Вычислительные технологии, 2020, том 25, № 4, с. 99–113. © ФИЦ ИВТ, 2020
Computational Technologies, 2020, vol. 25, no. 4, pp. 99–113. © FRC ICT, 2020
ISSN 1560-7534
eISSN 2313-691X

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

DOI:10.25743/ICT.2020.25.4.009

# Концепция риск-анализа технических систем с использованием цифровых двойников

А. М. Лепихин[1], Н. А. Махутов[2], Ю. И. Шокин[1], А. В. Юрченко[1,*]
[1]Федеральный исследовательский центр информационных и вычислительных технологий СО РАН, Новосибирск, Россия
[2]Институт машиноведения им. А. А. Благонравова РАН, Москва, Россия
*Контактный автор: Юрченко Андрей Васильевич, e-mail: yurchenko@ict.sbras.ru
*Поступила 11 июня 2020 г., доработана 29 июля 2020 г., принята в печать 7 августа 2020 г.*

Рассмотрены основные методологические аспекты анализа рисков технических систем с использованием цифровых двойников. Сформулирована концепция риск-анализа и предложена базовая модель для ее реализации. Рассмотрены информационные аспекты анализа неопределенностей модели риска. Показано, что технологии цифровых двойников позволяют эффективно сочетать результаты компьютерного моделирования с данными мониторинга реальных объектов, обеспечивая более глубокий риск-анализ объектов, с учетом множества вариантов конструкции, технологий и условий эксплуатации.

*Ключевые слова*: техническая система, цифровой двойник, модель риска, информация, неопределенность, анализ риска.

*Цитирование*: Лепихин А.М., Махутов Н.А., Шокин Ю.И., Юрченко А.В. Концепция риск-анализа технических систем с использованием цифровых двойников. Вычислительные технологии. 2020; 25(4):99–113. DOI:10.25743/ICT.2020.25.4.009.

## Введение

Современный этап развития техники и технологий характеризуется двумя особенностями. Первая особенность заключается в создании высоконагруженных и энергонасыщенных технических систем с высоким разрушительным потенциалом, требующим особого внимания к вопросам обеспечения безопасности. Применяемые конструкционные и технологические инновации имеют большой потенциал повышения безопасности, но одновременно они генерируют новые механизмы отказов и опасностей, создают новые риски, в том числе из-за новых или неизвестных ранее функциональных и структурных связей и зависимостей внутри и между системами. В связи с этим неуклонно возрастает актуальность вопросов обеспечения безопасности и методов риск-анализа техники и технологий [1]. Вторая особенность состоит в том, что ускоряющееся развитие техники и технологий, постоянное усложнение создаваемых технических систем, сопряженное с многократным ростом объемов информации, ставят под сомнение возможности традиционных методов проектирования, изготовления и эксплуатации в части обеспечения

требуемой эффективности и безопасности. В быстро меняющейся среде информационные атрибуты, связанные с надежностью компонентов систем и технологий, продолжают играть основополагающую роль, а вопросы безопасности и защищенности от аварий и катастроф приобретают еще большую актуальность [2].

Ключевым направлением решения указанных проблем является широкое использование методов математического и вычислительного моделирования. Развитие методов математического моделирования, информационных технологий и вычислительных средств привело к формированию нового уровня моделирования технических систем — созданию цифровых двойников (Digital Twins — $DT$) [3, 4]. Концепция $DT$ основана на технологиях 3D-моделирования, цифрового прототипирования и дополненной реальности. По сути, $DT$ представляют собой набор виртуальных информационных мультимасштабных и мультифизических конструкций, которые зеркально отражают заданные свойства и функции реального физического объекта [5]. Новизна $DT$ заключается не столько в моделях, сколько в организации связей моделей с потоками данных и моделей между собой.

Несмотря на активные исследования, ряд ключевых аспектов цифровых двойников в настоящее время не имеет соответствующих методологических обоснований и технических решений. В частности, не решены проблемы эффективного снижения порядка моделей и количественного учета факторов неопределенности различного вида. Не реализована концепция риск-информированного принятия решений при управлении жизненным циклом изделий. Фактически отсутствуют работы по методологии риск-анализа и управлению рисками с использованием $DT$.

В данной статье представлены основные методологические аспекты риск-анализа технических систем с использованием цифровых двойников. Риск-анализ рассматривается как систематическое использование информации для выявления опасностей, идентификации, оценки и мониторинга риска [6].

## 1. Концепции анализа риска технических систем

Фундаментальной основой для системного анализа опасностей и угроз, связанных с ускоренной эволюцией техносферы, являются концепции риска. Исходная (классическая) концепция риска, предложенная в работе [7], рассматривает риск как возможность возникновения событий или ситуаций с нежелательными последствиями для объектов, субъектов и окружающей среды. При этом риск определяется в форме триплета:

$$R = \{S_i, f_i, C_i\}, \quad i = 1, \ldots, N, \tag{1}$$

где $S_i$ — сценарий аварии; $f_i$ — частота сценариев; $C_i$ — результат сценария.

Сценарии рассматриваются как случайные последовательности рискообразующих событий $A_j$, $j = 1, \ldots, n$: $S_i = \{A_{i1}, A_{i2}, \ldots, A_{in}\}$. Частота событий обычно определяется по статистическим данным. Результат сценария представляется в виде финансовых, материальных, социальных, экологических или иных потерь.

Обобщение частотных оценок на вероятностные меры позволило сформулировать вероятностную концепцию риска, определяющую риск как вероятность потерь [2]:

$$R = \{S_i, P(A_i, C_i)\}, \quad i = 1, \ldots, N. \tag{2}$$

Обе концепции предполагают построение диаграмм риска, что связано с получением большого объема статистических данных об авариях и катастрофах. Проблема полу-

чения таких данных неоднократно обсуждалась в литературе. Необходимость оценок риска в условиях неизбежной ограниченности статистических данных привела к формулировке инженерной концепции с определением риска в виде средневзвешенных по вероятностям потерь [8]:

$$R = \sum_{i=1}^{N} P(A_i)C(A_i). \tag{3}$$

В отличие от (1) и (2) формула (3) ограничивается анализом конкретных сценариев, без необходимости построения диаграммы рисков.

