# Оценка функциональной (параметрической) полноты информационных рисков

А.С. Любухин

***Аннотация*—В данной статье представлено теоретическое исследование адаптации метода, основанного на критерии функциональной полноты, для применения его при проведении оценки информационных рисков. Рассмотрены теоретические положения метода определения функциональной полноты, предпосылки применения этого метода для оценки рисков, а также пример реализации данного механизма. Детализирован каждый из этапов алгоритма действий по ранжированию информационных рисков посредством построения матриц и анализа их содержания. Также описан процесс формирования входных данных и способы их получения экспертной группой. Описанный способ является одним из вариантов концепции оценки информационных рисков. Исследование проводится в рамках проекта «Методика оценки информационных рисков при проведении аудита безопасности объектов критической инфраструктуры», реализуемого за счет гранта МТУСИ.**

***Ключевые слова*—информационный риск, оценка рисков, метод оценки рисков, критерий функциональной полноты, функциональная полнота риска, ранжирование рисков, нечеткая логика, угрозы информационной безопасности, параметры угроз безопасности, входные данные.**

## I. Введение

Вопрос оценки информационных рисков является ключевым в цикле управления рисками. Многообразие и растущее количество рисков информационной безопасности обусловливает необходимость гибкого инструментария вычисления информационных рисков и их сравнения для построения эффективной системы защиты от них с учетом их характеристик. Риск рассматривается в основном с точки зрения вероятности возникновения его на практике. Однако информационный риск имеет ряд характеристик, которые влияют на его опасность для информационной системы.

Предлагаемый адаптируемый метод является одним из этапов комбинированной методики оценки информационных рисков при проведении аудита безопасности объектов критической инфраструктуры, поскольку для получения входных данных для анализа необходимо осуществить ряд последовательных итераций с целью формализации сведений об угрозах информационной безопасности, как структурной единицы информационного риска, которая определяет его направленность и опасность для критически важных объектов.

В ходе данного теоретического исследования предстоит доказать возможность адаптации критерия функциональной полноты для оценки информационных рисков с приведением основных доводов и рассмотрением практического примера. Для достижения этой цели необходимо проанализировать теоретические положения о функциональной полноте, сформулировать определение функциональной полноты информационного риска, определить соответствие переменных теории функциональной полноты и параметров информационных рисков.

Статья получена 22 июля 2024.

Автор Любухин Алексей Сергеевич, младший научный сотрудник Института развития технологий цифровой экономики РГЭУ (РИНХ)

## II. Критерий функциональной полноты и его ключевые особенности

### A. Алгоритм действий по вычислению функциональной полноты системы

Функционально полная система представляет собой систему булевых функций, суперпозицией которых может быть представлена любая булева функция, т.е. функционально полная система S булевых функций образует базис в логическом пространстве. В общем, общий алгоритм применения критерия функциональной полноты для выбора оптимальной сложной программной системы теоретически математическим языком можно описать следующим образом:

На первом этапе заполняется справочник систем и справочник функциональных операций. Далее формируется исходная таблица. Пусть $Z = \{Z_i\}$ (i = 1, 2, …, n) – множество тестовых систем; $R = \{r_i\}$ (j = 1, 2, …, m) – множество функциональных операций, которые может выполнять система. Исходная таблица – X, элементы которой определяются следующим образом:

$$x_{ij} = \begin{cases} 1, если\_\ f_j\_вып-ся\_\ S_i \\ 0, если\_\ f_j\_не\_вып-ся\_\ S_i, \end{cases}$$

.

Выделим системы $Z_i$ и $Z_k$ и введем следующие обозначения:

$P_{ik}^{(11)} = \{Z_i \cap Z_k\}$ – мощность пересечения множеств (число операций, выполняемых одновременно $Z_i$ и $Z_k$);

$P_{ik}^{(10)} = \{Z_i / Z_k\}$ – мощность разности множеств (число операций, выполняемых в $Z_i$ и невыполняемых в $Z_k$);

$P_{ik}^{(01)} = \{Z_k / Z_i\}$ – мощность разности множеств (число операций, выполняемых в $Z_k$ и невыполняемых в $Z_i$).

