МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ ПО ВЕРОЯТНОСТНОМУ ПРОГНОЗИРОВАНИЮ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ. Часть 3. МОДЕЛИРОВАНИЕ СЛОЖНЫХ СИСТЕМ. ИНТЕГРАЛЬНЫЙ АНАЛИЗ

Костогрызов А. И.[1], Нистратов А. А.[2], Голосов П. Е.[3]

DOI: 10.21681/2311-3456-2025-2-2-19

Окончание

Настоящая 3-я часть работы является окончанием статьи, 1-я часть которой опубликована в №3-2024 журнала «Правовая информатика», а 2-я часть – в №6-2024 журнала «Вопросы кибербезопасности».

Цель всей работы: *помочь системным аналитикам, участвующим в оценке качества функционирования информационных систем (ИС) при их создании, эксплуатации, модернизации, развитии, сформировать облик комплексной методики вероятностного прогнозирования, применимый в интересах обеспечения качества и безопасности, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле ИС.*

Цель 3-й части работы: *завершить детализацию общих методических положений по вероятностному прогнозированию качества функционирования ИС (с учетом укрупненного описания подхода в 1-й части статьи [1] и изложения основ детализации моделирования с помощью «черных ящиков» во 2-й части статьи [2]) путем предложения:*

- *формализации сложных моделируемых систем, состоящих из параллельно-последовательных структур, формируемых из «черных ящиков» и объединяемых с использованием логических соединений «И», «ИЛИ»;*
- *методов системного анализа качества функционирования ИС;*
- *основных компонентов облика комплексной методики вероятностного прогнозирования качества функционирования ИС, применимых системными аналитиками в интересах обеспечения качества и безопасности, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле конкретных ИС.*

Методы исследования включают: *методы теории вероятностей, методы системного анализа. В качестве моделируемой системы формально выступают «черные ящики» и сложные системы в виде параллельно-последовательных структур, формируемых из «черных ящиков», объединяемых с использованием логических соединений «И», «ИЛИ». Получаемые результаты математического моделирования используются в интерпретации к исходной ИС, в интересах которой проводятся соответствующие расчеты.*

Результат работы в целом: *на основе результатов исследований, представленных в [1, 2], созданы методические положения, формирующие основные компоненты облика комплексной методики вероятностного прогнозирования качества функционирования ИС согласно ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы». Использование предложенных методических положений призвано помочь системным аналитикам сформировать облик разносторонней комплексной методики вероятностного прогнозирования, применимый в интересах обеспечения качества и безопасности, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле конкретной ИС.*

Научная новизна работы: *с широким внедрением средств и систем современных информационных технологий проблематика, связанная со всесторонним изучением качества функционирования ИС, остается остро актуальной. Несмотря на то, что появилось множество стандартов системной инженерии, которые рекомендуют использование вероятностного системного анализа для различного рода систем, на практике формирование комплекса методик, применимого для прогнозирования показателей качества, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений в жизненном цикле ИС, вызывает у системных аналитиков практические затруднения. Эти затруднения и использование субъективных оценок связаны не только с многогранностью самого понятия качества функционирования ИС, но и сложностью математической формализации*

1 Костогрызов Андрей Иванович, доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва. Россия. E-mail: Akostogr@gmail.com

2 Нистратов Андрей Андреевич, кандидат технических наук, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва. Россия. E-mail: Andrey.nistratov@gmail.com

3 Голосов Павел Евгеньевич., кандидат технических наук, директор Института общественных наук Российской академии народного хозяйства и государственной службы (РАНХиГС), Москва. Россия. E-mail: pgolosov@gmail.com

