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 17, № 4, 2023

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 20.12.2023. 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: 10.55648/1998-6920-2023-17-4-3-14 УДК 681.84

Анализ искажений современных высокочастотных излучателей звука

М. С. Шушнов, Т. В. Шушнова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье проведено сравнение нелинейных и линейных искажений современных динамических головок купольного типа и ленточного излучателя. Даны рекомендации по подбору высокочастотных головок для построения мониторной акустической системы ближнего поля. Выполнена постановка оптимизационной задачи отбора серийных экземпляров или моделей высокочастотных излучателей звука.

Ключевые слова: звук, психоакустика, искажения, купольная головка, динамическая головка, ленточный излучатель, аудиосистема, мониторная система, оптимизация.

Для цитирования: Шушнов М. С., Шушнова Т. В. Анализ искажений современных высокочастотных излучателей звука // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 3–14. https://doi.org/10.55648/1998-6920-2023-17-4-3-14.

Статья поступила в редакцию 09.04.2023;
принята к публикации 27.04.2023.

1. Введение

Актуальность анализа нелинейных и линейных искажений современных высокочастотных (ВЧ) излучателей купольного и ленточного типов стоит перед проектировщиком акустической системы, если целью проектирования является разработка технического решения, позволяющего слышать нюансы (недостатки) записи. Для звукорежиссера в процессе выполнения трудовых функций необходимо слышать неискаженную звуковую картину с хорошо заметными недостатками фонограммы. Поэтому при построении мониторной акустической системы субъективные критерии оценки качества звуковоспроизведения, такие как прозрачность, разборчивость, являются важными, а объективные характеристики, например, рабочий диапазон частот и коэффициент гармоник, часто не принимаются во внимание, поскольку являются малоинформативными.

Однако благодаря выявленным в профессиональной среде звукорежиссеров зависимостям между психоакустическими критериями и объективными электрическими характеристиками можно сделать вывод о необходимости снижения уровня гармонических искажений с целью получения «прозрачного», достоверного звука и недопущения превышения уровня нечетных гармоник над уровнем четных, так как в противном случае снижается разборчивость звуковоспроизведения [1–4], получения максимально ровной амплитудно-частотной характеристики для исключения перекоса тонального баланса.

2. Основные особенности и параметры современных высокочастотных излучателей звука

2.1. Ленточные излучатели

В ленточном динамике звуковая катушка и излучатель являются одним целым – проводящей лентой. Излучатель в ленточном исполнении – токопроводящая лента из металла (чаще всего применяется алюминий) толщиной от 5 до 50 мкм, находящаяся между мощными магнитами. Через ленту пропускается переменный ток, что приводит к ее колебаниям и излучению звуковой волны за счет эффективной площади ленты. Таким образом, основное отличие ленточного излучателя заключается в отсутствии «посредников» между звуковой катушкой и излучателем, малой массе ленты и позволяет воспроизводить тончайшие звуковые нюансы, что отмечается слушателями как «прозрачность», «легкость», «голографичность».

Однако лента имеет очень низкое сопротивление – порядка десятков мОм. Для согласования низкого сопротивления ленты с выходом УМЗЧ применяется понижающий трансформатор, благодаря которому входное сопротивление динамика Z_{HOM} на рабочих частотах становится равным часто используемому номиналу 4–8 Ом.

Понижающий трансформатор обычно устанавливается внутри корпуса ленточного излучателя, из-за чего на самых низких частотах входное сопротивление ленточного излучателя с понижающим трансформатором очень мало и определяется в основном сопротивлением первичной обмотки трансформатора, которое находится в пределах 0.1–0.3 Ом. Понижающий трансформатор может вносить линейные и нелинейные искажения, поэтому его качество определяет частично качественные характеристики ленточного излучателя.

На рис. 1 показана кривая импеданса ленточного излучателя SRT-7 российской компании Viawave [5]. Кривая импеданса показывает, что в рабочем диапазоне входное сопротивление ленточного излучателя (с понижающим трансформатором) составляет единицы ом. Из рис. 1 хорошо видно, что на частотах ниже 1800 Гц импеданс Z_{HOM} имеет подъем, связанный с резонансной частотой ленточного излучателя, с дальнейшим резким спадом до значения около 1 Ом. В пределах рабочего диапазона частот (1800–30000 Гц) импеданс Z_{HOM} находится в пределах 6.5–12 Ом, что соответствует среднему номинальному значению 8 Ом. При работе в составе многополосной акустической системы ленточный излучатель необходимо отделять от выхода УМЗЧ по постоянному току, даже если УМЗЧ работает в составе с активным фильтром высоких частот (ФВЧ). В противном случае низкое сопротивление ленточного излучателя по постоянному току (по рис. 2 – около 1 Ом) может вызвать ложное срабатывание системы защиты выходного каскада УМЗЧ от перегрузки по току. В качестве разделительного элемента удобно использовать конденсатор, который может образовывать пассивный ФВЧ, либо использовать УМЗЧ с резисторно-конденсаторной связью с ленточным излучателем.

Следует отметить, что рост Z_{HOM} в области ВЧ на рис. 1 свидетельствует об индуктивном характере входного сопротивления ленточного излучателя из-за влияния индуктивности первичной обмотки понижающего трансформатора.

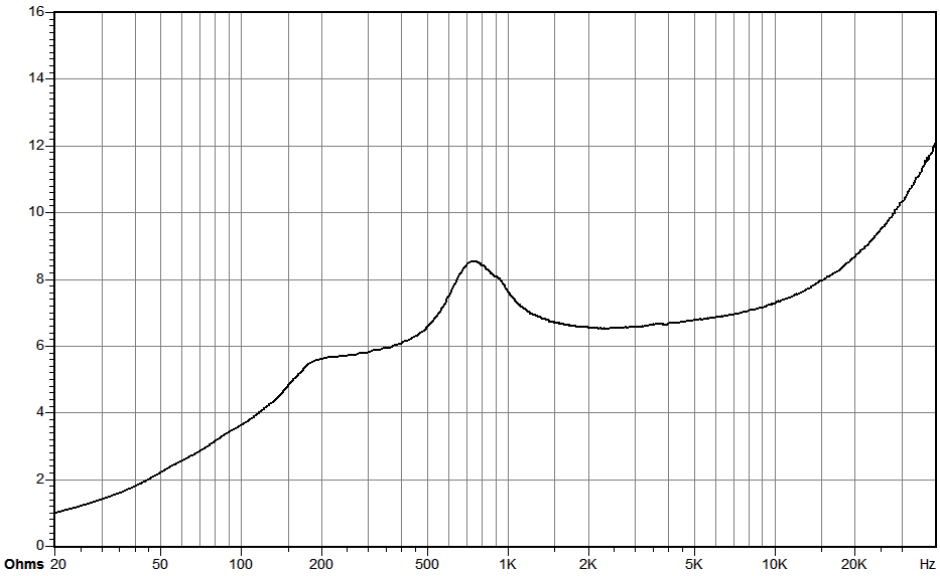

Рис. 1. Импеданс ленточного излучателя SRT-7 [5]

Производитель в [5] указывает на значение индуктивности L_E, равное 0.034 мГн, что хорошо согласуется с данными графика на рис. 1. Следует заметить, что индуктивность обычно приводит к снижению отдачи в области ВЧ и вызывает спад АЧХ (или неравномерность АЧХ ΔSPL) ленточного излучателя, хотя не является определяющей в формировании АЧХ.

В справочных данных на SRT-7 [5] (рис. 2) производитель приводит графики гармонических искажений по 2-й (H2) и 3-й (H3) гармонике.

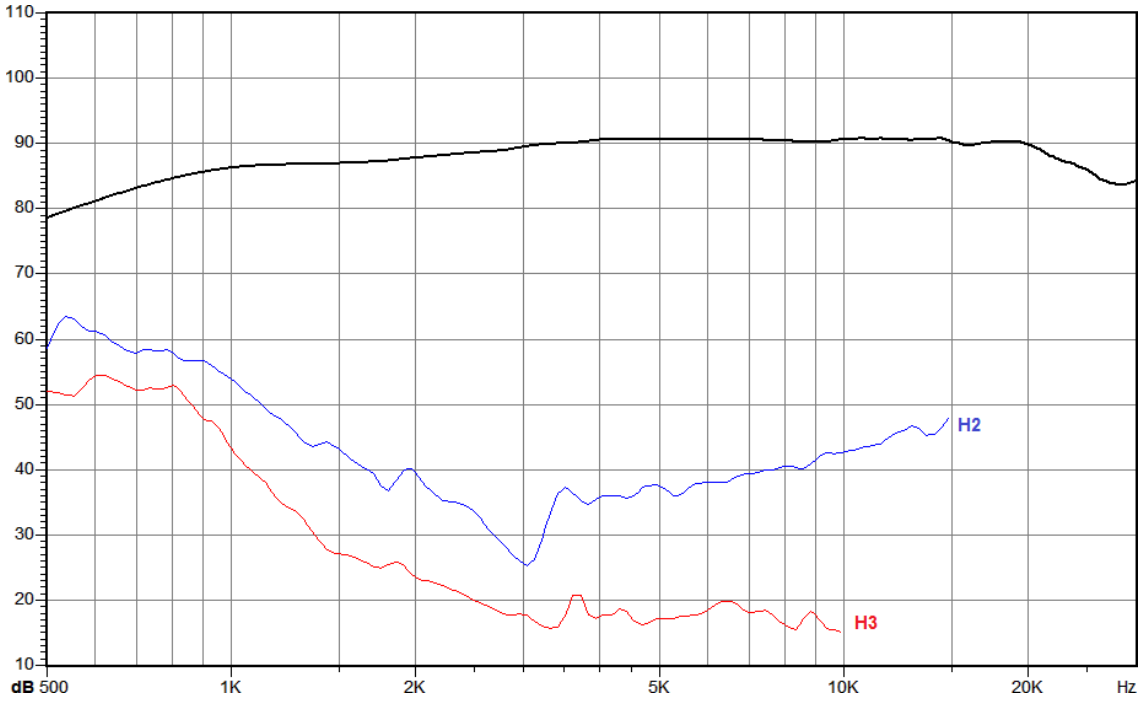

Рис. 2. Гармонические искажения в зависимости от частоты для SRT-7 при уровне звукового давления 90 дБ/м [5]

В рабочем диапазоне частот SRT-7 значение 2-й гармоники находится на уровне не более 43 дБ/м, а 3-й – не более 6 дБ/м. Чтобы определить привычные для понимания коэффициенты гармоник воспользуемся формулой пересчета:

$$K_{Г2} = \frac{U_2}{U_1}100\% = \frac{10^{SPL_2/20}}{10^{SPL_1/20}}100\%, \quad K_{Г3} = \frac{U_3}{U_1}100\% = \frac{10^{SPL_3/20}}{10^{SPL_1/20}}100\%, \qquad (1)$$

где U_1, U_2, U_3 – амплитуды напряжения 1-й, 2-й, 3-й гармоник; SPL_1, SPL_2, SPL_3 – уровни звукового давления по 1-й, 2-й и 3-й гармоникам.

В результате пересчета на средней частоте рабочего диапазона частот ВЧ-излучателя SRT-7 (7–10 кГц) получим значения $K_{Г2}$ = 0.46 % и $K_{Г3}$ = 0.007 %. Легко заметить, что $K_{Г3}$ находится на границе разрешающей способности современного измерительного оборудования и, скорее всего, определяется шумовой полкой измерительного комплекса (измерительного микрофона). Уровень $K_{Г2}$ низок и находится на уровне ниже замечаемого человеческим слухом предела. Следует предположить, что уровни гармонических искажений при повышении громкости будут пропорционально расти, а преобладающей останется 2-я гармоника. Учитывая номинальную мощности SRT-7 17 Вт, достижимый уровень SPL будет равен $95+10\lg(17)=107$ дБ, что не превышает комфортного уровня прослушивания 105–107 дБ. В то же время при длительной работе стандарт DIN15905-3 устанавливает допустимый уровень громкости не более 90 дБ. Такой уровень соответствует справочным значениям, рассчитанным выше по (1). Поскольку $K_{Г2}$ и $K_{Г3}$ SRT-7 ниже замечаемого предела в 0.5–2 %, то субъективная оценка звучания SRT-7 будет как «нейтральное», «неокрашенное», «мониторное», что соответствует [1] и подходит для задачи мониторинга звукового сигнала.

2.2. Купольные излучатели

Сегодня наиболее распространенным среди ВЧ-головок является купольный диффузор. Он может быть мягким (из текстиля, например шелка с пропиткой) или жестким – из металла или керамики. Конструкция типичного ВЧ-динамика отличается не только размером диффузора.

Купольные диффузоры, которые могут быть выпуклыми или, реже, вогнутыми, изготавливаются прессованием из натуральных или синтетических тканей с обязательной последующей пропиткой. Всё большее распространение получают диффузоры ВЧ-головок из синтетических полимерных пленок или металлической фольги. Для повышения жесткости диффузоры изготавливают методом осаждений из паровой фазы различных материалов: бора, бериллия и др. Существуют многочисленные примеры купольных диффузоров из керамики, которая, по сути, является окислом металлов, например, алюминия.

Подкупольное пространство часто заполнено звукопоглотителем для снижения влияния подкупольных отражений. Поскольку подкупольное пространство мало, то резонансная частота купольной головки может оказаться высокой. Для снижения резонансной частоты купольного ВЧ-излучателя применяется система звуковых каналов, расположенных в керне магнитной системы (полый керн или полый керн с присоединенным заглушенным объемом – акустической камерой). Также применяется метод снижения добротности резонанса купольного ВЧ-излучателя и индуктивности звуковой катушки. Для этого внутрь звуковой катушки помещается короткозамкнутый виток: крепится медное кольцо на керн магнитной системы или каркас звуковой катушки выполняется из алюминиевой фольги.

Таким образом, основное отличие купольного излучателя заключается в наличии «прямого» привода между звуковой катушкой и излучателем. Поскольку масса подвижной системы будет определяться материалом каркаса звуковой катушки, проводом обмотки и купола, то воспроизведение тончайших звуковых нюансов может осуществляться по-разному для разных моделей купольных ВЧ-головок. Звук купольных ВЧ-головок слушателями часто оценивается как «прозрачный», «мягкий», «объемный».

Звуковая катушка купольного ВЧ-динамика имеет сопротивление порядка единиц ом. Купольный ВЧ-излучатель можно подключить непосредственно к выходу УМЗЧ.

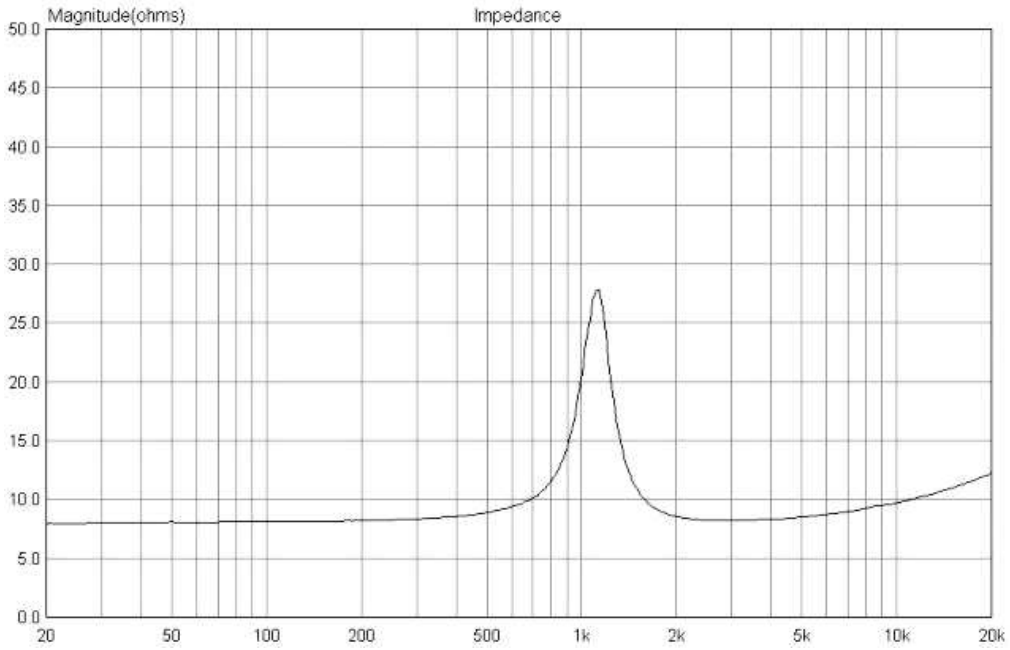

Рис. 3. Импеданс купольного ВЧ-излучателя T26.8 [6]

На рис. 3 показана кривая Z_{HOM} купольного ВЧ-динамика T26.8 производства российской компании АСА лаб [6]. Из рис. 3 видно, что на частотах ниже 2000 Гц импеданс имеет подъем, связанный с резонансной частотой купольного излучателя, с дальнейшим резким спадом до значения около 7 Ом. В пределах рабочего диапазона частот (2000–20000 Гц) импеданс Z_{HOM} находится в пределах 7–12 Ом, что соответствует среднему номинальному значению 8 Ом. При работе в составе многополосной акустической системы купольный ВЧ излучатель допустимо не отделять от выхода УМЗЧ по постоянному току. В качестве разделительного элемента можно использовать активный ФВЧ на входе УМЗЧ либо пассивный ФВЧ на выходе УМЗЧ, необходимый для ограничения рабочего диапазона частот ВЧ-излучателя.

Следует отметить, что рост импеданса Z_{HOM} в области ВЧ на рис. 3 имеет примерно такой же характер, как для ленточного излучателя на рис. 2. Характер сопротивления купольной динамической ВЧ-головки так же индуктивный из-за индуктивности звуковой катушки.

Производитель в [6] указывает на значение индуктивности L_E, равное 0.041 мГн, что хорошо согласуется с данными графика на рис. 3. Следует заметить, что индуктивность обычно приводит к снижению отдачи в области ВЧ и вызывает спад АЧХ (или неравномерность АЧХ) купольного излучателя.

Стоит заметить, что чем меньше изменение импеданса ΔZ_{HOM} в диапазоне рабочих частот, тем потенциально ниже неравномерность АЧХ излучателя.

В справочных данных на T26.8 [6] (рис. 4) производитель приводит графики гармонических искажений по 2-й (D2), 3-й (D3), 4-й (D4) и др. гармоникам.

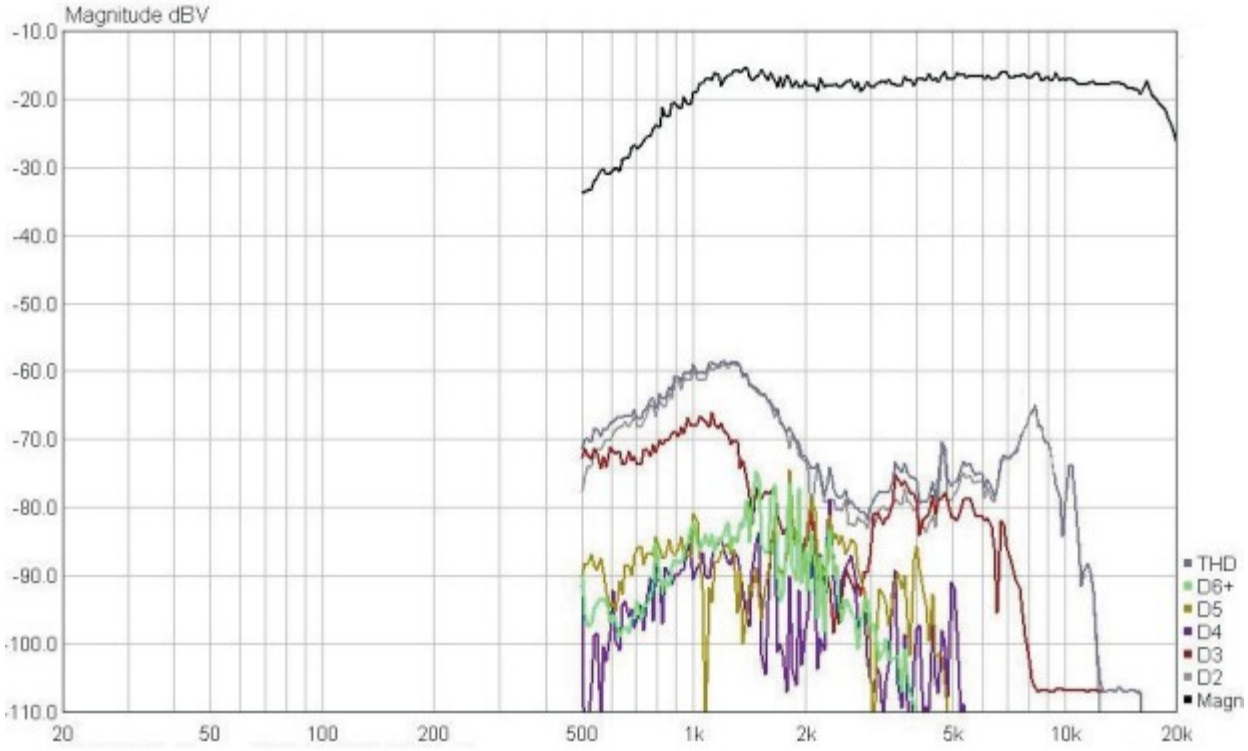

Рис. 4. Гармонические искажений от частоты для T26.8 при уровне звукового давления 90 дБ/м [6]

В рабочем диапазоне частот T26.8 относительно среднего уровня при измерениях -8 дБВ значение 2-й гармоники находится на уровне не более -57 дБВ, а 3-й – не более -74 дБВ. Чтобы определить привычные для понимания коэффициенты гармоник, воспользуемся формулой пересчета (1).

В результате пересчета на средней частоте рабочего диапазона частот ВЧ-излучателя T26.8 (7–10 кГц) получим значения $K_{Г2} = 0.0013$ % и $K_{Г3} = 0.000025$ %. Вклад более высоких гармоник незначителен и их можно не учитывать. Уровень $K_{Г2}$ низок и находится ниже замечаемого человеческим слухом предела. Следует предположить, что уровни гармонических искажений при повышении громкости будут пропорционально расти, а преобладающей останется 2-я гармоника. Учитывая номинальную мощности T26.8, равную 100 Вт, достижимый уровень SPL будет равен $95+10\lg(100)=110$ дБ, что превышает комфортный уровень прослушивания, составляющий 105–107 дБ. При уровне громкости не более 90 дБ значения $K_{Г2}$ и $K_{Г3}$ купольного ВЧ-динамика T26.8 будут ниже, чем у ленточного SRT-7, то есть еще ниже замечаемого предела в 0.5–2 %. Субъективная оценка звучания T26.8 будет такая же, как и для SRT-7: «нейтральное», «неокрашенное», «мониторное». Из анализа полученных данных можно сделать вывод, что T26.8 тоже подходит для задачи мониторинга звукового сигнала.

Следует отметить, что в случае с T26.8 имеется небольшой запас (110 – 107 = 3 дБ) по перегрузке по сравнению с SRT-7. Запас по перегрузке важен в студийной работе, для исключения выхода из строя динамической головки при резком увеличении уровня громкости (такие ситуации нередки в студийной практике). Но SRT-7 обладает большей чувствительностью – 95 дБ/Вт против 90 дБ/Вт для T26.8, что снижает требования к выходной мощности УМЗЧ в 3 раза.

3. Анализ АЧХ ВЧ-излучателей

В соответствии с правилами объективной оценки качества звуковоспроизведения сравним АЧХ ленточного излучателя SRT-7 (рис. 5) и купольного ВЧ-динамика T26.8 (рис. 6).

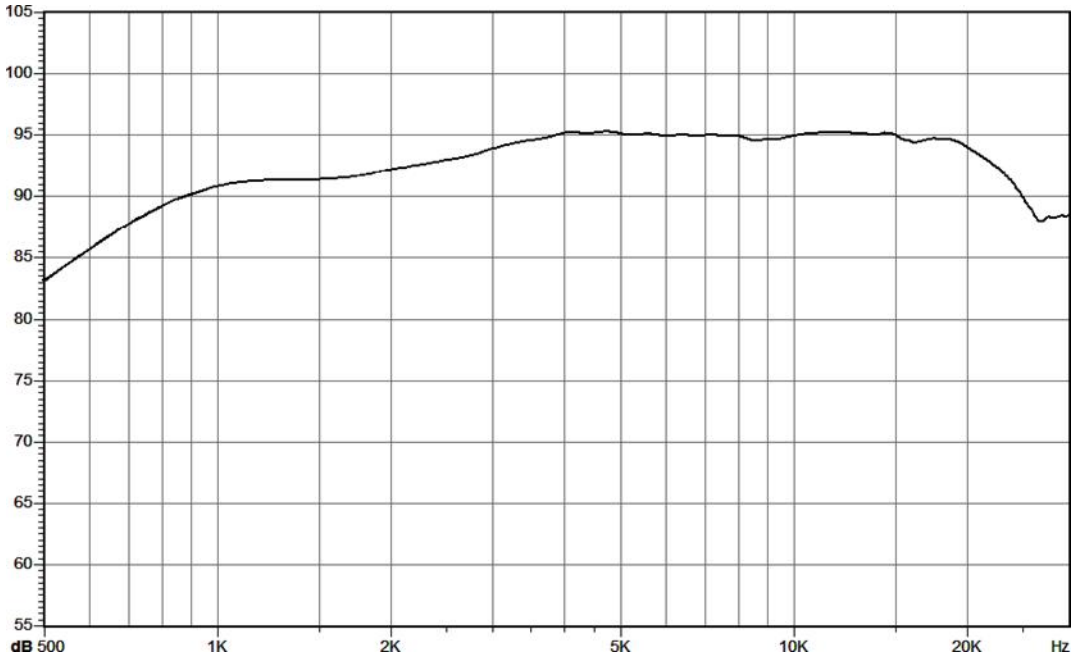

Рис. 5. АЧХ ленточного излучателя SRT-7 в горизонтальной плоскости при уровне звукового давления 90 дБ/м [5]

В пределах диапазона частот 2000–20000 Гц в направлении главной оси неравномерность АЧХ (ΔSPL) излучателя SRT-7 не превышает 3 дБ. В том же диапазоне частот купольная ВЧ-головка T26.8 имеет неравномерность АЧХ не более 5 дБ. Большая неравномерность АЧХ T26.8, скорее всего, связана с большей массой подвижной системы головки и большей индуктивностью звуковой катушки по сравнению с ленточным излучателем SRT-7.

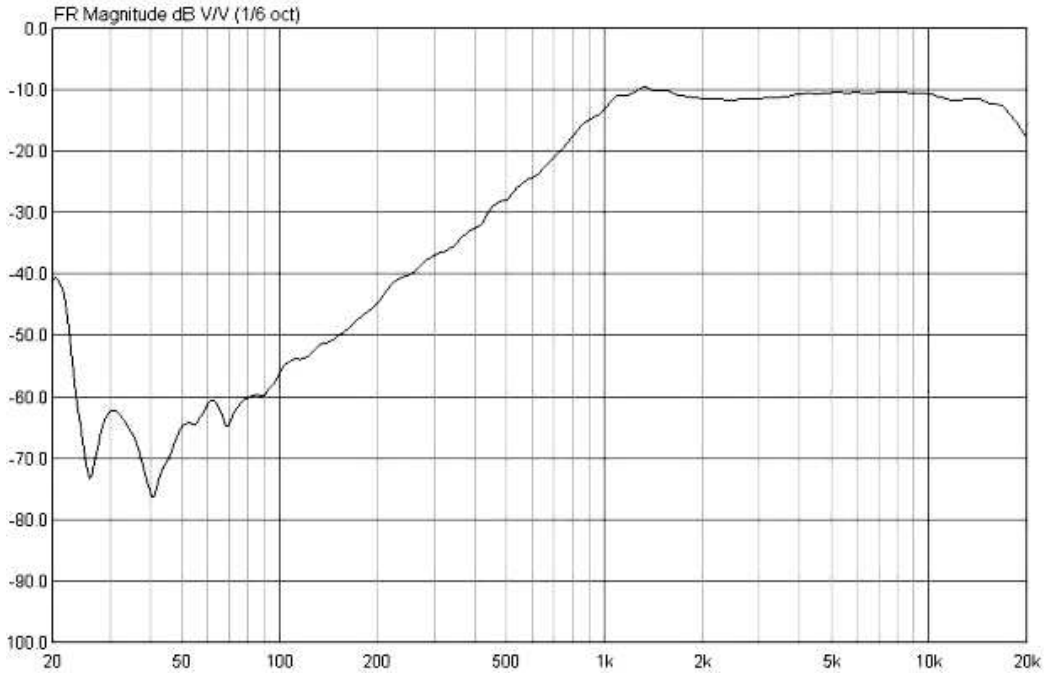

Рис. 6. АЧХ купольной ВЧ-головки T26.8 со сглаживанием 1/6 октавы при уровне звукового давления 90 дБ/м [6]

Следует заметить, что в конструкции T26.8 отсутствует короткозамкнутое кольцо в магнитной системе, снижающее индуктивность звуковой катушки, применен цельный керн и отсутствует акустическая камера за керном. Например, аналогичная по размеру купола динамическая ВЧ-головка с шелковым куполом H1149-06 27TDC [7] производства норвежской компании SEAS при большей индуктивности звуковой катушки (0.05 мГн) имеет неравномерность АЧХ в пределах диапазона частот 2000–20000 Гц не более 4 дБ. В конструкции H1149-06 27TDC применен полый керн с присоединенным заглушенным объемом акустической камеры и особый мягкий подвес, что позволило снизить резонансную частоту головки и массу подвижной системы Mms (H1149-06 27TDC имеет Mms 0.25 гр, а T26.8 – 1.25 гр.). Снизить неравномерность АЧХ T26.8 можно путем снижения массы подвижной системы за счет применения более тонкого материала купола, изменения конструкции подвеса, путем намотки звуковой катушки более легким проводом (алюминием) или с помощью модификации состава для пропитки текстильного купола. В ассортименте компании АСА лаб имеется модель купольной ВЧ динамической головки T280.8 [8], конструкция подкупольного пространства которой схожа с H1149-06 27TDC, но неравномерность АЧХ все же не удалось уменьшить, хотя рабочий диапазон частот был расширен в области ВЧ за счет применения алюминиевого каркаса звуковой катушки.

4. Оптимизационная задача поиска оптимальных экземпляров (моделей) высокочастотных излучателей звука

Поскольку при производстве высокочастотных излучателей имеет место технологический разброс электрических характеристик, различные модели излучателей имеют отличающиеся электрические характеристики, то существует задача поиска оптимальных экземпляров (моделей) высокочастотных излучателей.

Для решения задачи поиска оптимальных экземпляров высокочастотных излучателей для построения мониторной акустической системы можно воспользоваться методами математического моделирования.

Для формулировки оптимизационной задачи в рамках данной статьи необходимо учитывать только основные свойства и пренебрегать второстепенными.

В разделах 2 и 3 рассматривались три основных параметра в пределах диапазона рабочих частот излучателя: ΔSPL – неравномерность АЧХ; $K_{Г2}$ – величина 2-й гармоники; $K_{Г3}$ – величина 3-й гармоники; ΔZ_{HOM} – девиация номинального импеданса. При поиске оптимума по справочным данным вместо ΔZ_{HOM} будем использовать значение L_E.

При решении оптимизационной задачи необходимо обеспечить поиск оптимальных [10, 11] излучателей, характеризующихся величиной:

$$V = \Delta SPL \cdot K_{Г2} \cdot K_{Г3} \cdot \Delta Z_{HOM}. \quad (2)$$

Величина V определяется требованиями к допустимым значениям параметров в проекте ΔSPL, $K_{Г2}$, $K_{Г3}$ и ΔZ_{HOM}, тогда в решении используется значение V_0:

$$V_0 = \Delta SPL \cdot K_{Г2} \cdot K_{Г3} \cdot \Delta Z_{HOM}. \quad (3)$$

Поскольку значимость параметров может отличаться, то можно задать величину S через коэффициенты значимости K_i, где i – номер параметра:

$$S = K_1 \Delta SPL + K_2 K_{Г2} + K_3 K_{Г3} + K_4 \Delta Z_{HOM}. \quad (4)$$

Запишем постановку оптимизационной задачи в виде:

$$\begin{cases} F = S \to \min \\ V = V_0 \end{cases}, \tag{5}$$

где F – целевая функция; V – ограничение.

Тогда

$$\begin{cases} F = K_1 \Delta SPL + K_2 K_{Г2} + K_3 K_{Г3} + K_4 \Delta Z_{HOM} \to \min \\ \Delta SPL \cdot K_{Г2} \cdot K_{Г3} \cdot \Delta Z_{HOM} = V_0 \end{cases}. \tag{6}$$

В (6) очевидно, что ΔSPL, $K_{Г2}$, $K_{Г3}$ и $\Delta Z_{HOM} > 0$, и с учетом психоакустических свойств необходимо выполнить условие $K_{Г2} \geq K_{Г3}$. После введения в (6) граничных условий получим математическую модель:

$$\begin{cases} F = K_1 \Delta SPL + K_2 K_{Г2} + K_3 K_{Г3} + K_4 \Delta Z_{HOM} \to \min \\ \Delta SPL \cdot K_{Г2} \cdot K_{Г3} \cdot \Delta Z_{HOM} = V_0 \\ \Delta SPL, K_{Г2}, K_{Г3}, \Delta Z_{HOM} > 0 \text{ и } K_{Г2} \geq K_{Г3} \end{cases}. \tag{7}$$

Поскольку из (7) видно, что система имеет бесконечное множество решений, то имеется оптимальное решение, то есть существуют оптимальные экземпляры излучателей.

Сбор исходных данных для реализации математической модели (7) – необходимый этап работы при поиске оптимального решения. Осуществляться сбор может в процессе конвейерного производства на этапе контроля качества продукции путем проведения необходимых и достаточных измерений ΔSPL, $K_{Г2}$, $K_{Г3}$ и ΔZ_{HOM} и составления таблицы соответствия серийного номера изделия его параметрам. Для поиска (отбора) оптимальных экземпляров можно воспользоваться табличным редактором Excel, реализовав в нем алгоритм (7). При выполнении опытно-конструкторских работ на этапе поиска подходящих моделей ВЧ-излучателей исходные данные могут быть представлены в виде усредненных параметров. Для этого потребуется собрать на начальном этапе работы небольшое количество исходных данных для быстрой оценки правильности составленной модели, что тоже возможно сделать в Excel.

Отобранные экземпляры (модели) ВЧ-излучателей, удовлетворяющие (7), могут быть применены в конструкции мониторной акустической системы только после анализа полученного результата решения разработчиком, так как в ряде случаев в (7) могут быть учтены не все важные параметры, тогда (7) необходимо дополнять.

5. Заключение

Несмотря на некоторую технологическую отсталость высокочастотных излучателей российского производства, построение мониторной акустической системы ближнего поля с неравномерностью АЧХ в области ВЧ не хуже, чем у зарубежных аналогов, видится возможным. Так, популярная и недорогая модель активных мониторов производства Yamaha модели HS7 имеет неравномерность АЧХ в диапазоне частот 2000–20000 кГц не более 4–5 дБ [9]. Российские ВЧ-излучатели имеют схожие параметры неравномерности АЧХ, правда еще до учета неравномерности АЧХ, вносимой УМЗЧ и активным ФВЧ.

Характер подачи звукового материала сравниваемых в данной статье динамических головок STR-7 и T26.8 при оценке по психоакустическим критериям должен обеспечить возможность мониторинга звукового сигнала благодаря «нейтральной» подаче.

Для сохранения характера подачи необходимо на следующем этапе проектирования контролировать спектр искажений УМЗЧ и активного ФВЧ. Результирующие звуковые характе-

ристики мониторной акустической системы станет возможно оценить лишь после изготовления опытного образца.

Решение оптимизационной задачи поиска подходящих (оптимальных) экземпляров (моделей) ВЧ-излучателей по (7) в процессе производства или анализ по усредненным паспортным характеристикам значительно сократит сроки разработки на этапе опытно-конструкторских работ и снизит процент брака при массовом производстве продукции.

Литература

1. *Keeports D.* The warm, rich sound of valve guitar amplifiers. Physics Education. 52. 025010. 2017. DOI:10.1088/1361-6552/aa57b7.
2. *Li J.* Using Transistors to Emulate Vacuum Tube Sound Quality Based on Asymmetric Cycle Harmonic Injection Method. 752-753. 2019. DOI:10.1109/GCCE46687.2019.9015619.
3. *Bech S. and Zacharov N.* Perceptual Audio Evaluation – Theory, Method, and Application. John Wiley & Sons Ltd, 2006. DOI:10.1002/9780470869253.
4. *Раковский В. В.* Измерения в аппаратуре записи звука кинофильмов. М.: Искусство, 1962. 405 с.
5. Viawave SRT-7 sealed ribbon tweeter. «Viawave Audio» LLC, Russia, Petrozavodsk, 2019. URL: http://viawave.ru/files/SRT-7.pdf (дата обращения: 08.04.2023).
6. T26.8. Излучатель динамический высокочастотный. URL: http://www.asalab.net/sites/default/files/image/T/t26/t26_8/t26_8.pdf (дата обращения: 08.04.2023).
7. H1149-06 27TDC SEAS. URL: http://www.seas.no/images/stories/prestige/pdfdatasheet/h1149_27tdc_datasheet.pdf (дата обращения: 08.04.2023).
8. T280.8. Излучатель динамический высокочастотный. URL: http://www.asalab.net/sites/default/files/image/T/t28/t280/t280.8.pdf (дата обращения: 08.04.2023).
9. Yamaha HS-series. Powered speaker system Owner's Manual. URL: https://ru.yamaha.com/files/download/other_assets/4/793644/hs8i_en_om_c0.pdf (дата обращения: 08.04.2023).
10. *Корбут А. А., Финкельштейн Ю. Ю.* Дискретное программирование. М.: Наука, 1969. 368 с.
11. *Леонова Н. Л.* Задачи линейного программирования и методы их решения: учебно-методическое пособие. СПб.: ВШТЭ СПбГУПТД, 2017. 75 с.

Шушнов Максим Сергеевич

кандидат технических наук, доцент, заведующий кафедрой цифрового телерадиовещания и систем радиосвязи, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), e-mail: efemerian@gmail.com, ORCID ID: 0000-0002-1713-5177.

Шушнова Татьяна Владимировна

старший преподаватель кафедры цифрового телерадиовещания и систем радиосвязи, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), e-mail: t.shushnova@gmail.com, ORCID ID: 0009-0006-9977-1818.

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.*

Distortions Analysis of Modern Audio Tweeters

Maxim S. Shushnov, Tatiana V. Shushnova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: Nnonlinear and linear distortions of modern dome-type tweeters and ribbon emitters are considered in this article. Recommendations for the selection of high -frequency heads for constructing a near -field monitor system are given. The statement of the optimization problem was carried out with the aim of selecting audio tweeters and ribbon emitters models or serial specimen.

Keywords: sound, psychoacoustics, distortion, dome tweeter, dynamic tweeter, ribbon emitter, audio system, monitor system, optimization.

For citation: Shushnov M. S., Shushnova T. V. Distortions analysis of modern audio tweeters (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 3-14. https://doi.org/10.55648/1998-6920-2023-17-4-3-14.

The article was submitted: 09.04.2023;
accepted for publication 27.04.2023.

References

1. Keeports, David. The warm, rich sound of valve guitar amplifiers. *Physics Education.* 52. 025010. 2017. DOI:10.1088/1361-6552/aa57b7.
2. Li, Jerry. Using Transistors to Emulate Vacuum Tube Sound Quality Based on Asymmetric Cycle Harmonic Injection Method. *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, 2019, pp. 752-753. DOI:10.1109/GCCE46687.2019.9015619.
3. Soren Bech and Nick Zacharov. *Perceptual Audio Evaluation – Theory, Method, and Application*, John Wiley & Sons Ltd. 2006. DOI:10.1002/9780470869253.
4. Rakovskii V. V. *Izmereniya v apparature zapisi zvuka kinofil'mov* [Measurements in the technique of recording of the sound of films]. Moscow, Isskustvo, 1962. 405 c.
5. Viawave SRT-7 sealed ribbon tweeter. «Viawave Audio» LLC, Russia, Petrozavodsk, 2019, available at: http://viawave.ru/files/SRT-7.pdf (accessed 08.04.2023.)
6. T26.8. *Izluchatel' dinamicheskiy vysokochastotnyy* [The dynamic high –frequency radiator], available at: http://www.asalab.net/sites/default/files/image/T/t26/t26_8/t26_8.pdf (accessed: 08.04.2023.)
7. H1149-06 27TDC SEAS, available at: http://www.seas.no/images/stories/prestige/pdfdatasheet/h1149_27tdc_datasheet.pdf (accessed: 08.04.2023 г.)
8. T280.8. *Izluchatel' dinamicheskiy vysokochastotnyy* [The dynamic high –frequency radiator], available at: http://www.asalab.net/sites/default/files/image/T/t28/t280/t280.8.pdf (accessed: 08.04.2023.)
9. *Yamaha HS-series. Powered speaker system Owner's Manual*, available at: https://ru.yamaha.com/files/download/other_assets/4/793644/hs8i_en_om_c0.pdf (accessed: 08.04.2023.)
10. Korbut A. A., *Finkel'shein U.U. Diskretnoye programmirovaniye* [Discrete programming]. Moscow, Nauka, 1969. 368 p.

11. Leonova N. L. *Zadachi lineynogo programmirovaniya i metody ikh resheniya: uchebno-metodicheskoye posobiye* [Tasks of linear programming and methods for their solutions: a training manual]. Saint Petersburg, Vysshaya shkola tekhnologii i energetiki Sankt-Peterburgskogo gosudarstvennogo universiteta promyshlennykh tekhnologii i dizaina, 2017. 75 p.

Maxim S. Shushnov

Cand. of Sci. (Engineering), Associate Professor, Head of the Department of Digital Television, Radio Broadcasting and Radio Communication Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), e-mail: efemerian@gmail.com, ORCID ID: 0000-0002-1713-5177.

Tatiana V. Shushnova

Senior lecturer of the Department of Digital Television, Radio Broadcasting and Radio Communication Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), e-mail: t.shushnova@gmail.com, ORCID ID: 0009-0006-9977-1818.

DOI: 10.55648/1998-6920-2023-17-4-15-33 УДК 519.25

Структурная модель оценки квалификации ИТ-специалистов на основе интеллектуального анализа данных информационных систем

Э. И. Гаврильев, Т. В. Авдеенко

Новосибирский государственный технический университет (НГТУ)

Аннотация: Ключевыми факторами достижения успеха проекта ИТ-организации являются персонал и его профессиональные качества. Для выявления направлений карьерного роста руководство организаций проводит перманентное оценивание квалификации сотрудников. Однако низкий уровень надежности и точности результатов оценивания, связанный с субъективным мнением руководителей, может привести к негативным последствиям принимаемых на его основе решений. Для повышения точности результатов и выявления дополнительных критериев профессиональной компетентности были разработаны модели оценки квалификации разработчиков и тестировщиков ПО для поддержки принятия решений на основе большого количества показателей, полученных при помощи интеллектуального анализа данных информационных систем, в которых работают ИТ-специалисты. В настоящей работе был проведен факторный анализ для выявления структуры пространства показателей и обнаружения в них скрытых закономерностей. Результаты показали, что при оценивании квалификации ИТ-специалистов руководители учитывают факторы, связанные с решением технических задач, результативностью и оперативностью тестирования, а также коммуникативными навыками.

Ключевые слова: оценка персонала, разработчик, тестировщик, исследовательский факторный анализ, подтверждающий факторный анализ, интеллектуальный анализ данных.

Для цитирования: Гаврильев Э. И., Авдеенко Т. В. Структурная модель оценки квалификации ИТ-специалистов на основе интеллектуального анализа данных информационных систем // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 15–33. https://doi.org/10.55648/1998-6920-2023-17-4-15-33.

Статья поступила в редакцию 29.04.2023;
переработанный вариант – 14.05.2023;
принята к публикации 15.05.2023.

1. Введение

Инновации в ИТ-области считаются определяющими факторами изменений в экономической и социальной сферах. Например, информатизация и автоматизация могут существенно поменять процессы и индивидуальные профили должностей во многих отраслях, например, в здравоохранении [1].

Технологические инновации влияют также и на саму ИТ-индустрию: рост сложности разрабатываемых информационных систем, а также широкий спектр автоматизируемых областей требуют от ИТ-организаций специалистов с высоким уровнем профессиональной компетентности. В связи с этим особую актуальность приобретает система профессионального развития сотрудников. Её важным элементом является оценка персонала, на основе ко-

торой принимается множество управленческих решений: повышение, понижение, перевод кадров, расторжение трудового договора.