Инженерная концепция получила широкое практическое применение в виде методологий вероятностного анализа безопасности (PSA) и риска (PRA) [9]. Для реализации этих методологий разработаны статистические, вероятностные, интервальные, байесовские, теоретико-множественные и качественные методы оценки риска в форме (3). Наиболее известны методы FMEA, FTA, HAZOP, HAZID и др. [10].

Основной недостаток риска в форме (3) заключается в том, что события с малыми вероятностями и большими ущербами учитываются наравне с событиями с большой вероятностью и малыми ущербами. Поэтому риск наиболее опасных редких, но больших потерь может существенно нивелироваться множеством незначительных событий.

Одна из существенных проблем рассмотренных концепций заключается в том, что они опираются на обобщенную статистику, которая не всегда отражает особенности механизмов аварий. Помимо этого, они не позволяют провести различия между агентом (источником) риска и системой, воспринимающей риск. Как известно, воспринимаемый риск существенно зависит от уязвимости системы [1]. Под уязвимостью понимается степень, с которой воспринимающая риск система реагирует на воздействие источника риска. В более строгом представлении уязвимость понимают как неопределенность и серьезность последствий от воздействий агента риска [11].

Принимая во внимание указанные обстоятельства, более обоснованной является концепция оценки риска на основе рассмотрения комплекса ключевых понятий механики катастроф: “опасность (danger) — угроза (threat) — уязвимость (vulnerability) — авария (accident)” [12, 13]. В этом случае риск определяется как

$$R = \sum_{i}\sum_{j}\sum_{k}\sum_{l}\sum_{n} P(d_i)P(h_j|d_i)P(v_k|h_j)P(a_l|v_k)P(c_n|a_l), \tag{4}$$

где $d_i \in D$ — опасности; $h_j \in H$ — угрозы; $v_k \in V$ — уязвимости; $a_l \in A$ — аварийные ситуации; $c_n \in C$ — потери; $D$, $H$, $V$, $A$, $C$ — множества опасностей, угроз, уязвимостей, аварийных ситуаций и потерь соответственно.

Недостатки рассмотренных концепций риска состоят в следующем. Во-первых, определяющее допущение, лежащее в основе (1)–(4), заключается в том, что вероятности полагаются известными (оцениваемыми), а последствия — измеримыми. Фактически полнота сценариев всегда ограничена, и риск оценивается в условиях ограниченных знаний и приближенных моделей аварий. Во-вторых, риск является производной категорией. Он не может быть определен без предварительного анализа опасностей, угроз, уязвимостей, потерь. Причем риск всегда рассматривается в контексте конкретных целей анализа и в условиях трудно формализуемых неопределенностей, связанных с опасностями и угрозами. Используемые частотные и вероятностные оценки событий не охватывают и не исчерпывают весь спектр возможных мер неопределенностей. Поэтому в рамках рассмотренных концепций не существует “реального” или “объективного” риска. Получаемые оценки отражают тот уровень знаний о физическом объекте, который существует в рассматриваемый момент времени.

Основной недостаток заключается в том, что оценки риска проводятся post factum, по данным истории аварий и катастроф. Возможности прогнозных оценок риска ограничены ретроспективными статистическими трендами. Для уникальных технических систем и вновь создаваемых перспективных технических систем рассмотренные концепции оказываются малоэффективными.

Принципиальное значение для разработки современных методов риск-анализа технических систем имеет учет следующих постулатов:

— знания, информация и данные, доступные для анализа и характеристики опасностей, моделирования и анализа риска, существенно выросли и продолжают расти;
— современные возможности моделирования и вычислительные мощности позволяют проводить беспрецедентно глубокий анализ опасностей, недоступный ранее;
— постоянное повышение сложности технических систем с большим числом разнородных элементов (конструкционных, аппаратных, человеческих, цифровых), организованных в сильно взаимосвязанные структуры, приводит к поведению, которое трудно предвидеть или предсказать на основе классических расчетно-экспериментальных методов;
— для систематического и эффективного управления рисками необходимо рассматривать все возможные сценарии аварийных ситуаций и их фазы, которые могут возникнуть, включая предотвращение аварий, смягчение последствий, управление кризисными ситуациями и восстановление после аварий. Это влечет за собой существенное расширение методологии оценки рисков на все стадии жизненного цикла изделий с учетом риска принятия решений;
— риск не является статической мерой, а существенно меняется на разных стадиях жизненного цикла технических систем под действием изменяющихся условий и принимаемых мер по предотвращению, защите и смягчению последствий опасных событий;
— существенную роль в обеспечении безопасности начинают играть информационные технологии и киберфизические системы, открывающие новые возможности мониторинга состояний объектов.

## 2. Информационные аспекты анализа риска

Как отмечалось выше, на современном этапе развития техники и технологий информация и знания становятся определяющим фактором анализа риска. Результаты оценки риска обусловлены знаниями, доступными в анализируемой системе и/или процессе [14]. Признание этого факта стало настолько важным, что возникла необходимость разработки концепции, связывающей риск с накопленными знаниями. Одной из концептуальных формулировок, принимающих во внимание значимость информации и знаний, является представление риска в следующем виде [14]:

$$R = \{A, C, Q : I\}, \tag{5}$$

где $A$ — набор сценариев аварий, которые могут произойти; $C$ — набор последствий; $Q$ — метрика, используемая для количественного определения связанных неопределенностей; $I$ — совокупность знаний и информации, по которым проводится оценка риска (т. е. идентификация $A$ и количественная оценка $C$ и $Q$ основаны на $I$).

С позиций информационной концепции методики и подходы к анализу риска должны рассматриваться как получение и представление знаний об опасностях и угрозах для

обеспечения возможностей принятия упреждающих риск-информированных решений. Важно отметить, что формулировка (5) не ограничивает представление неопределенностей классической вероятностной формой в отличие от рассмотренных выше формулировок. Здесь могут использоваться альтернативные представления и качественные оценки в дополнение к количественным вероятностным оценкам [14, 15].

