенности речевой акустической информации. Для достижения требуемого результата планируется обучить нейронную сеть на различных данных, провести сравнительный анализ с существующим подходом, оценить производительность системы и провести валидацию результатов. Предложенный подход и его практическое применение позволят значительно повысить качество и расширить условия применения оценки защищенности речевой акустической информации.

Ключевые слова: глубокие нейронные сети, сверточные нейронные сети, отношение сигнал/шум, зашумленность аудиозаписи, распознавание речи, спектрограммы, мел-частотные кепстральные коэффициенты, оценка защищенности речевой акустической информации.

Для цитирования: Волков Н. А., Иванов А. В. Подход к оценке защищенности речевой акустической информации с применением нейронных сетей // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 43–56. https://doi.org/10.55648/1998-6920-2024-18-2-43-56.

Статья поступила в редакцию 13.10.2023;
переработанный вариант – 20.12.2023;
принята к публикации 22.12.2023.

1. Введение

Одной из ключевых задач в области обеспечения информационной безопасности является защита акустической речевой информации при проведении переговоров. Закрытая информация может быть подслушана при помощи технических средств акустической и виброакустической разведки [1].

Для оценки уровня защищенности от утечки информации по техническим каналам в помещении, которое предназначено для проведения закрытых переговоров, чаще всего используется общепринятый инструментально-расчетный подход, предложенный А. А. Хоревым,

В. К. Желязняком и Ю. К. Макаровым [2] на основании результатов экспериментальных исследований, проведенных Н. Б. Покровским [3]. Важно отметить, что формантный метод Н. Б. Покровского был предложен для оценки качества телефонных линий связи, поэтому условия проведения экспериментов существенно отличаются от условий оценки защищенности речевой информации. В связи с этим данный подход обладает рядом недостатков при его использовании для оценки защищенности помещений от утечки по техническим каналам акустической речевой информации [4]. Перечислим основные из них:

1) в качестве принимающей стороны не рассматривался злоумышленник, обладающий возможностью записи сигнала, многократного прослушивания, обработки сигнала (шумоочистка);

2) экспериментальные исследования (артикуляционные испытания, на основании которых были выведены все зависимости, используемые в методике [3]) проводились с использованием таблиц (слоговых, словесных и т.д.), где элементы были максимально некоррелированы между собой. Однако в реальных ситуациях мы имеем дело со связными, осмысленными текстами, что позволяет злоумышленнику понять те слова, которые не были им распознаны по общему содержанию переговоров;

3) не рассматривались условия с высоким уровнем маскирующих шумов, что оказывает влияние на зависимости восприятия речевых сигналов;

4) не учитываются индивидуальные особенности речи говорящих, всё основывается на усредненном спектре речи;

5) все зависимости амплитудного состава речи Н. Б. Покровским были получены при условии, что источник звука находился в 8 см от микрофона, в задачах же защиты информации все измерения и запись сигнала производятся на расстояниях более 1 м. Из этого следует, что использовать интегральные уровни по методу Н. Б. Покровского в наших задачах нельзя. Кроме того, спектры сигналов, измеренные на расстояниях 8 см и 1 м от микрофона, могут отличаться;

6) не рассматривался эффект форсирования речи (повышение уровня речи, вызванное усиленным напряжением голосовых связок) [5];

7) маскировка речи учитывается только с помощью помех на основе белого шума, исключая возможность оценки защищенности от помех типа «речевой хор» (такая помеха формируется путем смешения фрагментов речи нескольких дикторов) [6];

8) не учитывается влияние конфигурации помещения на оценку разборчивости речи (форма помещения, размер помещения, реверберация, поглощение звука) [7, 8].

Указанные недостатки подчеркивают необходимость корректировки существующих подходов к оценке защищенности речевой акустической информации. Корректировки должны позволить учесть реальные условия защиты информации, связность и осмысленность речи дикторов, разнообразие помех и индивидуальные особенности дикторов.

Реализация скорректированного подхода становится возможной при переходе от формантного метода к оценке защищенности речевой акустической информации с помощью интеллектуальной системы на основе нейронной сети. В случае реализации подобного подхода станет возможным учесть ряд существующих недостатков.

2. Нейросетевой подход к оценке защищенности речевой акустической информации

При оценке защищенности помещения от утечки информации по техническим каналам оператором проводится инструментально-расчетная оценка разборчивости речи в контрольных точках помещения. При проведении оценки используется комплект контрольно-измерительной аппаратуры, состоящий из генератора тестовых сигналов (в качестве которого чаще всего используется генератор белого шума), усилителя мощности, акустического излучателя, измерительного датчика (микрофон и акселерометр) и измерительного устройства

– шумомера со встроенными фильтрами (октавными). Также в контрольной точке устанавливают средство защиты информации для создания маскирующих помех. Состав измерительной установки приведен на рис. 1.

Рис. 1. Состав измерительной установки при оценке защищенности акустической речевой информации в помещении

Оценка защищенности производится в следующей последовательности:

1) измеряется уровень тестового сигнала, излучаемого акустической системой;

2) измеряется уровень фоновых шумов или шумов от средств защиты информации (СЗИ) в контрольной точке;

3) измеряется уровень смеси сигнал+шум в контрольной точке;

4) рассчитывается значение словесной разборчивости;

5) делается вывод о соответствии полученного значения норме.

На рис. 2 представлена предлагаемая интеллектуальная система оценки защищенности речевой акустической информации, в составе которой: источник речевого тестового сигнала, усилитель мощности, акустический излучатель, измерительный датчик (микрофон или акселерометр) и модуль оценки защищенности речевой акустической информации на основе нейронной сети. Также в контрольной точке установлено средство защиты информации.

Рис. 2. Схема предлагаемой интеллектуальной системы оценки защищенности речевой акустической информации

Алгоритм работы оператора с предлагаемой интеллектуальной системой оценки защищенности речевой акустической информации почти не отличается от общепринятой инструментально-расчетной оценки разборчивости речи в контрольных точках помещения – трудоемкость оператора не увеличивается, но вместо генератора тестовых сигналов мы используем источник речевого тестового сигнала; роль измерительного устройства теперь выполняет модуль оценки защищенности речевой акустической информации на основе нейронной сети.

Опишем более подробно этапы разработки интеллектуальной системы оценки защищенности речевой акустической информации на основе нейронной сети. Данные этапы представлены на рис. 3.

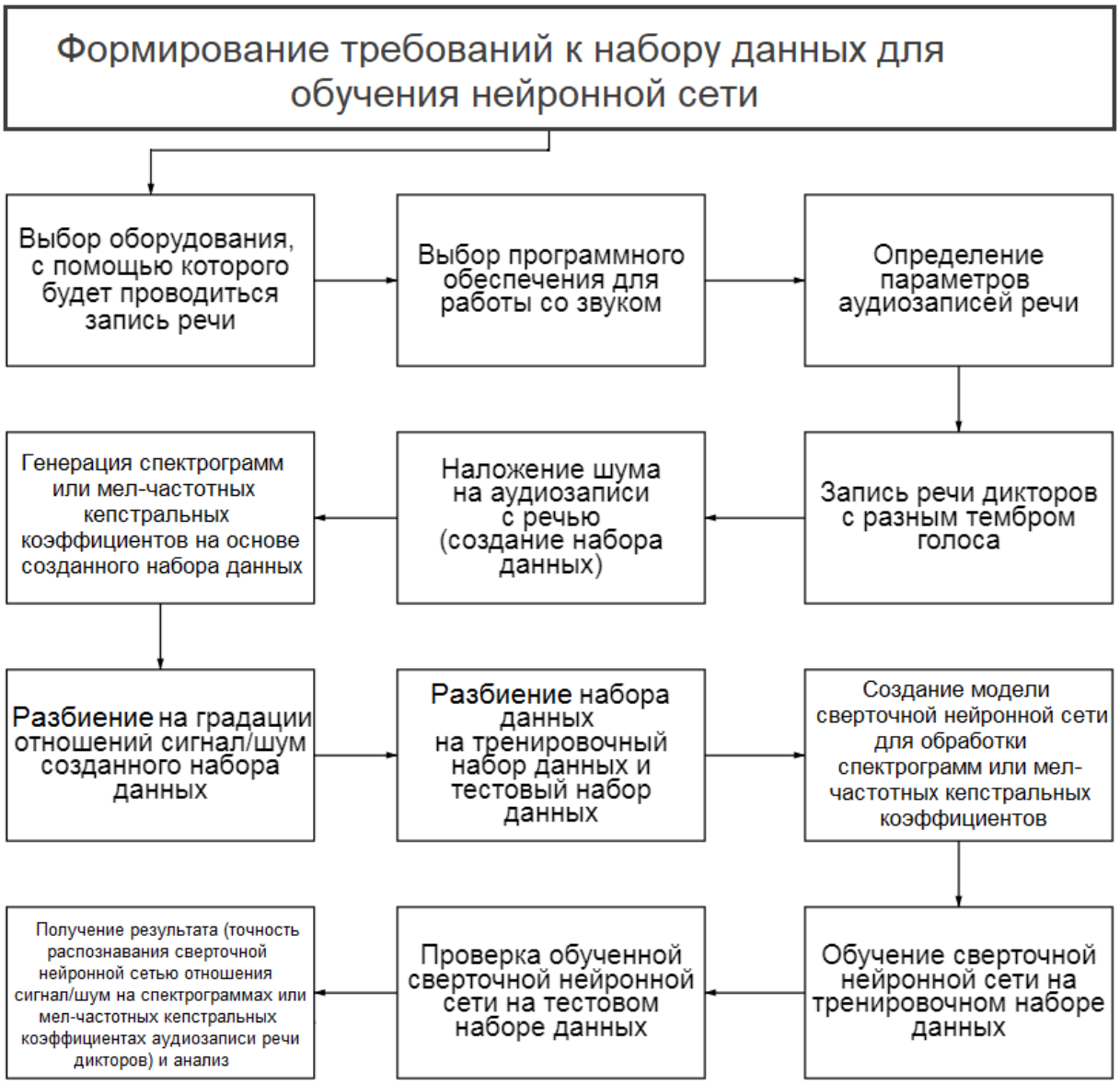


Рис. 3. Структурная схема этапов создания интеллектуальной системы оценки защищенности речевой акустической информации на основе нейронной сети

Рассмотрим более подробно приведенные этапы.

Для начала необходимо сформулировать требования к набору данных для обучения нейронной сети, а именно:

– какой вид данных будет использоваться для обучения нейронной сети – аудиозаписи или изображения;

– какое общее количество образцов будет использоваться в наборе данных;

– по каким классификациям необходимо разделить набор данных, а также необходимо определить количество таких классификаций;

– сколько образцов будет содержаться в тренировочном и тестовом наборах данных.

Для проведения записи голосов дикторов необходимо использовать программное обеспечение, которое имеет функционал обработки звука. Adobe Audition является широко признанным аудиоредактором, который пользуется популярностью среди исследователей в области защиты речевой информации [9, 10, 11]. Это программное обеспечение поддерживает все современные аудиоформаты и предлагает разнообразные функции. Встроенный спектральный анализатор позволяет анализировать спектр звука, а графический эквалайзер с тридцатью полосами предоставляет гибкую возможность регулировки звука. Программа позволяет корректировать фазу, тон и скорость воспроизведения, а также может генериро-

вать различные типы шумов (белый, розовый, коричневый). Дополнительно Adobe Audition обладает функциями исправления и удаления дефектов, таких как щелчки и шумоподавление, а также предоставляет множество других возможностей [12].

Для записи речи без искажения частотных характеристик и контроля уровня сигналов необходимо использовать измерительные микрофоны и шумомер с функцией записи сигнала либо с модулями аналого-цифрового преобразования для акустики (например, LTR 24-2).

Отметим также, что необходимо определить, для какого количества дикторов и с каким тембром голоса нужно провести запись речи (мужского низкого голоса, мужского высокого голоса, женского низкого голоса, женского высокого голоса).

Прежде чем проводить запись речи дикторов, необходимо определить параметры получаемых аудиодорожек, а именно:

– Частота дискретизации аудиозаписи. Обычно используется частота дискретизации, равная 44.1 кГц или 48 кГц.

– Длительность аудиозаписи. Определяется экспериментальным путем, начиная с длительности в 10 секунд, оценивая влияния длительности на результат обучения нейронной сети. Кроме того, необходимо определить, будет ли аудиозапись речи диктора иметь паузы или необходимо отредактировать аудиозапись и вырезать все паузы.

– Формат, в котором необходимо сохранять файлы. Предлагается использовать формат wav, так как он обеспечивает сохранение звука без потерь [19].

После проведения записи голосов дикторов мы получим несколько аудиозаписей – набор данных чистой речи.

Набор данных для обучения должен представлять из себя аудиозаписи с наложенными шумами различных спектров (для первоначального эксперимента предлагается взять белый и розовый шумы), имитирующими случай с оценкой защищенности речевой информации при использовании СЗИ. Для генерации шумов и наложения на первоначальном этапе предлагается воспользоваться программным обеспечением Adobe Audition. Но в дальнейшем для набора достаточного количества данных для обучения, поскольку процесс наложения шумов на аудиозаписи речи дикторов является довольно трудоемким, необходимо разработать программное обеспечение, которое при задании отношения сигнал/шум и выборе вида шума будет автоматически его накладывать на аудиозаписи речи дикторов. Предлагается использовать язык программирования Python для разработки такого программного обеспечения. Для обработки аудиофайлов в разрабатываемом программном обеспечении необходимо использовать соответствующие библиотеки, применяемые в данной области. Одной из важных библиотек для обработки звука является PyAudio [13]. Основная функциональность PyAudio заключается в записи аудиопотока в объекты типа “bytes”. В дальнейшем эти данные могут быть сохранены в формате wav с использованием библиотек, таких как SciPy или Wave.

Также существует библиотека Librosa [14], которая предназначена для сбора и воспроизведения аудио. Librosa является модулем на языке Python, который специализируется на анализе звуковых сигналов, обработке звука и голоса. Она предоставляет функции для воспроизведения аудиофайлов непосредственно в среде разработки Python, а также возможность визуализации аудиодорожки. В рамках данной библиотеки также имеются функции для построения спектрограммы – графического представления спектральных характеристик звукового сигнала.

В работе [15] рассматривается библиотека pyAudioAnalysis, которая предоставляет широкий спектр функциональных возможностей анализа звука с помощью простого в использовании комплексного программного дизайна. Данная библиотека может быть использована для извлечения аудиофайлов, обучения и применения аудиоклассификаторов, сегментации аудиопотока с использованием контролируемых или неконтролируемых методологий и визуализации аудиодорожки.

В исследовании [16] авторами представляется модуль PYO, предназначенный для цифровой обработки звука. Эта библиотека позволяет быстро интегрировать аудиопроцессы в

другие задачи программирования, такие как математические вычисления, сетевые коммуникации или программирование графических интерфейсов.

Следующим этапом разработки интеллектуальной системы является генерация спектрограмм или мел-частотных кепстральных коэффициентов на основе зашумленных аудиозаписей речи диктора. В настоящее время существуют различные подходы к анализу речевых сигналов как во временной, так и в частотной областях. В частности, широко применяются методы, основанные на создании спектрограмм и вычислении мел-частотных кепстральных коэффициентов. Спектрограмма представляет собой графическое отображение изменения спектральной плотности мощности сигнала в зависимости от времени. Для создания спектрограммы используется оконное преобразование Фурье, которое позволяет разбить сигнал на интервалы с определенными диапазонами частот и времени, характеризуемыми амплитудой сигнала на каждом интервале. Визуализация амплитуды на спектрограмме обычно осуществляется путем использования яркости или цвета (чаще всего более яркие области соответствуют большей амплитуде). Все последовательности разбиваются на одинаковые по частотному диапазону сегменты, а затем эти сегменты разделяются на временные отрезки, поскольку длительность сигналов может быть различной. Для обработки полученных фрагментов данных применяется быстрое преобразование Фурье [17]. На рис. 4 показана спектрограмма аудиозаписи речи диктора длиной 10 секунд без наложения шума.

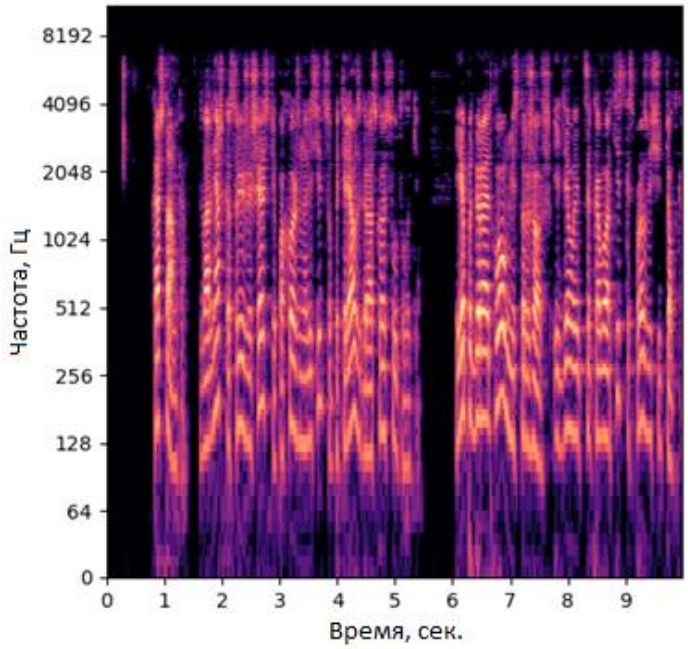


Рис. 4. Спектрограмма аудиозаписи речи диктора длиной 10 секунд без наложения шума

Мел-частотные кепстральные коэффициенты (MFCC) являются набором относительно небольших значений, которые описывают частотные характеристики сигнала. Этот метод основывается на равномерном распределении частотных полос по логарифмической шкале, соответствующей способности человека воспринимать звуки [18]. В результате преобразования получается величина, называемая мелом. Для вычисления MFCC используется оконное преобразование Фурье, а при обработке записи голоса, представленной одним словом, преобразование может производиться над всем образцом сигнала. Полученные спектральные значения проходят через треугольные оконные фильтры, после чего к полученным значениям в каждом окне применяется дискретное косинусное преобразование. Амплитуды результирующего спектра являются итоговыми мел-частотными кепстральными коэффициентами [19]. На рис. 5 показан пример мел-частотных кепстральных коэффициентов, полученных из аудиозаписи длиной 10 секунд без наложения шума.

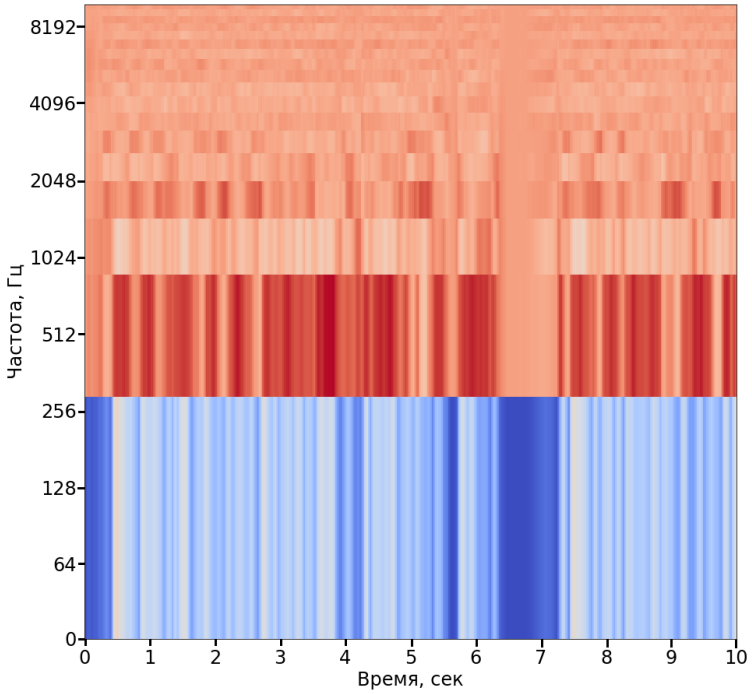


Рис. 5. Мел-частотные кепстральные коэффициенты аудиозаписи речи диктора длиной 10 секунд без наложения шума

Для того чтобы правильно сгенерировать спектрограмму или мел-частотные кепстральные коэффициенты, необходимо определить следующие параметры для зашумленной аудиозаписи речи:

– частота дискретизации;

– вид окна Фурье – обычно используются окна Хэмминга, Ханна или прямоугольные окна для создания спектрограммы или мел-частотных кепстральных коэффициентов;

– разрешение изображения – необходимо выбрать размер выходной спектрограммы или мел-частотных кепстральных коэффициентов в пикселях, учитывая баланс между размером данных и детализацией;

– количество признаков, которые необходимо выделить из аудиозаписи (при генерации мел-частотных кепстральных коэффициентов);

– временной отрезок, который необходимо обработать, – можно выбрать полную длительность аудиозаписи или определенный временной отрезок для обработки;

– отображаемые параметры по осям графика;

– вид представления изображения (линейный, логарифмический);

– возможно, для расширения набора данных провести «отзеркаливание» по горизонтали спектрограмм или мел-частотных кепстральных коэффициентов.

В языке программирования Python доступны библиотеки NumPy и Matplotlib, позволяющие работать с вышеперечисленными параметрами. NumPy представляет собой библиотеку, которая добавляет поддержку многомерных массивов и матриц, а также обширную коллекцию высокоуровневых (и очень быстрых) математических функций для работы с этими массивами [20]. Matplotlib, в свою очередь, является библиотекой, используемой для создания графиков и упрощения процесса их построения. Она часто используется совместно с библиотекой NumPy [21].

Для реализации инструмента определения соответствия значения разборчивости речи доле примеси шумового сигнала в речевом сигнале (а это основная задача в оценке защищенности) предлагается применить нейронную сеть, которая работает с изображениями.

В современном мире всё больше исследователей в области обработки звука используют машинное обучение в своих научных целях [22, 23, 24]. Особенно широкое распространение в данной области получил такой класс машинного обучения, как глубокое обучение. Всё ча-

ще исследователи используют архитектуры нейронных сетей, такие как генеративные состязательные сети (GAN), трансформеры и сверточные нейронные сети (CNN) [24, 25, 26]. Генеративные состязательные сети широко применяются в задачах, где необходимо сгенерировать новые данные, например, изображения, звуки, тексты. Они широко используются в области искусственного интеллекта для создания высококачественных и реалистичных данных [27]. В нашей задаче мы уже имеем данные и генерировать новые нет необходимости. Такой вид нейронных сетей, как трансформеры, используется для обработки последовательных данных – естественный язык, машинный перевод, задачи обработки текста [28]. В последние годы были разработаны модификации трансформеров, такие как Vision Transformer (ViT), которые успешно применяются в задачах обработки изображений [29]. Однако предобученный трансформер имеет фиксированное разрешение входного изображения, что может стать ограничением для ряда сценариев. Трансформеры изначально разрабатывались для работы с последовательными данными и не всегда эффективны при обработке пространственных зависимостей в изображениях. Это может привести к трудностям в анализе локальных структур и объектов на изображениях. Также стоит отметить, что при обработке больших изображений трансформерам может потребоваться разделение изображения на более мелкие фрагменты, что увеличивает вычислительную сложность и требует дополнительной обработки [30, 31]. Согласно последним исследованиям высокую эффективность в различных задачах распознавания имеют сверточные нейронные сети [32, 33]. Сверточные нейронные сети показали свою эффективность при использовании в задачах компьютерного зрения или распознавания изображений. Они эффективно улавливают локальные пространственные зависимости в данных, что является ключевым требованием в задачах компьютерного зрения. Сверточные нейронные сети, особенно при использовании предварительного обучения на больших наборах данных, могут быть вычислительно более эффективными и требовать меньше ресурсов – это важно при работе с большими объемами данных [26, 34, 35]. Кроме того, такие нейронные сети могут использоваться для распознавания речи, если в наборе данных использовать изображения спектрограмм или мел-частотных кепстральных коэффициентов, сгенерированных на основе зашумленных аудиозаписей. Сверточная нейронная сеть состоит из разных видов слоев: сверточные слои, субдискретизирующие слои (подвыборка) и выходной слой [36]. Пример архитектуры сверточной нейронной сети представлен на рис. 6, где обрабатывается спектрограмма аудиозаписи речи диктора с наложением белого шума с результатом распознавания нейронной сетью на выходе.

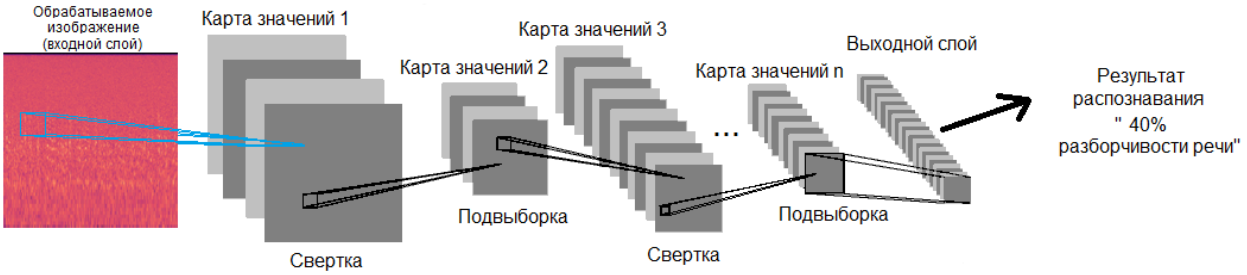


Рис. 6. Архитектура сверточной нейронной сети

Отметим, что при создании модели сверточной нейронной сети необходимо выделить её параметры и параметры обучения, а именно:

– количество слоев сверточной нейронной сети, включая сверточные слои, слои объединения и полносвязные слои;

– сколько необходимо полных прохождений обучения на наборе данных (эпох), которые позволят модели достичь сходимости. Можно использовать методы ранней остановки для предотвращения переобучения;

– вид, в котором будет представлена информация об успешном обучении, – какие метрики и графики будут использоваться для оценки успешности обучения модели, например, точность, потери, кривые обучения и валидации;

– вид, в котором подается на вход модели сверточной нейронной сети на распознавание тестовая информация – по одному изображению или пакетами.

Также необходимо разделить набор данных, представленный в виде спектрограмм или мел-частотных кепстральных коэффициентов, на тренировочный и тестовый. Такое разделение позволяет тестировать работу нейронной сети на ранее не использовавшихся данных и, соответственно, оценивать её точность распознавания. Чтобы не охватывать весь диапазон от 100 процентов разборчивости речи (аудиозапись речи без наложения шума) до 0 процентов (в аудиозаписи речи невозможно распознать ни одного слова), для начальной проверки работоспособности нейронной сети можно выделить несколько градаций процента разборчивости речи: например, от 20 до 30 процентов (каждой градации будет соответствовать 1 процент разборчивости речи). В соответствии с подходами для проведения артикуляционных испытаний [37] необходимо дать на прослушивание аудиторам зашумленную аудиозапись речи диктора – для нашего испытания ограничимся двумя мужчинами и двумя женщинами. Прослушивая зашумленную аудиозапись, аудитор оценивает, сколько слов он смог распознать. Зная заведомо количество слов в прослушиваемой аудиозаписи речи и сравнивая его с результатом распознавания аудитором количества слов, можно рассчитать процент разборчивости речи. Если взять четыре результата распознавания слов аудиторами, то получим среднее значение процента разборчивости речи. Полагаясь на это значение, необходимо провести градацию зашумленных аудиозаписей в наборе данных. В таком случае результатом работы предложенной реализации нейронной сети будет процент разборчивости речи, определенный в указанном диапазоне. Количество заданных градаций будет соответствовать итоговому количеству классов распознавания нейронной сети.

В дальнейшем для проверки предложенного подхода предлагается сравнить результат инструментально-расчетного подхода оценки разборчивости речи, разработанного А. А. Хоревым, В. К. Желязняком и Ю. К.Макаровым, с результатами работы интеллектуальной системы оценки защищенности речевой акустической информации на основе нейронной сети.

3. Заключение

В результате работы предложен подход к оценке защищенности речевой акустической информации с применением нейронных сетей. Для дальнейшей реализации данного подхода было сделано следующее:

1) предложена структурная схема этапов создания интеллектуальной системы оценки защищенности речевой акустической информации на основе нейронной сети;

2) сформулированы рекомендации по формированию наборов данных для обучения сверточной нейронной сети;

3) произведен выбор оборудования для записи речи диктора, программного обеспечения для работы с аудиофайлами и среды разработки программного обеспечения для реализации интеллектуальной системы оценки защищенности речевой акустической информации на основе нейронной сети;

4) предложены варианты представления данных для обучения сверточной нейронной сети.

Однако для получения оптимальных результатов необходимо обеспечить обучение и тестирование интеллектуальной системы на разнообразных данных (произвольные спектры помех и речи), чтобы она могла обрабатывать различные условия и шумовые сценарии. Также необходим сравнительный анализ результатов, полученных с помощью разработанной системы, и результатов, полученных с использованием традиционного инструментально-расчетного подхода. Результаты данного исследования могут быть использованы для совершенствования процесса оценки защищенности речевой акустической информации.

Литература

1. *Сагдеев К. М., Петренко В. И.* Методика оценки технической защищенности речевой информации в выделенных помещениях // Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 121–129.
2. *Железняк В. К., Макаров Ю. К., Хорев А. А.* Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4. С. 39–45.
3. *Покровский Н. Б.* Расчет и измерение разборчивости речи. М.: Связьиздат, 1962. 392 с.
4. *Трушин В. А., Рева И. Л., Иванов А. В.* Экспериментальная оценка разборчивости речи в задачах защиты информации на основе модифицированных артикуляционных измерений // Материалы X-й Междунар. конф. «Актуальные проблемы электронного приборостроения», НГТУ, Новосибирск, 2010. Т. 3. С. 133–136.
5. *Иванов А. В., Рева И. Л., Трушин В. А., Тудэвдагва У.* Корректировка методики оценки защищенности речевой информации от утечки по техническим каналам в условиях форсирования речи // Научный вестник Новосибирского государственного технического университета. 2014. № 2 (55). С. 183–189.
6. *Макаров Ю. К., Хорев А. А.* К оценке эффективности защиты акустической (речевой) информации // Специальная техника. 2000. № 5. С. 46–56.
7. *Иванов А. В., Салимов Ш. Р.* О возможности применения технологий распознавания речи в задачах оценки защищенности акустической информации от утечки по техническим каналам // Динамика систем, механизмов и машин. 2020. Т. 8, № 2. С. 109–114.
8. *Жабыко Е. И., Рублевская Н. И.* Акустическое проектирование залов многоцелевого назначения: учебное пособие. Владивосток: Издательство ДВГТУ, 2008. 89 с.
9. *Хорев А. А., Поров И. С.* Методика вероятностной оценки разборчивости // Защита информации. Инсайд. 2020. № 2 (92). С. 44–52.
10. *Трушин В. А., Заводовская А. И., Овешников И. А., Топорищев Э. В.* Исследование воздействия речеподобной помехи на психоэмоциональное состояние человека // Динамика систем, механизмов и машин. 2020. Т. 8, № 2. С. 138–144.
11. *Иванов А. В., Рева И. Л., Шемшетдинова Э. Э.* Исследование влияния различий в спектрах речи на результат оценки разборчивости // Динамика систем, механизмов и машин. 2017. Т. 5, № 4. С. 65–70.
12. Adobe Audition. Профессиональная студия звукозаписи [Электронный ресурс]. URL: `https://www.adobe.com/ru/products/audition.html` (дата обращения: 10.09.2023).
13. PyAudio 0.2.13 – Python Package Index [Электронный ресурс]. URL: `https://pypi.org/project/PyAudio/` (дата обращения: 10.09.2023).
14. Librosa 0.10 – Librosa - audio and music processing in Python [Электронный ресурс]. URL: `https://librosa.org/doc/latest/index.html` (дата обращения: 10.09.2023).
15. *Giannakopoulos T.* PyAudioAnalysis: An open-source python library for audio signal analysis // PLoS ONE. 2015. № 10 (12). P. 1–17.
16. *Bélanger O.* Pyo, the python DSP toolbox // Proc. ACM Multimedia Conference, 2016. P. 1214–1217.
17. *Умняшкин С. В.* Основы теории цифровой обработки сигналов: учебное пособие. М.: Техносфера, 2016. 528 с.
18. *Tyagi V., Wellekens C.* On desensitizing the Mel-cepstrum to spurious spectral components for robust speech recognition // Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. P. 1–21.
19. *Герасимов С. М., Жаринов О. О.* Исследование методов анализа речевых сигналов // Сборник докладов 73-й Международной студенческой научной конференции ГУАП, 2020. Ч. 3. С. 36–41.