Оценка квалификации сотрудников чаще всего базируется на субъективном мнении руководителей. Этот способ подвергается критике из-за низкого уровня надежности и точности [2–4]. Некорректная оценка сотрудника может негативно повлиять на его дальнейшее профессиональное развитие.

В предыдущих работах авторов [5, 6] для повышения точности и выявления дополнительных критериев профессиональной компетентности тестировщиков и разработчиков ПО были разработаны система поддержки принятия решений (СППР), процедура и модели оценивания квалификации. Модели оценивания включали большое количество показателей из информационных систем, в которых работают ИТ-специалисты, что увеличивает длительность и трудоемкость процесса оценивания. Поэтому целью данной работы является упрощение процедуры оценивания и повышение её точности за счет применения методов факторного анализа.

Настоящая работа состоит из следующих разделов. В разделе 2 описаны результаты анализа актуальных работ, связанных с методами и критериями оценивания квалификации ИТ-специалистов. В разделе 3 представлен подход к исследованию и описаны особенности организации, в рамках которой проводилось исследование. Раздел 4 содержит результаты исследования и их интерпретацию, и последний раздел – заключение.

2. Обзор актуальных работ

Вопрос оценивания квалификации разработчиков чаще всего рассматривался со стороны технических навыков и знаний, в основном связанных с программированием [7, 8]. Несмотря на это, часть исследований предоставляет целостное видение их компетенций, объединяющее технические и гибкие навыки.

В исследовании [9] был проведен опрос сотрудников Microsoft о характеристиках «великого» разработчика ПО. На основе результатов опроса было выделено 54 атрибута, классифицированных по 4 группам: «Личностные характеристики», «Принятие решений», «Работа с командой» и «Программный продукт». Наиболее высокий уровень важности получили атрибуты, связанные с разработкой ПО, а также индивидуальными способностями самого разработчика – например, обращение внимания на качество исходного кода, наличие достаточных умственных способностей для решения комплексных задач и хорошая осведомленность о заказчиках и продуктах компании.

В работе [10] представлена концептуальная теория компетентности в области разработки программного обеспечения (SDExp), основанная на ответах опроса 355 разработчиков ПО и литературе по тематике экспертных знаний и производительности труда. Было отмечено, что результативность разработчика зависит от уровня его знаний и опыта, а также ряда индивидуальных особенностей.

Следует отметить, что существующие публикации, изучающие методы оценивания квалификации разработчиков, в основном сфокусированы на программировании [11]. Однако они могут оказаться неэффективными при оценивании квалификации в целом, поскольку разработчики диверсифицировали свою деятельность по другим направлениям: сбор и анализ требований, тестирование, проектирование и т.д.

Подходы к оцениванию квалификации тестировщиков ПО рассматривались в литературе довольно фрагментарно, в отличие от подходов к оцениванию квалификации разработчиков ПО. Часть имеющихся публикаций изучает требования к тестировщикам для трудоустройства [12, 13]. Например, они должны уметь управлять процессом тестирования, писать тест-кейсы и разрабатывать автотесты. Другая часть работ рассматривает знания и навыки «эффективных» и «хороших» тестировщиков [14, 15]. В них упоминаются коммуникативные навыки, технические навыки (программирование, администрирование операционных систем)

и навыки тестирования, однако отсутствуют убедительные свидетельства того, что эти характеристики можно использовать при оценивании квалификации сотрудника.

В целом в имеющихся исследованиях не проанализированы методы, которые можно применить для оценивания навыков и знаний тестировщика. Метод, основанный на субъективном мнении непосредственного руководителя, может предоставить некорректные результаты ввиду следующих факторов: наличие особенностей во взаимоотношениях между руководителем и подчиненным; высокая требовательность руководителя; эффект края, при котором учитывается только последняя неделя работы и т.д.

Однако в отдельных публикациях для оценивания результатов деятельности ИТ-специалистов применяется интеллектуальный анализ данных из репозиториев проектов, над которыми они работали [16]. В них было продемонстрировано, что специалист с большим уровнем вклада в проект может иметь более высокий уровень «качества».

Из анализа имеющейся литературы можно заключить, что метод оценивания сотрудника, основанный на использовании данных из систем, в которых он работает, отличается более высоким уровнем объективности, чем мнение непосредственного руководителя, т.к. в основе этого метода лежат количественно измеряемые показатели и данные, соответствующие действительности.

3. Процедура сбора данных для оценки квалификации ИТ-специалистов

В своей ежедневной работе ИТ-специалисты используют системы контроля версий, управления задачами, управления тестированием и управления знаниями [17]. Система контроля версий (Version Control System) предназначена для фиксирования изменений в исходном коде приложения [18]. Система управления задачами (Issue Tracking System) используется для организации совместной деятельности проектной команды [19]. В этой системе проекты декомпозированы на задачи, например: исправление дефекта или проектирование интерфейса. Система управления тестированием (Test Management System) используется для администрирования и контроля процессов тестирования, разработки и хранения тест-кейсов и тест-планов [20]. Система управления знаниями (Knowledge Management System) применяется для поддержки создания, хранения и передачи знаний [21]. В ней, например, содержится проектная и техническая документация.

Информацию из этих систем можно обработать при помощи методов и инструментов интеллектуального анализа данных, чтобы оценить уровень квалификации ИТ-специалиста. На основе обзора актуальных работ были выделены показатели для расчета оценки профессиональных навыков и знаний тестировщиков и разработчиков. Например, информация из системы управления задачами используется для расчета показателей, связанных с оперативностью решения задач:

– среднее количество решенных задач в день;

– среднее количество задач, решенных в рамках и вне рамок оценки;

– количество созданных задач с типом «Ошибка» с приоритетами «Blocker», «Critical», «Major», «Minor».

Данные из системы управления тестированием используются для расчета показателей производительности разработки тест-кейсов:

– количество созданных тест-кейсов;

– среднее количество шагов в тест-кейсах;

– количество выполненных тестов в статусах «Пройден», «Заблокирован», «Провален» и «Не запускался».

Информация из системы контроля версий используется для расчета показателей комплексности написанного исходного кода:

– уровень поддерживаемости кода;

– цикломатическая сложность;

– меры сложности Холстеда.

Сведения из системы управления задачами используются для расчета показателей активности сотрудника, таких как количество созданных страниц и количество обновлений содержимого страниц.

Для проведения исследований был разработан прототип системы поддержки принятия решений на Node.js [5]. Прототип СППР состоит из двух подсистем: подсистемы загрузки данных из внешних систем и подсистемы оценивания сотрудника. Первая подсистема проводит миграцию информации из указанных выше систем в конце календарного дня, а вторая подсистема выполняет саму процедуру оценивания.

Разработанные СППР и реализованные в них модели принятия решений были внедрены в компанию среднего размера, которая разрабатывает ПО для банковской отрасли. Для разработки программных продуктов компании используется собственный low-code конструктор приложений. Оценивание профессиональных знаний и навыков сотрудников проводится непосредственными руководителями на основе 8 балльной шкалы, где 1 – это минимальное значение, а 8 – максимальное. Atlassian Jira используется как система управления задачами, Atlassian Confluence – как система управления знаниями, TestLink – как система управления тестированием, а в качестве системы контроля версий выступает собственный конструктор приложений.

После выполнения первичных расчетов и анализа результатов был проведен ряд интервью с ведущими специалистами и руководителями компании для корректировки набора показателей оценки. В результате для оценки квалификации тестировщиков был добавлен ряд показателей [22]:

– показатели оценки качества отчета о дефекте: индексы удобочитаемости описания дефекта, наличие фактического и ожидаемого результатов;

– показатели, связанные с результатом решения зарегистрированного дефекта: процент задач, решенных с резолюциями «Решено», «Не могу воспроизвести», «Дубликат»;

– показатели оценки производительности тестирования: среднее время тестирования задачи в минутах, среднее количество проверенных задач в день;

– показатели, относящиеся к менторству новых сотрудников: количество подключений к менторству, количество успешно закрытых стажировок.

Для оценки квалификации разработчиков были добавлены:

– показатели для подсчета количества объектов, разработанных в конструкторе приложений: количество форм, функций, процессов, SQL-запросов и т.д.;

– показатели для подсчета применяемых элементов языка программирования: количество применений Java-библиотек, функций для интеграции через JDBC- и HTTP-протоколы, функций для генерации запросов в форматах XML и JSON;

– показатели для подсчета упоминаний применяемых инструментов и технологий, а также типов решаемых задач.

Для подсчета количества упоминаний был использован инструмент Томита-парсер, который проводит обработку текстов на естественном языке и извлекает из них факты с учетом синтаксиса языка и морфологии [23]. Факты извлекаются из описаний задач, комментариев и журналов работ по задачам, а для их извлечения были подготовлены наборы ключевых слов, в которых перечислены различные варианты формулировок факта.

Например, для извлечения упоминаний XSD и WSDL в описаниях задач были подготовлены 2 правила, на основе которых парсер ищет согласованные по падежу слова, одно из которых должно упоминаться в наборе ключевых слов (Рис. 1).

```
// поиск XSD
S -> Word<c-agr[1]>* Word<kwset=[xsd], c-agr[1], rt> interp (DevTechXSD.Term::not_norm);

// поиск WSDL
S -> Word<c-agr[1]>* Word<kwset=[wsdl], c-agr[1], rt> interp (DevTechWSDL.Term::not_norm);
```

Рис. 1. Примеры правил для извлечения фактов

Составленные наборы ключевых слов могут включать в себя названия технологий и инструментов на английском и русском языках (Рис. 2).

```
TAuxDicArticle wsdl
{
    key = "wsdl"
    key = "всдл"
}

TAuxDicArticle xsd
{
    key = "xsd"
    key = "хсд"
}
```

Рис. 2. Пример словаря ключевых слов

В итоге для оценки профессиональных знаний и навыков тестировщика было выделено 50 показателей, а для оценки разработчика – 115 показателей. Начальная версия выборки включала в себя 66 результатов оценивания квалификации 25 тестировщиков и 494 результата оценивания 142 разработчиков в период с 2019–2022 гг. Для каждого результата был определен интервал дат, за который необходимо провести выгрузку данных из систем и расчет показателей. В итоге была загружена информация по 218167 задачам, 4206 страницам из системы управления знаниями, 75576 тест-кейсам из системы управления тестированием и был выгружен код из 39 репозиториев.

При оценивании квалификации использовалось большое количество показателей, которые можно объединить в факторы для упрощения процедуры и сокращения размерности данных, а также рассмотреть неявные закономерности и связи между показателями для более точных результатов. Для достижения этой цели были применены методы исследовательского факторного анализа (Exploratory Factor Analysis, EFA) и структурного моделирования (Structural Equation Modeling, SEM).

Перед проведением факторного анализа был проведен поиск выбросов на основе графика boxplot, из исходных данных результатов оценивания квалификации тестировщика были удалены показатели и сами выбросы (Рис. 3).

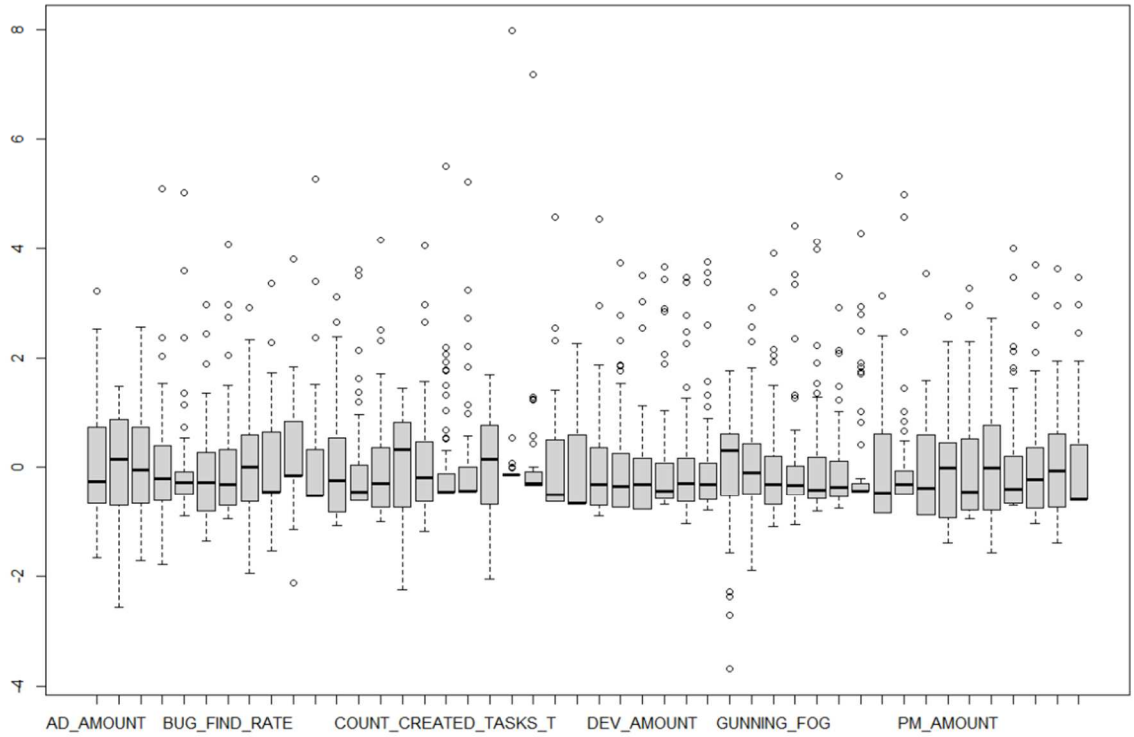

Рис. 3. График boxplot для стандартизованных значений показателей оценки квалификации тестировщика

При поиске аномалий в исходных данных оценок разработчиков было выявлено, что лишними являются результаты оценивания квалификации для руководителей команд разработки, которые в большей степени занимаются управленческими задачами (Рис. 4). После их удаления конечная версия выборки включала 237 результатов по 70 разработчикам.

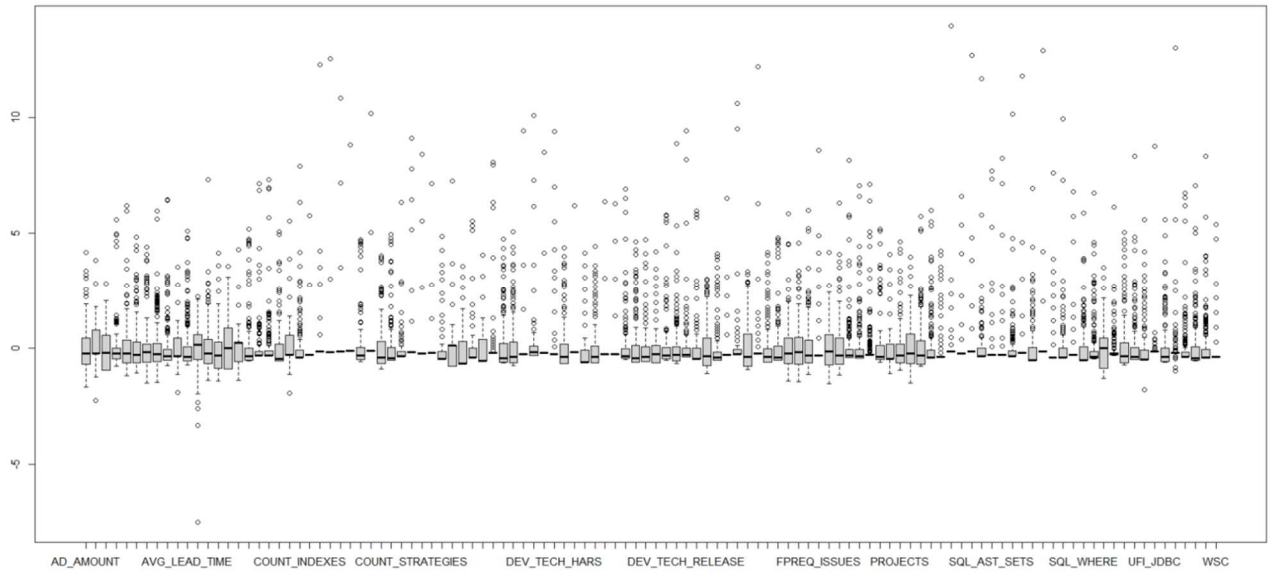

Рис. 4. График boxplot для стандартизованных значений показателей оценки квалификации разработчика

4. Факторный анализ

4.1. Анализ модели оценки профессиональных навыков и знаний тестировщиков

Для проведения исследовательского факторного анализа был использован метод главных компонент (Principal Component Analysis, PCA). Вначале была проведена оценка целесообразности проведения факторного анализа при помощи критериев Кайзера–Мейера–Олкина (KMO) и сферичности Бартлетта. Результаты теста Бартлетта указывали на хорошие перспективы анализа – 181.9 и p-value < 2.2e-16, но начальное значение теста KMO было низким, поэтому из модели были удалены показатели, у которых значение этого критерия было меньше критического (< 0.6) [24]. После их удаления значение критерия KMO было равно 0.74, что указывает на хорошие перспективы проведения факторного анализа.

Из графика «каменистой осыпи» на рис. 5 было определено возможное число факторов – оно варьировалось между 2 и 3. Факторный анализ был проведен при помощи функции базового пакета R – factanal. Итоговая версия модели состояла из 5 факторов, т.к. при её построении был получен наибольший p-value гипотезы достаточности факторов по сравнению с моделями из 2, 3 и 4 факторов, равный 0.263.

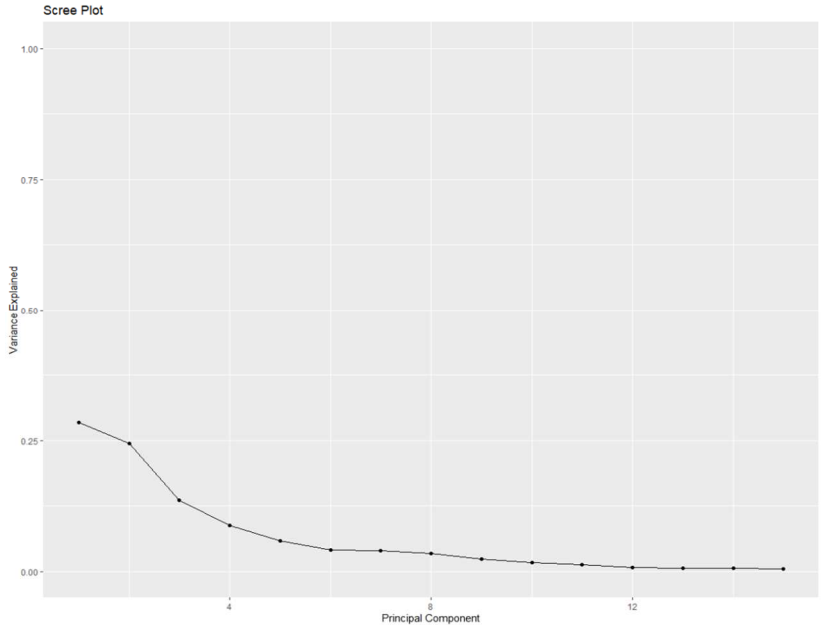

Рис. 5. График «Каменистая осыпь» для модели оценки квалификации тестировщиков

Нагрузки факторов, полученных при помощи метода вращения varimax, представлены в табл. 1, абсолютные значения меньше 0.4 не были включены в факторную модель.

Таблица 1. Таблица нагрузок для факторов оценки квалификации тестировщика

	F1	F2	F3	F4	F5
AUTOMATED_READABILITY		0.934			
BUG_FIND_RATE	0.668				
COLEMAN_LIAU		0.923			
COUNT_AVG_TEST_BY_DATE	0.891				
COUNT_BUGS_BY_DATE					0.649
COUNT_CREATED_TASKS_B			0.430		
COUNT_PLATF_UPD				0.627	
COUNT_REOPENS_BY_USER	0.954				
FIXED_ISSUES			0.789		

FIXED_ISSUES_NOT_WITHIN_EST			0.752		
FIXED_ISSUES_WITHIN_EST			0.968		
FLESCH_KINCAID	0.167	0.921			
LOG_FILES				0.708	
MULTIPLE_CASES	0.587				
PASSED_TRAINEE_AMOUNT				0.820	

Доля общей дисперсии, объясняемой каждым фактором, и накопление этих дисперсий представлены в табл. 2.

Таблица 2. Доля общей дисперсии и её накопление для факторов оценки квалификации тестировщика

	F1	**F2**	**F3**	**F4**	**F5**
SS loadings	2.972	2.851	2.491	1.814	0.690
Proportion Var	0.198	0.190	0.166	0.121	0.046
Cumulative Var	0.198	0.388	0.554	0.675	0.721

Полученную модель факторов можно интерпретировать следующим образом:

Фактор F1 – «Результативность тестирования». Включает в себя показатели:

– скорость обнаружения ошибок (BUG_FIND_RATE);

– количество зарегистрированных дефектов с несколькими кейсами воспроизведения ошибок (MULTIPLE_CASES);

– количество проверок задач в день (COUNT_AVG_TEST_BY_DATE);

– количество повторных открытий задач, инициированных сотрудником (COUNT_REOPENS_BY_USER).

Данный фактор характеризует результативность основной деятельности ИТ-специалиста – тестирование. От объема проверяемых сотрудником задач зависит уровень стабильности информационной системы. Каждый обнаруженный дефект или задание по разработке функционального элемента программного продукта регистрируется в системе управления задачами. После исправления дефекта или завершения разработки сотрудник изменяет статус задачи на «Решено», чтобы тестировщик начал проверку. После окончания проверки тестировщик переоткрывает задачу, если была обнаружена ошибка, или меняет её статус на «Проверено», если ошибки не были найдены.

Фактор F2 – «Письменные коммуникативные навыки». Содержит показатели:

– среднее значение индекса автоматической читаемости описания дефекта (AUTOMATED_READABILITY);

– среднее значение индекса Колмана–Лиау описания дефекта (COLEMAN_LIAU);

– среднее значение индекса Флеша–Кинкейда описания дефекта (FLESCH_KINCAID).

Этот фактор иллюстрирует степень легкости восприятия составленных описаний дефектов. Чем доступнее и понятнее отчет о дефекте, тем быстрее и эффективнее его сможет решить разработчик.

Фактор F3 – «Решение задач в рамках оценки». Объединяет переменные:

– количество решенных задач тестировщиком (FIXED_ISSUES);

– количество решенных задач вне рамок оценки (FIXED_ISSUES_NOT_WITHIN_EST);

– количество решенных задач в рамках оценки (FIXED_ISSUES_WITHIN_EST);

– процент зарегистрированных дефектов с приоритетом «Blocker» (COUNT_CREATED_TASK_B).

Текущий фактор описывает, насколько успешно сотрудник решает задачи в соответствии с оцененным количеством времени. Если задачи не выполняются за оцененное количество времени, то повышаются расходы проекта и риск срыва сроков его сдачи.

Фактор F4 – «Технические инструменты и наставничество». Состоит из показателей:

– количество упоминаний обновления версий конструктора приложений в задачах, журнале работ (COUNT_PLATF_UPD);

– количество вложений, связанных с журналированием работы системы (LOG_FILES);

– количество стажеров, успешно прошедших стажировку под менторством сотрудника (PASSED_TRAINEE_AMOUNT).

Фактор характеризует степень владения техническими инструментами, используемыми при тестировании, а также навыки наставничества. В процессе проверки системы тестировщикам требуется дополнительно собирать журналы работы сервера и архив запросов, чтобы разработчик оперативнее смог определить причину дефекта.

Иногда причиной дефекта является ошибка в работе конструктора приложений. Поэтому после исправления ошибки в новой версии конструктора приложений тестировщики устанавливают её, чтобы проверить актуальность дефекта. Сам процесс обновления версии конструктора требует от сотрудника знаний и навыков по администрированию сервера приложений и операционной системы, т.к. шаги по установке являются нетривиальными.

Наличие показателя, связанного с количеством стажеров, связано с тем, что в исследуемой компании более компетентным тестировщикам предлагают обучить новых сотрудников.

Фактор F5 – «Оперативность обнаружения дефектов». Последний фактор определяет, насколько оперативно тестировщик обнаруживает дефекты, он состоит из 1 показателя:

– количество зарегистрированных дефектов в день (COUNT_BUGS_BY_DATE).

Для проверки того, насколько точно модель соответствует данным, был проведен подтверждающий факторный анализ (Confirmatory Factor Analysis, CFA). В рамках него были рассчитаны 3 показателя, их значения указывают на относительно приемлемое качество модели:

– CFI (сравнительный индекс соответствия, > 0.950) – 0.894;

– RMSEA (среднеквадратичная ошибка аппроксимации, < 0.1) – 0.116;

– SRMR (стандартизованный среднеквадратичный остаток, < 0.1) – 0.105.

На основе результатов исследовательского факторного анализа была построена структурная модель зависимости между оценкой профессиональных навыков и знаний, полученной от руководителя, и выделенными факторами (Рис. 6). Для разработки структурной модели был использован пакет lavaan в R.

В рамках валидации структурной модели состав её факторов был изменен:

1. Из модели были удалены избыточные факторы, решение об их исключении принималось на основе p-value из коэффициентов структурной модели, его значение должно быть меньше 0.05.

2. Дополнительно были добавлены 2 фактора:

Фактор F6 «Инструменты тестирования веб-сервисов». Данный фактор характеризует степень владения сторонними инструментами для тестирования работы SOAP и REST веб-сервисов. Он включает в себя показатель – количество упоминаний инструментов тестирования веб-сервисов в описаниях задач, комментариях и журналах работ (COUNT_INTEGRATION_INSTR).

Фактор F7 «Длительность решения задач». Данный фактор характеризует объем трудозатрат тестировщика на решение назначенных задач. Состоит из показателя – общее время на решение задач (ALL_ISSUE_RES_TIME).

Эти показатели имели высокую степень значимости в регрессионной модели оценки профессиональных знаний и навыков, но они были исключены в рамках EFA, т.к. имели низкое значение индекса KMO.

Параметры оценки структурной модели также свидетельствуют об относительно приемлемом качестве:

– количество параметров – 17;

– степени свободы – 11;

– X2 – 20.197;

– CFI – 0.948;

– RMSEA – 0.113;
– SRMR – 0.054.

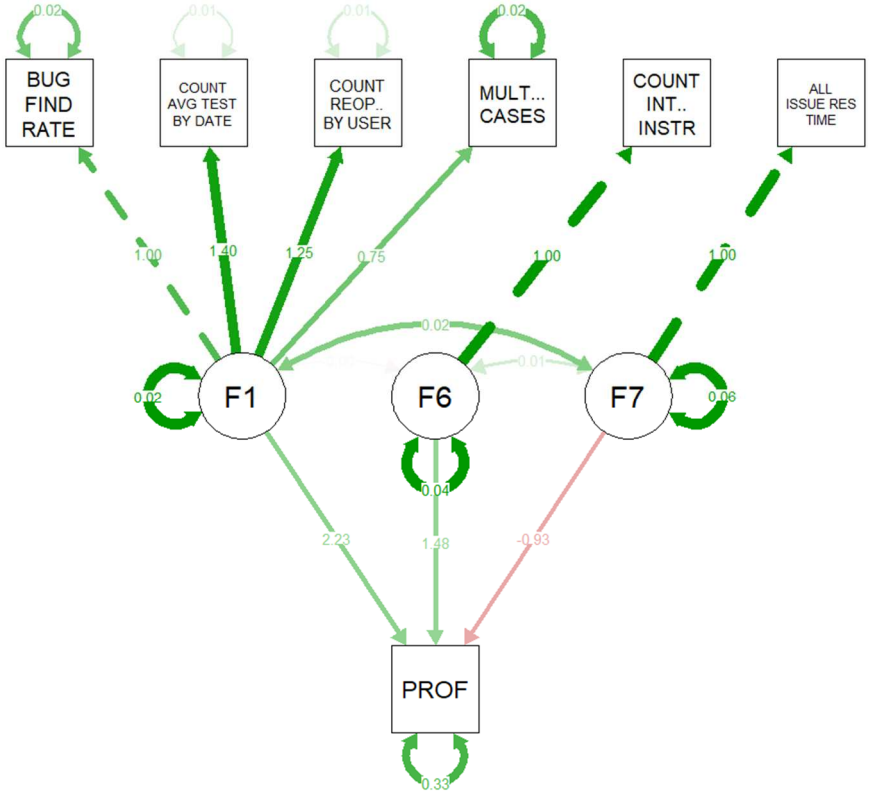

Рис. 6. Структурная модель оценки профессиональных знаний и навыков тестировщика

Полученные коэффициенты для разработанной структурной модели представлены в табл. 3.

Таблица 3. Коэффициенты структурной модели оценки профессиональных знаний и навыков тестировщика

PROF ~	**Estimate**	**Std.Err**	**t-value**	**P(> |t|)**
F1	2.230	0.718	3.106	0.002
F6	1.477	0.386	3.829	0.000
F7	-0.927	0.345	-2.688	0.007

По результатам построенной модели можно увидеть, что фактор F1 «Результативность тестирования» имеет положительное влияние на оценку, т.к. тестирование является основной должностной обязанностью работников. Чем больше изменений в новой версии программного продукта будет проверено, тем выше становится уровень её стабильности и надежности.

Знания и опыт работы с техническими инструментами позволяют провести более комплексное и тщательное тестирование программных продуктов, поэтому положительно на оценку влияет фактор F6 «Инструменты тестирования веб-сервисов». Сотрудники в исследуемой компании используют такие специальные пакеты ПО, как Soap UI, Postman и JMeter, т.к. они предоставляют тестировщикам возможность разработать автотесты, провести нагрузочное тестирование, а также собрать подробную статистику о пройденных и не пройденных тест-кейсах.

Негативно на оценку уровня профессиональных навыков влияет фактор F7 «Длительность решения задачи». Данный фактор тесно связан с бюджетом и сроком проекта: чем дольше решаются задачи, тем выше становится уровень операционных расходов и риск срыва установленных сроков. Более компетентные тестировщики за меньшее количество времени решают назначенные на них задачи.

4.2. Анализ модели оценки профессиональных навыков и знаний разработчиков

Для модели оценки профессиональных навыков и знаний разработчиков результаты теста Бартлетта указывали на хорошую возможность выполнения анализа – 436, p-value < 2e-16, но начальное значение теста KMO было средним, в связи с чем из модели были удалены избыточные показатели. После их удаления значение критерия KMO было равно 0.87.

Построенный график «Каменистая осыпь» свидетельствует о том, что подходящее число факторов варьировалось между 2 и 3 (Рис. 7).

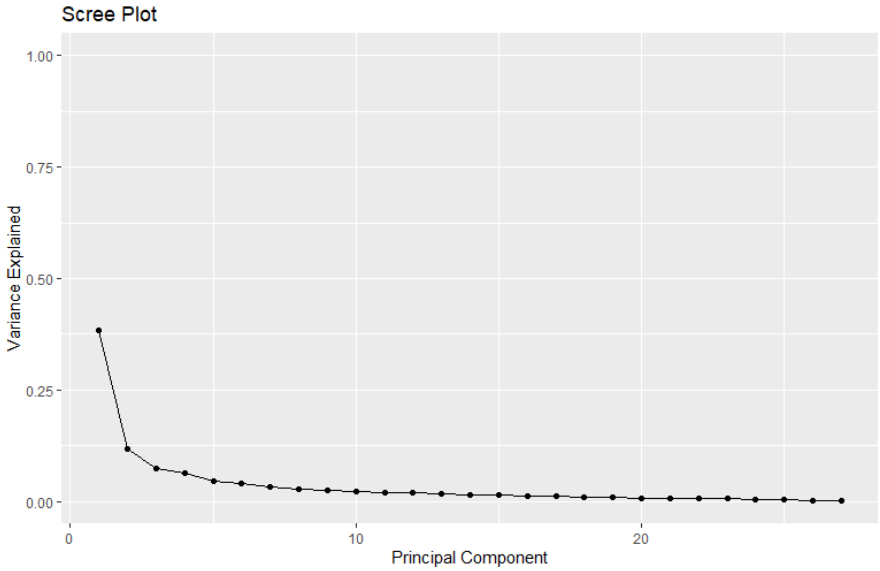

Рис. 7. График «Каменистая осыпь» для модели оценки квалификации разработчиков

После выполнения EFA и построения структур факторов был проведен CFA. Показатели указывали на удовлетворительную состоятельность моделей. Наибольшие значения показателей были получены для модели, состоящей из 4 факторов, по сравнению с моделями, состоящими из 2 и 3 факторов: CFI – 0.691, RMSEA – 0.143, SRMR – 0.112.

В результате корректировок набора показателей была построена новая версия модели, состоящая из 5 факторов, т.к. показатели CFA для этого количества факторов были лучше, чем для меньшего количества факторов. Рассчитанные при помощи метода varimax нагрузки факторов представлены в табл. 4.

Таблица 4. Таблица нагрузок для факторов оценки квалификации разработчика

	RC1	**RC2**	**RC3**	**RC4**	**RC5**
AVG_ISSUES_BY_WL				0.825	
COUNT_ENV_PARAMS		0.590			
COUNT_JS_CLIENT_LIBS			0.820		
COUNT_MC_CONSTRUCTOR		0.753			
COUNT_MC_SQL		0.858			
COUNT_XML_COMPS	0.820				
DEV_TECH_CONSULTATION				0.648	
DEV_TECH_HARS			0.831		
DEV_TECH_JAVA	0.614				
DEV_TECH_XSD					0.613
FPREQ_ISSUES			0.662		
MTYPE_ATTR	0.792				
TEMP_TYPES	0.826				
UDMS					0.778

UFI_HTTP	0.694				
UFI_JL		0.736			
UFI_XML					0.613

Доля общей дисперсии, объясняемой каждым фактором, и накопление этих дисперсий представлены в табл. 5.

Таблица 5. Доля общей дисперсии и ее накопление для факторов оценки квалификации разработчика

	RC1	**RC2**	**RC3**	**RC4**	**RC5**
SS loadings	3.804	2.875	2.482	1.818	2.042
Proportion Var	0.224	0.169	0.146	0.107	0.120
Cumulative Var	0.224	0.393	0.539	0.766	0.659

Построенную модель факторов можно интерпретировать следующим образом:

Фактор RC1 – «Разработка интеграционных сервисов». Включает в себя показатели:

– количество загруженных XSD-схем (COUNT_XML_COMPS);

– количество добавленных атрибутов в таблицы (MTYPE_ATTR);

– количество созданных временных таблиц (TEMP_TYPES);

– количество применений функций для взаимодействия с внешними системами через HTTP-протокол (UFI_HTTP);

– степень частоты упоминаний Java в назначенных задачах, комментариях и журнале работ (DEV_TECH_JAVA).

Этот фактор характеризует уровень технических навыков сотрудника и опыт разработки интеграционных сервисов. Интеграционные сервисы в программных продуктах исследуемой компании работают на основе REST-ресурсов, в которых системы обмениваются между собой XML-документами. Для формирования этих документов необходимо загрузить XSD-схему, а также сгенерировать на её основе временные таблицы и атрибуты. Сформированные XML-документы отправляются в другие системы через HTTP-протокол при помощи встроенных функций.

Фактор RC2 – «Написание SQL-запросов». Содержит показатели:

– количество разработанных поисковых методов типа «Конструктор» (COUNT_MC_CONSTRUCTOR);

– количество разработанных поисковых методов типа «SQL» (COUNT_MC_SQL);

– количество применений Java-библиотек (UFI_JL);

– количество созданных параметров приложения (COUNT_ENV_PARAMS).

Данный фактор также характеризует уровень технических навыков и опыт написания SQL-запросов. Для их исполнения в конструкторе приложений используются специальные объекты – поисковые методы, в которых разработчик может указать текст запроса. Еще одним распространенным способом является применение Java-библиотек для исполнения SQL-запросов через API JDBC.

Фактор RC3 – «Анализ дефектов конструктора приложений». Объединяет показатели:

– степень частоты упоминаний HAR-файлов в комментариях и журналах работ (DEV_TECH_HARS);

– количество зарегистрированных дефектов в проекте по поддержке конструктора приложений (FPREQ_ISSUES);

– количество разработанных JS-библиотек для экранных форм (COUNT_JS_CLIENT_LIBS).

Фактор характеризует степень владения инструментами для сбора отладочной информации и понимания основ работы конструктора приложений. В работе конструктора приложе-

ний могут возникать ошибки, и для их решения разработчики регистрируют дефекты в системе управления задачами, в проекте по поддержке конструктора. Для анализа дефектов требуется дополнительная информация, например, журналы работы сервера и HAR-файлы – архивы, содержащие историю отправленных запросов.

Фактор RC4 – «Коммуникативные навыки». Включает в себя 2 показателя: среднее количество задач, по которым работает сотрудник, в 1 день (AVG_ISSUES_BY_WL) и степень частоты упоминаний консультаций в журнале работ (DEV_TECH_CONSULTATION). Этот фактор характеризует устные коммуникативные навыки разработчика. Разработчики консультируют заказчиков и сотрудников компаний. Сами консультации запрашиваются в рамках созданных задач, поэтому разработчики с большим количеством проработанных задач в день, как правило, отвечают на вопросы.

Фактор RC5 – «Маппинг данных в интеграционных сервисах». Состоит из показателей:

– степень частоты упоминаний XSD в задачах, комментариях и журнале работ (DEV_TECH_XSD);

– количество разработанных пользовательских функций (UDMS);

– количество применений функций для генерации запросов в формате XML (UFI_XML).

Этот фактор характеризует опыт разработки обработчиков запросов и ответов из интеграционных сервисов. Маппинг данных – процесс сопоставления атрибутов запросов и ответов из внешней системы со связанными атрибутами таблиц разрабатываемого приложения [25]. При маппинге запросов и ответов из внешних систем разработчики используют встроенные функции по разбору XML-документа и пишут пользовательские функции для их обработки.

Результаты проведения CFA свидетельствуют об относительно приемлемом качестве модели: CFI – 0.841, RMSEA – 0.132, SRMR – 0.072.

На основе результатов EFA была разработана структурная модель зависимости между оценкой профессиональных навыков и знаний, полученной от руководителя, и выделенными факторами. В рамках валидации структурной модели из неё был удален избыточный фактор RC3, т.к. у него было высокое значение p-value – 0.845. Итоговая версия модели представлена на рис. 8.

Параметры оценки структурной модели также свидетельствуют об относительно приемлемом качестве:

– количество параметров – 39;

– степени свободы – 81;

– X2 – 425.515;

– CFI – 0.862;

– RMSEA – 0.134;

– SRMR – 0.064.

Полученные коэффициенты для разработанной модели представлены в табл. 6.

Таблица 6. Коэффициенты структурной модели оценки профессиональных знаний и навыков разработчика

PROF ~	**Estimate**	**Std. Err**	**t-value**	**P(> |t|)**
RC1	2.245	0.568	3.953	0.000
RC2	3.757	0.703	5.346	0.000
RC4	3.314	0.924	3.587	0.000
RC5	-3.747	0.657	-5.704	0.000

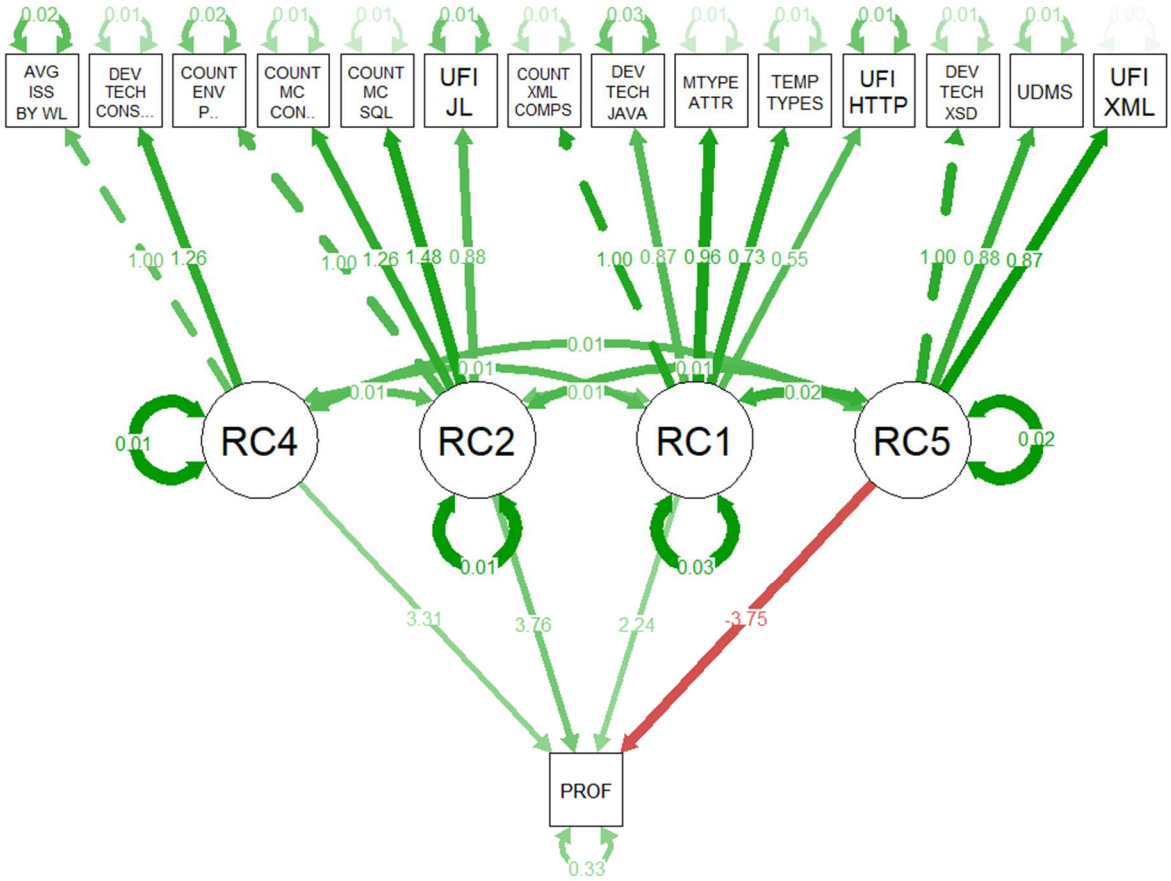

Рис. 8. Структурная модель оценки профессиональных знаний и навыков разработчика

Важными чертами квалификации разработчика являются глубокие знания инструментов для разработки и способов их применения в решении задач, поэтому положительное влияние на оценку имеют фактор RC1 «Разработка интеграционных сервисов» и фактор RC2 «Написание SQL-запросов». В большинстве случаев эти задачи требуют специфических знаний и опыта, поэтому более квалифицированные работники решают эти задачи в срок.

Коллеги, не знакомые с разрабатываемой системой, нуждаются в консультации более опытных разработчиков для выполнения назначенных задач. Также у сотрудников со стороны заказчика могут возникнуть вопросы по работе с системой и по её поддержке. В связи с чем положительное влияние на оценку оказывает фактор RC4 «Коммуникативные навыки».

Основной особенностью обмена знаниями в исследуемой компании является то, что обмен происходит в личных переписках или звонках, и знания редко фиксируются в Atlassian Confluence, поэтому показатели из этой системы оказались избыточными.

Негативное влияние на оценку имеет фактор RC5 «Маппинг данных в интеграционных сервисах». Возможно, это связано с исходными данными и невысоким уровнем сложности этой области задач: бо́льшие значения показателей данного фактора были у разработчиков, работавших в компании меньше 6 месяцев и имевших низкий уровень оценки профессиональных знаний и навыков. Чаще всего задачи, связанные с маппингом данных, назначаются на менее опытных сотрудников, т.к. они не требуют высокого уровня квалификации. В рамках этих задач разработчики пишут простой код, в котором происходит перезапись значений из одного поля в другое.

Регрессионная модель оценки из предыдущей работы [5] в большей степени рассматривала технические навыки разработчика в области клиентской части приложений (frontend), например, влиятельными оказались показатели, связанные с настройкой виджетов и количеством измененных строк кода интерфейсных форм. В то время как структурная модель учитывает технические навыки разработчика в области серверной части приложений (backend), например, факторы RC5 «Маппинг данных в интеграционных сервисах» и RC2 «Написание

SQL-запросов», но также она учитывает и нетехнические навыки, например, фактор RC4 «Коммуникативные навыки». Возможно, это связано с тем, что выборка в текущей работе включает в себя б*о*льший объем данных, а программные продукты компании за последние 2 года выступали как backend-решения, в то время как frontend-части были разработаны другими вендорами. Также разработчики начали принимать активное участие в процессах сопровождения и поддержки систем, поэтому коммуникативные навыки играют важную роль в решении задач.

При этом обе модели учитывают навыки разработчика, связанные с разработкой интеграционных сервисов: в регрессионной модели из предыдущей статьи важным оказался показатель подсчета количества применений функций для взаимодействия с внешними системами, а в структурной модели – фактор RC1 «Разработка интеграционных сервисов». Возможно, это связано с особенностями клиентов исследуемой компании: у финансовых организаций, как правило, есть комплексная ИТ-инфраструктура, в которой каждый программный продукт ответственен за исполнение ряда функций. Поэтому новые внедряемые системы должны иметь функционал для взаимодействия с другими системами заказчика для решения поставленных целей и задач.

