КОМПЛЕКСНАЯ ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ. I: КРАТКИЙ ОБЗОР ПОДХОДОВ И МЕТОДОВ

Рей А. С.[1], Калашников А. О.[2]
(*ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, Москва*)

Сложные информационные системы (в частности, системы Интернета вещей) характеризуются различными видами неопределённости. Среди них можно выделить неопределённость значений отдельных факторов оценки состояния системы в целом, неопределённость взаимного влияния элементов системы друг на друга, а также неопределённости зависимости риска системы в целом от значений локальных рисков как характерные для этого класса систем. Существующие методы оценки информационных рисков сложных систем не учитывают перечисленные типы неопределённости одновременно. В то же время, поскольку именно неопределённость является причиной отклонения системы от целевого режима функционирования, необходимость учитывать хотя бы основные её виды при оценке рисков очевидна. Предлагаемая статья содержит краткий обзор существующих подходов к оценке рисков информационных систем, а также анализ возможности учета перечисленных выше видов неопределенности в рамках каждого из них. По итогам анализа в качестве перспективного был выбран метод комплексной оценки, изначально разработанный для механизма комплексного оценивания организационных систем и в последние годы все чаще использующийся для оценки рисков, в том числе в информационных системах.

Ключевые слова: сложные информационные системы, интегральный риск, комплексная оценка, учет неопределенности.

1. Введение

Постановка и решение задач управления рисками сложных информационных систем в целом предполагает, что предварительно получены обоснованные оценки трех основных факторов информационной безопасности (ИБ): целостности, конфиденциальности и доступности [23]. При этом, хотя сами эти факторы являются универсальными и применимы к любой информационной системе, предложить столь же универсальный алгоритм их

[1] *Анастасия Сергеевна Рей, м.н.с.* (*a.rey@ipu.ru*).
[2] *Андрей Олегович Калашников, д.т.н., г.н.с.* (*aokalash@ipu.ru*).

оценки затруднительно ввиду широкого разнообразия классов информационных систем с различной спецификой.

В случае, если управление интегральным риском информационной системы производится на основе её математической модели с использованием количественного подхода (обычно сводящегося к решению некоторой задачи оптимизации или игры в нормальной форме), алгоритм оценки факторов информационной безопасности должен удовлетворять нескольким базовым критериям, а именно:

A. включать все значимые факторы риска;

B. отражать связи и взаимозависимость факторов риска;

C. выходные значения должны быть представлены как минимум в порядковой шкале (предпочтительно в интервальной или в шкале отношений).

Как будет показано далее, качественные подходы оценки рисков сложных информационных систем доминируют над количественными. По мнению авторов, одной из главных причин этого является отсутствие требования построения модели защищаемой системы для целей оценки её рисков в действующих стандартах ИБ. Отметим, что в нормативной документации не закреплено правило агрегирования оценок трех основных факторов информационной безопасности. Иными словами, даже получив каким-либо образом численные значения, характеризующие риск информационной системы в части конфиденциальности, целостности и доступности обрабатываемых с её помощью данных, специалист по ИБ не может воспользоваться каким-либо стандартным методом для того чтобы охарактеризовать безопасность системы в целом.

Для решения этой проблемы в ранее опубликованной работе [11] был предложен вариант оценки интегрального информационного риска путем агрегирования оценок конфиденциальности, целостности и доступности методом комплексного оценивания (КО) [5]. Будучи разработанным для оценки состояния организационных систем с активными агентами, он изначально проектировался устойчивым к манипуляциям значениями отдельных критериев. Возможность построения различных структур дерева

свёртки позволяет в достаточной мере учесть взаимосвязь критериев, а хорошая сочетаемость с экспертными методами обеспечивает применимость в ситуациях, когда количественная оценка факторов риска затруднена или невозможна. Однако автор работы [11] не обсуждал способы получения оценок этих факторов по отдельности.

Вторым важным вопросом при оценке информационных рисков является учёт различных видов неопределённости. Хотя сбор объективных данных о состоянии информационных систем в силу их природы проще, чем, скажем, для социально-экономических систем, следует учитывать фактор быстрого устаревания накопленных данных из-за высокой степени изменчивости как самих рассматриваемых систем, так и их операционного окружения (которое тоже зачастую представляет собой информационную систему, но большего масштаба). По этой причине необходимость учёта неопределённости при оценивании рисков является объективной и обусловлена их спецификой.

