

Метод оценки устойчивости информационного направления, функционирующего на ресурсах сети связи с отказами

С.А. Иванов¹*

¹Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация
*Адрес для переписки: sa-ivanov@inbox.ru

Информация о статье

Поступила в редакцию 19.10.2021

Поступила после рецензирования 14.11.2021

Принята к публикации 19.11.2021

Ссылка для цитирования: Иванов С.А. Метод оценки устойчивости информационного направления, функционирующего на ресурсах сети связи с отказами // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 85–94. DOI:10.31854/1813-324X-2021-7-4-85-94

Аннотация: В статье представлены основные направления качественной и количественной оценки устойчивости в области инфокоммуникаций, показаны различия в подходах к определению устойчивости. Предложен метод, отличающийся от известных обоснованным применением положений теории случайных импульсных потоков. Обобщенный импульсный поток описывает устойчивость передачи данных в информационном направлении. Метод оценки позволяет учитывать как состояния элементов составного канала, представленные импульсными потоками отказов и восстановлений, так и переходные процессы и подпроцессы информационного обмена (передачи по линии связи, коммутации, хранения в памяти, деструктивных воздействий и др.), представленные отдельными импульсными потоками. Вариативность состава импульсных потоков позволяет повышать точность и достоверность оценки.

Ключевые слова: устойчивость, информационное направление, сеть связи с отказами, импульсный поток.

Важным аспектом при эксплуатации инфокоммуникационных систем является обеспечение процессов передачи данных с требуемым качеством в обслуживаемых информационных направлениях. Элементы сетей связи, задействованные при построении маршрутов информационных направлений, могут быть подвержены внутренним и внешним деструктивным воздействиям непреднамеренного и преднамеренного характера. Наиболее емким интегральным свойством, отражающим реакцию системы на воздействие деструктивных факторов, является ее устойчивость. Обеспечение функционирования информационных направлений с заданными требованиями обуславливает необходимость поддержания показателей их устойчивости в заданном диапазоне значений, что требует достоверной оценки ее показателей.

Теория устойчивости в области инфотелекоммуникаций и ее количественной оценки развивается в ряде направлений, основными из которых являются: надежность и живучесть; структурная устойчивость; функциональная динамическая устойчивость.

К направлению надежности и живучести информационно-телекоммуникационных систем (ИТКС) относятся работы Б.Я. Дудника, В.Ф. Овчаренко [1], Б.П. Филина [2], Е.В. Гречишникова, А.С. Белова, А.В. Скубьева [3], К.А. Батенкова [4], В.Г. Иванова [5].

К направлению структурной устойчивости ИТКС относятся работы А.А. Привалова [6], Е.Е. Исакова [7], Ю.Ю. Громова [8], В.К. Попкова [9], J. Park [10], W. Jansen [11], N. Bartol [12].

К направлению функциональной динамической устойчивости ИТКС относятся работы Ю.И. Стародубцева [13], А.Н. Буренина, К.Е. Легкова [14], С.И. Макаренко [15, 16], М.А. Коцыняк, А.И. Осадчего [17], О.С. Лауты [17, 18], I. Linkov [10, 19, 20] P. Vocchini, [21], A. Ganin [20], D. Bodeau [22], И.В. Котенко, И.Б. Саенко [18], А.Е. Кучерявого [23].

Следует отметить, что в работах разных научных школ используются различные определения устойчивости, например:

– устойчивость как способность системы связи выполнять свои функции в условиях воздействия на ее элементы различных видов дестабилизирующих факторов [1, 2, 4–9, 14–16];

– устойчивость как состояние любых свойств системы, характеризующее вероятность нахождения их показателей в заданный период времени в пределах, обеспечивающих требуемый режим функционирования элементов системы и системы в целом [3, 13];

– устойчивость как способность системы планировать и подготавливаться к реагированию, компенсации и восстановлению после деструктивных воздействий и адаптироваться к новым условиям [10–12];

– устойчивость как способность предвидеть, продолжать действовать, корректно преодолевать трудности, восстанавливаться и развиваться с целью успешной адаптации к угрозам [22];

– оценка устойчивости основана на критических функциях и особенностях внешних воздействий на элементы сети [10, 19–21];

– рассматривается устойчивость с акцентом на информационно-технические воздействия [17, 18].

В части работ сохраняется подход, ориентированный на оценку и обеспечение устойчивости аналоговых сетей. В других работах разрабатываются методы и способы обеспечения киберустойчивости без учета, или с ограниченным учетом, ее взаимовлияний с другими свойствами. В третьей группе работ подходы к обеспечению устойчивости основаны на управлении другими свойствами, и, как правило, одним. Особенно необходимо отметить тот факт, что данные труды, опираясь на различные определения устойчивости в качестве основного ресурса сетей связи приняли пропускную способность линий связи.

Основные идеи методов и способов оценки устойчивости [1–25] базируются на классических теоремах сложения и умножения теории вероятностей, при этом вероятности функционирования элементов сети не учитывают распределение времени интервалов отказов во времени: значения коэффициентов готовности (исправного действия) принимаются на длительном временном интервале, исходя из надежных характеристик обслуживания, а внешние деструктивные воздействия учтены загруженными коэффициентами, исходя из эмпирических результатов, что снижает достоверность оценки. Кроме того, такая оценка не учитывает время, необходимое для переключения информационных направлений с одного маршрута на другой при неисправности первого.

Таким образом, существует задача разработки методического инструмента для решения класса задач по оценке устойчивости протекающих в инфокоммуникационных системах процессов, который позволит учитывать динамику деструктивных воздействий на сетевые элементы на протяжении интервалов любой продолжительности T , а также время δ , необходимое для переключения информационных направлений с одного маршрута на другой.

Результатом решения этой задачи стал метод оценки устойчивости информационного направления, представленный в статье. Данный метод основан на реализации положений теорий графов, случайных импульсных потоков, случайных процессов, комбинаторики, дифференциального и интегрального исчисления.