5. Заключение

В рамках этой работы был проведен факторный анализ и построены структурные модели для оценки профессиональных знаний и навыков тестировщиков и разработчиков. Было выявлено, что при оценивании квалификации тестировщиков учитываются результативность тестирования, навыки работы с инструментами тестирования веб-сервисов и длительность решения задач. Другие факторы оценки квалификации тестировщиков, выявленные в рамках исследовательского факторного анализа, оказались избыточными по результатам разработки структурной модели. Возможно, это связано с тем, что непосредственные руководители не учитывают эти данные при оценивании квалификации. Однако факторы, связанные с письменными коммуникативными навыками, техническими инструментами для тестирования и наставничеством, рекомендуется учитывать при оценивании. Умение устно и письменно общаться с коллегами и клиентами кратким и понятным языком играет важную роль в принятии решений. Кроме того, тестировщики, выступающие в роли ментора, систематизируют и валидируют собственные знания и опыт.

При оценивании квалификации разработчиков учитываются опыт решения технических задач: в частности, написание SQL-запросов и разработка интеграционных сервисов, а также устные коммуникативные навыки.

Профили деятельности и должностные обязанности тестировщиков и разработчиков в исследуемой компании сильно отличаются, в связи с чем выявленные факторы практически не включают в себя схожие показатели.

Интеллектуальный анализ данных систем, в которых работают ИТ-специалисты, может содействовать руководству в более точном оценивании уровня квалификации сотрудника, а также помочь лучше понять критерии оценивания, процессы разработки, тестирования и сопровождения программных продуктов за счет выявления скрытых факторов и закономерностей.

При помощи разработанных моделей менеджеры могут проводить оценку квалификации тестировщика и разработчика. В дальнейшем планируется подготовить методику для составления индивидуального плана развития ИТ-специалиста в области разработки ПО. Также модели будут внедрены в подсистему оценивания СППР, чтобы на основе полученных результатов и подготовленной методики сотруднику предлагались наиболее подходящие направления профессионального роста и задачи для развития профессиональных навыков и знаний.

Литература

1. *Gastaldi L., Corso M.* Smart Healthcare Digitalization: Using ICT to Effectively Balance Exploration and Exploitation within Hospitals // International Journal of Engineering Business Management. 2012. V. 4. P. 1–13.
2. *Pearlman K., Schmidt F. L., Hunter J. E.* Validity generalization for tests used to predict job proficiency and training success in clerical occupations // Journal of Applied Psychology. 1980. V. 65, № 4, P. 373–406.
3. *Rothstein H. R.* Interrater reliability of job performance ratings: Growth to asymptote level with increasing opportunity to observe // Journal of Applied Psychology. 1990. V. 75, № 3. P. 322–327.
4. *Viswesvaran C., Ones D. S., Schmidt F. L.* Comparative analysis of reliability of job performance ratings // Journal of Applied Psychology. 1996. V. 81, № 5. P. 557–574.
5. *Gavriliev E. I., Avdeenko T. V.* Model and Procedure for Assessing the Qualification of a Software Developer // Proc. IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM), 2022. P. 303–307.
6. *Гаврильев Э. И., Авдеенко Т. В.* Процедура оценки квалификации разработчика программного обеспечения // Сборник научных трудов «Наука. Технологии. Инновации»: в 10-и частях, Новосибирск, 06–10 декабря 2021 года. С. 145–148.
7. *Robillard M. P., Coelho W., Murphy G. C.* How effective developers investigate source code: an exploratory study // IEEE Transactions on Software Engineering. 2004. V. 30, № 12, P. 889-903.
8. *Surakka S.* What subjects and skills are important for software developers // Communications of the ACM. 2007. V. 50, №. 1. P. 73–78.
9. *Li P. L., Ko A. J., Begel A.* What Makes a Great Software Engineer? // Proc. 37th International Conference on Software Engineering, 2015. P. 700–710.
10. *Baltes S., Diehl S.* Towards a theory of software development expertise// Proc. 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), 2018.
11. *Bergersen G. R., Sjøberg D. I. K., Dybå T.* Construction and validation of an instrument for measuring programming skill // IEEE Trans. Softw. Eng. 2014. V. 40, №. 12. P. 1163–1184.
12. *Juristo N., Moreno A. M., Stigel W.* Guest editors' introduction: Software testing practices in industry // IEEE Software. 2006. V. 23, № 4. P. 19–21.
13. *Florea R., Stray V.* The skills that employers look for in software testers // Software Quality Journal. 2019. № 27. P. 1449–1479.
14. *Iivonen J., Mäntylä M.V., Itkonen J.* Characteristics of high performing testers: a case // Proc. ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2010. P. 1–9.
15. *Deak A.* What Characterizes a Good Software Tester? – A Survey in Four Norwegian Companies // Lecture Notes in Computer Science. 2014. № 8763. P. 162–172.
16. *Gousios G., Kalliamvakou D., Spinellis E. D.* Measuring developer contribution from software repository data // Proc. International working conference on Mining software repositories (MSR), 2008. P. 129–132.
17. *Lanubile F., Ebert C., Prikladnicki R., Herzig R. K.* A Collaboration Tools for Global Software Engineering // IEEE Software. 2010. V. 27, № 2. P. 52–55.
18. *Zolkifli N. N., Ngah A., Deraman A.* Version Control System: A Review // Lecture Notes in Computer Science. 2018. V. 135. P. 408–415.
19. *Макашов П. А., Романенко Н. А.* Сервис-ориентированный подход к управлению ИТ-проектами на примере использования программного продукта «JIRA» // Современные информационные технологии и ИТ-образование. 2015. V. 11, № 2. С. 127–132.

20. *Collins E. F., Lucena Jr. V.* Software Test Automation practices in agile development environment: An industry experience report // Proc. 7th International Workshop on Automation of Software Test (AST), 2012. P. 57–65.
21. *Apraci I., Al-Emran M., Al-Sharafi M. A.* The impact of knowledge management practices on the acceptance of Massive Open Online Courses (MOOCs) by engineering students: A cross-cultural comparison // Telematics and Informatics. 2020. № 54. P. 1–13.
22. *Гаврильев Э. И., Авдеенко Т. В.* Многофакторная регрессионная модель оценки квалификации тестировщика программного обеспечения // Доклады ТУСУР. 2022. V. 25, № 4. С. 115–121.
23. Томита-парсер [Электронный ресурс]. URL: `https://tech.yandex.ru/tomita/` (дата обращения: 02.04.2023).
24. Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy [Электронный ресурс]. URL: `https://www.statisticshowto.com/kaiser-meyer-olkin/` (дата обращения: 16.04.2023).
25. Understanding Data Mapping Tools, Process, and Techniques [Электронный ресурс]. URL: `https://www.astera.com/type/blog/understanding-data-mapping-and-its-techniques/` (дата обращения: 02.04.2023).

Гаврильев Эрчимэн Иванович
аспирант кафедры теоретической и прикладной информатики, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, просп. К. Маркса, д. 20), e-mail: `erchimen_gavriliev@outlook.com`, ORCID ID: 0000-0001-7289-3969.

Авдеенко Татьяна Владимировна
д.т.н., профессор кафедры теоретической и прикладной информатики, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, просп. К. Маркса, д. 20), e-mail: `tavdeenko@mail.ru`, ORCID ID: 0000-0002-8614-5934.

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.*

Structural Model of Indicators for IT Specialists' Qualification Assessment Based on Data Mining of Information Systems

Erchimen I. Gavriliev, Tatiana V. Avdeenko

Novosibirsk State Technical University (NSTU)

Abstract: The key factors for the success of an IT organization project are its people and professional quality. To meet the need for professional growth, management adheres to the constant assessment of the employee's qualification. However, the low level of reliability and accuracy of the assessment results associated with the subjective opinion of the management may lead to the negative consequences of decisions. For fast results and high accuracy of proficiency testing, assessment models and software testers have been developed to support decision-making based on a large number of results obtained using data mining of information systems in the work of IT specialists. In the present work, a factor analysis was carried out to identify detection

of such cases. The results of measurements, which are determined when evaluating the qualifications of IT specialists, cause factors associated with the occurrence of technical problems, the effectiveness and efficiency of testing as well as communication skills.
Keywords: personnel assessment, developer, tester, exploratory factor analysis, confirmatory factor analysis, data mining.

For citation: Gavriliev E. I., Avdeenko T. V. Structural model of indicators for IT specialists' qualification assessment based on data mining of information systems (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 15-33. https://doi.org/10.55648/1998-6920-2023-17-4-15-33.

The article was submitted: 29.04.2023;
revised version: 14.05.2023;
accepted for publication 15.05.2023.

References

1. Gastaldi L, Corso M. Smart Healthcare Digitalization: Using ICT to Effectively Balance Exploration and Exploitation within Hospitals. *International Journal of Engineering Business Management,* 2012, vol. 4. pp. 1-13.
2. Pearlman, K., Schmidt, F. L., Hunter, J. E. Validity generalization for tests used to predict job proficiency and training success in clerical occupations. *Journal of Applied Psychology,* 1980, vol. 65, no 4, pp. 373-406.
3. Rothstein H. R. Interrater reliability of job performance ratings: Growth to asymptote level with increasing opportunity to observe. *Journal of Applied Psychology*, 1990, vol. 75, no 3, pp. 322-327.
4. Viswesvaran C., Ones D. S., Schmidt F. L. Comparative analysis of reliability of job performance ratings. *Journal of Applied Psychology,* 1996, vol. 81, no 5, pp.557-574.
5. Gavriliev E. I., Avdeenko T. V. Model and Procedure for Assessing the Qualification of a Software Developer. *2022 IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM),* 2022, pp. 303–307.
6. Gavriliev E. I., Avdeenko T. V. Procedura ocenki kvalifikacii razrabotchika programmnogo obespecheniya [Procedure for assessing the qualifications of a software developer]. *Nauka. Tekhnologii. Innovacii*: Collection of scientific papers. In 10 parts, Novosibirsk, 06-10 December, 2021, pp. 145-148.
7. Robillard M. P., Coelho W., Murphy G. C. How effective developers investigate source code: an exploratory study. *IEEE Transactions on Software Engineering,* 2004. vol. 30, no. 12, pp. 889-903.
8. Surakka S. What subjects and skills are important for software developers. *Communications of the ACM*, 2007, vol. 50, no. 1, pp. 73-78.
9. Li P. L., Ko A. J, Begel A. What Makes a Great Software Engineer? *37th International Conference on Software Engineering,* 2015, pp. 700-710.
10. Baltes S., Diehl S. Towards a theory of software development expertise. *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2018*, 2018.
11. Bergersen G. R., Sjøberg D. I. K., Dybå T. Construction and validation of an instrument for measuring programming skill. *IEEE Trans. Softw. Eng*, 2014, vol. 40, no. 12, pp. 1163-1184.
12. Juristo N., Moreno A.M., Stigel W. Guest editors' introduction: Software testing practices in industry. *IEEE Software*, 2006, vol. 23, no. 4, pp. 19-21.
13. Florea R., Stray V. The skills that employers look for in software testers. *Software Quality Journal*, 2019, no. 27, pp. 1449-1479.
14. Iivonen J., Mäntylä M.V., Itkonen J. Characteristics of high performing testers: a case. *ESEM '10: Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, 2019, pp. 1-9.
15. Deak A. What Characterizes a Good Software Tester? – A Survey in Four Norwegian Companies. *Lecture Notes in Computer Science,* 2014, no. 8763, pp. 162-172.

16. Gousios G, Kalliamvakou D., Spinellis E.D. Measuring developer contribution from software repository data. *In Proceedings of the 2008 international working conference on Mining software repositories, MSR '08*, 2008, pp. 129-132.
17. Lanubile F., Ebert C., Prikladnicki R., Herzig R.K. A Collaboration Tools for Global Software Engineering. *IEEE Software,* 2010, vol. 27, no. 2, pp. 52–55.
18. Zolkifli N. N., Ngah A., Deraman A. Version Control System: A Review. *Lecture Notes in Computer Science,* 2018, vol. 135, pp. 408-415.
19. Makashov P.A., Romanenko N.A. Servis-orientirovannyj podhod k upravleniyu IT proektami na primere ispol'zova-niya programmnogo produkta «JIRA» [Service-oriented approach to IT project management on the example of using JIRA software product]. *Sovremennye informacionnye tekhnologii i IT-obrazovanie*, 2015, vol. 11, no. 2, pp. 127–132.
20. Collins E. F., Lucena Jr. V. Software Test Automation practices in agile development environment: An industry experience report. *2012 7th International Workshop on Automation of Software Test (AST)*, 2012, pp. 57–65.
21. Apraci I., Al-Emran M., Al-Sharafi M. A. The impact of knowledge management practices on the acceptance of Massive Open Online Courses (MOOCs) by engineering students: A cross-cultural comparison. *Telematics and Informatics*, 2020, no. 54, pp. 1–13.
22. Gavriliev E. I., Avdeenko T. V. Mnogofaktornaya regressionnaya model' ocenki kvalifikacii testirovshchika programm-nogo obespecheniya [Multivariate regression model for assessing the qualifica-tions of a software tester]. *Doklady TUSUR*, 2022, vol. 25, no. 4, pp. 115–121.
23. Tomita-parser, available at: `https://tech.yandex.ru/tomita/` (accessed: 02.04.2023).
24. Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy, available at: `https://www.statisticshowto.com/kaiser-meyer-olkin/` (accessed: 16.04.2023).
25. Understanding Data Mapping Tools, Process, and Techniques, available at: `https://www.astera.com/type/blog/understanding-data-mapping-and-its-techniques/` (accessed: 02.04.2023).

Erchimen I. Gavriliev

Postgraduate student, Department of Theoretical and Applied Computer Science, Novosibirsk State Technical University (NSTU, Russia, 630073, Novosibirsk, Karl Marks Ave. 20), e-mail: `erchimen_gavriliev@outlook.com`, ORCID ID: 0000-0001-7289-3969.

Tatiana V. Avdeenko

Dr. of Sci. (Engineering), Professor, Department of Theoretical and Applied Computer Science, Novosibirsk State Technical University (NSTU, Russia, 630073, Novosibirsk, Karl Marks Ave. 20), e-mail: `tavdeenko@mail.ru`, ORCID ID: 0000-0002-8614-5934.

DOI: 10.55648/1998-6920-2023-17-4-34-48 УДК 004.04: 378.147

Технология оценивания цифровой зрелости образовательной организации. Часть II *

Ю. В. Шевцова[1], Т. И. Монастырская[1], А. Н. Полетайкин[1, 2], Л. Ф. Данилова[1]

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

Аннотация: В статье отражена разработка технологии оценивания цифровой зрелости организационной системы и её применение на примере образовательной организации высшего образования. Технология предполагает опрос работников организации в форме анкетирования и использует аппарат нечёткой логики для вычисления уровня цифровой зрелости. Для формирования рациональной системы нечёткого вывода применяется процедура группового экспертного оценивания и метод минимизации логических функций, адаптированный к обработке небулевых переменных. Полученная технология обладает научной новизной, которая заключается в комплексировании разнородных методов и моделей, и является интеллектуальной. Апробация технологии показала приемлемые по достоверности результаты оценивания цифровой зрелости организационной системы.

Ключевые слова: организационная система, цифровая трансформация, цифровая зрелость, показатели цифровой зрелости, опрос работников организации, методы экспертной оценки, нечёткая модель, нечёткий логический вывод, минимизация небулевых функций.

Для цитирования: Шевцова Ю. В., Монастырская Т. И., Полетайкин А. Н. Данилова Л. Ф. Технология оценивания цифровой зрелости образовательной организации. Часть II // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 34–48. https://doi.org/10.55648/1998-6920-2023-17-4-34-48.

Статья поступила в редакцию 23.11.2022;
переработанный вариант – 29.03.2023;
принята к публикации 29.04.2023.

1. Введение

Все организации время от времени сталкиваются с необходимостью обновления своих информационных систем и развития бизнес-процессов, для того чтобы быть конкурентоспособными в рыночных условиях. Программы цифровой трансформации (ЦТ), как правило, выдвигают эти проблемы на первый план, особенно при выполнении реорганизации бизнес-процессов, таких как интеллектуальные рабочие процессы, информатизация и унифицированный клиентский опыт. За последние годы интерес к проблеме цифровой трансформации в России неуклонно растет, связано это с действием Национальной программы «Цифровая экономика Российской Федерации». Актуальность же данного исследования подкрепляется необходимостью разработки качественной технологии цифровой трансформации с целью повышения эффективности, конкурентоспособности и востребованности образовательных программ, которые реализуют организации высшего образования для формирования высоко-

* Работа выполнена в рамках государственного задания № 071-03-2022-001.

квалифицированных будущих кадров. Высокое качество образовательных программ необходимо обеспечивать не только фундаментальными составляющими, но и современными технологиями и инструментами, которые необходимы для соответствия требованиям активно развивающихся направлений цифровой экономики. Подробно данные обстоятельства рассмотрены авторами в первой части исследования [1].

Прежде чем подойти к выбору программы и стратегии цифровой трансформации организации, необходимо определить уровень её цифровой зрелости (ЦЗ). Так, по мнению Дирка Ифентхалера (Dirk Ifenthaler), модель цифровой зрелости вуза помогает определить текущее состояние внедрения и интеграции цифровых технологий, понимание и управление непрерывными изменениями, а также помогает упростить организационную трансформацию университета [2]. Углубленный и всеобъемлющий анализ цифровой трансформации университетов может осуществляться только посредством теоретически обоснованных моделей (эффективности) [3]. В этой связи основная задача исследования на текущем этапе состоит в создании точной, объективной и простой методики оценки ЦЗ образовательной организации высшего образования (ООВО), не требующей больших ресурсозатрат при её применении.

Интерес к выработке и применению методики оценки цифровой зрелости образовательных организаций высшей школы в последнее время достаточно часто встречается в научной литературе. Проводились исследования по оценке цифровой зрелости девяти профессиональных образовательных организаций г. Санкт-Петербурга [4], в Северо-Восточном федеральном университете им. М. К. Аммосова г. Якутска [5], Самарском государственном экономическом университете [6], в Омском государственном аграрном университете [7]. Все причисленные образовательные организации для решения задачи оценивания ЦЗ обращались к одной из двух существующих методик: «Паспорту цифровой зрелости», разработанному в Институте цифрового развития науки и образования МФТИ [8] и/или к разработке Центра перспективных управленческих решений [9]. Однако технологических решений, позволяющих не только получить оценки ЦЗ, но и подтвердить их достоверность, систематизировать исследуемую деятельность организационного объекта, а также обеспечить наработку лучших практик для решения задачи и эффективную их воспроизводимость, на текущий момент никто не предложил. Для таких целей создаются новые технологии (Know How), объединяющие определённым образом упорядоченную систему условий, критериев, форм, методов и средств решения поставленной задачи и достижения поставленной цели. Процесс создания новой технологии определённо является креативной деятельностью. Поэтому указанное здесь определение технологии задаёт не просто множество элементов технологии, а определенным образом упорядоченную их совокупность, то есть представляет технологию как систему [10].

В данном исследовании создаётся технология оценивания ЦЗ, новизна которой определяется следующими положениями:

– выполнена систематизация и усовершенствование набора показателей ЦЗ за счёт их дополнительного структурирования и введения двух новых блоков показателей;

– разработана новая математическая модель обработки результатов опроса на основе интеллектуального метода нечёткого логического вывода;

– получил развитие метод минимизации логических функций картами Карно, адаптированный к обработке небулевых переменных в четырёхзначной логике.

2. Постановка задачи

2.1. Исходные положения исследования

На предыдущем этапе исследования [1] авторами подробно рассмотрены такие компоненты технологии оценивания ЦЗ, как подходы к трактовке понятий «Цифровая трансформация» и «Цифровая зрелость» ООВО, условия и критерии конструктивизации цифровой

трансформации в образовании как её позитивного компонента, гармонизирующего отношения внутренних и внешних элементов образовательных систем за счёт применения современных информационно-коммуникационных средств и технологий. Также исследованы главенствующие модели и методики оценки уровня цифровой зрелости ООВО. Напомним, что под цифровой зрелостью мы предлагаем понимать состояние, характеризующее способность организации к реализации цифровой трансформации её деятельности. Очевидно, цифровая зрелость представляет собой комплексную многофакторную категорию, и измерение её уровня должно осуществляться через систему показателей, вместе в достаточной степени описывающих уровень цифрового развития организационного объекта.

2.2. Основные подходы к оценке уровня цифровой зрелости

Как уже представлено выше, на данном поле изысканий на настоящий момент обнаружено два концептуально разных подхода к идентификации и оценке показателей цифровой зрелости: разработки Института цифрового развития науки и образования МФТИ [8] и Центра перспективных управленческих решений [9].

Первый подход – нормативный (общесистемный), основан на определении значений различных показателей деятельности, которые согласно рекомендациям регулятора характеризуют уровень цифрового развития организации. Причём данные показатели проявляют, прежде всего, технико-технологическую составляющую категории цифровой зрелости организации, например, одним из показателей ЦЗ данной методики является следующий – «Доля сервисов для проведения исследований, действующих в ООВО, в общем количестве сервисов, действующих в ООВО» [8]. Это означает, что для применения данной методики организация должна обладать высокоразвитой, качественно поставленной системой сбора и верификации объективных данных для расчётов, что, в свою очередь, требует развитых интегрированных систем – информационной и методической – управления вузом. Однако концепция цифровой трансформации отрасли науки и высшего образования пока имеет недлительную историю существования в РФ [11], соответственно, необходимы методически более простые и менее ресурсозатратные методики оценки ЦЗ, которые организация могла бы применять на самых ранних этапах реализации стратегии и программы ЦТ.

Второй подход к оценке уровня ЦЗ, напротив, имеет выраженную когнитивную направленность и основан на проведении опроса сотрудников организации по различным направлениям цифровой трансформации деятельности и, соответственно, выражает их восприятие, способность и готовность к её реализации (пример одного из вопросов данной методики: «Как Вы можете описать уровень систематизации данных в рамках Вашей основной деятельности в подразделении?») [9]. Однако некоторые аспекты данной методики, а именно варианты ответов на её вопросы, которые, по сути, являются индикаторами проявления определённого уровня ЦЗ организации, находятся в закрытом формате (по крайней мере, для авторов настоящего исследования).

Таким образом, существующие на данный момент методические подходы к определению уровня ЦЗ организации оценивают либо технико-технологические [8], либо когнитивные [9] аспекты цифрового развития. В то время как комплексная всесторонняя оценка уровня ЦЗ объекта как организационной системы, на наш взгляд, должна основываться на интеграции оценок трёх ключевых направлений ЦТ организации: технико-технологического, когнитивного и личностного. Более подробно аргументация по данному поводу представлена в [1].

Также ключевым с точки зрения достоверности получаемых результатов методическим обстоятельством при оценке уровня ЦЗ является способ свёртки частных показателей ЦЗ в интегральный. Вычисление интегрального уровня ЦЗ организации во всех описываемых моделях в той или иной степени основывается, по сути, на вычислении средневзвешенного значения показателей, характеризующих ЦЗ. Например, в модели МФТИ «итоговый рейтинг цифровой зрелости ООВО рассчитывается путем сложения итоговых рейтингов по каждому критерию достижения цифровой зрелости, указанных в паспорте цифровой зрелости» [8].

Модель, разработанная Центром перспективных управленческих решений, в свою очередь, предполагает вычисление «итогового уровня цифровой зрелости» как среднего значения оценок уровня ЦЗ по различным «блокам направлений оценки». Также предлагается визуальное представление полученных оценок с помощью лепестковой диаграммы [9].

Кроме того, в Стратегии цифровой трансформации отрасли науки и высшего образования заявляется, что ООВО может самостоятельно выбирать методику оценки уровня ЦЗ [11].

2.3. Формализация задачи исследования

Ставится задача разработать методику вычисления уровня ЦЗ ООВО как ядро технологии оценивания цифровой зрелости:

– не предъявляющую высокие требования к развитости ИТ-инфраструктуры для реализации процедур оценивания и, соответственно, обеспечивающую возможность её применения на самых ранних этапах становления системы ЦТ организации;

– реализующую полноту проявления технико-технологического, когнитивного и личностного потенциалов цифрового развития организации высшего образования;

– основанную на индикаторах проявления уровней ЦЗ, отражающих особенности процессов именно образовательной организации высшего образования;

– поддерживающую возможность совместной обработки и объективных данных, и субъективных экспертных оценок, характеризующих различные аспекты цифрового развития организации.

Объектом исследования является цифровая трансформация образовательной деятельности ООВО посредством гибридного математического моделирования.

Предмет исследования – математические модели и методы оценки уровня цифровой зрелости ООВО.

3. Разработка методики оценки уровня цифровой зрелости ООВО

В наибольшей степени представленным выше требованиям к методике оценки уровня ЦЗ ООВО в качестве базовой соответствует методика Центра перспективных управленческих решений [9], главным образом потому что она не требует развитой информационной системы сбора и обработки оценочный данных, так как представляет собой опрос сотрудников организации, и, соответственно, может также рассматриваться и как экспресс самодиагностика организации на начальном этапе становления системы оценки ЦЗ для выявления цифровых слабостей организации как потенциала роста и приоритетных направлений развития и цифровых сил как ключевых конкурентных преимуществ.

При этом авторами исследования в методику оценки уровня ЦЗ ООВО Центра перспективных управленческих решений [9] внесены следующие модификации:

– методика оценки цифровой зрелости дополнена двумя оригинальными блоками показателей: «Личностный фактор» и «Глобальная цифровая среда», тем самым представлен весь спектр направлений цифровизации: технико-технический, когнитивный, личностный;

– выработаны индикаторы проявления уровней цифровой зрелости, отражающие особенности образовательных, административных и научно-исследовательских процессов именно образовательной организации высшего образования, так как данный аспект исходного опросного материала, как уже отмечалось, закрыт.

Заметим, что разработанная модель оценки уровня цифровой зрелости в полной конфигурации дана в работе [12], здесь же она представлена в укрупнённом формате.

Предлагается следующая модель структуры категории «Цифровая зрелость образовательной организации»:

– факторы ЦЗ: технико-технологический (ТТФ); когнитивный (КФ); личностный (ЛФ);

– блоки показателей ЦЗ: 1 Личностный фактор; 2 Компетенции; 3 Организационная культура; 4 Процессы; 5 Продукты; 6 Модели; 7 Данные; 8 Инфраструктура и инструменты; 9 Глобальная цифровая среда;

– частные показатели ЦЗ: 1.1 Степень адекватности понимания нравственного и социального аспектов цифровизации, 1.2 Степень демократичности цифровизации процессов, 1.3 Степень воздействия цифровизации на личностный рост; 2.1 Уровень развития цифровых компетенций сотрудников, 2.2 Уровень владения цифровыми и аналитическими инструментами, 2.3 Зрелость подхода к развитию цифровых компетенций; 3.1 Развитость цифровых инструментов управления задачами, 3.2 Инициативность исполнителей при управлении задачами, 3.3 Осуществление промежуточного контроля и оценки результатов; 4.1 Зрелость управления процессами, 4.2 Возможности оптимизации процессов, 4.3 Степень автоматизации процессов; 5.1 Участие в создании цифровых продуктов, 5.2 Применение цифровых технологий в создании продуктов, 5.3 Управление требованиями к цифровым продуктам; 6.1 Уровень владения аналитическими методами, 6.2 Уровень цифровизации траекторий развития обучающихся; 7.1 Степень систематизации данных, 7.2 Уровень обработки данных, 7.3 Качество данных; 8.1 Организация рабочих мест (техническое обеспечение учебных аудиторий), 8.2 Развитость цифровых сервисов для сотрудников, 8.3 Обеспечение информационной безопасности; 9.1 Степень цифрового единства, 9.2 Степень ясности понимания принадлежности к глобальной цифровой среде.

Структура описанной модели оценки уровня ЦЗ показана на рис. 1.

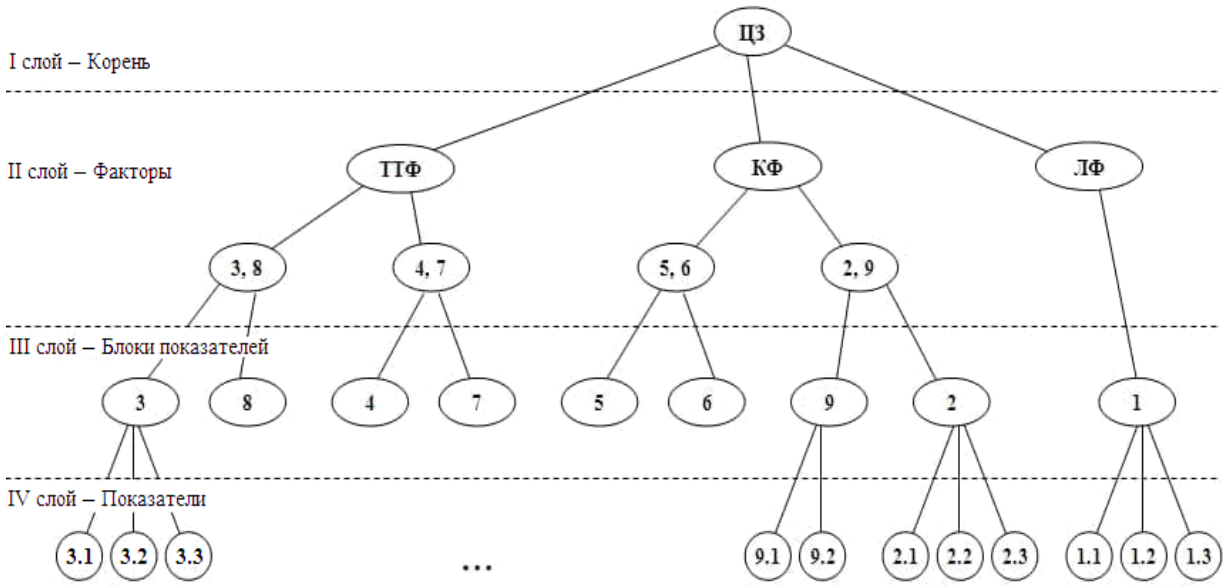

Рис. 1. Древовидная структура системы показателей уровня цифровой зрелости организации в контексте свёртки в системе правил нечёткого логического вывода (узлы нижнего уровня II-го слоя выполняют исключительно техническую функцию и не несут смысловой нагрузки)

Полученный набор показателей должен быть систематизирован путём применения адекватного формального математического аппарата и организован в форме системы компьютерного мониторинга ЦЗ ООВО. В условиях неопределенности исходных данных в качестве такого систематизирующего базиса целесообразно принять аппарат нечёткого логического вывода. Этот формализм достаточно хорошо зарекомендовал себя в решении задачи нечёткого оценивания сформированности компетенций [13], а его адекватность и достоверность обсуждались 2 года назад на страницах этого журнала [14]. Особо отметим, что аппарат нечёткого логического анализа обеспечивает совместную обработку различных по природе происхождения исходных данных: и объективных данных, характеризующих состояние системы, и данных, основанных на субъективных оценках экспертов об этом. Таким образом может вы-

полняться ранее установленное требование к методике оценки ЦЗ об интеграции разнородных данных.

Зададим представленные выше частные показатели цифровой зрелости организации и их свёртки: блоки показателей ЦЗ, факторы ЦЗ и её интегральную оценку – лингвистическими переменными:

$$<"Цифровая\ зрелость", D=[0,100],\ T=\{"Уровень\ 0",...,"Уровень\ 3"\}>,$$
$$<"Уровень\ 0"(ЦЗ), D=[0,100],\ \{(d,\ \mu_{"Уровень\ 0"(ЦЗ)}(d))\,|\,d\in D\}>,$$
$$\mu_{"Уровень\ 0"}(ЦЗ)=trap(0;0;20;40),\ \mu_{"Уровень\ 1"}(ЦЗ)=trap(0;20;40;70),$$
$$\mu_{"Уровень\ 2"}(ЦЗ)=trap(20;40;70;100),\ \mu_{"Уровень\ 3"}(ЦЗ)=trap(40;70;100;100);$$
$$<"7.3.\ Качество\ данных", U=[0,3],\ T=\{"Уровень\ 0",...,"Уровень\ 3"\}>,$$
$$<"Уровень\ 0"(x_{7.3}), U=[0,3],\ \{(u,\ \mu_{"Уровень\ 0"(x_{7.3})}(u))\,|\,u\in U\}>,$$
$$\mu_{"Уровень\ 0"}(x_{7.3})=tri(0;0;1),\ \mu_{"Уровень\ 1"}(x_{7.3})=tri(0;1;2),\ \mu_{"Уровень\ 2"}(x_{7.3})=tri(1;2;3),$$
$$\mu_{"Уровень\ 3"}(x_{7.3})=tri(2;3;3).$$

Установление формы и параметров функции принадлежности нечётких множеств ($\mu_{"\_"}(d)$, $\mu_{"\_"}(u)$), а также границ универсального множества каждой переменной (D,U) основано на их содержательной сущности. Множество термов каждой переменной модели (T) включает четыре её возможные состояния, соответствующие четырём уровням ЦЗ организации. Методическими рекомендациями [8] предписывается выделять четыре уровня ЦЗ организации, характеристика которых и диапазоны оценок по 3-балльной и 100-балльной шкалам действительных чисел показана в табл. 1.

Таблица 1. Уровни оценки цифровой зрелости организации

Уровень ЦЗ	Диапазоны оценок		Наименование и краткая характеристика уровня цифровой зрелости
	$U\in[0,3]$	$D\in[0,100]$	
Уровень 0	$u=0$	$d\in[0,20]$	Нулевой уровень ЦЗ: незрелость систем, персонала и связывающих их процессов и, как следствие, невозможность реализовать проекты цифровой трансформации
Уровень 1	$u=1$	$d\in[20,40]$	Начальный уровень ЦЗ: фрагментарная информатизация деятельности, значимых эффектов от цифровизации не достигнуто
Уровень 2	$u=2$	$d\in[40,70]$	Базовый уровень ЦЗ: системная цифровизация деятельности, за счет чего процессы оптимизируются, принятие решений осуществляется на основе интеллектуального анализа данных
Уровень 3	$u=3$	$d\in[70,100]$	Продвинутый уровень ЦЗ: состояние цифровой трансформации, в деятельности организации появляются новые процессы, продукты и модели с принципиально новыми свойствами

Крайняя оценка $u=3$ обозначает идеальный уровень ЦЗ по показателю. Крайняя оценка $d=100$ обозначает идеальный уровень ЦЗ организации в целом и отражает состояние тотальной цифровой трансформации её деятельности.

Свёртку частных показателей цифровой зрелости в укрупнённые и далее в интегральный показатель уровня ЦЗ предлагается осуществлять с помощью правил нечёткого логического вывода типа Мамдани. Выработка базы правил осуществлялась на основании экспертных суждений авторов методики, так как моделируемая предметная область находится в методически некомфортных условиях высокой информационной неопределенности: ограниченности исходных данных и отсутствия значений выходной моделируемой переменной – непосредственно значения уровня ЦЗ.

Каждым экспертом даны оценки значений выходной лингвистической переменной по полному набору конституент значений входных переменных нечёткой модели по принятой шкале $U = \{0, 1, 2, 3\}$, например, (If «7.1 Степень систематизации данных» = 0 and «7.2 Уровень обработки данных» = 0 and «7.3 Качество данных» = 0, then «7. Данные» = u). Степень согласованности экспертных оценок оценивалась с помощью показателя среднего абсолютного отклонения: $\overline{MAD} = 14.01\,\%$; $\max MAD = 24.80\,\%$. Таким образом, полученный экспертный материал следует считать в достаточной степени согласованным и пригодным для дальнейшего использования.

Далее для получения обобщённых формулировок правил нечёткого логического вывода оценки, полученные от всех экспертов, усреднялись. Таким образом было сгенерировано 688 правил ($8\times4^3+1\times4^2+4\times4^2+2\times4^2+4^3$ согласно структуре модели оценки, см. рис. 1). С целью минимизации полученной базы правил применялся модифицированный способ минимизации логических функций картами Карно для переменных, не являющихся булевыми. Детали данной минимизации раскрыты в статье [12]. В результате система правил нечёткого логического вывода была редуцирована до 255 правил, фрагмент которой в графической форме представлен на рис. 2. На этом можно заключить, что нечёткая модель оценки уровня ЦЗ ООВО построена.

При оценке качества работы построенной модели важно иметь в виду, что моделируемая категория – цифровая зрелость – является синтетической величиной, которая измеряется не непосредственно, а через систему показателей, вместе ассоциирующихся с уровнем цифрового развития организационного объекта. Соответственно, не имеется истинного значения выходной моделируемой переменной. Поэтому не представляется возможным провести тестирование модели в классическом смысле через количественную оценку ошибки результатов её работы. В таком случае оценка качества работы модели может осуществляться только экспертно, на рациональном уровне специалистами по цифровой трансформации организаций.

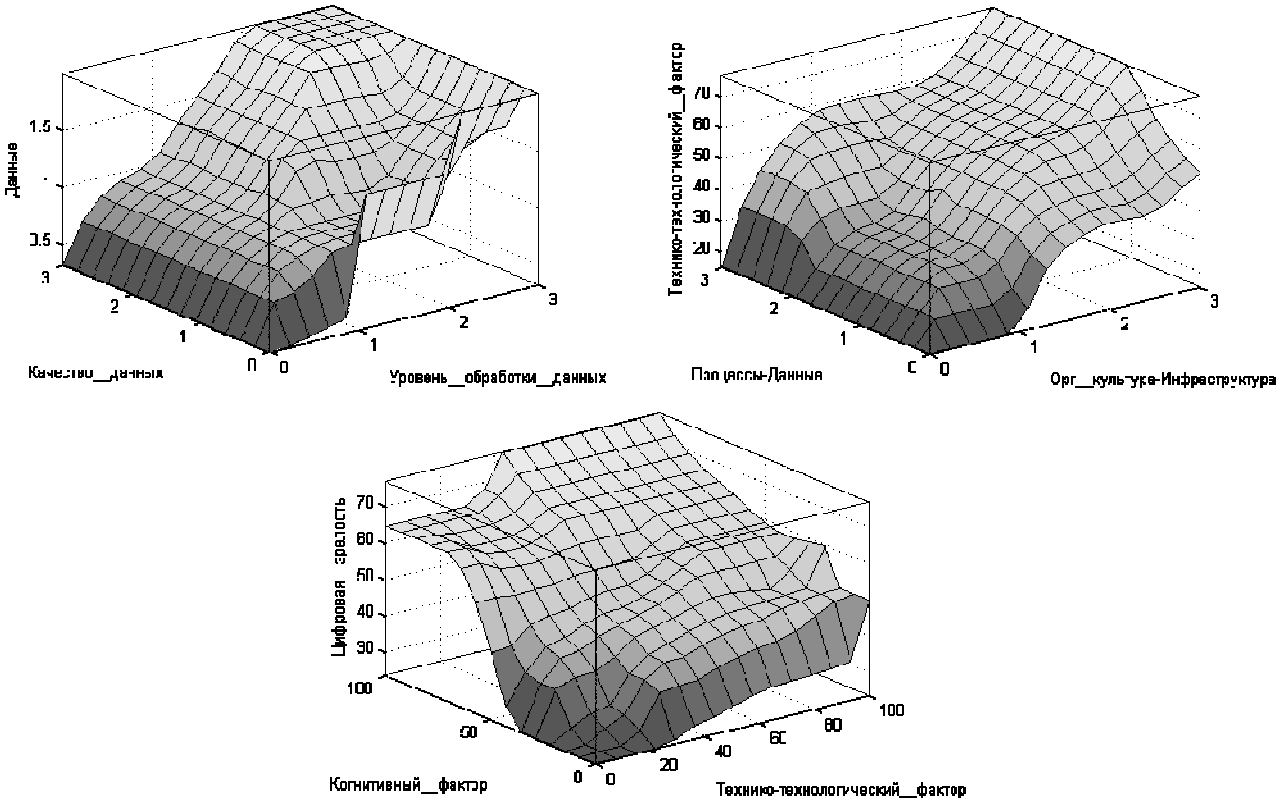

Рис. 2. Поверхности зависимости переменных нечёткой модели оценки уровня ЦЗ организации

Определим оценки чувствительности разработанной нечёткой модели на граничных значениях её некоторых входов (табл. 2). Основные выводы из этого анализа:

– ЦЗ организации не достигает 100-балльного уровня даже при 100-балльном значении всех модельных влияющих факторов. Это обстоятельство может быть объяснено, например, тем, что моделируемая предметная область относится к классу слабо структурированных задач в условиях неопределённости, когда на моделируемую переменную, очевидно, оказывают влияние не только идентифицированные в модели факторы;

– при прочих равных условиях набольшее индивидуальное влияние на уровень ЦЗ организации оказывает когнитивных фактор, а именно готовность и способность сотрудников организации к цифровой трансформации;

– при прочих равных условиях наибольшее совместное влияние на уровень ЦЗ организации оказывает связка когнитивного и технико-технологического факторов.

Таблица 2. Анализ чувствительности разработанной нечёткой системы оценки уровня ЦЗ ООВО

Вектор входных переменных, балл	Выходная переменная, балл
$(z_1, z_2, z_3) = (0; 0; 0)$	$DM = 15.3$
$(z_1, z_2, z_3) = (100; 100; 100)$	$DM = 76.9$
$(z_1, z_2, z_3) = (100; 0; 0)$	$DM = 50$
$(z_1, z_2, z_3) = (0; 100; 0)$	$DM = 76.9$
$(z_1, z_2, z_3) = (0; 0; 100)$	$DM = 27.9$
$(z_1, z_2, z_3) = (100; 100; 0)$	$DM = 76.9$
$(z_1, z_2, z_3) = (0; 100; 100)$	$DM = 55.1$
$(z_1, z_2, z_3) = (100; 0; 100)$	$DM = 50$

4. Апробация методики оценивания цифровой зрелости ООВО

4.1. Проведение эксперимента

Апробация разработанной методики оценивания ЦЗ проводилась в СибГУТИ в течение июня 2022 г. В исследовании приняли участие 80 сотрудников из 23 подразделений университета, среди обследованных в основном были доценты и старшие преподаватели, женщины в возрасте от 31 до 40 лет со стажем работы в университете от 11 до 20 лет. Большинство респондентов (22 чел.) работают на кафедре математического моделирования и цифрового развития бизнес-систем (ММиЦРБС), что обусловлено, на наш взгляд, прежде всего, тем, что пилотная апробация разработанной методики проводилась именно на кафедре ММиЦРБС [15]. В качестве метода исследования использовался опрос, в качестве разработанного социологического инструментария – электронная анкета на платформе Google Forms (URL: `https://forms.gle/5Srd3ChdXqpuMDoQA`).

Цифровой профиль СибГУТИ по частным показателям ЦЗ, блокам показателей ЦЗ и уровень ЦЗ университета в целом представлены на рис. 3. Прежде всего, обращает на себя внимание явно выраженная недостаточность автоматизации, что, очевидно, затрудняет процесс цифровой трансформации исследуемого объекта. Характерно, что в образовательной деятельности университета практически не используются прогрессивные интеллектуальные технологии и системы, необходимые для эффективной цифровой трансформации. Вместе с тем следует отметить наличие необходимого для цифрового развития организации кадрового

потенциала. Это выражается средними оценками блоков 1 и 2 и некоторых когнитивных компонентов блоков 3–5. Работники университета в отношении цифровой трансформации занимают ответственную и осознанную позицию, готовы к использованию цифровых продуктов и к участию в их разработке на базе организации. Для этого им необходимы цифровые инструменты, функционирующие на основе развитой ИТ-инфраструктуры вуза.

Рис. 3. Профиль цифровой зрелости СибГУТИ по частным показателям (а) и укрупнённым блокам показателей (б)

Полученные в результате опроса данные были подвержены корреляционному анализу Пирсона для оценки взаимосвязей показателей «Стаж работы» и «Возраст» с показателями анкеты. Так, для показателя «Возраст» выявлена положительная умеренная достоверная ($p < 0.05$) связь с показателем «С помощью каких инструментов в основном осуществляется постановка задач руководителем в рамках Вашей основной деятельности в подразделении?» ($r = 0.31$) и положительная слабая достоверная ($p < 0.05$) связь с показателем «Как чаще всего контролируется руководителем качество Вашей работы по реализации поставленных задач /выполненной работы?» ($r = 0.25$). Для показателя «Стаж работы» выявлена отрицательная слабая достоверная ($p < 0.05$) связь с показателем «В Вашей образовательной организации развернута и поддерживается дискуссия о целесообразности цифровой трансформации образования и науки, и в этой дискуссии открыто могут принять участие любые сотрудники и студенты, тем самым делая свой вклад в это общее дело?» ($r = -0.23$).