Информационная концепция риска признает возможность и неизбежность наличия компонентов риска, обусловленных неизвестными неопределенностями. В общем случае независимо от их физической сущности выделяются четыре категории неопределенностей [14]: неизвестные — неизвестные, неизвестные — известные, известные — неизвестные, известные — известные.

Первая группа определяет события и сценарии, которые были неизвестны специалистам во время оценки риска. Вторая группа относится к тем событиям и сценариям, которые неизвестны конкретным специалистам при анализе риска, но известны кому-то еще. Третья группа идентифицирует ситуации, когда известный тип события или сценария может произойти в будущем, но базовые знания о нем малы или отсутствуют вовсе. Четвертая группа указывает на события и сценарии, которые известны специалистам и по ним имеется достаточный объем информации.

Несмотря на широкие исследования, в целом проблема неопределенности в проблеме риск-анализа остается сложной. При оценке риска всегда можно утверждать, что все в некоторой степени неизвестно, и классификация аварийных событий и сценариев по четырем указанным категориям может быть сомнительной. Исходя из этого решение может быть "правильным" в том смысле, что оно согласуется с данной теоретической моделью и данной совокупностью знаний, но после этого оно может оказаться "неправильным" с точки зрения фактического результата, поскольку всегда есть вероятность, что совокупность знаний неполна для принятия "правильного" решения. Это верно для любой модели риска, которая построена и применяется на основе информации и знаний. Поэтому уровень знаний и объем располагаемой информация имеют ключевое значение при оценках рисков и управлении рисками.

Исходя из вышеизложенного, можно констатировать, что при использовании информационных технологий риск-анализ представляет собой исследование, направленное на систематизацию и организацию доступной информации и знаний по событиям, процессам и сценариям с целью оценки неопределенностей принимаемых решений. Значимость и обоснованность оценок зависят не только от объема знаний, но и от концептуальных положений риск-анализа.

Остановимся на еще одном концептуальном аспекте риск-анализа. Отмеченная выше ускоренная эволюция техносферы приводит к тому, что время становится одним из определяющих факторов принятия технических решений. Обоснование технических параметров и их воплощение в технических системах проводятся во все более сжатые сроки. Возможности длительного расчетно-экспериментального обоснования параметров изделий существенно сократились или вовсе утратили актуальность. Конструкции, материалы и технологии сейчас формируются в течение короткого цикла создания изделия. Причем все чаще эти циклы уникальны, не имеют прототипов, а часто оказываются и без широких перспектив повторного использования в будущем. Поэтому разрабатываемые концепции риск-анализа и модели риска должны обеспечивать возможность анализа уникальных объектов и учитывать фактор времени как в явном виде, так и опосредованно, в получаемом на данном этапе объеме информации и знаний об объекте риск-анализа.

## 3. Особенности задач риск-анализа технических систем

Наряду с оценками риска аварий и катастроф на основе отмеченных концепций для технических систем особую актуальность представляют методы риск-анализа, ориентированные на исследование и количественную оценку роли случайных факторов в формировании аварий и катастроф [16]. Риск-анализ рассматривает аварии и катастрофы как экстремальные (предельные) состояния технических систем, формирующиеся уникальной историей накопления повреждений при заданном комплексе нагрузок и воздействий. Выявление и характеристика сценариев экстремальных состояний являются фундаментальной задачей анализа знаний о технических системах и их окружении. Эта задача далеко не тривиальна на практике ввиду сложности систем и механизмов катастроф. Она не может быть решена на основе чисто статистического анализа комбинаторного набора возможных сценариев, событий и условий, из которых лишь немногие приводят к экстремальным и опасным по последствиям ситуациям. Необходим более детальный анализ технических систем в соответствующих параметрических, функциональных и критериальных пространствах.

Проектирование, изготовление и эксплуатация технических систем, по сути, заключается в обосновании (при проектировании) и наложении (при изготовлении и эксплуатации) параметрических, функциональных и критериальных ограничений, обеспечивающих работоспособность технических систем:

$$\begin{gathered} \boldsymbol{\alpha}_* \leqslant \boldsymbol{\alpha} \leqslant \boldsymbol{\alpha}_{**}, \\ \phi_*(\boldsymbol{\alpha}) \leqslant \phi(\boldsymbol{\alpha}) \leqslant \phi_{**}(\boldsymbol{\alpha}), \\ \Phi_*(\boldsymbol{\alpha}) \leqslant \Phi(\boldsymbol{\alpha}) \leqslant \Phi_{**}(\boldsymbol{\alpha}). \end{gathered} \tag{6}$$

Здесь $\boldsymbol{\alpha}$ — вектор конструктивно-технологических переменных; $\phi(\boldsymbol{\alpha})$ — заданные функции; $\Phi(\boldsymbol{\alpha})$ — заданные критериальные характеристики работоспособности; $\boldsymbol{\alpha}_*$, $\boldsymbol{\alpha}_{**}$ — верхние и нижние ограничения конструктивно-технологических переменных; $\phi(\boldsymbol{\alpha}_*)$, $\phi(\boldsymbol{\alpha}_{**})$ — верхние и нижние ограничения функций; $\Phi(\boldsymbol{\alpha}_*)$, $\Phi(\boldsymbol{\alpha}_{**})$ — верхние и нижние ограничения характеристик работоспособности.

С позиций (6) обеспечение устойчивого и безопасного функционирования технической системы заключается в удержании вектора решения $\mathbf{X}(\boldsymbol{\alpha}, \phi, \Phi)$ внутри области ограничений. Сложность задачи состоит в том, что в общем случае могут иметь место пересечения и наложения ограничений, приводящие к сложным конфигурациям пространств допустимых решений.

В результате решения задачи (6) создается физический объект $PO$ с заданными структурой (конструкцией) $\Sigma$, функциями $\phi$ и критериальными условиями работоспособности $\Phi$:

$$PO = \{\Sigma, \phi, \Phi\}. \tag{7}$$

Риск аварии $R_{PO}$ для физического объекта (7) можно представить как вероятность появления угроз $H$ при недопустимых вариациях структуры, функций и критериальных условий:

$$R_{PO} = P\left\{H | Var\left[\Sigma, \phi, \Phi\right] \notin \Omega_s^{PO}\right\}, \tag{8}$$

где $Var$ — вариации переменных; $\Omega_s^{PO}$ — область допустимых состояний физического объекта.