Постановка задачи

Пусть заданы:

– сеть связи (рисунок 1), описываемая графом G , состоящим из элементов k (узлов связи g и линий связи c);

– узлы подключения корреспондентов информационного направления I и требования к процессу передачи данных в нем (пропускной способности $C_{тр}$ и времени передачи $t_{тр}$);

– поток воздействий на каждый k -й элемент сети связи, описываемый плотностью вероятности пауз между импульсами воздействий $\omega_k(u)$;

– подсистемы восстановления элементов сети, описываемые плотностью вероятности времени восстановления элементов $\omega_k(t_b)$.

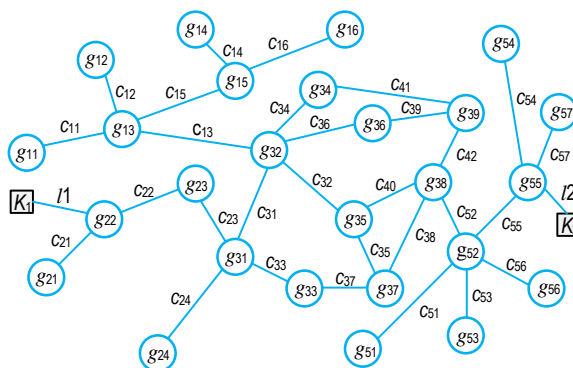


Рис. 1. Пример графа G сети связи, с подключенными посредством линий доступа $I1$ и $I2$, корреспонденты $K1$ и $K2$, между которыми сформировано информационное направление I_{12}

Fig. 1. An Example of a Graph G of a Communication Network with Connected Via Access Lines $I1$ and $I2$, Correspondents $K1$ and $K2$ between which an Information Direction is Formed I_{12}

Распределения $\omega_k(u)$ и $\omega_k(t_b)$ позволяют однозначно определить математическое ожидание соответствующих показателей и среднюю частоту потока отказов [26].

Для обеспечения функционирования информационного направления используются элементы сети, через которые могут проходить маршруты передачи данных (рисунок 2). На основе этих элементов формируется сеть информационного направления, описываемая графом G_I . На основе сети с графом G_I может быть построено M маршрутов, каждый из которых отличается хотя бы одним элементом. Каждый m -й маршрут формирует составной канал в информационном направлении I , включающий простые каналы (в данном случае понятия простой канал и линия связи c – тождественны), скоммутированные на узлах связи g (рисунок 3).

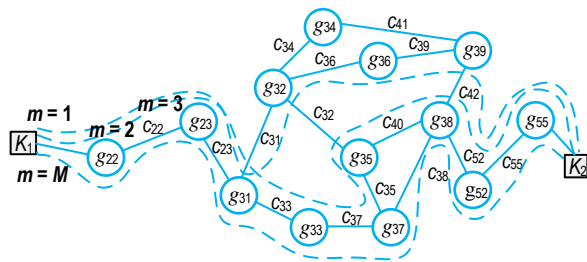


Рис. 2. Пример графа G_1 сети связи информационного направления I_{12}

Fig. 2. An Example of a Graph G_1 of a Communication Network of Information Direction I_{12}

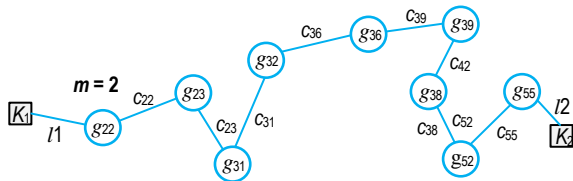


Рис. 3. Пример графа маршрута ($m = 2$) информационного направления I_{12}

Fig. 3. An Example of a Route Graph ($m = 2$) of Information Direction I_{12}

Цель метода: оценить вероятность функционирования информационного направления в сети связи с отказами описываемой графом G_I и образующей M маршрутов передачи данных в информационном направлении, для переключения между которыми необходимо время не более δ .

Суть метода заключается в поиске между корреспондентами информационного направления в любой момент времени хотя бы одного составного канала в сети, характеристики которого удовлетворяют требованиям информационного обмена, при этом интервалы работоспособности составных каналов должны пересекаться на время не меньше, чем необходимо для переключения потока данных между ними. Т. е. определяется, с какой вероятностью в случайный момент времени ζ будет существовать укороченный на δ временной интервал τ работоспособности хотя бы одного маршрута $P(\tau \geq \delta)$.

Обоснование применения теории случайных импульсных потоков

Примем *допущение* о том, что любой элемент сети связи в исправном состоянии удовлетворяет требованиям обмена данными в информационном направлении. Тогда процесс функционирования элемента с точки зрения обеспечения информационного обмена можно рассматривать в виде потока прямоугольных импульсов $X_k(t)$, который описывает элемент в двух состояниях $\xi_k \in \{0,1\}$. Значение $\xi_k = 0$ будем ставить в соответствие неработоспособному состоянию элемента в течение времени восстановления t_b , а значение $\xi_k = 1$ – работоспособному в течение времени его исправной работы τ .

В соответствии с принципами системного анализа и синтеза [27], подобные состояния $\xi_m \in \{0,1\}$ будут определять функционирование маршрутов информационного направления (их потоки прямоугольных импульсов $X_m(t)$), входящих в сеть информационного направления и самого информационного направления $\xi_I \in \{0,1\}$ (потока прямоугольных импульсов $X_I(t)$) (рисунок 4), где $\xi_I = 1$ соответствует состоянию, при котором требуемая для передачи данных в информационном направлении пропускная способность $C_{тр}$ не меньше пропускной способности динамического составного канала C .

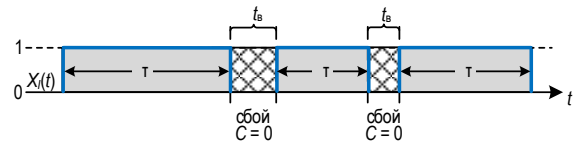


Рис. 4. Графическое отображение реализации процесса функционирования информационного направления I как случайного потока прямоугольных импульсов $X_I(t)$

Fig. 4. Graphic Display of the Implementation of the Process of Functioning of the Information Direction I as a Random Stream of Rectangular Pulses $X_I(t)$

Импульсный поток состояния элемента сети $X_k(t)$ *стационарен*: примем, что деструктивные воздействия на элементы сети связи носят случайный характер, т. е. вероятность отказа в случайно выбранном интервале $(\zeta, \zeta + \Delta t)$ не зависит от отказов на других интервалах.