Построим следующие матрицы:

$S_{ik} = P_{ik}^{(01)} / (P_{ik}^{(11)} + P_{ik}^{(10)})$ – мера рассогласования систем;

$H_{ik} = P_{ik}^{(11)} / (P_{ik}^{(11)} + P_{ik}^{(10)})$ – степень поглощения системой $Z_k$ системы $Z_i$;

$G_{ik} = P_{ik}^{(11)} / (P_{ik}^{(11)} + P_{ik}^{(10)} + P_{ik}^{01})$ – мера подобия Жаккарда.

Преобразуем матрицы P, S, H, G в логические матрицы отношения поглощения (включения), элементы которых определяются следующим образом:

$$P_{ik}^{0} = \begin{cases} 1, если\_P_{ik}^{(01)} \le \varepsilon_p\_u\_i \ne k \\ 0, если\_P_{ik}^{(01)} > \varepsilon_p\_u\_i = k \end{cases}$$

$$S_{ik}^{0} = \begin{cases} 1, если\_S_{ik} \le \varepsilon_s\_u\_i \ne k \\ 0, если\_S_{ik} > \varepsilon_s\_u\_i = k \end{cases}$$

$$H_{ik}^{0} = \begin{cases} 1, если\_H_{ik} \ge \varepsilon_h\_u\_i = k \\ 0, если\_H_{ik} < \varepsilon_h\_u\_i \ne k \end{cases}$$

$$G_{ik}^{0} = \begin{cases} 1, если\_G_{ik} \ge \varepsilon_g\_u\_i = k \\ 0, если\_G_{ik} < \varepsilon_g\_u\_i \ne k \end{cases}$$

,

где $\varepsilon_p$, $\varepsilon_s$, $\varepsilon_h$, $\varepsilon_g$ – пороговые (граничные) значения для матриц P, S, H и G соответственно.

Для разных граничных значений по матрице $G^0$ строятся графы взаимосвязи между системами. Анализ графов позволяет определить группы систем, связанных между собой по выполняемым функциям. По рассчитанной матрице $P^0 + (P^0)^2$ определяется ранжирование тестовых систем по критерию функциональной полноты.

Следующим шагом в данном исследовании является включение в расчеты перечня обязательных функций в качестве абстрактной (условной) системы. Выполняются все необходимые расчеты. По ним видно, какие из систем наиболее полно соответствуют требованию по наличию обязательных функций (другие системы как не реализующие нужные пользователю функции могут быть исключены из дальнейшего рассмотрения).

На третьем этапе необходимо сформировать новую исходную матрицу и рассчитать по ней все матрицы. Далее по $P^{01}$ строится таблица, в которой перечисляются функции, не предусмотренные в обязательном перечне, но реализуемые какой-либо из систем. По $P^{10}$ строится аналогичная таблица, в которой перечисляются функции, предусмотренные обязательным набором и нереализуемые системами.

По матрице $G^0$ строятся графы, показывающие степень взаимосвязи между системами по выполняемым функциям. По матрице $P^0 + (P^0)^2$ определяется ранжирование выделенных систем.

Из построенных таблиц пользователь может выбрать одну или несколько заинтересовавших его функций и дополнить ими строку с обязательными функциями, после чего процедура повторяется.

Таким образом, данный алгоритм позволяет осуществить следующее:

- составить полный перечень функций, реализуемых рассмотренными системами;
- систематизировать сведения о составе и функциональной полноте существующих систем;
- количественно оценить степень соответствия той или иной системы требованиям пользователя к функциональной полноте;
- проранжировать системы по критерию функциональной полноты;
- на стадии предварительного анализа исключить из дальнейшего рассмотрения системы, в которых не реализуются нужные пользователю функции;
- сформировать группу систем, имеющих одинаковую функциональную полноту, сопоставить их цены и другие характеристики;
- расширить для потребителя-пользователя возможности оптимального выбора на рынке систем, предоставив перечень выполняемых каждой системой функций, а разработчику системы показать место его продукта среди существующих систем.

### *B. Сферы применения критерия функциональной полноты*

Наиболее распространенной сферой применения критерия функциональной полноты сравнительный анализ нескольких систем с различным набором характеристик и функций. Чаще всего такими системами выступают программные системы в виде совокупности элементов и функций, выполняемых системой. Такой характер применения данного метода объясняется тем, что на рынке программных систем производителями представлен довольно широкий спектр программ, и пользователям таких систем зачастую бывает трудно определиться с выбором в соответствии с задачами, которые ставит перед системой заказчик.