Как следует из (8), задача риск-анализа технических систем заключается в исследовании вариаций структуры, функций и критериальных условий, создающих угрозы для

$PO$, других объектов и окружающей среды. Это крайне сложная задача, требующая совместного решения многомасштабных, мультифизических задач на основе имеющейся информации $I$. Данная информация накапливается по мере продвижения технической системы по стадиям жизненного цикла и включает сведения об изменениях и случайных вариациях структуры, функций и условий работоспособности. В общем случае структура $\Sigma$, функции $\phi$ и критериальные условия $\Phi$ являются случайными функциями или функционалами времени $t \in [0, T]$, где $T$ — рассматриваемое время "жизни" системы. Исходя из этого формулу (8) можно переписать в следующем виде:

$$R_{PO}(t) = P\left\{I_t : H_t | Var\left[\Sigma_t, \phi_t, \Phi_t\right] \notin \Omega_s^{PO}\right\}. \tag{9}$$

Представление риска в форме (9) означает необходимость совместного анализа вариаций структуры, функций и условий работоспособности технической системы в заданном интервале времени. Провести такой анализ в рамках традиционных расчетно-экспериментальных методов и ретроспективного статистического анализа не представляется возможным. Здесь необходимы новые подходы, модели и методы вычислительного моделирования, связанные непосредственно с физическими процессами в технической системе. Тем не менее рассмотренные выше концепции риска позволяют получать частные решения задачи (9) в пределах рассматриваемого набора сценариев вариаций переменных и имеющейся информации.

Сложность задачи (9) приводит к необходимости постановки более простых формулировок. Одним из таких упрощений является переход к анализу конструкционного риска [16]. В этом случае физический объект рассматривается как связанная структура $\Sigma$, состоящая из подсистем $\sigma$ и элементов $e$:

$$\Sigma = \bigcup_{i=1}^{n} \sigma_i \left( \bigcup_{j=1}^{m} e_{ij} \right). \tag{10}$$

Эволюцию объекта во времени $t$ (в течение жизненного цикла объекта) можно представить как последовательность изменяющихся структур $\Sigma_0 \to \Sigma_t \to \Sigma_f$, где $\Sigma_0$ — структура на стадии проектирования, $\Sigma_t$ — структура на стадии производства и эксплуатации, $\Sigma_f$ — структура на стадии вывода из эксплуатации или аварийного разрушения.

Изменения структур связаны с тем, что первоначальные "идеализированные" решения (6) получают неизбежные отклонения уже на стадии проектирования из-за ограниченной точности расчетных моделей и информации, ошибок, упущений и т. п. Далее, на стадиях изготовлении и эксплуатации возникают неизбежные изменения и случайные отклонения характеристик материалов, геометрических размеров, нагрузок и воздействий, появляются технологические дефекты и эксплуатационные повреждения. Могут вноситься также конструктивные изменения, выполняться ремонтные операции, реконструкции и проч. Все это приводит к изменениям риска по мере продвижения системы по стадиям жизненного цикла.

С учетом (10) конструкционный риск $R_\Sigma$ можно представить как вероятность возникновения опасностей при нарушении устойчивости состояний элементов:

$$R_\Sigma(t) = P\left\{I_t : H_t | Var\left[e_{ij}(t)\right] \notin \Omega_s^\Sigma\right\}, \tag{11}$$

где $Var$ — вариации состояний элементов; $\Omega_s^\Sigma$ — область устойчивых (безопасных) состояний.

Недопустимые вариации состояний элементов в данном случае определяются критериальными условиями работоспособности (6). Исследование этих вариаций выполняется расчетно-экспериментальными методами [1, 12, 16]. Сложность расчетно-экспериментального подхода связана с большой размерностью вектора базисных переменных $\boldsymbol{\alpha} \in \mathbb{R}^{n \times m \times k}$, где $n$ — число элементов в системе, $m$ — число физических процессов в элементе, $k$ — число переменных физического процесса. Обычно компоненты вектора $\boldsymbol{\alpha}$ являются функциями времени $t$, т. е. $\boldsymbol{\alpha} = \{\alpha_i(t), i = 1, \ldots, n; t \in [0, T]\}$, в связи с чем требуется решать задачи прогнозирования изменений переменных $\alpha_i(t)$ в условиях неопределенности. Такие задачи до сих пор являются серьезной проблемой и решаются только для некоторых частных случаев с детерминированными (через коэффициенты запаса) или вероятностными (через плотности распределений вероятностей) оценками неопределенностей. В этих условиях для зависимых от времени состояний элементов можно определить выборочную траекторию изменений риска $R(t)$ в неопределенном массиве возможных траекторий риска. Некоторые снижения неопределенностей можно получить с использованием байесовских методов на основе данных мониторинга состояний технических систем [17].

Представление риска в форме (9) и (11) можно использовать как для решения задач в рамках концепции обеспечения безопасности, так и для задач поддержки принятия решений в рамках концепции риск-информированного управления жизненным циклом изделий. В задачах обеспечения безопасности должны исследоваться экстремальные вариации структур, функций и критериальных условий, приводящие к катастрофическим последствиям. В задачах принятия решений требуется исследовать более широкие области, поскольку здесь важны не только экстремальные вариации, но и вариации, связанные с неоптимальным выбором параметров и неизбежными функциональными потерями. Эти потери формируют риски неоптимальной конструкции, неоптимальных технологий изготовления и эксплуатации. Косвенно, а иногда непосредственно неоптимальные решения могут приводить к рискам аварий и катастроф.

Таким образом, концепция риск-анализа безопасности технических систем и концепция риск-анализа решений по управлению жизненным циклом технических систем различаются не моделями и методами, а областями рассматриваемых вариаций состояний элементов в выражениях (9) и (11). Еще одним различием является то, что во втором случае выбор варианта решения проводится не на основе оценки риска (т. е. сравнения полученного риска с допустимым уровнем), а на основе информации о риске, путем сравнения вариантов с различными уровнями рисков, с учетом иной информации, не входящей, собственно, в анализ риска. С учетом изложенного риск-анализ безопасности и риск-анализ решений по управлению жизненным циклом технических систем могут основываться на одних и тех же информационных технологиях, моделях и методах вычислительного моделирования, связанных с физическими процессами в технической системе.