Таким образом, выявлено, что чем выше возраст обследованного, тем выше уровень ЦЗ при постановке задач и контроле выполнения задач в подразделении. Чем больше стаж работы обследованного, тем ниже его уверенность в наличии и поддержании дискуссии о целесообразности цифровой трансформации образования и науки, в которой открыто могут принять участие любые сотрудники и студенты.

Особо отметим, что при заполнении анкеты респондентам была дана возможность оставить свои дополнения и замечания к опросному материалу и проблематике цифровизации образования в целом, при этом получено несколько (3.75 %) негативных впечатлений, например: «Многие вопросы не понятны. Отвечал наобум», «Анкета непонятно о чём» и др. Ответы данных респондентов были исключены из анализа. Наличие подобных реакций интерпретируется, прежде всего, как то обстоятельство, что проведение подобных новационных исследований требует предварительной подготовки респондентской базы путем обучения, инструктажа, консультирования и т.п.

4.2. Исследование структурных свойств цифровой зрелости организации

При проведении анализа структуры полученных результатов обращает на себя внимание превалирование когнитивной составляющей ЦЗ (блоки 2, 5, 6, 9, см. рис. 1) над технико-технологической (блоки 3, 4, 7, 8) на 13 %. Личностный же фактор (блок 1) превышает оценку ТТФ на 38 %. Выражена явная диспропорция за счет недоразвитости технико-технологической составляющей организации, все блоки показателей которой находятся в области начального уровня ЦЗ. Это проблема непрерывного улучшения процессов организации за счет конструктивной цифровой трансформации, основные положения которой в отношении образовательной организации изложены в статье [1].

Для повышения ЦЗ необходимы квалифицированные организационные решения реинжиниринга бизнес-процессов по управлению: а) персоналом, б) процессами, в) продуктами, г) данными, д) качеством. С учетом выявленных проблем с ИТ-инфраструктурой и автоматизацией необходимы также адекватные решения по достаточному финансированию мероприятий а–д. Лишь такое комплексное решение позволит успешно выполнить утвержденную в 2021 году Стратегию цифровой трансформации отрасли науки и высшего образования [11]. Для эффективной реализации такого решения в числе прочего необходимо обеспечить компьютерный мониторинг ЦЗ ООВО в режиме реального времени с оперативным отражением реального профиля ЦЗ в паспорте цифровой зрелости организации. А при отсутствии такой возможности в силу недостаточной развитости ИТ-инфраструктуры и технологий управления данными следует осуществлять оценивание ЦЗ посредством предложенной технологии оценивания по крайней мере ежегодно и с максимально полной вовлечённостью работников организации в качестве респондентов в рамках принятия соответствующих организационных решений.

Полученный в результате процедуры оценивания профиль, пример которого представлен на рис. 3, позволит идентифицировать блоки показателей ЦЗ, требующие первоочередного

внимания со стороны руководства организации и приоритетного их развития. В приведенном примере таковыми являются блоки 7 и 9. Воздействия на «недоразвитые» блоки ожидаемо повысят цифровую зрелость и других блоков показателей ЦЗ в силу их опосредованного взаимовлияния. Например, при приоритетном решении задачи управления данными ООВО (для развития блока 7) неизбежно потребуется разработка моделей анализа данных, включая их программную реализацию и внедрение в производственный процесс в качестве цифрового продукта с вовлечённостью в его жизненный цикл работников ООВО. Это, в свою очередь, повлечёт приращение цифрового развития организации по всем остальным блокам, предположительно, и по блоку 9, так как результаты анализа данных и повышение их качества, скорее всего, положительно отразятся на понимании работниками принадлежности организации к глобальной цифровой среде. Позитивные тенденции цифрового развития ООВО, находящие отражение в публичной части паспорта ЦЗ, способствуют более глубокой интеграции вуза в глобальную цифровую среду, обеспечивая тем самым реализацию Стратегии [11].

5. Заключение

В результате исследования создана новая технология как система условий, критериев, форм, методов и средств для оценивания ЦЗ организационного объекта на примере ООВО. Для этого осуществлена формализация древовидной структуры системы показателей уровней цифровой зрелости организации, предложены новые методики построения системы правил нечёткого вывода с применением карт Карно и обработки результатов опроса работников организации с использованием аппарата нечёткой логики. Представлены результаты апробации созданной технологии на базе СибГУТИ, которые сопоставлены с результатами более ранней апробации в рамках структурного подразделения СибГУТИ – на кафедре ММиЦРБС. Также выявлены корреляционные зависимости показателей ЦЗ на основе ответов респондентов. Приведена оценка цифровой зрелости организации в целом и дифференциально по каждому из блоков показателей, которая дополнена интерпретацией полученных результатов. С учетом включения в состав технологии методов и подходов искусственного интеллекта, таких как нечёткая логика и групповая экспертиза, созданную технологию можно считать интеллектуальной.

Заметим, что разработанный вариант реализации технологии оценки ЦЗ организации, основанный на нечёткой обработке данных опроса работников, следует рассматривать лишь как начальный этап формирования системы оценки ЦЗ. Развитие данной интеллектуальной технологии до уровня сквозной требует включения в неё методов и средств поддержки принятия управленческих решений по цифровому развитию организации на всех этапах жизненного цикла её деятельности. Для этого в том числе необходимы методы и модели класса Data Mining, обеспечивающие сбор, предобработку и предварительный анализ объективных данных о деятельности организации в режиме реального времени (ещё раз подчеркнём, что предлагаемая технология нечёткого логического анализа обеспечивает совместную обработку как субъективных, так и объективных данных). Однако осуществление такого интеллектуального мониторинга требует наличия развитой ИТ-инфраструктуры организации, что само по себе является признаком высокого уровня цифрового развития объекта.

Таким образом, для эффективного цифрового развития организационного объекта в условиях применения созданной технологии необходима последовательная реализация следующих шагов:

1) приобретение, поставка и конфигурирование необходимой ИТ-инфраструктуры, достаточной для генерации и эффективной миграции данных о деятельности объекта;

2) разработка и внедрение автоматизированных средств реального времени для мониторинга и интеллектуального анализа показателей цифровой зрелости организации;

3) разработка на основе средств, указанных в пп. 1 и 2, и созданной технологии оценивания ЦЗ сквозной интеллектуальной технологии цифрового развития организации.

Дальнейшие исследования и будут направлены на создание такой сквозной интеллектуальной технологии, не противоречащей условиям и критериям конструктивности цифровой трансформации. Её создание и запуск в эксплуатацию будет означать достижение организацией в целом продвинутого уровня цифровой зрелости.

Выражение благодарности

Авторы выражают благодарность заместителю декана по научной работе факультета компьютерных технологий и прикладной математики, доценту кафедры информационных технологий Кубанского государственного университета Синице Сергею Геннадьевичу; заместителю директора по воспитательной работе института информатики и вычислительной техники, доценту кафедры социально-коммуникативных технологий СибГУТИ Логутовой Марине Алексеевне; профессору кафедры социально-коммуникативных технологий СибГУТИ Солодовой Галине Сергеевне; доценту кафедры математического моделирования и цифрового развития бизнес-систем СибГУТИ Черновой Наталье Исааковне за участие в тестировании методики оценивания ЦЗ ООВО; а также всем работникам СибГУТИ, которые приняли участие в опросе.

Также авторы выражают благодарность рецензентам за предложения по структуре и дополнения к тексту, которые учтены при доработке статьи.

Литература

1. *Канев В. С., Полетайкин А. Н., Шевцова Ю. В.* Технология оценивания цифровой зрелости образовательной организации. Часть I // Вестник СибГУТИ. 2021. № 3 (55). С. 63–76.
2. *Ifenthaler D., Egloffstein M.* Development and Implementation of a Maturity Model of Digital Transformation // TechTrends. 2020. № 64. P. 302–309. URL: `https://ifenthaler.info/website/?p=572` (дата обращения: 22.03.2022).
3. *Begičević Ređep N., Klačmer Čalopa M., Tomičić Pupek K.* The Challenge of Digital Transformation in European Education Systems // In: Moos L., Alfirević N., Pavičić J., Koren A., Čačija L. (eds) Educational Leadership, Improvement and Change. Palgrave Studies on Leadership and Learning in Teacher Education. Palgrave Pivot, Cham. URL: `https://link.springer.com/chapter/10.1007/978-3-030-47020-3_8` (дата обращения: 22.03.2022).
4. *Кашицин В. П.* Методика аудита цифровой зрелости организаций среднего профессионального образования // Вестник науки и образования. 2021. № 10-1 (113). С. 55–64.
5. *Саввинов В. М., Иванов П. П., Стрекаловский В. Н.* Методы и принципы оценки цифровой зрелости образовательных организаций // Вестник СВФУ им. М.К. Аммосова. Серия «Педагогика. Психология. Философия». 2021. № 2 (22). С. 28–40.
6. *Франтасов Д. Н.*, *Балановская А. В.* Цифровая зрелость как основа стратегического развития и цифровой трансформации образовательных организаций // Вестник Самарского государственного экономического университета. 2022. № 2 (208). С. 57–64.
7. *Шумакова О. В., Мозжерина Т. Г., Помогаев В. М., Крюкова О. Н.* Стратегия цифровой трансформации университета: вызовы и задачи реализации // Сборник трудов Всероссийской научно-практической конференции: Цифровизация аграрного образования: направления, методы, инструменты, Тюмень, 26 января 2022 года. Тюмень: Государственный аграрный университет Северного Зауралья, 2022. С. 112–122.
8. Паспорт цифровой зрелости / Институт цифрового развития науки и образования. URL: `https://scieddi.vsite.biz` (дата обращения: 30.09.2022).
9. Оценка цифровой зрелости / Центр перспективных управленческих решений. URL: `https://cpur.ru/projects_inside-project_grading` (дата обращения: 30.09.2022).

10. *Новиков Д. А.* Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. М.: ЛЕНАНД, 2016. 160 с.
11. Стратегия цифровой трансформации отрасли науки и высшего образования / Официальный сайт Минобрнауки России. URL: https://www.minobrnauki.gov.ru/documents/?ELEMENT_ID=36749 (дата обращения: 13.10.2022).
12. *Шевцова Ю. В., Данилова Л. Ф., Полетайкин А. Н., Монастырская Т. И.* Математическая модель нечёткого оценивания цифровой зрелости организационного объекта // Материалы XVIII международной азиатиатской школы-семинара «Проблемы оптимизации сложных систем», 20–30 июля 2022 г., Алматы, 2022. С. 5–16.
13. *Кунц Е. Ю., Полетайкин А. Н., Шевцова Ю. В.* Реализация модели нечеткого оценивания сформированности компетенций с помощью пакета MATLAB // Новые информационные технологии в образовании и науке. Екатеринбург: РГППУ. 2020. № 3. С. 66–72.
14. *Кунц Е. Ю., Полетайкин А. Н., Двуреченская Н. А.* Исследование достоверности нечеткой модели оценивания результатов обучения // Вестник СибГУТИ. 2020. № 4 (52). С. 92–97.
15. *Шевцова Ю. В., Полетайкин А. Н., Монастырская Т. И., Данилова Л. Ф.* Экспериментальное оценивание цифровой зрелости подразделения СибГУТИ // Материалы LXIII межвузовской научно-методической конференции «Актуальные вопросы совершенствования среднего профессионального и высшего образования в современных условиях», Новосибирск, СибГУТИ, 2022. С. 176–182.

Шевцова Юлия Владимировна
кандидат технических наук, доцент, доцент кафедры математического моделирования и цифрового развития бизнес-систем СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 269-82-78, e-mail: shevcova_yuliya@mail.ru, ORCID ID: 0000-0002-7464-068X.

Монастырская Татьяна Игоревна
кандидат социологических наук, доцент, доцент кафедры социально-коммуникативных технологий СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 269-82-78, e-mail: t.monastyrskaya@sibguti.ru, ORCID ID: 0000-0001-5458-0985.

Полетайкин Алексей Николаевич
кандидат технических наук, доцент, доцент кафедры информационных технологий Кубанского государственного университета (350040, Краснодар, ул. Ставропольская, 149), тел. (861) 219-95-77, e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952.

Данилова Любовь Филипповна
кандидат технических наук, доцент кафедры математического моделирования и цифрового развития бизнес-систем СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. (383) 269-82-78, e-mail: lubermolenko@yandex.ru, ORCID ID: 0000-0003-0907-0200.

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.*

Technology of Digital Maturity Estimation for an Educational Organization. Part II

Yuliya V. Shevtsova[1], Tatiana I. Monastirskaya[1],
Aleksey N. Poletaikin[1, 2], Lyubov Ph. Danilova[1]

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

Abstract: We present the developed system of estimating the digital maturity of an educational organization. The objective of estimating digital maturity has been formalized thanks to analyzing the existing approaches to validation of the digital maturity for an organizational object. The novelty of the given study is in introducing the fuzzy mechanism of integral estimation calculation of digital maturity into the digital maturity evaluation methodology. The methods of expert estimation, discrete mathematics and fuzzy logical inference were used to create the model. The utilization of the model developed is demonstrated on the example of higher education in the Russian Federation. The technique is adaptive and can be applied not only in educational organizations but also in organizations in other spheres of activity.

Keywords: organization, digital transformation, digital maturity, digital maturity indicators, employee survey, methods of expert assessment, fuzzy model, fuzzy logical inference, minimization of non-boolean functions.

For citation: Shevtsova Yu. V., Monastirskaya T. I., Poletaikin A. N., Danilova L. Ph. Technology of digital maturity estimation for an educational organization. Part II (in Russian). *Vestnik SibGUTI*, 2023. vol. 17, no. 4. pp. 34-48. https://doi.org/10.55648/1998-6920-2023-17-4-34-48.

The article was submitted: 23.11.2022;
revised version: 29.03.2023;
accepted for publication 29.04.2023.

References

1. Kanev V. S., Poletaykin A. N., Shevtsova Yu. V. Tekhnologiya otsenivaniya tsifrovoy zrelosti obrazovatelnoy organizatsii. Chast I [Technology of digital maturity estimation for an educational organization. Part I]. *Vestnik SibGUTI*, 2021, no. №3 (55), pp. 63-76.
2. Ifenthaler D., Egloffstein M. Development and Implementation of a Maturity Model of Digital Transformation. *TechTrends*, 2020, no. 64, pp. 302-309, available at: https://ifenthaler.info/website/?p=572 (accessed: 22.03.2022).
3. Begičević Ređep N., Klačmer Čalopa M., Tomičić Pupek K. The Challenge of Digital Transformation in European Education Systems. *Educational Leadership, Improvement and Change*, available at: https://link.springer.com/chapter/10.1007/978-3-030-47020-3_8 (accessed: 22.03.2022).
4. Kashitsin V. P. Metodika audita tsifrovoy zrelosti organizatsiy srednego professionalnogo obrazovaniya [Methodology of auditing the digital maturity for organizations of secondary vocational education]. *Vestnik nauki i obrazovaniya*, 2021, no. 10-1(113), pp. 55-64.
5. Savvinov V. M., Ivanov P. P., Strekalovskiy V. N. Metody i printsipy otsenki tsifrovoy zrelosti obrazovatelnykh organizatsiy [Methods and principles of digital maturity estimation for educational organizations]. *Vestnik SVFU im. M.K. Ammosova. Seriya «Pedagogika. Psikhologiya. Filosofiya»*, 2021, no. 2 (22), pp. 28-40.
6. Frantasov D. N., Balanovskaya A. V. Tsifrovaya zrelost kak osnova strategicheskogo razvitiya i tsifrovoy transformatsii obrazovatelnykh organizatsiy [Digital maturity as a basis for strategic development and digital transformation of educational organizations]. *Vestnik Samarskogo gosudarstvennogo ekonomicheskogo universiteta*, 2022, no. 2(208), pp. 57-64.

7. Shumakova O. V., Mozzherina T. G., Pomogaev V. M., Kryukova O. N. Strategiya tsifrovoy transformatsii universiteta: vyzovy i zadachi realizatsii [University digital transformation strategy: challenges and objectives]. *Sbornik trudov vserossiyskoy nauchno-prakticheskoy konferentsii «Tsifrovizatsiya agrarnogo obrazovaniya: napravleniya, metody, instrument*, 2022, pp. 112-122.
8. Pasport tsifrovoy zrelosti [Passport of digital maturity]. *Institut tsifrovogo razvitiya nauki i obrazovaniya,* available at: https://scieddi.vsite.biz, (accessed: 30.09.2022).
9. Otsenka tsifrovoy zrelosti [Digital maturity estimation]. *Tsentr perspektivnykh upravlencheskikh resheniy*, available at: https://cpur.ru/projects_inside-project_grading, (accessed: 30.09.2022).
10. Novikov D. A. *Kibernetika: Navigator. Istoriya kibernetiki, sovremennoe sostoyanie, perspektivy razvitiya* [Cybernetics: Navigator. History of cybernetics, current state, development prospects]. Moscow, LENAND, 2016. 160 p.
11. Strategiya tsifrovoy transformatsii otrasli nauki i vysshego obrazovaniya [Strategy of digital transformation for science and higher education]. *Ofitsialnyy sayt Minobrnauki Rossii*, available at: https://www.minobrnauki.gov.ru/documents/?ELEMENT_ID=36749, (accessed: 13.10.2022).
12. Shevtsova Yu. V., Danilova L. F., Poletaykin A. N., Monastyrskaya T. I. Matematicheskaya model nechetkogo otsenivaniya tsifrovoy zrelosti organizatsionnogo obekta [Mathematical model of fuzzy estimation of the digital maturity for an organizational object]. *Materialy XVIII mezhdunarodnoy aziatskoy shkoly-seminara «Problemy optimizatsii slozhnykh system»*, 2022, pp. 5-16.
13. Kunts E. Yu., Poletaykin A. N., Shevtsova Yu. V. Realizatsiya modeli nechetkogo otsenivaniya sformirovannosti kompetentsiy s pomoshchyu paketa MATLAB [Implementation of a fuzzy estimation model for the formation of competencies by MATLAB]. *Novye informatsionnye tekhnologii v obrazovanii i nauke*, 2020, no. 3, pp. 66-72.
14. Kunts E. Yu., Poletaykin A. N., Dvurechenskaya N. A. Issledovanie dostovernosti nechetkoy modeli otsenivaniya rezultatov obucheniya [Study of the reliability of a fuzzy model for estimation learning results]. *Vestnik SibGUTI*, 2020, no. 4 (52), pp. 92-97.
15. Shevtsova Yu. V., Poletaykin A. N., Monastyrskaya T. I, Danilova L. F. Eksperimentalnoe otsenivanie tsifrovoy zrelosti podrazdeleniya SibGUTI [Experimental estimation of the digital maturity for the SibSUTIS`s department]. Materialy LXIII mezhvuzovskoy nauchno-metodicheskoy konferentsii *«Aktualnye voprosy sovershenstvovaniya srednego professionalnogo i vysshego obrazovaniya v sovremennykh usloviyakh»*, 2022, pp. 176-182.

Yuliya V. Shevtsova

Cand. of Sci. (Engineering), Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: shevcova_yuliya@mail.ru, ORCID ID: 0000-0002-7464-068X, Scopus AuthorID: 56418422800, ResearcherID: ABG-4620-2020.

Tatiana I. Monastirskaya

Cand. of Sci. (Sociology), Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: t.monastyrskaya@sibguti.ru, ORCID ID: 0000-0001-5458-0985, Scopus AuthorID: 57217872787, ResearcherID: AAS-4398-2020.

Aleksey N. Poletaikin

Cand. of Sci. (Engineering), Assistant professor, Kuban State University (KubSU, Krasnodar, Russia), Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952, Scopus AuthorID: 57213829361, ResearcherID: ABF-6799-2020.

Lyubov Ph. Danilova

Cand. of Sci. (Engineering), Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: lubermolenko@yandex.ru, ORCID ID: 0000-0003-0907-0200, Scopus AuthorID: 57215304358, ResearcherID: ABG-8246-2020.

DOI: 10.55648/1998-6920-2023-17-4-49-61 УДК 04.056.5:378.3

Формирование вектора сетевых атак с учетом специфики связей техник и тактик

И. А. Ветров[1], В. В. Подтопельный[2]

[1] Балтийский федеральный университет им. И. Канта
[2] Калининградский государственный технический университет

Аннотация: Рассмотрены проблемы, возникающие при решении задачи построения вектора атаки в сетевой инфраструктуре. Приведены и охарактеризованы разновидности различных тактик и техник методик ФСТЭК, применяемых при построении вектора сетевой атаки, а также рассмотрена специфика их взаимосвязей с использованием марковских цепей при моделировании атакующих воздействий, рассмотрена их пригодность для различных процедур определения параметров вектора. При построении вектора сетевой атаки приводятся особенности определения вероятностей переходов системы в различные состояния компрометации сети. Формирование вектора атаки изучается в контексте эксплуатации многоуровневой корпоративной информационной системы. Определяются особенности построения упрощенного вектора атаки с учетом специфики связей тактик (состояний).

Ключевые слова: вектор атаки, информационная система, корпоративная сеть, уязвимость, марковские процессы, злоумышленник, тактики.

Для цитирования: Ветров И. А., Подтопельный В. В. Формирование вектора сетевых атак с учетом специфики связей техник и тактик // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 49–61. https://doi.org/10.55648/1998-6920-2023-17-4-49-61.

Статья поступила в редакцию 25.05.2023;
принята к публикации 07.06.2023.

1. Введение

В государственных учреждениях Российской Федерации для формирования вектора атаки, создаваемого в процессе аудита, используются различные руководящие документы государственных регуляторов в области информационной безопасности. Одним из основных документов является «Методика оценки угроз безопасности информации» ФСТЭК (далее – Методика). Описанный в данном документе способ построения вектора атаки предлагает использование тактик и принадлежащих им техник (различные приемы достижения некоего результирующего состояния, интерпретируются как тактика). При описании действий злоумышленника применяются разнообразные массивы данных о признаках угроз и уязвимостях. Затем с учетом экспертного мнения формируются векторы атак. При этом допускаются заимствования различных, в том числе зарубежных, способов описания сценариев реализации угрозы (CAPEC, OWASP, STIX, WASC, ATT&CK и др.) [1]. Также при формировании вектора учитывается потенциал возможных нарушителей (уровень их квалификации, средства атаки, цели).

Приведённая методика ориентирована на анализ открытых и распределенных информационных систем, использующих клиентско-серверную организацию, при этом не исключается рассмотрение локальных (замкнутых) систем. Однако в самой методике хотя и рассматривается понятие вероятности реализации различных тактик (фактически подразумевается прогноз возможных действий злоумышленника), сами численные значения вероятностей не применяются при описании сценария атаки. При этом описание вероятностей сопряжения и применения тактик основываются на экспертной оценке.

Таким образом, предлагаемое в методике описание сценария реализации несанкционированного доступа и вредоносного воздействия не подразумевает формальный учёт вероятностных показателей реализуемых тактик и, соответственно, техник злоумышленника, что не позволяет отследить изменение состояния вектора атаки при его развертывании.

Сегодня аспекты формирования сценария атаки исследуются разными способами. В частности, формирование векторов атаки изучают в контексте описания моделей угроз безопасности многоуровневых систем критически важных объектов. При составлении моделей могут использоваться табличные методы оценки риска [3]. Другие исследователи акцентируют свое внимание на методиках статистического анализа. В частности, предполагается «выявление аномалий в сетевом трафике за счет определения степени самоподобия трафика с использованием фрактального анализа и статистических методов» [4]. Также разрабатываются методики, учитывающие выявление взаимного влияния отдельных компьютерных атак на средства защиты сети [5]. Применяются различные методы искусственного интеллекта (нейронные сети, генетические алгоритмы, модели фильтрации на основе машинного обучения), вероятностные методы. В частности, используются различные виды марковских сетей. Предлагается использовать марковские и полумарковские модели описания действий злоумышленника для вычисления основных стационарных характеристик процесса проведения атаки [6]. Также описываются с помощью марковских процессов сценарии атак, модели функционирования сети с распределенными атакующими элементами [7]. Рассмотренные методики описания атак не связаны напрямую со специфическими особенностями способа формирования вектора атаки Методики ФСТЭК.

Таким образом, для более точного определения специфики атакующих воздействий предложенный в Методике способ построения вектора атаки можно дополнить простыми (то есть не вызывающими затруднения при построении модели угроз и в целом при аудите информационной безопасности) формальными способами определения вероятностей реализации тактик в едином сценарии с учетом вероятностей сопряжения различных техник, приводимых в Методике. Построение модели атаки с учетом вероятностей переходов из одного состояния компрометации в другое позволит прогнозировать появление событий безопасности в информационной системе с учетом атакующих воздействий внешнего нарушителя [2].

2. Проблемная область формирования вектора атаки

В большинстве случаев при аудите инфраструктуры организации изучается состояние безопасности многосегментной корпоративной информационной системы (КИС). Атакуемая сеть распределенного типа рассматривается как единое целое [7]. При атаке проявляются маркеры событий безопасности. Совокупность подобных маркеров интерпретируется как состояние из набора тактик, достигаемое техниками из приведенного в Методике списка (само осуществление техники уже может интерпретироваться как некое состояние компрометации). Сопряжение данных состояний, распределённых по времени и последовательно проявляющихся, требуется ассоциировать с компонентами инфраструктуры предприятия. Таким образом, формируется модель связанных между собой этапов атаки с учетом сетевой топологии.

При этом следует учитывать специфику модели нарушителя (в данном случае рассматривается внешний нарушитель). Соответственно, последовательность атакующих воздействий будет начинаться за границами описываемого сегмента сети, если атака реализуется по

отношению к сегменту, или за границами сети (при атаке на сеть в целом). Следует учитывать, что состояние компрометации сегмента сети может быть следствием компрометации всей инфраструктуры, которая была заражена после успешной атаки на другой ее сегмент. Поэтому необходимо четкое понимание того, где проходят границы сети и границы ее сегментов. При описании сценария компрометации всей инфраструктуры организации вектор атаки одного сегмента будет лишь одним из множества векторов и, следовательно, будет обозначен как один из множества этапов атакующих воздействий. Соответственно, вектор будет включен в общий граф состояний компрометации всей сети как одна из его вершин [6].

Нужно сказать, что при подобном подходе, следуя Методике оценки угроз ФСТЭК, критерием успешности атаки будет считаться не минимизация времени действий нарушителя (предполагается, что при более длительном проведении атаки злоумышленник рискует быть обнаруженным, и, следовательно, атака будет прервана), а сам факт достижения состояния реализации тактики № 10 («Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям») [1]. В таком случае следует определить причинно-следственные связи, которые позволили реализоваться конечному состоянию, маркирующему успешность атакующих действий. Соответственно, требуется исследовать промежуточные состояния между начальными техниками и конечными, их взаимосвязи, рассмотреть их возможные переходы из одного состояния в другое для достижения конечного состояния.

Также следует понимать, что событие, которое распознаётся как признак реализации одной из техник, может фиксироваться не только на начальных этапах компрометации, но и на промежуточных этапах (состояниях) развёртываемой атаки [7]. Задача аналитика безопасности состоит в том, чтобы определить специфику этого события, то есть его класс в соответствии с предложенной в Методике классификацией. Это необходимо для выявления либо предшествующий последовательности действий злоумышленника, которые были не замечены системами безопасности и которые следует обнаружить, либо последующей последовательности [8]. Воздействие на ресурсы инфраструктуры предприятия может произойти в любой момент, поэтому процесс перехода из состояния работоспособности в состояние аномального характера можно представить в виде дискретной марковской последовательности.

Таким образом, используя принципы формирования марковских цепей, можно создать вектор атаки с учетом вероятностей реализации разных этапов (состояний) компрометации и далее определить модель атаки.

3. Построение вектора атаки с учетом тактик атакующих воздействий

При построении вектора атаки создается последовательность связанных состояний, которые реализуются в виде череды фиксируемых в определённый период времени событий, маркирующих состояние компрометации на сетевых узлах. Последовательность состояний (маркируемых событий) с учетом периода фиксации и очередности событий, классифицируемых по принадлежности к тактикам, формируется с учетом возможного наличия других векторов атак. При этом в каждом случае предполагается различная величина вероятностей переходов к новым состояниям, которые ориентированы на приближение к итоговым целям злоумышленника. Это позволяет определить не только возможность реализации атаки в целом, но и отнести к какой-либо вероятностной последовательности некое маркированное событие безопасности, то есть к ряду событий конкретной атаки в череде множества атак [9]. В итоге это влияет на приоритет ветви вектора при выборе сценария действий злоумышленника, а значит, позволяет определить актуальность вектора. Таким образом, основным параметром в описании вектора состояний является вероятность перехода некоего компрометированного состояния в новое в соответствии с последовательностью классифицируемых в Методике тактик. На основе параметров вероятностей переходов и начальных состояний можно сформировать граф. Для этого необходимо ассоциировать тактики и состояния, которые будут

являться вершинами графа, описывающего марковские процессы. По требованиям Методики предполагается их последовательное соединение.

Выделяются следующие типы состояний, являющиеся результатом осуществления тактик:

1. Разведка (поиск и агрегация информации о системах и сетях целевой инфраструктуры) (Т1).
2. Первичная компрометация инфраструктурных компонентов систем и сетей (Т2).
3. Внедрение и эксплуатация средств разрушающего программного воздействия в системах и сетях (Т3).
4. Получение прав пользователя и сохранение доступа к системе или сети (Т4).
5. Управление средствами разрушающего программного воздействия в системах, сетях и (или) скомпрометированными компонентами (Т5).
6. Повышение уровня доступа к компонентам систем и сетей (Т6).
7. Сокрытие действий и применяемых при атаке средств (Т7).
8. Компрометация смежных подсистем (Т8).
9. Поиск и вывод данных из системы (Т9).
10. Несанкционированный доступ и компрометация инфраструктуры (Т10).

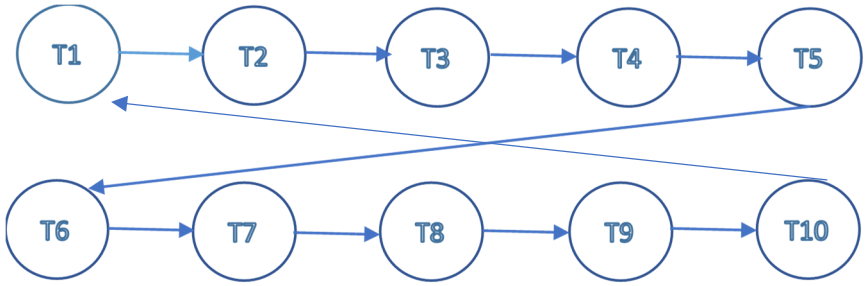

Рис. 1. Связанные состояния (этапы атаки) с учетом последовательности реализации

В графе присутствует связь состояний (как маркированных событий вредоносных воздействий). При распространении вектора атаки требуется условные распределения вероятностей сделать зависимыми только от предыдущего времени их фиксации:

$$\begin{aligned} P(y_3 \mid y_1, y_2) &= P(y_3 \mid y_2); \\ P(y_4 \mid y_1, y_2, y_3) &= P(y_4 \mid y_3); \\ P(y_n \mid y_1, \ldots, y_{n-1}) &= P(y_n \mid y_{n-1}). \end{aligned} \tag{1}$$

Далее классифицируются признаки событий, все случайные последовательности, которые соответствуют правилу марковской последовательности [2]:

$$P(y_1, \ldots, y_n) = P(y_1) \prod_{i=2}^{n} p(y_i \mid y_{i-1}), \tag{2}$$

где показатель y_{i-1} – предшествующее скомпрометированное состояние сетевого узла с фиксированным признаком атаки.

Процесс перехода из состояния (осуществленных тактик) в следующие состояния при соблюдении последовательностей на основе функциональной взаимосвязи описывается в виде дискретной марковской последовательности. Для выбранных периодов времени Δt вероятности перехода имеют вид [7]:

$$p_{ii}(t, t+\Delta t) = 1 - \lambda_{ii}(t) \cdot \Delta t + o(\Delta t),$$

$$p_{ij}\left(t, t+\Delta t\right) = \lambda_{ij}\left(t\right)\cdot\Delta t + o\left(\Delta t\right),\ i \neq j\ , \tag{3}$$

$\lambda_{ij}(t)$ – интенсивность перехода, характеризующая число переходов из состояния в новое состояние за определённый период.

Переходные вероятности p_{ij} в любой период времени t соответствуют простым линейным дифференциальным уравнениям [4]. При решении системы уравнений требуется внести начальные условия (начальные вероятности). Они выбираются с учетом специфики топологии систем и производимых атакующих воздействий [5]. Также необходимо ввести начальные условия, то есть вероятности присутствия во временной области реализации техники злоумышленника (в начальный период). При этом общая вероятность равна сумме начальных и условных вероятностей с учетом переходов в заданный момент [4].

Интенсивности переходов при следовании от одной тактики к другим зависят только от разности начального и переходного времени ($\tau = t - t_0$, т. е. $p_{ij}(t_o, t) = p_{ij}(\tau)$), и соответствуют формируемым дифференциальным уравнениям. Тогда задача сводится к решению системы дифференциальных уравнений вида [4]:

$$\frac{d}{dt} p_{ij}\left(\tau\right) = \sum_{g=1}^{G} \lambda_{ij}\left(t\right) p_{ij}\left(t\right). \tag{4}$$

На основании принципов построения марковских цепей формируется система уравнений, которая учитывает специфику зависимостей состояний (тактик), приводимых в Методике и описанных в графе (рис. 1), и интенсивность достижения состояний при осуществлении техник из начального состояния. Решение системы дифференциальных уравнений для разнообразных атакующих воздействий позволяет рассмотреть множество различных моделей атак с учетом того, что источником начальных состояний (начальных атакующий действий) является внешний нарушитель. Внутренний нарушитель становится актуальным при условии того, что часть информации уже ему известна, поэтому он может реализовать атакующие воздействия, используя промежуточные состояния (5).

Однако технология реализации атак не всегда предполагает четкую последовательность техник, приводимых в графе (рис. 1). Некоторые техники позволяют перейти к последующим тактикам без соблюдения обязательной последовательности переходов. Для определения подобных переходов нужно определить сопрягаемые техники различных тактик. В качестве критерия отбора связей для формирования модифицируемого графа используем следующий критерий: возможен ли переход без соблюдения последовательности техник, ближайших к рассматриваемому состоянию, в другие состояния, представленные другими техниками, и, соответственно, их тактиками [5]. Для этого требуется выделить те техники, которые позволяют осуществить подобный переход. Выявление подобных техник производится на основе сопоставления функций, которые в них заявлены. При этом предполагается, что результат одной функции можно использовать для реализации другой, принадлежащей к технике иной тактики, позволяющей получить новое состояние в графе компрометации.

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10} P_{T10}(t) - \lambda_{12} P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12} P_{T2}(t) - \lambda_{23} P_{T2}(t) \\ \frac{dP_{T3}}{dt} = \lambda_{23} P_{T3}(t) - \lambda_{34} P_{T3}(t) \\ \frac{dP_{T4}}{dt} = \lambda_{34} P_{T3}(t) - \lambda_{45} P_{T4}(t) \\ \frac{dP_{T5}}{dt} = \lambda_{45} P_{T4}(t) - \lambda_{56} P_{T5}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{56} P_{T5}(t) - \lambda_{67} P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67} P_{T6}(t) - \lambda_{78} P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78} P_{T7}(t) - \lambda_{69} P_{T8}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89} P_{T8}(t) - \lambda_{9,10} P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{9,10} P_{T9}(t) - \lambda_{10,1} P_{T10}(t) \end{cases}. \quad (5)$$

На основе анализа функциональных взаимосвязей техник выделяются следующие связи тактик [1]:

1. Из состояния T1 техники позволяют перейти в состояние (задействовать) T2. Доступ получен стандартными способами, предусмотренными тактиками Методики.

2. Из состояния T2 техники позволяют перейти в состояние (задействовать) T3. Доступ получен стандартными способами, предусмотренными тактиками Методики.

3. Из состояния T2 техники позволяют перейти в состояния (задействовать) T4 и T5. Используются техники: T2.4, T2.8, T2.9, T2.10, T2.11, T2.13, T2.6, T2.7. Переход в состояние T4 обеспечен различными тактиками, в том числе теми, которые подразумевают использование ошибок конфигурации различного сетевого оборудования, а также средств фильтрации сетевого трафика. Это может быть выражено в компрометации паролей со слабым алфавитом или неизменённых и заданных по умолчанию ключевых данных, то есть логинов и пин-кодов. Кроме того, в состояние T5 можно перейти, используя недокументированные возможности программного обеспечения и оборудования, в том числе используя возможности, которые оставляют сами разработчики с целью последующей отладки или получения нелегитимного доступа для сбора информации о субъектах доступа. Переход в состояние T5 может быть обеспечен различными уязвимостями, связанными с легитимным использованием программного обеспечения. Злоумышленники могут использовать различные способы компрометации: средства перебора пароля, в том числе может производиться поиск устаревших, но всё ещё актуальных ключевых данных, что может приводить к компрометации легитимных данных пользователей компьютерных систем. Также могут быть использованы различные сетевые атаки, связанные с применением классического варианта вредоносного воздействия «человек посередине», в том числе с применением инфраструктур смежных организаций или открытых сетей. Все это позволяет, находясь в состоянии T2, обойти T3 и перейти в следующее состояние T4 или сразу перейти в состояние T5.

4. Из состояния T2 техники позволяют перейти в состояние (задействовать) T6. Для этого используются техники: T2.6, T2.8, T2.10. Они позволяют использовать недокументированные

возможности программного обеспечения и осуществить несанкционированный доступ к программному обеспечению от аккаунтов сотрудников.

5. Из состояния Т3 техники позволяют перейти в состояния (задействовать) Т4, Т6 и Т7. Для перехода в Т6 и Т7 используются техники: Т3.6, Т3.7, Т3.8, Т3.9, Т3.10. Тактики позволяют автоматическое создание вредоносных скриптов и использование таковых, включая подмену легитимных программных файлов, их библиотек, ссылок на легитимные программные библиотеки (допускается использование сетевых ресурсов, веб-ресурсов), а также позволяют использовать недокументированные возможности приложений и подмену дистрибутивов со встроенным вредоносным программным обеспечением (включая маскировку вредоносного программного обеспечения с помощью цифровых подписей).

6. Из состояния Т4 техники позволяют перейти в состояния (задействовать) Т5 и Т6. Для перехода в Т6 используются техники: Т4.1, Т4.2, Т4.3. Эти техники позволяют использовать несанкционированные возможности взломанных учётных записей при применении штатных средств удалённого доступа, также подразумевают скрытую установку средств удалённого доступа и перехвата управления операционной системой с учётом внесения изменений в ее конфигурацию и изменения в составе программно-аппаратных средств вычислительной системы.

7. Из состояния Т5 техники позволяют, кроме перехода в Т6, перейти в состояние (задействовать) Т9. Используются техники Т5.2, Т5.3, Т5.4 для перехода в Т9. Тактики подразумевают внедрение различных средств эксплуатации удалённых сервисов, а также использование протоколов верхнего уровня модели OSI с возможностью подключения к внешним серверам управления, обеспечивают перехват управления операционной системой с помощью данных внешних сервисов и управляемых ими вредоносных объектов, заражающих операционную систему.

8. Из состояния Т6 техники позволяют перейти не только в состояния (задействовать) Т7, но и в Т8, Т9, Т10. Для этого используются техники Т6.1, Т6.2, Т6.3. Эти тактики используют сеть и подразумевают получение доступа к другим компьютерным системам. В частности, тактики подразумевают эксплуатацию уязвимостей программного обеспечения системного и пользовательского типа, подбор паролей к административным учётным записям, а также использование различных привилегированных аккаунтов. Также может использоваться перехват сессионных ключей.

9. Из состояния Т7 техники позволяют перейти в состояние (задействовать) Т8. Доступ получен стандартными способами, предусмотренными тактиками Методики.

10. Из состояния Т8 техники позволяют перейти не только в состояние (задействовать) Т9, но и в Т10. Тактики позволяют выводить данные из компьютерной системы различными способами, в том числе скрытыми, организовать криптографические каналы для выемки данных из атакованных узлов.

11. Из состояния Т9 техники позволяют перейти в состояние (задействовать) Т10. Доступ получен стандартными способами, предусмотренными тактиками Методики.

12. Состояние Т10 подразумевает достижение цели злоумышленником и переход к новой атакующей последовательности, то есть к состоянию Т1. Также повтор атакующей последовательности может произойти в результате полного краха атаки на последнем этапе.

Таким образом, приведенные тактики подразумевают множество вариантов атакующих воздействий и позволяют достичь состояния, которое определяется как тактика № 10, то есть состояния, подразумевающего успешность атаки. При этом не требуется обязательно соблюдать последовательность приводимых в Методике тактик, то есть техники позволяют некоторые этапы обходить. На основании приведённого анализа формируется граф атаки (рис. 2). Часть его вершин будет возможно обойти исходя из специфики техник и тактик, другие же вершины будут совмещать множество входящих дуг (переходов), тем самым аккумулируя вероятности переходов.

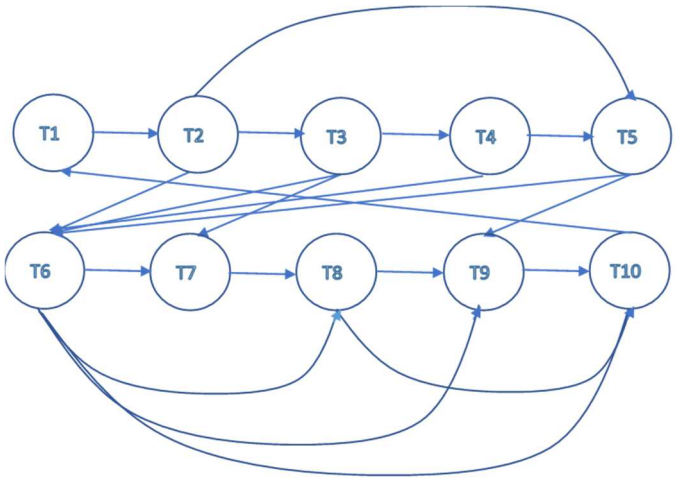

Рис. 2. Модифицированный граф состояний с учетом последовательности реализации

Модифицированный граф состояний с учетом выявленных особенностей в последовательности реализации тактик можно описать системой дифференциальных уравнений, на основании которых осуществляется оценка вероятностей перехода из начальных состояний в новые состояния:

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10}P_{T10}(t) - \lambda_{12}P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12}P_{T2}(t) - \lambda_{23}P_{T2}(t) - \lambda_{26}P_{T2}(t) \\ \frac{dP_{T3}}{dt} = \lambda_{23}P_{T3}(t) - \lambda_{34}P_{T3}(t) - \lambda_{36}P_{T3}(t) - \lambda_{37}P_{T3}(t) \\ \frac{dP_{T4}}{dt} = \lambda_{34}P_{T3}(t) - \lambda_{45}P_{T4}(t) \\ \frac{dP_{T5}}{dt} = \lambda_{25}P_{T2}(t) + \lambda_{45}P_{T4}(t) - \lambda_{56}P_{T5}(t) - \lambda_{59}P_{T5}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{26}P_{T2}(t) + \lambda_{36}P_{T4}(t) + \lambda_{46}P_{T4}(t) + \lambda_{56}P_{T4}(t) - \lambda_{67}P_{T6}(t) \\ -\lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) - \lambda_{6,10}P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67}P_{T6}(t) + \lambda_{37}P_{T3}(t) - \lambda_{78}P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78}P_{T7}(t) + \lambda_{68}P_{T6}(t) - \lambda_{89}P_{T6}(t) - \lambda_{8,10}P_{T6}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89}P_{T8}(t) + \lambda_{69}P_{T6}(t) + \lambda_{79}P_{T7}(t) - \lambda_{9,10}P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{8,10}P_{T8}(t) + \lambda_{9,10}P_{T9}(t) - \lambda_{10,1}P_{T10}(t) \end{cases}. \quad (6)$$

Из приведенной системы видно, что специфика связей предполагает множество различных сопряжений и взаимных влияний параметров вероятностей переходов, что приводит к усложнению вычислений. На основании сопряжения функции возможно упростить граф, используя приведённые вычисления. В графе (рис. 2) можно отметить, что состояния Т6 является результатом переходов из состояний Т2, Т3, Т4, Т5. Таким образом, можно упростить решение

задач вычисления переходных вероятностей, представив часть графа (Т2, Т3, Т4, Т5) в виде свёртки (рис. 3).