20. NumPy documentation [Электронный ресурс]. URL: https://numpy.org/doc/stable/ (дата обращения: 10.09.2023).
21. Matplotlib 3.7.2 documentation [Электронный ресурс]. URL: https://matplotlib.org/stable/tutorials/index.html (дата обращения: 10.09.2023).
22. *Li J., Deng L., Haeb-Umbach R., Gong Y.* Robust automatic speech recognition. A bridge to practical applications, 2016. 286 p.
23. *Fang Z., Yin B., Du Z. et al.* Fast environmental sound classification based on resource adaptive convolutional neural network // Scientific Reports. 2022. № 12. P. 1–18.
24. *Madhu A., Kumaraswamy S.* EnvGAN: a GAN-based augmentation to improve environmental sound classification // Artificial Intelligence Review. 2022. № 55. P. 6301–6320.
25. *Kim B., Kim J., Ye J. C.* Task-Agnostic Vision Transformer for Distributed Learning of Image Processing // Transactions on Image Processing. 2023. № 32. P. 203–218.
26. *Ullah R., Asif M., Shah W. A., Anjam F., Ullah I., Khurshaid T., Wuttisittikulkij L., Shah S., Ali S. M., Alibakhshikenari M.* Speech Emotion Recognition Using Convolution Neural Networks and Multi-Head Convolutional Transformer // Sensors. 2023. № 13. P. 1–20.
27. *Porkodi S. P., Sarada V., Maik V. et al.* Generic image application using GANs (Generative Adversarial Networks): A Review // Evolving Systems. 2023. № 14. P. 903–917.
28. *Song Q., Sun B., Li S.* Multimodal Sparse Transformer Network for Audio-Visual Speech Recognition // IEEE Transactions on Neural Networks and Learning Systems. 2023. V. 34, № 12. P. 10028–10038.
29. Vision Transformer: What It Is & How It Works (2023 Guide) [Электронный ресурс]. URL: https://www.v7labs.com/blog/vision-transformer-guide/ (дата обращения: 13.12.2023).
30. *Tay Y., Dehghani M., Gupta J., Bahri D., Aribandi V., Qin Z., Metzler D.* Are Pre-trained Convolutions Better than Pre-trained Transformers? 2022. arXiv: 2105.03322 [cs.CL].
31. *Sanford C., Hsu D., Telgarsky M.* Representational Strengths and Limitations of Transformers. 2023. arXiv:2306.02896 [cs.LG].
32. *Abdel-Hamid O., Mohamed A.-R., Jiang H., Penn G.* Applying convolutional neural networks concepts to hybrid NN-HMM model for speech recognition // Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), 2012. P. 4277–4280.
33. *Сикорский О. С.* Обзор свёрточных нейронных сетей для задачи классификации изображений // Новые информационные технологии в автоматизированных системах. 2017. № 20. С. 1–8.
34. *Ciretan D. C., Giusti A., Gambardella L. M., Schmidhuber J.* Deep neural networks segment neuronal membranes in electron microscopy images // Proc. NIPS. 2012. P. 1–9.
35. *Ciretan D. C., Meier U., Gambardella L. M., Schmidhuber J.* Deep, Big, Simple Neural Nets for Handwritten Digit Recognition // MIT Press. 2010. V. 22, № 12. P. 3207–3220.
36. Что такое свёрточная нейронная сеть – Хабр [Электронный ресурс]. URL: https://habr.com/ru/articles/309508/ (дата обращения: 10.09.2023).
37. *Трушин В. А.* Информационно-измерительная модель формантного метода определения разборчивости речи // Труды Научно-исследовательского института радио. 2017. № 4. С. 2–9.

Волков Никита Андреевич
аспирант кафедры «Электронные системы и информационная безопасность», Самарский государственный технический университет (СамГТУ, 443011, Самара, ул. Молодогвардейская, д. 244), e-mail: volkovnikandr@gmail.com, ORCID ID: 0000-0002-0644-6332.

Иванов Андрей Валерьевич
к.т.н., доцент кафедры «Электронные системы и информационная безопасность», Самарский государственный технический университет (СамГТУ, 443011, Самара, ул. Молодогвардейская, д. 244), тел. +7 846 337-31-96, e-mail: andrej.ivanov@corp.nstu.ru, ORCID ID: 0000-0003-2002-8572.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

An Approach to Assessing the Security of Speech Acoustic Information Using Neural Networks

Nikita A. Volkov, Andrey V. Ivanov

Samara State Technical University (SamSTU)

Abstract: The paper is devoted to the consideration of the methodology for assessing the security of speech acoustic information in the preparation of premises for private negotiations. Taking into account the disadvantages of existing approaches it is proposed to apply recognition methods based on convolutional neural networks. The paper proposes a block diagram of the stages for creating an intelligent system. The process of creating a training dataset in audio recording format with superimposed noises with different signal-to-noise ratios is described. The possibilities of the Adobe Audition audio editor and Python libraries for generating datasets are considered. It is proposed to classify spectrograms or mel-frequency cepstral coefficients of audio recordings using a neural network by the percentage of speech intelligibility in order to automate the process of assessing the security of speech acoustic information. To achieve the desired result, it is planned to train a neural network on various data, conduct a comparative analysis with the existing approach, evaluate the performance of the system and validate the results. The proposed approach and its practical application will significantly improve the quality and expand the conditions for the application of the security assessment of speech acoustic information.

Keywords: deep neural networks, convolutional neural networks, signal-to-noise ratio, audio recording noise, speech recognition, spectrograms, mel-frequency cepstral coefficients, assessment of the security of speech acoustic information.

For citation: Volkov N. A., Ivanov A. V. An approach to assessing the security of speech acoustic information using neural net-works (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 43-56. https://doi.org/10.55648/1998-6920-2024-18-2-43-56.

The article was submitted: 13.10.2023;
revised version: 20.12.2023;
accepted for publication 22.12.2023.

References

1. Sagdeev K. M., Petrenko V. I. Metodika otsenki tekhnicheskoi zashchishchennosti rechevoi informatsii v vydelennykh pomeshcheniyakh [Methodology for assessing the technical security of speech information in dedicated rooms]. *Izvestiya YuFU. Tekhnicheskie nauki*, 2012, no. 12 (137), pp. 121-129.
2. Zheleznyak V. K., Makarov Yu.K., Khorev A. A. Nekotorye metodicheskie podkhody k otsenke effektivnosti zashchity rechevoi informatsii [Some methodological approaches to evaluating the effectiveness of speech information protection]. *Spetsial'naya tekhnika*, 2000, no. 4, pp. 39-45.
3. Pokrovskii N. B. *Raschet i izmerenie razborchivosti rechi* [Calculation and measurement of speech intelligibility]. Moscow, Svyaz'izdat, 1962. 392 p.
4. Trushin V. A., Reva I. L., Ivanov A. V. Eksperimental'naya otsenka razborchivosti rechi v zadachakh zashchity informatsii na osnove modifitsirovannykh artikulyatsionnykh izmerenii [Experimental assessment of speech intelligibility in information security tasks based on modified articulation measurements]. *Aktual'nye problemy elektronnogo priborostroeniya: materialy X Mezhdunar. konf. (APEP 2010)*, Novosibirsk: NGTU, 2010, vol. 3, pp. 133–136.
5. Ivanov A. V., Reva I. L., Trushin V. A., Tudevdagva U. Korrektirovka metodiki otsenki zashchishchennosti rechevoi informatsii ot utechki po tekhnicheskim kanalam v usloviyakh forsirovaniya rechi [Correction of the methodology for assessing the security of speech information from leakage through technical channels in conditions of speech forcing]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta*, 2014, no. 2(55), pp. 183-189.
6. Makarov Yu. K., Khorev A. A. K otsenke effektivnosti zashchity akusticheskoi (rechevoi) informatsii [To assess the effectiveness of the protection of acoustic (speech) information]. *Spetsial'naya tekhnika*, 2000, no. 5, pp. 46–56.
7. Ivanov A. V., Salimov Sh. R. O vozmozhnosti primeneniya tekhnologii raspoznavaniya rechi v zadachakh otsenki zashchishchennosti akusticheskoi informatsii ot utechki po tekhnicheskim kanalam [On the possibility of using speech recognition technology in the tasks of assessing the security of acoustic information from leakage through technical channels]. *Dinamika sistem, mekhanizmov i mashin*, 2020, vol. 8, no 2, pp. 109–114.
8. Zhabyko E. I., Rublevskaya N. I. *Akusticheskoe proektirovanie zalov mnogotselevogo naznacheniya* [Acoustic design of multi-purpose halls]. Vladivostok, Izdatel'stvo DVGTU, 2008, 89 p.
9. Khorev A. A., Porev I. S. Metodika veroyatnostnoi otsenki razborchivosti [The method of probabilistic assessment of intelligibility]. *Zashchita informatsii. Insaid*, 2020, no. 2(92), pp. 44-52.
10. Trushin V. A., Zavodovskaya A. I., Oveshnikov I. A., Toporishchev E. V. Issledovanie vozdeistviya rechepodobnoi pomekhi na psikhoemotsional'noe sostoyanie cheloveka [Investigation of the impact of speech-like interference on the psychoemotional state of a person]. *Dinamika sistem, mekhanizmov i mashin*, 2020, vol. 8, no. 2, pp. 138-144.
11. *Ivanov A. V., Reva I. L., Shemshetdinova E. E.* Issledovanie vliyaniya razlichii v spektrakh rechi na rezul'tat otsenki razborchivosti [Investigation of the effect of differences in speech spectra on the result of the intelligibility assessment]. *Dinamika sistem, mekhanizmov i mashin*, 2017, vol. 5, no. 4, pp. 65–70.
12. *Adobe Audition. Professional'naya studiya zvukozapisi* [Adobe Audition. Professional recording studio], available at: `https://www.adobe.com/ru/products/audition.html` (accessed: 10.09.2023).
13. *PyAudio 0.2.13 – Python Package Index*, available at: `https://pypi.org/project/PyAudio/` (accessed: 10.09.2023).
14. *Librosa 0.10 – Librosa – audio and music processing in Python*, available at: `https://librosa.org/doc/latest/index.html` (accessed: 10.09.2023).
15. Giannakopoulos T. PyAudioAnalysis: An open-source python library for audio signal analysis. *PLoS ONE*, 2015, no. 10(12), pp. 1-17.
16. Bélanger O. Pyo, the python DSP toolbox. *MM 2016 - Proceedings of the 2016 ACM Multimedia Conference*, 2016, pp. 1214-1217.
17. Umnyashkin S. V. *Osnovy teorii tsifrovoi obrabotki signalov* [Fundamentals of the theory of digital signal processing]. Moscow, Tekhnosfera, 2016. 528 p.
18. Tyagi V., Wellekens C. On desensitizing the Mel-cepstrum to spurious spectral components for robust speech recognition. *Proceedings (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005, pp. 1-21.
19. Gerasimov S. M., Zharinov O. O. Issledovanie metodov analiza rechevykh signalov [Research of methods of speech signal analysis]. *Sbornik dokladov sem'desyat tret'ei mezhdunarodnoi studencheskoi nauchnoi konferentsii GUAP*, 2020, vol. 3, pp. 36-41.

20. *NumPy documentation*, available at: https://numpy.org/doc/stable/ (accessed: 10.09.2023).
21. *Matplotlib 3.7.2 documentation*, available at: https://matplotlib.org/stable/tutorials/index.html (accessed: 10.09.2023).
22. Li J., Deng L., Haeb-Umbach R., Gong Y. *Robust automatic speech recognition. A bridge to practical applications*, 2016, 286 p.
23. Fang Z., Yin B., Du Z. et al. Fast environmental sound classification based on resource adaptive convolutional neural network. *Scientific Reports*, 2022, no. 12, pp. 1-18.
24. Madhu A., Kumaraswamy S. EnvGAN: a GAN-based augmentation to improve environmental sound classification. *Artificial Intelligence Review*, 2022, no. 55, pp. 6301-6320.
25. Kim B., Kim J., Ye J. C. Task-Agnostic Vision Transformer for Distributed Learning of Image Processing. *Transactions on Image Processing*, 2023, no. 32, pp. 203-218.
26. Ullah R., Asif M., Shah W. A., Anjam F., Ullah I., Khurshaid T., Wuttisittikulkij L., Shah S., Ali S. M., Alibakhshikenari M. Speech Emotion Recognition Using Convolution Neural Networks and Multi-Head Convolutional Transformer. *Sensors 23*, 2023, no. 13, pp. 1-20.
27. Porkodi S. P., Sarada V., Maik V. et al. Generic image application using GANs (Generative Adversarial Networks): A Review. *Evolving Systems 14*, 2023, pp. 903-917.
28. Song Q., Sun B., Li S. Multimodal Sparse Transformer Network for Audio-Visual Speech Recognition. *IEEE Transactions on Neural Networks and Learning Systems*, 2023, vol. 34, no. 12, pp. 10028-10038.
29. *Vision Transformer: What It Is & How It Works (2023 Guide)*, available at: https://www.v7labs.com/blog/vision-transformer-guide/ (accessed: 13.12.2023).
30. Tay Y., Dehghani M., Gupta J., Bahri D., Aribandi V., Qin Z., Metzler D. Are Pre-trained Convolutions Better than Pre-trained Transformers? 2022, *arXiv: 2105.03322 [cs.CL]*.
31. Sanford C., Hsu D., Telgarsky M. Representational Strengths and Limitations of Transformers. 2023, *arXiv:2306.02896 [cs.LG]*.
32. Abdel-Hamid O., Mohamed A.-R., Jiang H., Penn G. Applying convolutional neural networks concepts to hybrid NN-HMM model for speech recognition. *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, 2012, pp. 4277-4280.
33. Sikorskii O. S. Obzor svertochnykh neironnykh setei dlya zadachi klassifikatsii izobra-zhenii [Overview of convolutional neural networks for image classification problem], *Novye informatsionnye tekhnologii v avtomatizirovannykh sistemakh*, 2017, no. 20, pp. 1-8.
34. Ciretan D. C., Giusti A., Gambardella L. M., Schmidhuber J. Deep neural networks segment neuronal membranes in electron microscopy images. *Proc. NIPS*, 2012, pp. 1-9.
35. Ciretan D. C., Meier U., Gambardella L. M., Schmidhuber J. Deep, Big, Simple Neural Nets for Handwritten Digit Recognition, *MIT Press*, 2010, vol. 22, no. 12, pp. 3207-3220.
36. Chto takoe svertochnaya neironnaya set' – Khabr [What is a convolutional neural network – Habr], available at: https://habr.com/ru/articles/309508/ (accessed: 10.09.2023).
37. Trushin V. A. Informatsionno-izmeritel'naya model' formantnogo metoda opredeleniya razborchivosti rechi [Information and measurement model of the formant method for determining speech intelligibility]. *Trudy Nauchno-issledovatel'skogo instituta radio*, 2017, no. 4, pp. 2-9.

Nikita A. Volkov

Postgraduate student of the Department of Electronic Systems and Information Security, Samara State Technical University (SamSTU, Russia, 443011, Samara, Molodogvordeyskaya St. 244), phone: +7 846 337-31-96, e-mail: volkovnikandr@gmail.com, ORCID ID: 0000-0002-0644-6332.

Andrey V. Ivanov

Cand. of Sci. (Engineering), Associate Professor of the Department of Electronic Systems and Information Security, Samara State Technical University (SamSTU, Russia, 443011, Samara, Molodogvordeyskaya St. 244), phone: +7 846 337-31-96, e-mail: andrej.ivanov@corp.nstu.ru, ORCID ID: 0000-0003-2002-8572.

DOI: 10.55648/1998-6920-2024-18-2-57-68 УДК 621.3.049.779

Принципы организации программно-аналитической системы для параллельной обработки сейсмических данных

А. Ю. Выродов, В. А. Перепёлкин, М. С. Хайретдинов, А. В. Хрыпченко

Институт вычислительной математики и математической геофизики СО РАН

Аннотация: Прогресс в развитии современных информационных технологий непосредственно связан с применением ресурсоемких приложений в наукоемких исследованиях, а также в промышленных прикладных задачах. В настоящее время остро стоит проблема анализа больших объемов геофизических данных и повышения производительности систем для их исследования. Один из путей решения данной проблемы заключается в применении многопроцессорных ЭВМ и многомашинных вычислительных комплексов, способных производить параллельную, в том числе распределенную, обработку данных. В работе представлены описание и реализация вычислительной модели для параллельной обработки сейсмических данных на базе системы LuNA для автоматического конструирования параллельных программ.

Ключевые слова: сейсмотрасса, быстрое преобразование Фурье, взаимокорреляционная функция, параллельная обработка, система LuNA, активные знания, сейсмические данные.

Для цитирования: Выродов А. Ю., Перепёлкин В. А., Хайретдинов М. С., Хрыпченко А. В. Принципы организации программно-аналитической системы для параллельной обработки сейсмических данных // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 57–68. https://doi.org/10.55648/1998-6920-2024-18-2-57-68.

Статья поступила в редакцию 11.12.2023;
принята к публикации 22.01.2024.

1. Введение

Построение эффективной системы управления вычислительными ресурсами современных систем обработки геофизических данных требует разработки новых методов, не зависящих от размеров системы и позволяющих автоматизировать процессы управления с учетом текущего состояния системы в целом и ее отдельных компонентов. Предметной областью является разработка системы. Для этого нужно описать сценарии и частичный порядок действий, связанных с организацией вычислительного процесса, специфицировать характеристики объектов данных, подаваемых на вход вычислительным программам, и результирующих объектов данных.

Теория синтеза параллельных программ и систем на вычислительных моделях [1], получившая развитие в концепции активных знаний [2], предлагает подход к автоматизации конструирования параллельных программ на основе формального описания предметной области,

в которой проводится моделирование, включая описание накопленных в этой области программных модулей. В качестве базового математического аппарата для такой формализации используются вычислительные модели. Это позволяет, с одной стороны, автоматически переиспользовать накопленные программные модули для решения новых задач в предметной области и, с другой стороны, автоматически решать формально поставленные в предметной области задачи с учетом предъявляемых нефункциональных требований [3]. В частности, в настоящей работе основным нефункциональным требованием является ускорение вычислений за счёт параллельной работы имеющихся модулей обработки сейсмических сигналов. В работе используется поддерживающая указанный подход система LuNA [4] для автоматического конструирования параллельной программы.

2. Требования, предъявляемые к системе

В техническом задании к разрабатываемой системе определяются:
- требования к системе в целом;
- требования к функциям (задачам), выполняемым системой;
- требования к видам обеспечения [5].

Примером реализации параллельной обработки данных является организация многоканальной свертки сейсмических сигналов с числом каналов до 100. Задачей представленной работы является организация программных средств многоканальной параллельной свертки, исследование производительности и визуализация результатов обработки. За основу реализации выбран язык Python и система LuNA. Для этого используется взаимокорреляционная функция, именуемая дальше ВКФ, и быстрое преобразование Фурье, именуемое дальше БПФ. Стоит также ввести термин «секционирование» – это процесс разбиения на отрезки во временном сигнале, необходимый для вычисления свертки в реальном времени.

Подробно алгоритм взаимокорреляционной функции описывается в книге Бендат Дж., Пирсол А. «Измерение и анализ случайных процессов» [11].

Расчет ВКФ с секционированием:

$$\hat{R}_{xy}(rh) = \sum_{n=1}^{511} x_n y_{n+r} + \sum_{n=512}^{1023} x_n y_{n+r} + \ldots + \sum_{n=512(M-1)}^{512M-1} x_n y_{n+r}, \quad (1)$$

где M – число секций. Размер секции – 512 элементов. Время расчета взаимокореляционной функции:

$$T = T_0 \cdot m \cdot N_{0n}, \quad (2)$$

T_0 – время выполнения элементарной операции, $N_{\text{оп}}$ – число отсчетов опорного сигнала [6].

В результате алгоритм должен быть реализован в параллельном виде в многоканальном режиме.

Задача реализации на практике имеет временные требования, обуславливающие необходимость применения параллельных вычислений: согласно техническим требованиям время вычислений не должно превышать 1 с.

Вычисление этой операции в реальном масштабе времени, т.е. в темпе поступления данных при априорно неизвестных временах прихода сейсмических и акустических колебаний, возможно лишь путем секционирования длинных временных последовательностей. К тому же использование алгоритма быстрого преобразования Фурье (БПФ) для обработки секционированных данных обеспечивает возможности высокопроизводительных вычислений.

Пусть Y – искомая коррелотрасса. При секционировании оценка ее вычисляется в итерационном виде:

$$Y^{i+1} = f\left(Y^i, X_{i+1}\right), \quad (3)$$

где Y^i – приближение Y на i-м шаге, X_{i+1} – текущие отсчеты данных.

Секционированные входные данные по мере поступления накапливаются во вспомогательных буферах и после заполнения очередного буфера обрабатываются при помощи БПФ. Таким образом, для того чтобы иметь возможность обрабатывать сигналы в режиме реального времени с использованием БПФ, надо представить апериодическую корреляционную свертку двух массивов большого размера как сумму циклических обычных сверток частей (секций) этих массивов. Причем это разбиение надо сделать таким образом, чтобы трудоемкость обработки одной секции зависела только от величины этой секции и не зависела от множества всех входных отсчетов размера *N*. Это аналогично тому, что имеет место в цифровой фильтрации, когда размер опорной последовательности, представляющей дискретный аналог импульсной функции фильтра, несоизмеримо меньше размеров входных и выходных массивов, которые можно считать бесконечными. Напротив, в задачах обработки вибросейсмических сигналов входной *X* и опорный *S* массивы имеют одинаково большие размерности, а результат их свертки *Y* представляется сравнительно небольшим числом отсчетов *M* (*M* << *N*). Это обстоятельство лежит в основе выбора подхода к разбиению массивов *X* и *S*.
С учетом этого алгоритм свертки обоих массивов может быть представлен в виде

$$\underset{m=0\ldots M-1}{Y_m} = \sum_{n=0}^{N-1} X_n \cdot S_{n-m} = \sum_{l=0}^{\frac{N}{M}-1} \sum_{n=0}^{M-1} X_{M\cdot l+n} \cdot S_{M\cdot l+n-m} = \sum_{l=0}^{\frac{N}{M}-1} \sum_{n=0}^{2L-1} A_n^l \cdot B^l_{\langle m-n\rangle_{2M}}, \quad (4)$$

где *M* – размер одной секции входного массива (подразумевается, что *N* делится на *M* нацело, в противном случае массив расширяется путем дописывания нулей). *A* и *B* – массивы, состоящие из 2*L* отсчетов и определяемые следующим образом:

$$A_i^l = \begin{cases} X_{m\cdot l+i}, \text{ если } 0 \le i \le M \\ 0, \text{ если } M \le i \le 2M \end{cases}, \quad (5)$$

$$B_i^l = S_{M\cdot(l-1)+\langle M-i\rangle_{2M}}, \quad (6)$$

$$0 \le i \le 2M. \quad (7)$$

В соответствии с теоремой о свертке для дискретного случая циклическая свертка двух массивов равна обратному дискретному преобразованию Фурье (ОДПФ) от произведения прямых ДПФ этих массивов, следовательно:

$$\underset{m=0\ldots M-1}{Y_m} = \frac{1}{N} \sum_{l=0}^{\frac{N}{M}-1} \sum_{k=0}^{2M-1} \left(\sum_{n=0}^{2M-1} A_n^l \cdot W^{-n\cdot k} \right) \cdot \left(\sum_{l=0}^{2M-1} B_n^l \cdot W^{-l\cdot k} \right) \cdot W^{k\cdot m}, \quad (8)$$

где $W = e^{j\cdot\frac{2\pi}{2M}}$

На рис. 1 приведена схема, иллюстрирующая порядок действий, производимых при обработке *i*-ой секции входной последовательности *X*. Значок * означает БПФ от массивов и умножение спектра массива *A* на спектр, комплексно сопряженный со спектром массива *B*. Такие действия производятся для каждой секции входной последовательности. По завершении работы вычисляется коррелограмма путем выполнения обратного БПФ от спектра *Y*.

Трудоемкость используемого алгоритма БПФ (двухточечного, рассчитанного на вещественные данные) составляет $\frac{N}{2}\cdot\left(3\cdot\log_2 N-5\right)+4$ операций сложения и $N\cdot\left(\log_2 N-3\right)+4$ операций умножения, т.е. в сумме: $\frac{N}{2}\cdot\left(5\cdot\log_2 N-11\right)+8$.

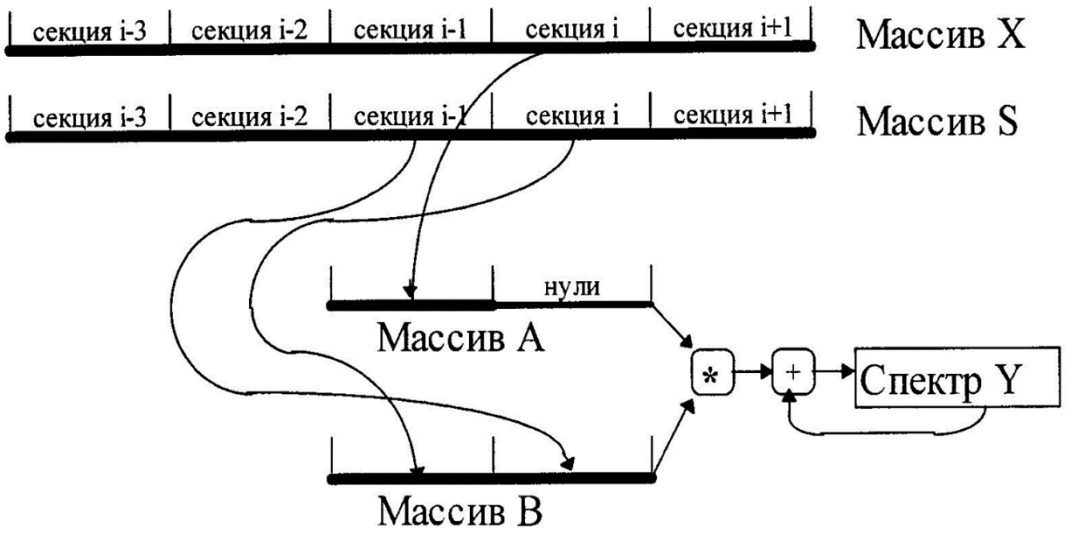


Рис. 1. Схема порядка действий, производимых при обработке *i*-ой секции входной последовательности *X*

3. Характеристики формата представления данных

Данные каждого сеанса представлены в виде отдельных файлов трасс. Каждый файл состоит из заголовка фиксированной длины и последовательно размещенных отсчетов одного канала.

Таблица 1. Представления файла коррелотрассы

Заголовок (*N* байт)
Отсчет 1 (*M* байт)
Отсчет 2 (*M* байт)
…
Отсчет *K* (*M* байт)

Таблица 2. Представления заголовка файла формата PC

Смещ.	**Длина**	**Тип и имя**	**Значение**	**Комментарии**
+00	2	int ID	ID=’PC’	Идентификатор формата
+02	1	char Ver	Ver=l	Номер версии
+03	1	char SubVer	SubVer=l	Номер подверсии
+04	2	int HLen	Hlen=42	Длина заголовка в байтах
+06	4	long Datetime		Дата и примерное время начала в секундах с 1 января 1970 г.
+10	4	long Duration		Длительность сеанса в секундах
+14	8	double Scale		Коэффициент пересчета в физическую величину
+22	1	char Year		Год начала сеанса

Смещ.	Длина	Тип и имя	Значение	Комментарии
+23	1	char Month		Месяц начала сеанса
+24	1	char Day		День начала сеанса
+25	1	char Hour		Час начала сеанса
+26	1	char Minute		Минута начала сеанса
+27	1	char Second		Секунда начала сеанса
+28	4	long MicroSec		Поправка в микросекундах к времени начала сеанса
+32	2	int SamplRate		Частота дискретизации в Гц
+34	4	long SamplNum		Число отсчетов в трассе
+38	2	int SamplType		Длина и тип отсчета: 0002h – int – знаковое 16 бит 0102h – unsigned – беззнаковое 0004h – long – двойное 32 бит 1004h – float – плавающая точка 1008h – double – двойное
+40	1	char TrNum		Номер трассы в исходном файле
+41	1	char Reserved	00	Зарезервировано, д.б. ноль

Формат отсчета задан полем SamplType. Типы int, unsigned, long, float и double подчиняются стандартам типов, принятым в Borland C++, v.3.1. Порядок байт – младший байт по младшему адресу. Стандарт чисел с плавающей точкой – IEEE. Стандарт отрицательных целых чисел – обратный дополнительный код [7].

Используемые форматы сейсмической записи – Seg-D, Seg-Y, Seg-B, Seg-A, Cray Seg-Y, CGG Geovecteur, PC.

4. Исходные данные экспериментов

Используются данные в виде записей сейсмических колебаний от вибрационного источника ЦВ-40 на удалении 50 км. Амплитуда возмущающей силы источника составляет 40 тс. Вибрационный источник ЦВ-40 излучает одновременно длительные сейсмические колебания в земле и акустические – в атмосфере.

Время начала сеансов излучения составляет 15, 17, 21 и 23 часа (по Гринвичу), полосы частот излучения Δf – 6.25–9.57 Гц, длительность T = 2850 с. [6].

Полученные записи $X(t)$ сворачиваются с опорным сигналом $Y(t)$ в соответствии с алгоритмом (1) с применением процедуры БПФ. Опорный сигнал синтезируется в точке приема.

В рамках решаемой задачи подготовлены тестовые данные в количестве 100 сейсмотрасс и опорного сигнала. Размер файла сейсмограммы – 1.34 Мб. На рис. 2 представлен эксперимент с последовательной обработкой сейсмотрасс для нахождения взаимокорреляционной свертки. В результате получаем время обработки более 4 с.