Анализом применения критерия функциональной полноты занимались такие исследователи как Г.Н. Хубаев, С.М. Щербаков и др. [1-7]. Данные исследования позволяют определить не только структуру и алгоритм вычисления функциональной полноты программных систем, но и основные особенности их применения, анализ которых позволяет предположить возможность применения данного способа для предметной области, в которой ранее метод не использовался.

Задача выбора оптимальной системы сообразно поставленной задаче характерна для различных сфер жизнедеятельности: медицинские, информационные, технические, биологические, экономические системы. В основе метода сравнения сложных систем по критерию функциональной полноты лежат математические знания из теории множеств, комбинаторики, матричного анализа, теории графов и математической логики. Алгоритм представляет собой расширение известного

метода оптимального выбора программных средств по критерию функциональной полноты.

## III. Предпосылки адаптации критерия функциональной полноты к оценке рисков

Функционально полной системой называется система, обладающая необходимым для выполнения задачи набором функций, параметров и характеристик, которые на языке математических операций являются функциями переменных, которые путем подстановки одной в другую представляют результирующую функцию (суперпозицию функций) в виде функционально полной программной системы.

Если в виде суперпозиции функций можно представить программную систему, где математическими функциями являются параметры и функции системы, то можно предположить, что аналогичным образом возможно представить и информационный риск. Информационный риск обладает набором параметров и характеристик, которые достаточно полноценно его описывают и позволяют достаточно объективно оценить, сравнив совокупность этих параметров для каждого риска. Информационные риски, как возможность воплощения угроз безопасности, на практике, напрямую зависят от характеристик угроз безопасности информации.

Для полноты и качества исследования вопроса оценки информационных рисков при помощи механизмов критерия функциональной полноты целесообразно будет ввести такое понятие как «функциональная полнота риска», которое позволит рассматривать риск с позиции информационной системы, а параметры рисков с позиции функций программной системы.

Функционально (параметрически) полным называют информационный риск как совокупность булевых функций, суперпозицией которых может быть представлена любая булева функция, образуя базис в логическом пространстве. В случае сопоставления параметра риска булевой функции возможно транспонировать физическое понимание полноты информационного риска в математическое представление в виде соответствия либо несоответствия заданному критерию.

Исходная матрица состоит только из 0 и 1, которые располагаются на пересечении строк с наименованием систем и столбцов с наименованием функции системы. Для оценки информационных рисков строки будут описывать не программные системы, а информационные риски, а столбцы – не функции, реализуемые программами, а параметры рисков.

Каждый из параметров информационных рисков при анализе можно представить в виде булевой функции по аналогии с процессом определения функциональной полноты системы. Соответствие заданному значению параметра риска, характеризующему значительный уровень опасности, можно обозначить единицей по аналогии с обозначением наличия определенной функции у программной системы, а не соответствие будет обозначаться в таком случае 0. Суперпозицией этих функций будет функция информационных рисков, в которой наиболее функционально (параметрически) полный риск будет считаться самым опасным для рассматриваемой информационной системы. Наличие механизма формализации и перевода в математический язык исходных данных является еще одной предпосылкой для использования критерия функциональной полноты в качестве метода оценки информационных рисков.

Формализация и масштабируемый гибкий математический аппарат сводит в минимуму участие специалистов по информационной безопасности на этом этапе анализа информационных рисков при проведении аудита безопасности, тем самым снижая степень субъективности получаемого результата.

Процесс оценки информационных рисков с точки зрения критичности и опасности их параметров довольно сложен, поскольку количество самих рисков (в зависимости от степени их детализации) и параметров рисков может быть большим аналогично большому количеству функциональных особенностей и характеристик сложных программных систем, анализируемых при помощи критерия функциональной полноты. Формализованный математический аппарат данного метода позволяет сравнивать большое количество программных систем с большим набором функций. Исходя из этого, можно утверждать, что автоматизация и упрощение оценки информационных рисков является одной из характеристик предлагаемого адаптируемого метода.

## IV. Особенности применения критерия функциональной полноты для оценки информационных рисков

Для описания механизма действия критерия функциональной полноты при оценке информационных рисков введем следующие обозначения для задания исходной матрицы X: $Z_i$ – информационный риск, $R_j$ – параметр информационного риска, $X_{ij}$ – значение параметра для конкретного риска. При этом значение 0 будет характеризовать низкий уровень значения конкретного параметра для конкретного риска, а 1 – уровень «средний» и выше, т.е. представляющий существенную опасность для системы. Более подробно процесс получения и формализации входных данных для данного примера исследован в отдельном материале, т.к. представляет собой последовательный процесс из нескольких взаимосвязанных итераций по анализу предметной области и переходу от примерных значений к формализованным численным параметрам.