с учетом специфики каждой системы. В итоге многие важные аспекты оказываются вне поля рассмотрения аналитика, специфичные измеряемые показатели качества оказываются несоизмеримыми по единой количественной шкале, а обратные аналитические задачи упреждающего противодействия угрозам в жизненном цикле системы и ее составных элементов не решаются. Т.е. на практике возникает противоречие между потребностями в системной аналитике ИС и возможностями для решения актуальных задач системного анализа. Для преодоления этого противоречия в предлагаемых методических положениях сформулирована общая цель функционирования ИС различного функционального приложения – это обеспечение надежности и своевременности предоставления необходимой информации, полноты, достоверности и безопасности используемой информации для последующего применения по назначению. Предложенные в статье основные компоненты облика комплексной методики вероятностного прогнозирования качества функционирования ИС определили научную новизну данной работы, ориентированной как раз на достижение этой общей сформулированной цели функционирования ИС.

Ключевые слова: *вероятность, модель, прогнозирование, риск, система, системный анализ, угроза.*

1. Введение

Методические положения предназначены для вероятностного прогнозирования качества функционирования рассматриваемой ИС (далее по тексту – «Системы» с заглавной буквы) как сложной системы и ее составных элементов (которые также могут представлять собой какую-либо систему) с использованием понятия «моделируемой системы». Для общности изложения сложная система определена как система, обладающая эмерджентными свойствами, которые не могут быть сведены к свойствам отдельных ее подсистем или элементов. В свою очередь, под «моделируемой системой» понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения.

В 1-й части статьи [1] обоснована актуальность работы, предложен общий подход к вероятностному прогнозированию качества функционирования ИС, основанный на использовании моделей и методов ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы». Подход представлен в виде основных методических положений, раскрывающих базовые термины и определения, рассматриваемые объекты ИС, цель и задачи прогнозирования, принятые предположения, условия и допущения, оцениваемые показатели, перечень вероятностных моделей, порядок проведения моделирования, интерпретация и системный анализ результатов расчетов. Тем самым по-крупному описаны контуры облика комплексной методики вероятностного прогнозирования качества функционирования ИС.

Во 2-й части статьи [2] для детализации общих методических положений 1-й части предложены вероятностные модели, представляющие систему в виде «черного ящика», когда известны исходные данные для моделирования и выходные результаты, но неизвестно внутреннее устройство системы. Были описаны следующие модели и метод: «Модели для оценки надежности предоставления информации и выполнения операций»; «Модели для оценки своевременности предоставления информации и выполнения операций»; «Модели для оценки полноты используемой информации»; «Модели для оценки актуальности используемой информации»; «Модели для оценки безошибочности информации после контроля»; «Модели для оценки корректности информации после обработки»; «Модели для оценки безошибочности действий пользователей и персонала»; «Модели для оценки защищенности системы от опасного программно-технического воздействия»; «Модели для оценки защищенности активов от несанкционированного доступа»; «Модели для оценки конфиденциальности используемой информации», «Метод использования универсальной вспомогательной модели показателя для определения исходных данных в расчетах». Тем самым представленные модели и метод охватывают базовые основы для практического воплощения основной идеи оценки качества функционирования ИС на вероятностном уровне достижения общей цели – обеспечения надежности и своевременности предоставления необходимой информации, полноты, достоверности и безопасности используемой информации для последующего применения по назначению.

В настоящей 3-й части работы для детализации облика комплексной методики вероятностного прогнозирования качества функционирования ИС описаны «Методы учета дополнительных специфических требований и сложности моделируемой системы» и «Методы оценки обобщенных и интегрального показателей качества функционирования ИС». Даны рекомендации по применению предложенных в работе моделей и методов.

На примерах продемонстрировано, как предложенный облик комплексной методики вероятностного прогнозирования качества функционирования ИС может быть применен при прогнозировании

частных, обобщенных и интегрального показателей рисков, обосновании допустимых рисков, выявлении существенных угроз и поддержке принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле ИС, см. также [3–20].

Тем самым завершено изложение методических положений по вероятностному прогнозированию качества функционирования ИС, замысел и базовая детализации которых были представлены в [1-2].