В первой части настоящей работы приведена общая постановка задачи управления рисками сложных систем в условиях неопределенности, представлен краткий обзор существующих подходов и методов оценки информационных рисков, а также анализ возможности их модификации для учёта видов неопределённости, характерных для сложных информационных систем.

Во второй части работы авторы разовьют идею, лежащую в основе работы [11], и предложат алгоритм построения дерева комплексной оценки для получения значений рисков по основным факторам (ИБ): целостности, конфиденциальности и доступности в порядковой шкале. Обоснование выбора именно этого подхода представлено в первой части.

2. Формальная постановка задачи управления сложной системой

Пусть Q – множество состояний сложной системы; Θ – множество состояний внешней для системы среды; $\theta \in \Theta$ – наблюдаемое в данный момент состояние внешней среды; U – множество

наборов управляющих воздействий; $u \in U$ – применяемое воздействие; $q = q(u, \theta) \in Q$ – состояние системы, определенное применяемым воздействием и состоянием внешней среды.

Опишем зависимость целевой функции управления от состояния системы и состояния внешней среды функционалом $K = K(u, q, \theta) = K\big(q(u, \theta)\big)$. Тогда задача управления заключается в поиске таких оптимальных управляющих воздействий $u^* \in U$, что

(1) $K(u^*, q, \theta) = \max_{u \in U} K(u, q, \theta)$.

Предположим, что существует набор (u^*, q^*, θ^*), при котором целевая функция достигает максимально возможного значения:

(2) $K(u^*, q^*, \theta^*) = \max_{u \in U} \max_{q \in Q} \max_{\theta \in \Theta} K(u, q, \theta)$.

Введем функцию потерь, равную разности максимальных значений целевой функции и текущего состояния сложной системы:

(3) $\varphi(u, q, \theta) = K(u^*, q^*, \theta^*) - K(u, q, \theta)$.

Из (3) следует, что задача максимизации целевой функции эквивалентна задачи минимизации функции потерь, т.е. $K(u^*, q^*, \theta^*) - \max_{u \in U} K(u, q, \theta) = \min_{u \in U} \varphi(u, q, \theta)$.

Однако в сложных информационных системах полная информированность встречается редко. Чаще всего управляющая система встречается с неопределенностью, т.е. отсутствием полной или достоверной информации о состоянии управляемой системы.

Введем устраняющий неопределенность оператор $\mathfrak{I} = \mathfrak{I}K(u, \cdot, \cdot)$. Результат его применения к целевой функции зависит только от выбранного управления u. Тогда задачу поиска оптимального управляющего воздействия u^*, максимизирующего значение целевой функции в условиях неопределенности, можно представить следующим образом:

(4) $\mathfrak{I}(u^*) = \max_{u \in U} \mathfrak{I}(u)$.

Введем функцию риска

(5) $\rho(u) = \mathfrak{I}(u^*) - \mathfrak{I}(u)$,

где $\rho(u)$ – риск сложной системы, связанный с применением управляющего воздействия. Тогда задача минимизация риска записывается как

(6) $\rho(u^*) = \min_{u \in U} \rho(u)$,
и справедливо следующее:
(7) $u^* = \mathrm{Argmax}_{u \in U}\, \Im(u) = \mathrm{Argmim}_{u \in U}\, \rho(u)$.

Иными словами, задача управления сложной системой в условиях неопределенности и эквивалентна задачи минимизации риска.

Отметим, что для её решения необходимо вначале идентифицировать вид функции оценки интегрального риска и, в частности, снимающего неопределённость функционала. Далее в настоящей работе приведён краткий обзор существующих подходов и методов оценки информационных рисков и анализ их на предмет возможности комплексирования с методами учёта видов неопределенности, характерных для информационных систем.

3. Краткий обзор существующих подходов и методов оценки информационных рисков

В семействе стандартов ISO/IEC 27005 [23] риск определен как отклонение ожидаемого состояния системы от ее целевого состояния под воздействием неопределенности. Под неопределенностью при этом понимается то состояние, при котором присутствует недостаток информации о событии, в частности, отсутствие знаний о самом событии либо вероятности или последствий его наступления. Классификация рисков, в том числе и информационной безопасности, а также методология их оценки в общем виде представлены в стандартах, таких как [7, 8, 23, 24]. Предлагаемая в вышеперечисленных стандартах методология оценки рисков в основном сводится к оценке частоты возникновения угрозы и расчета величины ущерба для актива системы. Методы же оценки рисков делятся на количественные, качественные и комбинированные [23].