Заполним матрицу исходными данными и получим таблицу следующего вида.

Таблица 1 – Исходная матрица X

| | $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ | $R_6$ |
|---|---|---|---|---|---|---|
| $Z_1$ | 0 | 1 | 0 | 1 | 1 | 0 |
| $Z_2$ | 0 | 1 | 1 | 1 | 0 | 1 |
| $Z_3$ | 0 | 1 | 1 | 1 | 1 | 1 |
| $Z_4$ | 1 | 1 | 1 | 1 | 1 | 0 |
| $Z_5$ | 1 | 1 | 0 | 0 | 0 | 1 |
| $Z_6$ | 1 | 0 | 1 | 0 | 1 | 1 |

Выделим риски $Z_i$ и $Z_k$ и введем следующие обозначения:

$P_{ik}^{(11)} = \{Z_i \cap Z_k\}$ – мощность пересечения множеств (число существенных параметров рисков, принадлежащих одновременно $Z_i$ и $Z_k$);

$P_{ik}^{(10)} = \{Z_i / Z_k\}$ – мощность разности множеств (число операций, выполняемых в $Z_i$ и невыполняемых в $Z_k$);

$P_{ik}^{(01)} = \{Z_k / Z_i\}$ – мощность разности множеств (число существенных параметров, принадлежащих риску $Z_k$ и не принадлежащих $Z_i$).

Построим матрицу поглощения рисков.

$H_{ik} = P_{ik}^{(11)} / (P_{ik}^{(11)} + P_{ik}^{(10)})$ – степень поглощения риском $Z_k$ риска $Z_i$ (Таблица 2);

Таблица 2 – Матрица поглощения H

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 0.666 | 1 | 1 | 0,333 | 0,333 |
| 2 | 0,5 | 1 | 1 | 0,75 | 0,5 | 0,5 |
| 3 | 0,6 | 0,8 | 1 | 0,8 | 0,4 | 0,6 |
| 4 | 0,6 | 0,6 | 0,8 | 1 | 0,4 | 0,6 |
| 5 | 0,333 | 0,666 | 0,666 | 0,666 | 1 | 0,666 |
| 6 | 0,25 | 0,5 | 0,75 | 0,5 | 0,5 | 1 |

Данная матрица описывает степень поглощения каждым информационным риском других рисков, т.е. степень превосходства одного риска над другим по совокупности значений параметров.

Далее построим матрицу подобия Жаккарда для информационных рисков, которая показывает степень сходства каждого из рисков с другими рисками, исходя из значений совокупности параметров рисков.

$G_{ik} = P_{ik}^{(11)} / (P_{ik}^{(11)} + P_{ik}^{(10)} + P_{ik}^{01})$ – мера подобия Жаккарда (Таблица 3).

Таблица 3 – Матрица подобия Жаккарда G

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 0,4 | 0,6 | 0,6 | 0,2 | 0,166 |
| 2 | 0,4 | 1 | 0,8 | 0,5 | 0,4 | 0,333 |
| 3 | 0,6 | 0,8 | 1 | 0,666 | 0,333 | 0,5 |
| 4 | 0,6 | 0,5 | 0,666 | 1 | 0,333 | 0,5 |
| 5 | 0,2 | 0,4 | 0,333 | 0,333 | 1 | 0,4 |
| 6 | 0,166 | 0,333 | 0,5 | 0,5 | 0,4 | 1 |

Преобразуем матрицы P, S, H, G в логические матрицы отношения поглощения (включения), элементы которых определяются следующим образом:

$$P_{ik}^0 = \begin{cases} 1, если\_P_{ik}^{(01)} \le \varepsilon_p\_u\_i \ne k \\ 0, если\_P_{ik}^{(01)} > \varepsilon_p\_u\_i = k \end{cases}$$

$$S_{ik}^0 = \begin{cases} 1, если\_S_{ik} \le \varepsilon_s\_u\_i \ne k \\ 0, если\_S_{ik} > \varepsilon_s\_u\_i = k \end{cases}$$

$$H_{ik}^0 = \begin{cases} 1, если\_H_{ik} \ge \varepsilon_h\_u\_i = k \\ 0, если\_H_{ik} < \varepsilon_h\_u\_i \ne k \end{cases}$$

$$G_{ik}^0 = \begin{cases} 1, если\_G_{ik} \ge \varepsilon_g\_u\_i = k \\ 0, если\_G_{ik} < \varepsilon_g\_u\_i \ne k \end{cases}$$

,

где $\varepsilon_p$, $\varepsilon_s$, $\varepsilon_h$, $\varepsilon_g$ – пороговые (граничные) значения для матриц P, S, H и G соответственно.