Импульсный поток состояния элемента сети состоит из *взаимно неперекрывающихся* импульсов – элемент либо исправен, либо нет (отказ):

$$T_{zi} = t_{zi} - t_{zi-1} > \tau_i. \tag{1}$$

Импульсные потоки состояний элементов сети *независимы*: данное утверждение также основано на допущении о случайности деструктивных воздействий на элементы сети.

Импульсные потоки состояний маршрутов $X_m(t)$ информационного направления *независимы*: различные маршруты отличаются хотя бы одним элементом. Если формируемый импульсный поток маршрута отличается от потока другого маршрута хотя бы одним случайным составляющим потоком, то их импульсные потоки этих маршрутов *независимы*.

Представление процесса передачи данных в информационном направлении рядом *стационарных* и *независимых* импульсных потоков, каждый из которых удовлетворяет условию (1), дает основание для применения положений теории случайных импульсных потоков [28, 29].

Обобщенный показатель устойчивости информационного направления находится в условиях классической постановки теоремы о повторении опытов (схемы Бернулли) на общий случай [30].

Структура метода

Очевидно, что для выполнения требования к устойчивости P_y передачи с $t_{тр}$ данных в информационном направлении на интервале времени T должно выполняться условие:

$$P_{\xi_I=1} \geq P_y. \tag{2}$$

Вероятность $P_{\xi_I=1}$ в течение T будет определяться характеристиками элементов сети, на основе которых в множестве $\{M\}$ маршрутов формируются составные каналы в информационном направлении, характеристиками потоков воздействий на элементы сети, а также временем δ , необходимым для переключения информационного направления между маршрутами.

Отказ передачи данных в текущем маршруте информационного направления определяет необходимость переключения на другой, работоспособный маршрут. Сеть информационного направления с отказами, описываемая графом G_I , может функционировать с требуемой устойчивостью при условии наличия в любой момент интервала T работоспособного маршрута (составного канала) с вероятностью, удовлетворяющей условию (2). В результате переключения в I составных каналов по причине отказов в информационном направлении формируется *динамический составной канал*.

Метод оценки устойчивости информационного направления проводится в три этапа (рисунок 5).

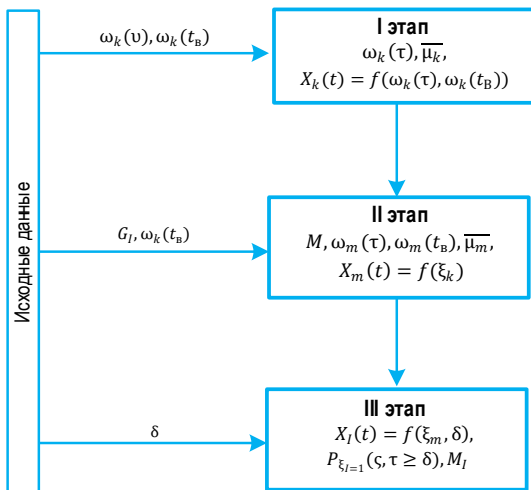


Рис. 5. Структура метода оценки устойчивости информационного направления

Fig. 5. Structure of the Stability Assessment Method Information Direction

На первом этапе оцениваются импульсные вероятностно-временные характеристики состояния $X_k(t) = f(\omega_k(\tau), \omega_k(t_B))$ всех элементов сети, описываемых графом G_I . На втором этапе оцениваются импульсные вероятностно-временные характеристики состояния $X_m(t) = f(\xi_k)$ каждого возможного маршрута (составного канала) информацион-

ного направления. Последовательность расположения элементов в маршруте предопределяет возможность существования импульса в потоке $\xi_m = 1$ только при существовании импульса в потоках каждого элемента составного канала $\xi_k = 1$. На третьем этапе оценивается импульсная вероятностно-временная характеристика состояния импульсного потока $X_I(t) = f(\xi_m, \delta)$, являющаяся обобщенной характеристикой его устойчивости.

Логическая параллельность функционирования маршрутов предопределяет возможность существования импульса в потоке информационного направления при существовании импульса хотя бы в одном (любом) потоке маршрутов $\forall \xi_m = 1$.

Описание метода

На **первом этапе** необходимо найти плотность вероятности длительности интервалов исправной работы (импульсов потока) элементов сети связи $\omega_k(\tau)$ и среднюю частоту следования интервалов исправной работы элементов сети связи $\overline{\mu}_k$. Имеющиеся характеристики элементов сети $\omega_k(v)$, $\omega_k(t_B)$, задействованных в обеспечении функционирования информационного направления, позволяют найти вышеуказанную плотность этих элементов.

Учитывая, что импульс воздействия входит в интервал неисправной работы элемента – времени его восстановления (рисунок 6), интервал его исправной работы можно найти из условия:

$$\tau = v - t_B. \tag{3}$$

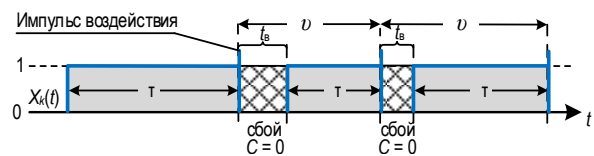


Рис. 6. Графическое отображение реализации процесса функционирования k-го элемента сети связи как случайного потока прямоугольных импульсов $X_k(t)$

Fig. 6. Graphic Display of the Implementation of the Process of Functioning of the k-th Element of the Communication Network as a Random Stream of Rectangular Pulses $X_k(t)$