Исследований в области оценки рисков информационных систем в настоящий момент проводится достаточно много. Специалисты применяют различные подходы и методы с целью построения объективной (по возможности) их оценки. В этом смысле количественный подход является предпочтительным по сравнению с качественным [16], поэтому в последнее время ак-

тивно растет число работ, в которых предлагаются различные методы количественной оценки рисков. Среди последних следует выделить статистические методы [27], в том числе использующие стохастическое моделирование (например методом Монте-Карло). С целью решения последней задачи часто применяются аппарат нечеткой логики [12, 13], энтропийный подход [18], расчет риска с использованием открытого стандарта CVSS (Common Vulnerability Scoring System) [9]. Для построения количественных прогнозов обычно используют теоретико-графовый подход – методы теории графов и матричной записи [20].

Стоит отметить также и попытки учесть неопределенность, вызываемую взаимным влиянием элементов друг на друга. Так, в работе [10] рассматривался системный граф с передачей риска между элементами по его рёбрам в ходе импульсного процесса («Когнитивная игра» [14]). Было найдено условие, которому должна удовлетворять матрица собственных значений такого графа для того, чтобы импульсный процесс был сходящимся. В работе [32] рассматривается другая постановка, при которой сами риски между элементами не передаются, но значение локального риска зависит от положения элемента в системе. Получены точные или приближённые решения для простых структур типа «цепь» и «звезда».

Отметим, что получить релевантные количественные оценки сложнее, чем качественные. Так, довольно распространённым является вычисление значения риска на основе ретроспективных статистических данных, для применения которых необходимо обладать достаточно большим массивом исторических данных о защищаемой системе. Учитывая, что характерной особенностью информационных систем является их непрерывная адаптация под изменяющиеся задачи и операционное окружение, на практике накопленные ретроспективные данные могут оказаться нерелевантными для оценивания рисков. По этой причине для оценки информационных рисков широко применяются (и будут применяться в ближайшем будущем) качественные методы. Например, для построения качественного прогноза используют теоретико-графовые подходы, но связанные с построением деревьев отказов, защиты от атак и иных древовидных структур [22, 30, 31, 35]. К данной группе можно отнести и безмодельный

подход с использованием алгоритмов, основанных на анализе больших данных и машинном обучении [26, 29, 37]. А в работах [6, 25], авторы используют социотехнический подход при оценке рисков с учетом состояния окружающей среды и пользователей системы. С целью качественной объективизации экспертных оценок используется метод попарного сравнения [34] или статистические методы [15]. В работах [4, 28] применяется метод анализа иерархий с последующим агрегированием оценок отдельных факторов в виде взвешенной суммы, в работе [17, 19] применён сценарный подход с целью ранжирования серьезности последствий, а в работе [36] для этой же цели применён метод STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege – подмена, фальсификация, отказ от ответственности, раскрытие информации, отказ в обслуживании и повышение привилегий), в работе [33] предлагается ранжировать риски с помощью FMEA-анализа (анализ режимов отказов и последствий). В работе [21] используется метод анализа уровня блокады и защиты. Авторы выражают оценку рисков через уровни защищенности активов. Уровни защищенности рассчитываются в долях, а затем полученные значения переводятся в качественную шкалу, соответствующую уровню риска. Среди качественных методов стоит отметить и механизм КО [1, 2, 5], позволяющий агрегировать экспертные оценки с результатами объективных измерений (с редукцией в порядковую шкалу). В результате получается структура агрегирования в виде бинарного дерева, причём можно настраивать как порядок свёртывания критериев, так и сами матрицы свёртки.

В дополнение к основанию классификации, закреплённому в стандарте, авторы полагают целесообразным при рассмотрении методов оценки рисков определять, в какой степени тот или иной из них учитывает неопределённость. Последняя играет ключевую роль при построении оценок рисков ввиду того, что является причиной отклонения системы от целевого режима функционирования. При работе со сложными системами наиболее часто приходится иметь дело с неопределенностями следующих видов:

А. неопределённость значений отдельных факторов оценки состояния системы в целом;

B. неопределённость взаимного влияния элементов системы друг на друга;

C. неопределённость зависимости риска системы в целом от значений локальных (точечных) рисков.

Отметим, что даже если ограничиться одним классом сложных систем – информационными системами, методов оценки рисков для таких систем предлагается очень много. В связи с этим представляется разумным попытаться классифицировать предлагаемые методы и инструменты, с тем чтобы отыскать возможные пробелы в этом многообразии. Были проанализированы источники за 2019–2023 гг., направленные на разработку подходов по оценке рисков информационных систем. Результаты исследования сведены в таблицу 1.