Примечание. Детализированный в статье перечень вероятностных моделей и методов не исчерпывает всего множества существующих подходов, практически приемлемых для достижения поставленных целей применения в прогнозировании качества функционирования ИС.

2. Общий подход к моделированию

За основу предлагаемого подхода к моделированию принят подход, изложенный в разные годы в приложении к различным системам [4, 5, 10, 11] и доведенный до реализации на уровне ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы», ГОСТ Р 59991-2022 «Системная инженерия. Системный анализ процесса управления рисками для системы». С учетом неопределенностей расчет

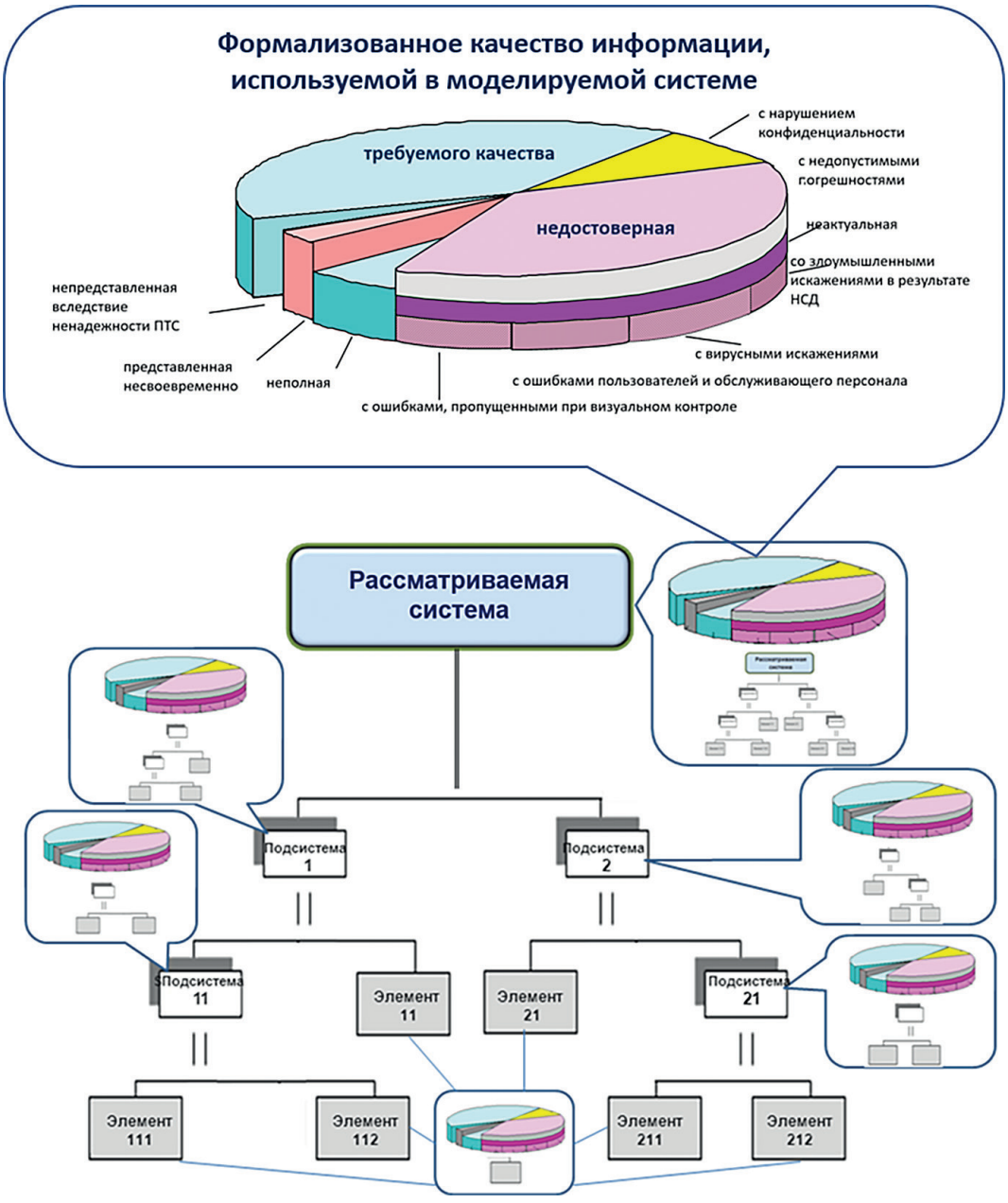

Рис. 1. Абстрактная иллюстрация качества используемой информации и пример декомпозиции рассматриваемой сложной системы до уровня составных подсистем и элементов

вероятностных показателей делается в принятых предположениях, условиях и допущениях с использованием моделей и методов [1-2].

В зависимости от целей системного анализа рассматриваемая сложная система может быть декомпозирована до уровня составных подсистем и элементов (каждый элемент логически представляется как «черный ящик» со своим пространством элементарных событий) – см. рис. 1. В этом случае настоящие методические положения могут быть применимы к подсистемам, каждому из составных элементов и сложной системе в целом, компонуемой из этих элементов.

Расчет частных показателей осуществляется по каждому из элементов с использованием моделей, детально описанных в [2]. Обобщенные показатели формируются из частных с учетом специфики и требований системного анализа составных элементов и подсистем. Показатель интегрального риска нарушения качества функционирования ИС позволяет оценить способность Системы обеспечить надежность и своевременность предоставления, полноты, достоверности и безопасности используемой информации и соблюдение требований по защите информации и, при необходимости, дополнительных специфических требований. Обобщенные и интегральный риски используют для сравнения весомости прогнозируемых частных рисков, выявления явных и скрытых угроз и поддержки принятия решений для задач системного анализа.

3. Методы учета дополнительных специфических требований и сложности моделируемой системы