16_11011500_14.U8831Vk02 - OK A=9.38 SNR=27.0
16_11011500_15.U8831Vk00 - OK A=19.64 SNR=28.0
16_11011500_15.U8831Vk01 - OK A=17.48 SNR=21.6
16_11011500_15.U8831Vk02 - OK A=9.38 SNR=27.0
16_11011500_16.U8831Vk00 - OK A=19.64 SNR=28.0
16_11011500_16.U8831Vk01 - OK A=17.48 SNR=21.6
16_11011500_16.U8831Vk02 - OK A=9.38 SNR=27.0
processing time: 4.14s

Рис. 2. Время обработки 100 сейсмотрасс

Чтобы уменьшить временные затраты на обработку сигналов, решено применить параллельные вычисления, используя систему LuNA для автоматического конструирования параллельной программы.

5. Принцип параллелизма в системе LuNA

Проанализируем задачу с точки зрения параллельной обработки данных. Обработка сейсмотрасс для каждого канала может осуществляться независимо, в т.ч. параллельно. В идеале для N каналов это даёт возможность ускорить вычисления за счёт параллельной обработки в N раз. На практике эта величина будет меньше вследствие отсутствия достаточного количества вычислительных ядер для одновременной обработки всех каналов, одновременного доступа параллельных процессов обработки к общей файловой системе (локальной или сетевой), а также накладных расходов операционной системы на создание требуемого количества процессов. Предварительное исследование производительности последовательной программы показало, что для удовлетворения требования по времени обработки в 1 секунду требуется достичь ускорения в несколько раз (около 5 раз). Таким образом, наличие около 100 каналов создаёт достаточное количество задач для достижения требуемой производительности. В качестве аппаратного обеспечения может быть использован параллельный вычислитель с общей или распределенной памятью с 5 и более ядрами.

В качестве подхода к реализации параллельной обработки сейсмотрасс предлагается применить подход активных знаний [8]. Этот подход целесообразно применять в случаях, когда, во-первых, некоторый программный модуль используется многократно для решения различных задач и, во-вторых, когда одна и та же задача должна решаться в различных условиях – на вычислителях с разной конфигурацией, для разных классов входных данных, с разными нефункциональными требованиями (по времени выполнения, по энергоэффективности, по надёжности и т.п.). Ручное программирование потребовало бы переработки программы под изменяющиеся условия, поэтому целесообразно применение методов автоматизации конструирования программ.

Применение системы LuNA для автоматического конструирования параллельной программы на основе концепции активных знаний подразумевает формальное описание предметной области в виде вычислительной модели [9]. По существу, это означает описание множества переменных – величин предметной области, а также множества операций, задающих возможность вычислять одни величины из других. Каждой операции ставится в соответствие вычислительный модуль (например, последовательная программа или процедура) с указанием его нефункциональных свойств. Далее ставится задача в виде перечня входных и выходных переменных, а система автоматически конструирует требуемую программу, выводя частично упорядоченное множество операций, обеспечивающих вычисление выходных переменных из входных.

Применительно к исследуемой задаче вычислительная модель будет содержать множество из 100 информационно независимых операций. По этому описанию система LuNA автоматически построит параллельную программу, обеспечивающую параллельную обработку данных.

6. Вычислительная модель проектируемой системы

Для того чтобы использовать систему LuNA, необходимо было описать вычислительную модель, представленную в виде двудольного графа операций и переменных.

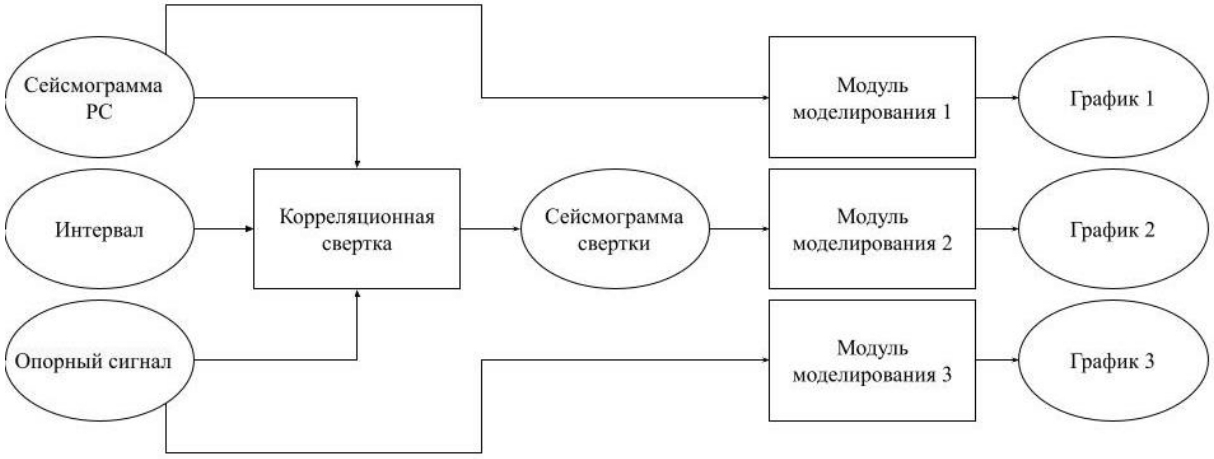


Рис. 3. Сценарий вычислительной модели

На рис. 3 представлен сценарий вычислительной модели, описывающий нахождение корреляционной свертки и построение графика. Овалами обозначены данные, прямоугольниками – операции.

Совокупность сценариев описывается вычислительной моделью и позволяет пользователям, задавая входные и выходные данные, получать результат, избавляя пользователя от рутины, не связанной с сутью решаемых задач [10].

Таким образом, описав вычислительную модель, получаем файл, представленный ниже (код содержит незначительные упрощения). Файл содержит описание всех входных и выходных переменных, а также операций, производимых над ними.

```
#!/usr/bin/env cm
{
"variables": ["files","opora","path","t1","t2","f","step","f1","f2","duration","spec_one_out-
put","get_file_output",
"spec_one_output","corr_output","draw_output","draw_plot_out-
put","RHO_output","FMax_output"],
   "operations": {
      "spec": {
         "inputs": ["get_file_output"],
         "outputs": ["spec_one_output"],
         "type": "external_cmd",
         "external_cmd": "python ./Python/spec.py"
      },
      "draw": {
         "inputs": ["spec_one_output"],
         "outputs": ["draw_output"],
         "type": "external_cmd",
         "external_cmd": "python ./Python/draw.py"
      },
      "draw_plot": {
         "inputs": ["get_file_output"],
         "outputs": ["draw_plot_output"],
```

```
        "type": "external_cmd",
        "external_cmd": "python ./Python/draw_plot.py"
      },
      "get_file": {
        "inputs": ["path","t1","t2","f","step","f1","f2"],
        "outputs": ["get_file_output"],
        "type": "external_cmd",
        "external_cmd": "python ./Python/get_file.py"
      },
      "calc_rho": {
        "inputs": ["spec_one_output"],
        "outputs": ["RHO_output"],
        "type": "external_cmd",
        "external_cmd": "python ./Python/calc_rho.py"
      },
      "calc_fmax": {
        "inputs": ["get_file_output","spec_one_output"
        ],
        "outputs": ["FMax_output"],
        "type": "external_cmd",
        "external_cmd": "python ./Python/calc_fmax.py"
      },
      "corr": {
        "inputs": ["files","opora","duration"],
        "outputs": ["corr_output"],
        "type": "external_cmd",
        "external_cmd": "./corr/corr.exe"
      }
    }
}
```

Рис. 4. Вычислительная модель

7. Краткая характеристика результатов корреляционной обработки

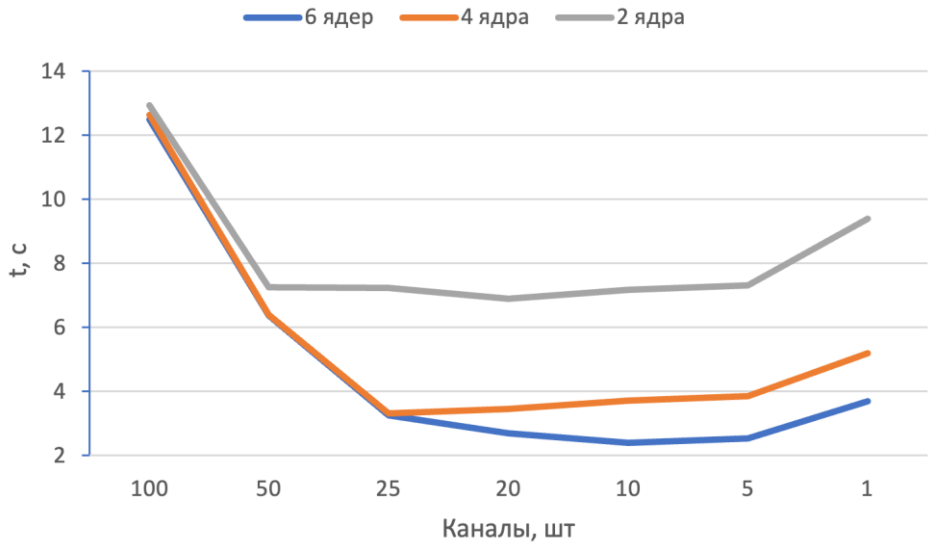


Рис. 5. Зависимость времени обработки от количества ядер процессора

Тестирование выполнялось на компьютере MacBook Pro с процессором M1 Pro, 12 Гб оперативной памяти и частотой процессора 3.2 ГГц. В ходе экспериментов параллельно запускалось разное количество фрагментов. Каждый фрагмент содержал равное количество каналов (1 фрагмент – 100 каналов, 2 фрагмента – 50 каналов в каждом и т.д). Из рис. 5 видно, что для 6-ядерного процессора оптимальным является параллельный запуск 10 фрагментов по 10 каналов в каждом. Из графика видно, что ускорение близко к линейному (около 2 раз на 2 ядрах, около 4 раз на 4 ядрах и около 6 раз на 6 ядрах), поэтому и на большем числе ядер можно ожидать ускорение в соответствующее число раз.

Как следует из анализа полученных результатов обработки в виде коррелотрасс, параллельная обработка дала прирост производительности и уменьшение времени обработки сигналов. Время обработки уменьшилось до 2.4 с (рис. 5). Для улучшения результатов необходимо провести эксперимент на 8-ядерном процессоре.

8. Заключение

Организация программно-аналитической системы для параллельной обработки сейсмических данных является важным шагом в развитии сейсмологии и геологии. Внедрение такой системы позволит значительно улучшить скорость и точность обработки данных, сократить время и затраты на исследования, а также повысить эффективность принятия решений в области геологического исследования. В ходе работы был проведен корреляционный анализ данных вибрационного зондирования наземной и атмосферной трасс распространения геоакустических колебаний.

В результате применения параллельных вычислений на основе системы LuNA было уменьшено время многоканальной обработки сейсмотрасс в 4 раза. Кроме того, программно-аналитическая система способна обеспечить параллельную обработку больших объемов данных, что особенно актуально в контексте современных глобальных вызовов, таких как изменение климата и использование природных ресурсов. Благодаря использованию современных технологий и надежным принципам организации данная система обеспечивает возможность более эффективного изучения сейсмических явлений и разработки новых методов прогнозирования и предотвращения природных катаклизмов. Однако для полного использования потенциала такой системы необходимо дальнейшее исследование и развитие методов анализа данных, а также реализация принципа параллельных вычислений для поточной свертки, применяемой в решении задач, связанных с обработкой сейсмических данных в системе LuNA.

Литература

1. A foreign function library for Python// Python Documentation [Электронный ресурс]. URL: `https://docs.python.org/2/library/ctypes.html` (дата обращения: 2023).
2. *Kholodkov K. I., Aleshin I. M*. Exact calculation of a posteriori probability distribution with distributed computing systems // Computer Research and Modeling. 2015. P. 539–542.
3. *Malyshkin V.* Active Knowledge, LuNA and Literacy for Oncoming Centuries // Programming Languages with Applications to Biology and Security: Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday // Lecture Notes in Computer Science. Springer Cham. 2015. V. 9465. P. 292–303. DOI 10.1007/978-3-319-25527-9_19.
4. *Malyshkin V. E., Perepelkin V. A.* LuNA Fragmented Programming System, Main Functions and Peculiarities of Run-Time Subsystem // Parallel Computing Technologies. 2011. LNCS 6873. P. 53–61.
5. Matplotlib: Python plotting – Matplotlib 3.2.1 documentation // Matplotlib Documentation [Электронный ресурс]. URL: `https://matplotlib. org/` (дата обращения: 2023).

6. *Караваев Д. А., Якименко А. А., Булавина Н. А.* Технология моделирования полного сейсмического поля на высокопроизводительных вычислительных системах // Труды XIII Международной научно-технической конференции «Актуальные проблемы электронного приборостроения», 3–6 октября 2016, Новосибирск. С. 41–45.
7. Python interface to Tcl/Tk // Python Documentation [Электронный ресурс]. URL: https://docs.python.org/3/library/tkinter.html (дата обращения: 2023).
8. The sound amplifying forest with emphasis on sounds from wind turbines‖ Elis Johansson // Department of Civil and Environmental Engineering. Division of Applied Acoustics. Chalmers University of Technology. Sweden. 2010. 97 p.
9. *Марапулец Ю. В., Сенкевич Ю. И., Луковенкова О. О., Солодчук А. А., Ларионов И. А., Мищенко М. А., Малкин Е. И., Щербина А. О., Гапеев М. И.* Комплексный анализ акустических и электромагнитных сигналов для оценки уровня сейсмической опасности: монография. Владивосток: Дальнаука, 2020. 120 с.
10. *Вальковский В. А., Малышкин В. Э.* Синтез параллельных программ и систем на вычислительных моделях. Новосибирск: Наука, 1988. 129 с.
11. *Bendat J. S., Piersol A. G.* Random data: analysis and measurement procedures. New York (N.Y.) Wiley-Interscience, 1971. 88 p.

Выродов Алексей Юрьевич
аспирант, Институт вычислительной математики и математической геофизики СО РАН, e-mail: g47711@gmail.com, ORCID ID: 0009-0002-3399-3603.

Перепёлкин Владислав Александрович
к.т.н., Институт вычислительной математики и математической геофизики СО РАН, e-mail: perepelkin@ssd.sscc.ru, ORCID ID: 0000-0002-6998-4525.

Хайретдинов Марат Саматович
д.т.н., г.н.с., профессор, Институт вычислительной математики и математической геофизики СО РАН (ИВМиМГ СО РАН, 630090, Новосибирск, просп. Ак. Лаврентьева, 6), тел. +7 383 330 87 43, e-mail: marat@opg.sscc.ru, ORCID ID: 0000-0002-3250-521X.

Хрыпченко Алёна Валерьевна
аспирант, Институт вычислительной математики и математической геофизики СО РАН, e-mail: ahrypchenko@yandex.ru, ORCID ID: 0009-0002-7627-6276.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Principles of Organizing a Software-analytical System for Parallel Processing of Seismic Data

Alexey Y. Vyrodov, Vladislav A. Perepelkin, Marat S. Khayretdinov, Alena V. Khrypchenko

Institute of Computational Mathematics and Mathematical Geophysics SB RAS

Abstract: Progress in the development of modern information technologies is directly related to the use of resource-intensive applications in science-intensive research, as well as in industrial applications. Currently, there is an acute problem of analyzing large volumes of geophysical data and increasing the productivity of systems for their study. One of the ways to solve this problem is to use multiprocessor computers and multi-machine computing systems capable of performing parallel, including distributed data processing. The paper presents a description and implementation of a computational model for parallel processing of seismic data based on the LuNA system for the automatic construction of parallel programs.

Keywords: seismic trace, fast Fourier transform, cross-correlation function, parallel processing, LuNA system, active knowledge, seismic data.

For citation: Vyrodov A. Yu., Perepelkin V. A., Khayretdinov M. S., Khrypchenko A. V. Principles of organizing a software-analytical system for parallel processing of seismic data (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 57-68. https://doi.org/10.55648/1998-6920-2024-18-2-57-68.

The article was submitted: 11.12.2023;
accepted for publication 22.01.2024.

References

1. *A foreign function library for Python. Python Documentation*, available at: https://docs.python.org/2/library/ctypes.html (accessed: 2023).
2. Kholodkov K. I., Aleshin I. M., Exact calculation of a posteriori probability distribution with distributed computing systems. *Computer Research and Modeling*, 2015, vol. 7, pp. 539-542.
3. Malyshkin V. Active Knowledge, LuNA and Literacy for Oncoming Centuries. *Programming Languages with Applications to Biology and Security: Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday. Lecture Notes in Computer Science*, Springer Cham, 2015, vol. 9465, pp. 292-303, DOI 10.1007/978-3-319-25527-9_19.
4. Malyshkin V. E., Perepelkin V. A. 2011. LuNA Fragmented Programming System, Main Functions and Peculiarities of Run-Time Subsystem. *Parallel Computing Technologies*, LNCS 6873, pp. 53-61.
5. Matplotlib: Python plotting – Matplotlib 3.2.1 documentation. *Matplotlib Documentation*, available at: https://matplotlib. org/ (accessed: 2023).
6. Karavaev D. A., Yakimenko A. A., Bulavina N. A. *Technology for modeling the full seismic field on high-performance computing systems*, 2016.
7. Python interface to Tcl/Tk. *Python Documentation*, available at: https://docs.python.org/3/library/tkinter.html (accessed: 2023).
8. The sound amplifying forest with emphasis on sounds from wind turbines‖ Elis Johansson. *Department of Civil and Environmental Engineering. Division of Applied Acoustics*, Chalmers University of Technology, Sweden, 2010, 97 p.
9. Marapulets Yu. V., Senkevich Yu. I., Lukovenkova O. O., Solodchuk A. A., Larionov I. A., Mishchenko M. A., Malkin E. I., Shcherbina A. O., Gapeev M. I. *Comprehensive analysis of acoustic and electromagnetic signals to assess the level of seismic hazard*, 2020.

10. Valkovsky V. A., Malyshkin V. E. *Synthesis of parallel programs and systems using computational models. — Novosibirsk: Science. Sib. department*, 1988, 129 p.
11. Julius S. Bendat, Allan G. Piersol. *Random data: analysis and measurement procedures*. New York (N.Y.) Wiley-Interscience, 1971, 88 p.

Alexey Yu. Vyrodov
Postgraduate student, Institute of Computational Mathematics and Mathematical Geophysics SB RAS, e-mail: g47711@gmail.com, ORCID ID: 0009-0002-3399-3603.

Vladislav A. Perepelkin
Ph.D., Institute of Computational Mathematics and Mathematical Geophysics SB RAS, e-mail: perepelkin@ssd.sscc.ru, ORCID ID: 0000-0002-6998-4525.

Marat S. Khairetdinov
Doctor of Technical Sciences, Chief Researcher, Professor, Institute of Computational Mathematics and Mathematical Geophysics SB RAS (ICM&MG SB RAS, 630090, Novosibirsk, Academician Lavrentiev Avenue, 6), tel. +7 383 330 87 43, e-mail: marat@opg.sscc.ru, ORCID ID: 0000-0002-3250-521X.

Alena V. Khrypchenko
Postgraduate student, Institute of Computational Mathematics and Mathematical Geophysics SB RAS, e-mail: ahrypchenko@yandex.ru, ORCID ID: 0009-0002-7627-6276.

DOI: 10.55648/1998-6920-2024-18-2-69-78 УДК 004.56

Разработка метода оценки покрытия кода при фаззинг-тестировании программного обеспечения методом черного ящика с использованием аппаратной виртуализации для оценки тестового покрытия

Н. Н. Самарин

ФГУП «Научно-исследовательский институт «Квант»» (г. Москва)

Аннотация: В настоящей статье представлен разработанный метод оценки покрытия при проведении фаззинг-тестирования программного обеспечения, использующий технологии аппаратной виртуализации. Тестируемое программное обеспечение рассматривается как черный ящик. Особенностью предлагаемого метода является возможность выполнения контроля состояния виртуальной машины, в которой осуществляется фаззинг-тестирование, в том числе осуществление мониторинга состояния процессора и входных данных в режиме реального времени. Проведенные эксперименты показали, что разработанный метод позволяет получить оценку тестового покрытия кода с высокой точностью, сопоставимой с методом оценки на основе статической инструментации, который, однако, применим только при проведении фаззинг-тестирования методом белого ящика.

Ключевые слова: информационная безопасность, тестирование, аппаратная виртуализация, оценка покрытия, фаззинг черного ящика.

Для цитирования: Самарин Н. Н. Разработка метода оценки покрытия кода при фаззинг-тестировании программного обеспечения методом черного ящика с использованием аппаратной виртуализации для оценки тестового покрытия // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 69–78. https://doi.org/10.55648/1998-6920-2024-18-2-69-78.

Статья поступила в редакцию 10.11.2023;
принята к публикации 13.02.2024.

1. Введение

Фаззинг-тестирование – одно из наиболее активно развивающихся направлений поиска архитектурных и логических ошибок, которые являются причиной возникновения уязвимостей в программном обеспечении (ПО) [1]. Основной задачей фаззинг-тестирования является автоматизация поиска уязвимостей с минимизацией вовлечения в процесс человека [1, 2]. При традиционном фаззинг-тестировании вовлечение эксперта необходимо на этапе запуска фаззера – для подготовки входных данных и оценки результатов после завершения тестирования.

Одной из проблем фаззинг-тестирования является поиск способов оценки покрытия исполняемого кода программы, когда она представляет собой черный ящик [1]. В таком случае эксперт не имеет возможности проведения инструментации тестируемой программы на уровне исходных текстов ввиду их отсутствия. Наиболее популярным методом инструмента-

ции в этом случае является бинарная инструментация, однако она ограничена возможностями операционной системы (ОС) [3].

Существуют методы инструментации на базе эмуляторов, к примеру, эмулятора QEMU, позволяющие отслеживать состояния тестируемой программы на низком уровне [3, 4]. Однако эмуляторы накладывают некоторые ограничения – при таком подходе не учитывается состояние физического процессора и целевой (для исполнения тестируемой программы) ОС. Более того, оценка покрытия с использованием эмулятора также ограничена возможностями самого эмулятора и требует больших вычислительных ресурсов для сокращения времени фаззинг-тестирования [3].

В качестве решения обозначенной проблемы предлагается использовать разработанный в рамках данной работы метод покрытия на основе аппаратной виртуализации. Суть метода заключается в том, что электронно-вычислительная машина (ЭВМ), на которой производится фаззинг-тестирование, находится под управлением прозрачного гипервизора одной виртуальной машины. Применение аппаратной виртуализации в контексте оценки покрытия позволяет не только полностью контролировать состояние программы в оперативной памяти, но также контролировать состояние процессора и операционной системы, тем самым фиксируя трассы, исполняемые тестируемой программой.

Аппаратную виртуализацию поддерживают лидирующие компании по производству процессоров – Intel и AMD [5]. В общих чертах реализация поддержки аппаратной виртуализации у данных производителей схожа, однако детали реализации отличаются.

В данной статье проведен анализ технологии аппаратной виртуализации, реализованной как в процессорах Intel, так и в процессорах AMD, а также приведено описание разработанного метода. Проведена практическая апробация разработанного метода с целью оценки покрытия при фаззинг-тестировании на хостовой ОС семейства Linux, эмуляторе QEMU и виртуализированной ОС семейства Linux.

2. Особенности аппаратной виртуализации

Аппаратная виртуализация подразумевает установку и функционирование гипервизора или монитора виртуальных машин на аппаратной составляющей ЭВМ [5]. Аппаратная виртуализация выступает в качестве промежуточного узла между ПО, функционирующим на более высоком уровне абстракции (к примеру, ОС), и аппаратным обеспечением. К наиболее распространенным средствам аппаратной виртуализации относятся VMware vSphere и Microsoft Hyper-V [5, 6, 7].

Отличительной особенностью аппаратной виртуализации от программной является тип установки гипервизора. В случае с аппаратной виртуализацией гипервизор устанавливается на аппаратное обеспечение без какой-либо прослойки – фактически становится своего рода ОС, главной задачей которой является реализация возможности запуска других ОС [6]. При этом гипервизор получает полный контроль над ОС, установленными внутри виртуальных машин, ввиду работы на более низком уровне абстракции.

Зачастую средства аппаратной виртуализации поддерживают несколько виртуальных машин, создаваемых внутри своего пространства. Это достигается благодаря разделению аппаратных ресурсов и выделению для каждой виртуальной машины собственного экземпляра виртуального устройства – будь то центральный процессор или контроллер USB [8].

Выделяется три типа аппаратной виртуализации: полная виртуализация, паравиртуализация и представление с аппаратной поддержкой [9]. Полная виртуализация подразумевает полную имитацию оборудования, в результате чего создается легкопереносимая среда. При использовании паравиртуализации разработчиком создается специальная сборка ОС, в которой изменен набор используемых компонентов в зависимости от предоставляемых ей ресурсов. Представление с аппаратной поддержкой реализует для виртуальной машины полностью виртуализированную среду без доступа к физическому аппаратному обеспечению.

К главному преимуществу аппаратной виртуализации относят исключительную простоту настройки и гибкость масштабирования при увеличение аппаратных ресурсов [7, 10]. Кроме того, важным аспектом является возможность создания 64-разрядной виртуальной машины даже на базе 32-разрядного процессора. При этом программным компонентам, исполняющимся внутри виртуальной машины, не удастся отличить виртуальное оборудование от реального [10].

Наиболее распространенными технологиями аппаратной виртуализации являются Intel VT-x и AMD-V. Далее будет кратко рассмотрена каждая технология.

3. Обзор Intel VT-x и AMD-V

Intel VT-x является расширением для виртуализации архитектуры процессора IA-32 [11]. Оно включает в себя набор инструкций обеспечения аппаратной виртуализации и два режима работы процессора. Основными преимуществами Intel VT-x являются:

– возможность полной изоляции виртуальных машин между собой и аппаратных компонентов ЭВМ;

– упрощенный интерфейс для управления аппаратным обеспечением, с помощью которого можно динамически выделять необходимые ресурсы для виртуальных машин в режиме реального времени;

– надежный механизм обеспечения безопасности данных за счет разграничения ресурсов на низком уровне абстракции.

Добавление дополнительных режимов работы к архитектуре IA-32 обусловлено необходимостью эффективного перехвата и эмуляции ряда служебных инструкций [11]. Первый режим работы – «root» – используется в качестве монитора виртуальных машин, а второй – «non-root» – для монитора гостевых окружений. Вход в режим «root» обеспечивается посредством выполнения инструкции VMXON, а входы в режим «non-root» – посредством выполнения инструкций VMLAUNCH/VMRESUME.

Важным процессом при разработке и применении технологии аппаратной виртуализации является сохранение состояния процессора при переключении между хостовой и гостевой операционными системами, а также при вызове функционирования в режиме монитора виртуальных машин. Для хранения состояния применяется структура VMCS (Virtual Machine Control Structure), которая создается индивидуально для каждой гостевой ОС [7, 11].

Кроме этого, в реализации технологии аппаратной виртуализации Intel применяется механизм, который позволяет гипервизору управлять порядком разметки виртуальных адресов и их проецирования на физические адреса памяти. Таким механизмом является EPT (Extended Page Table) [8, 11]. Он представляет собой таблицу трансляции адресов второго уровня и обеспечивает значительный прирост производительности работы блока управления памятью [11].

Реализация технологии аппаратной виртуализации от производителя AMD во многих архитектурных аспектах совпадает с реализацией от Intel. Так, процессоры AMD поддерживают режим работы процессора GuestMode, аналогичный режиму работы «non-root» в процессорах Intel, структуру VMCB – аналог VMCS – инструкцию для перехода в виртуальное окружение VMRUN и аналог EPT – Real Mode w/ Paging [12]. Однако в сравнении с Intel выделяется и ряд отличий. Например, для поддержки механизма Real Mode w/ Paging используется аппаратный контроллер памяти с поддержкой виртуализации. Это необходимо в первую очередь для обеспечения безопасности контроллера DMA (Direct Memory Access) [12]. Кроме того, используется защищенный монитор виртуальных машин – SVM (Secure Virtual Monitor), который обеспечивает безопасный запуск и контроль гостевой ОС на базе доверенного модуля платформы – TPM (Trusted Platform Module) [12].

Алгоритмы работы аппаратной виртуализации от Intel и AMD также аналогичны и предоставляют не только изоляцию тестируемой программы от аппаратных компонентов, но

и позволяют отслеживать состояние ее исполнения для оценки покрытия при фаззинг-тестировании. Поддержка аппаратной виртуализации двумя наиболее распространенными производителями процессоров позволяет обеспечить предлагаемый метод переносимостью без необходимости его доработки под конкретное аппаратное обеспечение.

4. Существующие методы оценки покрытия

Для оценки покрытия традиционно используются два метода – инструментация и отслеживание входных корпусов [13]. При этом инструментация делится на статическую (на уровне исходных текстов или на уровне исполняемого кода) и динамическую [13, 14]. Статическая инструментация на уровне исходных текстов включает в себя процесс компиляции тестируемого ПО с целью размещения внутри функциональных объектов специальных маркеров, при достижении которых средство фаззинг-тестирования получает сведения о прохождении трассы [15]. В результате сбора и накопления таких сведений рассчитывается общее покрытие тестируемого ПО.

Статическая инструментация на уровне исполняемого кода также заключается в добавлении специальных маркеров, однако может быть выполнена в отношении различных уровней детализации ПО – начиная от уровня инструкция и заканчивая уровнем образа исполняемого файла [16]. Так, например, средство для профилирования Valgrind осуществляет инструментацию на уровне функциональных объектов по следующему принципу:

1. В исполняемом коде выявляются все вызовы функциональных объектов.
2. Valgrind создает теневой стек с адресами возврата выявленных функций.
3. В ходе профилирования сравнивается значение адреса возврата функции с адресом, приведенным на теневом стеке.
4. Если адрес возврата на теневом и оригинальном стеках не совпадают, запоминается адрес инструкции, которая изменила стек.
5. В результате профилирования полученные адреса агрегируются, и на их основе рассчитывается итоговое покрытие.

Существенным недостатком такого подхода является тот факт, что сведения о покрытии могут быть получены только в результате нарушения работы тестируемой программы, что сказывается на точности оценки покрытия при низком количестве нарушений работ.

Динамическая инструментация работает схожим образом и применяется при невозможности использования статической инструментации [14, 16]. В этом случае маркеры устанавливаются в оперативной памяти, в которую загружена тестируемая программа. Динамическая инструментация имеет качественно более низкие оценки покрытия в связи с тем, что представление функциональных объектов в памяти может быть изменено компилятором на безусловные переходы вместо традиционного вызова [15]. Кроме того, в данном методе остается существенный недостаток, связанный с возможностью фиксирования показателей покрытия только при нарушении работы программы, что также накладывает ограничения при оценке итогового покрытия в контексте ее точности [17].

Реализация конкретного метода динамической инструментации может отличаться в зависимости от исходного алгоритма. Одним из наиболее распространенных алгоритмов является промежуточное представление исполняемого кода в памяти, которое модифицируется средством инструментации [18]. Это, в свою очередь, позволяет обеспечить целостность памяти, в которую размещен исполняемый код, и исключить возможные нарушения работы, связанные именно с процессом инструментации, такие как нарушение целостности данных программы, которые контролируются самой программой.