Статистический подход. К статистическому подходу можно отнести стохастическое моделирование [27] и статистический метод объективизации экспертных оценок [15]. С помощью данного подхода можно учесть неопределенность вида A путем введения в оценку рисков параметров вероятности или влияния в виде диапазона значений, как в [27], или же посредством генерации дискретного распределения на основе взвешенных мнений экспертов [15].

Нечеткая математика. Подходы с применением нечеткой логики [12, 13] предполагают использование лингвистических переменных для формирования функции принадлежности на интервальном промежутке, что позволяет учитывать неопределенность вида A.

Энтропийный подход. Чаще всего энтропийный подход в задачах по оценке рисков используется с целью определения веса экспертной оценки. В работе [18] авторы используют энтропию Шеннона с целью преобразования нечетких мнений экспертов в числовые значения, тем самым учитывая, в некотором роде, неопределенность вида A.

Использование открытых стандартов. Еще одним подходом для оценки рисков является определение факторов риска в рамках системы оценки уязвимостей, заданной некоторым стандартом (открытый стандарт CVSS, стандарты семейств ISO 27005) [9, 23]. В стандартах неопределенность значения факторов предполагается, но в явном виде не учитывается. Тем не менее

в работах, где в алгоритмах с использованием иерархии рисков применяется открытый стандарт, например в [9], в некотором роде учитывается неопределенность вида С в случае, если локальные риски полагаются независимыми.

Теоретико-графовый подход. К данному подходу можно отнести методы теории графов [20], включая построение древовидных структур [22, 30, 31, 35]. В работе [20] матрица зависимости функционирования объектов системы позволяет строить оценки, учитывающие взаимное влияние элементов системы, т.е. учитывать неопределенность вида В. При построении древовидных структур (графов атак, отказов, защиты) узлы представляют собой или действия злоумышленников, или решения ЛПР. Элементы же системы в структуру дерева чаще всего не включены и рассматриваются в качестве своего рода «вспомогательных активов» и, следовательно, учет их взаимного влияния не происходит. Тем не менее, поскольку их значения учитываются при оценке интегрального риска системы (см., например, [31]), можно говорить о наличии в рамках подхода механизма учета неопределенности вида С.

«Когнитивная игра». Данный метод был специально разработан для формализованной оценки и управления рисками в сложных сетях в условиях, когда элементы системы влияют друг на друга и на интегральный риск [10, 14], что позволяет учитывать неопределенности вида В и С.

Безмодельный подход. К безмодельному подходу относятся методы машинного обучения [26, 29, 37], алгоритмы которых собирают и классифицируют большие массивы данных о состоянии системы, а также идентифицируют аномалии, сравнивая неизвестные значения параметров с параметрами, определенными раннее. Это позволяет отнести данные методы к тем, что учитывают неопределенность вида А. Однако учесть неопределенности видов В и С в рамках указанного подхода невозможно.

Социотехнический подход. К данному подходу, в первую очередь, относится метод профилирования [6, 25]. Несмотря на то, что авторы работают с неопределенным объектом, так как параметры злоумышленника не могут быть определены точно, они рассматривают исключительно детерминированные случаи, не учитывая неопределенности видов А, В и С.

Попарное сравнение. Метод попарного сравнения в большинстве случаев используется с целью объективизации оценок экспертов с дальнейшей их приоритезацией [34]. Параметры оценки рисков информационных систем основаны на точно-заданных весовых коэффициентах, определенных экспертами. Весовые значения критериев и их подкритериев попарно сравниваются без учета взаимного влияния элементов системы друг на друга. Механизмов учета неопределенности рассматриваемых видов метод не содержит.

Анализ иерархий. Подход представляет собой качественную оценку рисков и применяется для поддержки принятия решений на основе индексов важности множества критериев. Так, например, в работах [15, 28] оценки экспертов агрегируются в виде взвешенной суммы.