Описанные в [2] модели применимы для проведения оценок, когда моделируемая система представляется в виде «черного ящика» со своим пространством элементарных событий (состояний), логически характеризующим его целостность. В условиях такого представления, когда известны исходные данные для моделирования и выходные результаты, но неизвестно внутреннее устройство системы, одни и те же модели могут быть использованы для расчетов показателей, различных по области их приложения, т.е. различных по семантическому наименованию и содержанию в специфической области их приложения, но идентичных по математическому смыслу и методам расчета. Тем самым дополнительные специфические требования в таких моделях учитываются на уровне значений используемых исходных данных. Например, для оценки надежности предоставления информации и выполнения операций, безошибочности действий пользователей и персонала системы и безопасности информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий применяется идентичная модель, описанная в ГОСТ Р 59341, приложениях В.3.2, В.3.8, В.3.9.2 и представленная в [2] в рамках «Модели для оценки надежности предоставления информации и выполнения операций», «Модели для оценки безошибочности действий пользователей и персонала», «Модели для оценки защищенности системы от опасного программно-технического воздействия».

При применении этих моделей с учетом специфики значения времени системной диагностики и восстановления нарушенной целостности моделируемой системы могут различаться. Так, в упомянутых моделях ГОСТ Р 59341 время системного контроля (диагностики) по составному элементу включает в себя время восстановления целостности и равно в среднем $T_{диаг}$. Вместе с тем в большинстве случаев на практике восстановление целостности при контроле не требуется, т.к. ее сохранение имеет место быть (нарушений не было). Но если по результатам контроля требуются дополнительные меры для восстановления нарушенных возможностей моделируемой системы в течение времени $T_{восст}$, то для расчетов усредненное время контроля $T_{диаг}$ должно быть увеличено (если $T_{диаг} < T_{восст}$) или уменьшено (если $T_{диаг} > T_{восст}$) с учетом частоты восстановлений. В этом случае для повышения адекватности моделирования усредненное время контроля может быть вычислено итеративно с заданной точностью:

- 1-я итерация определяет $T^{(1)}_{диаг} = T_{диаг}$, задаваемое на входе модели.

Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемых возможностей (т. е. в рамках времени диагностики);

- 2-я итерация осуществляется после расчета риска $R^{(1)}$ по исходным данным после 1-й итерации

$$T^{(2)}_{диаг} = T^{(1)}_{диаг} \cdot (1 - R^{(1)}) + R^{(1)} \cdot T_{восст}, \quad (1)$$

где $R^{(1)}$ – риск нарушения целостности моделируемой системы с исходным для расчетов значением $T^{(1)}_{диаг}$, этот риск вычисляется с использованием упомянутых моделей ГОСТ Р 59341. Здесь, поскольку на 1-й итерации $T^{(1)}_{диаг}$ не учитывает времени восстановления, рассчитываемый риск $R^{(1)}$ начинает приближаться к более адекватному значению (учитывающему частоту нарушений);

- ... r-я итерация осуществляется после расчета риска $R^{(r-1)}$ по исходным данным после $(r-1)$-й итерации

$$T^{(r)}_{диаг} = T^{(r-1)}_{диаг} \cdot (1 - R^{(r-1)} + R^{(r-1)}) \cdot T_{восст}, \quad (2)$$

где $R^{(r-1)}$ вычисляют по упомянутым моделям ГОСТ Р 59341, но в качестве исходного уже выступает $T^{(r-1)}_{диаг}$, рассчитанное на предыдущем шаге ите-

рации. Здесь в большей степени учитывается время восстановления с частотой, стремящейся к реальной. Соответственно риск $R^{(r-1)}$ так же приближается к более адекватному значению.

С увеличением r указанная последовательность $T^{(r)}_{\text{диаг}}$ сходится, и для дальнейших расчетов используется значение, отличающееся от точного предела $T^{(\infty)}_{\text{диаг}}$ на величину, пренебрежимо малую по сравнению с задаваемой изначально точностью ε расчетов при итерации:

$$|R^{(r)} - R^{(r-1)}| \le \varepsilon.$$

Такой способ позволяет вместо одного исходного данного (среднего времени системной диагностики, включая восстановление нарушенной целостности моделируемой системы) учитывать два, которые могут быть различны по своему значению: $T_{\text{диаг}}$ – среднее время системной диагностики возможностей в моделируемой системе и $T_{\text{восст}}$ – среднее время восстановления нарушенных возможностей в моделируемой системе.

Учет сложности декомпозируемой моделируемой системы (см. например, структуру на рис. 1) возможен с использованием нижеследующего способа.

Способ позволяет переходить от оценок моделируемых систем или отдельных элементов, представляемых в виде «черного ящика», к оценкам систем сложной параллельно-последовательной логической структуры с учетом принятых условий и допущений (см. [1]). В формируемой структуре, исходя из реализуемых технологий для моделируемой системы, состоящей из двух элементов, указывается характер их логического соединения. Если два элемента соединяются последовательно, что означает логическое соединение «И» (см. рис. 2), то на принятом пространстве элементарных событий это интерпретируется так: «целостность системы обеспечена» в течение времени t, если «И» 1-й элемент, «И» 2-й элемент сохраняют свои возможности по функционированию согласно назначению в течение этого времени, т.е. для каждого из них «целостность элемента обеспечена» в течение времени t. Если два элемента соединяются параллельно, что означает логическое соединение «ИЛИ» (см. рис. 3), это интерпретируется так: система сохраняет возможности по функционированию согласно назначению в течение времени t, если 1-й элемент «ИЛИ» 2-й элемент сохраняют свои возможности в течение этого времени, т.е. если хотя бы для одного из них «целостность элемента обеспечена» в течение времени t.