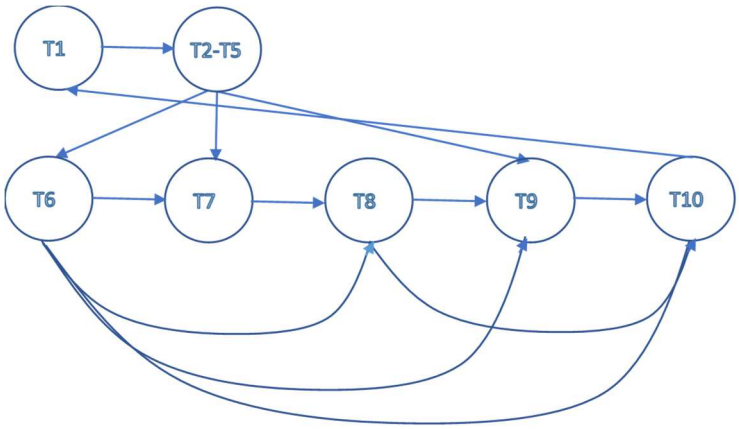

Рис. 3. Сокращенный модифицированный граф состояний с учетом последовательности реализации

Сокращенный модифицированный граф состояний с учетом последовательности реализаций тактик описывается иной системой дифференциальных уравнений:

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10}P_{T10}(t) - \lambda_{12}P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12}P_{T2}(t) - \lambda_{27}P_{T2}(t) - \lambda_{26}P_{T2}(t) - \lambda_{29}P_{T2}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{26}P_{T2}(t) - \lambda_{67}P_{T6}(t) - \lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) - \lambda_{6,10}P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67}P_{T6}(t) + \lambda_{27}P_{T2}(t) - \lambda_{78}P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78}P_{T7}(t) + \lambda_{68}P_{T6}(t) - \lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89}P_{T8}(t) + \lambda_{69}P_{T6}(t) + \lambda_{29}P_{T2}(t) - \lambda_{9,10}P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{8,10}P_{T8}(t) + \lambda_{9,10}P_{T9}(t) - \lambda_{10,1}P_{T10}(t) \end{cases} . \quad (7)$$

Очевидно, что количество вычислений, требуемых для расчёта переходных вероятностей сокращенного графа, стало меньше. Кроме того, с учётом упрощения графа точность рассчитываемых переходных вероятностей может падать, если переходы между состояниями Т2, Т3, Т4, Т5 должны присутствовать обязательно. Это определяется исходя из специфики атаки.

Моделирование атак типа «спуфинг» (при использовании аппарата марковских цепей и тактик Методики ФСТЭК) предполагает рассмотрение упрощенного графа (рис. 3) с изъятием состояния Т9, так как его тактики не используются при достижении Т10. Поэтому систему уравнений вероятности переходов (7) можно еще более упростить.

Определим стационарные характеристики процесса, описывающего действия злоумышленника при реализации атаки. Учитывая статистику отраженных и реализованных атак, а также опыт технической эксплуатации защищенных распределенных систем, в качестве переходных вероятностей были приняты следующие значения [10]:

$$\Pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.3 & 0 & 0 & 0.7 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (8)$$

В качестве распределений времени пребывания в состояниях принято экспоненциальное распределение со следующей матрицей интенсивностей переходов:

$$\Lambda = \begin{pmatrix} 0 & 0.005 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.005 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.008 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.008 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.05 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (9)$$

По итогам расчетов на основе предложенной модели (с учетом числа и специфики тактик сокращённого графа) были получены стационарные вероятности пребывания в каждом из состояний рассматриваемого графа: [0.469; 0.147; 0.023; 0; 0; 0.341; 0; 0.289; 0; 0.041]. В то же время по итогам расчетов при использовании полного графа стационарные вероятности несколько отличаются от предыдущих значений: [0.56; 0.15; 0.016; $4.68 \cdot 10^{-5}$; 0.047; 0.103; $2.31 \cdot 10^{-4}$; 0.045; 0.4; 0.21; 0.055].

Расхождения в значениях вероятностей присутствуют, хотя они минимальны в конечных состояниях, советующих тактике Т10, и в большей степени наблюдаются на промежуточных этапах развития атаки. Это объясняется влиянием исключенных из сокращённого графа и присутствующих в полном графе тактик: их значения обновляются при каждой итерации. Незначительная величина расхождения состояний Т10 обоих графов объясняется минимальным влиянием техник Т3, Т4, Т5, Т9 при реализации технологии атак типа «спуфинг».

4. Заключение

Таким образом, при определении вектора атаки в дополнение к способам, изложенным в методических документах ФСТЭК, можно использовать марковские последовательности. Их применение представлено в виде двух реализаций: полного графа со всеми функциональными взаимосвязями и сокращенного, включающего в свой состав свёртку вероятностей переходов с Т2 по Т5.

При моделировании следуют учитывать требуемую при аудите, анализе угроз и уязвимостей точность. При этом оба подхода могут дать представление об изменении состояния безопасности системы. Граф с полным набором состояний можно применять для расследования инцидентов, проверки гипотез о компрометации ресурсов систем. Граф с сокращенным набором состояний можно применять при отслеживании развертывания атак для быстрого определения конечного направления атакующих действий (конечных целей) злоумышленника.

Литература

1. Методика оценки угроз безопасности информации Методический документ ФСТЭК России: утв. ФСТЭК России 5 февраля 2021 г.
2. ГОСТ Р 56546-2015 Национальный стандарт российской федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2018 г.
3. *Горбачев И. Е., Глухов А. П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры// Труды СПИИРАН. 2015. Вып. 1 (38). С. 112–135.
4. *Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А. М.* Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6. С. 64–71.
5. *Добрышин М. М.* Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. № 12. С. 31–35.
6. *Канаев А. К., Опарин Е. В., Опарина Е. В.* Обобщенная модель действий злоумышленника при манипулировании сообщениями, содержащими сигналы точного времени // T-Comm. 2022. Т. 16, № 6.
7. *Петров М. Ю., Фаткиева Р. Р.* Модель синтеза распределенных атакующих элементов в компьютерной сети // Труды учебных заведений связи. 2020. Т. 6, № 2. С. 113–120. DOI:10.31854/ 1813-324X-2020-6-2-113-120.
8. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004. 384 с.
9. *Галатенко В. А.* Управление рисками: обзор употребительных подходов (часть 2) // Jet Info. 2018. № 12.
10. Canadian Institute for Cybersecurity: NSL-KDD dataset [Электронный ресурс]. URL: `https://www.unb.ca/cic/datasets/nsl.html` (дата обращения: 17.05.2020).

Ветров Игорь Анатольевич

к.т.н., доцент, ОНК «Институт высоких технологий», Балтийский федеральный университет им. И. Канта (236041, Калининград, ул. Александра Невского, 14), e-mail: `vetrov.gosha2009@yandex.ru`, ORCID ID: 0000-0002-3189-9085.

Подтопельный Владислав Владимирович

старший преподаватель, Институт цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» (236022, Калининград, Советский пр., 1), e-mail: `ionpvv@mail.ru`, ORCID ID: 00000-0002-7618-3224.

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.*

Formation of the network attack vector taking into account the connections specifics of techniques and tactics

Igor A. Vetrov[1], Vladislav V. Podtopelny[2],

[1] Immanuel Kant Baltic Federal University (IKBFU)
[2] Kaliningrad State Technical University (KSTU).

Abstract: The problems arising with the tasks of constructing an attack vector in a network infrastructure are considered. The varieties of various tactics and techniques of FSTEC techniques used in the construction of a network attack vector are presented and characterized as well as the specifics of their interrelations with the use of Markov chains in the modeling of attacking influences, their suitability for various procedures for determining vector parameters. When constructing a network attack vector, the features of determining the probabilities of system transitions to various states of network compromise are considered. The formation of the attack vector is studied taking into account the specifics of the multilevel organization of the corporate information system. The features of the construction of a simplified vector are determined taking into account the specifics of tactical relationships (states).

Keywords: attack vector, information system, corporate network, vulnerability, Markov processes, intruder, tactics.

For citation: Vetrov I. A., Podtopelny V. V. Formation of the network attack vector taking into account the connections specifics of techniques and tactics (in Russian). *Vestnik SibGUTI*, 2023. vol. 17, no. 4. pp. 49-61. https://doi.org/10.55648/1998-6920-2023-17-4-49-61.

The article was submitted: 25.05.2023;
accepted for publication 07.06.2023.

References

1. *Metodika otsenki ugroz bezopasnosti informatsii Metodicheskii dokument FSTEK Rossii: utv. FSTEK Rossii 5 fevralya 2021.* [Methodology for assessing threats to information security Methodological document of the FSTEC of Russia]. Moscow, 2021.
2. *GOST R 56546-2015 Natsional'nyi standart rossiiskoi federatsii. Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostei informatsionnykh system* [National Standard of the Russian Federation. Data protection. Vulnerabilities of information systems. Classification of vulnerabilities of information systems]. Moscow, Standartinform, 2018.
3. Gorbachev I. E., Glukhov A. P. Modelirovanie protsessov narusheniya informatsionnoi bezopasnosti kriticheskoi infrastruktury [Modeling the processes of violation of information security of critical infrastructure]. *Trudy SPIIRAN*, Moscow, 2015, iss. 1(38), pp. 112 – 135.
4. Kotenko I. V., Saenko I. B., Lauta O. S., Kribel' A. M. Metod rannego obnaruzheniya kiberatak na osnove integracii fraktal'nogo analiza i statisticheskih metodov [Method for early detection of cyber-attacks based on the integration of fractal analysis and statistical methods]. *Pervaya milya*, 2021, no. 6, pp. 64-71.
5. Dobryshin M. M. Model' raznorodnyh komp'yuternyh atak, provodimyh odnovremenno na uzel komp'yuternoj seti svyazi [Model of heterogeneous computer attacks carried out simultaneously on a computer communication network node]. *Telekommunikacii*, 2019, no. 12, pp. 31-35.

6. Kanaev A. K., Oparin E. V., Oparina E. V. Obobshchennaya model' dejstvij zloumyshlennika pri manipulirovanii soobshcheniyami, soderzhashchimi signaly tochnogo vremeni [A generalized model of an attacker's actions when manipulating messages containing precise time signals]. *T-Comm*, vol.16, no. 6, 2022.
7. Petrov M. YU., Fatkieva R. R. Model' sinteza raspredelennyh atakuyushchih elementov v komp'yuternoj seti [Model for the synthesis of distributed attack elements in a computer network]. *Trudy uchebnyh zavedenij svyazi*. 2020, vol. 6, no. 2, pp. 113-120. DOI:10.31854/ 1813-324X-2020-6-2-113-120.
8. Shcheglov A. YU. *Zashchita komp'yuternoj informacii ot nesankcionirovannogo dostupa* [Protecting computer information from unauthorized access]. Saint Petersburg, Nauka i Tekhnika, 2004. 384 p.
9. Galatenko V. A. Upravlenie riskami: obzor upotrebitel'nykh podkhodov (chast' 2) [Risk management: a review of common approaches (part 2)]. *Jet Info*, no. 12, 2018, available at: https://www.jetinfo.ru/upravlenie-riskami-obzor-upotrebitelnykh-podkhodovchast-2/ (accessed: 29.01.2022).
10. Canadian Institute for Cybersecurity: NSL-KDD dataset, 2009. available at: https://www.unb.ca/cic/datasets/nsl.html (accessed: 17.05.2020).

Vetrov Igor A.

Cand. of Sci. (Engineering), Associate Professor, Institute of High Technologies, I. Kant Baltic Federal University (236041, Kaliningrad, Alexander Nevsky Str., 14), e-mail: vetrov.gosha2009@yandex.ru, ORCID ID: 0000-0002-3189-9085.

Podtopelny Vladislav V.

Senior lecturer, Institute of Digital Technologies of KSTU (236022, Kaliningrad, Sovetsky ave., 1), e-mail: ionpvv@mail.ru, ORCID ID: 00000-0002-7618-3224.

DOI: 10.55648/1998-6920-2023-17-4-62-73 УДК 123.456.789

Организация защищенного обмена данными внутри программно-управляемой локальной сети *

Е. А. Кушко, Н. Ю. Паротькин, В. В. Золотарев

Сибирский университет науки и технологий (Красноярск)

Аннотация: **Введение.** Для обеспечения защищенного обмена данными внутри локальной вычислительной сети информационной системы недостаточно защиты лишь внешнего периметра. Данный факт подтверждается аналитическими отчетами ведущих компаний в области информационной безопасности. Как правило, после преодоления внешнего сетевого периметра перед проведением атаки злоумышленник выполняет действия по сетевой разведке. Успех выполнения сетевой атаки зависит от полноты собранной информации. Постоянные изменения топологии сети не позволяют злоумышленнику обладать долгосрочной информацией о ней, в результате чего он вынужден более интенсивно собирать информацию, тем самым выдав себя. В противном случае эффективность планируемой атаки снижается. Целью данного исследования является повышение защищенности сторон внутрисетевого обмена методом динамической реконфигурации топологии сети. Авторами предложено новое решение для обеспечения безопасного взаимодействия узлов в сети от внутреннего и преодолевшего защиту сетевого периметра внешнего злоумышленника.

Материалы и методы. Предлагаемое решение построено на базе программно-управляемой сети и технологии VxLAN. Решение предполагает постоянную реконфигурацию сети как с определенной периодичностью, так и по наступлении определенных событий, чтобы злоумышленник не мог обладать долгосрочной информацией о ней. В случае, если злоумышленник был обнаружен или возник инцидент информационной безопасности, сеть в автоматическом режиме реконфигурируется так, чтобы минимизировать или исключить возможные последствия.

Результаты. Полученные результаты экспериментов по применению предлагаемого решения показывают, что периодические изменения топологии сети не позволяют злоумышленнику собрать полную информацию о сети в скрытом режиме. В результате работы предлагаемого решения он может быть обнаружен, а также изолирован.

Обсуждение и заключение. Предлагаемое решение показало потенциальную применимость для организации защищенного обмена данными внутри локальной вычислительной сети информационной системы.

Ключевые слова: программно-управляемая сеть, технология защиты движущейся цели, безопасность обмена данными, защита от исследования, защищенная передача данных.

Для цитирования: Кушко Е. А., Паротькин Н. Ю., Золотарев В. В. Организация защищенного обмена внутри программно-управляемой локальной сети // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 62–73. https://doi.org/10.55648/1998-6920-2023-17-4-62-73.

Статья поступила в редакцию 05.04.2023;
принята к публикации 07.06.2023.

* Данное исследование выполнено при финансовой поддержке Минцифры РФ (Грант ИБ). Проект №40469-07/2021-К.

1. Введение

Несмотря на наличие защиты внешнего сетевого периметра информационной системы, злоумышленники находят недостатки и уязвимости в ней – компания Positive Technologies в своей аналитике [1] приводит следующую статистику:

- в рамках внешнего тестирования на проникновение различных компаний в 92 % случаев был получен доступ к их локальной вычислительной сети;
- в 100 % случаев злоумышленник может подключиться к корпоративным беспроводным сетям;
- в 63 % систем через беспроводные сети получен доступ к ресурсам локальных вычислительных сетей.

Для решения этой проблемы исследовательские группы разрабатывают системы автоматизации сбора, мониторинга и анализа событий информационной безопасности с целью выявления инцидентов информационной безопасности и последующего реагирования на них. Но существует также и другой подход, появившийся относительно недавно, а именно технология Moving-Target Defense (MTD, технология защиты от движущейся цели) [2].

Как правило, после проникновения в локальную сеть информационной системы злоумышленник выполняет следующие действия [3]:

1) закрепление в системе;
2) сбор информации;
3) изучение окружения;
4) построение топологии сети;
5) сканирование портов;
6) идентификация узлов, сервисов и операционных систем;
7) определение ролей узлов;
8) поиск уязвимостей;
9) определение вектора атаки и её реализация.

Это также подтверждается статистикой инцидентов информационной безопасности:

1) компания Positive Technologies отмечает, что в 33 % компаний наблюдалось сканирование внутренней сети, а в 19 % – сбор информации [1];

2) компания Ростелеком Солар также в своем отчете указывает на то, что после проникновения в сеть злоумышленник выполняет её сканирование [4];

3) компания Kaspersky ICS CERT установила, что APT-группировки используют инструменты для сканирования и кражи данных [5].

Для обеспечения безопасности сети технология защиты движущейся цели предполагает периодические изменения информации о конечной точке (IP, MAC, используемые порты) и маршрутах передачи данных. Технология защиты движущейся цели обычно не предполагает активного противодействия злоумышленнику, но при этом не позволяет ему обладать актуальной информацией о сети, на основе которой он принимает решения при реализации своей атаки. В результате, не осуществив этап сетевой разведки и, следовательно, не получив нужную информацию, злоумышленник не может эффективно осуществить атаку [6].

2. Сравнение с существующими решениями и методами защиты

Традиционно для защиты передаваемых данных от перехвата используют построение эшелонированной системы защиты, а для защиты от анализа – шифрование. В случае, если злоумышленник преодолел один или несколько эшелонов защиты, он очень часто ничем не ограничен, что косвенно подтверждает приведенная ранее статистика (данные собраны в организациях, которые имели систему защиты информации). Шифрование защищает данные от анализа, однако перехват даже зашифрованных пакетов позволяет получить злоумышленнику некоторые полезные данные [7].

В настоящий момент решения технологии защиты движущейся цели для локальных вычислительных сетей имеют ряд существенных недостатков:

1) неконтролируемый рост энтропии, ухудшающий производительность системы [8];

2) разрывы связи между легитимными пользователями и объектами защиты [9];

3) невозможность использовать в устаревшей сетевой инфраструктуре [10];

4) недостаточный уровень исследования применения технологии для реальных сетей и высокое разнообразие тестовых сред, которое затрудняет сравнение различных методов и стратегий друг с другом [11].

Большинство недостатков текущих реализаций связано с попыткой исследователей и разработчиков защитить всю сеть при помощи технологии движущейся цели. В своем решении авторы предполагают защитить не всю сеть, а лишь её часть, предназначенную для обмена критичными данными.

К аналогичным предлагаемому авторами решению с точки зрения активного противодействия злоумышленнику относятся решения из класса систем Security Orchestration, Automation and Response (SOAR, платформы оркестрации, автоматизации и реагирования на инциденты безопасности). Решения данного класса предполагают реконфигурирование сети и информационной системы таким образом, чтобы злоумышленник в случае его обнаружения был немедленно изолирован. В результате работы решений данного класса часто возникают ошибки первого рода [12], из-за которых доступ к легитимным сервисам в сети может быть нарушен. Соответственно, в результате применения предлагаемого авторами решения на базе коммуникационного оборудования будет создано дополнительное буферное время. Это позволит снизить вероятность ошибки первого рода за счет дополнительного времени для сигнализации и анализа информации, поступающей от средств защиты, а сам злоумышленник будет переведен на этап изучения окружения.

В настоящее время широко применяемыми решениями проблемы защиты от исследования являются следующие технологии: deep packet inspection (DPI), брокер сетевых пакетов, virtual private network (VPN), software-defined network (SDN), стегоканал.

Технология DPI предназначена для анализа трафика в режиме реального времени, включая уровень приложений модели OSI. Сетевой трафик, в зависимости от заданных правил, может быть заблокирован, перенаправлен, модифицирован, ограничен по скорости и т.д. Решения из класса DPI также позволяют обнаружить вредоносный трафик. Производительность напрямую зависит от аппаратной платформы, причем данная технология предполагает кластеризацию. Решения DPI имеют распределенную структуру: сервер и сенсоры. В случае, если устройство DPI подключается «в разрыв», могут возникнуть проблемы с передачей данных. Также устройство DPI может быть интегрировано с другими средствами защиты информации [13].

Брокеры сетевых пакетов, в отличие от средств DPI, прежде всего направлены на распределение и балансировку сетевого трафика с учетом требований целостности сессий. Фильтрация трафика осуществляется до транспортного уровня включительно. Основная цель фильтрации – повышение надежности сеть и эффективности анализа сетевого трафика: балансировка нагрузки, детуннелирование, из заголовков пакетов удаляются избыточные данные, удаление повторяющихся пакетов, дешифрация пакетов, сбор статистики проходящего трафика и т.д. Кроме того, брокеры сетевых пакетов предлагают функционал по маскированию сетевых пакетов с целью анонимизации трафика. Производительность также зависит от аппаратной платформы. Брокеры сетевых пакетов могут быть интегрированы с другими средствами защиты информации [14].

VPN переводится как виртуальная частная сеть. VPN – это оверлейная сеть, которая предназначена для защищенной передачи данных через публичные сети. Пользователь подключается к шлюзу, через который осуществляется подключение к внутренней сети. Данные шифруются только при передаче по небезопасному каналу. Требования к вычислительным ресурсам зависят от количества клиентов. Некоторые VPN-протоколы поддерживают сокрытие метаданных соединения [15].

SDN – это сеть передачи данных, управление которой осуществляется программно, в том числе и в режиме реального времени. SDN предназначена для централизованного управления всей сетью, чтобы оперативно конфигурировать сеть и реагировать на изменения в сети, оптимизировать передачу трафика, упрощать процесс конфигурирования, централизованно применять политики и т.д. Управляющие пакеты данных могут быть зашифрованы. Управление осуществляется централизованно. Специальных требований к вычислительным ресурсам у данной технологии нет [16].

Еще одним решением, которое может быть применено для защиты от исследования, является стегоканал. Стегоканал – это канал передачи сообщений, в котором данные кодируются методами стеганографии. В случае передачи данных по сети, как правило, данные скрываются в заголовках и полях полезной нагрузки сетевых пакетов, также применяется модификация последовательности передачи данных. Дополнительно применяется шифрование для защиты передаваемых данных. Однако объем данных, который можно передать средствами сетевой стеганографии, существенно ограничен [17].

Для сравнения предлагаемого решения (табл. 1) с ранее упомянутыми технологиями выбраны следующие критерии:

1) возможная пропускная способность канала;
2) наличие возможности изменения правил управления каналом в режиме реального времени;
3) требуемая вычислительная мощность решения;
4) наличие шифрования;
5) наличие сокрытия метаданных соединения;
6) система управления каналом – децентрализованная, частично централизованная, централизованная;
7) наличие возможности работы в качестве источника событий для SIEM;
8) негативное влияние на стабильность работы всей сети и конечных узлов;
9) сложность технологии.

Таблица 1. Сравнение с существующими решениями

Крит.	DPI	Брокер сетевых пакетов	VPN	SDN	Стегоканал	Предлагаемое решение
1	Высокая	Высокая	Высокая	Высокая	Низкая	Высокая
2	Да	Да	Нет	Да	Нет	Да
3	Высокая	Высокая	Средняя	Низкая	Низкая	Низкая
4	Нет	Нет	Да	Нет	Да	Да
5	Нет	Да	Да	Нет	Да	Да
6	Центр.	Центр.	Центр.	Центр.	Децентр.	Центр.
7	Да	Да	Да	Нет	Нет	Да
8	Да	Нет	Нет	Да	Нет	Да
9	Высокая	Высокая	Высокая	Средняя	Средняя	Средняя

3. Описание предлагаемого решения

Предлагаемое авторами решение сочетает в себе два подхода:

1) постоянные изменения структуры сети, в результате чего актуальность собранных злоумышленником данных имеет малое время жизни;

2) в случае обнаружения злоумышленника сеть реконфигурируется таким образом, что злоумышленник будет изолирован от остальной сети.

В основе решения лежат принципы сети SDN, в которой узлы имеют доступ к ней и её ресурсам строго в соответствии с определенными политиками, которые задаются админи-

стратором программными средствами централизованно и применяются на каждом устройстве сети от единой точки управления [18].

Решение построено на базе технологии Virtual Extensible Local Area Network (VxLAN, виртуальная расширенная частная сеть). Каждый узел подключен как минимум к двум виртуальным сетям, одна из которых является базовой для всех узлов, обеспечивающих выполнение базового сетевого взаимодействия и обмена открытой информацией, а другие сети – для организации защищенного обмена данными. Выбор технологии VxLAN обусловлен его преимуществами относительно других аналогичных технологий: масштабируемость, гибкость, эффективность, простота конфигурации и управления [19].

Технология VxLAN, как правило, применяется для разделения потоков передачи данных в рамках одной физической среды, например, для центров обработки данных [20], IoT-решений (Internet of Things, интернет вещей) [21], систем мобильной связи [22]. Исследования безопасности VxLAN показывают, что данная технология действительно обеспечивает изоляцию оверлейных сетей, имеет устойчивость к распространенным атакам, и её недостатки могут быть исправлены правильным конфигурированием сетевого оборудования, а также использованием средств обнаружения вторжений [23].

Решение предполагает постоянное реконфигурирование сети, т.е. перемещение узлов по виртуальным сетям по наступлении некоторых событий:

1) по истечении некоторого временного интервала, чтобы злоумышленник не мог обладать актуальной информацией о всей сети;

2) в результате обнаружения злоумышленника для его изоляции;

3) в результате возникновения некоторого инцидента для предотвращения или минимизации его последствий.

4. Описание экспериментов

Для практического исследования данного решения была собрана одноранговая сеть в среде виртуальной лаборатории EVE-NG (рис. 1). Узел, который обозначен на рисунке как «Nmap», осуществляет сканирование сети соответствующей утилитой. Узел, обозначенный как «Snort», является контроллером сети, на котором развернуто соответствующее средство обнаружения вторжений. Остальные узлы образуют инфраструктуру сети. Все узлы подключены к виртуальному коммутатору под управлением операционной системы Cisco NX-OS.

Конфигурирование осуществляется следующим образом. Каждый узел подключен к двум виртуальным сетям: одна сеть предназначена для взаимодействия с контроллером сети, а другая – для организации защищенного обмена данными. Контроллер сети сообщает узлам по запросу VLAN ID и параметры виртуальной сети, к которой необходимо подключиться на следующей итерации реконфигурирования. Данный идентификатор сопоставляется сетевым оборудованием с VxLAN Network Identifier (VNI, сетевой идентификатор VxLAN) виртуальной сети и гарантирует соответствие инфраструктуры конфигурации контроллера.

При наступлении следующей итерации реконфигурирования сети контроллер настраивает сетевое оборудование таким образом, чтобы каждый узел был подключен к той виртуальной сети и имел доступ к тем сетевым ресурсам, которые определены политикой контроллера. В случае, если был обнаружен узел сети, скомпрометированный злоумышленником, контроллер конфигурирует сеть так, чтобы этот узел был изолирован от остальной инфраструктуры. Правила обнаружения заданы таким образом, чтобы обнаруживать сканирование Nmap [24], что моделирует худший вариант реализации системы защиты для злоумышленника.

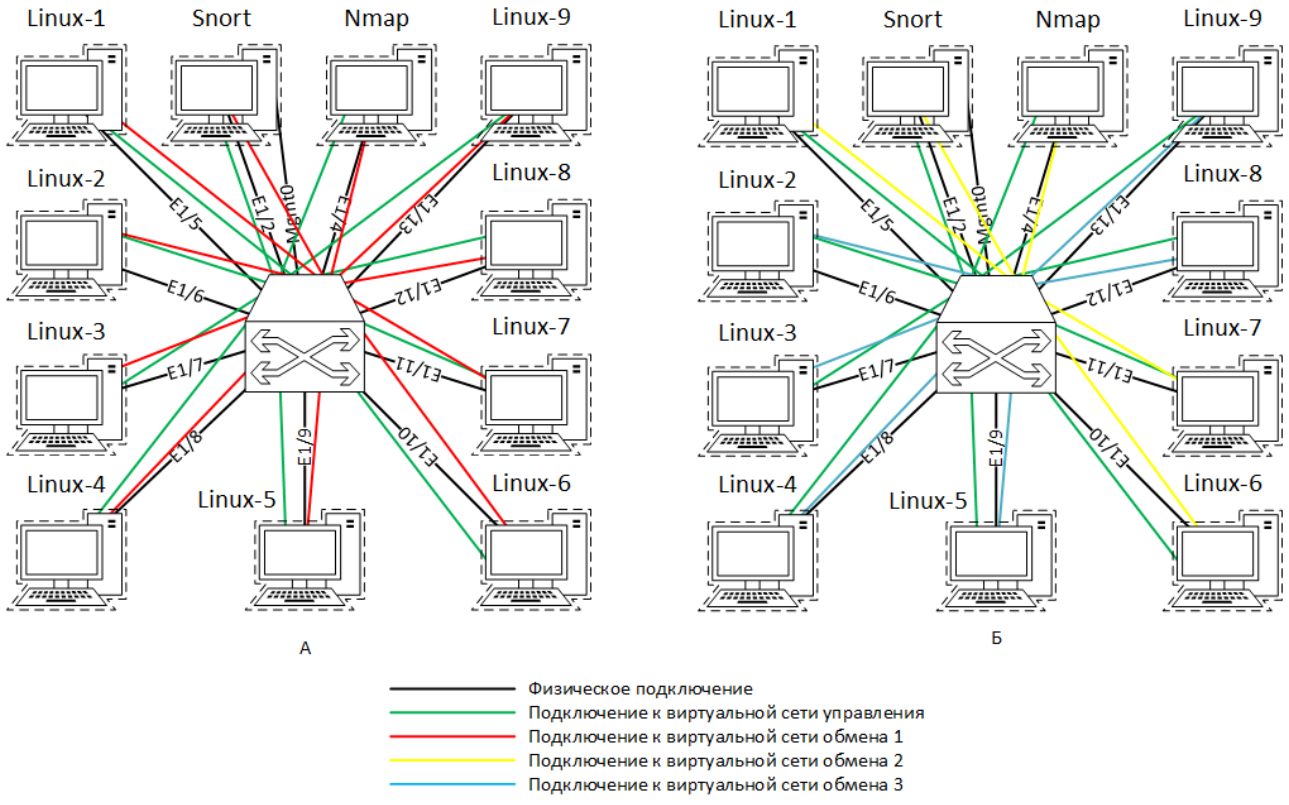

Рис. 1. Конфигурация сети: А – до реконфигурации, Б – после реконфигурации по таймеру

Взаимодействие узлов построено на основе протокола JSON-RPC 2.0 [25] over HTTP(s) для конфигурирования контроллером сетевого оборудования (NX-API) и JSON-RPC 2.0 over WebSocket для взаимодействия узлов (клиентов) с контроллером (сервером).

5. Результаты

Эксперимент построен на двух типах сканирования (табл. 2): безумный (5 – insane) и хитрый (1 – sneaky), а также проведен для трех типов триггеров реконфигурирования [26]:

1) без реагирования;

2) истечение временного интервала;

3) возникновение инцидента информационной безопасности, в данном случае – обнаружение сканирования.

Эксперимент необходим для получения количественной оценки результата анализа защищаемой сети злоумышленником.

Таблица 2. Результаты эксперимента

Тип сканирования	Без реагирования	Истечение временного интервала 60 с	Обнаружение сканирования
Безумный (Insane)	Сканирование завершено за 305.16 с	Прервано на 11.04 % (сканирование портов)	Прервано на 0.76 % (сканирование портов)
Хитрый (Sneaky)	Сканирование завершено за 1478.77 с	Прервано на 20.20 % (обнаружение хостов)	Прервано на 0.76 % (сканирование портов)

Также была осуществлена оценка потерь при переконфигурации сети. Первый эксперимент был проведен при помощи утилиты ping. Опрос осуществлялся в течение одной минуты

с интервалом в 1 секунду, размер пакета – 64 байта. Через 10 секунд после начала эксперимента инициировалась реконфигурация сети. В первом эксперименте происходит потеря не более чем 18 пакетов icmp (в худшем случае) и 10 пакетов icmp (в среднем) при взаимодействии через защищенную сеть между любыми двумя узлами. Второй эксперимент был проведен при помощи утилиты iperf. На скорости 1 Мбит/с в течение одной минуты генерировался синтетический udp-трафик, а через 10 секунд после начала эксперимента инициировалась реконфигурация сети. Были использованы различные размеры пакетов: 64, 128, 256, 512, 1024, 1280 и 1518 байт. Во втором эксперименте, вне зависимости от размера пакета, наблюдалась потеря 50 % пакетов (в среднем) и 51 % (в худшем случае). Стоит отметить, что без переконфигурации сети потерь нет. Для каждого эксперимента проведено не менее чем 10 испытаний. Использовалась виртуальная сеть EVE-NG с максимальной пропускной способностью 1 Гбит/с. Другой трафик в сети отсутствовал.

На основе результатов эксперимента можно сделать вывод о том, что реконфигурации необходимо осуществлять по оповещениям от средств защиты информации, и в случае, если есть подозрение на то, что злоумышленник все-таки преодолел внешний сетевой периметр, а также скомпрометировал некоторый узел и успешно избежал свое обнаружение, необходимо реконфигурировать сеть через интервалы времени, при которых злоумышленник не сможет обладать долгосрочной информацией, не выдав себя, осуществляя более интенсивный сбор данных.

6. Заключение

Из статистики инцидентов информационной безопасности очевидно, что защиты внешнего сетевого периметра недостаточно. После проникновения в сеть злоумышленник обычно осуществляет сетевую разведку – это, как правило, один из ключевых этапов реализации сетевой атаки. В качестве меры защиты, как правило, используют сбор, анализ и мониторинг событий информационной безопасности для выявления инцидентов и реагирования на них.

Также данную проблему можно решить при помощи другого подхода – технологии защиты движущейся цели, которая заключается в постоянных изменениях в сети, при котором злоумышленник не может обладать долгосрочной информацией о ней и в результате не сможет эффективно осуществить свою атаку. Такое решение авторами было представлено при изменении информационной топологии сети с использованием multicast-групп в беспроводной среде с высоким риском перехвата пакетов, но обладающее ограниченной областью применения для работы в сенсорных сетях [27].

В данной работе авторами предложено решение, которое объединяет оба подхода: с одной стороны, сеть реконфигурируется по истечении временного интервала, а с другой – по оповещениям средств защиты информации. В случае обнаружения злоумышленника сеть реконфигурируется таким образом, что злоумышленник изолируется от остальной сети. Данное решение построено на принципах SDN и технологии VxLAN с сохранением функциональных характеристик сети.

Предлагаемое решение может являться частью SOAR-системы, то есть средством автоматической реакции на действия злоумышленника, приводящим систему в базовое состояние, в котором злоумышленнику требуется начинать реализацию атаки сначала.

Литература

1. Positive Research 2020 [Электронный ресурс]. URL: `https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf` (дата обращения: 04.04.2023).

2. *Lei C., Zhang, H., Tan J., Zhang, Y., and Liu X.* Moving target defense techniques: A survey // Security and Communication Networks. 2018. V. 2018.
3. *Galtsev A. A., Sukhov A. M.* Network attack detection at flow level // Smart Spaces and Next Generation Wired/Wireless Networking. Springer, Berlin, Heidelberg, 2011. P. 326 –334.
4. Solar JSOC Security Report 2020 [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf (дата обращения: 04.04.2023).
5. APT-атаки на промышленные компании в 2020 году [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-companies-in-2020-Ru.pdf (дата обращения: 04.04.2023).
6. *Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., and Kambhampati S.* A survey of moving target defenses for network security // IEEE Communications Surveys and Tutorials. 2020. V. 22, № 3. P. 1909–1941.
7. *Velan P., Čermák M., Čeleda P., and Drašar M.* A survey of methods for encrypted traffic classification and analysis // International Journal of Network Management. 2015. V. 25, № 5. P. 355–374.
8. *DeLoach S., Ou X., Zhuang R, and Zhang S.* Model-driven, moving-target defense for enterprise network security // Models@ run. time. 2014. P. 137–161.
9. *Cho J., Sharma D., Alavizadeh H., Yoon S., Ben-Asher N., Moore T., Kim D., Lim H., and Nelson F.* Toward proactive, adaptive defense: A survey on moving target defense // IEEE Communications Surveys and Tutorials. 2020. V. 22, № 1. P. 709–745.
10. *Xu X., Hu H., Liu Y., Zhang H., and Chang D.* An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector // Security and Communication Networks. 2021. V. 2021.
11. *Jalowski Ł., Zmuda M., Rawski M.* A Survey on Moving Target Defense for Networks: A Practical View // Electronics. 2022. V. 11, № 18.
12. *Mir A., Ramachandran R.* Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems // Proc. 6th International Conference on Intelligent Computing and Applications. Singapore, 2021. V. 3. P. 157–169.
13. *Кошепаров Д. Я.* Программная реализация систем глубокой проверки пакетов // Вестник науки и образования. 2020. № 12-1 (90). С. 21–25.
14. Современные решения для построения систем информационной безопасности – брокеры сетевых пакетов (Network Packet Broker) [Электронный ресурс]. URL: https://habr.com/ru/company/dsol/blog/490252/ (дата обращения: 04.04.2023).
15. *Ezra P., Misra S., Agrawal A., Oluranti J., Maskeliunas R., and Damasevicius R.* Secured communication using virtual private network (VPN) // Proc. International Conference on Cyber Security and Digital Forensics (ICCSDF), 2021. P. 309-319.
16. *Goransson P., Black C., Culver T.* Software defined networks: a comprehensive approach. Morgan Kaufmann, 2016.
17. *Пескова О. Ю., Халабурда Г. Ю.* Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет // Материалы Всероссийской объединенной конференции «Интернет и современное общество». Санкт- Петербург, 10 – 12 октября, 2012. С. 348–354.
18. *Shin S., Xu L., Hong S., and Gu G.* Enhancing network security through software defined networking (SDN) // Proc. 25th International conference on computer communication and networks (ICCCN), Waikoloa, HI, USA, 2016. P. 1–9.
19. *Shahrokhkhani V.* An Analysis on Network Virtualization Protocols and Technologies [Электронный ресурс]. URL: https://era.library.ualberta.ca/items/2c481b73-7ebf-4a51-b6e9-ff5b1224fada/view/f0cd1ea5-7314-4e12-a85a-99e76022195a/Shahrokhkhani.pdf (дата обращения: 04.04.2023).

20. *Pu H., Wang Y., An X.* Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology // Journal of Computer and Communications. 2020. V. 8, № 8. P. 45–58.
21. *Shif L., Wang F., Lung C.* Improvement of security and scalability for IoT network using SD-VPN // Proc. IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 2018. P. 1–5.
22. *Gu R., Zhang X., Yu L., and Zhang J.* Enhancing Security and Scalability in Software Defined LTE Core Networks // Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, USA, 2018. P. 837–842.
23. *Reyes G., Dammers M., Kastanja M.* Security assessment on a VXLAN-based network // Haettu. 2014. V. 10, № 2017. P. 2013–2014.
24. *Liao S., Zhou C., Zhao Y., Zhang Z., Zhang C., Gao Y., and Zhong G.* A Comprehensive detection approach of Nmap: principles, rules and experiments // Proc. International conference on cyber-enabled distributed computing and knowledge discovery (CyberC), Chongqing, China, 2020. P. 64–71.
25. JSON-RPC Working Group. JSON-RPC 2.0 Specification [Электронный ресурс]. URL: `https://www.jsonrpc.org/specification` (дата обращения: 04.04.2023).
26. *Jetty S.* Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7. Packt Publishing Ltd, 2018.
27. *Кушко Е. А.* Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. 2020. № 4 (52). С. 39–52.

Кушко Евгений Александрович
старший преподаватель кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва, e-mail: `evgeny.kushko@gmail.com`, ORCID ID: 0000-0003-1290-7075.

Паротькин Николай Юрьевич
к.т.н., доцент кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва, e-mail: `ny-parotkin@yandex.ru`, ORCID ID: 0000-0002-3486-0602.

Золотарев Вячеслав Владимирович
к.т.н., заведующий кафедрой безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва (СибГУ, 660037, Красноярск, пр. имени газеты «Красноярский рабочий», д. 31), тел. +7 391 222 7639, e-mail: `amida.2@yandex.ru`, ORCID ID: 0000-0002-8054-8564.

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.*

Ensuring Secure Data Exchange in Software-defined Local Network

Evgenii A. Kushko, Nikolai Yu. Parotkin, Vyacheslav V. Zolotarev

Reshetnev Siberian State University of Science and Technology

Abstract: **Introduction.** Protecting outer perimeter is not enough to ensure secure data communication in the information system of local area network. Analytical reports of leading information security companies confirm this fact. Usually, an attacker having overcome the outer perimeter conducts network reconnaissance before carrying out an attack. The success of a network attack depends on the completeness of the information collected. The constantly changing network topology does not provide an attacker with long-term network topology information, as a result, the attacker is forced to collect information more intensively thereby identifying himself. Otherwise, the effectiveness of the planned attack is reduced. The aim of this research is to increase the intra-network data transfer security level by means of network topology dynamic reconfiguration. The authors proposed a new solution for ensuring secure node interaction countering both internal and external attackers having overcome an outer perimeter.
Materials and methods. The proposed solution is based on a software-defined network and VxLAN technology. The solution involves constant network reconfiguration both with a certain frequency and on the occurrence of certain events, so that an attacker could not have long-term information. If an intruder is detected or an information security incident occurs, the network is automatically reconfigured in such a way as to lessen or prevent possible consequences.
Results. The obtained results show that periodic network changes do not allow an attacker to covertly collect complete information about the network, and the proposed solution may allow to detect and isolate the attacker.
Discussion and conclusion. The obtained results show that it is possible to apply the proposed solution for organizing secure data communication within the local computer network of the information system.

Keywords: software-defined network, moving target defense, data exchange security, network scanning protection, secure data communication.

For citation: Kushko E. A., Parotkin N. Yu., Zolotarev V. V. Ensuring secure data exchange in software-defined local network (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 1, pp. 62-73. https://doi.org/10.55648/1998-6920-2023-17-4-62-73.

The article was submitted: 05.04.2023;
accepted for publication 07.06.2023.

References

1. Positive Research 2020, available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (accessed: 04.04.2023).
2. Lei C., Zhang, H., Tan J., Zhang, Y., Liu X. Moving target defense techniques: A survey, *Security and Communication Networks*. 2018, vol. 2018.
3. Galtsev A. A., Sukhov A. M. Network attack detection at flow level. *Smart Spaces and Next Generation Wired/Wireless Networking*, Springer, Berlin, Heidelberg, 2011, pp. 326 - 334.
4. Rostelecom Solar. Solar JSOC Security Report 2020, available at: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf (accessed: 04.04.2023).
5. Kaspersky ICS CERT. APT-ataki na promyshlennye kompanii v 2020 godu [APT attacks on industrial companies in 2020], available at: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-companies-in-2020-Ru.pdf (accessed: 04.04.2023).
6. Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., and Kambhampati S. A survey of moving target defenses for network security. *IEEE Communications Surveys and Tutorials,* 2020, vol. 22, no. 3, pp. 1909-1941.
7. Velan P., Čermák M., Čeleda P., and Drašar M. A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management*, 2015, vol. 25, no. 5, pp. 355-374.
8. DeLoach S., Ou X., Zhuang R, and Zhang S. Model-driven, moving-target defense for enterprise network security. *Models@ run. Time*, 2014, pp. 137-161.

9. Cho J., Sharma D., Alavizadeh H., Yoon S., Ben-Asher N., Moore T., Kim D., Lim H., and Nelson F. Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys and Tutorials*, 2020, vol. 22, no. 1, pp. 709-745.
10. Xu X., Hu H., Liu Y., Zhang H., and Chang D. An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector. *Security and Communication Networks*, 2021, vol. 2021.
11. Jalowski Ł., Zmuda M., Rawski M. A Survey on Moving Target Defense for Networks: A Practical View. *Electronics*, 2022, vol. 11, no. 18.
12. Mir A., Ramachandran R. Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems. *6th International Conference on Intelligent Computing and Applications*, Singapore, 2021, vol. 3, pp. 157-169.
13. Kosheparov D. Ya. Programmnaya realizaciya sistem glubokoj proverki paketov [Software implementation of deep packet inspection systems]. *Vestnik nauki i obrazovaniya*, 2020, no. 12-1(90), pp. 21-25.
14. Sovremennye resheniya dlya postroeniya sistem informacionnoj bezopasnosti – brokery setevyh paketov (Network Packet Broker) [Modern solutions for building information security systems - network packet brokers], available at: `https://habr.com/ru/company/dsol/blog/490252/` (accessed: 04.04.2023).
15. Ezra P., Misra S., Agrawal A., Oluranti J., Maskeliunas R., and Damasevicius R. Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 2022, pp. 309-319.
16. Goransson P., Black C., Culver T. *Software defined networks: a comprehensive approach*. Morgan Kaufmann. 2016.
17. Peskova O. Yu., Halaburda G. Yu. *Primenenie setevoj steganografii dlya zashchity dannyh, peredavaemyh po otkrytym kanalam Internet* [Application of network steganography for protection of the data transferred over the internet]. *Materialy Vserossijskoj ob"edinennoj konferencii «Internet i sovremennoe obshchestvo»*, 2012, pp. 348-354.
18. Shin S., Xu L., Hong S., and Gu G. Enhancing network security through software defined networking (SDN). *2016 25th international conference on computer communication and networks (ICCCN)*, Waikoloa, HI, USA, 2016, pp. 1-9.
19. Shahrokhkhani V. An Analysis on Network Virtualization Protocols and Technologies, available at: `https://era.library.ualberta.ca/items/2c481b73-7ebf-4a51-b6e9-ff5b1224fada/view/f0cd1ea5-7314-4e12-a85a-99e76022195a/Shahrokhkhani.pdf` (accessed: 04.04.2023).
20. Pu H., Wang Y., An X. Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology. *Journal of Computer and Communications*, 2020, vol. 8, no. 8, pp. 45-58.
21. Shif L., Wang F. Lung C. Improvement of security and scalability for IoT network using SD-VPN. *2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, Taiwan, 2018, pp. 1-5.
22. Gu R., Zhang X., Yu L., and Zhang J. Enhancing Security and Scalability in Software Defined LTE Core Networks. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE),* New York, USA, 2018, pp. 837-842.
23. Reyes G., Dammers M., Kastanja M. Security assessment on a VXLAN-based network. *Haettu*, 2014, vol. 10, no. 2017, pp. 2013–2014.
24. Liao S., Zhou C., Zhao Y., Zhang Z., Zhang C., Gao Y., and Zhong, G. A Comprehensive detection approach of Nmap: principles, rules and experiments. *2020 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, Chongqing, China, 2020, pp. 64–71.
25. JSON-RPC Working Group. JSON-RPC 2.0 Specification, available at: `https://www.jsonrpc.org/specification` (accessed: 04.04.2023).
26. Jetty S. *Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7*. Packt Publishing Ltd. 2018.
27. Kushko.E. A. *Metod realizacii zashchishchennogo obmena dannymi na osnove dinamicheskoj topologii seti* [Secure data communication implementing method based on dynamic network topology]. Vestnik SibGUTI, 2020, no. 4(52), pp. 39-52.