Отслеживание входных корпусов реализовано в виде режима фаззинг-тестирования на базе QEMU, а также в таких средствах инструментации, как Gcov и Lcov [3, 19]. Данные средства минимизируют объем входного корпуса с целью сбора как можно большего покрытия в кратчайшие сроки. При этом в памяти отслеживается состояние входного корпуса, и в

случае его уникальной модификации в процессе работы тестируемой программы считается, что достигнута новая трасса и, как следствие, получен прирост к покрытию.

Отслеживание входных корпусов основано на принципе создания большого количества входных данных фиксированного небольшого объема. На каждой итерации для функциональных объектов, в которые передаются входные данные, отслеживается их состояние, и в случае изменения данных фиксируется адрес, по которому вызывается модифицирующий код. По результатам тестирования множество адресов, по которым произведена модификация входных данных, анализируется, затем рассчитывается оценка покрытия. Важно отметить, что в случае, если входные данные в тестируемой программе не модифицируются, оценка покрытия будет нулевая, что, в сущности, не будет соответствовать действительности.

Таким образом, наиболее надежным способом инструментации является статическая инструментация на уровне исходных текстов, однако она неприменима при проведении фаззинг-тестирования черного ящика [19]. Предлагаемый метод, описанный далее, позволяет добиться точности оценки покрытия, близкой к точности оценки при статической инструментации, за счет возможности отслеживания состояния и содержимого аппаратных ресурсов ОС, на которой проводится фаззинг-тестирование.

5. Описание предлагаемого метода на основе аппаратной виртуализации для оценки покрытия

Одной из ключевых особенностей предлагаемого метода является поддержка большинства известных средств для проведения фаззинг-тестирования. Это обеспечивается за счет функционирования метода на уровне абстракции ниже ОС, что позволяет реализовать совместимость и мониторинг тестируемого ПО вне зависимости от среды исполнения.

Виртуальная машина, находящаяся под управлением гипервизора, предоставляет необходимые программные интерфейсы для доступа к состоянию виртуального процессора, оперативной памяти и видеопамяти [9]. В ходе мониторинга состояния виртуальной машины, на которой производится фаззинг-тестирование, гипервизор фиксирует уникальные трассы, исполняемые процессором, и отслеживает входные данные, находящиеся в оперативной памяти или видеопамяти. При выявлении уникальных трасс фиксируется прирост покрытия. Дополнительным источником сведений о приросте покрытия выступают данные в памяти, которые также отслеживаются в части их уникальной модификации.

Разработанный метод состоит из следующих шагов:

1. В виртуальной машине под управлением гипервизора запускается фаззинг-тестирование с заранее подготовленными входными корпусами для их дальнейшей мутации.
2. Осуществляется запуск тестируемой программы и передача ей входных данных.
3. Для каждого функционального объекта в рамках одной итерации гипервизор фиксирует трассу.
   3.1. Извлекается состояние процессора из структуры VMCS.
   3.2. Функциональные объекты определяются по инструкциям call и по подготовке регистров к вызову функции вместе с инструкцией безусловного перехода.
   3.3. Фиксируется состояние входных данных, переданных средством фаззинг-тестирования ПО в памяти на предмет их модификации.
4. По окончании одной итерации код гипервизора, функционирующий внутри ОС, создает файл-отчет, содержащий представление пройденных трасс и путей модификации входных данных.
5. Входные данные проходят процесс мутации штатным или доработанным модулем средства фаззинг-тестирования, затем происходит повторная итерация в соответствии с шагом 2. Если цели фаззинг-тестирования по покрытию или времени достигнуты, алгоритм завершается.

6. По окончании фаззинг-тестирования код гипервизора, функционирующий внутри ОС, агрегирует файлы отчетов покрытия, на основе совокупности которых рассчитывается итоговое покрытие для тестируемого ПО.

Состояние процессора во время фаззинг-тестирования извлекается из структуры VMCS, а оперативная память и видеопамять отслеживаются в режиме реального времени с целью мониторинга состояния переданных входных данных. За счет возможности отслеживания состояния процессора и памяти исключается возможность ложного определения или пропуска новой трассы, что, в свою очередь, положительно сказывается на точности оценки покрытия. Для подтверждения работы предложенного метода проведен эксперимент, описанный далее.

6. Проведение экспериментов для оценки покрытия с использованием предложенного метода

В ходе проведения экспериментов точность определения степени покрытия оценивалась относительно статической инструментации с использованием средства фаззинг-тестирования AFL (S1). В качестве тестируемого программного обеспечения выбраны утилиты cURL – используется для передачи данных по ссылке типа URL, iptables – утилита для настройки и ограничения сетевых подключений и vlc – медиаплеер с возможностью запуска проигрывания из командной строки. Кроме статической инструментации AFL, для оценки покрытия в эксперименте использовалась оценка на базе эмулятора QEMU (S2) и инструментация с использованием Gcov (S3). Фаззинг-тестирование проводилось на протяжении 24 часов. Для чистоты эксперимента модулю мутации AFL передана инициирующая входная последовательность, которая обеспечит мутацию одинаковыми методами и алгоритмами для каждого экземпляра средства фаззинг-тестирования.

Результаты эксперимента приведены в табл. 1. Предложенный метод условно отмечен в таблице как S4.

Таблица 1. Результаты эксперимента по оценке покрытия с использованием предложенного метода

Метод оценки покрытия / **Программное обеспечение**	**S1**	**S2**	**S3**	**S4**
cURL	21.8 %	19.9 %	17.6 %	20.2 %
iptables	16.3 %	15.4 %	14.1 %	15.9 %
vlc	7.8 %	2.5 %	6.6 %	8.3 %

В ходе оценки результатов выявлено, что покрытие при фаззинг-тестировании vlc методом S2 значительно ниже покрытия, определенного другими методами. QEMU в режиме оценки покрытия не имеет графического интерфейса, и при попытке открытия vlc для воспроизведения работа плеера завершалась с ошибкой, свидетельствующей о том, что в ходе работы не удалось создать окно.

Предложенный метод показал наиболее близкую к референсному значению, представленному методом S1, оценку покрытия.

7. Заключение

Технология аппаратной виртуализации предоставляет широкие возможности по контролю состояния виртуальной машины. При этом исполняемый код, функционирующий внутри виртуальной машины, исполняется, как если бы он исполнялся на физическом оборудовании. Это позволяет исключить потенциально нестабильное поведение тестируемого программного обеспечения, что в конечном счете обеспечивает чистоту результатов работы средства фаззинг-тестирования и оценки покрытия при проведении тестирования методом черного ящика.

Разработанный метод в ходе эксперимента показал удовлетворительные результаты, приближенные к результатам, полученным при статической инструментации исходных текстов, что свидетельствует о его применимости для фаззинг-тестирования методом черного ящика.

Полученные результаты позволяют продолжить исследования в области методов на основе аппаратной виртуализации для фаззинг-тестирования. За счет возможности взаимодействия с виртуальной машиной и отслеживания ее состояния становится возможным создание универсального монитора процесса фаззинг-тестирования, который не только фиксирует состояние данных и процессора, но и позволяет восстанавливать спецификацию программы.

Дальнейшие исследования должны быть направлены на анализ методов фаззинг-тестирования программного обеспечения, которое требует взаимодействия с различными аппаратными компонентами.

Литература

1. *Ерышов В. Г.* Фаззинг-тестирование. Классификация современных средств фаззинга // Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие»: Международные научные конференции, Санкт-Петербург, 26–31 августа 2021 года. С. 287–289. DOI 10.37539/AUG298.2021.94.77.007.
2. *Zhang C., Chen J.* Fuzzing Methods Recommendation Based on Feature Vectors // Proc. 36th IEEE/ACM International Conference on Automated Software Engineering, 2021. P. 1079–1081. DOI 10.1109/ASE51524.2021.9678630.
3. *Eisele M., Maugeri M., Shriwas R. et al.* Embedded fuzzing: a review of challenges, tools, and solutions // Cybersecurity. 2022. V. 5, № 1. P. 1–18. DOI 10.1186/s42400-022-00123-y.
4. *Kim S., Cho Ja., Lee Ch., Shon T.* Smart seed selection-based effective black box fuzzing for IIoT protocol // The Journal of Supercomputing. 2020. V. 76, № 12. P. 10140–10154. DOI 10.1007/s11227-020-03245-7.
5. *Silakov D. V.* The use of hardware virtualization in the context of information security // Programming and Computer Software. 2012. V. 38, № 5. P. 276–280. DOI 10.1134/S0361768812050064.
6. *Epishkina A. V., Kanner A. M., Kanner T. M.* Comprehensive Testing of Software and Hardware Data Security Tools Using Virtualization // Mechanisms and Machine Science (book series). 2020. V. 80. P. 79–87. DOI 10.1007/978-3-030-33491-8_9.
7. *Куликов С. С., Клименков Е. И.* Миграция и виртуализация как технологии обеспечения совместимости аппаратных и программных средств в образовательном процессе // Информатизация образования. 2010. № 1 (58). С. 82–94.
8. *Борисенко Б. Б., Килюшева Е. Д.* Обнаружение гипервизора, использующего технологию аппаратной виртуализации // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 76–84.

9. *Егоров В. Ю., Карпов И. В., Матвеев Е. А.* Методика управления оперативной памятью в технологиях аппаратной виртуализации VT и SVM // Наукоемкие технологии. 2010. Т. 11, № 4. С. 35–45.
10. *Du J., Zwaenepoel W., Sehrawat N.* Performance profiling in a virtualized environment // Proc. 2nd USENIX Workshop on Hot Topics in Cloud Computing, 2010, Boston, MA.
11. *Юлюгин Е. А.* Корректное и быстрое исполнение отдельных инструкций архитектуры Intel® 64 в виртуальном окружении // Информационные технологии. 2019. Т. 25, № 3. С. 157–164. DOI 10.17587/it.25.157-164.
12. Intel software development manual [Электронный ресурс]. URL: `https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html` (дата обращения: 01.12.2023).
13. AMD documentation hub [Электронный ресурс]. URL: `https://www.amd.com/en/search/documentation/hub.html` (дата обращения: 01.12.2023).
14. *Радаев В. А.* Методика тестирования приложений на основе анализа покрытия исходного кода и фаззинга // Материалы Межвузовской научно-технической конференции студентов, аспирантов и молодых специалистов им. Е. В. Арменского, Москва, 25 февраля – 04 марта 2020 года. С. 165.
15. *Воронина Е. Н.* Сравнительный анализ подходов к поиску уязвимостей программного обеспечения методом фаззинг-тестирования //Сборник трудов Десятой международной научно-технической конференции «Безопасные информационные технологии», Москва, 03–04 декабря 2019 года. С. 75–80.
16. *Вишняков А. В.* Поиск ошибок в бинарном коде методами динамической символьной интерпретации: специальность 23.50.00: диссертация на соискание ученой степени кандидата физико-математических наук, 2022. 131 с.
17. *Созин М. В.* Фаззинг на основании состояния исполнения программы // Материалы VIII Всероссийской молодежной школы-семинара по проблемам информационной безопасности «Перспектива», Таганрог, 10–13 октября 2019 года. С. 12–17.
18. *Валеев Д. Р., Котенко И. В.* Анализ подходов к автоматической обработке результатов фаззинг-тестирования // Сборник научных статей XII Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО). Санкт-Петербург, 28 февраля – 01 марта 2023 года. Т. 1. С. 219–224.
19. *Попов В. И., Тюрин М. Е., Семибратов А. С.* Анализ современных инструментальных средств, реализующих фаззинг-тестирование // Сборник трудов II Всероссийской научно-технической конференции «Состояние и перспективы развития современной науки по направлению «ИТ-технологии»», Анапа, 23–24 марта 2023 года. Т. 2. С. 83–94.

Самарин Николай Николаевич

к.т.н., ФГУП «Научно-исследовательский институт «Квант»» (125438, Москва, 4-й Лихачёвский переулок, 15), e-mail: `samarin_nik@mail.ru`, ORCID: 0009-0007-4911-8471, AuthorID: 1100538, SPIN-код: 2176-0939.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Development of the Method for Assessing Code Coverage During Black-Box Fuzz-Testing of Software Using Hardware Virtualization to Evaluate Test Coverage

Nikolay N. Samarin

Scientific Research Institute "Kvant" (Moscow)

Abstract: This article presents a developed method for assessing code coverage during fuzz-testing of software using hardware virtualization. The tested software is considered as a black box. The proposed method's feature is the ability to monitor the state of the virtual machine in which the fuzz testing is carried out, including monitoring the processor's state and input data in real-time. The experiments conducted showed that the developed method allows us to obtain an accurate assessment of code test coverage comparable to the static instrumentation-based method, which is only applicable when conducting white-box fuzz testing.

Keywords: information security, testing, hardware virtualization, coverage assessment, black-box fuzzing.

For citation: Samarin N. N. Development of the method for assessing code coverage during black-box fuzz-testing of software using hardware virtualization to evaluate test coverage (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 69-78. https://doi.org/10.55648/1998-6920-2024-18-2-69-78.

The article was submitted: 10.11.2023;
accepted for publication 13.02.2024.

References

1. Yeryshov V. G. Fazzing testirovaniye. Klassifikatsiya sovremennykh sredstv fazzinga. *Sbornik izbrannykh statey po materialam nauchnykh konferentsiy GNII "Natsrazvitiye»: Mezhdunarodnyye nauchnyye konferentsii*, Sankt-Peterburg, 26-31 August, 2021, pp 287-289. DOI 10.37539/AUG298.2021.94.77.007.
2. Zhang C., Chen J. Fuzzing Methods Recommendation Based on Feature Vectors. *Proceedings - 2021 36th IEEE/ACM International Conference on Automated Software Engineering*, 15-19 November, 2021 pp. 1079-1081. DOI 10.1109/ASE51524.2021.9678630. EDN BXHZDT.
3. Eisele M., Maugeri M., Shriwas R., et al. Embedded fuzzing: a review of challenges, tools, and solutions. *Cybersecurity*, 2022. vol. 5, no. 1, pp 1-18. DOI 10.1186/s42400-022-00123-y. EDN JCXYPZ.
4. Kim S., Cho Ja., Lee Ch., Shon T. Smart seed selection-based effective black box fuzzing for IIoT protocol. *The Journal of Supercomputing*, 2020, vol. 76, no. 12, pp. 10140-10154. DOI 10.1007/s11227-020-03245-7. EDN KYWZAP.
5. Silakov D. V. The use of hardware virtualization in the context of information security. *Programming and Computer Software*, 2012, vol. 38, no. 5, pp. 276-280. DOI 10.1134/S0361768812050064. EDN RGNETF.
6. Epishkina A. V., Kanner A. M., Kanner T. M. Comprehensive Testing of Software and Hardware Data Security Tools Using Virtualization. *Mechanisms and Machine Science (book series)*, 2020, vol. 80, pp. 79-87. DOI 10.1007/978-3-030-33491-8_9. EDN EIFAXP.
7. Kulikov S. S., Klimenkov Ye. I. Migratsiya i virtualizatsiya kak tekhnologii obespecheniya sovmestimosti apparatnykh i programmnykh sredstv v obrazovatel'nom protsesse [Migration and virtualization as technologies for ensuring compatibility of hardware and software in the educational process]. *Informatizatsiya obrazovaniya*, 2010, no. 1(58), pp. 82-94. EDN XMRDYT.
8. Borisenko B. B., Kilyusheva Ye. D. Obnaruzheniye gipervizora, ispol'zuyushchego tekhnologiyu apparatnoy virtualizatsii [Detecting a hypervisor that uses hardware virtualization technology *Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy*, 2014, no. 4, pp. 76-84. EDN TJZKKV.
9. Yegorov V. YU., Karpov I. V., Matveyev Ye. A. Metodika upravleniya operativnoy pamyat'yu v tekhnologiyakh apparatnoy virtualizatsii VT i SVM [Methodology for managing RAM in VT and SVM

hardware virtualization technologies]. *Naukoyemkiye tekhnologii*, 2010, vol. 11, no. 4, pp. 035-045. EDN QCTKPH.
10. Du J., Zwaenepoel W., Sehrawat N. Performance profiling in a virtualized environment []. *2nd USENIX Workshop on Hot Topics in Cloud Computing, HotCloud 2010: 2*, Boston, MA, 22 June, 2010. EDN NZEKCW.
11. Yulyugin Ye. A. Korrektnoye i bystroye ispolneniye otdel'nykh instruktsiy arkhitektury Intel® 64 v virtual'nom okruzhenii / Ye. A. Yulyugin [Correct and fast execution of individual Intel® 64 architecture instructions in a virtual environment]. *Informatsionnyye tekhnologii*, 2019, vol. 25, no. 3, pp. 157-164. DOI 10.17587/it.25.157-164. EDN VWTPFI.
12. *Intel software development manual*, available at: `https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html` (accessed 01.12.2023).
13. *AMD documentation hub*, available at: `https://www.amd.com/en/search/documentation/hub.html` (accessed 01.12.2023).
14. Radayev V. A. Metodika testirovaniya prilozheniy na osnove analiza pokrytiya iskhodnogo koda i fazzinga [Methodology for testing applications based on source code coverage analysis and fuzzing]. *Mezhvuzovskaya nauchno-tekhnicheskaya konferentsiya studentov, aspirantov i molodykh spetsialistov im. Ye.V. Armenskogo*, Moscow, 25 Febrary, 2020, p. 165. EDN ZQSZQP.
15. Voronina Ye. N. Sravnitel'nyy analiz podkhodov k poisku uyazvimostey programmnogo obespecheniya metodom fazzing-testirovaniya [Comparative analysis of approaches to searching for software vulnerabilities using fuzzing testing]. *Bezopasnyye informatsionnyye tekhnologii: Sbornik trudov Desyatoy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii*, Moscow, 03–04 December, 2019. pp. 75-80. EDN DXEHYH.
16. Vishnyakov A. V. Poisk oshibok v binarnom kode metodami dinamicheskoy simvol'noy interpretatsii: spetsial'nost' [Comparative analysis of approaches to searching for software vulnerabilities using fuzzing testing]. Abstract of Ph. D. thesis., 2022, p.131. EDN MRBRIF.
17. Sozin M. V. Fazzing na osnovanii sostoyaniya ispolneniya programmy [Fuzzing based on program execution state]. *Perspektiva-2019: Materialy VIII Vserossiyskoy molodezhnoy shkoly-seminara po problemam informatsionnoy bezopasnosti*, Taganrog, 10-13 October, 2019, pp. 12-17. EDN HVJPAW.
18. Valeyev D. R., Kotenko I. V. Analiz podkhodov k avtomaticheskoy obrabotke rezul'tatov fazzing-testirovaniya [Analysis of approaches to automatic processing of fuzzing testing results]. *Aktual'nyye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2023): Sbornik nauchnykh statey. XII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya*, Sankt-Peterburg, 28 Fevrary, 2023, vol. 1. pp. 219-224. EDN HOECIC.
19. Popov V. I., Tyurin M. Ye., Semibratov A. S. Analiz sovremennykh instrumental'nykh sredstv, realizuyushchikh fazzing-testirovaniye [Analysis of modern tools that implement fuzzing testing]. *Sostoyaniye i perspektivy razvitiya sovremennoy nauki po napravleniyu IT-tekhnologii: Sbornik trudov II Vserossiyskoy nauchno-tekhnicheskoy konferentsii*, Anapa, 23-24 March, 2023, vol. 2. pp. 83-94. EDN DZVUMH.

Nikolay N. Samarin

Cand. of Sci. (Engineering), Scientific Research Institute "Kvant" (125438, Moscow, 4th Likhachevsky per. 15), e-mail: `samarin_nik@mail.ru`, ORCID: 0009-0007-4911-8471, AuthorID: 1100538, SPIN code: 2176-0939.

Research interests: information security, information protection, software analysis for undocumented capabilities, fuzzing testing, security assessments of automated systems.

DOI: 10.55648/1998-6920-2024-18-2-79-87 УДК 123.456.789

Сравнение способов построения лазерных излучателей в импульсных полупроводниковых дальномерах

А. Ф. Уляшин, А. А. Величко, А. Н. Галянтич

Новосибирский государственный технический университет (НГТУ)

Аннотация: В работе проводится сравнение различных способов построения лазерных излучателей в импульсных полупроводниковых дальномерах. Рассмотрены два полупроводниковых лазерных излучателя с длиной волны 905 нм, входящих в состав импульсного дальномера. Оптическая схема передающего и приемного каналов дальномера состоит из асферической линзы и объектива. Отличие между лазерными излучателями заключается в наличии в одном из них встроенной цилиндрической линзы. Продемонстрированы результаты измерения расстояния до цели дальномером с обоими вариантами построения излучателей в различных условиях.

Ключевые слова: импульсный полупроводниковый дальномер, лазерный излучатель, цилиндрическая линза, фокус, длина волны, поле зрения, дальность, угол охвата.

Для цитирования: Уляшин А. Ф., Величко А. А., Галянтич А. Н. Сравнение способов построения лазерных излучателей в импульсных полупроводниковых дальномерах // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 79–87. https://doi.org/10.55648/1998-6920-2024-18-2-79-87.

Статья поступила в редакцию 31.05.2023;
принята к публикации 25.12.2023.

1. Введение

В дальнометрии очень важны такие параметры, как габариты и масса передающего канала дальномера [1]. Производители стремятся к снижению данных показателей, и этого возможно достичь благодаря использованию в дальномерах полупроводниковых излучателей (рис. 1). Также данный тип излучателей обладает высоким КПД [2], высокой стойкостью к механическим и климатическим нагрузкам, длительным сроком службы, низкой стоимостью и простотой контроля параметров излучения – к ним относятся частота, скважность и мощность [3].

Рис. 1. Полупроводниковый излучатель

Устройство оптической системы дальномера приведено на рис. 2. Основными составными частями являются источник излучения, линза и объектив [4].

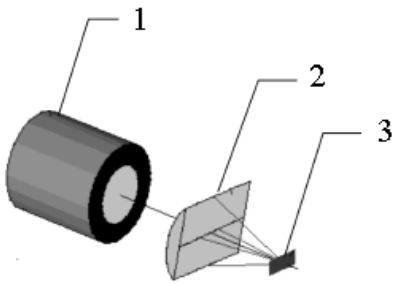


Рис. 2. Оптическая система дальномера: 1 – объектив, 2 – линза,
3 – источник излучения

Оптимизация оптической системы для лазерного импульсного дальномера (рис. 3) включает в себя формирование необходимой индикатрисы излучения с минимальными габаритами системы [5] и как можно меньшим количеством оптических элементов. В работе приведены результаты определения основных параметров дальномера с использованием излучателя с цилиндрической линзой и без нее. Также определено нахождение положения излучателя относительно объектива, при котором на выходе системы достигается требуемая расходимость излучения и энергетические потери сведены к минимуму.

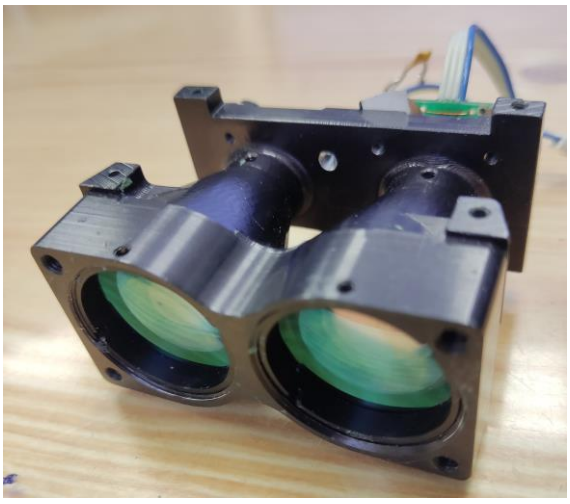


Рис. 3. Импульсный полупроводниковый дальномер

Вид объектива импульсного полупроводникового дальномера в разрезе показан на рис. 4.

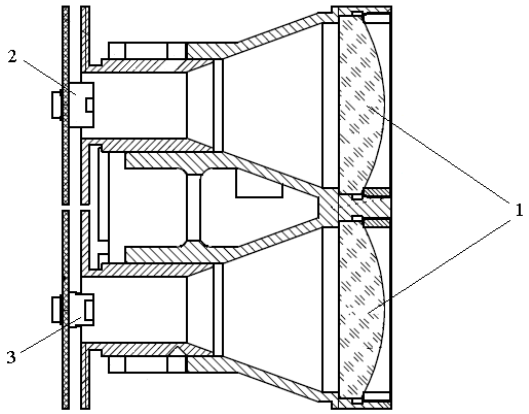


Рис. 4. Вид объектива дальномера в разрезе: 1 – асферическая линза,
2 – излучатель, 3 – фотоприемное устройство

Модель формирующей системы, состоящая из объектива с асферической линзой и излучателя без встроенной цилиндрической линзы, имеет неоднородное пятно подсвета [6]. Если сделать расфокусировку объектива [7], можно гомогенизировать пятно подсвета, но в то же время происходит значительное увеличение размера пятна и энергетических потерь.

Необходимо достичь гомогенности пятна подсвета в пределах допустимых габаритов системы и минимизации энергетических потерь [8]. После прохождения цилиндрической линзы излучение лазерного диода имеет одинаковую расходимость в сагиттальном и меридиональном сечениях [9], а сопряженный объектив формирует необходимую расходимость передающего канала дальномера. Цилиндрическая линза в плоскости с малой расходимостью (меридиональное сечение) представляет собой плоскопараллельную пластину [10].

Задача работы состоит в исследовании и сравнении оптических систем импульсного лазерного дальномера: простой системы с объективом и системы с использованием цилиндрической линзы. Также необходимо определить фокусное расстояние от источника излучения до асферической линзы, обеспечивающее наиболее высокий уровень освещенности. Получены значения основных параметров импульсного дальномера на обеих системах и приведены графики данных параметров. К параметрам относятся: размер пятна на цели по уровню 0.2 метра по горизонтали и вертикали, размер пятна на цели по уровню 0.5 метра по горизонтали и вертикали, угол охвата, процент использования излучения лазера и максимальная освещенность в пятне рассеяния.

2. Моделирование оптической системы

Расчет всех параметров произведен в программе Zemax [11] с использованием фирменного файла с данными индикатрисы излучения лазера. Расчет производился для дальности 2.5 км. В качестве коллимирующих объективов использовались объективы с фокусными расстояниями в интервале от 20 до 160 мм. Световой диаметр всех объективов одинаковый – 25 мм. Все объективы имеют дифракционное качество изображения.

Моделирование в программе Zemax показало существенное отличие в размерах пятна на цели по уровню 0.2 метра по вертикали между дальномерными системами (рис. 5).

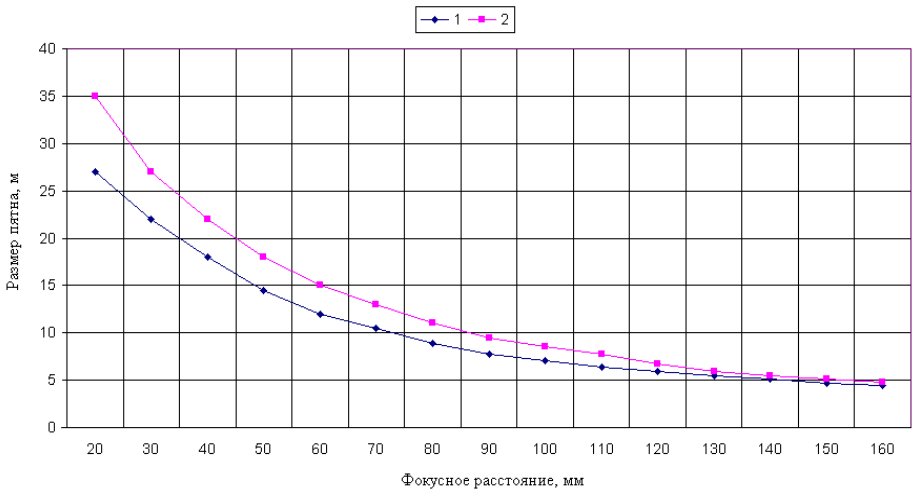


Рис. 5. Размер пятна на цели по уровню 0.2 метра по вертикали:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Размер пятна на цели по горизонтали также имеет расхождение между дальномерными системами (рис. 6).

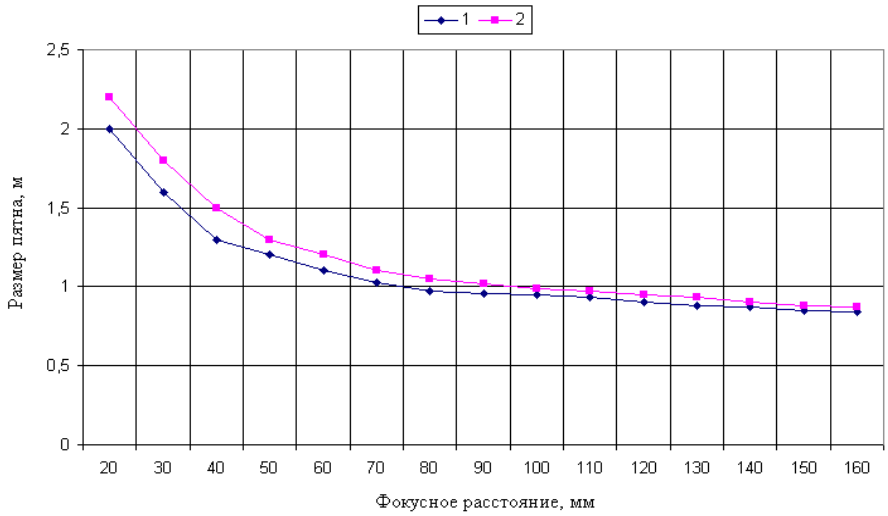


Рис. 6. Размер пятна на цели по уровню 0.2 метра по горизонтали:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Как видно из графиков, представленных на рис. 5 и 6, с увеличением фокусного расстояния от источника излучения до асферической линзы существенно уменьшается размер пятна на цели. В диапазоне от 20 до 160 мм фокусного расстояния средний размер пятна на цели по вертикали составил 12.98 метра для системы с цилиндрической линзой и 10.65 метра для системы без цилиндрической линзы, что означает прирост на 21 %.

Средний размер пятна на цели по горизонтали в диапазоне от 20 до 160 мм фокусного расстояния составил 1.17 метра для системы с цилиндрической линзой и 1.09 метра без цилиндрической линзы, что означает прирост на 7 %.

Моделирование в программе Zemax показало существенное отличие в размерах пятна на цели по уровню 0.5 метра по вертикали между дальномерными системами (рис. 7). В диапазоне от 20 до 160 мм фокусного расстояния средний размер пятна на цели по вертикали составил 8.72 метра для системы с цилиндрической линзой и 7.35 метра для системы без цилиндрической линзы, что означает прирост на 18 %.