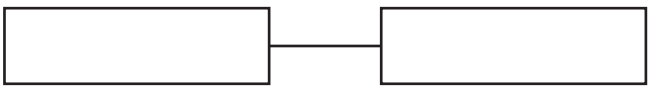

Рис. 2. Система из последовательно соединенных элементов («И»)

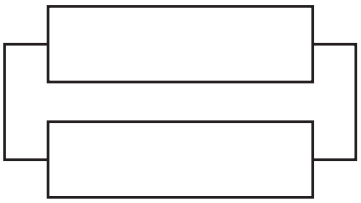

Рис. 3 Система из параллельно соединенных элементов («ИЛИ»)

Для комплексной оценки в приложении к сложным системам используются рассчитанные на моделях вероятности нарушения целостности каждого из составных элементов за заданное время t. Тогда для простейшей структуры из двух независимых элементов вероятность нарушения целостности за время t определяется по формулам:

- для моделируемой системы из двух последовательно соединенных элементов

$$P(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)]; \quad (3)$$

- для моделируемой системы из двух параллельно соединенных элементов

$$P(t) = P_1(t) \cdot P_2(t), \quad (4)$$

где $P_m(t)$ — вероятность нарушения целостности m-го элемента за заданное время t, $m = 1, 2$.

Рекурсивное применение соотношений (3), (4) снизу-вверх по структуре (см., например, структуру на рис. 1) обеспечивает интегрированное получение соответствующих вероятностных оценок для системы сколь угодно сложной логической структуры с параллельно-последовательным логическим соединением элементов. Рекурсивное применение снизу-вверх означает первичное применение моделей сначала для отдельных системных элементов, представляемых в виде «черного ящика» в принятой сложной логической структуре моделируемой системы, затем, учитывая характер логического объединения («И» или «ИЛИ») в принятой структуре, по формулам (3) и (4) проводится расчет вероятности нарушения целостности за время t для объединяемых элементов. И так – до объединения на уровне сложной системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (3) или (4) от исходных параметров моделей, примененных в каждом из элементов. Это возможно, т.к. если для каждого элемента просчитать вероятность нарушения целостности m-го элемента за заданное время t для всех точек t от нуля до бесконечности, получится траектория функции распределения (ФР) времени нарушения целостности в зависимости от реализуемых мер контроля и восстановления нарушенных возможностей каждого из элементов, т. е. то, что используется

в формулах (3) и (4). Полученный численный вид ФР, построенной по точкам (например, с использованием расчетных программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения целостности каждого из элементов и моделируемой системы в целом. С точки зрения системной инженерии, это среднее время для системы простой и сложной структуры интерпретируется как виртуальная средняя наработка на нарушение целостности при вероятностном прогнозировании риска по предложенным моделям. Обратная величина этого среднего времени представляет собой частоту нарушений целостности в условиях определенных угроз и применяемых методов контроля и восстановления возможностей по обеспечению целостности для составных элементов. Именно эти исходные данные необходимы для последующего применения различных моделей «черного ящика».

При оценке рисков расчетной вероятности нарушения целостности системы сопоставляется возможный ущерб.

Примечание. Способы интерпретации и применения результатов расчетов на примере фрагмента ФР, демонстрирующего возможные варианты зависимостей ограничений на допустимый риск, экспоненциальную и более адекватную аппроксимацию ФР рассмотрены в [1].

4. Методы оценки обобщенных и интегрального показателей качества функционирования ИС

Обобщенные показатели для элементов, подсистемы, системы учитывают различные свойства, характеризующие качество. Интегральный показатель учитывает логическую структуру системы и поэлементные обобщенные показатели.

В интересах системного анализа результатов моделирования в оценках обобщенных и интегрального показателей качества функционирования ИС задают допустимые уровни для расчетных вероятностных показателей и совокупные условия α, которые могут по-своему характеризовать различные свойства качества применительно к элементу, подсистеме, системе. Для оценки обобщенных показателей указывают, какие элементы и/или подсистемы рассматриваются, какие частные показатели, характеризующие качество, используются при обобщении.