С учетом независимости времени восстановления и интервалов между импульсами воздействия, нахождение закона распределения интервала исправной работы сводится к составлению композиции законов распределения v и t_B :

$$\begin{aligned} \omega_k(\tau) &= \int_0^{\infty} \omega_k(v) \omega_k(v - \tau) dv = \\ &= \int_0^{\infty} \omega_k(t_B) \omega_k(t_B + \tau) dv. \end{aligned} \tag{4}$$

Средняя частота следования интервалов исправной работы элементов сети находится по формуле:

$$\overline{\mu}_k = \frac{1}{\tau_k + t_{Bk}}, \tag{5}$$

где $\overline{\tau}_k$ и $\overline{t_{Bk}}$ – математическое ожидание интервала исправной работы и времени восстановления k -го элемента, соответственно, которые определяются выражениями [31]:

$$\overline{\tau}_k = \int_0^{\infty} \tau \cdot \omega_k(\tau) d\tau, \tag{6}$$

$$\overline{t_{Bk}} = \int_0^{\infty} t_B \cdot \omega_k(t_B) dt_B. \tag{7}$$

На **втором этапе** по установленному алгоритму (например, алгоритм поиска максимальных паросочетаний, алгоритм поиска кратчайших маршрутов [23, 32, 33]) и критериям определяются все возможные маршруты информационного направления, образующие соответствующие составные каналы передачи данных из K_m элементов сети. В предельном случае количество маршрутов соответствует всем возможным вариантам, отличающихся хотя бы одним элементом.

Каждый составной канал, в зависимости от комбинации простых каналов, имеет поток отказов (пауз, восстановлений) (рисунок 7), характеризующихся плотностью вероятности длительности интервалов исправной работы и восстановления.

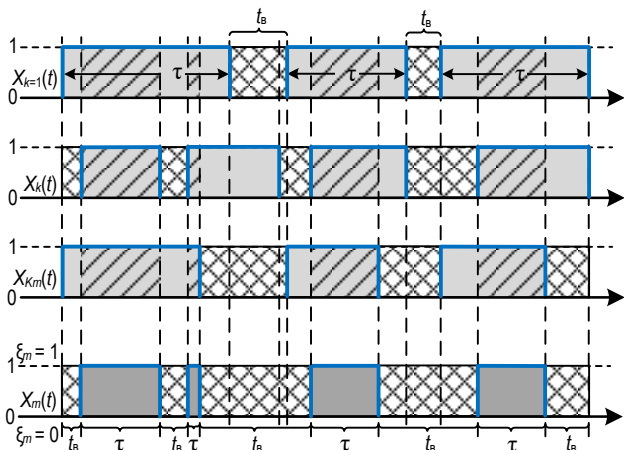


Рис. 7. Графическое отображение реализации процесса функционирования составного канала связи m -го маршрута как случайного потока прямоугольных импульсов $X_m(t)$, сформированного в результате последовательного объединения потоков прямоугольных импульсов элементов сети $X_k(t)$

Fig. 7. Graphic Display of the Implementation of the Process of Functioning of the Composite Communication Channel of the m -th Route as a Random Stream of Rectangular Impulses $X_m(t)$, Formed as a Result of Sequential Combination of Streams of Rectangular Pulses of Network Elements $X_k(t)$

На данном этапе необходимо для каждого маршрута найти, с какой вероятностью в случайный момент времени ζ будет существовать интервал его исправной работы – $P_m(\tau)$:

– плотность вероятности длительности интервалов исправной работы (импульсов потока) маршрутов информационного направления $\omega_m(\tau)$;

– плотность вероятности длительности времени восстановления (пауз потока) маршрутов информационного направления $\omega_m(t_B)$;

– среднюю частоту следования интервалов исправной работы маршрутов информационного направления $\overline{\mu}_m$.

Последовательность расположения элементов в маршруте предопределяет возможность существования импульса в его потоке только при существовании импульса в потоках каждого элемента составного канала.

В этом случае вероятность исправной работы маршрута будет определяться без учета δ выражением [28], которое по сути является формулой Бернулли, расширенной на общий случай решения задачи о повторении независимых испытаний [30]:

$$P_m(\tau) = P_{K_m, K_m}(\tau) = \frac{1}{K_m!} \frac{d^{K_m}}{d\lambda^{K_m}} \prod_{k=1}^{K_m} [Q_k(\tau) + \lambda \cdot P_k(\tau)]_{\lambda=0}, \tag{8}$$

где $P_k(\tau)$ и $Q_k(\tau)$ – вероятность существования и отсутствия импульса в потоке состояния k -го элемента сети, относящегося к m -му маршруту, которые находятся в соответствии с выражениями [28]:

$$P_k(\tau) = \overline{\mu}_k \int_0^{\infty} \tau \cdot \omega_k(\tau) d\tau, \tag{9}$$

$$Q_k(\tau) = \overline{\mu}_k \int_0^{\infty} t_B \cdot \omega_k(t_B) dt_B \tag{10}$$

и связаны между собой соотношением:

$$Q_k(\tau) = 1 - P_k(\tau). \tag{11}$$

Средняя частота следования импульсов совпадения маршрута определяется выражением [28]:

$$\overline{\mu}_m = \overline{\mu}_{K_m, K_m} = \frac{P_{K_m, K_m}(\tau)}{\tau_{K_m, K_m}}, \tag{12}$$

где τ_{K_m, K_m} определяется как:

$$\tau_{K_m, K_m} = \left(\sum_{k=1}^{K_m} \frac{1}{\tau_k} \right). \tag{13}$$

Распределение длительности интервалов исправной работы (импульсов потока) маршрутов определяется плотностью вероятности [28]:

$$\omega_m(\tau) = \omega_{K_m, K_m}(\tau) = \overline{\mu}_m \frac{d^2}{d\tau^2} P_m(\tau), \tag{14}$$

а распределение длительности времени восстановления (пауз потока) маршрутов (с учетом последовательной схемы подключения элементов) определяется плотностью вероятности [28]:

$$\omega_m(t_B) = \omega_{K_m, 1}(t_B) = \overline{\mu}_m \frac{d^2}{dt_B^2} P_m(t_B), \tag{15}$$

где

$$P_m(t_B) = P_{K_{m,1}}(t_B) = \frac{d}{d\lambda} \prod_{k=1}^{K_m} [P_k(\tau) + \lambda \cdot Q_k(\tau)]_{\lambda=0}. \quad (16)$$

Третий этап. Рассмотрим оценку устойчивости в трех вариантах функционирования динамического составного канала: при мгновенном переключении между составными каналами, удовлетворяющими требованиям информационного направления (ИН); при переключении между составными каналами, удовлетворяющими требованиям ИН с учетом переходных процессов в ходе переключения; при переключении между составными каналами, каждый из которых по отдельности не удовлетворяет требованиям ИН с учетом переходных процессов в ходе переключения.