Матрицы $P_0$, $H_0$, $G_0$ представлены в таблицах 4-6.

Таблица 4 Матрица $P_0$

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 0 | 1 | 1 | 1 |
| 4 | 1 | 1 | 1 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 | 1 | 0 | 1 |
| 6 | 1 | 1 | 1 | 1 | 1 | 0 |

Таблица 5 Матрица $H_0$

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 2 | 0 | 0 | 1 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 | 1 | 0 | 0 |
| 4 | 0 | 0 | 1 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 1 | 1 | 0 | 0 |

Таблица 6 Матрица $G_0$

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |

Для разных граничных значений по матрице $G^0$ строятся графы взаимосвязи между рисками. Анализ графов позволяет определить группы рисков, связанных между собой по значениям их характеристик. По рассчитанной матрице $P^0 + (P^0)^2$ определяется ранжирование информационных рисков по критерию функциональной полноты.

Так, например, на основе данных матриц можно сделать выводы о степени поглощения рисками друг друга, т.е. о функциональном превосходстве и относительной полноте. Так, степень поглощения риска $Z_1$ риском $Z_2$ составляет 0, 666, а риски $Z_3$ и $Z_4$ полностью поглощают риск $Z_1$, т.к. степень поглощения равна 1.

Риски $Z_2$ $Z_3$ имеют самую высокую степень подобия между собой равную 0,8. Также риски $Z_1$ и $Z_3$ имеют значительную степень подобия, также как и риски $Z_1$ и $Z_4$ равную 0,6, т.е. более 50%. Рассмотрим граф подобия для построенной матрицы.

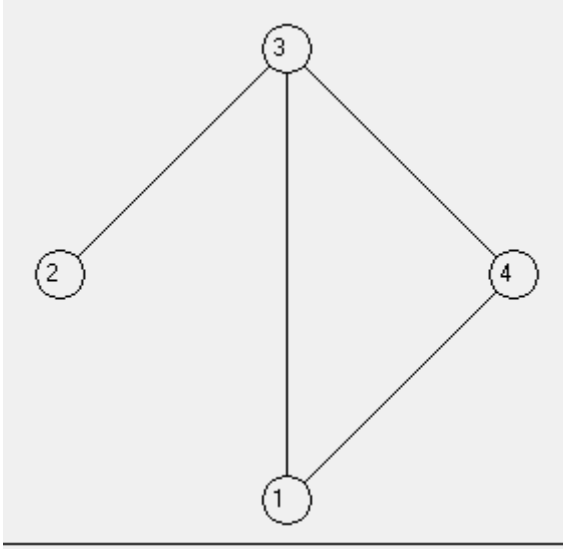


Рисунок 1 – Граф подобия информационных рисков при пороговом значении 0,6

Как видно из рисунка, на графе присутствуют риски $Z_1$, $Z_2$, $Z_3$ и $Z_4$. Т.е. риски, которые были обозначены ранее как риски, имеющие наибольшую степень подобия между собой. Т.е. на графе обозначаются риски, значение степени подобия которых превышает заданное значение. Вершины графа представляют собой сами информационные риски, а соединяются вершины прямыми с теми вершинами (рисками), которые имеют степень подобия с этим риском выше заданного порогового значения (как правило это значение более половины). Аналогичным образом строится и анализируется граф поглощения информационных рисков и выявляется наиболее опасный, а также следующие по уровню опасности информационные риски.

Построенные графы позволяют сделать вывод о комплексном характере применения данного способа, позволяющего оценивать опасность риска по совокупности показателей, а не по степени вероятности возникновения на практике, как это делается при реализации традиционных методов оценивания рисков.