Условие α, касающееся надежности предоставления информации, формулируется в виде ограничений: $P_{\text{над предст}}(T_{\text{зад}}) \geq P_{\text{доп над}}(T_{\text{зад}})$ и возможный ущерб от нарушения не превышает допустимого (это – формулировка условия α для свойства надежности). Учет результатов моделирования с применением «Модели для оценки надежности предоставления информации и выполнения операций» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{над предст}}(T_{\text{зад}})$

$$Z_{\text{над предст}}(T_{\text{зад}}) = \begin{cases} 1, \text{ если условие надежности предоставления информации } \alpha \text{ выполнено,} \\ P_{\text{над предст}}(T_{\text{зад}}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для оценки своевременности предоставления информации используется понятие относительной доли своевременно обработанных в системе запросов $C_{\text{своевр}}$. Этот вспомогательный показатель охватывает лишь те типы запросов, для которых выполнены требования потребителя информации, этот показатель вычисляется по формуле

$$C_{\text{своевр}} = \sum_{i=1}^{I} \lambda_i P_{\text{св}\,i}(T_{\text{зад}\,i})[Ind(\alpha_1) + Ind(\alpha_2)] \,/\, \sum_{i=1}^{I} \lambda_i, \quad (5)$$

где λ_i – частота поступления на обработку запросов i-го типа на предоставление информации;

Критерий своевременности обработки каждого типа запросов устанавливается с использованием индикаторной функции $Ind(\alpha)$:

$$Ind(\alpha) = \begin{cases} 1, \text{ если условие } \alpha \text{ истинно,} \\ 0, \text{ если условие } \alpha \text{ ложно.} \end{cases}$$

При этом для i-го типа запросов условие своевременности α с учетом возможных ущербов определяется одним из условий α_1 или α_2:

- α_1 – условие, когда для i-го типа запросов задан критерий своевременности по среднему времени реакции и $T_i \leq T_{\text{зад}\,i}$.
- α_2 – условие, когда для i-го типа запросов задан вероятностный критерий своевременности и $P_{\text{св}\,i}(\tau_i \leq \mathrm{T}_{\text{зад}\,i}) \geq P_{\text{св зад}\,i}$.

Статистическими методами или с использованием моделей массового обслуживания, в т.ч. «Модели для оценки своевременности предоставления информации и выполнения операций» [2], определяются показатели $P_{\text{св}\,i}(\tau_i \leq \mathrm{T}_{\text{зад}\,i})$, T_i.

Для оценки интегрального риска условие своевременности предоставления информации α формулируется в виде условий α_1 или α_2 с добавлением, что в случае их нарушения возможный ущерб не превышает допустимого (это формулировка условия α по всем типам запросов). Учет результатов моделирования в интегральных оценках осуществляется с использованием индикатора своевременности обработки запросов $Z_{\text{своевр}}$:

$$Z_{\text{своевр}} = \begin{cases} 1, \text{ если условия своевременности } \alpha \text{ выполнены для всех типов запросов,} \\ C_{\text{своевр}}, \text{ если хотя бы одно условие не выполнено.} \end{cases}$$

Для оценки полноты информации задается допустимый уровень $P_{\text{доп полн}}$ и условие α. Условие α касается полноты оперативного отражения в системе новых объектов и явлений и формулируется в виде

ограничений: $P_{\text{полн}} \geq P_{\text{доп полн}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования с применением «Модели для оценки полноты используемой информации» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{полн}}$

$$Z_{\text{полн}} = \begin{cases} 1, \text{ если условие полноты отражения в системе объектов и явлений } \alpha \text{ выполнено,} \\ P_{\text{полн}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для оценки актуальности информации задаются допустимый уровень $P_{\text{доп акт}}$ и условие α. Условие α касается сохранения актуальности информации в системе на момент ее использования и формулируется в виде ограничений: $P_{\text{акт}} \geq P_{\text{доп акт}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования с применением «Модели для оценки актуальности используемой информации» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{акт}}$