Оценка устойчивости при мгновенном переключении между составными каналами, удовлетворяющими требованиям ИН

При параллельном соединении M составных каналов (маршрутов) в информационное направление наличие импульса хотя бы в одном (любом) канале $\xi_m = 1$ будет соответствовать наличию импульса $\xi_I = 1$ в потоке динамического составного канала информационного направления (рисунок 8а).

В этом случае вероятность существования импульса в потоке состояния ИН будет определяться выражением:

$$P_{\xi_I=1} = P_{M,1}(\tau) = \frac{d}{d\lambda} \prod_{m=1}^M [Q_m(\tau) + \lambda \cdot P_m(\tau)]_{\lambda=0} \omega_m(t_B) = \omega_{K_{m,1}}(t_B) = \overline{\mu}_m \frac{d^2}{d\tau^2} P_m(t_B), \quad (17)$$

где $P_m(\tau)$ и $Q_m(\tau)$ – вероятность существования и отсутствия импульса в потоке состояния m -го маршрута ИН, которые по аналогии с (9) и (10) находятся в соответствии с выражениями:

$$P_m(\tau) = \overline{\mu}_m \int_0^{\infty} \tau \cdot \omega_m(\tau) d\tau, \quad (18)$$

$$Q_m(\tau) = \overline{\mu}_m \int_0^{\infty} t_B \cdot \omega_m(t_B) dt_B. \quad (19)$$

Оценка устойчивости при переключении между составными каналами, удовлетворяющими требованиям ИН с учетом переходных процессов в ходе переключения

Переключение информационного направления между маршрутами сопровождается переходными процессами, занимающими время не менее некоторого значения δ . Для учета этих процессов при оценке устойчивости направления, необходимо укорачивать на величину δ импульсы совпадения потоков состояния составных каналов (рисунок 8б).

Тогда выражение (17) примет вид:

$$P_{\xi_I=1} = P_{M,1}(\delta) = \frac{d}{d\lambda} \prod_{m=1}^M [Q_m(\delta) + \lambda \cdot P_m(\delta)]_{\lambda=0}, \quad (20)$$

где $P_m(\delta)$ и $Q_m(\delta)$ – вероятность существования и отсутствия укороченного на δ импульса в потоке состояния m -го маршрута информационного направления, которые по аналогии с (9) и (10) находятся в соответствии с выражениями:

$$P_m(\delta) = \overline{\mu}_m \int_0^{\infty} (\tau - \delta) \cdot \omega_m(\tau) d\tau, \quad (21)$$

$$Q_m(\delta) = \overline{\mu}_m \int_0^{\infty} (t_B - \delta) \cdot \omega_m(t_B) dt_B. \quad (22)$$

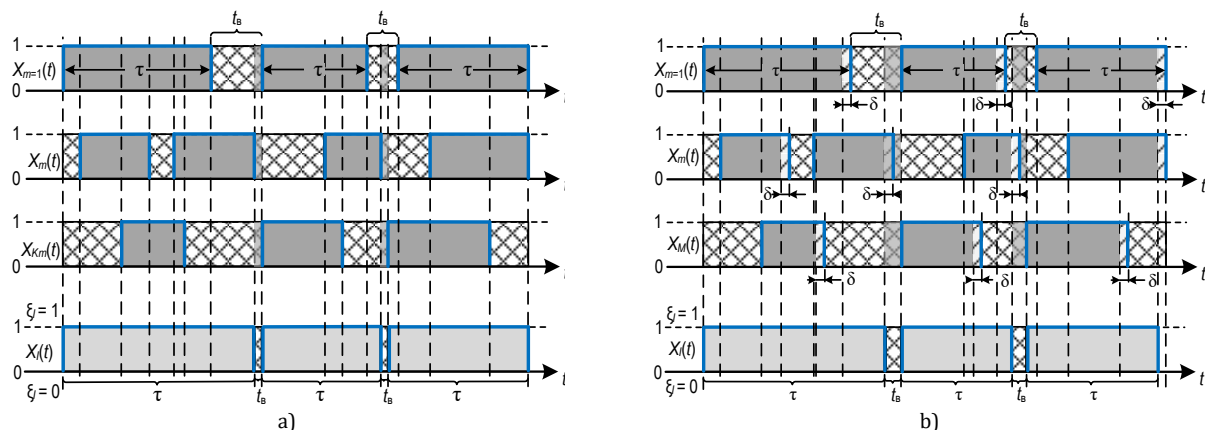


Рис. 8. Графическое отображение реализации функции состояний процесса передачи данных в информационном направлении $X_I(t)$, полученной в результате объединения параллельных потоков прямоугольных (полноразмерных) импульсов $X_m(t)$ (а) и импульсов, укороченных на δ (б), соответствующих состояниям процесса функционирования составных каналов M маршрутов

Fig. 8. Graphical Display of the Function's Implementation of the States of the Data Transfer Process in the Information Direction $X_I(t)$, Obtained as a Result of Combining Parallel Flows of Rectangular (Full-Size) Pulses $X_m(t)$ (a) and Pulses Shortened by δ (b), Corresponding to the States of the Process of Functioning of Composite Channels of M Routes

Оценка устойчивости при переключении между составными каналами, каждый из которых по отдельности не удовлетворяет требованиям ИН с учетом переходных процессов в ходе переключения

Представляя состояние составного канала m -го маршрута потоком импульсов $X_m(t)$ с амплитудой равной единице ($\xi_m = 1$), состояние ИН, включающего M маршрутов, можно представить суммой (рисунок 9):

$$X_I(t) = \sum_{m=1}^M X_m(t). \quad (23)$$

Тогда $X_I(t)$ может принимать целочисленные значения от 0 до M , что будет соответствовать событиям от полного отсутствия маршрута с заданными требованиями в информационном направлении до работоспособности любого из M маршрутов с заданными требованиями.