Сценарный подход. Метод сценарного анализа чаще всего используют для расчета риска возникновения сценария с последующим ранжированием в зависимости от тяжести последствий. Например, в работах [17, 19] рассматривают вероятностные рисковые ситуации и их воздействия на основе экспертного мнения. Параметры оценивания определяются в детерминированных шкалах. По задумке авторов, вероятность рассмотренных сценариев зависит от ключевых показателей эффективности, а именно, конфиденциальности, целостности, реальности, специальных возможностей, обслуживания, гибкости, безопасности. При этом возможное взаимное влияние этих показателей на риски других сценариев не учитывается. Риск каждого отдельно взятого сценария рассчитывается без учета структуры системы в целом. Таким образом, в сценарном подходе не учтен ни один из рассматриваемых в данной работе видов неопределенности.

Ранжирование. Помимо методов, встречающихся в сценарном подходе, для приоритезации факторов риска используют такие методы, как например, FMEA (анализ режимов отказов и последствий) [33] или STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege – подмена, фальсификация, отказ от ответственности, раскрытие информации, отказ в обслуживании и повышение привилегий) [36]. Данные методы включают в себя параметры оценки

локальных рисков сложных систем на основе точно-заданных весовых коэффициентов. Учет неопределенностей видов A, B, C в этих методах не производится.

Анализ уровня защиты и блокады. Данный подход представляет собой пример качественной оценки рисков активов и сценариев с помощью анализа уровня блокады и защиты (BDLA) [21] без дальнейшего агрегирования в интегральную оценку и учета рассмотренных в данной работе видов неопределенности.

Методы агрегирования должны применяться при переходе от оценки локальных рисков к интегральному. К основным методам можно отнести метод порогового агрегирования [3] и механизм комплексного оценивания [1, 2, 5]. Последний проектировался для использования при управлении организационными системами и потому разработан так, чтобы быть устойчивым к небольшим изменениям значений отдельных критериев. Таким образом, манипулируя структурой дерева и матриц свертки критериев, метод позволяет учесть зависимость интегрального риска от значений локальных рисков и тем самым учесть влияние неопределенности вида B и C.

Таблица 1. Учет неопределенности в методах и подходах оценки риска при оценке интегрального риска сложных систем

Группа методов	Основной метод	Возможность количественной оценки риска	Учет неопределенности вида:			Ссылки
			A	B	C	
Статистический подход	Стохастическое моделирование	Да	Да	Нет	Нет	[27]
	Объективизация экспертных оценок	Нет	Да	Нет	Нет	[15]
Нечеткая математика	Методы нечеткой логики	Да	Да	Нет	Нет	[12, 13]
Энтропийный подход	Энтропия Шеннона	Да	Да	Нет	Нет	[18]

Таблица 1 (*продолжение*).

Использование открытых стандартов	Методы оценки рисков в соответствии со стандартами CVSS, ISO27005	Да	Нет	Нет	Да	[9, 23]
Теоретико-графовый подход	Методы теории графов и матричной записи	Да	Нет	Да	Нет	[20]
	Построение графов отказов, атак, защиты	Нет	Нет	Нет	Да	[22, 30, 31, 35].
«Когнитивная игра»	Когнитивное игровое моделирование	Да	Нет	Да	Да	[10, 14]
Структурный подход			Нет	Да	Нет	[32]
Безмодельный подход	Методы машинного обучения	Нет	Да	Нет	Нет	[26, 29, 37]
Социотехнический подход	Профилирование	Нет	Нет	Нет	Нет	[6, 25]
Попарное сравнение	Метод попарного сравнения	Нет	Нет	Нет	Нет	[34]
Анализ иерархий	Метод анализа иерархий	Нет	Нет	Нет	Нет	[4, 28]
Сценарный подход	Сценарный анализ	Нет	Нет	Нет	Нет	[17, 19]
Ранжирование	FMEA, STRIDE	Нет	Нет	Нет	Нет	[32, 36]
Анализ уровня защиты и блокады	Метод анализа уровня блокады и защиты	Нет	Нет	Нет	Нет	[21]
Методы агрегирования	Пороговое агрегирование	Нет	Нет	Нет	Да	[3]
	Комплексная оценка	Нет	Нет	Да	Да	[1, 2, 5]

По итогам анализа рассмотренных отечественных и зарубежных источников были выявлены следующие недостатки имеющихся подходов и методов, направленных на оценку рисков

сложных систем. Несмотря на то, что для решения задач управления сложными системами, в частности, информационными, возникает необходимость получения оценок текущих значений как локальных рисков защищаемой системы, так и интегрального, характеризующего систему в целом, большинство исследований сфокусировано на оценке локальных рисков. При этом для получения адекватной оценки считается необходимым учесть некоторые неопределенности. Тем не менее крайне мало работ, учитывающих неопределенность значений отдельных факторов оценки системы в целом.