Т.е., например, говоря о традиционных способах оценки рисков, например о методе нечетких лингвистических переменных [8], оценивается вероятность возникновения риска, и если вероятность высокая, то и риск соответствующий. Однако, возможна ситуация, при которой, несмотря на высокую вероятность возникновения риска, ценность активов, которые подвергаются опасности при реализации риска очень мала, а стоимость защиты системы от данного риска слишком высока, что при комплексном подходе дает возможность понять, что степень опасности и важности для системы защиты информации данного риска будет не столь высокой, как это было бы при традиционных методах оценки рисков. В данном случае, комплексный подход имеет преимущественное значение как при построении системы защиты информационной безопасности организации, так и при осуществлении оценки рисков [9]. Соответственно при потенциально малых потерях от воплощения риска и при существенных затратах на построение защитных барьеров от угроз данного риска считать этот риск опасным нецелесообразно, несмотря на вероятность его возникновения.

.

## V. Заключение

Таким образом, в ходе теоретического анализа вопроса адаптации и применимости для оценки информационных рисков критерия функциональной полноты, на практическом примере была продемонстрирована возможность этого не только в теории, но и на практике. Применимость механизмов критерия функциональной полноты для оценки информационных рисков позволяет оценивать информационные риски не с позиции вероятности их реализации на практике, а с позиции степени опасности для рассматриваемой информационной системы по значениям совокупности показателей (параметров) информационных рисков. Для формулирования данного вывода был проанализирован ряд научных публикаций, посвященных методам оценки рисков [10-12].

Реализация практического примера позволяет сделать следующие выводы о результатах применения адаптированного критерия функциональной полноты для оценки информационных рисков:

- данный алгоритм позволяет систематизировать сведения о характеристиках и функциональной полноте информационных рисков;
- метод дает возможность проранжировать информационные риски по критерию функциональной полноты;
- небольшое количество параметров риска, являющихся общими для всех рисков, весьма немногочисленно, что является недостатком при проведении оценки рисков ввиду отсутствия в системе сравнения ключевых параметров риска, которые являются индивидуальными для каждого риска, что способствует формированию информационно-методологической базы для дальнейшего исследования вопроса адаптации метода функциональной полноты для оценки рисков;
- выполнение последовательности математических и логических преобразований по данному методу позволяет сформировать группу информационных рисков, имеющих одинаковую функциональную полноту.

Наиболее важным и существенным преимуществом предложенного метода оценки информационных рисков является возможность анализа и сравнения информационных рисков не только с позиции вероятностных характеристик возможности воплощения риска на практике, а по совокупности параметров риска, определяющих его опасность для защищаемой информационной системы, что позволяет оценить ситуацию с потенциально возможными рисками не с одной позиции, а применив комплексный подход.

## Благодарности

Автор выражает благодарность научному

руководителю – к.т.н., доценту кафедры Информационной безопасности Ростовского государственного экономического университета (РИНХ) Серпенинову О.В. за методическую поддержку исследования проблемы.

## Библиография

[1] Хубаев Г.Н. Ранжирование объектов по множеству количественных показателей: универсальный алгоритм // РИСК: Ресурсы, информация, снабжение, конкуренция. – 2018. - №1. – с.213-217.

[2] Калиниченко В.И., Хубаев Г.Н., Калиниченко Д.В. Сравнительная оценка потребительского качества аудитов медицинских организаций по критерию функциональной полноты на основе чек-листов // Менеджмент качества в медицине. – 2021. - №1. – с.84-91.

[3] Хубаев Г.Н., Велько Н.Э. Сравнительный анализ функциональной полноты информационных систем для поиска и аренды жилья // Бюллетень науки и практики. – 2017. - №6 (19). – с. 153-158.

[4] Хубаев Г.Н., Широбокова С.Н., Журба А.К., Продан Е.А., Сушкова М.С. Сравнительный анализ функциональной полноты информационных систем управления учебным процессом // Роль науки в развитии общества: Сборник статей Международной научно-практической конференции. – Уфа: АЭТЭРНА, 2015. – с. 286-292.

[5] Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы (SOFTWARE&SYSTEMS), 1998, №2, с.6-9.

[6] Щербаков С.М. Метод анализа сложных систем по критерию функциональной полноты: расширение и адаптация // Системное управление. 2010. №2 (8). Режим доступа: http://sisupr.mrsu.ru/2010-2/pdf/scherbakov_1.pdf].– 0421000072/0027

[7] Хубаев Г.Н., Щербаков С.М., Аручиди Н.А. ПС анализа сложных систем по критерию функциональной полноты «Ireland» // Свидетельство об официальной регистрации программы для ЭВМ RUS №2009615296. М.: РОСПАТЕНТ, 2009.