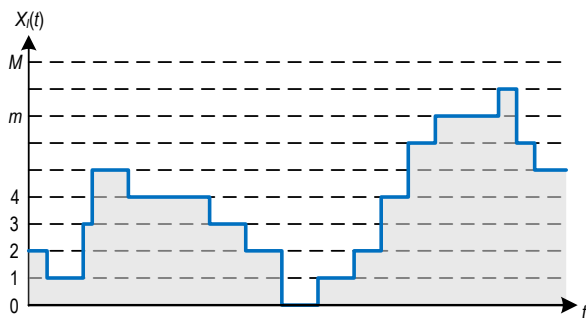


Рис. 9. Вариант функции $X_I(t)$ состояний процесса передачи данных в информационном направлении, включающем M маршрутов

Fig. 9. A Variant of the Function $X_I(t)$ of the States of the Data Transfer Process in the Information Direction, Including M Routes

По условиям задачи, для обеспечения функционирования ИН достаточно наличия импульса в любой момент времени в составном канале хотя бы в одного маршрута. При допущении того, что наличие импульса соответствует только части требуемой пропускной способности для передачи данных в ИН, необходимо оценить вероятность существования укороченного на δ импульса совпадения M_I маршрутов (рисунок 9):

$$M_I \geq \left\lceil \frac{C_{\text{тп}}}{C} \right\rceil, \quad (24)$$

где $M_I \in \mathbb{N}$.

Тогда выражение (17) примет вид:

$$P_{\xi_I=1} = P_{M, M_I}(\delta) = \frac{1}{M_I!} \frac{d^{M_I}}{d\lambda^{M_I}} \prod_{m=1}^M [Q_m(\delta) + \lambda \cdot P_m(\delta)]_{\lambda=0}. \quad (25)$$

Решение задачи обеспечения устойчивости обмена данных в ИН сводится к нахождению численными методами по выражению (25) необходимого количества маршрутов для выполнения условий (2) и (24).

Достоверность метода

По сравнению с традиционными методами, использующими средневзвешенную оценку (коэффициенты готовности и оперативной готовности), повышение достоверности и точности оценки устойчивости в разработанном методе обусловлено:

- учетом распределения времени отказов (состояния элемента по отношению к требованиям информационного обмена) каждого элемента сети на всем интервале оценки;
- учетом времени, необходимого для переключения между составными каналами различных маршрутов.

Кроме того, дополнительными импульсными потоками можно представлять задержки, вызываемые обработкой заголовков, очередями при отказах и перегрузках каналов, внешними и внутренними деструктивными воздействиями, линейным кодированием/декодированием и т. д. Такая возможность указывает на высокую чувствительность метода оценки устойчивости ИН к изменениям внутренних и внешних условий функционирования сети связи.

Достоверность представленного метода оценки подтверждается применением апробированных положений теорий графов, случайных импульсных потоков, случайных процессов, комбинаторики, дифференциального и интегрального исчисления.

Заключение

Метод оценки устойчивости направлен на определение в любой момент времени вероятности исправного функционирования ИН в зависимости от вероятностно-временных характеристик состояния элементов сети связи и характеристик подпроцессов информационного обмена.

Основным отличием метода от известных и его научной новизной является обоснованное применение положений теории случайных импульсных потоков, позволяющей совместно с традиционными методами, используемыми при оценке устойчивости, учитывать ключевые традиционные и дополнительные характеристики сети в условиях деструктивных воздействий.

Для повышения точности и достоверности оценки устойчивости метод позволяет представить подпроцессы информационного обмена (например, передачи по линии связи, коммутации, хранения в памяти) отдельными импульсными потоками. Представленный в статье результат учитывает время, необходимое для переключения составных каналов связи при управлении конфигурацией динамического составного канала ИН. Переключение составных каналов также можно представить отдельным импульсным потоком.

Вариативность состава импульсных потоков, включенных в общий поток, описывающий устойчивость передачи данных в ИН, позволяет повышать точность и достоверность оценки, масштабировать при этом перечень учитываемых показателей, выявлять пути повышения устойчивости информационного обмена.

Практическое применение представленного метода оценки требует дальнейшей проработки:

- порядка адаптации метода к внутренним и внешним условиям функционирования объекта оценки;
- порядка получения данных о внутренних параметрах сети связи;
- оптимизации периодичности контроля параметров сети связи;
- мониторинга состояния кабельной инфраструктуры в условиях внешних физических деструктивных воздействий.