## 4. Концепция риска в цифровых двойниках

Новым уровнем вычислительного моделирования, обеспечивающим непосредственную связь с физическими процессами в технических системах, является создание цифровых двойников. Концепция двойников изделий впервые была сформулирована в NASA в конце 1960-х гг. для решения задач наземной отработки основных операций и анализа возможных нештатных ситуаций космических аппаратов. Развитием этой концепции

стала идея создания информационного зеркала физического объекта для решения задач управления жизненным циклом изделий [18]. Собственно термин "$DT$" впервые был использован в NASA в 2010 г. и подразумевал создание имитационной модели, отражающей поведение космического аппарата.

Согласно определению из [19], цифровой двойник — это интегрированное мультифизическое, многомасштабное, вероятностное моделирование объекта, которое использует доступные физические модели, показания датчиков и предысторию для отражения его жизненного цикла. В формальном представлении $DT$ рассматривается как пятимерная конструкция следующего вида [19]:

$$DT = \{PO, VM, SN, DB, CN\}, \tag{12}$$

где $PO$ — физический объект; $VM$ — виртуальная модель объекта; $SN$ — сервисы; $DB$ — данные; $CN$ — связи.

Физический объект рассматривается с учетом особенностей структуры, функций и критериев работоспособности. Виртуальная модель содержит геометрические и физические модели объекта. Сервисы обеспечивают возможность моделирования, мониторинга и верификации, а также прогнозирования, оптимизации и проч. Связи обеспечивают различные виды соединений и связей [19]:

- соединение между физическими объектами и виртуальными моделями ($PO \leftrightarrow VM$);
- соединение между физическими объектами и данными ($PO \leftrightarrow DB$);
- соединение между физическими объектами и сервисами ($PO \leftrightarrow SN$);
- соединение между виртуальными моделями и данными ($VM \leftrightarrow DB$);
- связь между виртуальными моделями и сервисами ($VM \leftrightarrow SN$);
- связь между сервисами и данными ($SN \leftrightarrow DB$).

Ключевым элементом $DT$ является виртуальная модель $VM$, которая создается как зеркальное отражение физического объекта (7) в виде набора виртуальных моделей структуры $V\Sigma$, функций $V\phi$ и критериальных условий $V\Phi$:

$$VM = \{V\Sigma, V\phi, V\Phi\}. \tag{13}$$

При разработке $DT$ и $VM$ неизбежно возникают неопределенности. Виртуальная модель (13) содержит два типа неопределенностей: неопределенности физического объекта и неопределенности моделирования. Неопределенность физического объекта является объективной и практически неустранимой. Неопределенность моделирования может корректироваться за счет связи $PO \leftrightarrow VM$. Для учета неопределенностей необходим вероятностный подход, обеспечивающий возможность построения вероятностного цифрового двойника $PDT$ с вероятностной виртуальной моделью $PVM$ и вероятностной базой данных $PDB$:

$$PDT = \{PO, PVM, SN, PDB, CN\}. \tag{14}$$

Вероятностная виртуальная модель в этом случае должна содержать вероятностные описания структуры $PV\Sigma$, функций $PV\phi$ и критериальных условий $PV\Phi$:

$$PVM = \{PV\Sigma, PV\phi, PV\Phi\}. \tag{15}$$

На основании (14) с учетом (15) риск можно представить как вероятность возникновения опасностей при недопустимых вариациях параметров виртуальной модели в рассматриваемые моменты времени $t$:

$$R_{VM}(t) = P\left\{I_t : H_t | Var\left[PVM(t)\right] \notin \Omega_s^{VM}\right\}. \tag{16}$$

Необходимо отметить, что объектом риска в данном случае является виртуальная модель, а не физический объект. Чем точнее виртуальная модель, тем точнее и обоснованнее становится риск-анализ.

Принципиальным отличием риск-анализа в форме (16) от риск-анализа в форме (9) является возможность исследований большого числа вариантов наборов вектора базисных переменных, структур, функций и критериальных условий. При заданной размерности пространства базисных переменных этот набор ограничен только вычислительными ресурсами. Задача (16) может решаться методами статистических испытаний (Монте-Карло) и стохастического математического моделирования [20, 21]. Для задач большой размерности классический прямой метод Монте-Карло оказывается малоэффективен. В таких случаях более подходящими являются методы моделирования выборки по важности, адаптивной выборки по важности и метод выборки по подмножествам [22, 23].

Поскольку $VM$ непосредственно связана с $PO$, выражение (16) позволяет проводить риск-анализ на разных стадиях жизненного цикла физического объекта с учетом изменений переменных в интервале времени $t + \tau$ с горизонтом прогноза $\tau$. Указанные выше модели изменения базисных переменных $\alpha_i(t + \tau)$ в этом случае являются адаптивными, постоянно улучшаемыми по мере получения данных с датчиков и сенсоров на реальном объекте.

Необходимо подчеркнуть, что формула (16) позволяет решать как задачи риск-анализа безопасности, так и задачи риск-анализа принятия решений. Особенность заключается в том, что получаемые оценки риска являются оперативными, соответствующими не только заданной стадии жизненного цикла, но и рассматриваемой технологической или эксплуатационной операции. Эти оценки являются предиктивными и прогностическими для следующих стадий жизненного цикла. Уточнение оценок происходит автоматически, по мере продвижения по стадиям жизненного цикла.

Преимущества использования $DT$ для решения задач риск-анализа заключаются в том, что:

1) $DT$ способны обеспечить более точные представления особенностей взаимодействия технической системы с внешней средой за счет получения данных в реальном времени;
2) $DT$ позволяют объединять результаты моделирования с данными мониторинга реальных объектов, обеспечивая этим более глубокое понимание состояния объектов;
3) $DT$ обеспечивают возможность рассмотрения множества вариантов конструктивной компоновки, технологий исполнения и условий эксплуатации технических систем, недостижимого при анализе физических систем;
4) $DT$ обеспечивают возможность предиктивного, прогностического риск-анализа вместо традиционных оценок риска post factum.