[8] Любухин А.С. Методы анализа рисков информационной безопасности: нечеткая логика / Любухин А.С. // International Journal of Open Information Technologies. – 2023. – Т.11, №2. – с. 66-71.

[9] Любухин А.С. Основы комплексного подхода к анализу информационных рисков / Любухин А.С. // Наука и образование: отечественный и зарубежный опыт: сборник трудов Международной научно-практической конференции, Белгород, 21 декабря 2020 года. – Белгород: ООО ГиК, 2020. – с. 10-14.

[10] Куркина Елена Павловна, Шувалова Дарья Георгиевна Оценка риска: экспертный метод // Проблемы науки. 2017. №1 (14). Режим доступа: https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod

[11] Палютина Г.Н. Подход к адаптивной оценке рисков информационной безопасности объектов критической информационной инфраструктуры / Г.Н. Палютина // Угрозы и риски на Юге России в условиях геополитического кризиса. Достижения и перспективы научных исследований молодых ученых Юга России: Материалы научных мероприятий: Всероссийской конференции с международным участием; XIX Ежегодной молодежной научной конференции, Ростов-на-Дону, 15 марта – 29 2023 года. – Ростов-на-Дону: Федеральное государственное бюджетное учреждение науки «Федеральный исследовательский центр Южный научный центр Российской академии наук», 2023. – с.309

[12] Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. – Т.4, №1, 2019.

Любухин А.С. Родился в 1996 году в Ростовской области, Россия. Имеет квалификацию Бакалавр по специальности «Информационная безопасность», Магистр по специальности «Программная инженерия», «Исследователь. Преподаватель-исследователь» по специальности «Информационная безопасность». Основной областью исследования автора являются методики анализа информационных рисков при проведении аудита защищенности объектов критической информационной инфраструктуры. Любухин А.С. является победителем Всероссийского конкурса научных проектов аспирантов, соискателей и молодых ученых на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики (конкурс «Гранты ИБ»).

Научные публикации автора:

Любухин А.С. Методы анализа рисков информационной безопасности: нечеткая логика // International Journal of Open Information Technologies, Том 11, №2, 2023 г.

Любухин А.С. Моделирование процесса категорирования объектов критической информационной инфраструктуры // Информационная безопасность цифровой экономики (Россия, г. Улан-Удэ, Сибирский государственный университет телекоммуникаций и информатики, 2023 г.),

Любухин А.С. Основные тенденции и проблемы развития правового регулирования информационной безопасности РФ (на примере критической информационной инфраструктуры) // Молодежная инициатива 2023 (Россия, г. Ростов-на-Дону, Южно-Российский институт управления (филиал ФГБОУ ВПО Российская академия народного хозяйства и государственной службы при президенте Российской Федерации, 2023 г.)

Предыдущие исследовательские интересы автора: нормативно-правовое регулирование информационной безопасности, языки программирования, моделирование средствами языка UML, теория графовых грамматик.

Текущие исследовательские интересы: оценка информационных рисков, критерий функциональной полноты, категорирование объектов критической информационной инфраструктуры, риск-менеджмент, нормативно-правовое регулирование сферы КИИ, аудит защищенности.

# Assessment of the functional (parametric) completeness of information risks

A.S. Lyubukhin

*Abstract* - **This article presents a theoretical study of adapting a method based on the criterion of functional completeness for its application in assessing information risks. The theoretical principles of the method for determining functional completeness, the prerequisites for using this method for risk assessment, as well as an example of the implementation of this mechanism are considered. Each stage of the algorithm of actions for ranking information risks is detailed by constructing matrices and analyzing their content. The process of generating input data and methods for obtaining it by the expert group is also described. The described method is one of the variants of the concept of assessing information risks. The research is carried out within the framework of the project "Methodology for assessing information risks when conducting a security audit of critical infrastructure facilities," implemented through a grant from MTUCI.**

***Key words* — information risk, risk assessment, risk assessment method, criterion of functional completeness, functional completeness of risk, risk ranking, fuzzy logic, information security threats, security threat parameters, input data.**

## REFERENCES

[1] Khubaev G.N. Ranking of objects according to multiple quantitative indicators: a universal algorithm // RISK: Resources, information, supply, competition . – 2018. - No 1. – p.213-217.