Список используемых источников

1. Дудник Б.Я., Овчаренко В.Ф., Орлов В.К. и др. Надежность и живучесть систем связи. М.: Радио и связь, 1984. 216 с.
2. Филин Б.П. Методы анализа структурной надежности сетей связи. М.: Радио и связь, 1988. 208 с.
3. Гречишников Е.В., Белов А.С., Скубьев А.В. Способ обеспечения живучести сети связи в зоне обслуживания подвижных абонентов // Телекоммуникации. 2016. № 7. С. 13–18.
4. Батенков К.А. Устойчивость сетей связи: учебное пособие. Орел: Академия ФСО России, 2016. 278 с.
5. Иванов В.Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи. СПб.: СПбПУ, 2018. 214 с.
6. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб.: ВМА, 2000. 240 с.
7. Исаков Е.Е. Устойчивость военной связи в условиях информационного противоборства. СПб.: Изд-во Политехнического университета, 2009. 400 с.
8. Громов Ю.Ю., Драчев В.О., Набатов К.А., Иванова О.Г. Синтез и анализ живучести сетевых систем. М.: Изд-во Машиностроение-1, 2007. 152 с.
9. Попков В.К. Математические модели связности. Новосибирск: ИВМиМГ СО РАН, 2006. 490 с.
10. Park J., Seager T.P., Rao P.S.C., Convertino M., Linkov I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems // Risk Analysis. 2013. Vol. 33. Iss. 3. PP. 356–367. DOI:10.1111/j.1539-6924.2012.01885.x
11. Jansen W. Directions in Security Metrics Research. National Institute of Standards and Technology, 2009. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf> (дата обращения 23.11.2021)
12. Bartol N., Bates B., Goertzel K.M., Winograd T. Measuring Cyber Security and Information Assurance: A State-of-the-Art Report. Herndon: Information Assurance Technology Analysis Center, 2009.
13. Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации в интересах органов государственной власти и военного управления // Военная мысль. 2021. № 4. С. 39–49.
14. Буренин А.Н., Легков К.Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения управления. М.: Медиа паблишер, 2015. 348 с.
15. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. СПб.: Научное издание, 2020. 337 с.
16. Макаренко С.И. Усовершенствование функций маршрутизации и сигнализации протокола PNNI с целью повышения устойчивости сети связи // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 45–59. DOI:10.31854/1813-324X-2020-6-2-45-59
17. Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Лаута О.С., Деметьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2015. 126 с.
18. Kottenko I., Saenko I., Lauta O. Modeling the Impact of Cyber Attacks // In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Cham: Springer, 2019. PP. 135–169. DOI:10.1007/978-3-319-77492-3_7
19. Linkov I., Eisenberg D.A., Plourde K., Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems // Environment Systems & Decisions. 2012. Iss. 33. PP. 471–476. DOI:10.1007/s10669-013-9485-y
20. Ganin A.A., Massaro E., Gutfrain A., Steen N., Keisler J.M., Kott A., et al. Operational resilience: Concepts, design and analysis // Scientific Reports. 2016. Iss. 6. DOI:10.1038/srep19540
21. Bocchini P., Frangopol D.M., Ummenhofer T., Zinke T. Resilience and Sustainability of Civil Infrastructure: Toward a Unified Approach // Journal of Infrastructure Systems. 2014. Vol. 20. Iss. 2.
22. Bodeau D., Graubart R., Heinbockel W., Laderman E. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. Bedford: MITRE Corporation, 2015. URL: <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf> (дата обращения 23.11.2021)
23. Кучерявый А.Е., Махмуд О.А., Парамонов А.И. Метод маршрутизации трафика в сети Интернета Вещей на основе минимума вероятности коллизий // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 37–44. DOI:10.31854/1813-324X-2019-5-3-37-44
24. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. М.: Стандартинформ, 2009. 16 с.

25. Казаченко Ю.М., Патрина Н.С. Методическое обеспечение устойчивого функционирования сетей связи в условиях ЧС // Т-Сот: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 26–30.
26. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука, 2001. 295 с.
27. Попов А.А., Телушкин С.Н., Бушуев С.Н. Основы общей теории систем. Часть I. СПб.: ВАС, 1992. 248 с.
28. Седакин Н.М. Элементы теории случайных импульсных потоков. М.: Советское радио, 1965. 261 с.
29. Смагин В.А. Вероятностные модели сложных систем. СПб.: ВКА им. А.Ф. Можайского, 2004. 171 с.
30. Венцель Е.С. Теория вероятностей. М.: Государственное издание физико-математической литературы, 1962. 564 с.
31. Половко А.М., Гуров С.В. Основы теории надежности. СПб.: БХВ-Петербург, 2006. 704 с.
32. Харари Ф. Теория графов. Пер. с англ. М.: ЛЕНАНД, 2018. 304 с.
33. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2020. 1008 с.

* * *

Method for Assessing the Sustainability of the Information Direction, Functioning on the Resources of the Communication Network with Failures

S. Ivanov¹ 

¹Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-85-94

Received 19th October 2021

Revised 14th November 2021

Accepted 19th November 2021

For citation: Ivanov S. Method for Assessing the Sustainability of the Information Direction, Functioning on the Resources of the Communication Network with Failures. *Proc. of Telecom. Universities*. 2021;7(4):85–94. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-85-94

Abstract: *The article presents the main directions of the qualitative and quantitative assessment of sustainability in the field of infocommunications, shows the differences in approaches to the definition of sustainability. A method is proposed that differs from the known well-grounded application of the provisions of the theory of random impulse flows. The generalized impulse flow describes the robustness of data transmission in the information direction. The estimation method allows one to take into account both the states of the elements of a composite channel, represented by impulse flows of failures and restorations, and transient processes and sub-processes of information exchange (transmission over a communication line, switching, storage in memory, destructive influences, etc.), represented by separate impulse streams. The variability of the composition of the impulse streams makes it possible to increase the accuracy and reliability of the assessment.*

Keywords: *stability, information direction, communication network with failures, impulse flow.*


References

1. Dudnik B.Ya., Ovcharenko V.F., Orlov V.K., et al. *Reliability and Survivability of Communication Systems*. Moscow: Radio i sviaz Publ.; 1984. 216 p. (in Russ.)
2. Filin B.P. *Methods for Analyzing the Structural Reliability of Communication Networks*. Moscow: Radio i sviaz Publ.; 1988. 208 p. (in Russ.)
3. Grechishnikov E.V., Belov A.S., Skubyev A.V. Survivability Support Method of Telecommunication Network in Service Area of Mobile Users. *Telekommunikatsii (Telecommunications)*. 2016;7:13–18. (in Russ.)
4. Batenkov K.A. *Stability of Communication Networks*. Orel: Russian Federation Security Guard Service Federal Academy Publ.; 2016. 278 p. (in Russ.)
5. Ivanov V.G. *Model of the Technical Basis of a Special-Purpose Control System in a Single Information Space Based on the Converged Infrastructure of the Communication System*. St. Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2018. 214 p. (in Russ.)