В большинстве своем авторы используют точно заданные параметры, полученные на основе статистических данных, на основе заранее установленной шкалы или на основе предположений, что заведомо неопределенная ситуация является детерминированной. Случаи же с неопределенностью данного вида разрешаются переходом к точному значению либо в виде математического ожидания случайной величины, либо вовсе экспертным методом. Еще одним недостатком в современных подходах к оценке риска сложных систем является то, что влияние риска или критерия одного элемента на другой практически совсем не рассматривается.

Таким образом, анализ показал, что в настоящее время ни один из рассмотренных методов не учитывает одновременно все три вида неопределенности. Тем не менее среди основных методов оценки рисков можно выделить метод комплексного оценивания, делающий упор на качественную оценку, и метод «когнитивной игры», делающий упор на количественную, и каждый из которых по-своему учитывает два вида неопределенности из трех.

Для количественной оценки требуется большой набор данных. Информационные системы имеют возможность накапливать большой массив информации. Однако одной из особенностей данного вида систем является их непрерывная эволюция и изменение порядка своего функционирования, что делает накопленные раннее данные бесполезными. В связи с этим видится разумным для учета всех видов неопределенности сложных информационных систем адаптировать качественный метод, метод КО.

4. Заключение

Для решения задачи эффективного управления сложными информационными системами, формально записываемой в виде (1), можно воспользоваться решением эквивалентной ей задачи минимизации риска (6). Для этого нужно научиться вычислять значения функции риска $\rho(u) = \Im(u^*) - \Im(u)$, где $\Im = \Im K(u, \cdot, \cdot)$ – снимающий неопределенность функционал, зависящий только от выбранного управляющего воздействия; $K\big(q(u,\theta)\big)$ – функционал, описывающий зависимость состояния системы q от управляющего воздействия $u \in U$ и состояния внешней среды $\theta \in \Theta$; U и Θ – множества допустимых управляющих воздействий и возможных состояний внешней среды соответственно. Иными словами, необходимо идентифицировать вид функций риска и снимающего неопределенность функционала.

Существующие модели и методы оценки информационных рисков в большинстве своем разрабатывались без учёта видов неопределенности, характерной для сложных информационных систем. В настоящей работе они рассмотрены с точки зрения их потенциала в части учета характерных для рассматриваемого класса систем видов неопределённости. К таковым авторы относят неопределённость значений отдельных факторов оценки состояния системы в целом, неопределённость взаимного влияния элементов системы друг на друга, а также неопределённости зависимости риска системы в целом от значений локальных рисков. По итогам анализа был выделен ряд методов, представляющих с этой точки зрения максимальный интерес.

Среди них особенно перспективным выглядит метод комплексной оценки. Изначально разработанный для механизма комплексного оценивания организационных систем, он обладает рядом дополнительных важных при решении задач оценки рисков свойств и может быть сравнительно легко адаптирован для оценивания рисков любых сложных систем.

Во второй части данной статьи авторы предлагают формализованный алгоритм формирования структуры дерева комплексной оценки интегрального риска сложных систем.

Литература

1. АЛЕКСЕЕВ А.О. *Исследование устойчивости механизмов комплексного оценивания к стратегическому поведению агентов (на примере согласования политики организации в области риск-менеджмента)* // Прикладная математика и вопросы управления. – 2019. – №4. – С. 136–154.
2. АЛЕКСЕЕВ А.О., КАТАЕВА Т.А. *Применение механизмов комплексного оценивания и матричных неанонимных обобщенных медианных механизмов согласования интересов агентов* // Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2021. – №3. – С. 75–89.
3. АЛЕСКЕРОВ Ф.Т., ЯКУБА В.И. *Метод порогового агрегирования трехградационных ранжировок* // Доклады академии наук. – 2007. – Т. 413, №2. – С. 181–183
4. БАКЕЕВ Д.Ш., ТИШИНА Н.А. *Программная реализация оценки рисков безопасности информации на основе гибридного метода* // Приоритетные направления инновационной деятельности в промышленности. Сборник научных статей по итогам пятой международной научной конференции. – 2020. – Т. 2. – С. 6–12.
5. БАРКАЛОВ С.А., НОВИКОВ Д.А., НОВОСЕЛЬЦЕВ В.И. и др. *Модели управления конфликтами и рисками* / Под ред. Д.А. Новикова. – Воронеж: Научная книга, 2008. – 495 с.
6. БЕЗЗАТЕЕВ С.В., ЕЛИНА Т.Н., МЫЛЬНИКОВ В.А. и др. *Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности* // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21, №4. – С. 553–561.
7. *ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем. – Официальное издание*. – М.: ИПК Изд-во стандартов, 2002 год.
8. *ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. – Официальное издание*. – М.: Стандартинформ, 2019 год.