Evgenii A. Kushko
Senior lecturer of the department of information technologies security, Reshetnev Siberian State University of Science and Technology (660037, Russia, Krasnoyarsk, Imeni gazety «Krasnoyarskiy rabochiy» pr. 31), phone: +7 391 222 7639, e-mail: evgeny.kushko@gmail.com, ORCID ID: 0000-0003-1290-7075.

Nikolay Yu. Parotkin
Cand. of Sci. (Engineering), assistant professor of the department of information technologies security, Reshetnev Siberian State University of Science and Technology, e-mail: nyparotkin@yandex.ru, ORCID ID: 0000-0002-3486-0602.

Vyacheslav V. Zolotarev
Cand. of Sci. (Engineering), head of department of information technologies security, Reshetnev Siberian State University of Science and Technology, e-mail: amida.2@yandex.ru, ORCID ID: 0000-0002-8054-8564.

DOI: 10.55648/1998-6920-2023-17-4-74-88 УДК 004.9

Опыт организации информационной инфраструктуры Правительства Алтайского края в ответ на вызовы угроз безопасности

В. В. Снесарь, Е. А. Зрюмов, Д. Ю. Илли,
Е. М. Янкин, О. В. Чумак, С. О. Вольвач

Министерство цифрового развития и связи Алтайского края

Аннотация: Рассмотрены вопросы организации комплексной информационной инфраструктуры Правительства Алтайского края. Описаны этапы построения информационной инфраструктуры Правительства Алтайского края, которые включают определение требований, проектирование и внедрение информационной инфраструктуры, заключающееся в централизации каналов связи и цифровых сервисов, построении регионального центра обработки и хранения данных, установке системы мониторинга сетевого трафика и управления средствами антивирусной защиты.

Ключевые слова: информационная инфраструктура, корпоративная компьютерная сеть, цифровое государственное управление.

Для цитирования: Снесарь В. В., Зрюмов Е. А., Илли Д. Ю., Янкин Е. М., Чумак О. В., Вольвач С. О. Опыт организации информационной инфраструктуры Правительства Алтайского края в ответ на вызовы угроз безопасности // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 73–88. https://doi.org/10.55648/1998-6920-2023-17-4-73-88.

Статья поступила в редакцию 14.11.2022;
переработанный вариант – 07.12.2022;
принята к публикации 18.07.2023.

1. Введение

Информационные технологии стирают границы между государствами и становятся неотъемлемой частью практически всех сфер деятельности человека и общества. Эффективное применение цифровых решений является приоритетным фактором ускорения экономического развития государства и значимым конкурентным преимуществом на глобальных рынках [1, 2].

Глобализация информационной сферы предоставляет широкие возможности для обеспечения реализации стратегических национальных приоритетов Российской Федерации, но при этом несет и угрозы суверенитету, независимости, защите традиционных духовно-нравственных основ российского общества, обеспечению обороны и безопасности [3].

Возможности трансграничного оборота информации и глобальных цифровых экосистем всё чаще используются для достижения геополитических, противоречащих международному праву, а также террористических, экстремистских и криминальных целей в ущерб международной безопасности и стратегической стабильности [1].

Расширяются масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, возрастает количество атак на российские информационные ресурсы с территорий иностранных государств с целью блокировки работы государственных организаций, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека, в том числе в части неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий и методов социальной инженерии [1].

Ежедневно фиксируются факты DDoS-атак на различные государственные информационные сервисы, рассылки спам-сообщений на электронную почту организаций, распространения вредоносного программного обеспечения. Это приводит в ряде случаев к непоправимым последствиям: потере конфиденциальной информации, обрабатываемой в государственных информационных системах, скрытому майнингу криптовалют на рабочих местах сотрудников, несанкционированному управлению автоматизированных систем, в том числе относящихся к объектам критической информационной инфраструктуры.

Исходя из вышесказанного, информационная безопасность является одним из важнейших стратегических национальных приоритетов [4].

Первичный теоретический анализ проблем контроля безопасности на объектах коммуникационных систем, функционирующих в органах государственной власти субъектов Российской Федерации, содержит описание объекта защиты информации, угроз безопасности информации, общей структуры системы безопасности [5]. Однако при практической организации информационной инфраструктуры в высших органах исполнительной власти субъектов Российской Федерации нет единых подходов к обеспечению информационной безопасности. Например, оценка возможности применения методики централизованного управления системами и информационными рисками в органах государственной власти Республики Тыва произведена лишь в четырех органах власти, размещенных в одном здании, где основной целью является оптимизация затрат на приобретение средств защиты информации, а также фонда оплаты труда обслуживающего технического персонала [6].

Зачастую отсутствие централизованной политики обеспечения информационной безопасности на уровне региона приводит к потере управляемости мониторингом инцидентов информационной безопасности и невозможности оперативно устранять или купировать последствия атак на информационную инфраструктуру, использованию конфликтующих между собой программных и аппаратных средств защиты информации.

Целью статьи является формирование универсальных подходов к организации комплексной информационной инфраструктуры Правительства Алтайского края, которые могут быть использованы при централизации обеспечения информационной безопасности во всех субъектах Российской Федерации [7, 8].

Для организации комплексной информационной инфраструктуры Правительства Алтайского края были пройдены стадии, характерные для создания инфраструктурного объекта в области цифровизации [9] в соответствии с моделью жизненного цикла системы защиты информации[10]. Рассмотрим каждый из них более подробно.

2. Определение требований к информационной инфраструктуре

На первом этапе проведен анализ нормативных правовых актов [11–13], методических документов, национальных стандартов и приказов регуляторов [14–16], которым должна соответствовать информационная инфраструктура Правительства Алтайского края. Проведенное исследование позволило выявить и классифицировать государственные информационные системы, информационные системы персональных данных, каналы связи, средства криптографической защиты информации, используемые в информационной инфраструктуре Правительства Алтайского края. На основе этого определены угрозы безопасности информации, реализация которых может привести к нарушению работоспособности. Среди самых значимых проблем можно выделить следующие:

- самостоятельное обеспечение доступа в сеть Интернет каждым органом исполнительной власти Алтайского края;
- отсутствие в органах исполнительной власти Алтайского края контроля доступа в сеть Интернет;
- использование устаревших, зачастую не сертифицированных, устройств маршрутизации;
- большое количество вредоносных и спам-сообщений электронной почты на рабочих местах государственных гражданских служащих;
- вирусная (вредоносная) активность на компьютерах государственных гражданских служащих;
- отсутствие надлежащего контроля и мониторинга доступа государственных гражданских служащих к собственным информационным системам на уровне межсетевого экранирования и средств обнаружения вторжений;
- самостоятельная закупка каждым органом исполнительной власти Алтайского края программных и аппаратных средств преимущественно иностранного производства;
- отсутствие регламентов реагирования на возникающие события, связанные с нарушением информационной безопасности и порядка действий по их устранению (предотвращению);
- низкий уровень подготовки специалистов в сфере информационной безопасности.

В рамках исполнения данного этапа зафиксировано отсутствие единой политики обеспечения информационной безопасности на уровне Правительства Алтайского края, что создавало предпосылки для деструктивного воздействия на существующую информационную инфраструктуру. На основе выявленных недостатков сформированы требования к системе защиты информации информационной инфраструктуры Правительства Алтайского края.

3. Проектирование информационной инфраструктуры

На этапе проектирования построена архитектура информационной инфраструктуры Правительства Алтайского края, которая включает профессиональные высокопроизводительные и сертифицированные отечественные решения по обеспечению информационной безопасности. Выделим основные результаты, достигнутые при реализации этого этапа:

- централизация каналов доступа в сеть Интернет для всех органов исполнительной власти Алтайского края;
- создание единой точки доступа и обеспечение надлежащего контроля доступа к информационным системам и в сеть Интернет;
- мониторинг единой точки доступа с использованием средств обнаружения вторжений (IDS) и анализа событий информационной безопасности (TIAS) и последующее подключение информационной инфраструктуры каждого органа власти к системе мониторинга средствами обнаружения вторжений;
- централизация системы электронной почты Правительства Алтайского края;
- ввод в эксплуатацию специализированного программного обеспечения для анализа и проверки всех сообщений электронной почты, приходящих в адрес органов исполнительной власти Алтайского края;
- централизация размещения информационных систем и ресурсов органов исполнительной власти Алтайского края в региональном центре обработки и хранения данных (ЦОД);
- централизация средств антивирусной защиты с внедрением единой системы управления средствами антивирусной защиты вплоть до конкретного рабочего места государственного гражданского служащего;
- контроль процесса импортозамещения посредством централизации закупок отечественного программного и аппаратного обеспечения для нужд органов исполнительной власти Алтайского края;

- создание проекта регионального закона о государственных информационных системах в Алтайском крае;
- разработка регламента взаимодействия при возникновении событий, связанных с нарушением информационной безопасности;
- создание межведомственной рабочей группы по решению вопросов в сфере информационной безопасности;
- выстраивание системы повышения квалификации специалистов органов исполнительной власти Алтайского края, в том числе и по образовательным программам в сфере информационной безопасности, сертифицированным ФСТЭК России.

Создание единой политики обеспечения информационной безопасности на уровне Правительства Алтайского края базировалось на централизации практически всех функций в области информационной безопасности на органе исполнительной власти Алтайского края, уполномоченном в организации и координации мероприятий по совершенствованию систем защиты информации в информационных системах и информационных ресурсах – Министерстве цифрового развития и связи Алтайского края [17], что позволило:

- обеспечить единое управление политикой безопасности при работе государственных гражданских служащих в сети Интернет, а также при их доступе к информационным системам и ресурсам, размещённым в центре обработки и хранения данных;
- обеспечить контроль и фильтрацию трафика, мониторинг активности вредоносного программного обеспечения и оперативную реакцию на события информационной безопасности;
- обеспечить более высокий уровень защиты за счет использования эффективных средств информационной безопасности;
- увеличить степень внедрения отечественного программного и аппаратного обеспечения в органах исполнительной власти Алтайского края;
- снизить, а в ряде случаев полностью исключить, финансовые затраты органов исполнительной власти Алтайского края на самостоятельное обеспечение информационной безопасности, приобретение аппаратно-программных средств, каналов доступа в сеть Интернет, ведомственных каналов связи и эксплуатационные расходы на обеспечение работоспособности информационных систем и ресурсов, размещенных в региональном центре обработки и хранения данных.

Исходя из принципа реализации «практической безопасности», централизация является основой построения эффективной системы информационной безопасности.

4. Внедрение информационной инфраструктуры

Для внедрения спроектированной архитектуры информационной инфраструктуры Правительства Алтайского края были решены следующие задачи:

- проведение работ по централизации каналов связи и цифровых сервисов;
- формирование единой системы электронной почты;
- создание регионального центра обработки и хранения данных и обеспечение его средствами защиты для размещения государственных информационных систем;
- реализация системы мониторинга сетевого трафика и управления средствами антивирусной защиты.

Для реализации поставленных задач был организован центр компетенций, в который вошли специалисты отдела по администрированию информационной инфраструктуры и отдела информационной безопасности Министерства цифрового развития и связи Алтайского края, а также отдела импортозамещения подведомственного Министерству КГБУ «Оператор электронного правительства Алтайского края». Текущий статус выполнения работ рассматривался на заседаниях межведомственной рабочей группы по решению оперативных задач в обла-

сти информационной безопасности, в состав которой входят уполномоченные специалисты из каждого органа исполнительной власти Алтайского края. Общая координация работ осуществлялась Советом по защите информации при Губернаторе Алтайского края.

4.1. Централизация каналов связи

Сначала была произведена централизация каналов связи и доступа в сеть Интернет (рис. 1), которая включала в себя [18]:

- создание корпоративной сети передачи данных (КСПД) уровня L2 на базе одного из региональных провайдеров;
- приобретение автономной системы и блока независимых от провайдера IP-адресов;
- установку в каждый орган исполнительной власти Алтайского края оборудования, обеспечивающего криптографическую защиту канала связи и маршрутизацию (точка подключения);
- организацию и обеспечение доступа в сеть Интернет с помощью основного и резервного каналов, которые обеспечивают два провайдера с собственными магистральными каналами связи;
- организацию и обеспечение доступа в корпоративную сеть передачи данных.

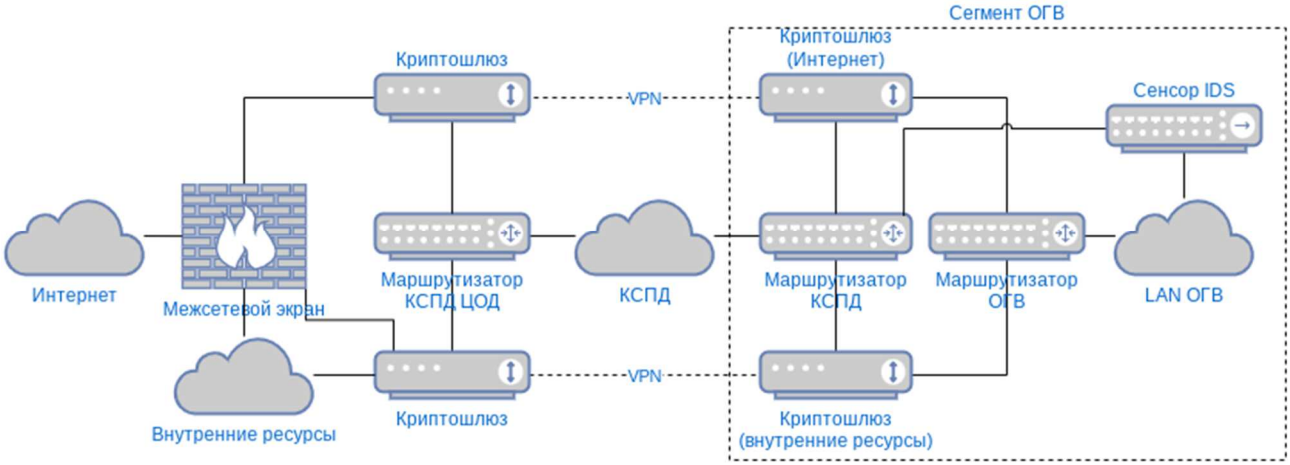

Рис. 1. Типовая схема подключения органов исполнительной власти Алтайского края

Эффект от централизации каналов связи оказался значительным. Если до этого каждый орган исполнительной власти Алтайского края самостоятельно приобретал каналы связи с пропускной способностью до 100 Мбит/с, что в совокупности предполагало использование канала с пропускной способностью 2.5 Гбит/с, то после проведенных мероприятий был сформирован единый канал связи для всех органов власти (основной и резервный с пропускной способностью 1 Гбит/с) при средней нагрузке от 300 до 550 Мбит/с при соотношении входящего и исходящего трафика – 80/20 процентов и 4000 рабочих мест (рис. 2 и 3).

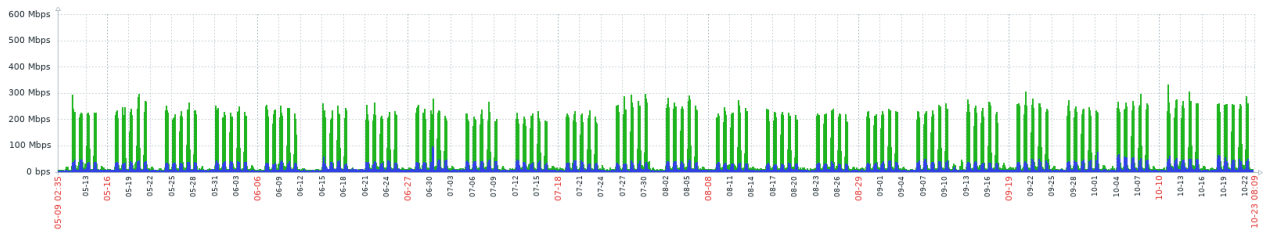

Рис. 2. Нагрузка на каналы связи в течение месяца

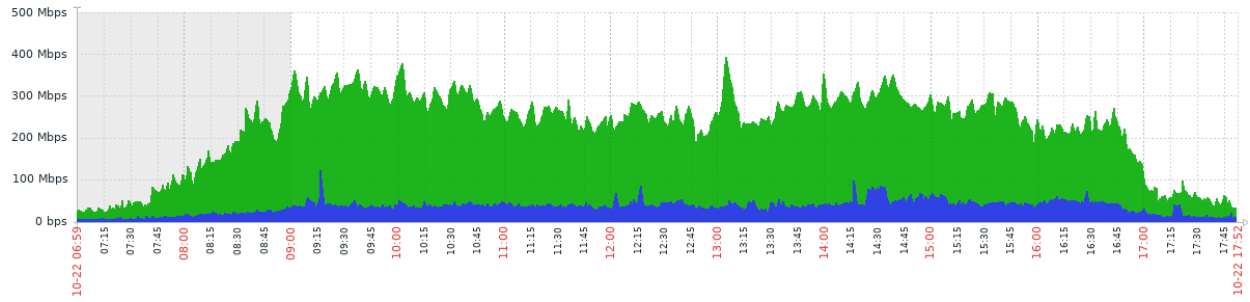

Рис. 3. Нагрузка на каналы связи в течение рабочего дня

После централизации каналов связи и доступа в сеть Интернет органы исполнительной власти Алтайского края перестали самостоятельно оплачивать услуги по доступу к корпоративной сети передачи данных, эта работа была организована на базе Министерства цифрового развития и связи Алтайского края.

4.2. Централизация системы электронной почты

Далее проводилась работа по централизации системы электронной почты как для серверов электронной почты органов исполнительной власти Алтайского края, так и для их подведомственных учреждений в виде сервиса. Для этого был сформирован шлюз безопасности, на основе решения «Kaspersky Security Mail Gateway», через который проходят все сообщения электронной почты и после необходимых проверок на спам и вредоносное программное обеспечение доставляются в почтовые ящики государственных гражданских служащих (рис. 4).

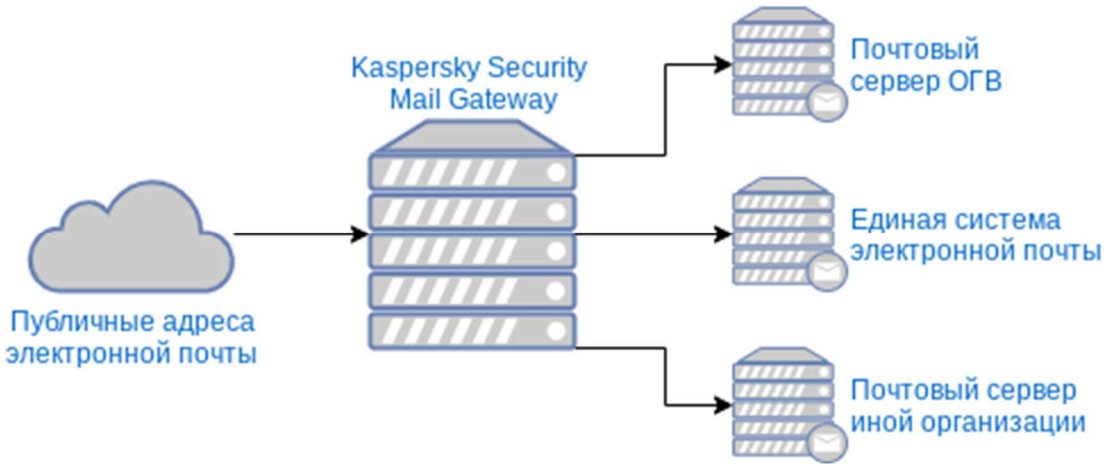

Рис. 4. Схема работы шлюза безопасности электронной почты

Единая система электронной почты Алтайского края была создана на базе двух отечественных продуктов – «CommuniGate Pro» и «Почта Mail.Ru», включенных в реестр отечественного программного обеспечения. Обе системы электронной почты размещены в центре обработки и хранения данных Алтайского края, что исключает доступ к почтовым сообщениям третьей стороны и обеспечивает надлежащий контроль пересылаемых электронных писем и вложений.

4.3. Региональный центр обработки и хранения данных

Далее были проведены работы по созданию регионального центра обработки и хранения данных, которые включали следующие этапы:

- обследование информационных систем органов исполнительной власти Алтайского края для определения потребности в вычислительных ресурсах и объемах хранения информации с учетом резервирования вычислительных ресурсов, резервного копирования информации и планируемого роста нагрузки на инфраструктуру в ближайшие три года;
- подготовка специализированных помещений для размещения серверного оборудования и систем хранения данных с учетом обеспечения гарантированного электроснабжения, надежного охлаждения и пожаротушения;
- создание инфраструктуры размещения информационных систем и ресурсов с использованием передовых технологий виртуализации аппаратных ресурсов и резервного копирования информации;
- формирование единой системы информационной безопасности в части защиты размещаемых информационных систем и ресурсов и обеспечения доступа к ним;
- создание многоуровневой распределенной автоматизированной системы мониторинга, обеспечивающей контроль состояния и управление оборудованием инфраструктуры размещения информационных систем, а также климатических параметров помещений;
- принятие закона Алтайского края от 24.12.2019 № 120-ЗС «О государственных информационных системах Алтайского края»;
- закрепление нормативно-правовым актом регионального центра обработки и хранения данных как приоритетной инфраструктуры для размещения информационных систем органов исполнительной власти Алтайского края.

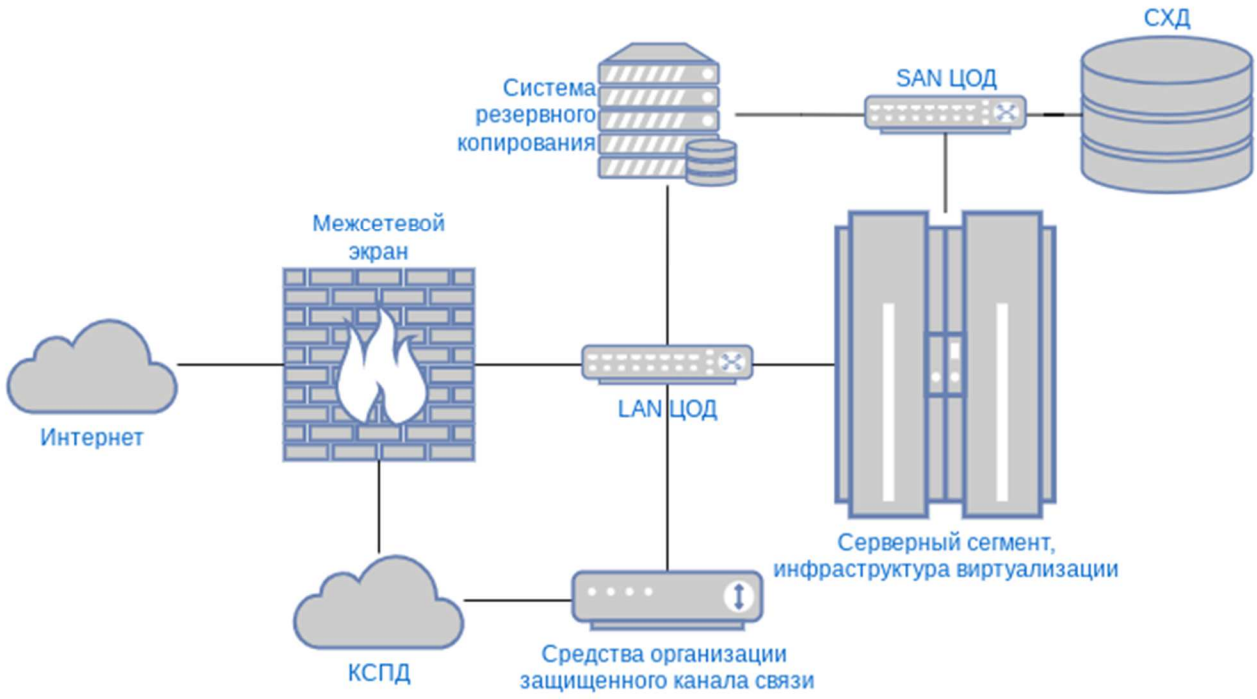

Рис. 5. Схема центра обработки и хранения данных

Созданный региональный центр обработки и хранения данных (рис. 5) обеспечен ресурсами в объеме: 1200 vCPU, 10.5 ТБ оперативной памяти, 167 ТБ емкости для хранения данных (50 ТБ – SSD, 88 ТБ – SAS, 29 ТБ – NLSAS), 370 ТБ – для хранения ежесуточных резервных копий в течение минимум тридцати дней.

В части информационной безопасности региональный центр обработки и хранения данных Алтайского края обеспечен сертифицированными средствами:

- организации защищенного канала связи (ViPNet CUSTOM 4.x, ViPNet TLS Gateway);
- межсетевого экранирования;
- межсетевого экранирования уровня приложений («Positive Technologies Application Firewall»);
- защиты среды виртуализации от несанкционированного доступа («vGate»);
- обнаружения вторжений (ViPNet IDS, ViPNet TIAS);
- анализа уязвимостей («Сканер-ВС»);
- доверенной загрузки (ПАК «Соболь»).

Доступ к информационным системам и ресурсам органов исполнительной власти Алтайского края обеспечен защитой от DDoS-атак на канальном уровне с использованием центров очистки трафика, расположенных на территории Российской Федерации.

На текущий момент в региональном центре обработки и хранения данных размещено 80 % информационных систем органов исполнительной власти Алтайского края, включая государственные системы и ресурсы, в абсолютном выражении это порядка двухсот виртуальных серверов.

4.4. Система мониторинга сетевого трафика и управления средствами антивирусной защиты

Следующий блок работ был посвящен выстраиванию системы мониторинга событий информационной безопасности в органах исполнительной власти Алтайского края и на рабочих местах государственных гражданских служащих и включал следующие этапы:

- создание единой системы управления средствами антивирусной защиты, вплоть до конкретного рабочего места государственного гражданского служащего;
- создание системы мониторинга сетевого трафика локальной инфраструктуры каждого органа исполнительной власти Алтайского края с использованием средств обнаружения вторжений и хранения журналов подключения к ресурсам сети Интернет;
- создание системы анализа событий информационной безопасности на основе баз экспертных данных;
- подключение информационной инфраструктуры к внешнему центру мониторинга информационной безопасности (Security Operations Center, SOC) компании «ИнфоТеКС» для обеспечения наиболее качественной экспертизы событий информационной безопасности и получения рекомендаций по их устранению (предотвращению);
- ежемесячное направление в адрес органов исполнительной власти Алтайского края бюллетеней об информационной безопасности, подготовленных сотрудниками Министерства на основе получаемой информации из центра мониторинга «СОПКА» об актуальных уязвимостях в оборудовании и программном обеспечении, банка данных угроз безопасности информации ФСТЭК России «bdu.fstec.ru» и собственных систем мониторинга;
- принятие Постановления Правительства Алтайского края от 19.11.2020 № 497 «Об утверждении Порядка взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности».

Система мониторинга трафика (рис. 6) на первый взгляд кажется сложной в реализации. Однако выбор решений, зарекомендовавших себя при эксплуатации во многих субъектах Российской Федерации, позволил создать единую точку регистрации и анализа событий с разграничением доступа для каждого органа исполнительной власти Алтайского края. К таким решениям относятся:

- средства обнаружения вторжений – ViPNet IDS;
- средства анализа событий информационной безопасности – ViPNet TIAS;
- средства управления поверхности внешней атаки – Attack Surface Management компании Group-IB.

Единый сервис журналирования и хранения данных о подключениях, как часть системы мониторинга, был реализован на базе стандартного протокола netflow.

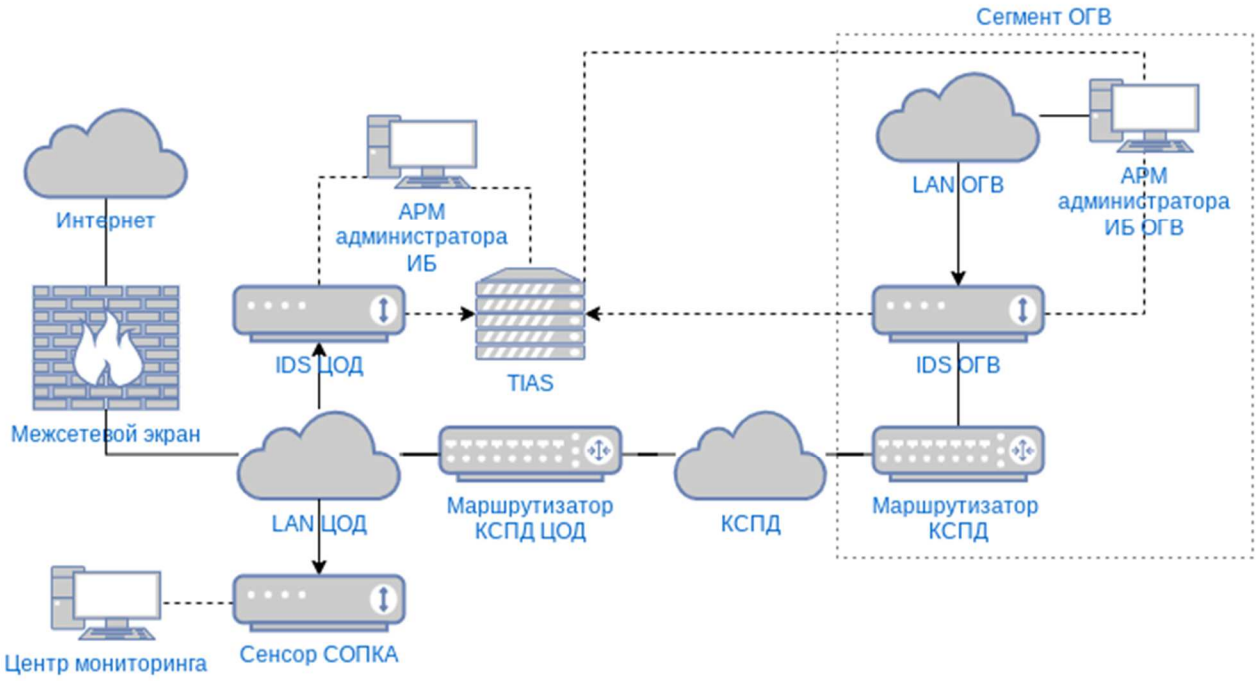

Рис. 6. Схема мониторинга событий информационной безопасности

Сформированная схема управления средствами антивирусной защиты позволила оперативно выявлять конкретное рабочее место – источник вредоносной активности (рис. 7), своевременно его блокировать и предотвращать распространение вредоносного воздействия на объекты информационной инфраструктуры Правительства Алтайского края.

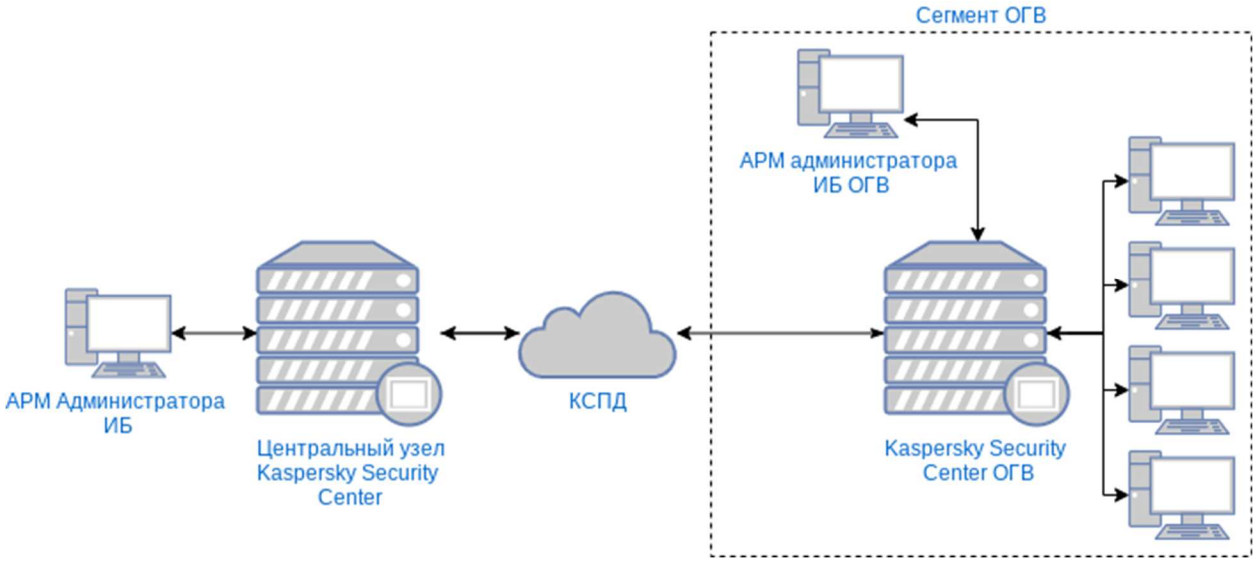

Рис. 7. Схема управления средствами антивирусной защиты

Важно отметить, что вместе с собственными системами мониторинга повысить эффективность выявления вредоносной активности позволяет подключение центрального узла доступа в сеть Интернет к центру мониторинга «СОПКА» и дальнейшее оперативное взаимодействие с сотрудниками центра.

5. Повышение компетенций в области информационной безопасности

Не менее важной задачей при выстраивании информационной инфраструктуры является подготовка и переподготовка кадров, которые в дальнейшем должны ее сопровождать и использовать, так как фиксируется недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности. Начиная с 2020 года проведены:

- очное обучение тридцати специалистов органов исполнительной власти Алтайского края, отвечающих за развитие информационных технологий, по сертифицированной ФСТЭК России программе повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» (72 часа);
- очное обучение пятидесяти муниципальных служащих по программе «Обеспечение защиты информации в органах местного самоуправления Алтайского края» (24 часа);
- краевой конкурс профессионального мастерства «Лучший по профессии» в номинации «Лучший системный администратор», включающий раздел, посвященный обеспечению информационной безопасности;
- тренировка в области информационной безопасности с органами исполнительной власти Алтайского края, в рамках которой на официальные адреса электронной почты государственных гражданских служащих были направлены спам-сообщения, содержащие ссылку для перехода на условно «зараженный» ресурс;
- обучение учителей общеобразовательных организаций Алтайского края по дополнительной профессиональной программе повышения квалификации «Кибербезопасность школ и профилактика правонарушений в сфере информационных технологий», разработанной Министерством цифрового развития и связи Алтайского края, Министерством образования и науки Алтайского края и компанией «Акронис-Инфозащита»;
- занятия со школьниками по теме информационной безопасности в рамках всероссийского образовательного проекта «Урок цифры» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерства просвещения Российской Федерации и АНО «Цифровая экономика».

6. Централизованное обеспечение компьютерной техникой

В рамках унификации подходов к обеспечению информационной безопасности Министерством цифрового развития и связи Алтайского края проводятся единые закупочные процедуры преимущественно отечественного программного обеспечения и аппаратных средств для нужд органов исполнительной власти Алтайского края на средства краевого бюджета. Типовое автоматизированное рабочее место государственного гражданского служащего состоит из:

- операционной системы «Astra Linux» или «ALT Linux»;
- офисного пакета «Р7-офис»;
- справочно-правовой системы «Консультант+» или «Гарант»;
- криптопровайдера для работы с электронной подписью и приложениями через протокол TLS «Крипто ПРО» или «ViPNet CSP»;
- браузера от компании «Yandex» или «Chromium GOST»;
- средства антивирусной защиты «Kaspersky» или «Dr.Web»;
- средства защиты от несанкционированного доступа «Secret Net» или «Dallas Lock»;
- средства доверенной загрузки ПАК «Соболь» (в случае необходимости).

7. Заключение

Проведенная в течение трех лет работа по организации комплексной информационной инфраструктуры Правительства Алтайского края показала свою эффективность как в организационном плане при реагировании на инциденты информационной безопасности, так и в финансовом плане при оптимизации расходов на приобретение программно-аппаратных комплексов.

Разработанные универсальные подходы к организации комплексной информационной инфраструктуры Правительства Алтайского края позволили:

- организовать централизованную защиту от DDoS-атак государственных информационных систем и ресурсов;
- обеспечить постоянный мониторинг, выявление и устранение уязвимостей в публичных информационных ресурсах;
- блокировать доступ к информационным системам с вредоносных IP-адресов (ресурсов), в том числе иностранных.

Описанный практический опыт построения информационной инфраструктуры Правительства Алтайского края является универсальным и может быть использован во всех субъектах Российской Федерации для обеспечения информационной безопасности государственных информационных систем и ресурсов с помощью отечественных программных и аппаратных средств.

Литература

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
2. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы».
3. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
4. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации (утв. Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31.08.2017).
5. *Демидов А. А.* Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: учебное пособие. СПб.: Университет ИТМО, 2015. 70 с.
6. *Донгак Б. С., Шатохин А. С., Мещеряков Р. В.* Эффективность централизованного использования цифровых технологий, информационных ресурсов и средств защиты информации в органах власти на примере республики Тыва // Известия Юго-Западного государственного университета. 2019. Т. 23, № 6. С. 99–114.
7. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. № 16).
8. Постановление Правительства Алтайского края от 24 января 2020 г. № 25 «Об утверждении государственной программы Алтайского края «Цифровое развитие экономики и информационной среды Алтайского края».
9. Постановление Правительства РФ от 06.06.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

10. *Соловьев М. Л., Минеева Т. Е., Конев А. А., Буинцев Д. Н.* Модель угроз безопасности, возникающих при управлении системой защиты информации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22, № 3. С. 31–36.
11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
13. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры».
14. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
15. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
16. Приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
17. Указ Губернатора Алтайского края от 6 декабря 2018 г. № 194 «Об утверждении Положения о Министерстве цифрового развития и связи Алтайского края».
18. Указ Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

Снесарь Виталий Владимирович
заместитель председателя Правительства Алтайского края – руководитель Администрации Губернатора и Правительства Алтайского края (656049, Барнаул, пр. Ленина, 59), e-mail: snesar@alregn.ru.

Зрюмов Евгений Александрович
д.т.н., доцент, министр цифрового развития и связи Алтайского края (656038, Барнаул, ул. К. Маркса, д. 1), e-mail: eaz@alregn.ru.

Илли Денис Юрьевич
начальник отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края (656038, Барнаул, ул. К. Маркса, д. 1), e-mail: iden@alregn.ru.

Янкин Евгений Михайлович
к.т.н., заместитель начальника отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: yankin@alregn.ru.

Чумак Олег Владимирович
консультант отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: ov.chumak@alregn.ru.

Вольвач Сергей Олегович
консультант отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: volvach@alregn.ru.

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.*

Experience in Organizing the Information Infrastructure of the Government of the Altai Region in Response to Security Threats

Snesar Vitaly V., Zryumov Evgeny A., Illi Denis U.,
Yankin Evgeny M., Chumak Oleg V., Volvach Sergey O.

Ministry of Digital Development and Communications of the Altai Region

Abstract: In this paper, complex information infrastructure of the government of the Altai Region is considered. The authors identify three possible stages of information infrastructure development of the government of the Altai Region, such as requirements definition, design, and implementation.

Keywords: information infrastructure, corporate network, digital public administration.

For citation: Snesar V. V., Zryumov E. A., Illi D. U., Yankin E. M., Chumak O. V., Volvach S. O. Experience in Organizing the Information Infrastructure of the Government of the Altai Region in Response to Security Threats (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 74-88. https://doi.org/10.55648/1998-6920-2023-17-4-74-88.

The article was submitted: 14.11.2022;
revised version: 07.12.2022;
accepted for publication 18.07.2023.

References

1. *Ukaz Prezidenta Rossiiskoi Federatsii «Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation “On approval of the Information Security Doctrine of the Russian Federation”]. 5 December, 2016, no. 646.
2. *Ukaz Prezidenta RF «O Strategii razvitiya informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017 - 2030 gody»* [Decree of the President of the Russian Federation “Strategy of the Information Society Development in the Russian Federation for 2017 – 2030”]. 9 May, 2017, no. 203.
3. *Ukaz Prezidenta Rossiiskoi Federatsii «O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation “On the National Security Strategy of the Russian Federation], 2 July, 2021, no. 400.
4. *Vypiska iz Osnovnykh napravlenii nauchnykh issledovanii v oblasti obespecheniya informatsionnoi bezopasnosti Rossiiskoi Federatsii (utv. Sekretarem Soveta Bezopasno-sti Rossiiskoi Federatsii N.P. Patrushevym)* [Extract from the Main Directions of Scientific Research in the Field of Ensuring Information Security of the Russian Federation]. 31 August, 2017.
5. Demodov A. A. *Problemy kontrolya bezopasnosti informatsii na ob"ektakh telekommunikatsionnykh sistem organov gosudarstvennogo upravleniya* [Problems of Information Security Control at the Objects of Telecommunication Systems of Government Bodies]. Saint Petersburg, ITMO University, 2015, 70 p.
6. Dongak B. S., Shatokhin R. V., Mescheryakov R. V. Effektivnost' tsentralizovannogo ispol'zovaniya tsifrovykh tekhnologii, informatsionnykh resursov i sredstv zashchity informatsii v organakh vlasti na primere respubliki Tyva [The effectiveness of the Centralized Use of Digital Technologies, Information

Resources and Information Protection Tools in Government by the Example of the Republic of Tyva]. *Proceedings of the Southwest State University*, 2019, vol.23 no. 6, pp. 99-114.

7. *Pasport natsional'noi programmy «Tsifrovaya ekonomika Rossiiskoi Federatsii» (utv. prezidiumom Soveta pri Prezidente Rossiiskoi Federatsii po strategicheskomu razvitiyu i natsional'nym proektam)* [Passport of the National Program "Digital Economy of the Russian Federation", approved by presidium of Council at the President of the Russian Federation for strategic development and national projects]. 24 December, 2018, no. 16.
8. *Postanovlenie Pravitel'stva Altaiskogo kraya ot 24 yanvarya 2020 g. №25 «Ob utverzhdenii gosudarstvennoi programmy Altaiskogo kraya «Tsifrovoe razvitie ekonomiki i informatsionnoi sredy Altaiskogo kraya»* [Decree of the Government of the Altai Territory "On approval of the state program of the Altai Territory "Digital development of the economy and information environment of the Altai Territory"]. 24 January, 2020, no. 25.
9. Postanovlenie Pravitel'stva RF «O trebovaniyakh k poryadku sozda-niya, razvitiya, vvoda v ekspluatatsiyu, ekspluatatsii i vyvoda iz ekspluatatsii gosudar-stvennykh informatsionnykh sistem i dal'neishego khraneniya soderzhashcheisya v ikh bazakh dannykh informatsii» [Decree of the Government of the Russian Federation "On Requirements for the Procedure for the Creation, Development, Commissioning, Operation and Decommissioning of State Information Systems, and Further Storage of Information Contained in their Databases"]. 6 July, 2015, no. 676.
10. Soloviev M. L., Mineeva T. E., Konev A. A., Buintsev D. N. Model' ugroz bezopasnosti, voznikayushchikh pri upravlenii sistemoi zashchity informatsii [Model of Security Threats Arising from the Management of Information Security Systems]. *Proceedings of the Tusur University*, Tomsk, 2019, vol. 22, no. 3, pp. 31-36.
11. *Federal'nyi zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»* [Federal "On information, information technologies and information protection"]. 27 July, 2006, no. 149-FZ.
12. *Federal'nyi zakon «O personal'nykh dannykh»*. [Federal Law "On personal data"]. 27 July, 2006, no.152-FZ.
13. *Federal'nyi zakon «O bezopasnosti kriticheskoi informatsionnoi infrastruktury»* [Federal Law "About safety of critical information infrastructure of the Russian Federation"]. 26 July, 2017, no.187-FZ
14. *Prikaz FAPSI «Ob utverzhdenii instruktsii ob organizatsii i obespechenii bezopasnosti khraneniya, obrabotki i peredachi po kanalam svyazi s ispol'zovaniem sredstv kriptograficheskoi zashchity informatsii s ogranichennym dostupom, ne soderzhashchei svedenii, sostavlyayushchikh gosudarstvennuyu tainu»* [FAPSI Order "On approval of the Instruction on the organization and security of storage, processing and transmission through communication channels using cryptographic protection of information with limited access, which does not contain information constituting a state secret"]. 13 June, 2001, no. 152.
15. *Prikaz FSTEK Rossii «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 Federal Service for Technical and Export Control OF Russia "About statement of Structure and content of organizational and technical measures for safety of personal data in case of their processing in personal data information systems"]. 18 February, 2013, no. 21.
16. *Prikaz FSTEK «Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavlyayushchei gosudarstvennuyu tainu, soderzhashcheisya v gosudarstvennykh informatsionnykh sistemakh»* [Order of Federal Service for Technical and Export Control OF Russia "Requirements for the protection of information that does not constitute a state secret contained in State information systems"]. 11 February, 2013, no. 17.
17. *Ukaz Gubernatora Altaiskogo kraya «Ob utverzhdenii Polozhe-niya o Ministerstve tsifrovogo razvitiya i svyazi Altaiskogo kraya»* [Decree of the Governor of the Altai Territory "On approval of the Regulations on the Ministry of Digital Development and Communications of the Altai Territory"]. 6 December, 2018, no. 194.
18. *Ukaz Prezidenta Rossiiskoi Federatsii «O nekotorykh voprosakh informatsionnoi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation "On Certain Issues of Information Security of the Russian Federation"]. 22 May, 2015, no. 260.