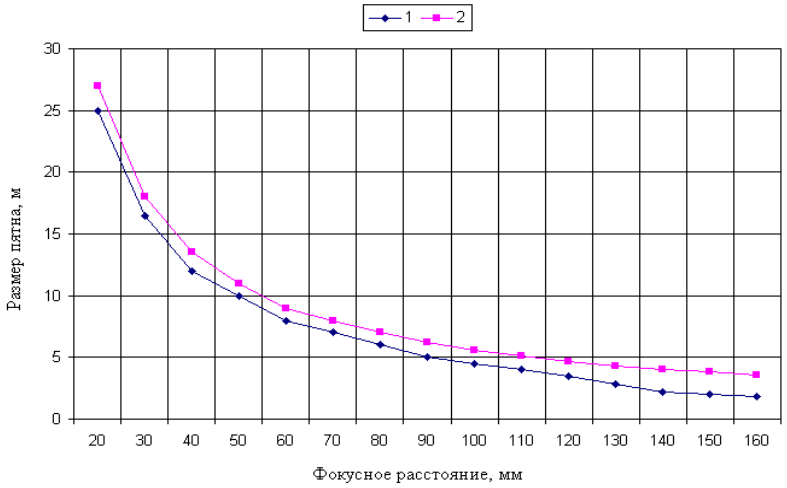


Рис. 7. Размер пятна на цели по уровню 0.5 метра по вертикали:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Размер пятна на цели по горизонтали также имеет расхождение между дальномерными системами (рис. 8).

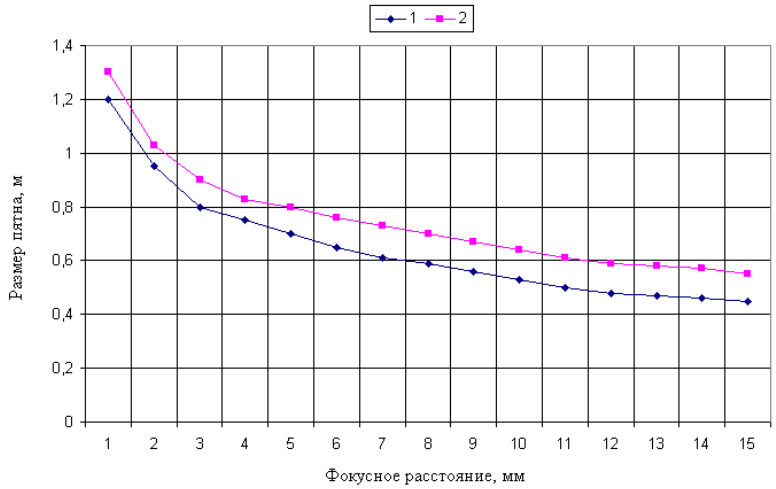


Рис. 8. Размер пятна на цели по уровню 0.5 метра по вертикали:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Средний размер пятна на цели по горизонтали в диапазоне от 20 до 160 мм фокусного расстояния составил 0.75 метра для системы с цилиндрической линзой и 0.64 метра – без цилиндрической линзы, что означает прирост на 17 %.

Также немаловажным показателем является процент использования излучения лазера дальномером. На рис. 9 приведен результат моделирования двух систем.

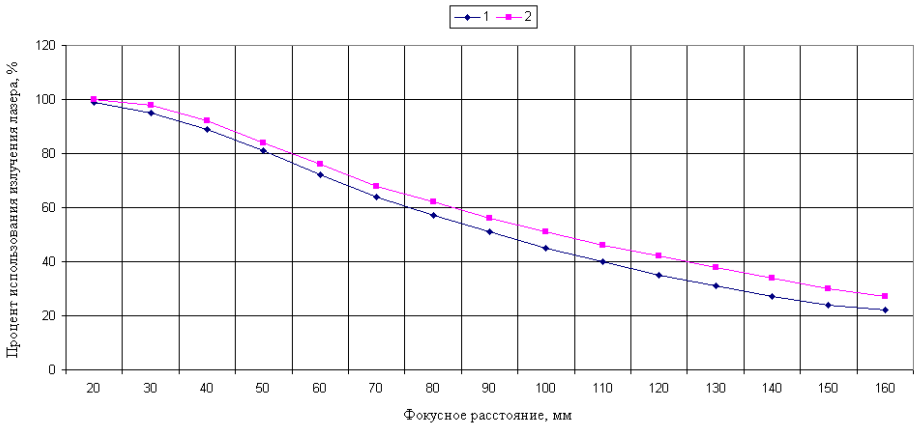


Рис. 9. Процент использования излучения лазера:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Средний процент использования излучения лазера в диапазоне от 20 до 160 мм фокусного расстояния составил 60.26 % для системы с цилиндрической линзой и 55.4 % – без цилиндрической линзы, что означает прирост на 8.7 %.

Основной характеристикой дальномерной системы является максимальная освещенность в пятне рассеяния. В диапазоне от 20 до 160 мм фокусного расстояния величина этого параметра составила 115.14 Вт/см^2 *10^{-5} для системы с цилиндрической линзой, 72.13 Вт/см^2 *10^{-5} – без цилиндрической линзы, что означает прирост на 59 % (рис. 10).

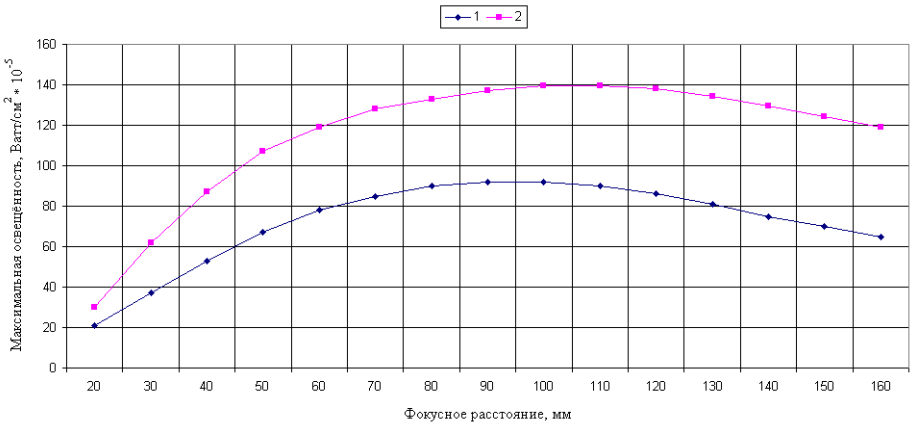


Рис. 10. Максимальная освещённость в пятне рассеяния:
1 – дальномер с излучателем без цилиндрической линзы,
2 – дальномер с излучателем со встроенной цилиндрической линзой

Выявлено, что максимальная освещённость в системе без цилиндрической линзы достигается в диапазоне от 80 до 110 мм и составляет 92 Вт/см^2 *10^{-5}. Для системы с использованием цилиндрической линзы максимальная освещённость достигается в диапазоне от 100 до 120 мм фокусного расстояния и составляет 139.7 Вт/см^2 *10^{-5}.

3. Результаты работы

В работе проведено исследование и сравнение оптических систем импульсного лазерного дальномера: простой системы с объективом и системы с использованием цилиндрической линзы в конкретных условиях. Определено фокусное расстояние от источника излучения до асферической линзы, обеспечивающее наиболее высокий уровень освещенности. Получены значения основных параметров импульсного дальномера на обеих системах и приведены

графики данных параметров. К параметрам относятся: размер пятна на цели по уровню 0.2 метра по горизонтали и вертикали, размер пятна на цели по уровню 0.5 метра по горизонтали и вертикали, процент использования излучения лазера и максимальная освещенность в пятне рассеяния. Основной целью работы была демонстрация различий между обычным вариантом исполнения оптической системы излучателя и вариантом интеграции цилиндрической линзы в оптическую систему. Как показало исследование, при фокусном расстоянии от 20 до 160 мм размер пятна на цели по уровню 0.2 метра на излучателе с цилиндрической линзой возрос на 21 % в вертикальном направлении и на 7 % в горизонтальном направлении. Размер пятна на цели по уровню 0.5 метра возрос на 18 % в вертикальном направлении и на 17 % в горизонтальном направлении. Процент использования излучения лазера дальномером возрос на 8.7 %, а максимальная освещенность в пятне рассеяния увеличилась на 59 %. Это свидетельствует о том, что использование цилиндрической линзы оправдано и она может быть применена как часть оптической системы излучательного канала дальномера для достижения б*о*льших дальностей измерения, что очень важно для такой отрасли, как военное дело.

Литература

1. *Аснис Л. А., Васильев В. П., Волканский В. Б.* Лазерная дальнометрия. М.: Радио и связь, 1995. 256 с.
2. *Барышников Н. В., Бокшанский В. Б., Карасик В. Е.* Приемопередающие устройства лазерных локационных изображающих систем. М.: Изд-во МГТУ им. Н. Э. Баумана, 2004. 84 с.
3. *Бокшанский В. Б., Бондаренко Д. А., Вязовых М. В., Животовский И. В., Сахаров А. А., Семенков В. П.* Лазерные приборы и методы измерения дальности: учебное пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2012. 92 с.
4. *Берников Б. О, Бокшанский В. Б., Вязовых М. В., Федоров С. В.* Методы повышения точности измерения дальности в лазерных фазовых дальномерах // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение», 2012.
5. *Белов И. Ю.* Физические основы оптической дальнометрии: учебно-методическое пособие. Казань: КГУ, 2009. 72 с.
6. *Попов Л. Н., Фролкин В. Т.* Импульсные устройства: учебник для вузов. М.: Советское радио, 1980. 547 с.
7. *Грицевский П. М., Мамченко А. Е., Степенский Б. М.* Основы автоматики, импульсной и вычислительной техники: учебник для техникумов. М.: Радио и связь, 1987. 632 с.
8. *Якубовский С. В.* Аналоговые и цифровые интегральные схемы: справочник. М.: Советское радио, 2008. 336 с.
9. *Голубев А. Н.* Приборы и методы электронной дальнометрии и тахеометрии. М.: «Недра», 1991. 249 с.
10. *Poujouly S., Journet B.* A twofold modulation frequency laser range finder // Journal of optics A: Pure and Applied Optics. 2002. P. 356–363.
11. *Geary J. M.* Introduction to lens design with practical Zemax examples, 2002. 462 p.

Уляшин Александр Федорович
аспирант кафедры полупроводниковых приборов и микроэлектроники, Новосибирский государственный технический университет, e-mail: ulyashin_2018@mail.ru, ORCID ID: 0000-0003-4555-2813.

Величко Александр Андреевич
д.т.н., профессор кафедры полупроводниковых приборов и микроэлектроники, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр-т. К. Маркса, д.20), e-mail: vel6049@mail.ru, ORCID ID: 0000-0002-7304-2813.

Галянтич Алексей Николаевич
аспирант кафедры теоретических основ радиотехники, Новосибирский государственный технический университет, e-mail: ag_nsk@mail.ru, ORCID ID: 0009-0008-6894-0652.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Study of Methods for Measuring Distances in Scanning Range

Alexander F. Ulyashin, Alexander A. Velichko, Alexei N. Gallantich

Novosibirsk State Technical University (NSTU)

Abstract: The paper compares various methods for constructing laser emitters in pulsed semiconductor rangefinders. Two semiconductor laser emitters with a wavelength of 905 nm, which are part of a pulsed range finder, are considered. The optical scheme of the transmitting and receiving channels of the range finder consists of an aspherical lens and an objective. The difference between laser emitters is the presence of a built-in cylindrical lens in one of them. The results of measuring the distance to the target by a rangefinder with both options for constructing emitters under various conditions are demonstrated.

Keywords: pulse semiconductor rangefinder, laser emitter, cylindrical lens, focus, wavelength, field of view, range, coverage angle.

For citation: Ulyashin A. F., Velicko A. A., Gallantich A. N. Study of methods for measuring distances in scanning range (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 79-87. https://doi.org/10.55648/1998-6920-2024-18-2-79-87.

The article was submitted: 31.05.2023;
accepted for publication 25.12.2023.

References

1. Asnis L. A., Vasil'ev V. P., Volkanskii, V. B. Lazernaya dal'nometriya [*Laser rangefinder*]. Moscow, Radio i svyaz', 1995, 256 p.
2. Baryshnikov N. V., Bokshanskii V. B., Karasik V. E. *Priemoperedayushchie ustroi-stva lazernykh lokatsionnykh izobrazhayushchikh sistem* [Transceiver devices of laser location imaging systems]. Moscow, publishing house of Bauman Moscow state technical University, 2004, 84 p.
3. Bokshanskii V. B., Bondarenko D. A., Vyazovykh M. V., Zhivotovskii I. V., Sakharov A. A., Semenkov V. P. *Lazernye pribory i metody izmereniya dal'nosti* [Laser devic,es and methods for measuring range]. Moscow, Publishing house of Bauman Moscow state technical University, 2012, 92 p.
4. Bernikov B. O, Bokshansky V. B., Vyazovykh M. V., Fedorov S. V. *Metody povysheniya tochnosti izmereniya dal'nosti v lazernykh fazovykh dal'nomerakh* [Methods for improving the accuracy of distance measurement in laser phase range finders]. Bulletin of Bauman Moscow state technical University. "Instrument engineering", 2012.
5. Belov I. Yu. *Fizicheskie osnovy opticheskoi dal'nometrii* [Physical bases of optical rangefinder], Kazan, 2009, 72 p.
6. Popov L. N., Frolkin V. T. Impul'snye ustroistva [Pulsed devices]. 3rd ed., Moscow, Sovetskoe radio, 1980. 547 p.
7. Gritsevsky P. M., Mamchenko A. E., Gradovsky B. M. *Osnovy avtomatiki* [Fundamentals of automation, pulse and computer technology]. Moscow, Radio and communications, 1987, 632 p.
8. Yakubovsky S. V. *Analogovye i tsifrovye integral'nye skhemy: spravochnik* [Analog and digital integrated circuits: Handbook]. Moscow, Sov. Radio, 2008. 336 p.
9. Golubev A. N. *Pribory i metody elektronnoi dal'nometrii i takheometrii* [Devices and methods of electronic rangefinder and tacheometry]. Moscow, "Nedra", 1991, 249 p.
10. Poujouly S., Journet B. A twofold modulation frequency laser range finder. *Journal of Optics A: Pure and Applied Optics*, 2002. pp. 356-363.
11. Joseph M. Geary. *Introduction to lens design with practical Zemax examples*, 2002, 462 p.

Alexander F. Ulyashin

postgraduate student of the Department of semiconductor devices and microelectronics, Novosibirsk State Technical University (NSTU, Russia, 630073, Novosibirsk, 20 Karl Marks Avenue), e-mail: ulyashin_2018@mail.ru, ORCID ID: 0000-0003-4555-2813.

Alexander A. Velichko

Dr. of Sci. (Engineering), professor of the Department of semiconductor devices and microelectronics, Novosibirsk State Technical University (NSTU, Russia, 630073, Novosibirsk, 20 Karl Marks Avenue), e-mail: vel6049@mail.ru, ORCID ID: 0000-0002-7304-2813.

Alexei N. Gallantich

postgraduate student of the Department of theoretical fundamentals of radio engineering, Novosibirsk State Technical University (NSTU, Russia, 630073, Novosibirsk, 20 Karl Marks Avenue), e-mail: ag_nsk@mail.ru, ORCID ID: 0009-0008-6894-0652.

DOI: 10.55648/1998-6920-2024-18-2-88-102 УДК 004.056

Оценка уровня доверия к процессу управления инцидентами информационной безопасности

А. В. Иванов, И. А. Огнев, И. В. Никрошкин, М. А. Киселев

Новосибирский государственный технический университет (НГТУ)

Аннотация: Существующие методики оценки уровня доверия к процессу управления инцидентами информационной безопасности и к процессам систем мониторинга событий информационной безопасности крайне ограничены. Данные методики основаны на экспертной оценке и носят периодический характер с большим промежутком времени между оценками. Целью данного исследования является разработка методики оценки уровня доверия к процессу управления инцидентами информационной безопасности, которая позволит проводить оценку в автоматизированном режиме с минимальным участием экспертов. В результате была разработана методика оценки уровня доверия к процессу управления инцидентами информационной безопасности, которая включает в себя перечень критериев доверия и метрик для их оценки, в её основе лежит методика SOMM и ГОСТ ISO/IEC 27035. Разработанная методика основана на трехэтапной оценке показателей доверия: оценка метрик доверия, оценка критериев доверия, оценка уровня доверия к процессу управления инцидентами информационной безопасности. Сформирован математический аппарат расчета числовых значений метрик доверия, критериев доверия и общего уровня доверия к процессу управления инцидентами информационной безопасности. Разработанная методика может быть включена в общую методику оценки уровня доверия к процессам информационной безопасности, входящим в состав процесса мониторинга событий информационной безопасности.

Ключевые слова: инциденты информационной безопасности, управление инцидентами, оценка процессов, уровень доверия, доверие, информационная безопасность, мониторинг информационной безопасности, кибербезопасность.

Для цитирования: Иванов А. В., Огнев И. А., Никрошкин И. В., Киселев М. А. Оценка уровня доверия к процессу управления инцидентами информационной безопасности // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 88–102. https://doi.org/10.55648/1998-6920-2024-18-2-88-102.

Статья поступила в редакцию 09.02.2024;
принята к публикации 29.02.2024.

1. Введение

Переход к более высокому уровню развития компании осуществляется путем улучшения ее показателей при положительной динамике ключевых характеристик [1–6]. Это делает организацию более конкурентоспособной, позволяет динамично реагировать на требования рынка и оптимально использовать свои внутренние ресурсы. Существуют определенные подходы к оценке каждого уровня развития компании: например, модели, описывающие этапы развития, известные как модели уровней зрелости.

В области информационной безопасности (ИБ) использование моделей зрелости может помочь выделить организации, в которых информационная безопасность полностью интегрирована в бизнес-процессы, из тех, где она выполняет в основном вспомогательную функцию: соответствие стандартам для закрытия основных требований ИБ [7–10]. Это, в свою очередь, демонстрирует уровень доверия к организации с точки зрения контрагентов. Поэтому в данном исследовании оценку уровня доверия к процессу управления инцидентами информационной безопасности будем приравнивать к оценке уровня зрелости процесса управления инцидентами информационной безопасности.

Одна из ключевых причин использования моделей зрелости в данном контексте заключается в том, что внедрение улучшений по всей организации требует значительного времени. В области кибербезопасности модель зрелости предоставляет руководству средство оценки прогресса в обеспечении безопасности в повседневных и стратегических задачах. Эта модель служит инструментом для оценки эффективности интеграции бизнес-процессов в организации, позволяя руководству установить долгосрочные цели и эффективно отслеживать прогресс. Применение моделей зрелости также помогает компаниям выявлять свои сильные и слабые стороны.

Подобно моделям зрелости, где компании оценивают свой уровень зрелости в определенных областях, оценка доверия [11] к управлению инцидентами позволяет определить, насколько организация доверяет своим контрагентам в вопросах управления инцидентами информационной безопасности и в сфере информационной безопасности в целом. Этот подход помогает выявить сильные стороны, а также слабые места в управлении инцидентами, что, в свою очередь, способствует разработке и реализации улучшений для повышения эффективности и надежности процесса управления инцидентами информационной безопасности.

2. Постановка задачи исследования

Существующее количество методик для оценки зрелости процессов управления инцидентами в области информационной безопасности крайне ограничено [12–17], и все они являются зарубежными. Одной из самых популярных методик, позволяющих в той или иной степени оценить качество процесса управления инцидентами информационной безопасности, является методика SOMM (Security Operations Maturity Model) [12], разработанная Университетом Карнеги–Меллона (Carnegie Mellon University). Данная методика включает в себя 5 ключевых уровней зрелости от 0 до 5, уровни зрелости данной методики представлены в табл. 1. Оценка управления инцидентами информационной безопасности разбивается на поддиапазоны от недостаточного до экстремального уровня оценки зрелости. Но у данной методики есть несколько недостатков, которые не позволяют полноценно оценить зрелость процесса управления инцидентами информационной безопасности на всех его этапах. Описание каждого уровня не включает в себя набор определенных метрик, позволяющий более точно и правильно оценить ключевые процессы управления инцидентами информационной безопасности. Вторым недостатком данной методики является экспертная оценка, которая больше зависит от человеческого фактора и не представляет возможности объективно оценить процессы управления инцидентами информационной безопасности.

Для решения данной проблемы была продумана и разработана собственная методика оценки уровня доверия (зрелости) к процессам управления инцидентами информационной безопасности, включающая в себя 6 основных критериев и более 30 метрик для проведения качественной и объективной оценки выполнения процессов управления инцидентами информационной безопасности. Выбор 6 основных критериев для методики оценки зрелости процессов управления инцидентами информационной безопасности обоснован стремлением охватить важнейшие аспекты и этапы данного процесса. Каждый из этих критериев представляет ключевой этап в жизненном цикле управления инцидентами, обеспечивая комплексное понимание и оценку эффективности системы безопасности организации. Выбор 34 метрик для

оценки зрелости процессов управления инцидентами информационной безопасности обусловлен необходимостью получения детального и многогранного представления об эффективности каждого из выбранных критериев. Каждая метрика была тщательно отобрана для того, чтобы внести специализированный вклад в измерение конкретных аспектов каждого этапа управления инцидентами. Критерии и метрики процесса управления инцидентами информационной безопасности представлены на рис 1.

Таблица 1. Уровни зрелости по методике SOMM

Уровень SOMM	**Оценка управления инцидентами ИБ**	**Описание**
Уровень 0	Недостаточный	Ключевые составляющие управления инцидентами ИБ (мониторинг, документирование, SLA) отсутствуют.
Уровень 1	Начальный	Управление инцидентами присутствует, но нет документированных процессов.
Уровень 2	Базовый	Выполнение нормативных и бизнес-требований. Большинство процессов управления документированы, но пересматриваются по ситуации.
Уровень 3	Надлежащий	Процессы управления хорошо документированы, регулярно пересматриваются с учетом текущих лучших практик.
Уровень 4	Осмысленный	Эффективность управления инцидентами регулярно оценивается по метрикам производительности. Процессы выстраиваются для достижения KPI бизнеса.
Уровень 5	Экстремальный	По всем направлениям управления инцидентами приняты программы развития. Процессы максимально конкретизированы и отточены.

3. Методика оценки доверия к процессу управления инцидентами информационной безопасности

Предлагаемая методика реализации процесса оценки уровня доверия к процессу управления инцидентами информационной безопасности включает в себя трехэтапную иерархическую оценку показателей доверия:

1. Оценка метрик доверия.
2. Оценка критериев доверия – подпроцессы процесса управления инцидентами информационной безопасности.
3. Оценка уровня доверия к процессу управления инцидентами информационной безопасности.

В качестве критериев будем использовать следующие подпроцессы [18]:

1. Планирование и подготовка.
2. Обнаружение и оповещение.
3. Оценка и принятие решений.
4. Расследование инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Улучшение процесса управления инцидентами ИБ.

Каждый из критериев оценивается по определенной шкале, и на основе совокупности оценок формируется общая картина доверия к процессу управления инцидентами ИБ.

Каждый из этих критериев сопровождается набором конкретных метрик, которые также подвергаются оценке. Этот процесс позволяет получить конечные объективные результаты для каждой метрики и каждого критерия. Таким образом формируется итоговая оценка

доверия к процессу управления инцидентами ИБ на основе совокупности оценок, обеспечивая глубокое понимание эффективности данных процессов в организации.

Опишем кратко все этапы процесса управления инцидентами информационной безопасности для формирования эффективной оценки доверия.

3.1. Планирование и подготовка

Первый этап является началом построения процесса управления инцидентами ИБ и включает в себя формирование основных регламентов и актов, позволяющих в дальнейшим использовать их для построения грамотного процесса управления инцидентами ИБ. В данный подпроцесс входят создание политики управления инцидентами ИБ, создание группы по реагированию на инциденты ИБ, формирование внутреннего и внешнего SLA организаций и др.

3.2. Обнаружение и оповещение

Второй этап управления инцидентами ИБ – обнаружение и оповещение – в рамках управления инцидентами информационной безопасности включает в себя выявление событий ИБ, сбор и обобщение связанной с ними информации, а также создание отчетов о их возникновении и выявленных уязвимостях с применением как ручных, так и автоматических методов.

3.3. Оценка и принятие решений

На данном этапе формируется оценка степени серьезности события/инцидента ИБ после факта его выявления системой мониторинга или каким-либо другим средством экспертизы анализа данных. Также на данном этапе производится актуализация баз данных ИБ для формирования правильной и точной оценки события ИБ.

3.4. Расследование инцидентов ИБ

Четвертый этап является одним из ключевых подпроцессов управления инцидентами ИБ и включает в себя формирование регламента по расследованию инцидентов ИБ, в котором отражаются следующие ключевые шаги:

- распределение обязанностей и ответственности среди специалистов для эффективного проведения расследования;
- формирование версий, объясняющих причины возникновения инцидента;
- приоритизация версий по степени вероятности возникновения инцидента ИБ на основе сформированной базы знаний с этапа «Оценка и принятие решений», а также на базе собственного опыта.

Заканчивается данный этап на создании отчета о проведении расследования и передачи информации группе реагирования на инциденты ИБ.

3.5. Реагирование на инциденты ИБ

Пятый этап управления инцидентами информационной безопасности – реагирование на инциденты ИБ – нацелен на эффективное устранение последствий инцидента и восстановление штатного функционирования информационной системы организации. Данный этап также является ключевым подпроцессом управления инцидентами информационной безопасности. Четвертый и пятый этапы, по сути, являются основными этапами всего процесса управления инцидентами. Исходя из имеющихся данных, эти два этапа являются неразрывными друг для друга, поэтому продуманный и тщательно проанализированный этап расследования приведет к качественным мерам реагирования на инциденты ИБ.

Рис. 1. Зрелость процесса управления инцидентами информационной безопасности

3.6. Улучшение процесса управления инцидентами ИБ

Шестой этап является заключительным в формировании процесса управления инцидентами ИБ. На данном этапе формируются результаты расследования и реагирования на инциденты. С целью усовершенствования процесса управления инцидентами анализируются все

предыдущие шаги и выявляются слабые стороны одного из перечисленных ранее процессов для их дальнейшего усовершенствования.

Итоговый набор всех критериев оценки доверия к процессам управления инцидентами ИБ и их метрикам представлен на рис. 1.

4. Показатели оценки уровня доверия

4.1. Формирование математического аппарата

За основу методики расчета уровня доверия возьмем процедуру оценки соответствия – ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия» [19].

Настоящий стандарт содержит в себе требования к методике и оформлению результатов проведенной проверки в соответствии с ГОСТ Р 57580.1-2017 [20] и предназначен для организаций, осуществляющих оценку соответствия защиты информации (ЗИ) финансовых организаций.

ГОСТ Р 57580.1-2017 определяет пять уровней соответствия ЗИ (табл. 2).

Таблица 2. Уровни соответствия ЗИ по ГОСТ Р 57580.1-2017

Уровень соответствия	**Реализация мер ЗИ**	**Подход к реализации мер ЗИ**	**Контроль и совершенствование системы ЗИ**
Нулевой	Не реализуются / реализуются бессистемно	Нет общего подхода	Отсутствует
Первый	Реализуются бессистемно в незначительном количестве	Нет общего подхода	Отсутствует
Второй	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в единичных случаях	Практически отсутствует
Третий	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Бессистемный / эпизодический контроль и совершенствование
Четвертый	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Системный контроль и совершенствование
Пятый	Реализуются в полном / практически полном объеме на постоянной основе	Общие подходы установлены в значительном количестве	Постоянный контроль и совершенствование

Для каждого раздела мер стандарт устанавливает свою систему оценок соответствия, например, Раздел 8. «Требования к организации и правлению защитой информации». Для оценок, характеризующих полноту реализации каждой из мер, определяют следующие числовые значения:

- 0 – мера не реализуется, т.е. у проверяющей организации отсутствуют свидетельства реализации оцениваемой меры;
- 0.5 – мера реализуется частично, не в полном объеме;
- 1 – мера реализуется в полном объеме, т.е. проверяющей организации предоставлены свидетельства полной реализации оцениваемой меры.

В данном ГОСТ также перечисляются основные источники свидетельств, на основании которых выставляются оценки соответствия:

• документы и иные материалы проверяемой организации в бумажном или электронном виде и при необходимости документы третьих лиц, относящиеся к обеспечению ЗИ финансовой организации и находящиеся в распоряжении проверяемой организации;

• устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия ЗИ;

• результаты наблюдений членов проверяющей группы за процессами системы ЗИ и деятельностью сотрудников проверяемой организации в области оценки соответствия ЗИ;

• параметры конфигураций и настроек технических объектов информатизации и средств ЗИ;

• технические и программные средства сбора свидетельств полноты реализации мер ЗИ (анализ электронных журналов регистрации, анализ фактических настроек, анализ уязвимостей, проведение тестирования на проникновение и т.п.).

В завершении методики оценивания есть качественная и количественная оценка соответствия процессов ЗИ. Качественная оценка выставляется в соответствии с приведенной в стандарте таблицей, которая, в свою очередь, основывается на расчетных значениях. Ниже приведена табл. 3 для качественной оценки уровня соответствия.

Таблица 3. Качественная оценка соответствия процессов системы ЗИ

E_i	**Уровень соответствия**
$E_i = 0$	Нулевой
$0 < E_i \leq 0.5$	Первый
$0.5 < E_i \leq 0.7$	Второй
$0.7 < E_i \leq 0.85$	Третий
$0.85 < E_i \leq 0.9$	Четвертый
$0.9 < E_i \leq 1$	Пятый

E_i – сумма числовых оценок контуров безопасности с учетом их весовых коэффициентов. Количественную оценку вычисляют как среднеарифметическое значение оценок E_i для всех процессов системы защиты информации и оценки полноты применения организационных и технических мер на этапах жизненного цикла без учета количества нарушений, выявленных проверяющей группой в процессе аудита.

4.2. Расчет показателей доверия

Взяв за основу ГОСТ Р 57580.1-2017, формализуем формулы для расчета каждого этапа оценки уровня доверия к процессу управления инцидентами информационной безопасности:

Показатели 1 этапа – метрики оценки уровня доверия к процессу управления инцидентами ИБ:

$$E_{1\text{ji}} = \begin{cases} 0, & \text{доказательство доверия отсутствует} \\ 1, & \text{доказательство доверия присутствует} \end{cases}, \quad (1)$$

где E_{1ji} – i-й показатель 1-го этапа (метрика) для вычисления j-го показателя 2-го этапа (критерия).

Показатели 2-го этапа – критерии оценки уровня доверия к процессу управления инцидентами ИБ:

$$E_{2j} = \frac{\sum_{i=1}^{N_j} E_{1ji}}{N_j}, \quad (2)$$

где E_{2j} – j-й показатель 2-го этапа (критерий), E_{1ji} – i-й показатель 1-го этапа (метрика) для вычисления j-го показателя 2-го этапа (критерия), N_j – количество показателей 1-го этапа (метрик), предназначенных для вычисления j-го показателя 2-го этапа (критерия).

Показатели 3-го этапа – уровень доверия к процессу управления инцидентами ИБ:

$$E = \frac{\sum_{j=1}^{N} E_{2j}}{N}, \quad (3)$$

где E – уровень доверия (зрелости) к процессу управления инцидентами информационной безопасности, E_{2j} – j-й показатель 2-го этапа (критерий), N – количество показателей 2-го этапа (критериев), предназначенных для вычисления показателя 3-го этапа (уровня доверия). В нашем случае $N = 6$.