9. ЗИМА В.М., КРЮКОВ Р.О., КРАВЧУК А.В. *Методика оценивания информационных рисков на основе анализа уязвимостей* // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2019. – №11–12. – С. 36–46.
10. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Модели управления информационными рисками сложных систем* // Информационная безопасность. – 2020. – Т. 23, №2. – С. 191–202.
11. КАЛАШНИКОВ А.О. *Управление информационными рисками организационных систем: механизмы комплексного оценивания* // Информационная безопасность. – 2016. – Т. 3, №1. – С. 315–322.
12. КИСЕЛЕВА Т.В., МАСЛОВА Е.В. *Классификация рисков ИТ-сервисов и способы оценивания вероятностей их возникновения* // ИТНОУ: информационные технологии в науке, образовании и управлении. – 2020. – №1 (15). – С. 67–71.
13. КОЛОСОК И.Н., ГУРИНА Л.А. *Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств* // Методические вопросы исследования надежности больших систем энергетики. – 2019. – Т. 1, №70. – С. 238–247.
14. НОВИКОВ Д.А. *«Когнитивные игры»: линейная импульсная модель* // Проблемы управления. – 2008. – №3. – С. 14–22.
15. AKINROLABU O., NURSE J.R.C., MARTIN A. et al. *Cyber risk assessment in cloud provider environments: Current models and future needs* // Computers & Security. – 2019. – Vol. 87. – P. 101600.
16. ALHAJRI R.M., ALSUNAIDI S.J., ZAGROUBA R. et al. *Dynamic interpretation approaches for information security risk assessment* // Int. Conf. on Computer and Information Sciences (ICCIS-2019). – IEEE, 2019. – P. 1–6.
17. BOLBOT V., THEOTOKATOS G., BOULOUGOURIS E. et al. *A novel cyber-risk assessment method for ship systems* // Safety Science. – 2020. – P. 104908.
18. ERSHADI M.J., FOROUZANDEH M. *Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy FMEA, AHP, TOPSIS and Shannon Entropy* // J. Digit. Inf. Manag. – 2019. – Vol. 17, No. 6. – P. 321.

19. GUNES B., KAYISOGLU G., BOLAT P. *Cyber security risk assessment for seaports: A case study of a container port* // Computers & Security. – 2021. – Vol. 103. – P. 102196.
20. HÄCKEL B. *Assessing IT availability risks in smart factory networks* // Business Research. – 2019. – Vol. 12., No. 2. – P. 523–558.
21. HAN C.H., HAN C.H. *Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis* // Process Safety and Environmental Protection. – 2021. – Vol. 155. – P. 306–316.
22. HE W., LI H., LI J. *Unknown vulnerability risk assessment based on directed graph models: a survey* // IEEE Access. – 2019. – Vol. 7. – P. 168201–168225.
23. *ISO/IEC 27005:2022(EN) Information security, cybersecurity and privacy protection — Guidance on managing information security risks* [Электронный ресурс]. – Режим доступа: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en.
24. *ISO/IEC 31010:2019(EN) Risk management – Risk assessment techniques* [Электронный ресурс]. – Режим доступа: https://www.iso.org/obp/ui/ru/#!iso:std:72140:en.
25. KIOSKLI K., POLEMI N. *A Socio-Technical Approach to Cyber-Risk Assessment* // World Academy of Science, Engineering and Technology Int. Journal of Electrical and Computer Engineering. – 2020. – Vol. 14, No. 10. – P. 305–309.
26. KORNEEV N.V., KORNEEVA J.V., YURKEVICHYUS S.P. et al. *An Approach to Risk Assessment and Threat Prediction for Complex Object Security Based on a Predicative Self-Configuring Neural System* // Symmetry. – 2022. – Vol. 14, No. 1. – P. 102.
27. KRISPER M., DOBAJ J., MACHER G. et al. *RISKEE: a risk-tree based method for assessing risk in cyber security* // European Conf. on Software Process Improvement. – 2019. – P. 45–56.
28. NTAFLOUKAS K., MCCRUM D.P., PASQUALE L. *A Socio-Technical Approach to Cyber-Risk Assessment* // A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure. – 2022. – Vol. 12, No. 18. – P. 9241.
29. PALKO D., BABENKO T., BIGDAN A. et al. *Cyber Security Risk Modeling in Distributed Information Systems* // Appl. Sci. – 2023. – Vol. 13, No. 4. – P. 2393.