Vitaly V. Snesar
Deputy Head of the Government of the Altai Region – Head of the Administration of the Governor and the Government of the Altai Region (Lenina av., 59, Barnaul, Russia, 656049), e-mail: snesar@alregn.ru.

Evgeny A. Zryumov
Dr. of Sci. (Engineering), Docent, Minister of Digital Development and Communications of the Altai Region (K. Marksa st., 1, Barnaul, Russia, 656038), e-mail: eaz@alregn.ru.

Denis U. Illi
Head of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Territory, e-mail: iden@alregn.ru.

Evgeny M. Yankin
Cand. of Sci. (Engineering), Deputy Head of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Territory, e-mail: yankin@alregn.ru.

Oleg V. Chumak
Consultant of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Region, e-mail: ov.chumak@alregn.ru.

Sergey O. Volvach
Consultant of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Region, e-mail: volvach@alregn.ru.

DOI: 10.55648/1998-6920-2023-17-4-89-96 УДК 536. 2 (075)

Ортогональные методы взвешенных невязок в задачах теплопроводности для многослойных конструкций

Р. М. Клеблеев

Самарский государственный технический университет (СамГТУ)

Аннотация: На основе метода Галеркина, используя дополнительные краевые условия (ДКУ), получено аналитическое решение задачи теплопроводности для двухслойной пластины. ДКУ находятся так, чтобы их выполнение было адекватно выполнению исходных уравнений в точках границы. Выполнение уравнений в точках границы приводит к их выполнению во всем диапазоне пространственной координаты. Использование ДКУ позволяет получать цепочные системы алгебраических уравнений для неизвестных коэффициентов решения. Уравнения этих систем имеют сильно разре́женные хорошо обусловленные квадратные матрицы. В связи с чем их решения настолько упрощаются, что при большом числе приближений в общем виде следует решать систему лишь двух алгебраических уравнений. Наблюдается высокая точность нахождения собственных чисел, объясняемая применением особой конструкции ДКУ.

Ключевые слова: двухслойная пластина, метод Галеркина, дополнительные краевые условия, приближенное решение.

Для цитирования: Клеблеев Р. М. Ортогональные методы взвешенных невязок в задачах теплопроводности для многослойных конструкций // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 89–96. https://doi.org/10.55648/1998-6920-2023-17-4-89-96.

Статья поступила в редакцию 27.04.2023;
принята к публикации 16.08.2023.

1. Введение

Трудности нахождения точных решений краевых задач теплопроводности для многослойных тел обусловлены тем, что при определении собственных чисел возникает необходимость решения трансцендентного уравнения для собственных чисел задачи. Для получения его решения применяются численные методы [1 – 4]. Получение приближенных аналитических решений связано с использованием методов, основанных на системах координатных функций, удовлетворяющих всем краевым условиям (включая условия сопряжения) [3]. Однако получаемые таким путём решения плохо сходятся с увеличением числа приближений, что объясняется малой точностью определения собственных чисел. Ниже используется метод, связанный с построением дополнительных краевых условий (ДКУ) [5, 6], выполняемых лишь в точках границы, исключая точки контакта.

2. Математическая постановка задачи

Рассмотрим получение решения задачи теплопроводности для двухслойной пластины (рис. 1).

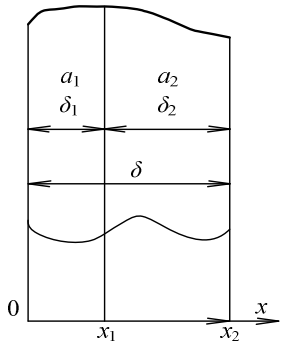

Рис. 1. Схема теплообмена

$$\frac{\partial T_i(x,t)}{\partial t} = a_i \frac{\partial^2 T_i(x,t)}{\partial x^2}; \tag{1}$$

$$(t > 0;\ \ x_{i-1} < x < x_i;\ \ i = 1,2;\ \ x_0 = 0;\ \ x_2 = \delta);$$

$$T_i(x,0) = T_0; \tag{2}$$

$$\partial T_1(0,t)/\partial x = 0; \tag{3}$$

$$T_1(x_1,t) = T_2(x_1,t); \tag{4}$$

$$\lambda_1 \partial T_1(x_1,t)/\partial x = \lambda_2 \partial T_2(x_1,t)/\partial x; \tag{5}$$

$$\partial T_2(x_2,t)/\partial x = 0, \tag{6}$$

где T, x, t – температура, координата, время;

a, λ_i – коэффициенты температуропроводности и теплопроводности;

$\delta = \delta_1 + \delta_2$ – суммарная толщина двух слоев;

δ_1, δ_2 – толщины слоёв; T_0 – начальная температура;

T_c – температура при $x = x_2 = \delta$.

Обозначим

$$\Theta_i(\xi, \mathrm{Fo}) = \frac{T_i(x,t) - T_c}{T_0 - T_c}, \quad (i = 1, 2); \quad \xi = \frac{x}{\delta}; \quad \mathrm{Fo} = \frac{a_1 t}{\delta^2}; \quad \xi_1 = \frac{x_1}{\delta}; \quad \xi_2 = \frac{x_2}{\delta}, \tag{7}$$

где Θ_i, $(i = 1, 2)$, ξ, Fo, – соответственно безразмерные температура, координата, время.

Учитывая (7), задача (1) – (6) преобразуется к виду

$$\frac{\partial \Theta_i(\xi, \mathrm{Fo})}{\partial \mathrm{Fo}} = \frac{a_i}{a_1} \frac{\partial^2 \Theta_i(\xi, \mathrm{Fo})}{\partial \xi^2}; \tag{8}$$

$$(\mathrm{Fo} > 0;\ \ \xi_{i-1} < \xi < \xi_i;\ \ i = 1,2;\ \ \xi_0 = 0;\ \ \xi_2 = 1);$$

$$\Theta_i(\xi, 0) = 1; \tag{9}$$

$$\partial \Theta_1(0, \mathrm{Fo})/\partial \xi = 0; \tag{10}$$

$$\Theta_1(\xi_1, \mathrm{Fo}) = \Theta_2(\xi_1, \mathrm{Fo}); \tag{11}$$

$$\partial \Theta_1(\xi_1, \mathrm{Fo})/\partial \xi = \lambda \partial \Theta_2(\xi_1, \mathrm{Fo})/\partial \xi; \tag{12}$$

$$\Theta_2(1, \mathrm{Fo}) = 0, \tag{13}$$

где $\lambda = \lambda_2 / \lambda_1$.

3. Получение аналитического решения

Решение задачи (8) – (13) примем в виде произведения

$$\Theta_i(\xi, \mathrm{Fo}) = \phi_i(\mathrm{Fo})\Psi_i(\xi), \quad (i = 1, 2), \tag{14}$$

где $\phi_i(\mathrm{Fo})$, $\Psi_i(\xi)$ – функции, зависящие от времени и координаты.

Подставив (14) в (8), имеем

$$d\phi_i(\mathrm{Fo}) / d\mathrm{Fo} + \mu\phi_i(Fo) = 0; \tag{15}$$

$$ad^2\Psi_i(\xi) / d\xi^2 + \mu\Psi_i(\xi) = 0, \tag{16}$$

где μ – постоянная; $a = a_i / a_1$, $(i = 1, 2)$.

Интеграл уравнения (15) имеет вид

$$\phi_i(\mathrm{Fo}) = A\exp(-\mu\mathrm{Fo}), \tag{17}$$

где A – постоянная интегрирования.

Подставив (14) в (10) – (13), находим

$$d\Psi_1(0) / d\xi = 0; \tag{18}$$

$$\Psi_1(\xi_1) = \Psi_2(\xi_1); \tag{19}$$

$$d\Psi_1(\xi_1) / d\xi = \lambda d\Psi_2(\xi_1) / d\xi; \tag{20}$$

$$\Psi_2(1) = 0. \tag{21}$$

Решения для уравнений (16) для каждого из слоев представляются в виде

$$\Psi_1(\xi) = 1 + \sum_{k=1}^{n} C_k\eta_k(\xi); \tag{22}$$

$$\Psi_2(\xi) = \sum_{k=1}^{n} B_k\gamma_k(\xi), \tag{23}$$

где C_k, B_k – постоянные; $\eta_k(\xi) = \xi^{2k}$, $\gamma_k(\xi) = 1 - \xi^{2k-1}$ – координатные функции ($k = \overline{1, n}$).

Отметим, что условия (18), (21) решениями (22), (23) выполняются. Константы C_k, B_k находятся из (19), (20) и ДКУ, определяемых в точках $\xi = \xi_0 = 0$ и $\xi = \xi_2 = 1$. Они находятся из условия, чтобы в указанных точках удовлетворялись уравнения (16). В [5, 7] математически доказывается, что выполнение уравнений на границах приводит к их выполнению и внутри слоев.

В точке $\xi = 0$ уравнение (16) (при $i = 1$) будет выполнено, если ДКУ для этой точки определять в виде

$$\frac{d^2\Psi_1(0)}{d\xi^2} + \mu\Psi_1(0) = 0. \tag{24}$$

Продифференцировав (24) по ξ, находим

$$\frac{d^3\Psi_1(0)}{d\xi^3} + \mu\frac{d\Psi_1(0)}{d\xi} = 0. \tag{25}$$

Соотношение (25) с учётом (18) приводится ко второму ДКУ в точке $\xi = 0$

$$\frac{d^3\Psi_1(0)}{d\xi^3} = 0. \tag{26}$$

Очевидно, что ДКУ (26) решением (22) выполняется. Продифференцируем (24) дважды по ξ

$$\frac{d^4\Psi_1(0)}{d\xi^4} + \mu\frac{d^2\Psi_1(0)}{d\xi^2} = 0. \tag{27}$$

Соотношение (27), учитывая (24), приводится к следующему ДКУ

$$\frac{d^4\Psi_1(0)}{d\xi^4}+\mu^2\Psi_1(0)=0\,. \tag{28}$$

Продифференцируем (24) три раза по ξ

$$\frac{d^5\Psi_1(0)}{d\xi^5}+\mu\frac{d^3\Psi_1(0)}{d\xi^3}=0\,. \tag{29}$$

Соотношение (29), учитывая (26), приводится к ДКУ вида

$$\frac{d^5\Psi_1(0)}{d\xi^5}=0\,. \tag{30}$$

Очевидно, что ДКУ (30) решением (22) удовлетворяется.

Следовательно, все ДКУ с нечётными номерами производных решением (22) выполняются. Общая формула ДКУ с чётными номерами производных, учитывая, что $\Psi_1(0)=1$ (так как $d\Psi_i(0)/d\xi=0$, то $\Psi_1(0)=const=1$), имеет вид

$$\frac{d^{2i}\Psi_1(0)}{\partial\xi^{2i}}=\pm\mu^i;\quad (i=\overline{1,n}), \tag{31}$$

где «плюс» – четные i, «минус» – нечетные.

В точке $\xi=1$ уравнение (16) (при $i=2$) будет выполнено, если ДКУ здесь определять в виде

$$a\frac{d^2\Psi_2(1)}{d\xi^2}+\mu\Psi_2(1)=0\,. \tag{32}$$

ДКУ (32), учитывая (21), упрощается и принимает вид

$$\frac{d^2\Psi_2(1)}{d\xi^2}=0\,. \tag{33}$$

Так как в точке $\xi=1$ имеем граничное условие первого рода (21), то ограничимся выполнением в этой точке лишь одного ДКУ вида (33).

Решение в первом приближении находится подстановкой (22), (23) (при трех членах рядов) в (19), (20), (31) (при $i=1,2,3$) и (33). Относительно C_k, B_k ($k=1,2,3$) имеем цепочную систему, включающую шесть алгебраических уравнений вида

$$\left.\begin{aligned}
&1+C_1\xi_1^2+C_2\xi_1^4+C_3\xi_1^6=B_1(1-\xi_1)+B_2(1-\xi_1^3)+B_3(1-\xi_1^5);\\
&2C_1\xi_1+4C_2\xi_1^3+6C_3\xi_1^5=-\lambda(B_1+3B_2\xi_1^2+5B_3\xi_1^5);\\
&(2C_1+12C_2\xi^2+30C_3\xi^4)_{\xi=0}=-\mu;\\
&(24C_2+360C_3\xi^2)_{\xi=0}=\mu^2;\\
&720C_3=-\mu^3;\\
&(6B_2\xi+20B_3\xi^3)_{\xi=1}=0\,.
\end{aligned}\right\} \tag{34}$$

Ввиду цепочности из системы уравнений (34) можно найти следующие коэффициенты (примем $\lambda=\lambda_1/\lambda_2=1$)

$$C_1=-0.5\mu;\ C_2=\mu^2/24;\ C_3=-\mu^3/720;\ B_2=-(10/3)B_3\,. \tag{35}$$

Подставляя полученные коэффициенты в первые два уравнения системы (34), для неизвестных B_1, B_3 имеем систему двух уравнений, решение которой будет

$$B_1 = \frac{105\cdot\mu}{328} - \frac{35\cdot\mu^2}{5248} + \frac{7\cdot\mu^3}{125952} + \frac{187\mu(\mu^2 - 80\cdot\mu + 1920)}{314880} - \frac{105}{41};$$

$$B_3 = \frac{6\mu}{41} - \frac{\mu^2}{328} - \frac{\mu^3}{39360} - \frac{\mu(\mu^2 - 80\cdot\mu + 1920)}{6560} + \frac{48}{41}.$$

Используя ортогональный метод Галеркина, составим интеграл невязки уравнений (16)

$$\int_0^{\xi_1}\left[\sum_{k=1}^{n} C_k \frac{\partial^2\eta_k}{\partial\xi^2} + \mu\left(1 + \sum_{k=1}^{n} C_k\eta_k\right)\right]d\xi + \int_{\xi_1}^{1}\left[\sum_{k=1}^{n} B_k \frac{\partial^2\gamma_k}{\partial\xi^2} + \mu\left(1 + \sum_{k=1}^{n} B_k\gamma_k\right)\right]d\xi = 0. \qquad (36)$$

Подставляя (22), (23), учитывая найденные значения C_k, B_k ($k = 1, 2, 3$), в (36), после нахождения интегралов для μ_k имеем степенное уравнение

$$1.557926\mu - 0.101562\mu^2 + 0.002103\mu^3 - 0.000018\mu^4 - 3.29268 = 0. \qquad (37)$$

Решение уравнения (37) будет

$$\mu_1 = 2.5004259; \qquad \mu_2 = 21.985176;$$

$$\mu_3 = 45.907 + 34.69i; \qquad \mu_4 = 45.907 - 34.69i.$$

Точные величины двух первых собственных чисел: $\mu_1 = 2.467401$; $\mu_2 = 22.2068$. Мнимые корни μ_3, μ_4 не используются.

Для уточнения собственных чисел потребуем удовлетворения условий ортогональности невязок уравнения (36) к функциям $\psi_1(\xi)$, $\psi_2(\xi)$

$$\int_0^{\xi_1}\left[\sum_{k=1}^{n} C_k \frac{\partial^2\eta_k}{\partial\xi^2} + \mu\left(1 + \sum_{k=1}^{n} C_k\eta_k\right)\right]\psi_1(\xi)d\xi +$$

$$+\int_{\xi_1}^{1}\left[\sum_{k=1}^{n} B_k \frac{\partial^2\gamma_k}{\partial\xi^2} + \mu\left(1 + \sum_{k=1}^{n} B_k\gamma_k\right)\right]\psi_2 d\xi = 0, \quad (k = 1, 2, 3). \qquad (38)$$

Отсюда относительно μ_k получаем алгебраический полином седьмой степени, из решения которого находим: $\mu_1 = 2.46787$; $\mu_2 = 22.2162$. Как видно, первое и второе собственные числа существенно уточнились.

Во втором приближении ко всем использованным в первом приближении основным граничным условиям и ДКУ добавляется ещё ДКУ (31) (при $i = 4, 5$). Ограничиваясь четырьмя членами рядов (22), (23), для неизвестных C_k, B_k ($k = \overline{1, 4}$) будем иметь цепочную систему восьми алгебраических уравнений. Ввиду цепочности шесть неизвестных находятся вне системы. Оставшиеся коэффициенты находятся из решения системы двух уравнений.

Подставляя (17), (22), (23) в (14), получаем

$$\Theta_1(\xi, \mathrm{Fo}) = \sum_{j=1}^{2}\left[A_j \exp(-\mu_j Fo)\left(1 + \sum_{k=1}^{3} C_k\eta_k(\xi)\right)\right]; \qquad (39)$$

$$\Theta_2(\xi, \mathrm{Fo}) = \sum_{j=1}^{2}\left[A_j \exp(-\mu_j Fo)\left(1 + \sum_{k=1}^{3} B_k\gamma_k(\xi)\right)\right]. \qquad (40)$$

Неизвестные A_j ($j = 1, 2$) находятся из невязки начального условия (9) путем выполнения условия ее ортогональности к функциям $\eta_k(\xi)$ и $\gamma_k(\xi)$ ($k = 1, 2$)

$$\int_0^{\xi_1}\left[\Theta_1(\xi, \mathrm{Fo}) - 1\right]\eta_k(\xi)d\xi + \int_{\xi_1}^{1}\left[\Theta_1(\xi, \mathrm{Fo}) - 1\right]\gamma_k(\xi)d\xi = 0; \quad (k = 1, 2). \qquad (41)$$

Подставим (39), (40) в (41)

$$\int_0^{\xi_1}\left[\sum_{i=1}^{2} A_j\left(1-\sum_{k=1}^{3} C_k\eta_k(\xi)\right)\right]\eta_k(\xi)d\xi+\int_{\xi_1}^{1}\left[A_j\left(1+\sum_{k=1}^{3} B_k\gamma_k(\xi)\right)\right]\gamma_k(\xi)d\xi=0\,. \quad (42)$$

Соотношение (42) является системой, включающей два алгебраических уравнения относительно A_j ($j=1,2$). Её решение: $A_1=1.338854$; $A_2=-0.310830$.

4. Анализ полученных результатов

Из расчетов по соотношениям (39), (40) (для $\lambda=1$, $a=1$ – однослойная система) следует, что при $0.1\le \mathrm{Fo}<\infty$ рассогласование с точным решением не более $4\,\%$ (рис. 2).

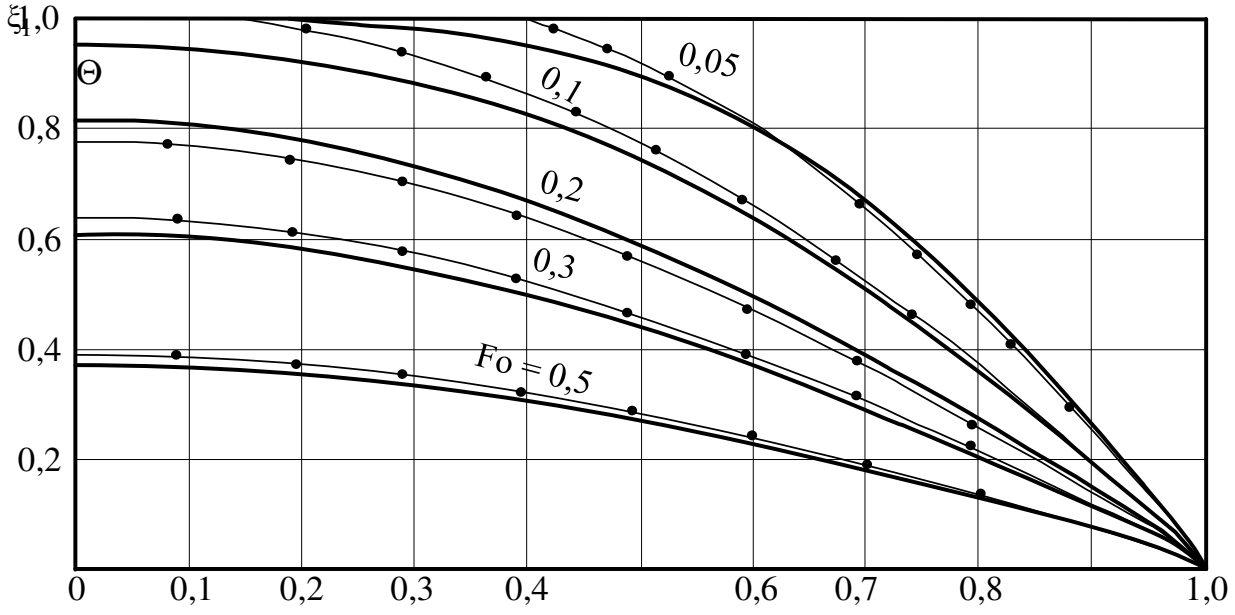

Рис. 2. Распределение температуры —●— – по формулам (39), (40);
——— – точное решение [1, 2]

5. Заключение

1. Получено аналитическое решение краевой задачи теплопроводности для двухслойной конструкции на основе использования ДКУ в ортогональных методах взвешенных невязок (метод Галеркина).

2. ДКУ находятся путем выполнения исходных уравнений в точках границы, что приводит к их удовлетворению и внутри слоев.

Литература

1. *Лыков А. В.* Теория теплопроводности. М.: Высшая школа, 1967. 600 с.
2. *Карташов Э. М.* Аналитические методы в теории теплопроводности твердых тел. М.: Высшая школа, 2001. 550 с.
3. *Карташов Э. М., Кудинов В. А., Калашников В. В.* Теория тепломассопереноса: решение задач для многослойных конструкций. М.: Издательство Юрайт, 2018. 435 с.

4. *Беляев Н. М., Рядно А. А.* Методы нестационарной теплопроводности. М.: Высшая школа, 1978. 328 с.
5. *Кудинов И. В., Котова Е. В., Кудинов В. А.* Метод получения аналитических решений краевых задач на основе определения дополнительных граничных условий и дополнительных искомых функций // Сибирский журнал вычислительной математики. 2019. Т. 22, № 2. С.153–165.
6. *Кудинов В. А., Аверин Б. В., Стефанюк Е. В.* Теплопроводность и термоупругость в многослойных конструкциях. М.: Высшая школа, 2008. 305 с.
7. *Федоров Ф. М.* Граничный метод решения прикладных задач математической физики. Новосибирск: Наука, 2000. 220 с.

Клеблеев Руслан Мухтарович
Старший преподаватель кафедры теоретических основ теплотехники и гидромеханики, Самарский государственный технический университет (СамГТУ, 443100, Самара, ул. Молодогвардейская, д. 244), e-mail: uio1123@list.ru, ORCID ID: 0000-0002-6944-8503.

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

Orthogonal Methods of Weighted Residuals in Thermal Conductivity Problems for Multilayer Structures

Ruslan M. Klebleev

Samara State Technical University (SamSTU)

Abstract: An analytical solution of the heat conduction problem for a two-layer plate based on the Galerkin method and usage of additional boundary conditions (ABC) is obtained. The ABCs are found in such a way that their implementation is to be adequate to the implementation of the original equations at the boundary points. Execution of equations at boundary points leads to their execution over the entire range of spatial coordinates. The use of ABC allows us to obtain chain systems of algebraic equations for unknown solution coefficients. The equations of these systems have highly sparse well-conditioned square matrices. In this connection, their solutions are so simplified that with a large number of approximations, in general form, a system of only two algebraic equations should be solved. A high accuracy of finding the eigenvalues is observed that is explained by the use of a special ABC design.

Keywords: two-layer plate, Galerkin method, additional boundary conditions, approximate solution.

For citation: Klebleev R. M. Orthogonal methods of weighted residuals in thermal conductivity problems for multilayer structures (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 89-96. https://doi.org/10.55648/1998-6920-2023-17-4-89-96.

The article was submitted: 27.04.2023;
accepted for publication 16.08.2023.

References

1. Lykov A. V. *Teoriya teploprovodnosti* [Theory of thermal conductivity]. Moscow, Vysshaya shkola, 1967. 600 p.
2. Kartashov E. M. *Analiticheskie metody v teorii teploprovodnosti tverdykh tel* [Analytical methods in the theory of thermal conductivity of solids]. Moscow, Vysshaya shkola, 2001. 550 p.
3. Kartashov E. M., Kudinov V. A., Kalashnikov V. V. *Teoriya teplomassoperenosa: reshenie zadach dlya mnogosloinykh konstruktsii* [Theory of heat and mass transfer: solving problems for multilayer structures]. Moscow, Yurait, 2018. 435 p.
4. Belyaev N. M., Ryadno A. A. *Metody nestatsionarnoi teploprovodnosti* [Methods of unsteady thermal conductivity]. Moscow, Vysshaya shkola, 1978. 328 p.
5. Kudinov I. V., Kotova E. V., Kudinov V. A. Metod polucheniya analiticheskikh reshenii kraevykh zadach na osnove opredeleniya dopolnitel'nykh granichnykh uslovii i dopolnitel'nykh iskomykh funktsii [A method for obtaining analytical solutions to boundary value problems based on determining additional boundary conditions and additional required functions]. *Siberian Journal of Computational Mathematics,* Novosibirsk, 2019, vol. 22, no. 2, pp. 153-165.
6. Kudinov V. A., Averin B. V., Stefanyuk E. V. *Teploprovodnost' i termouprugost' v mnogosloinykh konstruktsiyakh* [Thermal conductivity and thermoelasticity in multilayer structures]. Moscow, Vysshaya shkola, 2008. 305 p.
7. Fedorov F. M. *Granichnyi metod resheniya prikladnykh zadach matematicheskoi fiziki* [Boundary method for solving applied problems of mathematical physics]. Novosibirsk, Nauka, 2000. 220 p.

Ruslan M. Klebleev

Senior lecturer of the Department of Theoretical Foundations of Heat Engineering and Fluid Mechanics, Samara State Technical University (SamSTU, Russia, 443100, Samara, Molodogvardeyskaya St., 244), e-mail: uio1123@list.ru, ORCID ID: 0000-0002-6944-8503.

DOI: 10.55648/1998-6920-2023-17-4-97-108 УДК 004.728.3

Анализ эффективности использования частотно-временного ресурса для различных CORESET-конфигураций в сетях 5G NR *

Т. С. Шелихова, В. Г. Дроздова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: Мобильные сети 5-го поколения New Radio предназначены для решения задач обеспечения беспроводным доступом к сети Интернет пользователей с самым разными требованиями к качеству обслуживания. Для осуществления этих задач функции распределения ресурсов радиоинтерфейса, реализуемые производителями оборудования и программного обеспечения на базовых станциях, должны динамически информировать пользователей о своих решениях посредством так называемых элементов каналов управления, которые, в свою очередь, располагаются в области сконфигурированных CORESET. Настройка и конфигурация параметров CORESET оказывает существенное влияние на эффективность использования ресурсов радиоканала. В рамках данной статьи рассмотрены вопросы конфигурации CORESET и их влияние на ключевые показатели эффективности использования радиоресурсов.

Ключевые слова: 5G, NR, New Radio, PDCH, CORESET.

Для цитирования: Шелихова Т. С., Дроздова В. Г. Анализ эффективности использования частотно-временного ресурса для различных CORESET-конфигураций в сетях 5G NR // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 97–108. https://doi.org/10.55648/1998-6920-2023-17-4-97-108.

Статья поступила в редакцию 31.05.2023;
переработанный вариант – 14.07.2023;
принята к публикации 23.07.2023.

1. Введение

В настоящее время сети 5G NR представляют собой одну из наиболее перспективных технологий беспроводной связи, которая уже находится в процессе коммерциализации. Эти сети обеспечивают более высокий уровень производительности, надежности и масштабируемости по сравнению с предыдущими поколениями мобильных сетей [1]. Разработка программного обеспечения для таких технологий является нетривиальной задачей, в ходе которой производители базовых станций имплементируют различные алгоритмы, обеспечивающие эффективное (прежде всего, в смысле использования вычислительных ресурсов процессора или ПЛИС) функционирование системы в соответствии со стандартными спецификациями 3GPP (3rd Generation Partnership Project) [2]. Однако в стандартах 5G, как правило, описываются лишь общие принципы функционирования и не затрагиваются вопросы реализации самих алгоритмов, в связи с чем разработка данных алгоритмов становится актуальной

* Работа выполнена в рамках государственного задания № 123030900019-8.

задачей, особенно с учетом огромного количества входных параметров, оказывающих существенное влияние на результирующую производительность системы.

Одним из важных аспектов разработки и оптимизации сетей 5G NR является использование так называемых CORESET-ресурсов (Control Resource Set). CORESET представляют собой набор ресурсов, выделенных для передачи управляющей информации CCE (например, управляющих каналов PDCCH). CORESET может быть настроен для различных сценариев использования, что позволяет оптимизировать качество обслуживания и использование ресурсов сети.

Изучение понятия CORESET является актуальным в контексте разработки и оптимизации сетей 5G NR. Многие исследования, направленные на улучшение производительности и надежности в 5G NR, уделяют внимание именно CORESET-ресурсам [3–5]. В частности, изучение возможностей и ограничений использования CORESET-ресурсов является важным элементом оптимизации показателей качества обслуживания в 5G NR, как показано в [6].

В [7] авторами выполнен всесторонний анализ вероятности блокировки канала трафика из-за перегрузки по PDCCH для различных размеров CORESET-канала.

Таким образом, исследование различных конфигураций CORESET является важным шагом в оптимизации использования ресурсов сети 5G NR. Полученные в этом исследовании данные могут быть использованы для дальнейшей оптимизации параметров сети и повышения ее эффективности.

2. Нисходящий канал управления PDCCH и форматы DCI

Для назначения пользователям частотно-временных ресурсов в обоих направлениях (нисходящий канал DL и восходящий канал UL) планировщик базовой станции gNB (Scheduler – программная реализация функции динамического распределения радиоресурсов) использует физический нисходящий канал управления PDCCH (Physical Downlink Control CHannel) [8]. Этот канал используется на радиоинтерфейсе 5G для того, чтобы передавать абонентам так называемые DCI-сообщения (Downlink Control Information – информация канала управления PDCCH). DCI – это как раз те данные, которые будут на выходе функции Scheduler.

DCI-сообщения требуются для того, чтобы проинформировать пользователей UE (User Equipment) о том, как распределены ресурсы DL/UL, а именно каналы PDSCH/PUSCH: в каких слотах (или даже мини-слотах), в каких частотных ресурсных блоках и с какой кодово-модуляционной схемой MCS (Modulation and coding Scheme) передаются данные.

UE принимает решение о том, что данный DCI предназначен именно ему, благодаря тому что на gNB этот DCI скремблируется с помощью C-RNTI пользователя (Cell Radio Network Temporary ID — временный идентификатор UE на радиоинтерфейсе). Аналогично абонент определяет, что DCI используется для назначения ресурсов под процедуры пейджинга (вызова абонентов), ответа на запросы при случайном доступе RAR (Random Access Response), блоков системной информации SIB (System Information Block) – эти DCI скремблированы соответствующими известными всем абонентам идентификаторами.

Если UE не смог декодировать PDCCH, который был ему назначен, например, канал PDSCH (Physical DL Shared Channel), он будет продолжать декодирование PDCCH в остальных PDCCH-кандидатах с учетом уровня агрегирования элементов канала управления CCE (Control Channel Elements), который может быть повышен при следующей попытке декодирования в рамках адаптации канала.

Кроме того, стоит отметить, что стандартом 3GPP TS 38.212 [9] описываются различные форматы DCI-сообщений, которые используются базовой станцией в зависимости от того, под какие именно данные выделяется частотно-временной ресурс ее планировщиком.

3. Агрегация элементов канала управления CCE и конфигурация ресурсов для CORESET

Минимальная порция частотно-временного ресурса в сетях 5G NR внутри канала управления PDCCH, с помощью которой можно распределять ресурсы остальных каналов, называется элементом канала управления CCE [8]. Уровень агрегации CCE PDCCH – это число элементов канала управления CCE, необходимое для передачи DCI, предназначенного одному пользователю или пользователям, слушающим широковещательные сообщения. Один CCE состоит из 72 ресурсных элементов (Resource Elements RE) или из 6 REG (RE Group=12 Res). Стандартом 3GPP TS38.212, п. 7.3. [9] предусматривается возможность агрегации 1, 2, 4, 8 и 16 CCE для пользователей, при этом возможное число DCI-кандидатов определяется уровнем агрегации AL (Aggregation Level). На рис. 1 показан пример агрегации CCE в нисходящем канале управления PDCCH.

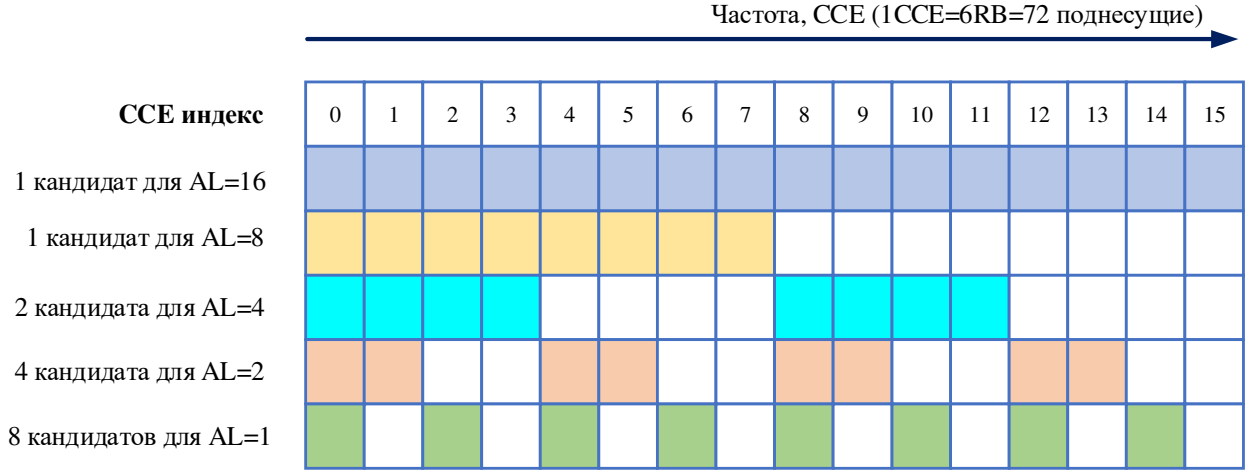

Рис. 1. Агрегация CCE в нисходящем канале управления PDCCH

Стоит отметить, что не все из 72 RE-элементов в REG выделены под PDCCH, а лишь 54. 18 ресурсных элементов предназначены для передачи пилотных сигналов DM-RS (демодуляционные опорные сигналы), с помощью которых абонентские станции и выполняют оценку канала.

Канал PDCCH, структурированный в форме CCE, передается внутри области CORESET. Различают CORESET#0, предназначенный для назначения SIB1-блока, и другие типы – для всего остального (хотя в CORESET#0 и не запрещено передавать другие DCI). Принципиально отличается подход к планированию этих типов CORESET. Ресурсы 0-го CORESET всегда распределяются в рамках параметров, передаваемых внутри MIB-блока (канал PBCH), в то время как конфигурация остальных CORESET осуществляется через RRC-сообщения (RRC – Radio Resource Control [10]) во время установления соединения. На рис. 2 показан пример информационного элемента внутри RRC-сообщения, с помощью которого конфигурируется CORESET#1. Во-первых, это параметр *frequencyDomainResources*, значение которого является битовой последовательностью, где единицы – это группы ресурсных блоков (CCE), объединенные по 6, которые можно использовать для передачи CORESET, а нули – соответственно, CCE, не содержащие в себе данные канала PDCCH.

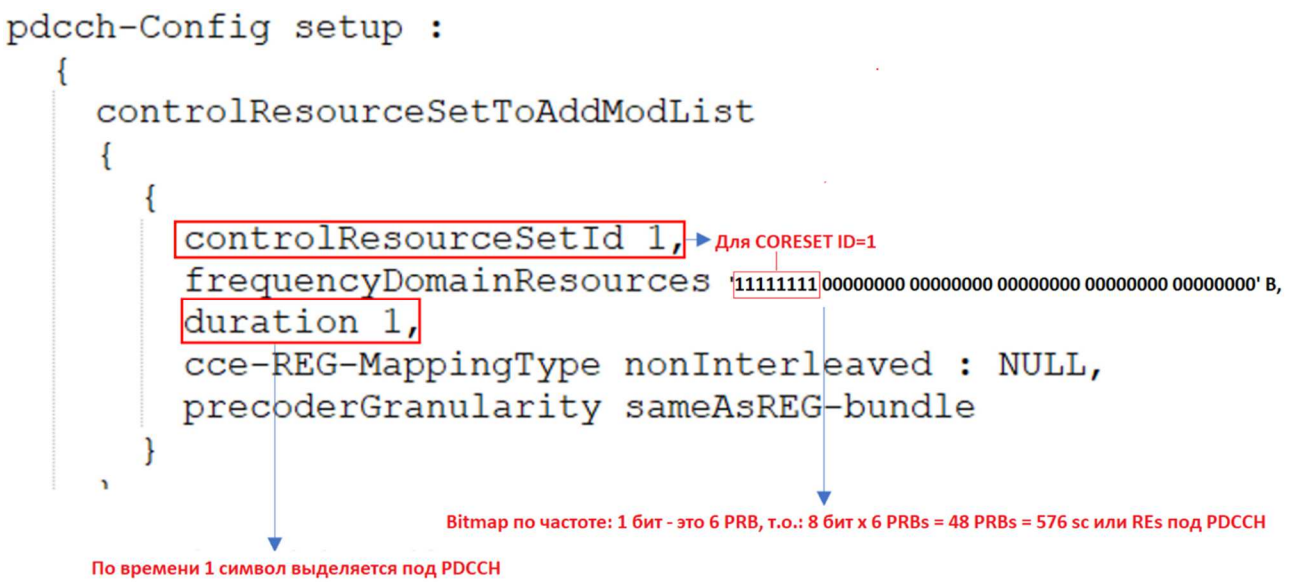

Рис. 2. Пример параметров, конфигурирующих CORESET#1

Второй параметр – *duration*. Это длительность CORESET внутри слота в символах. Кроме того, параметрами *cce-REG-MappingType* и *PrecoderGranularity* можно сконфигурировать возможность дополнительного перемежения CCE и способа прекодирования.

4. Конфигурация пространства поиска (Search Space)

Абоненты NR обычно не должны декодировать каждого PDCCH-кандидата, так как это слишком вычислительно затратно (вызов функции полярного декодирования, деперемежителя, вычисления CRC и пр.). Вместо этого пользователям конфигурируются так называемые пространства поиска Search Spaces (SS).

Search Space – это набор последовательных CCE, которые абоненты должны считывать с некоторой заданной периодичностью, находясь в состоянии RRC_Connected, ожидая, что в одном из таких пространств им могут быть выделены ресурсы планировщиком (то есть придет DCI, скремблированный C-RNTI-идентификатором данного пользователя).

Существует два типа Search Spaces для управления ресурсами на каждой несущей (Component Carrier):

– Common Search Space (CSS): CRC для DCI таких пространств скремблируются SI-RNTI (System Information), RA-RNTI (Random Access), TC-RNTI (Temporary Cell RNTI), P-RNTI (Paging), INT-RNTI (Interruption), SFI-RNTI (Slot Format Indication), TPC-PUCCH-RNTI (Tx Power Control), TPC-PUSCH-RNTI, TPC-SRS-RNTI, C-RNTI (Cell RNTI), CS-RNTI (Configured Scheduling). То есть это пространство используется для назначения общих управляющих каналов (CCCH, BCCH, PCCH). Это пространство поиска могут декодировать все абоненты соты.

– UE-Specific Search Space (USS): CRC для DCI таких пространств скремблируются C-RNTI (Cell RNTI), CS-RNTI (Configured Scheduling). Они предназначены для назначения каналов, выделенных пользователям UE (DTCH, DCCH).

В 3GPP-спецификации TS 38.212 [9] говорится, что UE должны декодировать PDCCH в 4 USS с уровнями агрегации 1, 2, 4 и 8 и 2 CSS с уровнями AL 4 и 8.

CSS- и USS-пространства для различных абонентов могут мультиплекироваться на CCE-уровне. Для того чтобы эффективно использовать ресурсы и минимизировать конфликты, одни и те же REG/CCE могут быть совместно использованы разными пространствами поиска, но каждое пространство может хэшировать различные CCE. В TS 38.213, п. 10.1 [11] приводится маппинг между типами RNTI и PDCCH Search Space. Там же описывается, как происходит процесс поиска нужного абонентским станциям SS. На рис. 3 представлен пример

информационных элементов для *pdcch-Config*, который используется терминалами для того, чтобы идентифицировать те SS, которые требуется декодировать.