При этом в качестве доказательств доверия (источников информации для оценки уровня доверия) будем использовать автоматизированный анализ составляющих организационно-правового поля исследуемой организации.

Соответствие уровней доверия к процессу управления инцидентами информационной безопасности основано на уровнях соответствия ГОСТ Р 57580.1-2017 (табл. 3).

4.3. Метрики доверия

Далее рассмотрим метрики оценки каждого критерия доверия, которые были определены выше:

1. Планирование и подготовка.
2. Обнаружение и оповещение.
3. Оценка и принятие решений.
4. Расследование инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Улучшение процесса управления инцидентами ИБ.

4.3.1. Метрики оценки доверия к критерию «Планирование и подготовка»

Пусть критерий «Планирование и подготовка» будет иметь обозначение E_{21}, тогда метрики оценки данного критерия будут носить обозначения E_{11i} (табл. 4).

Таблица 4. Метрики оценки доверия к критерию «Планирование и подготовка»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{111}	Наличие политики управления инцидентами ИБ	[0, 1]
E_{112}	Наличие регламента по обновлению политики управления инцидентами ИБ	[0, 1]
E_{113}	Наличие плана управления инцидентами ИБ	[0, 1]
E_{114}	Наличие приказа о формировании группы реагирования на инциденты ИБ	[0, 1]
E_{115}	Наличие регламента взаимодействия с внутренними и внешними организациями по вопросам управления инцидентами ИБ	[0, 1]
E_{116}	Наличие регламента по повышению квалификации специалистов по управлению инцидентами ИБ	[0, 1]
E_{117}	Наличие журнала прохождения повышения квалификации специалистами по управлению инцидентами ИБ	[0, 1]

E_{118}	Наличие акта, подтверждающего факт проведения киберучений	[0, 1]
E_{119}	Наличие внутреннего и внешнего SLA	[0, 1]

Тогда количество метрик в данном критерии $N_1 = 9$.

4.3.2. Метрики оценки доверия к критерию «Обнаружение и оповещение»

Пусть критерий «Обнаружение и оповещение» будет иметь обозначение E_{22}, тогда метрики оценки данного критерия будут носить обозначения E_{12i} (табл. 5).

Таблица 5. Метрики оценки доверия к критерию «Обнаружение и оповещение»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{121}	Наличие регламента по осуществлению мониторинга ИС	[0, 1]
E_{122}	Наличие регламента по журналированию событий ИБ в ИС	[0, 1]
E_{123}	Наличие регламента по анализу сетевой активности в ИС	[0, 1]
E_{124}	Наличие регламента по подключение источников к системе мониторинга ИБ организации	[0, 1]
E_{125}	Наличие регламента по инвентаризации активов ИС	[0, 1]
E_{126}	Наличие регламента оповещения о событии/уязвимости ИБ	[0, 1]
E_{127}	Наличие отчетов о реагировании на КИ	[0, 1]

Тогда количество метрик в данном критерии $N_2 = 7$.

4.3.3. Метрики оценки доверия к критерию «Оценка и принятие решений»

Пусть критерий «Оценка и принятие решений» будет иметь обозначение E_{23}, тогда метрики оценки данного критерия будут носить обозначения E_{13i} (табл. 6).

Таблица 6. Метрики оценки доверия к критерию «Оценка и принятие решений»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{131}	Наличие регламента по формированию степени серьезности события ИБ	[0, 1]
E_{132}	Наличие регламента о передаче события/инцидента в группу по расследованию инцидентов ИБ	[0, 1]
E_{133}	Наличие регламента контроля за изменениями и обновлениями баз знаний ИБ	[0, 1]
E_{134}	Наличие журнала обновлений изменений баз знаний ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_3 = 4$.

4.3.4. Метрики оценки доверия к критерию «Расследование инцидентов ИБ»

Пусть критерий «Расследование инцидентов ИБ» будет иметь обозначение E_{24}, тогда метрики оценки данного критерия будут носить обозначения E_{14i} (табл. 7).

Таблица 7. Метрики оценки доверия к критерию «Расследование инцидентов ИБ»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{141}	Наличие регламента по расследованию инцидентов информационной безопасности	[0, 1]
E_{142}	Наличие акта о внедрении средств автоматизации процесса обогащения данных об инциденте ИБ	[0, 1]
E_{143}	Наличие отчета о проведении расследования инцидента ИБ	[0, 1]
E_{144}	Наличие формы отчета о проведении расследования инцидента ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_4 = 4$.

4.3.5. Метрики оценки доверия к критерию «Реагирование на инциденты ИБ»

Пусть критерий «Реагирование на инциденты ИБ» будет иметь обозначение E_{25}, тогда метрики оценки данного критерия будут носить обозначения E_{15i} (табл. 8).

Таблица 8. Метрики оценки доверия к критерию «Реагирование на инциденты ИБ»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{151}	Наличие регламента по реагированию на инциденты информационной безопасности	[0, 1]
E_{152}	Наличие отчета о проведении мероприятий по реагированию на инцидент ИБ	[0, 1]
E_{153}	Наличие формы отчета о проведении мероприятий по реагированию на инцидент ИБ	[0, 1]
E_{154}	Наличие инструкции об использовании средств автоматизации процесса обогащения данных об инциденте ИБ	[0, 1]
E_{155}	Наличие информации об инцидентах ИБ в перечне конфиденциальной информации организации	[0, 1]

Тогда количество метрик в данном критерии $N_5 = 5$.

4.3.6. Метрики оценки доверия к критерию «Улучшение процесса управления инцидентами информационной безопасности»

Пусть критерий «Улучшение процесса управления инцидентами информационной безопасности» будет иметь обозначение E_{26}, тогда метрики оценки данного критерия будут носить обозначения E_{16i} (табл. 9).

Таблица 9. Метрики оценки доверия к критерию
«Улучшение процесса управления инцидентами информационной безопасности»

Номер метрики	Наименование метрики оценивания	Допустимые значения
E_{161}	Наличие регламента обработки результатов расследования и реагирования на инциденты ИБ	[0, 1]
E_{162}	Наличие журнала изменений системы защиты информации	[0, 1]
E_{163}	Наличие регламента по проведению киберучений	[0, 1]
E_{164}	Наличие KPI для сотрудников группы по расследованию инцидентов ИБ	[0, 1]
E_{165}	Наличие KPI для сотрудников группы по реагированию на инциденты ИБ	[0, 1]

Тогда количество метрик в данном критерии $N_6 = 5$.

5. Заключение

Разработана методика оценки уровня доверия (зрелости) к процессу управления инцидентами информационной безопасности, позволяющая провести автоматизированную оценку на основе объективных показателей, снижая при этом влияние человеческого фактора и повышая скорость её проведения за счет возможности применения средств автоматизации. Методика основана на анализе нормативно-правовых аспектов центров мониторинга за состоянием безопасности информационных систем (SOC). Сформированная методика содержит в себе набор критериев и метрик доверия для проведения оценки, набор формул для расчета каждой метрики и критериев доверия, а также формулу расчета итогового уровня доверия к процессу управления инцидентами информационной безопасности.

Разработанная методика может быть доработана путём анализа технических аспектов SOC и всей организации в целом. Помимо этого, данная методика может войти в состав общей методики оценки уровня доверия к процессам SOC, которая будет направлена на комплексный анализ всех процессов мониторинга безопасности информационных систем с целью получения объективных свидетельств, позволяющих в автоматизированном режиме провести расчет уровня зрелости SOC.

Литература

1. *Велигодский С. С., Милославская Н. Г.* Унифицированная модель зрелости центров управления сетевой безопасностью информационно-телекоммуникационных сетей // Известия ЮФУ. Технические науки. 2023. №3 (233). С. 157–172.
2. *Селезнёв В. М., Боровская О. Е.* Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ // Международный научно-исследовательский журнал. 2022. № 10 (124). С. 1–9.
3. *Веревкин С. А., Кравчук А. В., Беляков М. И.* Методика управления инцидентами информационной безопасности на объектах критической информационной инфраструктуры // Известия Тульского гос. университета. Технические науки. 2022. № 8. С. 116–120.
4. *Сухов А. М.* Оценивание эффективности процесса функционирования системы обеспечения информационной безопасности на основе теории стохастической индикации // Информационно-управляющие системы. 2022. № 3. С. 31–44.
5. *Иванов А. В., Никрошкин И. В. , Огнев И. А., Киселев М. А.* Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы TI

(Threat Intelligence) // Безопасность цифровых технологий. 2023. № 2 (109). С. 34–51. DOI: 10.17212/2782-2230-2023-2-34-51.
6. *Рева И. Л., Медведев М. А., Воронцова И. В.* Исследование проблематики методик определения типа контента во входящем трафике // Системы анализа и обработки данных. 2022. № 4 (92). С. 69–84. DOI: 10.17212/2782-2001-2023-4-69-84.
7. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
10. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
11. *Селифанов В. В., Аникеева В. В., Огнев И. А.* Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. 2023. № 1 (108). С. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.
12. Security Operations Maturity Model // StarLink. [Электронный ресурс] Режим доступа: https://assets.starlinkme.net/gitex-vendor-assets/logrhythm/uk-security-operations-maturity-model-white-paper.pdf (дата обращения: 30.01.2024).
13. *Al-Matari O. M. M., Helal I. M. A., Mazen Sh. A., Elhennawy Sh.* Adopting security maturity model to the organizations' capability model // Egyptian Informatics Journal. 2021. № 2 (22). P. 193–199.
14. *Muthukrishnan S. M., Palaniappan S.* Security metrics maturity model for operational security // Proc. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, 2016. P. 101–106.
15. *Sulistyowati D., Handayani F., Suryanto Y.* Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS // International Journal on Informatics Visualization. 2020. № 4 (4). P. 225–230.
16. *Rabii A., Assoul S., Ouazzani Touhami K., Roudies O.* Information and cyber security maturity models: a systematic literature review // Information and Computer Security. 2020. № 4 (28). P. 627–644.
17. *Arenas E., Palomino J., Mansilla J.* Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST // Proc. IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, 2023. P. 1–8.
18. ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles and process.
19. ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия».
20. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Иванов Андрей Валерьевич
к.т.н., доцент, заведующий кафедрой защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: andrej.ivanov@corp.nstu.ru, ORCID: 0000-0003-2002-8572.

Огнев Игорь Александрович
ассистент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: i.ognev.2016@corp.nstu.ru, ORCID: 0000-0003-3884-7170.

Никрошкин Иван Владимирович
ассистент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: i.nikroshkin@corp.nstu.ru, ORCID: 0000-0003-4824-7419.

Киселев Максим Алексеевич
лаборант кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса 20), e-mail: m.kiselev.2019@stud.nstu.ru, ORCID ID: 0009-0009-8248-2800.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Assessment of the Level of Trust in the Information Security Incident Management Process

Andrey V. Ivanov, Igor A. Ognev, Ivan V. Nikroshkin, Maxim A. Kiselev

Novosibirsk State Technical University (NSTU)

Abstract: The existing methods for assessing the level of trust in the information security incident management process and in the processes of information security event monitoring systems are extremely limited. These methods are based on an expert assessment and are periodic in nature with a long-time interval between assessments. The purpose of this study is to develop a methodology for assessing the level of trust in the information security incident management process, which is suitable for an automated assessment with minimal expert participation. As a result of the work, a methodology has been developed to assess the level of confidence in the information security incident management process, which includes a list of trust criteria and metrics for their assessment. The methodology is based on the SOMM methodology and GOST ISO/IEC 27035. The developed methodology is based on a three-stage assessment of trust indicators: assessment of trust metrics, assessment of trust criteria, assessment of the level of trust in the information incident management process.

Keywords: information security incidents, incident management, process assessment, level of trust, trust, information security, information security monitoring, cybersecurity.

For citation: Ivanov A. V., Ognev I. A., Nikroshkin I. V., Kiselev M. A. Assessment of the level of trust in the information security incident management process (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 88-102. https://doi.org/10.55648/1998-6920-2024-18-2-88-102.

The article was submitted: 09.02.2024; accepted for publication 29.02.2024.

References

1. Veligodskii S. S., Miloslavskaya N. G. Unifitsirovannaya model' zrelosti tsentrov upravleniya setevoi bezopasnost'yu informatsionno-telekommunikatsionnykh setei [Unified Maturity Model for Network Security Control Centers of Information and Telecommunication Networks]. *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*., 2023, no. 3 (233), pp. 157-172.
2. Seleznev V. M., Borovskaya O. E. Vstraivanie instrumentov SOAR-platform v ekosistemu SOC dlya avtomatizatsii protsessa reagirovaniya na intsidenty IB [Embedding SOAR platform tools into the SOC ecosystem to automate the process of responding to information security incidents]. *International Research Journa*l, 2022, no. 10 (124), pp. 1-9.
3. Verevkin S. A., Kravchuk A. V., Belyakov M. I. Metodika upravleniya intsidentami informatsionnoi bezopasnosti na ob"ektakh kriticheskoi informatsionnoi infrastruktury [Information Security Incident Management Methodology at Critical Information Infrastructure Facilities]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki*, 2022, no. 8, pp. 116-120.
4. Sukhov A. M. Otsenivanie effektivnosti protsessa funktsionirovaniya sistemy obespecheniya informatsionnoi bezopasnosti na osnove teorii stokhasticheskoi indikatsii [Evaluation of the Efficiency of the Information Security System Functioning Process Based on the Stochastic Indication Theory]. *Informatsionno-upravlyayushchie sistemy*, 2022, no. 3, pp. 31-44.
5. Ivanov A. V., Nikroshkin I. V., Ognev I. A., Kiselev M. A. Primenenie sredstv ekspertizy Blue Team v protsesse monitoringa informatsionnykh sistem na primere platformy TI (Threat Intelligence) [Application of the Blue Team expertise tools in the process of monitoring information systems on the example of the TI platform (Threat Intelligence)]. *Bezopasnost' tsifrovykh tekhnologii*, 2023, no. 2 (109), pp. 34-51. DOI: 10.17212/2782-2230-2023-2-34-51.
6. Reva I. L., Medvedev M. A., Vorontsova I. V. Issledovanie problematiki metodik opredeleniya tipa kontenta vo vkhodyashchem trafike [Study of the issues of methods for determining the type of content in incoming traffic]. *Sistemy analiza i obrabotki dannykh*, 2023, no. 4 (92), pp. 69-84. DOI: 10.17212/2782-2001-2023-4-69-84.
7. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 11 fevralya 2013 g. N 17 "Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavlyayushchei gosudarstvennuyu tainu, soderzhashcheisya v gosudarstvennykh informatsionnykh sistemakh"* [Order of the Federal Service for Technical and Export Control No. 17 of February 11, 2013 "On Approval of the Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems"].
8. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 18 fevralya 2013 g. N 21 "Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh* [Order of the Federal Service for Technical and Export Control No. 21 of February 18, 2013 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems"].
9. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. N 31 "Ob utverzhdenii Trebovanii k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudei i dlya okruzhayushchei prirodnoi sredy"* [Order of the Federal Service for Technical and Export Control No. 31 of March 14, 2014 "On Approval of the Requirements for Ensuring Information Security in Automated Control Systems for Production and Technological Processes at Critical Facilities, Potentially Hazardous Facilities, as well as Facilities Posing an Increased Danger to Human Life and Health and the Environment"].

10. *Prikaz Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 25 dekabrya 2017 g. N 239 "Ob utverzhdenii Trebovanii po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii"* [Order of the Federal Service for Technical and Export Control No. 239 of December 25, 2017 "On Approval of the Requirements for Ensuring the Security of Significant Facilities of the Critical Information Infrastructure of the Russian Federation"].
11. Selifanov V. V., Anikeeva V. V., Ognev I. A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. Bezopasnost' tsifrovykh tekhnologii, 2023, no. 1 (108), pp. 69-82. DOI: 10.17212/2782-2230-2023-1-69-82.
12. Security Operations Maturity Model. *StarLink*, available at: `https://assets.starlinkme.net/gitex-vendor-assets/logrhythm/uk-security-operations-maturity-model-white-paper.pdf` (accessed: 30.01.2024).
13. Al-Matari O. M. M., Helal I. M. A., Mazen Sh. A., Elhennawy Sh. Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal*., 2021, no. 2 (22), pp. 193-199.
14. Muthukrishnan S. M., Palaniappan S. Security metrics maturity model for operational security. *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, IEEE Xplore, 2016, pp. 101-106.
15. Sulistyowati D., Handayani F., Suryanto Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, 2020, vol 4, no. 4, pp. 225-230.
16. Rabii A., Assoul S., Ouazzani Touhami K., Roudies O. Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, 2020, vol.28, no. 4, pp. 627-644.
17. Arenas E., Palomino J., Mansilla J. Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST. *2023 IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Lima, IEEE Xplore, 2023, pp. 1-8.
18. *ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles and process*.
19. *GOST R 57580.2-2018 «Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer. Metodika otsenki sootvetstviya»* [GOST R 57580.2-2018 "Security of Financial (Banking) Transactions. Protection of information of financial institutions. Basic composition of organizational and technical measures. Conformity Assessment Methodology"].
20. *GOST R 57580.1-2017 «Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer»* [GOST R 57580.1-2017 "Security of Financial (Banking) Transactions. Protection of information of financial institutions. Basic Composition of Organizational and Technical Measures"].

Andrey V. Ivanov

PhD in Technology, Head of the Department of Information Security, Associate Professor, Novosibirsk State Technical University, e-mail: `andrej.ivanov@corp.nstu.ru`, ORCID: 0000-0003-2002-8572.

Igor A. Ognev

Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `i.ognev.2016@corp.nstu.ru`, ORCID: 0000-0003-3884-7170.

Ivan V. Nikroshkin

Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `i.nikroshkin@corp.nstu.ru`, ORCID: 0000-0003-4824-7419.

Maksim A. Kiselev

Laboratory Assistant of the Department of Information Security, Novosibirsk State Technical University (NSTU, 630073, Novosibirsk, Karl Marx Ave. 20), e-mail: `m.kiselev.2019@stud.nstu.ru`, ORCID ID: 0009-0009-8248-2800.

DOI: 10.55648/1998-6920-2024-18-2-103-112 УДК 004.04: 378.147

Методика оценивания эффективности образовательной онлайн-платформы вуза

Н. В. Кулешова[1], А. Н. Полетайкин[2], Е. Г. Струкова[1], В. Г. Котельников[2]

[1] Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)
[2] Кубанский государственный университет (КубГУ)

Аннотация: В статье рассмотрены вопросы конструктивной цифровой трансформации учебного процесса посредством использования образовательных онлайн-платформ. На основе анализа существующих решений разработана авторская методика дифференцированного оценивания образовательной онлайн-платформы вуза. Встроенная в платформу метрическая модель на основе рискового термометра являет собой новый подход в области образовательного технологического проектирования учебного процесса. Практическая значимость методики оценивания эффективности образовательной онлайн-платформы состоит в получении релевантной информации для принятия решений по развитию платформы, что, в свою очередь, обеспечит эффективную организацию и повысит результативность учебного процесса в вузе.

Ключевые слова: цифровая трансформация, цифровая среда, учебный процесс, образовательная онлайн-платформа, метрики эффективности, рисковый термометр.

Для цитирования: Кулешова Н. В., Полетайкин А. Н., Струкова Е. Г., Котельников В. Г. Методика оценивания эффективности образовательной онлайн-платформы вуза // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 103–112. https://doi.org/10.55648/1998-6920-2024-18-2-103-112.

Статья поступила в редакцию 27.04.2024;
переработанный вариант – 27.05.2024;
принята к публикации 28.05.2024.

1. Введение

В современном мире онлайн-образование становится всё более популярным. После так называемой пандемии 2020–2021 годов многие вузы РФ перешли к смешанному формату образования, допускающему наряду с обучением on-campus дистанционный формат on-line. Для реализации такого подхода вузам необходима образовательная онлайн-платформа (ООЛП), на базе которой может быть реализована открытая электронная информационно-образовательная среда (ЭИОС). Поэтому сегодня сфера образования стала полем активного проникновения новых технологий, к которым, в частности, относятся ООЛП. Основания для реализации ООЛП в образовании прописаны в статье 16 Федерального закона об образовании в РФ от 29.12.2012 г. № 273-ФЗ, п. 1 которого определяет понятия электронного и дистанционного обучения, а п. 3 предписывает образовательным организациям создание условий для функционирования ЭИОС. С введением в действие ФГОС версии 3 появилось требование использования ЭИОС в образовательном процессе очной формы обучения. В 2017 году при модификации ФГОС 3+ были усилены и детализированы требования к условиям реализации основных образовательных программ, в частности, к их ресурсному обеспечению. Данное обстоятельство потребовало от вузов масштабной деятельности по созданию и

развитию ЭИОС, интегрирующих в себе всю нематериальную ресурсную базу образовательного процесса. Это, в свою очередь, потребовало создания собственных либо использования сторонних ООЛП. Всё это закономерно обусловило цифровизацию образовательного процесса и в последние годы составляет значительную часть цифровой трансформации сферы российского образования в частности и экономики страны вообще [1].

В связи с этим актуальной задачей является интенсификация развития системы образования, одним из важнейших компонентов которой в условиях реализации Стратегии цифровой трансформации науки и высшего образования [2] от 14 июля 2021 года является формирование высокоэффективных ООЛП. Следовательно, развитие ООЛП в вузах выступает существенным фактором конструктивной цифровой трансформации образовательной организации, базовыми условиями которой являются минимизация рутинной занятости субъектов учебного процесса, позволяющая им уделять больше внимания креативной деятельности; рациональная адекватность модельно-методического комплекса ООЛП; приоритет живого творческого общения во взаимодействии «преподаватель – студент». В этом заключается суть конструктивности, определяющей ядро цифровой трансформации образовательной деятельности [3]. Недавние исследования существующих цифровых ООЛП [4, 5] показывают их разнообразие в организационном, структурно-функциональном и временно́м аспектах. Акцентируется внимание на пользовательском и административном уровнях ООЛП, на недостатках, связанных со слабой цифровой зрелостью, на цифровых разрывах, затрудняющих эффективную работу на платформе. Фиксируется недостаток конструктивности электронного обучения посредством ООЛП в контексте указанных выше базовых условий. Цель данной статьи – проанализировать конструктивность цифровой трансформации вуза по направлению развития ООЛП как цифрового аналога учебного процесса, выступающей объектом исследования. Предмет исследования – цифровое отображение учебного процесса на платформе и средства оценивания её эффективности.

2. Подходы к оцениванию эффективности ООЛП

Поскольку менеджерам образовательной организации необходимо знать недоработки и «узкие места», а также фактические и потенциальные конкурентные преимущества своих платформ на рынке образования, возникает актуальная задача получения комплексной оценки эффективности образовательной платформы.

Существуют различные подходы и методы для оценивания эффективности онлайн-обучения. Один из подходов к оцениванию качества ООЛП заключается в использовании метода GAP-анализа [6], который позволяет выявить разрывы между ожиданиями студентов и их восприятием процесса обучения. Этот метод включает в себя такие критерии, как удовлетворенность студентов, надежность и отзывчивость платформы. GAP-анализ универсален и хорошо сочетается с другими методами анализа. В то же время его недостатком является субъективность используемых результатов опроса студентов.

Одним из разработанных методов оценки взаимодействия образовательной организации и пользователей в едином информационном и образовательном пространстве, где существуют единые требования к содержанию и качеству образования, является бизнес-модель ООЛП «Канвас» [7]. Она отражает риски онлайн-платформы и внешних вызовов для сотрудничества пользователей и образовательной организации на базе данной ООЛП.

Распространенным методом оценивания образовательных платформ является измерение их эффективности с помощью различных метрик (критериев). В разных источниках можно насчитать десятки метрик. В разделе 3 представлена авторская структура метрик, включающая 35 метрик, поровну разделённых на семь групп.

3. Система метрик ООЛП

Система метрик получена в результате коллективного анализа комплекса показателей эффективности образовательных онлайн-ресурсов, частично извлечённых из результатов других прикладных исследований [4, 5], частично сформулированных в рамках текущего исследования, и последующей его апробации с привлечением экспертов в данной области.

1. **Метрики удовлетворенности пользователя** показывают, насколько субъекты учебного процесса удовлетворены обучением:
   - 1.1) общая удовлетворенность качеством платформы;
   - 1.2) скорость работы платформы;
   - 1.3) возможность рекомендации платформы другим людям;
   - 1.4) возможность дальнейшего использования платформы;
   - 1.5) общее впечатление о платформе.
2. **Метрики юзабилити** характеризуют удобство работы с платформой, её понимаемость, эргономичность и привлекательность для пользователя:
   - 2.1) появление сообщений об ошибке;
   - 2.2) необходимость перезапуска задач;
   - 2.3) оперативность выполнения задач;
   - 2.4) простота использования платформы;
   - 2.5) простота поиска данных на платформе.
3. **Метрики структурных свойств платформы** отражают качество организации образовательного контента на платформе:
   - 3.1) общий дизайн и оформление платформы;
   - 3.2) интуитивная понятность и логичность структуры платформы;
   - 3.3) возможность отслеживания последовательности изучения учебных курсов;
   - 3.4) возможности по размещению разных видов контента;
   - 3.5) техническая поддержка платформы.
4. **Метрики взаимодействия** позволяют оценить качество образования на платформе в контексте коммуникации пользователей и организации обратной связи:
   - 4.1) возможность отслеживания прогресса изучения учебных курсов и их элементов;
   - 4.2) возможности для оперативного анализа успеваемости;
   - 4.3) средства для оперативной связи между пользователями;
   - 4.4) средства для оперативной связи пользователей с администрацией университета;
   - 4.5) способствование мотивации к обучению у студентов.
5. **Метрики управления образовательным процессом** дают представление об организационных и аналитических возможностях платформы:
   - 5.1) возможности персонализации;
   - 5.2) удовлетворение индивидуальных образовательных потребностей обучающихся;
   - 5.3) возможности отслеживания активности пользователей на платформе;
   - 5.4) инструменты аналитики на платформе;
   - 5.5) тайминг основных действий пользователя на платформе.
6. **Метрики интенсивности** оценивают производительность обучающихся и скорость восприятия ими материала, а также активность всех категорий пользователей:
   - 6.1) активность обучающихся на платформе;
   - 6.2) активность преподавателей на платформе;
   - 6.3) активность административных работников на платформе;
   - 6.4) время пребывания обучающихся на платформе;
   - 6.5) время пребывания преподавателей на платформе.
7. **Метрики качества обучения** показывают, с какой успешностью студенты осваивают учебный материал на платформе:
   - 7.1) доходимость (доля студентов, завершивших обучение);
   - 7.2) результативность (доля студентов, трудоустроившихся по специальности);

7.3) отчисление (доля студентов, не завершивших обучение по курсу/модулю за вычетом переведённых на другой курс/модуль);
7.4) посещаемость мероприятий контактной работы на платформе;
7.5) качественная успеваемость на платформе.

Среди указанных метрик объективному оцениванию на основе анализа цифровых следов пользователей платформы подлежат лишь 10 метрик групп 6 и 7. Практически все известные ООЛП собирают соответствующие данные об активностях своих пользователей и цифровых сервисов. Остальные 25 метрик могут быть оценены посредством экспертизы либо опроса пользователей платформы. Учитывая специфику предмета оценивания – ООЛП, на которой регулярно работает большое количество пользователей, опрос представляется наилучшим решением. В силу различий в функционале ООЛП для трёх категорий пользователей (см. группу 6) были разработаны три соответствующие модификации опросника. Также в опросники добавлен раздел «Данные о себе», позволяющий идентифицировать пол, возраст, статус, стаж, область знаний респондента, а также опыт и тайминг использования платформы. В интерактивном тестировании опросника приняли участие 19 опытных пользователей разных ООЛП, используемых в СибГУТИ, НГУЭУ и КубГУ: 6 студентов, 8 преподавателей, 5 административных работников. В результате тестирования в опросник внесены более 100 изменений. Критериальная валидность опросника по десяти характерным метрикам: 1.2, 2.1, 3.3, 3.5, 4.1–4.4, 5.3 и 5.4, для которых были получены экспертные данные о поведении оцениваемой ООЛП, составила 0.665, что является приемлемой оценкой качества опросника.

4. Оценивание эффективности ООЛП

4.1. Модифицированный рисковый термометр оценивания эффективности ООЛП

Полученные оценки метрик предлагается обрабатывать комплексно посредством методики рискового термометра. Применение данной методики в отношении организации образовательной деятельности было разработано авторами в статье [8]. В данном случае под рисковой температурой понимается степень эффективности ООЛП. Нормальное состояние платформы приравнивается к отметке 36.6 °C. Повышенная температура отражает наличие проблем, а величина превышения соответствует степени неэффективности ООЛП.

Применительно к обработке результатов опроса рисковый термометр работает следующим образом. Каждому *j*-му варианту ответа ($j = \overline{1, m}$) на *i*-й вопрос опросника ($i = \overline{1, n}$) присваивается соответствующий вес (коэффициент) k_{ij}^{l}, соответствующий *l*-му рисковому состоянию ООЛП ($l = \overline{1, p}$). Полученные результаты обрабатываются статистическими методами и приводятся к интегральному показателю, который отражает рисковую температуру как ООЛП в целом, так и по каждой из семи групп метрик. Каждая группа метрик – целевой фактор, управляющие воздействия на которые приводят ООЛП в нормальное (соответствующее ожиданиям пользователя и нормативным требованиям законодательной базы) состояние.

Интегральный показатель рисковой температуры (*T*) определяется по формуле:

$$T = \sum_{i=1}^{n} \sum_{j=1}^{m_i} k_{ij}^{l} x_{ij},$$

где x_{ij} – бинарная переменная *j*-го ответа на *i*-й вопрос: $x_{ij} = 1$ – если *i*-му вопросу соответствует *j*-й вариант ответа, $x_{ij} = 0$ – иначе; k_{ij}^{l} – рисковый вес *j*-го ответа на *i*-й вопрос; $l = \overline{1, p}$ – индекс рискового состояния объекта; *p* – число таких состояний; *n* – число вопросов.

Рисковые веса (k_{ij}^{l}) выступают нормирующими коэффициентами, приводящими интегральные результаты к определённым температурным состояниям T_l:

$$k^l = \frac{T_l}{n}.$$

Так, в отношении ООЛП разумно видеть следующие температурные состояния (табл. 1) и соответствующие им рисковые веса для системы из 35 метрик.

Таблица 1. Показатели рискового фона ООЛП для измерения рисковым термометром

№	Состояние ООЛП	T_l, °C	k^l	Оценка эффективности ООЛП
1	нормальное	36.6	1.046	Вполне эффективна
2	лихорадочное	38	1.086	Частично эффективна (в отдельных аспектах)
3	критическое	40	1.143	Малоэффективна
4	катастрофическое	42	1.200	Полностью неэффективна

Фрагмент структуры анкеты преподавателя (доступна для ознакомления по ссылке: `https://forms.gle/dzo7vC9vQ8XpUkFWA`) по целевому фактору удовлетворенности пользователя представлен в табл. 2 с зафиксированными рисковыми весами ответов согласно табл. 1. Аналогичный фрагмент термометра представлен в табл. 3 по целевому фактору качества обучения.