## 5. Модель риска

Для проведения риск-анализа в форме (14) необходима эффективная модель риска. Поскольку $PVM$ является параметрической, модель риска должна рассматриваться в параметрическом пространстве. Это отличает риск-анализ с использованием $PDT$ от риск-анализа физических объектов, где доминируют структурные модели и сценарный анализ.

Для разработки модели риска введем проектный срок службы $T$ системы. Интервал времени $[t, T]$, где $t$ — рассматриваемый момент времени, будем называть интервалом риска, а разницу $(T - t)$ будем определять как горизонт риска. Также положим, что для виртуальной модели может быть задано вероятностное пространство $(\Omega, \mathcal{F}, P)$, где $\Omega$ — множество событий, $\mathcal{F}$ — множество исходов, $P$ — вероятности исходов.

Функциональность и работоспособность $PVM$ будем характеризовать множеством производных обобщенных переменных $X$, состоящих из измеряемых случайных величин $X := L^{\infty}(\Omega, \mathcal{F}, P)$. В общем случае любой набор переменных можно рассматривать как случайный обобщенный вектор решений $\mathbf{X}^{t,T}(\omega)$ в параметрическом пространстве конструктивно-технологических переменных $\alpha$, определяющий функциональные и критериальные характеристики физического объекта $PO$. В дополнение к этим переменным зададим случайные факторы риска $h : [t, T] \times \Omega$ на интервале времени $[t, T]$, принадлежащие множеству $H_{t,T}$. Множество $H_{t,T}$ может иметь риск-факторы различной физической природы, как-то: повреждение материалов и конструкций, экстремальные нагрузки и воздействия, отклонения функциональных параметров и проч.

Риск-факторы будем разделять на следующие категории: неизвестные — неизвестные (риск-факторы неизвестны и информации о них нет); неизвестные — известные (риск-факторы неизвестны при анализе, но могут быть определены позднее); известные — неизвестные (риск-факторы известны, но информации о них недостаточно для учета в анализе); известные — известные (риск-факторы известны и информации о них достаточно для количественного анализа). Для идентификации риск-факторов важное значение имеет предшествующий моменту $t$ интервал времени $[0, t]$, поскольку здесь накапливается необходимая для анализа информация. В общем случае в этот интервал могут включаться вся предыстория и опыт создания подобных систем.

С использованием накопленной информации и соответствующих физических моделей всегда может быть задано отображение $X^{t,T} : H_{t,T} \to X_H$, присваивающее каждому фактору риска $h$ уникальный набор переменных $X_h^{t,T}(\omega)$. В зависимости от постановки задачи набор $X_h^{t,T}(\omega)$ может быть интерпретирован как случайные потери от риск-фактора, заключающиеся в снижении функциональных характеристик и характеристик работоспособности. Подчеркнем, что пределы набора определяются информацией $I$, представленной в базе данных $DB$ цифрового двойника.

С учетом этого риск $R$ можно представить как вероятностную меру функции потерь $U$ от реализации случайного набора переменных $X_h^{t,T}(\omega)$ в интервале времени $[t, T]$:

$$R\left\{X_h^{t,T}(\omega)\right\} = P\left\{I : U\left[X_h^{t,T}(\omega)\right]\right\}. \tag{17}$$

Данная вероятностная мера может содержать комбинации детерминированных и вероятностных функций, а также количественных и качественных экспертных оценок переменных состояния $X_h^{t,T}(\omega)$.

Допустимое по риску множество результатов $A_R$ определим как набор, удовлетворяющий заданному ограничению по величине риска $R_n$:

$$A_R = \left\{X_h^{t,T}(\omega) \in X_H : R\left\{X_h^{t,T}(\omega)\right\} \leqslant R_n\right\}. \tag{18}$$

Задача принятия технического решения на рассматриваемом этапе жизненного цикла технической системы будет заключаться в выборе варианта из допустимого множества

$A_R$, удовлетворяющего условию (18). Если невозможно установить допустимый риск $R_n$, то выбирается решение, обеспечивающее наименьший риск $R_A$:

$$R_A = \inf \left\{ R \left[ X_h^{t,T}(\omega) \right] | X_h^{t,T}(\omega) \in X_H \right\}. \tag{19}$$

Задача риск-анализа (17) и задачи выбора риск-информированного решения (18) и (19) могут решаться не только для всего срока эксплуатации системы $[t, T]$, но и для любого заданного интервала риска $[t, \tau]$, относящегося к рассматриваемой стадии жизненного цикла.

Изменение риска на различных стадиях жизненного цикла в общем случае может включать: увеличение или снижение первоначально установленного риска, вновь созданный риск (на рассматриваемом этапе возникли новые риск-факторы), вновь выявленный риск (риск-факторы существовали ранее, но были установлены на рассматриваемом этапе), неизвестный риск (риск-факторы предполагаются, но они не установлены на данном этапе). Однако во всех случаях выбор риск-информированного решения должен соответствовать условиям (18) или (19).

В статье не обсуждались вопросы построения вероятностных моделей вектора $\mathbf{X}_h^{t,T}(\omega)$. Построение таких моделей определяется конкретным объектом и целями риск-анализа. Основой для решения такой задачи являются методы стохастического моделирования неопределенностей на основе методов механики деформируемого тела и механики разрушения [16, 20].

## Заключение

Рассмотрен круг вопросов, связанных с возможностями риск-анализа технических систем с использованием цифровых двойников. Показано, что технологии цифровых двойников позволяют объединять результаты моделирования с данными мониторинга реальных объектов, обеспечивая более глубокое понимание состояния объектов, с учетом множества вариантов конструктивной компоновки, технологий исполнения и условий эксплуатации технических систем.