[2] Kalinichenko V.I., Khubaev G.N., Kalinichenko D.V. Comparative assessment of consumer quality of audits of medical organizations according to the criterion of functional completeness based on checklists // Quality Management in Medicine. – 2021. - No 1. – p.84-91.

[3] Khubaev G.N., Velko N.E. Comparative analysis of the functional completeness of information systems for searching and renting housing // Bulletin of Science and Practice. – 2017. - No. 6 (19). - p. 153-158.

[4] Khubaev G.N., Shirobokova S.N., Zhurba A.K., Prodan E.A., Sushkova M.S. Comparative analysis of the functional completeness of information systems for managing the educational process // The role of science in the development of society: Collection of articles of the International Scientific and Practical Conference. – Ufa: AETERNA, 2015 . – p. 286-292.

[5] Khubaev G.N. Comparison of complex software systems according to the criterion of functional completeness // Software products and systems (SOFTWARE&SYSTEMS), 1998, No. 2, p.6-9.

[6] Shcherbakov S.M. Method of analysis of complex systems according to the criterion of functional completeness: expansion and adaptation // System management. 2010. No. 2 (8). Access mode: http://sisupr.mrsu.ru/2010-2/pdf/scherbakov_1.pdf].– 0421000072/0027

[7] Khubaev G.N., Shcherbakov S.M., Aruchidi N.A. PS for the analysis of complex systems according to the criterion of functional completeness "Ireland" // Certificate of official registration of the computer program RUS No. 2009615296. M.: ROSPATENT, 2009.

[8] Lyubukhin A.S. Methods for analyzing information security risks: fuzzy logic /Lyubukhin A.S. // International Journal of Open Information Technologies. – 2023. – T.11, No. 2 . – p. 66-71.

[9] Lyubukhin A.S. Fundamentals of an integrated approach to the analysis of information risks / Lyubukhin A.S. // Science and education: domestic and foreign experience: collection of proceedings of the International Scientific and Practical Conference, Belgorod, December 21, 2020. – Belgorod: LLC GiK, 2020 . – p. 10-14.

[10] Kurkina Elena Pavlovna, Shuvalova Daria Georgievna Risk assessment: expert method // Problems of science. 2017. No. 1 (14). Access mode: https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod

[11] Palyutina G.N. Approach to adaptive assessment of information security risks of critical information infrastructure facilities / G.N. Palyutina // Threats and risks in the South of Russia in the context of a geopolitical crisis. Achievements and prospects for scientific research of young scientists in the South of Russia: Proceedings of scientific events: All-Russian conference with international participation; XIX Annual youth scientific conference, Rostov-on-Don, March 15 - 29, 2023. - Rostov-on-Don: Federal State Budgetary Institution of Science "Federal Research Center Southern Scientific Center of the Russian Academy of Sciences", 2023 – p.309

[12] Maslova M.A. Analysis and determination of information security risks // Scientific result. Information technologies. - V.4, No.1, 2019.

**Lyubukhin A.S.** Born in 1996 in Rostov Oblast, Russia. Bachelor's degree in Information Security, Master's degree in Software Engineering, Researcher. Research Teacher in Information Security. The author's main area of research is methods for analyzing information risks when conducting an audit of the security of critical information infrastructure facilities. Lyubukhin A.S. is the winner of the All-Russian competition of scientific projects of postgraduate students, applicants and young scientists to conduct scientific research and development in the field of information security for the tasks of the digital economy (the "IS Grants" competition).

Scientific publications of the author:

Lyubukhin A.S. Methods of information security risk analysis: fuzzy logic // International Journal of Open Information Technologies, Vol. 11, No. 2, 2023

Lyubukhin A.S. Modeling the process of categorizing critical information infrastructure objects // Information security of the digital economy (Russia, Ulan-Ude, Siberian State University of Telecommunications and Informatics, 2023),

Lyubukhin A.S. Main trends and problems of development of legal regulation of information security of the Russian Federation (on the example of critical information infrastructure) // Youth Initiative 2023 (Russia, Rostov-on-Don, South-Russian Institute of Management (branch of the Russian Presidential Academy of National Economy and Public Administration, 2023)

The author's previous research interests: legal regulation of information security, programming languages, modeling using the UML language, graph grammar theory.

Current research interests: information risk assessment, functional completeness criterion, categorization of critical information infrastructure objects, risk management, legal regulation of the critical information infrastructure sphere, security audit.