Таблица 2. Рисковый термометр образовательной онлайн-платформы (фрагмент по целевому фактору 1 – Удовлетворенность пользователя)

Вопросы	Варианты ответов	Рисковый вес ответа
Насколько Вы вообще удовлетворены качеством платформы?	Да, вполне удовлетворен	1.046
	Скорее удовлетворен	1.086
	Скорее не удовлетворен	1.143
	Нет, не удовлетворен	1.200
	Затрудняюсь ответить	1.143
Как Вы оцениваете скорость работы платформы?	Да, вполне удовлетворен	1.046
	Скорее удовлетворен	1.086
	Скорее не удовлетворен	1.143
	Нет, не удовлетворен	1.200
	Затрудняюсь ответить	1.143
Порекомендуете ли Вы данную платформу своим коллегам?	Да, порекомендую	1.046
	Скорее да	1.086
	Скорее нет	1.143
	Однозначно нет	1.200
Хотели бы Вы и далее использовать данную платформу для обеспечения образовательного процесса по своим учебным дисциплинам?	Да, конечно	1.046
	Скорее да	1.086
	Скорее нет	1.143
	Однозначно нет	1.200
Оцените Ваше общее впечатление о данной образовательной платформе по 10-балльной шкале (10 – высшая оценка, 0 – низшая оценка)	8–10	1.046
	5–7	1.086
	2–4	1.143
	0, 1	1.200

Таблица 3. Рисковый термометр образовательной онлайн-платформы
(фрагмент по целевому фактору 7 – Качество обучения)

Показатели (принятая методика их оценивания)	Интервалы значений	Рисковый вес интервала
Доходимость (доля студентов, завершивших обучение). Результативность (доля студентов, трудоустроившихся по специальности). Посещаемость мероприятий контактной работы (доля студентов, оставивших на платформе эти цифровые следы). Качественная успеваемость (доля студентов с успеваемостью на платформе не ниже чем «хорошо»)	0.90…1.00	1.046
	0.75…0.90	1.086
	0.50…0.75	1.143
	0.00…0.50	1.200
Отчисление (доля студентов, не завершивших обучение на платформе по курсу/модулю за вычетом переведённых на другой курс/модуль)	0.00…0.10	1.046
	0.10…0.25	1.086
	0.25…0.50	1.143
	0.50…1.00	1.200

Поскольку оценки метрик этой группы рассчитываются на основе анализа цифровых следов пользователей ООЛП, распределение рисковых весов выполнено экспертно по интервалам фактических значений этих метрик. Заметим, что разработанные три модификации опросника и их структуры индифферентны оцениваемым ООЛП и различаются только относительно категории субъектов учебной деятельности.

Дифференциальная (частная) рисковая температура (T^s) по группе метрик (в данном случае имеет место 7 целевых факторов, $q = 7$) определяется следующим образом:

$$T^s = \frac{n}{n^s} \sum_{i=1}^{n^s} \sum_{j=1}^{m} k_{ij}^l x_{ij},$$

где n^s – число метрик в группе s-го целевого фактора, $s = \overline{1,q}$.

4.2. Температурный профиль ООЛП

Оценивание и анализ метрик определяет эффективность ООЛП в целом и по группам, что позволяет принять управленческие решения относительно повышения эффективности платформы. На основе полученной актуальной информации об эффективности ООЛП по разным метрикам и целевым факторам могут вырабатываться рекомендации для развития платформы, для организации внутренней системы оценивания качества образования, а также формироваться рейтинги реализуемых на платформе образовательных программ. Кроме того, такой инструмент может помочь упростить процедуры мониторинга достижений обучающихся и выстраивать их индивидуальные траектории обучения, а также мотивировать образовательные организации совершенствовать содержание учебных курсов и организацию учебного процесса, повышая таким образом его результативность.

В качестве рабочего примера рассмотрим образовательную платформу дистанционного образования, используемую в СибГУТИ с 2005 года. Данные для оценивания метрик групп 6 и 7 были выгружены из хранилища данных платформы и обработаны статистически в соответствии с принятой методикой, краткое изложение которой см., например, в табл. 3. Данные для расчёта метрик 6.3–6.5 и 7.4 в хранилище этой платформы отсутствуют. Кроме того, в опроснике студентов отсутствует вопрос по метрике 5.4. Поэтому общее число метрик для расчета эффективности ООЛП на основе опроса студентов составляет 30, а с использованием опросников преподавателей и работников администрации – 31.

Метрики групп 1–5 оценивались на основе результатов опроса пользователей платформы (см. подраздел 4.1). Всего в опросе приняли участие 77 студентов и 42 преподавателя, рабо-

тающих на платформе, а также 5 административных работников института заочного образования СибГУТИ, обеспечивающих функционирование платформы.

На рис. 1 показан температурный профиль эффективности исследуемой ООЛП. Оценки целевых факторов 1–5 и интегральной температуры показывают значительно бóльшую удовлетворённость студентов сервисами ООЛП. Во многом это объясняется более развитым и периодически совершенствуемым функционалом кабинета студента на платформе. Кабинет же преподавателя сколько-нибудь существенного развития за годы эксплуатации платформы не получил. Кроме того, преподаватели на вопросы по метрикам групп 3–5 в 32 % случаев затруднились ответить, что показывает слабое владение инструментарием платформы и также является маркером её неэффективности. Более умеренные оценки административных работников, которые испытали затруднения с ответами на вопросы по метрикам групп 3–5 лишь в 18 % случаев, дают более реалистичную картину эффективности оцениваемой ООЛП.

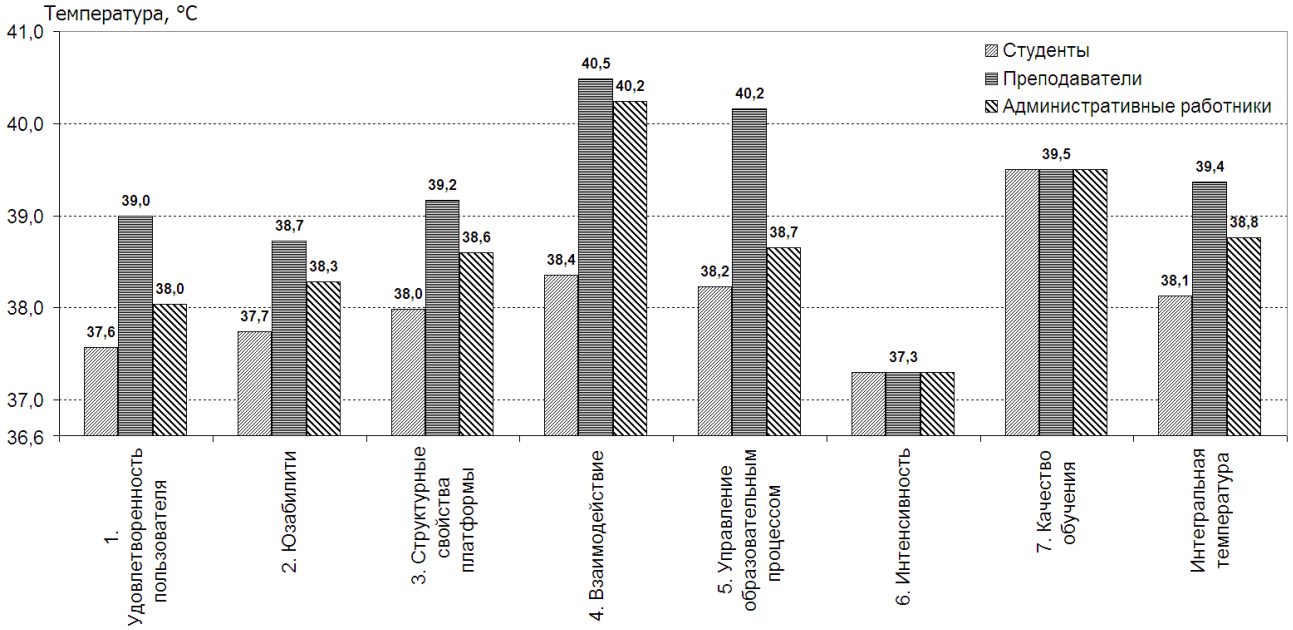


Рис. 1. Температурный профиль эффективности платформы дистанционного образования СибГУТИ

5. Заключение

Разработанная методика даёт возможность организовать автоматизированный канал обратной связи от субъектов учебного процесса, обеспечивающий доставку цифровых следов, включая результаты опросов, проводимых с правильной периодичностью (например, обязательные опросы студентов по завершении некоторого периода обучения и регулярные опросы преподавателей в директивно определённые сроки). Это позволит актуализировать данные об эффективности ООЛП и на их основе принимать решения по цифровому развитию вуза. При этом *необходимым фактором* и индикатором конструктивности этого развития в аспекте реализации ООЛП выступает её рисковая температура. Интегральная температура находится в т.н. оранжевой зоне и в среднем составляет 38.8 °C (см. рис. 1), а в аспекте взаимодействия (средняя температура 39.6 °C) платформа и вовсе находится в состоянии, близком к кризисному. Однако уже на данном этапе можно констатировать наличие необходимой конструктивности цифровой трансформации образовательной организации в силу обеспечиваемой платформой существенной минимизации рутинной занятости субъектов учебного процесса. Как отмечено во введении, данный фактор определяет ядро цифровой трансформации образовательной деятельности.

Дальнейшие исследования будут направлены на разработку новой функционально-структурной концепции цифровой среды организационной системы. На примере образовательной системы вообще и учебного процесса в частности с применением положений информационной динамики и гибридного математического моделирования образовательной деятельности будет построен модельно-методический комплекс ООЛП. Рациональная адекватность этого комплекса выступит *достаточным фактором* конструктивности цифровой трансформации вуза. К сожалению, важный достаточный фактор конструктивности – приоритет живого творческого человеческого общения во взаимодействии «преподаватель – студент» – реализуем лишь в смешанном обучении «on-line – on-campus» либо при цифровой поддержке дневной формы обучения в варианте ЭИОС. Однако при наличии прочих факторов и режим дистанционного онлайн-обучения будет обладать приемлемой степенью конструктивности.

Выражение благодарности

Авторы выражают благодарность студентам и работникам СибГУТИ, НГУЭУ и КубГУ, принявшим участие в тестировании опросного материала, персонально доценту кафедры ММиЦРБС Шевцовой Юлии Владимировне за множество конструктивных замечаний, а также руководителю группы разработки программного обеспечения УИТ СибГУТИ Пономарёву Эдуарду Анатольевичу за информационную поддержку исследования.

Литература

1. *Никифорова Д. П.* Электронное обучение как инструмент реализации цифровой среды // Научное образование. 2023. № 1 (18). С. 93–96.
2. Стратегия цифровой трансформации отрасли науки и высшего образования / Официальный сайт Минобрнауки России. URL: `https://www.minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllr6uwtujw.pdf` (дата обращения: 29.03.2024).
3. *Канев В. С., Полетайкин А. Н., Монастырская Т. И., Шевцова Ю. В.* Конструктивность цифровой трансформации образовательной деятельности вуза // Сб. трудов VI междун. науч.-практ. конф. «Информационные системы и технологии в моделировании и управлении», 24–26 мая 2021 г., Симферополь. С. 256–260.
4. *Шелепаева А. Х.* Образовательные онлайн-платформы: классификация и критерии оценивания // Открытое образование. 2022. №26 (3). С. 27–34.
5. *Итинсон К. С., Чиркова В. М.* Обзор платформ электронного обучения: инструменты, преимущества, недостатки // Балтийский гуманитарный журнал. 2021. Т. 10, № 3 (36). С. 194–197. DOI 10.26140/bgz3-2021-1003-0048.
6. *Хромова И. Н.* Практические аспекты применения GAP-анализа при обосновании стратегических управленческих решений // Сб. мат. VI междун. науч.-практ. конф. «Развитие науки и практики в глобально меняющемся мире в условиях рисков», 15 октября 2021. С. 143–149.
7. *Карлов И. А. и др.* Анализ цифровых образовательных ресурсов и сервисов для организации учебного процесса // Современная аналитика образования. 2020. № 10 (40). С. 9.
8. *Шевцова Ю. В., Канев В. С., Полетайкин А. Н., Кулешова Н. В.* Новая математическая модель риск-менеджмента образовательной деятельности вуза // Вестник СибГУТИ. 2019. № 4. С. 42–55.

Кулешова Наталия Владимировна

к.э.н., доцент, и.о. проректора по учебной и методической работе, доцент кафедры математического моделирования и цифрового развития бизнес-систем СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел.: +7 383 2698 202, e-mail: natkuleshova@yandex.ru, ORCID ID: 0000-0002-7708-958X, , Scopus AuthorID: 57215324667.

Полетайкин Алексей Николаевич

к.т.н., доцент, доцент кафедры информационных технологий Кубанского государственного университета (350040, Краснодар, ул. Ставропольская, 149), тел. +7 861 2199 577, e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952, Scopus AuthorID: 57213829361, ResearcherID: ABF-6799-2020.

Струкова Елена Геннадьевна

начальник управления маркетинга и развития образования, старший преподаватель кафедры социально-коммуникативных технологий СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел.: +7 383 2698 301, e-mail: strukova@sibguti.ru, ORCID ID: 0000-0002-5128-1952.

Котельников Владислав Геннадьевич

студент 4-го курса факультета компьютерных технологий и прикладной математики Кубанского государственного университета (350040, Краснодар, ул. Ставропольская, 149), тел. +7 861 2199 577, e-mail: vladkot2711@gmail.com, ORCID ID: 0000-0001-7952-8593.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Methodology for Measuring the Effectiveness of University Online Educational Platforms

Nataliya V. Kuleshova[1], Aleksey N. Poletaikin[1,2], Elena G. Strukova[1], Vladislav G. Kotelnikov[2]

[1] Siberian State University of Telecommunications and Information Science (SibSUTIS)
[2] Kuban State University (KubSU)

Abstract: This article deals with the issues of constructive digital transformation of the learning process using educational online platforms. The metric model based on the risk thermometer embedded in the platform is a new approach in the field of educational technological design. The practical significance of the educational process consists in obtaining relevant information for decision-making on the development of online educational platforms, which in turn will ensure the effective organization and improve the effectiveness of the educational process.

Keywords: digital transformation, digital area, learning process, online educational platform, performance metrics, risk thermometer.

For citation: Kuleshova N. V., Poletaikin A. N., Strukova E. G., Kotelnikov V. G. Methodology for measuring the effectiveness of university online educational platforms (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 103-112. https://doi.org/10.55648/1998-6920-2024-18-2-103-112.

The article was submitted: 27.04.2024;
revised version: 27.05.2024;
accepted for publication 28.05.2024.

References

1. Nikiforova D. P. Jelektronnoe obuchenie kak instrument realizacii cifrovoj sredy [E-learning as a tool for realizing the digital environment]. *Nauchnoe obrazovanie*, 2023, no. 1(18), pp. 93-96.
2. Strategija cifrovoj transformacii otrasli nauki i vysshego obrazovanija [Strategy for digital transformation of the science and higher education industries]. *Oficial'nyj sajt Minobrnauki Rossii*, URL: https://www.minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllr6uwtujw.pdf (accessed: 29.03.2024).
3. Kanev V. S., Poletajkin A. N., Monastyrskaja T. I., Shevcova Ju. V. Konstruktivnost' cifrovoj transformacii obrazovatel'noj dejatel'nosti vuza [Constructiveness of digital transformation of educational activities of a university]. *Informacionnye sistemy i tehnologii v modelirovanii i upravlenii, sbornik trudov VI Mezhdunarodnoj nauchno-prakticheskoj konferencii*, 24-26 May, 2021, Simferopol', Tipografija RIAL, pp. 256-260.
4. Shelepaeva A. H. Obrazovatel'nye onlajn-platformy. Klassifikacija i kriterii ocenivanija [Educational online platforms: classification and evaluation criteria]. *Open Education*, 2022, no. 26(3), pp. 27-34. https://doi.org/10.21686/1818-4243-2022-3-27-34.
5. Itinson K. S., Chirkova V. M. Obzor platform jelektronnogo obuchenija. Instrumenty, preimushhestva, nedostatki [Review of e-learning platforms: tools, advantages, disadvantages]. *Baltijskij gumanitarnyj zhurnal*, 2021, vol. 10, no. 3(36), pp. 194-197. DOI 10.26140/bgz3-2021-1003-0048.
6. Hromova I. N. Prakticheskie aspekty primenenija GAP-analiza pri obosnovanii strategicheskih upravlencheskih reshenij [Practical aspects of using GAP analysis in substantiating strategic management decisions]. *Razvitie nauki i praktiki v global'no menjajushhemsja mire v uslovijah riskov, sbornik materialov VI mezhdunarodnoj nauchno-prakticheskoj konferencii*, 15 October, 2021, Moscow, pp. 143-149.
7. Karlov I. A. et al. Analiz cifrovyh obrazovatel'nyh resursov i servisov dlja organizacii uchebnogo processa [Analysis of digital educational resources and services for organizing the educational process]. *Sovremennaja analitika obrazovanija*, Moscow, Vysshaja shkola jekonomiki, 2020, no. 10(40). p. 9.
8. Shevcova Ju. V., Kanev V. S., Poletajkin A. N., Kuleshova N. V. Novaja matematicheskaja model' riskmenedzhmenta obrazovatel'noj dejatel'nosti vuza [New mathematical model of risk management of educational activities of a university]. *Vestnik Sibirskii gosudarstvennyi universitet telekommunikatsii i informatiki*, Novosibirsk, 2019, no. 4, pp. 42-55.

Nataliya V. Kuleshova

Cand. of Sci. (Economics), Act. Vice-Rector for Academic and Methodological Work, Assistant Professor of the Department of Mathematical Modeling and Digital Development of Business Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 202 e-mail: natkuleshova@yandex.ru, ORCID ID: 0000-0002-7708-958X, Scopus AuthorID: 57215324667.

Aleksey N. Poletaikin

Cand. of Sci. (Engineering), Assistant Professor at the Information Technologies Department, Kuban State University (KubSU, Russia, 350040, Krasnodar, Stavropolskaya st., 149), phone: +7 861 2199 577, e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952, Scopus AuthorID: 57213829361, ResearcherID: ABF-6799-2020.

Elena G. Strukova

Head of Marketing and Education Development Department, M, Siberian State University of Telecommunications and Information Sciences, (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 301, e-mail: strukova@sibguti.ru, ORCID: 0000-0001-7952-8593.

Vladislav G. Kotelnikov

Student of the 4th year of the Faculty of Computer Technologies and Applied Mathematics, Kuban State University (KubSU, Russia, 350040, Krasnodar, Stavropolskaya st., 149), phone: +7 861 2199 577, e-mail: vladkot2711@gmail.com, ORCID ID: 0009-0007-8800-6050.

DOI: 10.55648/1998-6920-2024-18-2-113-126 УДК 003.26

Построение стегосистемы RDH на основе статистических свойств областей изображения *

Е. Ю. Мерзлякова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье рассмотрен метод обратимого скрытия данных (RDH) для растровых изображений. Статистические свойства контейнера учитываются путем разделения изображения на связные области методом «лесного пожара» и сбора статистики младших бит для формирования встраиваемой последовательности с заданным распределением. Для разделения изображения на часть для сбора статистических свойств контейнера и часть для встраивания информации применяется метод интерполяции INP. Получение последовательности бит с заданным распределением обеспечивается арифметическим декодером. Построенная стегосистема имеет ёмкость встраивания 0.6 бит/пиксель. Проводится RS-стегоанализ на базе изображений BOSS_v1.01 и оценка свойств полученных контейнеров по показателям визуального искажения.

Ключевые слова: стеганография, цифровые изображения, встраивание информации, интерполяция, стегоанализ.

Для цитирования: Мерзлякова Е. Ю. Построение стегосистемы RDH на основе статистических свойств областей изображения // Вестник СибГУТИ. 2024. Т. 18, № 2. С. 113–126. https://doi.org/10.55648/1998-6920-2024-18-2-113-126.

Статья поступила в редакцию 28.04.2024;
переработанный вариант – 02.05.2024;
принята к публикации 19.05.2024.

1. Введение

На сегодняшний день задача обеспечения безопасности передачи информации путем цифровой коммуникации имеет высокую степень значимости, и ее решение основывается на методах криптографии и стеганографии [1]. Классическая задача криптографии состоит в том, чтобы скрыть от третьих лиц содержание сообщения, в то время как классическая задача стеганографии – скрыть сам факт передачи сообщения. Данные области взаимосвязаны, например, стеганографические схемы могут использоваться для надежной передачи ключей в безусловно стойких криптосистемах [2], а криптографические методы, в свою очередь, повышают безопасность стеганографических схем [3–6].

Стеганография как наука возникла достаточно давно, развиваясь в направлении повышения надежности и безопасности методов передачи скрытой информации в безобидных на вид контейнерах. В качестве контейнеров в настоящее время могут использоваться текстовые файлы, исполняемые файлы, графические и звуковые файлы, а также графы [7]. Заполненный скрытой информацией контейнер называют стегоконтейнером. В стегосистеме,

* Работа выполнена в рамках госзадания СибГУТИ № 071-03-2024-008 от 19.01.2024.

предназначенной для скрытой передачи информации, противоборствующая сторона представлена пассивным нарушителем [1], который пытается установить факт применения стегосистемы, не воздействуя на стегоконтейнеры.

Отдельную значимую область занимает стеганография цифровых изображений. Внесение искажений в определенные данные изображений остаются незаметными для человека, в особенности при наличии некоторого шума квантования, свойственного оцифрованным объектам. Чаще всего информация встраивается в наименее значащие биты (LSB) элементов контейнера [8–10]. Особенный интерес представляют методы обратимого скрытия данных (RDH) в изображениях. Один из общих подходов к разработке стеганографических систем RDH состоит в применении методов интерполяции [11–16], позволяющих увеличить полезную нагрузку контейнера, сохраняя визуальное качество. Изображение интерполируется без изменения оригинальных пикселей, затем интерполированные пиксели используются для встраивания информации. Применяемые алгоритмы интерполяции в целях сокрытия данных исследуют с помощью показателей визуального искажения [17], выбирая наиболее оптимальный метод. Так, если значение показателя меры искажения изображения (PSNR) более 40 дБ, то качество обработки изображения считается высоким [18]. В [13] A. Tripathi и J. Prakash предложили новый подход к применению интерполяции изображений и достигли лучших значений индекса PSNR для полученного LSB-метода по сравнению с известными стегосистемами данного вида. Методы RDH особенно полезны при скрытии данных пациента в медицинских изображениях, а также в обеспечении конфиденциальности и целостности обрабатываемых данных интернета вещей (IoT), когда в качестве контейнера чаще всего используются цифровые изображения [19, 20].

Наряду с методами встраивания данных активно развиваются и методы раскрытия стеганографических систем [21], называемые стегоанализом. Под раскрытием стеганографической системы понимается нахождение ее уязвимости, которая позволяет определить факт скрытия информации в контейнере и возможность доказать данное утверждение третьей стороне с высокой степенью достоверности [1]. Один из простых и доступных методов обнаружения наличия встроенных данных для стеганографических систем LSB-замены – это метод визульной атаки, в котором отдельно рассматриваются младшие биты изображения. Более современные подходы к стегоанализу включают в себя модели оценки корреляций в изображениях [22], методы машинного обучения [23, 24] и сверточные нейронные сети [25, 26]. При разработке новых алгоритмов встраивания информации немаловажную роль играет применение универсальных методов стегоанализа к полученным контейнерам, но чаще всего исследования ограничиваются подсчетом показателя PSNR.

Цель данной работы заключается в построении RDH-стегосистемы для скрытия информации в младших битах растрового изображения, использующей кодирование встраиваемой информации в соответствии с оценками вероятностей появления значений младшего бита, что приблизит стегосистему к совершенной [27]. Для оценивания статистических свойств контейнера используется исходное растровое изображение, матрица пикселей которого разбивается на множество связных областей методом «лесного пожара» [28]. Затем исходное изображение интерполируется и добавленные пиксели используются для встраивания скрытой информации с учетом статистики младших бит по областям. Для получения последовательности заданного распределения целесообразно использовать арифметический декодер, а для восстановления встроенной информации – соответствующий арифметический кодер [29]. Разработанный метод может быть легко реализован на практике для большинства графических форматов данных, использующих неискажающие методы сжатия.

Для оценки разработанной системы, помимо показателей качества контейнеров, использующихся в большинстве работ по схожей тематике, применяется метод оценки визуального искажения, а также метод двойной статистики, полученной из пространственных корреляций в изображениях [22]. Это позволит более полно оценить результаты работы стегосистемы, выявить ее недостатки и определить дальнейшие пути улучшения стойкости к стегоанализу.

2. Материалы и методы

2.1. Общая схема предложенной стегосистемы

Рассмотрим алгоритм работы предлагаемой стегосистемы в общем виде. Исходными данными отправителя являются сообщение $\boldsymbol{M}$ и оригинальный контейнер $\boldsymbol{A}$. Сообщение представляет собой псевдослучайную битовую последовательность, которая имитирует зашифрованную информацию, предназначенную для хранения в контейнере. Оригинальный контейнер – это 8-битное bmp-изображение в оттенках серого (в данном случае размером 256 на 256 точек), представляющее собой информационную ценность при передаче. В данных исследованиях для формирования тестового набора контейнеров использовались 1000 изображений из базы данных BOSSBase vl.01 [30], содержащей файлы формата pgm размером 512 на 512 точек. Стандартными средствами изображения из базы были преобразованы в формат bmp для формирования набора **изображений-источников** и затем уменьшены до размера 256 на 256 точек для набора оригинальных контейнеров.

На первом шаге алгоритма в контейнере $\boldsymbol{A}$ определяются связные области, для каждой из которых происходит сбор статистики младших бит данного контейнера. Под связной областью изображения здесь понимается такая его область, в которой все точки имеют одинаковое значение признака и в которой между любыми двумя точками существует непрерывный путь точек данной области [28]. В представленной в данной работе стегосистеме области выделяются методом «лесного пожара» по признаку попадания в определенные диапазоны значений яркости. Таким образом, формируется большое количество наборов областей изображения со своим распределением.

На втором шаге применяется алгоритм интерполяции для оригинального контейнера $\boldsymbol{A}$, в результате которого создается контейнер-обложка $\boldsymbol{C}$ размером 512 на 512 точек, содержащий точки оригинального контейнера и интерполированные значения.

На третьем шаге происходит аналогичное выделение областей для интерполированных значений контейнера-обложки $\boldsymbol{C}$. Для каждой такой области используется собранная статистика младших бит соответствующей области оригинального контейнера $\boldsymbol{A}$, чтобы преобразовать сообщение $\boldsymbol{M}$ в код с заданным распределением вероятностей. Соответствующий код записывается в младшие биты каждой из выделенных областей контейнера-обложки $\boldsymbol{C}$ со своей статистикой, в результате чего создается стегоконтейнер $\boldsymbol{S}$ со встроенным сообщением (рис. 1).

Рис. 1. Схема встраивания сообщения $\boldsymbol{M}$ в контейнер $\boldsymbol{C}$

Для извлечения сообщения из $\boldsymbol{S}$ восстанавливается оригинальный контейнер $\boldsymbol{A}$, по которому определяется статистика младших бит по выделенным областям тем же способом, что и при встраивании. Затем $\boldsymbol{A}$ снова интерполируется, чтобы получить контейнер $\boldsymbol{C}$ без

встроенного сообщения для безошибочного определения соответствующих областей в $\boldsymbol{S}$. Далее с помощью полученного распределения вероятностей младших бит по областям контейнера $\boldsymbol{A}$ восстанавливается сообщение $\boldsymbol{M}$ из кода, находящегося в областях $\boldsymbol{S}$ (рис. 2).

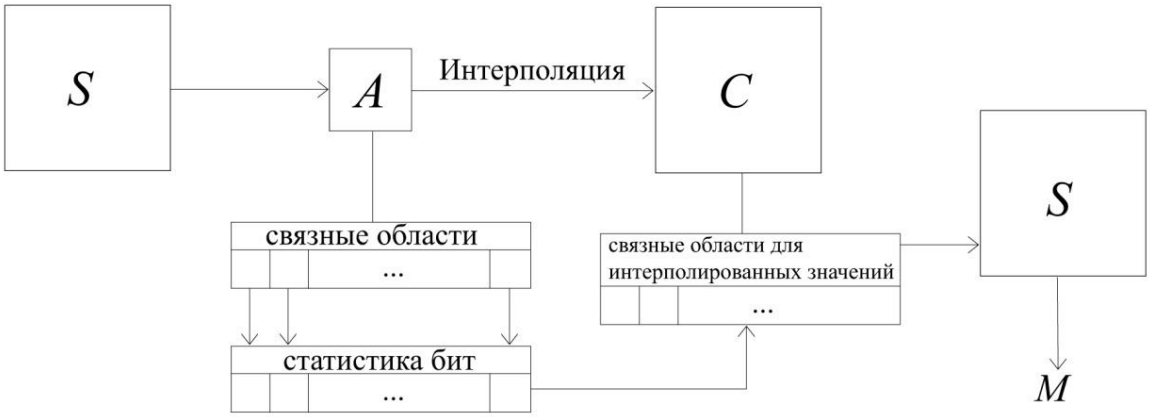


Рис. 2. Схема извлечения сообщения $\boldsymbol{M}$ из контейнера $\boldsymbol{S}$

Таким образом, контейнер $\boldsymbol{S}$ всегда содержит в себе пиксели оригинального контейнера $\boldsymbol{A}$, который сам по себе может иметь информационную нагрузку при передаче, являясь, например, произведением искусства, медицинским снимком или изображением с камеры умного дома.

2.2. Метод интерполяции

В представленной стегосистеме за основу может быть взят любой алгоритм интерполяции изображений. Критерием выбора алгоритма является показатель PSNR. Для того, чтобы его оценить, необходимо иметь источник оригинального контейнера того же размера, что и контейнер-обложка, полученный путем интерполяции оригинального изображения. Поэтому для оценки метода интерполяции используется тестовый набор изображений- источников, о которых шла речь в разд. 2.1. Заметим, что непосредственно в работе стегосистемы изображения-источники не принимают участия и используются только для оценки качества метода.

Исследования [31, 32] показали, что алгоритм INP [16] является наиболее оптимальным с точки зрения качества получаемого контейнера в стегосистемах RDH. В представленной в данной работе стегосистеме также применяется алгоритм интерполяции INP. Значения точек с координатами i и j контейнера-обложки $\boldsymbol{C}$ из оригинального изображения $\boldsymbol{A}$ размером m на n пикселей вычисляются по формуле:

$$C(i,j)=\begin{cases} A(i,j),\ i=2m,\ j=2n, \\ \dfrac{\left(A(i,j-1)+\left(\dfrac{A(i,j-1)+A(i,j+1)}{2}\right)\right)}{2},\ i=2m,\ j=2n+1, \\ \dfrac{\left(A(i-1,j)+\left(\dfrac{A(i-1,j)+A(i+1,j)}{2}\right)\right)}{2},\ i=2m+1,\ j=2n, \\ \dfrac{C(i-1,j)+C(i,j-1)}{2},\ \text{иначе.} \end{cases}. \quad (1)$$

Пример вычисления интерполированных значений на фрагменте некоторого изображения $\boldsymbol{A}$ показан на рис. 3. Серым цветом выделены значения контейнера $\boldsymbol{C}$, полученные по формуле (1).