6. Privalov A.A. *The Method of Topological Transformation of Stochastic Networks and its Use for the Analysis of Communication Systems of the Navy*. St. Petersburg: S. M. Kirov Military Medical Academy Publ.; 2000. 240 p. (in Russ.)
7. Isakov E.E. *Stability of Military Communications in the Context of Information Confrontation*. St. Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2009. 400 p. (in Russ.)
8. Gromov Yu.Yu., Drachev V.O., Nabatov K.A., Ivanova O.G. *Synthesis and Analysis of the Survivability of Network Systems*. Moscow: Mashinostroenie-1 Publ.; 2007. p. 152 (in Russ.)
9. Popkov V.K. *Mathematical Models of Connectivity*. Novosibirsk: Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences Publ.; 2006. 490 p. (in Russ.)
10. Park J., Seager T.P., Rao P.S.C., Convertino M., Linkov I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*. 2013;33(3):356–367. DOI:10.1111/j.1539-6924.2012.01885.x
11. Jansen W. *Directions in Security Metrics Research*. National Institute of Standards and Technology; 2009. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf> [Accessed 23rd November 2021]
12. Bartol N., Bates B., Goertzel K.M., Winograd T. *Measuring Cyber Security and Information Assurance: A State-of-the-Art Report*. Herndon: Information Assurance Technology Analysis Center; 2009.
13. Starodubtsev Y., Ivanov S., Zakalkin P. Conceptual Trends in Solving the Issue of Stability for the Uniform Network of Electrocommunications in the Russian Federation. *Voennaya mysl*. 2021;4:39–49. (in Russ.)
14. Burenin A.N., Legkov K.E. *Modern Infocommunication Systems and Special Purpose Networks. The Basics of Building Management*. Moscow: Media Publ.; 2015. 348 p. (in Russ.)
15. Makarenko S.I. *Communication System Models under the Conditions of Deliberate Destabilizing Influences and Reconnaissance*. St. Petersburg: Naukoemkie tekhnologii Publ.; 2020. 337 p. (in Russ.)
16. Makarenko S. Improved Routing and Signaling Functions of PNNI Protocol for High Network Stability. *Proc. of Telecom. Universities*. 2020;6(2):45–59. (in Russ.) DOI:10.31854/1813-324X-2020-6-2-45-59
17. Kotsynyak M.A., Osadchiy A.I., Kotsynyak M.M., Lauta O.S., Dementyev V.E., Vasyukov D.Yu. Ensuring the Stability of Information and Telecommunication Systems in the Context of Information Confrontation. St. Petersburg: Central Research Institute of Communications Publ.; 2015. 126 p. (in Russ.)
18. Kotenko I., Saenko I., Lauta O. Modeling the Impact of Cyber Attacks. In: *Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks*. Cham: Springer; 2019. p.135–169. DOI:10.1007/978-3-319-77492-3_7
19. Linkov I., Eisenberg D.A., Plourde K., Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems. *Environment Systems & Decisions*. 2012;33:471–476. DOI:10.1007/s10669-013-9485-y
20. Ganin A.A., Massaro E., Gutfrain A., Steen N., Keisler J.M., Kott A., et al. Operational resilience: Concepts, design and analysis. *Scientific Reports*. 2016;6. DOI:10.1038/srep19540
21. Bocchini P., Frangopol D.M., Ummenhofer T., Zinke T. Resilience and Sustainability of Civil Infrastructure: Toward a Unified Approach. *Journal of Infrastructure Systems*. 2014;20(2).
22. Bodeau D., Graubart R., Heinbockel W., Laderman E. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. Bedford: MITRE Corporation; 2015. Available from: <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-up-date.pdf> [Accessed 23rd November 2021]
23. Koucheryavy A., Mahmood O.A., Paramonov A. Traffic Routing Method for the Internet of Things Based on the Minimum of Collisions Probability. *Proc. of Telecom. Universities*. 2019;5(3):37–44. (in Russ.) DOI:10.31854/1813-324X-2019-5-3-37-44
24. GOST P 53111-2008. *Stability of functioning of the public communications network. Requirements and check methods*. Moscow: Standartinform Publ.; 2009. 16 p. (in Russ.)
25. Kozachenko Yu.M., Patrina N.S. Methodological support of sustainable operation of communication networks in emergency situations. *T-Comm*. 2017;11(9):26–30. (in Russ.)
26. Vadzinsky R.N. *Probability Distributions Handbook*. St. Petersburg: Nauka Publ.; 2001. 295 p. (in Russ.)
27. Popov A.A., Telushkin S.N., Bushuev S.N. *Foundations of General Systems Theory. Part I*. St. Petersburg: Military Academy of Communications Publ.; 1992. 248 p. (in Russ.)
28. Sedyakin N.M. *Elements of the Theory of Random Impulse Flows*. Moscow: Sovetskoe radio Publ.; 1965. 261 p. (in Russ.)
29. Smagin V.A. *Probabilistic Models of Complex Systems*. St. Petersburg: Mozhaisky Military Space Academy Publ.; 2004. 171 p. (in Russ.)
30. Wenzel E.S. *Probability Theory*. Moscow: Gosudarstvennoe izdanie fiziko-matematicheskoi literatury Publ.; 1962. 564 p. (in Russ.)
31. Polovko A.M., Gurov S.V. *Fundamentals of the Theory of Reliability*. St. Petersburg: BKHV-Peterburg Publ.; 2006. 704 p. (in Russ.)
32. Harari F. *Graph Theory*. Translated from English. Moscow: LENAND Publ.; 2018. 304 p. (in Russ.)
33. Olifer V., Olifer N. *Computer Networks. Principles, Technologies, Protocols*. St. Petersburg: Piter Publ.; 2020. 1008 p. (in Russ.)

Сведения об авторе:

ИВАНОВ
Сергей Александрович

кандидат технических наук, докторант Военной академии связи имени Маршала Советского Союза С. М. Буденного, sa-ivanov@inbox.ru
 <https://orcid.org/0000-0002-0528-276X>