Технологии цифровых двойников создают предпосылки для формирования нового направления риск-анализа, основанного на информационно-вычислительном моделировании. Такой подход открывает широкие возможности для обеспечения безопасности технических систем и риск-информированного управления жизненным циклом изделий. Фундаментальной проблемой в этом направлении является построение параметрических моделей риска, зеркально отображающих физические аспекты достижения экстремальных состояний технических систем в цифровых двойниках.

С позиций информационной концепции подходы и методы анализа риска должны рассматриваться как получение и представление знаний об опасностях и угрозах для обеспечения возможностей принятия упреждающих риск-информированных решений. При этом концепции и модели риска должны включать как классические вероятностные оценки неопределенностей, так и качественные и экспертные оценки.

## Список литературы

[1] **Махутов Н.А.** Безопасность и прочность. Фундаментальные и прикладные исследования. Новосибирск: Наука; 2008: 528.

[2] **Zio E.** The future of risk assessment. Reliability engineering and system safety. Elsevier; 2018: 176–190. DOI:10.1016/j.ress.2018.04.020.hal-01988966.

[3] **Jones D., Snider C., Nassehi A., Yon Ja., Hicks B.** Characterizing the digital twin: A systematic literature review. CIRP Journal of Manufacturing Science and Technology. 2020; Part A. (29):36–52. Available at: `https://doi.org/10.1016/j.cirpj.2020.02.002` (accessed 05.08.2020).

[4] **Deuter A.** The digital twin theory. DOI:10.30844/I40M_19-1_S27-30. Avaiable at: `https://www.researchgate.net/publication/330883447` (accessed 05.08.2020).

[5] **Qi Q., Tao F., Hu T., Anwer N.** Enabling technologies and tools for digital twin. DOI:10.1016/j.jmsy.2019.10.001. Avaiable at: `https://www.researchgate.net/publication/336870688` (accessed 05.08.2020).

[6] ГОСТ Р ИСО/МЭК 13355-1-2006. Информационные технологии. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

[7] **Kaplan S., Garrick B.** On the quantitative definition of risk. Risk Anaysis. 1981; 1(1):11–27.

[8] **Wilson R., Crouch E.A.C.** Risk benefit analysis. Cambridge, MA: Ballinger; 1982: 218.

[9] **Rausand M.** Risk assessment. Theory, methods, and applications. Hoboken: Wiley & Sons; 2011: 649.

[10] **Sotic A., Rajic R.** The rewiev of the definition of risk. Online Journal of Applied Knowledge Management. 2015; 3(3):17–26.

[11] **Pardue N.** Advanced methods for the risk, vulnerability and resilience assessment of safety-critical engineering components, systems and infrastructures, in the presence of uncertainties. Avaiable at: `https://hal.archives-ouvertes.fr` (accessed 05.08.2020).

[12] **Махутов Н.А., Петров В.П., Резников Д.О.** Оценка живучести сложных технических систем. Проблемы безопасности и чрезвычайных ситуаций. 2009; (3):47–66.

[13] **Lepikhin A., Moskvichev V., Machutov N.** Probabilistic modelling in solving analytical problems of system engineering. Probabilistic Modeling in System Engineering. London: IntechOpen Limited; 2018: 3–22. ISBN:978-1-78923-775-7. DOI:10.5772/intechopen.75686.

[14] **Aven T.** Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management. Abingdon: Routledge; 2014: 276. ISBN:9781315755175.

[15] **Aven T.** On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis. 2011; 31(4):515–22. DOI:10.1111/j.1539-6924.2010.01528.x

[16] **Лепихин А.М., Махутов Н.А., Москвичев В.В., Черняев А.П.** Вероятностный риск-анализ конструкции технических систем. Новосибирск: Наука; 2003: 174.

[17] **Kelly D., Smith Ch.** Bayesian inference for probabilistic risk assessment. A practitioner's guidebook. Springer Series in Reliability Engineering. London: Springer-Verlag Limited; 2011: 238. DOI:10.1007/978-1-84996-187-5.

[18] **Dahmen U., Rossman J.** Experimentable digital twins for a modeling and simulation-based engineering approach. Avaiable at: `https://www.researchgate.net/publication/329298561` (accessed 05.08.2020).

[19] **Qi Q., Tao F., Hu T., Anwer N., Liu A., Wei Y., Wang L.** Enabling technologies and tools for digital twin. Available at: `https://doi.org/10.1016/j.jmsy.2019.10.001` (accessed 05.08.2020).

[20] Computation stochastic mechanics. Ed. P.D. Spanos, C.A. Brebbia. Springer Netherlands; 1991: 898.

[21] **Soize C.** Stochastic models of uncertainties in computational mechanics. American Society of Civil Engineers. 2012: 125–134. ISBN:978-0-7844-7686-4.

[22] **Shayanfar M.A., Barkhordari M.A., Roudak M.A.** An adaptive importance sampling-based algorithm using the first order method for structural reliability. International Journal of Optimization in Civil Engineering. 2017; 7(1):93–107.

[23] **Au S.K., Beck J.L.** Estimation of small failure probabilities in high dimensions by subset simulation. Probabilistic Engineering Mechanics. 2001. 16:263–277. DOI:10.1016/S0266-8920(01)00019-4.

Вычислительные технологии, 2020, том 25, № 4, с. 99–113. © ФИЦ ИВТ, 2020 ISSN 1560-7534
Computational Technologies, 2020, vol. 25, no. 4, pp. 99–113. © FCR ICT, 2020 eISSN 2313-691X

INFORMATION TECHNOLOGIES

DOI:10.25743/ICT.2020.25.4.009

## Analysis of risk concept for technical systems using digital twins

Lepikhin Anatoly M.[1], Makhutov Nikolay A.[2], Shokin Yurii I.[1], Yurchenko Andrey V.[1,*]

[1]Federal Research Center for Information and Computational Technologies SB RAS, Novosibirsk, Russia