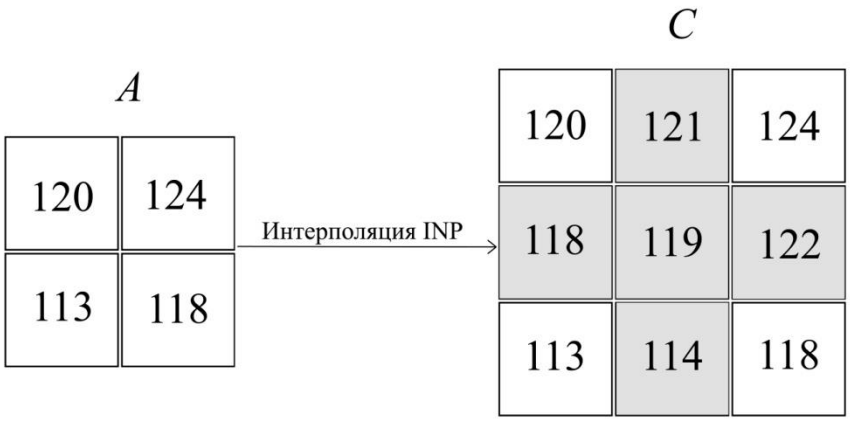


Рис. 3. Пример вычисления значений интерполяции

2.3. Оценка статистики младших бит

Известно, что существует статистическая зависимость младших бит от остальных элементов контейнера. Эта зависимость нарушается, если независимые данные будут записаны в младшие биты. В работе [33] ранее была предложена адаптивная статистическая модель, позволяющая оценить вероятности распределения младших бит в контейнере. С помощью оценки частотной энтропии были выявлены наиболее существенные элементы контекста, в наибольшей степени связанные с младшими битами. В качестве обучающей части была использована половина изображения-контейнера, выделенная в шахматном порядке. Но в настоящей работе мы используем метод интерполяции для отделения обучающей части изображения, что накладывает определенные условия на формирование контекста, так как каждая вторая строка не будет содержать обучающих данных для сбора статистики. В качестве обучающей матрицы для формирования статистики здесь используется оригинальное изображение $\boldsymbol{A}$, которое затем интерполируется.

Вероятности оцениваются по пикселям оригинального изображения, причем адаптивно к каждой конкретной области. Пространство состояний для оценки вероятностей определяется с учетом частотной энтропии: чем меньше величина энтропии, тем ближе статистическая модель к реальному источнику. Оптимальный контекст состоит из самых младших бит предыдущего и последующего пикселей, а также второго, третьего и четвертого младших бит из текущего пикселя. Заметим, что предыдущий и последующий пиксели в контейнере $\boldsymbol{C}$ относятся к матрице оригинального изображения $\boldsymbol{A}$, поэтому они остаются неизменными при встраивании информации, и их наименее значащие биты можно использовать при восстановлении статистики. Используемые биты текущего пикселя также остаются неизменными и используются при восстановлении статистики, так как информация будет записываться в наименее значащий бит интерполированных значений матрицы пикселей $\boldsymbol{C}$.

2.4. Метод получения заданного распределения

Наиболее эффективным приближенным решением задачи кодирования, преобразующего зашифрованное сообщение в поток бит с заданным распределением, является арифметическое декодирование [34]. Арифметическому декодеру указывается требуемое распределение вероятностей нуля и единицы для каждого следующего выходного символа, в соответствии с которым он воспроизводит этот символ, рассматривая зашифрованное сообщение как код, построенный ранее соответствующим арифметическим кодером. Чтобы восстановить

зашифрованное сообщение из его кода, применяется арифметический кодер, на вход которого подаются те же самые распределения вероятностей, что и декодеру.

Для оценки статистики младших бит и внедрения информации с учетом этой статистики, следуя схемам на рис. 1, 2, используется контейнер $\boldsymbol{A}$, пиксели которого являются «обучающей» частью контейнера $\boldsymbol{C}$ при внедрении и контейнера $\boldsymbol{S}$ при извлечении сообщения $\boldsymbol{M}$.

2.5. Метод выделения связных областей изображения

Ранее в подобных экспериментах был использован метод разделения изображения на связные области по яркостям. Всё изображение делилось на 16 связных областей по заданным диапазонам яркости. Но такой подход позволял собирать в одну область пиксели, которые могли находиться в разных частях изображения, что в определенных случаях искажало статистические свойства контейнера.

В данной работе использован стековый алгоритм прослеживания связных областей методом «лесного пожара» [28]. Идея данного метода состоит в том, что область «поджигается» в одной точке, а затем каждая «подожжённая» точка далее «поджигает» все соседние точки, имеющие ту же яркость. Сначала «поджог» начинается с левой верхней точки изображения. Каждая «подожжённая» точка имеет свою метку номера области и затем для формирования последующих областей точка нового «поджога» берется как следующая точка, не имеющая метки. В итоге мы получаем некоторое количество непересекающихся связных областей, для каждого изображения разное. Объем выжженной области может варьироваться от 1 до максимально возможного количества пикселей в картинке заданного размера. Важно учесть, что каждая полученная область будет использоваться для сбора статистики младших бит в определенном контексте, размер которого в данной работе составляет 5 элементов. Поэтому необходимо адаптировать метод выделения областей под данную задачу сбора статистики.

Типичное изображение-контейнер для встраивания данных представляет собой достаточно шумную оцифрованную фотографию. Если в методе лесного пожара каждая область будет выделяться по точному значению яркости, то мы получим огромное количество областей, большинство из которых будет содержать недостаточное количество пикселей для сбора представительной статистики. Поэтому в данной работе предлагается определять пиксели в ту или иную область по принципу попадания в общий диапазон значений для каждой области. Чем меньше разброс значений в диапазоне, тем больше количество областей и меньше их объем. Таким образом, необходимо установить наиболее эффективное значение диапазонов, при котором будет получено достаточное количество представительных областей для сбора статистики, позволяющих достигнуть наибольшей ёмкости метода встраивания.

Пусть R – это максимальная разность между пикселями в каждой выделяемой области. Тогда, например, при $R = 16$ пиксели изображения будут распределены на области из диапазонов: 0 – 16, 17 – 33, 34 – 50, 51 – 67, 68 – 84 и так далее. При $R = 8$ диапазоны будут: 0 – 8, 9 – 17, 18 – 26, 27 – 35, 36 – 44 и так далее. Заметим, что при любом значении R неизбежно будет встречаться некоторое количество мелких областей, которые не позволят сформировать статистику и при встраивании будут иметь скорее случайное распределение младших бит. В то же время большие области при встраивании информации будут иметь наиболее приближенное к истинному распределение вероятностей младших бит.

2.6. Используемые методы стегоанализа

Первое условие, которое выполняют все стеганографические программы, состоит в том, что искажения, вносимые в контейнер при внедрении сообщения, должны быть незаметны для человека. Так, даже при стопроцентном заполнении, т.е. при замене всех младших бит матрицы изображения, мы обычно не видим искажений, особенно если под рукой нет исходного файла для сравнения. Однако при помощи простого визуального метода стегоанализа легко

обнаружить замену младших бит. Для этого значения пикселей контейнера $\boldsymbol{S}$ преобразуются в соответствии с правилом:

$$S'(i,j)=\begin{cases}255, \text{ если } S(i,j)=1,\\ 0, \text{ если } S(i,j)=0,\end{cases} \tag{2}$$

где i, j – индексы текущего пикселя.

Далее методом визуальной оценки происходит сравнение общих контуров на изображении до и после преобразования. Так, при замене младших бит мы увидим случайный шум, а при сохранении корреляций в младших битах будут определяться общие контуры изображения.

В данной работе также применяется метод RS-анализа (Regular-Singular) для оценки стегостойкости полученного метода. Суть анализа заключается в поиске пространственных корреляций в контейнере: изображение разбивается на связные группы пикселей, для которых затем определяется вещественная функция гладкости:

$$f(G)=\sum_{i=1}^{n}\left|x_{i+1}-x_i\right|, \tag{3}$$

где G – это набор из n групп $x_1 \ldots x_n$ связных пикселей контейнера. Чем больше значение данной функции, тем более зашумленной является группа G. Затем моделируется обратимое добавление шума в группы, что увеличивает функцию гладкости в случае пустых контейнеров и усиливает всплески значений в заполненных контейнерах [26]. На основании результатов группы делятся на регулярные (regular) и сингулярные (singular), вычисляются их количественные характеристики, по которым строится график. На выходе получают предполагаемую длину встроенной в контейнер информации (L). Метод RS может указать небольшую ненулевую длину сообщения из-за случайных отклонений даже для пустого контейнера [22]. В работе [35] установлено, что при $L \geq 5$ RS-анализ классифицирует контейнер как заполненный.

В стеганографии задача классификации контейнеров сводится к выбору одной из двух гипотез: H_0 – контейнер является пустым и H_1 – контейнер имеет встроенную информацию. Но любые стегоалгоритмы могут ошибочно классифицировать контейнер. В связи с этим принято разделять ошибки на два рода: ошибка первого рода возникает, когда стегоаналитиком выбрана гипотеза H_1 при пустом контейнере (ложное срабатывание), и ошибка второго рода, когда выбрана гипотеза H_0 при заполненном контейнере (пропуск). Поэтому, прежде чем оценивать метод на устойчивость к обнаружению, необходимо определить долю ложных срабатываний для тестового набора пустых контейнеров.

Для оценки качества заполненных контейнеров в стеганографии также используется показатель максимального соотношения сигнал/шум (PSNR):

$$\text{PSNR} = 10 * \log \frac{255^2}{\varepsilon}, \tag{4}$$

где $\varepsilon = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}\left(S(i,j)-I(i,j)\right)^2$ – искажение, M, N – высота и ширина изображения соответственно. Чем больше значение PSNR, тем меньше расхождений между сравниваемыми изображениями.

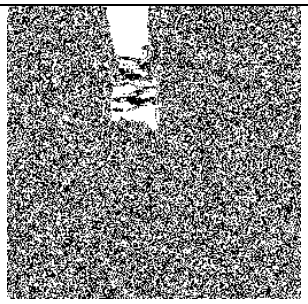
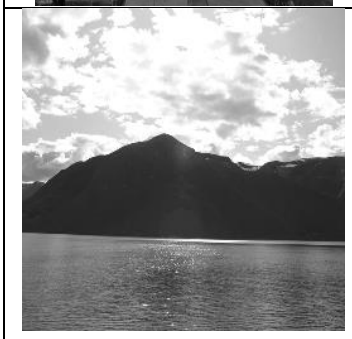
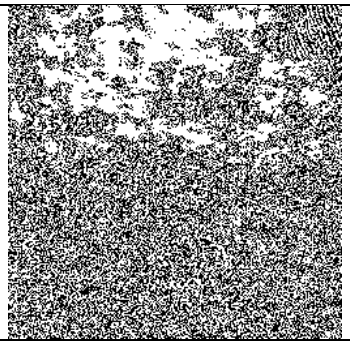
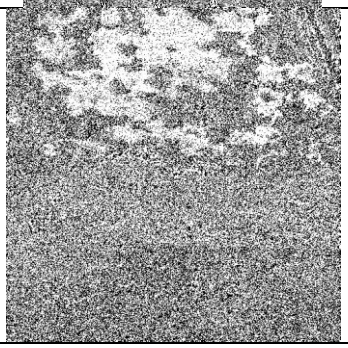
3. Результаты

Максимальная средняя ёмкость встраивания по предложенному в данной работе стеганографическому алгоритму составила 0.6 бит/пиксель при $R = 8$.

Визуальный метод анализа показал, что некоторые корреляции младших бит заметно сохраняются в заполненном контейнере. В табл. 1 показаны значения младших бит, следуя

формуле (2) для изображения-источника, для пустого интерполированного контейнера и для заполненного контейнера. Размеры представленных контейнеров: 512 на 512.

Таблица 1. Визуальный анализ младших бит

Источник	Источник $'$	Заполненный контейнер S'
		
		

Метод RS-анализа на наборе из 1000 пустых контейнеров-источников размером 512 на 512 показал ошибку первого рода 27 %. Для соответствующих заполненных контейнеров процент файлов, классифицированных как заполненные, составил 35 %, что говорит о 8 % раскрытых стегоконтейнеров.

Таблица 2. RS-анализ пустых и заполненных контейнеров

L	0	1–4	5 и более
Изображения-источники	16 %	57 %	27 %
Контейнеры S	9 %	56 %	35 %

Значения PSNR для нескольких тестовых контейнеров приведены в табл. 3. Данный показатель в разработанном методе свидетельствует о достаточно хорошем качестве полученных стегоконтейнеров и превосходит результат методов, основанных на интерполяции без использования статистики [11, 16, 12], в которых ёмкость встраивания составляла 0.4–0.9 бит/пиксель.

Таблица 3. PSNR контейнеров

Изображения-источники	Контейнеры S	PSNR	Бит/пиксель
		59	0.55
		65	0.57
		57	0.62
		61	0.59
		58	0.60

4. Обсуждение и заключения

Предложенная стеганографическая схема имеет более высокий показатель PSNR по сравнению с другими стеганографическими схемами, использующими методы интерполяции в RDH и при этом сохраняет корреляцию в младших битах контейнеров. Ёмкость встраивания для большинства контейнеров составляет 0.6 бит/пиксель, за исключением тех контейнеров, которые содержат большие однотонные области, в которых значение яркости идентично. Однотонные непрерывные области растягивают последовательность бит на выходе декодера, тем самым сокращая полезную нагрузку. Такие файлы легко исключить из набора контейнеров, так как даже визуально их несложно определить.

Анализ методом RS показал, что часть контейнеров уязвимы к стегоанализу, что указывает на необходимость более качественного учёта зависимостей в значениях младших бит изображения. В то же время полученный результат оказался лучше, чем предыдущий с разделением областей, что свидетельствует об эффективности применения метода «лесного пожара» для выделения связных областей. Некоторое искажение статистики младших бит в стегоконтейнере ожидаемо по причине неизбежного наличия мелких связных областей, не подходящих для сбора статистики. Таким образом, в дальнейшем планируется адаптировать данный алгоритм, используя мелкие связные области для встраивания с применением других стегометодов.

Литература

1. *Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.* Прикладная стеганография: для студентов, аспирантов, научных работников, изучающих вопросы обеспечения безопасности информации. Саров: Российский Федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики, 2021. 484 с.
2. *Ryabko B.* Unconditionally secure short key ciphers based on data compression and randomization // Designs, Codes, and Cryptography. 2023. V. 91, № 6. P. 2201–2212.
3. *Монарёв В. А., Фионов А. Н., Шокин Ю. И.* Обзор современных теоретико-информационных подходов к решению основных задач криптографии и стеганографии // Вычислительные технологии. 2010. Т. 15, № 2. С. 69–86.
4. *Tutuncu K., Çataltaş Ö.* Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach // Computer Science and Information Systems. 2021. V. 18, № 4. P. 1311–1332.
5. *Talasila S., Vijaya Kumar G., Vijaya Babu E., Nainika K., Veda Sahithi M., Mohan P.* The Hybrid Model of LSB-Technique in Image Steganography Using AES and RSA Algorithms // Soft Computing and Signal Processing. 2023. V. 840. P. 403–413.
6. *Rajabi-Ghaleh S., Olyaeefar B., Kheradmand R., Ahmadi-Kandjani S.* Image security using steganography and cryptography with sweeping computational ghost imaging // Frontiers in Physics. 2024. V. 12. № 1336795.
7. *Нечта И. В.* Цифровая стеганография в программах и текстовых файлах. М.: Горячая линия – Телеком, 2023. 112 с.
8. *Novanto F., Nugraha A., Kurniawan J., Prayogo A.* Optimizing Digital Image Steganography through Hybridization of LSB and Zstandard Compression // Sinkron. 2024. V. 9, № 1. P. 75–82.
9. *Wu W., Li H.* A novel scheme for random sequential high-capacity data hiding based on PVD and LSB // Signal, Image and Video Processing. 2023. V. 18. P. 2277–2287.
10. *Mali A., Dongre M.* Block Based Self-Secured LSB Embedding Scheme for Reversible Steganography // IOT with Smart Systems. 2023. V. 2. P. 625–635.

11. *Mohammad A., Al-Haj A., Farfoura M.* An improved capacity data hiding technique based on image interpolation // Multimedia Tools and Applications. 2018. V. 78, № 6. P. 7181–7205.
12. *Jung K., Yoo K.* Data hiding method using image interpolation // Computer Standards & Interfaces. 2009. V. 31, № 2. P. 465–470.
13. *Tripathi A., Prakash J.* Interpolation Based Reversible Data Hiding using Pixel Intensity Classes // International Journal of Next-Generation Computing. 2023. V. 14, № 4. P. 621–643.
14. *Punia R., Malik A., Singh S.* An interpolation-based reversible data hiding scheme for internet of things applications // Discover Internet of Things. 2023. V. 3, № 18.
15. *Mohammad A. A.* high quality interpolation-based reversible data hiding technique using dual images // Multimedia Tools and Applications. 2023. V. 82. P. 36713–36737.
16. *Lee C-F., Huang Y-L.* An efficient image interpolation increasing payload in reversible data hiding // Expert Systems with Applications. 2012. V. 39, № 8. P. 6712–6719.
17. *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография: теория и практика. Киев: МК–Пресс, 2006. 283 с.
18. *Kumari L., Ramanathan P., Rani J., Vinothkumar D., Sneha A., Amalarani V., Joe B.* Selection of optimum compression algorithms based on the characterization on feasibility for medical image // Biomedical Research. 2017. V. 28, № 13. P. 5633–5637.
19. *Евсютин О. О., Кокурина А. С., Мещеряков Р. В.* Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. 2019. Т. 43, № 1. P. 137–154.
20. *Kuri J., Rafi M.* Securing Data in Internet of Things (IoT) using Cryptography and Steganography Techniques // International Journal for Research in Applied Science & Engineering Technology. 2020. V. 8, № 7. P. 1933–1939.
21. *Шелухин О. И.* Стеганография. Алгоритмы и программная реализация. М.: Горячая линия – Телеком, 2017. 592 с.
22. *Fridrich J., Goljan M., Du R.* Reliable Detection of LSB Steganography in Grayscale and Color Images // Special Session on Multimedia Security and Watermarking. Ottawa, Canada, 2001. P. 27–30.
23. *Pevny T., Bas P., Fridrich J.* Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on Information Forensics and Security. 2010. V. 5, № 2. P. 215–224.
24. *Holub V., Fridrich J.* Random projections of residuals for digital image steganalysis // IEEE Transactions on Information Forensics and Security. 2013. V. 8, № 12. P. 1996–2006.
25. *Сирота А. А., Дрюченко М. А., Иванков А. Ю.* Стегоанализ цифровых изображений с использованием методов поверхностного и глубокого машинного обучения: известные подходы и новые решения // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2021. № 1. С. 33–52.
26. *Полунин А. А., Яндашевская Э. А.* Использование аппарата свёрточных нейронных сетей для стегоанализа цифровых изображений // Труды Института системного программирования РАН. 2020. Т. 32, № 4. С. 155–164.
27. *Ryabko B., Ryabko D.* Information-theoretic approach to steganographic systems // Proc. IEEE International Symposium on Information Theory, Nice, France, 2007. P. 2461–2464.
28. *Визильтер Ю. В., Желтов С. Ю., Бондаренко А. В., Ососков М. В., Моржин А. В.* Обработка и анализ изображений в задачах машинного зрения: курс лекций и практических занятий. М.: Физматкнига, 2010. 672 с.
29. *Said A.* Introduction to Arithmetic Coding – Theory and Practice. Hewlett-Packard Laboratories Report. USA, 2004. 64 p.
30. База BOSS изображений для исследований методов стеганографии [сайт]. URL: `http://agents.fel.cvut.cz/boss/index.php?mode=VIEW& tmpl=about` (дата обращения: 26.03.2024).
31. *Mahasree M.* Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy // International Journal of Emerging Trends in Engineering Research. 2020. V. 8. P. 3495–3501.

32. *Lu T.-C., Lin M.-C., Huang C.-C., Deng K.-M.* Reversible Data Hiding Based on Image Interpolation with a Secret Message Reduction Strategy // International Journal of Computer Software Engineering. 2016. V. 1. P. 124–130.
33. *Eltysheva K., Fionov A.* Stegosystem construction on the basis of statistical structure of covertext // Proc. XII International Symposium on Problems of Redundancy, St.-Petersburg, May 26–30, 2009. P. 180–185.
34. *Рябко Б. Я., Фионов А. Н.* Эффективный метод адаптивного арифметического кодирования для источников с большими алфавитами // Проблемы передачи информации. 1999. Т. 35, № 4. С. 1–14.
35. *Жилкин М. Ю.* Теоретико-информационные методы стегоанализа графических данных: дис. … канд. тех. наук: 05.12.13. Сиб. гос. ун-т телекоммуникаций и информатики, Новосибирск, 2009. 153 с.

Мерзлякова Екатерина Юрьевна
к.т.н., доцент кафедры прикладной математики и кибернетики, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 272, e-mail: katerina.artist@yandex.ru, ORCID ID: 0000-0001-6847-5588.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Construction of the RDH Stegosystem Based on the Statistical Properties of Image Areas

Ekaterina Yu. Merzlyakova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: This article discusses the reversible data hiding (RDH) method for raster images. The statistical properties of the container are taken into account by dividing the image into coherent regions using a wildfire method and collecting statistics of the least significant bits to form an embedded sequence with a given distribution. The INP interpolation method is used to divide the image into a part for collecting statistical properties of the container and a part for embedding information. Obtaining a sequence of bits with a given distribution is provided by an arithmetic decoder. The constructed stegosystem has an embedding capacity of 0.6 bits/pixel. RS steganalysis is carried out on the basis of BOSS_v1.01 images and the properties of the resulting containers are assessed based on visual distortion indicators.

Keywords: steganography, digital images, information embedding, interpolation, steganalysis.

For citation: Merzlyakova E. Yu. Construction of the RDH stegosystem based on the statistical properties of image areas. 2024 (in Russian). *Vestnik SibGUTI*, 2024, vol. 18, no. 2, pp. 113-126. https://doi.org/10.55648/1998-6920-2024-18-2-113-126.

The article was submitted: 28.04.2024;
revised version: 02.05.2024;
accepted for publication 19.05.2024.

References

1. Gribunin V. G., Kostyukov V. E., Martynov A. P., Nikolaev D. B., Fomchenko V. N. *Prikladnaya steganografiya: dlya studentov, aspirantov, nauchnykh rabotnikov, izuchayushchikh voprosy obespecheniya bezopasnosti informatsii* [Applied steganography: for students, graduate students, researchers studying information security issues]. Sarov, Rossiiskii Federal'nyi yadernyi tsentr - Vserossiiskii nauchno-issledovatel'skii institut eksperimental'noi fiziki, 2021, 484 p.
2. Ryabko B. Unconditionally secure short key ciphers based on data compression and randomization. *Designs, Codes, and Cryptography*, 2023, vol. 91, no. 6, pp. 2201-2212.
3. Monarev V. A., Fionov A. N., Shokin Yu. I. Obzor sovremennykh teoretiko-informatsionnykh podkhodov k resheniyu osnovnykh zadach kriptografii i steganografii [Review of modern information-theoretic approaches to solving basic problems of cryptography and steganography]. *Vychislitel'nye tekhnologii*, 2010, vol. 15, no. 2, pp. 69-86.
4. Tutuncu K., Çataltaş Ö. Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. *Computer Science and Information Systems*, 2021, vol. 18, no 4, pp. 1311-1332.
5. Talasila S., Vijaya Kumar G., Vijaya Babu E., Nainika K., Veda Sahithi M., Mohan P. The Hybrid Model of LSB-Technique in Image Steganography Using AES and RSA Algorithms. *Soft Computing and Signal Processing*, 2023, vol. 840, pp. 403–413.
6. Rajabi-Ghaleh S., Olyaeefar B., Kheradmand R., Ahmadi-Kandjani S. Image security using steganography and cryptography with sweeping computational ghost imaging. *Frontiers in Physics*, 2024, vol.12, no. 1336795.
7. Nechta I. V. *Tsifrovaya steganografiya v programmakh i tekstovykh failakh* [Digital steganography in programs and text files]. Moscow, Goryachaya liniya, Telekom, 2023, 112 p.
8. Novanto F., Nugraha A., Kurniawan J., Prayogo A. Optimizing Digital Image Steganography through Hybridization of LSB and Zstandard Compression. *Sinkron*, 2024, vol. 9, no. 1. pp. 75-82.
9. Wu W., Li H., A novel scheme for random sequential high-capacity data hiding based on PVD and LSB. *Signal, Image and Video Processing*, 2023, vol. 18, pp. 2277-2287.
10. Mali A., Dongre M. Block Based Self-Secured LSB Embedding Scheme for Reversible Steganography. *IOT with Smart Systems*, 2023, vol. 2, pp. 625-635.
11. Mohammad A., Al-Haj A., Farfoura M. An improved capacity data hiding technique based on image interpolation. *Multimedia Tools and Applications*, 2018, vol. 78, no. 6, pp. 7181-7205.
12. K. Jung, K. Yoo. Data hiding method using image interpolation. *Computer Standards & Interfaces*, 2009, vol. 31, no. 2, pp. 465-470.
13. Tripathi A., Prakash J. Interpolation Based Reversible Data Hiding using Pixel Intensity Classes. *International Journal of Next-Generation Computing*, 2023, vol. 14, no. 4, pp. 621-643.
14. Punia R., Malik A., Singh S. An interpolation-based reversible data hiding scheme for internet of things applications. *Discover Internet of Things*, 2023, vol. 3, no. 18.
15. Mohammad A. A. High quality interpolation-based reversible data hiding technique using dual images. *Multimedia Tools and Applications*, 2023, vol. 82, pp. 36713-36737.
16. Lee C-F., Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding. *Expert Systems with Applications*, 2012, vol. 39, no. 8, pp. 6712-6719.
17. Konakhovich G. F., Puzyrenko A. Yu. *Komp'yuternaya steganografiya: teoriya i praktika* [Computer steganography: theory and practice]. Kyiv: MK-Press, 2006, 283 p.
18. Kumari L., Ramanathan Pandian., Rani J., Vinothkumar D., Sneha A., Amalarani V., Joe B. Selection of optimum compression algorithms based on the characterization on feasibility formedical image. *Biomedical Research*, 2017, vol. 28, no. 13, pp. 5633-5637.
19. Evsyutin O. O., Kokurina A. S., Meshcheryakov R. V., Obzor metodov vstraivaniya informatsii v tsifrovye ob"ekty dlya obespecheniya bezopasnosti v «internete veshchei» [Review of methods for embedding information into digital objects to ensure security in the Internet of Things]. *Komp'yuternaya optika*, 2019, vol. 43, no. 1, pp.137-154.
20. Kuri J., Rafi M. Securing Data in Internet of Things (IoT) using Cryptography and Steganography Techniques. *International Journal for Research in Applied Science & Engineering Technology*, 2020, vol. 8, no. 7, pp. 1933-1939.
21. Shelukhin O. I. *Steganografiya. Algoritmy i programmnaya realizatsiya* [Steganography. Algorithms and software implementation]. Moscow, Goryachaya liniya - Telekom, 2017, 592 p.

22. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Grayscale and Color Images. *Special Session on Multimedia Security and Watermarking*. Ottawa, Canada, 2001, pp. 27-30.
23. Pevny T., Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 2010, vol. 5, no. 2, pp. 215-224.
24. Holub V., Fridrich J. Random projections of residuals for digital image steganalysis. *IEEE Transactions on Information Forensics and Security*, 2013, vol. 8, no. 12, pp. 1996-2006.
25. Sirota A. A., Dryuchenko M. A., Ivankov A. Yu. Stegoanaliz tsifrovykh izobrazhenii s is-pol'zovaniem metodov poverkhnostnogo i glubokogo mashinnogo obucheniya: izvestnye podkhody i novye resheniya [Steganalysis of digital images using shallow and deep machine learning methods: known approaches and new solutions]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyi analiz i informatsionnye tekhnologii*, 2021, no. 1, pp. 33-52.
26. Polunin, A. A., Yandashevskaya E. A. Ispol'zovanie apparata svertochnykh neironnykh setei dlya stegoanaliza tsifrovykh izobrazhenii [Using convolutional neural networks for steganalysis of digital images]. *Trudy Instituta sistemnogo programmirovaniya RAN*, 2020, vol. 32, no 4, pp. 155-164.
27. Ryabko B., Ryabko D. Information-theoretic approach to steganographic systems. *IEEE International Symposium on Information Theory.* Nice, France, 2007, pp. 2461-2464.
28. Vizil'ter Yu. V., Zheltov S. Yu., Bondarenko A. V., Ososkov M.V., Morzhin A.V. *Obrabotka i analiz izobrazhenii v zadachakh mashinnogo zreniya: kurs lektsii i prakticheskikh zanyatii* [Image processing and analysis in computer vision problems: a course of lectures and practical exercises]. Moscow, Fizmatkniga, 2010, 672 p.
29. Said A. Introduction to Arithmetic Coding – Theory and Practice. *Hewlett-Packard Laboratories Report*, USA, 2004, p. 64.
30. *Baza BOSS izobrazhenii dlya issledovanii metodov steganografii* [BOSS Image Database for Steganography Research], available at: `http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=about` (accessed 26.03.2024).
31. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy. *International Journal of Emerging Trends in Engineering Research*, 2020, vol. 8, pp. 3495-3501.
32. Lu T.-C., Lin M.-C., Huang C.-C., Deng K.-M. Reversible Data Hiding Based on Image Interpolation with a Secret Message Reduction Strategy. *International Journal of Computer Software Engineering*, 2016, vol. 1, pp.124-130.
33. Eltysheva K., Fionov A. Stegosystem construction on the basis of statistical structure of covertext. *XII International Symposium on Problems of Redundancy*, St.-Petersburg, 26-30 May, 2009, pp. 180-185.
34. Ryabko B. Ya., Fionov A. N. Effektivnyi metod adaptivnogo arifmeticheskogo kodirovaniya dlya istochnikov s bol'shimi alfavitami [An Efficient Adaptive Arithmetic Coding Method for Sources with Large Alphabets]. *Problemy peredachi informatsii*, 1999, vol. 35, no. 4, pp. 1-14.
35. Zhilkin M. Yu. *Teoretiko-informatsionnye metody stegoanaliza graficheskikh dannykh* [Information-theoretic methods for steganalysis of graphical data]. Ph. D. thesis. Novosibirsk, 2009, 153 p.

Ekaterina Yu.Merzlyakova

PhD (Engineering), Docent of the Department of Applied Mathematics and Cybernetics, Siberian State University of Telecommunications and Informatition Science (SibSUTIS, 630102, Novosibirsk, Kirova str., 86), tel. +7 383 2698 272, e-mail: `katerina.artist@yandex.ru`, ORCID ID: 0000-0001-6847-5588.