30. RIOS E., REGO A., ITURBE E. et al. *Continuous quantitative risk management in smart grids using attack defense trees* // Sensors. – 2020. – Vol. 20. – P. 4404.
31. SCHMITZ C., PAPE S. *LiSRA: Lightweight security risk assessment for decision support in information security* // Computers & Security. – 2020. – Vol. 90. – P. 101656.
32. SHIROKY A., KALASHNIKOV A. *Influence of the Internal Structure on the Integral Risk of a Complex System on the Example of the Risk Minimization Problem in a "Star" Type Structure* // Mathematics. – 2023. – Vol. 11(4). – e998.
33. SUBRIADI A.P., NAJWA N.F. *The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment* // Heliyon. – 2020. – Vol. 6, No. 1. – e03161.
34. TUSHER H.M., MUNIM Z.H., NOTTEBOOM T.E. et al. *Cyber security risk assessment in autonomous shipping* // Maritime Economics & Logistics. – 2022. – Vol. 24, No. 2. – P. 208–227.
35. TUSHER H.M., MUNIM Z.H., NOTTEBOOM T.E. et al. *Development of the mechanism of assessing cyber risks in the internet of things projects* // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 12th Conf., ruSMART-2019. St. Petersburg: Springer International Publishing. – 2019.– P. 481–494.
36. WANG Y., WANG Y.-H., QIN H. et al. *A systematic risk assessment framework of automotive cybersecurity* // Automotive Innovation. – 2021. – Vol. 4. – P. 253–261.
37. WANG Y., XUE W., ZHANG A. *Application of Big Data Technology in Enterprise Information Security Management and Risk Assessment* // Journal of Global Information Management. – 2023. – Vol. 31, No. 3. – P. 1–16.

COMPLEX INFORMATION RISKS ASSESSMENT. I: A BRIEF OVERVIEW OF APPROACHES AND METHODS

Anastasiya Rey, V.A. Trapeznikov Institute of Control Sciences of RAS, Moscow, junior researcher (a.rey@ipu.ru).
Andrey Kalashnikov, V.A. Trapeznikov Institute of Control Sciences of RAS, Moscow, Dr. Sc. Eng., chief researcher (aokalash@pu.ru).

Abstract: Complex information systems (in particular, Internet of Things systems) are characterized by various types of uncertainty. Among them, one can distinguish the uncertainty of the values of individual factors for assessing the state of the system as a whole, the uncertainty of the mutual influence of system elements on each other, as well as the uncertainty of the dependence of the risk of the system as a whole on the values of local risks — as characteristic of this class of systems. The existing methods of assessing information risks of complex systems do not take into account the listed types of uncertainty at the same time. At the same time, since uncertainty is the reason for the deviation of the system from the target mode of operation, the need to take into account at least its main types when assessing risks is obvious. The proposed article contains a brief overview of existing approaches to risk assessment of information systems, as well as an analysis of the possibility of taking into account the above types of uncertainty within each of them. Based on the results of the analysis, the integrated assessment method was chosen as a promising one, originally developed for the mechanism of integrated assessment of organizational systems, and in recent years it has been increasingly used for risk assessment, including in information systems.

Keywords: complex information systems, integral risk, complex assessment, accounting for uncertainty.

УДК 004.056.5
ББК 16.8
DOI: 10.25728/ubs.2024.110.3

Статья представлена к публикации
членом редакционной коллегии А.В. Горбуновой.

Поступила в редакцию 18.04.2024.
Опубликована 31.07.2024.