[2]Blagonravov Mechanical Engineering Research Institute RAS, Moskow, Russia

*Corresponding author: Yurchenko Andrey V., e-mail: yurchenko@ict.sbras.ru

*Received June 11, 2020, revised July 29, 2020, accepted August 7, 2020*

**Abstract**

Development of technology and technical systems significantly increases in the volume of information. Traditional methods for designing, manufacturing and operating of technical systems do not allow processing such volumes of information. In this regard, the modern strategy for creating technical systems is based on the use of digital twins. Solving the problems of risk analysis and risk management for technical systems at all stages of the life cycle appears to be one of the promising areas for application of the digital twins technology. Despite of active research, using digital twins in risk analysis currently do not have appropriate methodological justifications and technical solutions in a number of key aspects. In particular, effective reductions of the order of risk models and quantifying uncertainty factors of various types have not been solved. The concept of the risk-informed decision making in product lifecycle management has not been implemented. In fact, there are very few publications on the risk analysis and risk management methodology using digital twins. The article discusses the main methodological aspects of risk analysis of technical systems using digital twins. The concept of risk analysis is formulated and a basic model for its implementation is proposed. The informational aspects of the analysis of uncertainties of the risk model are considered. It is shown that digital twin technologies allow effective combination of the results of computer modelling with the data monitoring of real objects, providing a deeper analysis of objects, taking into account a variety of design options, technologies and operating conditions.

*Keywords*: technical systems, digital twins, risk model, information, uncertainties, risk analysis.

*Citation*: Lepikhin A.M., Makhutov N.A., Shokin Yu.I., Yurchenko A.V. Analysis of risk concept for technical systems using digital twins. Computational Technologies. 2020; 25(4):99–113. DOI:10.25743/ICT.2020.25.4.009. (In Russ.)

**References**


1. Makhutov N.A. Bezopasnost' i prochnost'. Fundamental'nye i prikladnye issledovaniya [Safety and durability. Basic and applied research]. Novosibirsk: Nauka; 2008: 528. (In Russ.)
2. Zio E. The future of risk assessment. Reliability engineering and system safety. Elsevier; 2018: 176–190. DOI:10.1016/j.ress.2018.04.020.hal-01988966.
3. Jones D., Snider C., Nassehi A., Yon Ja., Hicks B. Characterizing the digital twin: A systematic literature review. CIRP Journal of Manufacturing Science and Technology. 2020; Part A. (29):36–52. Available at: `https://doi.org/10.1016/j.cirpj.2020.02.002` (accessed 05.08.2020).
4. Deuter A. The digital twin theory. DOI:10.30844/I40M_19-1_S27-30. Avaiable at: `https://www.researchgate.net/publication/330883447` (accessed 05.08.2020).
5. Qi Q., Tao F., Hu T., Anwer N. Enabling technologies and tools for digital twin. DOI:10.1016/j.jmsy.2019. 10.001. Avaiable at: `https://www.researchgate.net/publication/336870688` (accessed 05.08.2020).
6. GOST R ISO/MEK 13355-1-2006. Informatsionnye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Chast' 1. Kontseptsiya i modeli menedzhmenta bezopasnosti informatsionnykh i telekommunikatsionnykh tekhnologiy [Information Technology. Security methods and tools. Part 1. Concept and models of security management of information and telecommunication technologies].
7. Kaplan S., Garrick B. On the quantitative definition of risk. Risk Anaysis. 1981; 1(1):11–27.
8. Wilson R., Crouch E.A.C. Risk benefit analysis. Cambridge, MA: Ballinger; 1982: 218.
9. Rausand M. Risk assessment. Theory, methods, and applications. Hoboken: Wiley & Sons; 2011: 649.
10. Sotic A., Rajic R. The rewiev of the definition of risk. Online Journal of Applied Knowledge Management. 2015; 3(3):17–26.
11. Pardue N. Advanced methods for the risk, vulnerability and resilience assessment of safety-critical engineering components, systems and infrastructures, in the presence of uncertainties. Avaiable at: `https://hal.archives-ouvertes.fr` (accessed 05.08.2020).
12. Makhutov N.A., Petrov V.P., Reznikov D.O. Assesment of complex technical systems robustness. Safety and Emergencies Problems. 2009; (3):47–66. (In Russ.)
13. Lepikhin A., Moskvichev V., Machutov N. Probabilistic modelling in solving analytical problems of system engineering. Probabilistic Modeling in System Engineering. London: IntechOpen Limited; 2018: 3–22. ISBN:978-1-78923-775-7. DOI:10.5772/intechopen.75686.
14. Aven T. Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management. Abingdon: Routledge; 2014: 276. ISBN:9781315755175.
15. Aven T. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis. 2011; 31(4):515–22. DOI:10.1111/j.1539-6924.2010.01528.x
16. Lepikhin A.M., Makhutov N.A., Moskvichev V.V., Chernyaev A.P. Veroyatnostnyy risk-analiz konstruktsii tekhnicheskikh sistem [Probabilistic risk analysis of technical systems constructions]. Novosibirsk: Nauka; 2003: 174.
17. Kelly D., Smith Ch. Bayesian inference for probabilistic risk assessment. A practitioner's guidebook. Springer Series in Reliability Engineering. London: Springer-Verlag Limited; 2011: 238. DOI:10.1007/978-1-84996-187-5.
18. Dahmen U., Rossman J. Experimentable digital twins for a modeling and simulation-based engineering approach. Avaiable at: `https://www.researchgate.net/publication/329298561` (accessed 05.08.2020).
19. Qi Q., Tao F., Hu T., Anwer N., Liu A., Wei Y., Wang L. Enabling technologies and tools for digital twin. Available at: `https://doi.org/10.1016/j.jmsy.2019.10.001` (accessed 05.08.2020).
20. Computation stochastic mechanics. Ed. P.D. Spanos, C.A. Brebbia. Springer Netherlands; 1991: 898.
21. Soize C. Stochastic models of uncertainties in computational mechanics. American Society of Civil Engineers. 2012: 125–134. ISBN:978-0-7844-7686-4.
22. Shayanfar M.A., Barkhordari M.A., Roudak M.A. An adaptive importance sampling-based algorithm using the first order method for structural reliability. International Journal of Optimization in Civil Engineering. 2017; 7(1):93–107.
23. Au S.K., Beck J.L. Estimation of small failure probabilities in high dimensions by subset simulation. Probabilistic Engineering Mechanics. 2001. 16:263–277. DOI:10.1016/S0266-8920(01)00019-4.