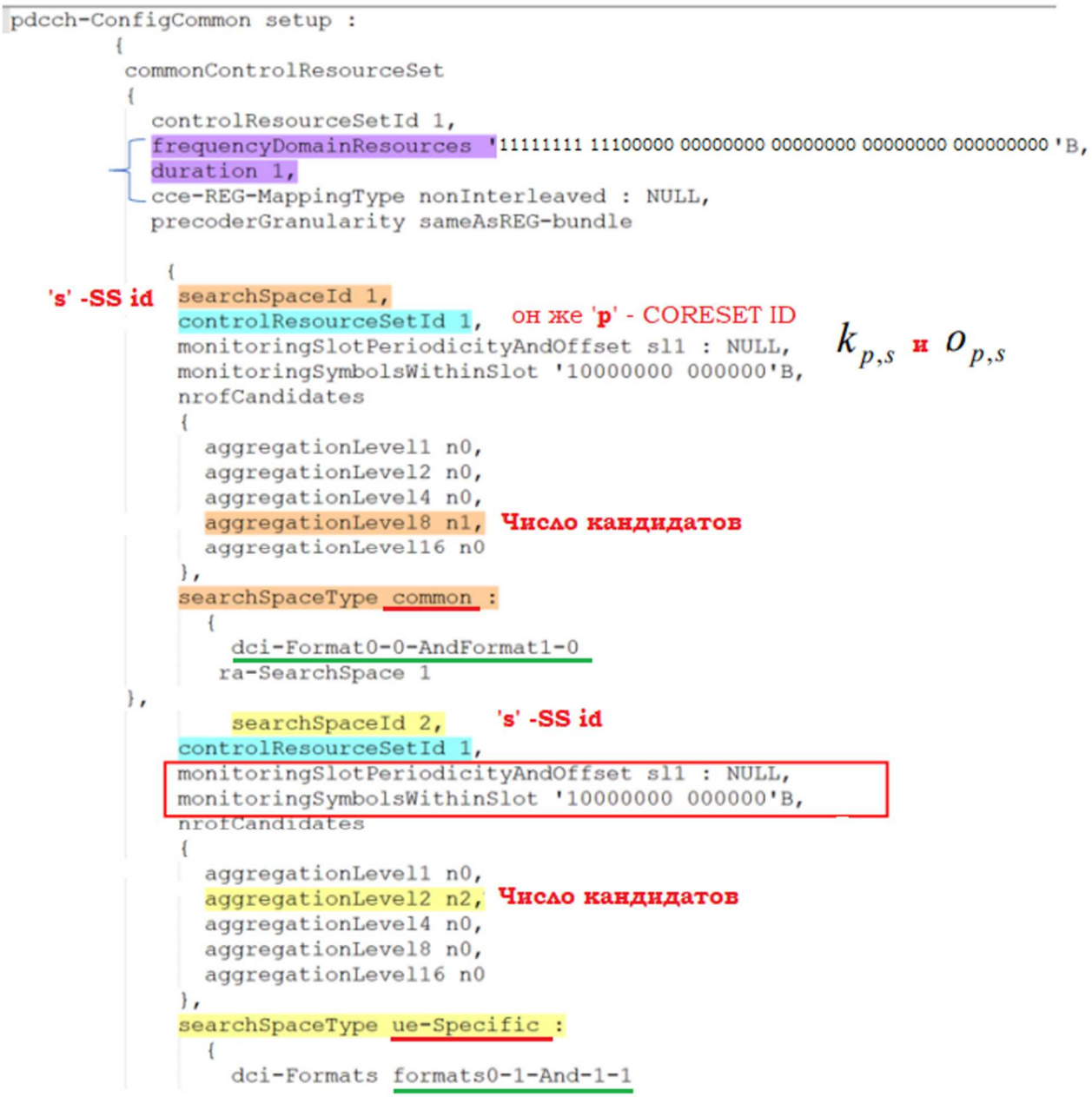

Рис. 3. Пример параметров, конфигурирующих CORESET#1

Для начала абонентам необходимо определить индексы или номера PDCCH-кандидатов $CCEindex_{m_{s,n_{CI}}}$, которые нужно декодировать (m – это индекс кандидата в SS, s – индекс слота в кадре). Это делается с помощью формулы:

$$CCEindex_{m_{s,n_{CI}}} = L \cdot \left\{ \left(Y_{p,n^{\mu}_{s,f}} + \frac{m_{s,n_{CI}} \cdot N_{CCE,p}}{L \cdot M^{(L)}_{p,s,max}} + n_{CI} \right) mod \left. N_{CCE,p} \middle/ L \right. \right\} + i \ , \quad (1)$$

где $L \in \{1, 2, 4, 8, 16\}$ – это уровень агрегации CCE;

$Y_{p,n^{\mu}_{s,f}} = 0$ – для CSS и

$$Y_{p,n^{\mu}_{s,f}} = \left(A_p \cdot Y_{p,n^{\mu}_{s,f}-1} \right) modD, Y_{p,-1} = n_{RNTI} \neq 0; \quad (2)$$

- $A_p = 39827$ для $p \; mod \; 3 = 0$;
- $A_p = 39829$ для $p \; mod \; 3 = 1$;
- $A_p = 39839$ для $p \; mod \; 3 = 2$;

$D = 65537$;

$i = 0, \dots, L - 1$;

$N_{CCE,p}$ – число CCE в корсете p;

n_{CI} – индикатор несущей (carrier indicator), нужен только для Cross-Carrier Scheduling, во всех остальных случаях, включая все CSS = 0;

$m_{s,n_{CI}} = 0, \dots M_{p,s,n_{CI}}^{(L)} - 1$ – индексы сконфигурированных абонентам PDCCH-кандидатов с L-уровнем агрегации в s-пространстве p-го корсета;

$M_{p,s,n_{CI}}^{(L)}$ – число сконфигурированных кандидатов;

$M_{p,s,max}^{(L)} = M_{p,s,0}^{(L)}$ для любого CSS;

$M_{p,s,max}^{(L)} = max\left(M_{p,s,n_{CI}}^{(L)}\right)$ для USS;

n_{RNTI} – это C-RNTI.

Рассмотрим Алгоритм 1 для определения абонентскими станциями индексов CCE, которые требуется декодировать для кандидатов USS с разными уровнями агрегации.

Алгоритм 1: Определение абонентскими станциями индексов CCE, которые требуется декодировать для кандидатов USS с разными уровнями агрегации

Входные параметры: $A = [39827,39829,39839]$, $N_{CCE,p} = 11$, $n_{RNTI} = 100$, $D = 65537$, $i = 0$, $n_{CI} = 0$, $M_{p,s,max}^{(L)} = 4$.

Выход функции: матрица значений индексов для слотов, типов CORESET и кандидатов $CCEindex$;

For $p = 0;\ p \le 2$slot $\le$ workTime; $p++$slot$++$ // цикл по всем CORESET

| **For** $slot = 0;\ slot \le 9$slot $\le$ workTime; $slot++$slot$++$ // цикл по слотам кадра с 15кГц SCS

| | if $slot = 0$

| | | $Y_{p,slot} = \left(A_p \cdot n_{RNTI}\right) mod D$

| | else

| | | $Y_{p,slot} = \left(A_p \cdot Y_{p,slot-1}\right) mod D$

For $slot = 0;\ slot \le 9$slot $\le$ workTime; $slot++$slot$++$ // цикл по слотам кадра с 15кГц SCS

| **For** $m = 0;\ m \le M_{p,s,max}^{(L)}$slot $\le$ workTime; $m++$slot$++$ // цикл по индексам сконфигурированных абонентам

| // PDCCH-кандидатов с L-уровнем агрегации в s-пространстве p-го корсета

| | $$CCEindex_{slot,m} = L \cdot \left\{ \left(Y_{p,slot} + \frac{m_{s,n_{CI}} \cdot N_{CCE,p}}{L \cdot M_{p,s,max}^{(L)}} + n_{CI} \right) mod \; N_{CCE,p} / L \right\} + i$$

Возвращается матрица значений индексов для слотов, типов CORESET и кандидатов $CCEindex$

На рис. 4 продемонстрирован пример получившихся значений индексов кандидатов внутри отдельных слотов и для разных типов CORESET для $L = 2$.

CORESET#0

Слоты	0	1	2	3
0	0	2	4	8
1	6	8	0	4
2	6	8	0	4
3	4	6	8	2
4	4	6	8	2
5	2	4	6	0
6	6	8	0	4
7	0	2	4	8
8	2	4	6	0
9	0	2	4	8

CORESET#1

	0	1	2	3
0	0	2	4	8
1	4	6	8	2
2	6	8	0	4
3	8	0	2	6
4	2	4	6	0
5	0	2	4	8
6	8	0	2	6
7	4	6	8	2
8	6	8	0	4
9	8	0	2	6

CORESET#2

	0	1	2	3
0	0	2	4	8
1	0	2	4	8
2	2	4	6	0
3	4	6	8	2
4	6	8	0	4
5	6	8	0	4
6	0	2	4	8
7	6	8	0	4
8	8	0	2	6
9	2	4	6	0

Рис. 4. Пример вычисленных CCE-индексов для различных слотов и кандидатов в CORESET

Иными словами: абонент с C-RNTI = 100 в 0-м слоте COREST#0 (p = 1) будет считывать CCE с индексами 0 и 1 (L = 2); абонент с C-RNTI = 100 в 1-м слоте COREST#0 (p = 1) будет считывать CCE с индексами 2 и 3 (L = 2) и т.д. Таким образом, функция распределения ресурсов на базовой станции, зная C-RNTI абонентов, с помощью описанной выше хэш-функции легко определит, какие индексы CCE будут использовать для последующего декодирования терминалы в USS CORESET, и именно в эти CCE данная функция размещает соответствующие DCI. Также очевидно, что несколько абонентов могут сканировать одни и те же CCE-индексы, и чем меньше размер CORESET, тем выше данная вероятность.

5. Оценка эффективности использования частотно-временных ресурсов для 5G NR для различных конфигураций CORESET

Для оптимизации использования частотно-временного ресурса в 5G NR необходимо провести оценку эффективности использования каждой конфигурации CORESET в различных сценариях. Оценка может включать в себя различные метрики производительности, такие как пропускная способность, задержка, эффективность передачи данных и другие.

Для оценки эффективности использования частотно-временного ресурса при различных конфигурациях CORESET могут быть использованы методы моделирования или симуляции в различных сценариях использования сети 5G NR. Эти методы могут помочь определить оптимальную конфигурацию CORESET для достижения наилучшей производительности сети.

Имитационная модель для механизма распределения ресурсов радиоинтерфйеса в 5G NR и назначения каналов трафика PDCSH была выполнена в программной среде Mathcad 15 в соответствии с упрощенным алгоритмом, показанным на рис. 5.

Для имитационного моделирования были использованы следующие входные параметры:

- ширина полосы частот – 100 МГц;
- максимальное число ресурсных блоков – 273 PRB;
- разнос между поднесущими – 30 кГц;
- максимальный размер CORESET – 273 ресурсных блока на 2 символа (91 CCE);
- тип трафика абонентов – мультисервисный;
- алгоритм планировщика – round robin;
- уровни агрегирования CCE – 1/2/4/8/16;

- доля CCE для назначения канала PDSCH (нисходящий канал) – 2/3;
- максимальное число абонентов – 50.

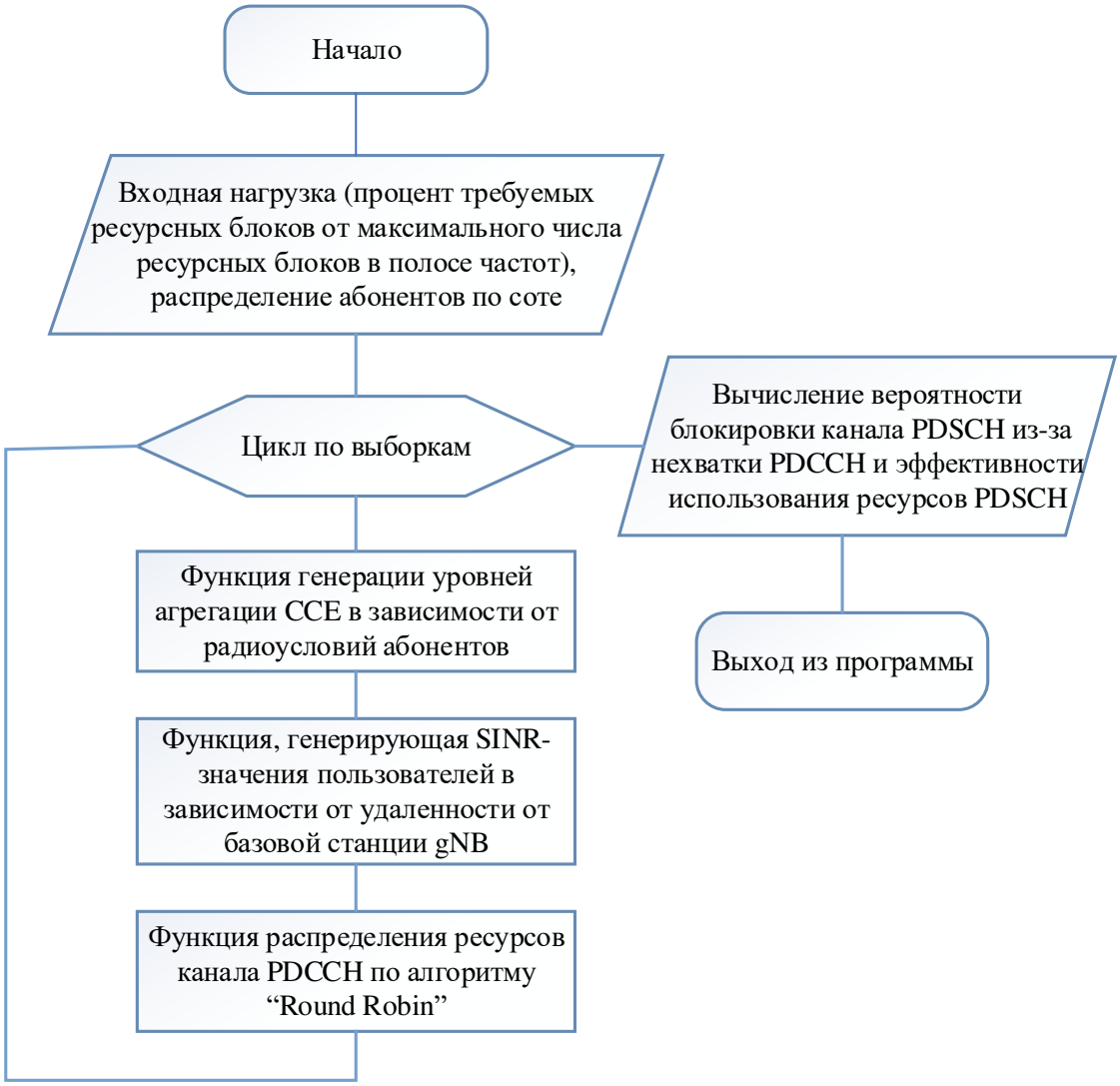

Рис. 5. Функциональная блок-схема алгоритма моделирования характеристик радиоинтерфейса NR

Иными словами: абонент с C-RNTI = 100 в 0-м слоте COREST#0 (p = 1) будет считывать CCE с индексами 0 и 1 (L = 2); абонент с C-RNTI = 100 в 1-м слоте COREST#0 (p = 1) будет считывать CCE с индексами 2 и 3 (L = 2).

В ходе имитационного моделирования были получены зависимости вероятности блокировки канала трафика, вызванной отсутствием свободных CCE (рис. 6а) и коэффициента эффективности использования частотно-временных ресурсов при передаче данных или КПД использования частотно-временного ресурса канала PDSCH (рис. 6б) от интенсивности входной нагрузки при различных возможных значениях уровня агрегирования каналов управления (1, 2, 4, 8, 16). Эффективность использования ресурсов радиоканала определяется как отношение числа использованных ресурсных блоков к общему количеству имеющихся блоков.

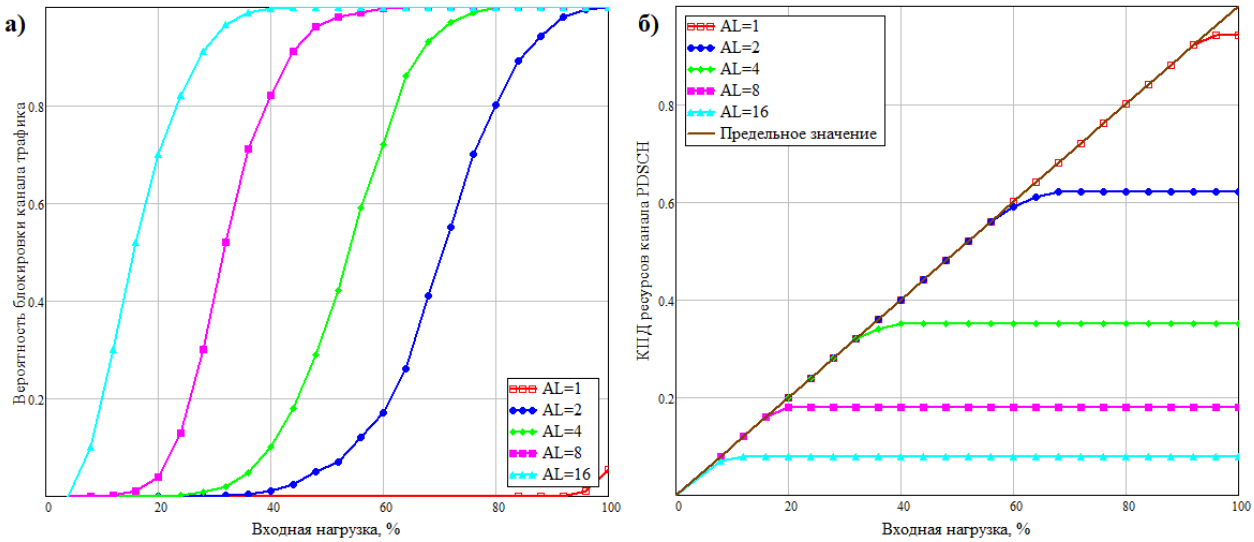

Рис. 6. Зависимости вероятности блокировки канала трафика (а)
и КПД использования ресурсов канала PDSCH (б) от процента входной нагрузки

Очевидно, что если все абоненты находятся в идеальных радиоусловиях (им достаточно всего одного элемента канала управления), то ресурсов канала управления PDCCH (размера сконфигурированного CORESET) достаточно для того, чтобы назначить всем пользователям транспортные блоки. Однако следует отметить, что максимальное число одновременно активных абонентов при имитационном моделировании равно 50 и количество запрашиваемых ими ресурсных блоков варьировалось от 1 до 150, в зависимости от типа трафика и требуемой скорости передачи данных. Увеличение числа абонентов приводит к росту вероятности блокировки канала трафика и снижению относительной пропускной способности сети или коэффициента эффективного использования радиоресурсов канала PDSCH, особенно с увеличением уровня агрегации CCE от 1 до 16.

Уровень агрегации CCE повышается в случае ухудшения радиоусловий пользователей. Радиоусловия при моделировании определялись как отношение SINR (Signal to Noise and Interference Ratio), зависящее от удаленности пользователей от базовых станций. Анализируя зависимости, можно отметить, насколько значительный эффект оказывает ухудшение радиоусловий (уровень агрегирования выше одного) на эффективность использования радиоресурсов (на рис. 6б – КПД) – это число блоков, назначаемых пользователям из всех имеющихся. Абоненты оказываются в ситуации, когда им не достаются каналы управления (высокая вероятность блокировки), что блокирует использование каналов PDSCH для передачи трафика на уровне 10–60 %, в зависимости от агрегации CCE.

Таким образом, оценка эффективности использования частотно-временного ресурса для различных конфигураций CORESET является важным шагом в оптимизации параметров сети 5G NR. Методы моделирования и симуляции могут помочь определить оптимальную конфигурацию CORESET для различных сценариев использования сети и максимизировать ее производительность.

Проведение сравнительного анализа результатов моделирования позволяет определить, какие из конфигураций CORESET обеспечивают наилучшую производительность и эффективность передачи данных при различных параметрах сети.

Для обеспечения оптимального использования частотно-временного ресурса в конкретных сценариях использования 5G NR необходимо определить оптимальные настройки CORESET. Оптимальные настройки CORESET зависят от множества факторов, таких как скорость передачи данных, тип данных (голосовые сообщения, интернет вещей и т.д.), количество устройств, которые используют сеть, и многих других.

Таким образом, определение оптимальных настроек CORESET для конкретных сценариев использования 5G NR является важным шагом для обеспечения максимальной производительности и эффективности передачи данных. Для достижения этой цели необходимо проведение экспериментов и моделирования в различных сценариях использования сети.

6. Заключение

В настоящей работе проведено исследование вопросов использования частотно-временных ресурсов NR путем изменения конфигурации CORESET, количества UE с DCI в одном слоте и оценка вероятности блокирования каналом PDCCH блоков канала PDSC для различных уровней агрегирования CCE и модели Full buffer.

Для определения оптимальной конфигурации CORESET и количества UE с DCI в одном слоте рекомендуется использовать следующие критерии: максимизация пропускной способности и минимизация вероятности блокировки каналом PDCCH ресурсов канала PDSCH.

Таким образом, оптимизация использования частотно-временных ресурсов NR путем изменения конфигурации CORESET, в частности адаптация AL для CCE, количества UE с DCI в одном слоте и оценка вероятности блокирования канала PDCCH является возможным способом улучшения эффективности использования ресурсов. Дальнейшие исследования могут быть проведены для проверки этих результатов на различных сценариях использования 5G NR.

Литература

1. *Rinaldi F., Raschellà A., Pizzi S.* 5G NR system design: a concise survey of key features and capabilities // Wireless Networks. 2021. P. 45.
2. 3GPP Specification series. URL: `https://www.3gpp.org/dynareport?code=38-series.htm`.
3. *Takeda K., Xu H., Kim T., Schober K., Lin X.* Understanding the Heart of the 5G Air Interface: An Overview of Physical Downlink Control Channel for 5G New Radio (NR) // IEEE Communications Standards Magazine. 2020. V. 4, Is. 3. P. 22.
4. *Volker B.* 5G NR Physical Downlink Control Channel: Design, Performance and Enhancements // Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2019. P. 1–6.
5. *Hamidi-Sepehr F.* 5G NR PDCCH: Design and Performance // IEEE 5G World Forum (5GWF), 2018. P. 250–255.
6. *Xingqin L.* 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology // IEEE Communications Standards Magazine. 2018. № 3. P. 30–37.
7. *Mozaffari M.* Blocking Probability Analysis for 5G New Radio (NR) Physical Downlink Control Channel // Proc. IEEE International Conference on Communications (ICC), 2020. P. 1–6.
8. *Zaidi A., Athley F., Medbo J., Gustavsson U., Durisi G., Chen X.* 5G Physical Layer: Principles, Models and Technology Components. 2018. P. 322.
9. TS 38.212 NR; Multiplexing and channel coding.
10. TS 38.331 NR; Radio Resource Control (RRC); Protocol specification.
11. TS 38.213 NR; Physical layer procedures for control.

Шелихова Татьяна Сергеевна
старший преподаватель кафедры телекоммуникационных систем и вычислительных средств, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 272, e-mail: tana696@mail.ru, ORCID ID: 0009-0005-0415-4933.

Дроздова Вера Геннадьевна
к.т.н., доцент, зав. кафедрой телекоммуникационных систем и вычислительных средств, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 272, e-mail: drozdova@sibguti.ru, ORCID ID: 0009-0002-0427-9929.

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.*

The Analysis of the Usage Efficiency of the Time-frequency Resources for Different 5G NR CORESET Configuration Settings

Tatiana S. Shelikhova, Vera G. Drozdova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The 5G mobile networks is a New Radio for finding wireless access solutions for Internet access of users with the most demanding requirements for quality service. To implement it radio interface resource allocation functions implemented by hardware and software vendors at base stations must notify subscribers about their decisions with so-called control channels the functions of which are distributed in the CORESET configuration area. The settings of the CORESET parameters affect the efficiency of using radio channel resources. This article discusses CORESET issues and their impact on the efficiency of using radio resources.

Keywords: 5G, NR, New Radio, PDCCH, CORESET.

For citation: Shelikhova T. S., Drozdova V. G. The analysis of the usage efficiency of the time-frequency resources for different 5G NR CORESET configuration settings (In Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 97-108. https://doi.org/10.55648/1998-6920-2023-17-4-97-108.

The article was submitted: 31.05.2023;
revised version: 14.07.2023;
accepted for publication 23.07.2023.

References

1. Rinaldi F., Raschellà A., Pizzi S. *5G NR system design: a concise survey of key features and capabilities*, Wireless Networks, 2021. p. 45.
2. 3GPP Specification series, available at: https://www.3gpp.org/dynareport?code=38-series.htm
3. Takeda K., Xu H., Kim T., Schober K., Lin X. Understanding the Heart of the 5G Air Interface: An Overview of Physical Downlink Control Channel for 5G New Radio (NR). *IEEE Communications*

Standards Magazine, vol. 4, iss. 3, September 2020, p. 22.
4. Volker B. 5G NR Physical Downlink Control Channel: Design, Performance and Enhancements. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1-6.
5. Hamidi-Sepehr F. 5G NR PDCCH: Design and Performance. *IEEE 5G World Forum (5GWF)*, 2018, pp. 250-255.
6. Xingqin L. 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology. *IEEE Communications Standards Magazine*, no. 3, 2018, pp. 30-37.
7. Mozaffari M. Blocking Probability Analysis for 5G New Radio (NR) Physical Downlink Control Channel. *ICC 2021 - IEEE International Conference on Communications*, 2020, pp.1-6.
8. Zaidi A., Athley F., Medbo J., Gustavsson U., Durisi G., Chen X. *5G Physical Layer: Principles, Models and Technology Components*, 2018. p. 322.
9. TS 38.212 NR; Multiplexing and channel coding.
10. TS 38.331 NR; Radio Resource Control (RRC); Protocol specification.
11. TS 38.213 NR; Physical layer procedures for control.

Tatiana S. Shelikhova

The lecturer of the Department of Telecommunication systems and computing, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 272, e-mail: tana696@mail.ru, ORCID ID: 0009-0005-0415-4933.

Vera G. Drozdova

Head of the Department of Telecommunication systems and computing, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 272, e-mail: drozdova@sibguti.ru, ORCID ID: 0009-0002-0427-9929.

DOI: 10.55648/1998-6920-2023-17-4-109-115 УДК 519.723

Кодирование сообщений, порождённых произвольным марковским источником, при неизвестной статистике сообщений *

В. К. Трофимов

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: Доказано существование универсального кодирования произвольного множества марковских источников, а также произведена оценка его эффективности в зависимости от ε-энтропии множества источников.

Ключевые слова: источник сообщений, универсальное кодирование, марковский источник, энтропия, стоимость кодирования, избыточность кодирования.

Для цитирования: Трофимов В. К. Кодирование сообщений, порождённых произвольным марковским источником, при неизвестной статистике сообщений // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 109–115. https://doi.org/10.55648/1998-6920-2023-17-4-109-115.

Статья поступила в редакцию 20.05.2023;
принята к публикации 25.07.2023.

1. Введение

Данная работа посвящена обобщению результатов автора [1] на произвольное множество марковских источников с конечной памятью и конечным алфавитом. В этой работе доказано существование универсального кодирования произвольного множества марковских источников в зависимости от его структуры. Дана оценка избыточности этого кодирования в зависимости от ε-энтропии множества источников. В качестве следствия получаются оценки для множества всех источников без памяти, полученных Р. Е. Кричевским [2], и для множества всех марковских источников, изученных Ю. М. Штарьковым [3] и автором [4].

2. Основные определения

Пусть буквы конечного алфавита $A=\{a_1, a_2, \ldots, a_k\}$, $2 \le k < \infty$, называемого в дальнейшем входным, порождаются марковским источником с памятью $0 \le s < \infty$. В этом случае источник θ однозначно определяется переходными вероятностями:

$$p(a_i a_\alpha) = \theta_{ai}, \text{ где } a_\alpha \in A^s,\ i = \overline{1,k}.$$

* Работа выполнена в рамках государственного задания № 071-03-2023-001 от 19.01.2023.

При $\alpha=(i_1,i_2,\ldots,i_s)$, $a_\alpha=a_{i1}a_{i2}\ldots a_{is}$, $a_\alpha\in A^s, t=\overline{1,s}$. Очевидно, всегда выполняется равенство $p(a_{\alpha1})+p(a_{\alpha2})+\ldots+p(a_{\alpha k})=1$, при любом $a_\alpha\in A^s$. Таким образом, каждый марковский источник с памятью s однозначно определяется набором (вектором) переходных вероятностей. Размерность этого вектора равна $k^s(k-1)$. Верно и обратное утверждение. Отсюда видно, что множество марковских источников с памятью s является единичным кубом размерности $k^s(k-1)$.

Множество всех слов A^n, взятых в алфавите A, назовем кодовым. Тогда произвольная полубесконечная последовательность букв входного алфавита, порождаемая источником, однозначно разбивается на последовательность слов $u\in A^n$. Число букв, входящих в произвольное слово u, будем обозначать $|u|$ и называть его длиной.

Произвольная полубесконечная последовательность букв входного алфавита, порождаемая источником θ, однозначно разбивается на последовательность слов длины n. Каждому слову $u\in A^n$ с помощью отображения φ поставим в соответствие слово $\varphi(u)$ в выходном алфавите B. Не умаляя общности, можно считать B – двоичным, т.е. $B=\{0,1\}$.

В работе рассматриваются только дешифруемые кодирования, т.е. множество слов в выходном алфавите $\varphi(A^n)=\{|\varphi(u)|, u\in A^n\}$ являются префиксными или, что то же самое, что для совокупности чисел $\{|\varphi(u)|, u\in A^n\}$ выполняется неравенство Крафта [5]. В этом случае существуют различные алгоритмы построения дешифруемых кодов. Мы не ставим задачи построить код, наша задача – оценить эффективность этих кодов.

Стоимостью кодирования φ при кодировании блоков длины n источником θ назовем величину $C(n,\theta,\varphi)$, которая определяется как среднее число букв выходного алфавита, приходящихся на одну входную [6], т.е.

$$C(n,\theta,\varphi)=\frac{1}{n}\sum_{|u|=n}P_\theta(u)|\varphi(u)|, \tag{1}$$

где $P_\theta(u)$ – вероятность порождения слова u источником θ.

Энтропию источника θ обозначим $H(\theta)$. В нашем случае:

$$H(\theta)=-\sum_{a_\alpha\in A^S}\theta_{o\alpha}\sum_{i=1}^{k}\theta_{\alpha i}\log\theta_{\alpha i}, \tag{2}$$

где $\theta_{o\alpha}$ – начальные стационарные вероятности для блоков a_α, $\theta_{\alpha i}$ – вероятность получения буквы a_i после блока a_α, $a_\alpha\in A^s$, $i=\overline{1,k}$.

Здесь и далее: $\log x=\log_2 x$.

Как показано в [6]:

$$H(\theta)=\lim_{n\to\infty}-\frac{1}{n}\sum_{|u|=n}P_\theta(u)\log P_\theta(u).$$

Избыточность кодирования $r(n,\theta,\varphi)$ определяется разностью между стоимостью кодирования $C(n,\theta,\varphi)$ и энтропией источника $H(\theta)$, определенных равенствами (1) и (2) соответственно. Таким образом, по определению

$$r(n,\theta,\varphi)=C(n,\theta,\varphi)-H(\theta). \tag{3}$$

Избыточностью универсального кодирования для множества источников Ω, $\Omega \subseteq \Omega_s$ при кодировании слов длины n назовём, как обычно [7], величину

$$R(n, \Omega) = inf_{\varphi}\, sup_{\theta \in \Omega} r(n, \theta, \varphi), \tag{4}$$

где Ω_s – множество всех марковских источников с памятью s. История поведения $R(n, \theta, \varphi)$ подробно рассмотрена в [8].

В настоящей работе получена оценка сверху для $R(n, \Omega)$. Доказано, что

$$R(n, \Omega) \le \frac{h_{1/\sqrt{n}}(\Omega)}{n} + \frac{\lambda}{n}. \tag{5}$$

Здесь и в дальнейшем $h_{\varepsilon}(\Omega)$ – ε-энтропия Ω, определяемая обычным образом [9], если принять во внимание, что источник θ определяется точкой в $k^s(k-1)$ единичном кубе. Расстояние между точками – обычное евклидово. Для конечного множества источников Ω при $\varepsilon \to 0$, очевидно, $H_{\varepsilon}(\Omega) = \log \Omega$, где Ω – число элементов в Ω.

3. Оценка избыточности универсального кодирования

Пусть Ω – произвольное подмножество источников из Ω s, и пусть для источников из Ω выполняются неравенства $\theta_{\alpha i} \ge \nu > 0$, $\alpha \in A^s$ $i = \overline{1,k}$. Пусть ε, $\varepsilon > 0$, сколько угодно малое. Построим ε-сеть для Ω. Элементы минимальной ε-сети обозначим $\Omega(\varepsilon)$. Тогда для каждого источника θ из Ω найдется по крайней мере один источник из $\Omega(\varepsilon)$, такой что

$$\tilde{\theta}_{\alpha i} - \theta_{\alpha i} = \Delta_{\alpha i},\ |\Delta_{\alpha i}| < \varepsilon,\ a_{\alpha} \in A^s,\ i = \overline{1, k}. \tag{6}$$

Докажем справедливость следующего утверждения.

Лемма. *Для произвольного множества источников Ω и произвольного ε, $\varepsilon < \min \theta_{\alpha i}$, $\theta \in \Omega$, существует ε-сеть $\Omega(\varepsilon)$, такая что для любого источника θ, $\theta \in \Omega$, найдется источник $\tilde{\theta}$, $\tilde{\theta} \in \Omega(\varepsilon)$, для которого справедливы неравенства:*

$$0 \le -\sum_{a_{\alpha} \in A^s} \theta_{o\alpha} \sum_{i=1}^{k} \theta_{\alpha i} (\log \tilde{\theta}_{\alpha i} - \log \theta_{\alpha i}) < \lambda \varepsilon^2, \tag{7}$$

где λ не зависит от θ.

Доказательство. Для доказательства (7) достаточно установить справедливость соотношений

$$0 \le -\sum_{i=1}^{k} \theta_{\alpha i} \log \tilde{\theta}_{\alpha i} + \sum_{i=1}^{k} \theta_{\alpha i} \log \theta_{\alpha i} \le \lambda \varepsilon^2,\ a_{\alpha} \in A^s. \tag{8}$$

Из равенств: $\theta_{\alpha 1} + \theta_{\alpha 2} + \ldots + \theta_{\alpha k} = 1$, $a_{\alpha} \in A^s$ и теоремы К. Шеннона для канала без шума [6] следует нижняя оценка в (8). Докажем справедливость верхней оценки. Как было отмечено выше, для любого источника из Ω найдется источник θ из $\Omega(\varepsilon)$, для которого выполнены условия (6). Соотношение (8) можно переписать в виде:

$$-\sum_{i=1}^{k} \theta_{\alpha i} \log \tilde{\theta}_{\alpha i} + \sum_{i=1}^{k} \theta_{\alpha i} \log \theta_{\alpha i} = -\sum_{i=1}^{k} \theta_{\alpha i} \log\left(1 + \frac{\Delta_{\alpha i}}{\theta_{\alpha i}}\right).$$

Воспользовавшись разложением в ряд функции $\log(1+x)$ из последнего неравенства, получаем:

$$-\sum_{i=1}^{k}\theta_{\alpha i}\log\tilde{\theta}_{\alpha i}+\sum_{i=1}^{k}\theta_{\alpha i}\log\theta_{\alpha i}\le\left[\sum_{i=1}^{k}\Delta_{\alpha i}+\frac{1}{2}\sum_{i=1}^{k}\frac{{\Delta_{\alpha i}}^2}{\theta_{\alpha i}}\right]\log e. \qquad (9)$$

Просуммировав общие части (7) по $i=\overline{1,k}$ и учитывая, что при любом α выполняются равенства $\sum_{i=1}^{k}\theta_{\alpha i}=\sum_{i=1}^{k}\tilde{\theta}_{\alpha i}=1$, окончательно получаем, что при любом α выполняется равенство $\sum_{i=1}^{k}\Delta_{\alpha i}=0$. Отсюда и из (9) вытекает справедливость верхней оценки в (8). Таким образом, утверждение леммы полностью доказано. □

Перейдем к оценке универсального кодирования произвольного множества марковских источников.

Теорема. *Для произвольного множества марковских источников* Ω, *у которых* $\delta<\min\theta_{\alpha i}$, $\theta\in\Omega$, $\varepsilon<\delta$, *для* $R\left(n,\Omega,(\delta)\right)$ *избыточности универсального кодирования множества источников* Ω *выполняется неравенство:*

$$R\left(n,\Omega(\delta)\right)\le\frac{\log\Omega(\varepsilon)}{n}+C_1\varepsilon^2+\frac{C_2}{n}.$$

Здесь C_1 *и* C_2 *не зависят от ε, ε – сколь угодно малое.*

Доказательство. Возьмем произвольное ε, $\varepsilon>0$, удовлетворяющее условию леммы, и построим минимальную ε-сеть $\Omega(\varepsilon)$. Элементы из множества $\Omega(\varepsilon)$ занумеруем произвольным образом: $\tilde{\theta}_1$, $\tilde{\theta}_2,\ldots,\tilde{\theta}_{\Omega(\varepsilon)}$. Рассмотрим кодирование φ_ε, которое каждому слову u, $u\in A^n$ ставит в соответствие слово $\varphi_\varepsilon(u)$ длины

$$\left|\varphi_\varepsilon(u)\right|=-\log([\sum_{i=1}^{\Omega(\varepsilon)}P_{\tilde{\theta}i}(u)]/\Omega(\varepsilon)). \qquad (10)$$

Существование дешифруемого кодирования φ_ε с длинами кодовых слов, удовлетворяющих равенствам (10), вытекает из выполнения неравенства Крафта [5] для чисел $\left|\varphi_\varepsilon(u)\right|$, $u\in A^n$. Оценим эффективность кодирования φ_ε. Из определения $r\left(n,\theta,\varphi_\varepsilon\right)$ избыточности кодирования φ_ε при заданном источнике θ и из (10) имеем:

$$r\left(n,\theta,\varphi_\varepsilon\right)=1/\left(n-\hat{s}+1\right)\sum_{u=n}P_\theta(u)\left|\varphi_\varepsilon(u)\right|-H(\theta)\le$$

$$\le-1/\left(n-\hat{s}+1\right)\sum_{u=n}P_\theta(u)\log\left(\left[\sum\nolimits_{i=1}^{\Omega(\varepsilon)}P_{\tilde{\theta}_i}(u)\right]/\Omega(\varepsilon)\right)-H(\theta)+1/\left(n-\hat{s}+1\right).$$

Предположим, что источник θ находится в ε-окрестности источника θ_{i_0}, $\theta_{i_0}\in\Omega(\varepsilon)$, тогда предыдущее неравенство можно переписать в виде:

$$r\left(n,\theta,\varphi_\varepsilon\right)\le\log\Omega(\varepsilon)/\left(n-\hat{s}+1\right)-H(\theta)-1/\left(n-\hat{s}+1\right)\sum_{u=n}P_\theta(u)\log P_{\theta_{i_0}}(u)+1/\left(n-\hat{s}+1\right)-$$

$$-1/\left(n-\hat{s}+1\right)\sum_{u=n}P_\theta(u)\log\left(1+\sum\nolimits_{i=1,i\ne i_0}^{\Omega(\varepsilon)}P_{\theta_i}(u)/P_{\theta_{i_0}}(u)\right). \qquad (11)$$

Так как $\sum_{i=1,\,i\ne i_0}^{\Omega(\varepsilon)}P_{\theta_i}(u)/P_{\theta_{i_0}}(u)\ge0$, то имеем неравенство

$$-\log\left(1+\sum\nolimits_{i=1,\,i\ne i_0}^{\Omega(\varepsilon)}P_{\theta_i}(u)/P_{\theta_{i_0}}(u)\right)\le0.$$

Поэтому из (11) и определения $H(\theta)$ получаем:

$$r(n,\theta,\varphi_\varepsilon)\le\frac{\log\Omega(\varepsilon)}{n-\hat{s}+1}+\frac{1}{n-\hat{s}+1}-\sum_{\alpha}\theta_{o\alpha}\sum_{i=1}^{k}\theta_{\alpha i}(\log\tilde{\theta}_{\alpha i}^{j}-\log\theta_{\alpha i}).$$

Воспользовавшись леммой из (11), имеем:

$$r(n,\theta,\varphi_\varepsilon)\le\frac{\log\Omega(\varepsilon)}{n-\hat{s}+1}+C\varepsilon^2+\frac{1}{n-\hat{s}+1}.$$

Отсюда и из определения $R(n,\Omega)$ вытекает справедливость утверждения теоремы. □

Из доказанной теоремы вытекает:

Следствие 1. *Для избыточности $r(n,\theta)$ универсального кодирования марковских источников справедливо неравенство:*

$$r(n,\theta,\varphi_\varepsilon)\le\frac{h_{1/\sqrt{n}}(\Omega)}{n}+\frac{C(\theta)}{n}.$$

Доказательство. Для фиксированного марковского источника существует δ, такое что $\theta_{\alpha i}>\delta>0$, $a\in A^s$, $i=\overline{1,k}$. Отсюда и из теоремы вытекает справедливость следствия при $\varepsilon=1/\sqrt{n}$. □

Следствие 2. *Для избыточности $R(n,\Omega(\delta))$ универсального кодирования произвольного множества марковских источников $\Omega(\delta)$, удовлетворяющих условию $\theta_{\alpha i}>\delta>0$, $a_\alpha\in A^s$, $i=\overline{1,k}$, выполняется неравенство, где λ не зависит от источника:*

$$R(n,\Omega(\delta))\le\frac{h_{1/\sqrt{n}}(\Omega(\delta))}{n}+\frac{\lambda}{n}.$$

Доказательство. Справедливость утверждения вытекает из теоремы и следствия 1 при $\varepsilon=1/\sqrt{n}$. □

4. Заключение

В настоящей работе было доказано существование универсального кодирования, зависящего от массивности множества марковских источников с конечной памятью. Получены оценки избыточности кодирования в зависимости от мощности множества. В частности, если источников конечное число, то избыточность убывает со скоростью $\frac{C}{n}$, если же кодируется всё множество источников, то избыточность убывает со скоростью $(k^s(k-1)\log n)/n$, а при $s=0$ получаем известный результат Кричевского.

Литература

1. *Трофимов В. К.* универсальное кодирование произвольного множества источников без памяти // Вестник СибГУТИ. 2018. № 4. С. 30–34.
2. *Кричевский Р. Е.* Длина блока, необходимая для получения заданной избыточности // Доклады АН СССР. 1965. Т. 171, № 1. С. 37–40.
3. *Штарьков Ю. М.* Кодирование сообщений конечной длины на выходе источника с неизвестной статистикой // Труды V конференции по теории кодирования и передачи информации, 1972. Кн. 1. С. 147–152.
4. *Трофимов В. К.* Избыточность универсального кодирования произвольных марковских источников // Проблемы передачи информации. 1974. Т. X, № 4. С. 16–24.

5. *Галлагер Р. Г.* Теория информации и надежная связь. М.: Советское радио, 1974. 719 с.
6. *Шеннон К.* Математическая теория связи. Работы по теории информации и кибернетике. 1963. С. 243–332.
7. *Кричевский Р. Е.* Связь между избыточностью кодирования и достоверностью сведений об источнике // Проблемы передачи информации. 1968. Т. 4, № 3. С. 48–57.
8. *Krichevsky R. E., Trofimov V. K.* The performance of universal encoding // IEEE Transactions on Information Theory. 1981. V. 27, № 2. P. 199–207.
9. *Витрушкин А. Г.* оценка сложности задачи табулирования. М.: Гос. изд. физ.-мат. лит. С. 195–228.

Трофимов Виктор Куприянович
доктор технических наук, профессор, профессор кафедры высшей математики СибГУТИ (630102, Новосибирск, ул.Кирова 86), e-mail: trofimov@sibguti.ru.

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

Encoding of Messages Generated by an Arbitrary Markov Source with Unknown Message Statistics

Viktor K. Trofimov

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The method of universal coding of an arbitrary set of Markov sources with finite memory is proposed. An estimation of the universal coding is obtained depending on the ε-entropy of the set of sources describing the massive of this set.

Keywords: coding, redundancy, Markov sources, entropy, storage and processing of information, the source of messages.

For citation: Trofimov V. K. Encoding of messages generated by an arbitrary Markov source with unknown message statistics (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 109-115. https://doi.org/10.55648/1998-6920-2023-17-4-109-115.

The article was submitted: 20.05.2023;
accepted for publication 25.07.2023.

References

1. Trofimov V. K. Universal'noe kodirovanie proizvol'nogo mnozhestva istochnikov bez pamyati [universal memoryless encoding of an arbitrary set of sources]. *Vestnik SibGUTI*, 2018, no.4, pp.30-34.
2. Krichevskii R. E. Dlina bloka, neobkhodimaya dlya polucheniya zadannoi izbytochnosti [Universal memoryless encoding of an arbitrary set of sources]. *Doklady akademii nauk SSSR*, 1965, vol.171, no. 1, pp.37-40.

3. Shtar'kov Yu. M. Kodirovanie soobshchenii konechnoi dliny na vykhode istochnika s neizvestnoi statistikoi [Encoding messages of finite length at the output of a source with unknown statistics]. *V konferentsiya po teorii kodirovaniya i peredachi informatsii*, 1972, Moscow, book 1, pp. 147-152.
4. Trofimov V. K. Izbytochnost' universal'nogo kodirovaniya proizvol'nykh markovskikh istochnikov [Redundancy of universal coding of arbitrary Markov sources]. *Problemy peredachi informatsii,* 1974, vol. X, no. 4, pp.16-24.
5. Gallager R. G. *Teoriya informatsii i nadezhnaya svyaz'* [Information Theory and Reliable Communication]. Moscow, Sovetskoe radio, 1974. p.719.
6. Shennon K. Matematicheskaya teoriya svyazi [Mathematical communication theory]. *Raboty po teorii informatsii i kibernetike*, 1963, Moscow, pp.243-332.
7. Krichevskii R. E. Svyaz' mezhdu izbytochnost'yu kodirovaniya i dostovernost'yu svedenii ob istochnike [The Relationship Between Coding Redundancy and Source Credibility]. *Problemy peredachi informatsii*, 1968, vol. 4, no. 3, pp.48-57.
8. Krichevsky R. E., Trofimov V. K. The performance of universal encoding. *IEEE Transactions On Information Theory*, 1981, v. 27, no. 2, pp.199-207.
9. Vitrushkin A. G. *Otsenka slozhnosti zadachi tabulirovaniya* [Otsenka slozhnosti zadachi tabulirovaniya]. Moscow, Fizmatlit, pp.195-228.

Trofimov Viktor Kupriyanovich

Dr. of Sci. (Engineering), Professor, Professor of the Department of Higher Mathematics, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), e-mail: trofimov@sibguti.ru.