$$Z_{\text{акт}} = \begin{cases} 1, \text{ если условие сохранения актуальности информации в системе } \alpha \text{ выполнено,} \\ P_{\text{акт}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для оценки безошибочности информации после контроля задаются допустимый уровень $P_{\text{доп безош}}$ и условие α. Условие α касается обеспечения безошибочности информации после контроля и формулируется в виде ограничений: $P_{\text{безош}} \geq P_{\text{доп безош}}$, и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования с применением «Модели для оценки безошибочности информации после контроля» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{безош}}$

$$Z_{\text{безош}} = \begin{cases} 1, \text{ если условие безошибочности информации после контроля } \alpha \text{ выполнено,} \\ P_{\text{безош}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для оценки корректности обработки информации задаются допустимый уровень $P_{\text{доп корр}}$ и условие α. Условие α касается обеспечения корректности обработки информации и формулируется в виде ограничений: $P_{\text{корр}} \geq P_{\text{доп корр}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования с применением «Модели для оценки корректности информации после обработки» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{корр}}$

$$Z_{\text{корр}} = \begin{cases} 1, \text{ если условие обеспечения корректности обработки информации } \alpha \text{ выполнено,} \\ P_{\text{корр}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для оценки влияния «человеческого фактора» задаются допустимый уровень $P_{\text{доп чел}}(T_{\text{зад}})$ и условие α. Условие α касается безошибочности действий пользователей и персонала системы и формулируется в виде ограничений: $P_{\text{чел}}(T_{\text{зад}}) \geq P_{\text{доп чел}}(T_{\text{зад}})$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования с применением «Модели для оценки безошибочности действий пользователей и персонала» [2] в интегральных оценках осуществляется с использованием индикатора $Z_{\text{чел}}(T_{\text{зад}})$

$$Z_{\text{чел}}(T_{\text{зад}}) = \begin{cases} 1, \text{ если условие безошибочности действий } \alpha \text{ выполнено,} \\ P_{\text{чел}}(T_{\text{зад}}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы упомянутых показателей-индикаторов $(1 - Z\ldots)$ в качестве вероятностного выражения соответствующего риска.

Рассмотрим метод оценки интегрального риска на примере учета основных свойств, характеризующих качество функционирования ИС (к таковым в рамках нижеследующего примера интеграции отнесем свойства надежности и своевременности предоставления информации, полноты и достоверности используемой информации, безошибочности действий пользователей и персонала), и специфических свойств (к таковым в рамках нижеследующего примера интеграции отнесем свойства безопасности используемой информации). Такое разделение чисто условное, оно принято для облегчения понимания алгоритма расчета обобщенных и интегрального рисков по известным составным показателям.

Тогда, если положить, что специфические требования к системе связаны с защитой информации, то в сопоставлении с возможным ущербом интегральный риск нарушения качества функционирования ИС с учетом специфических требований $R_{\text{интегр}}(T_{\text{зад}})$ для прогнозного периода $T_{\text{зад}}$ может быть определен по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - [1 - R_{\text{осн}}(T_{\text{зад}})] \cdot [1 - R_{\text{специф}}(T_{\text{зад}})], \quad (6)$$

где $R_{\text{осн}}(T_{\text{зад}})$ — вероятность нарушения основных свойств качества функционирования ИС в течение периода прогноза $T_{\text{зад}}$ без учета специфических требований, рассчитывается с использованием «Модели для оценки надежности предоставления информации и выполнения операций»; «Модели для оценки своевременности предоставления информации и выполнения операций»; «Модели для оценки полноты используемой информации»; «Модели для оценки актуальности используемой информации»; «Модели для оценки безошибочности информации после

контроля»; «Модели для оценки корректности информации после обработки»; «Модели для оценки безошибочности действий пользователей и персонала» [2]; $R_{специф}(T_{зад})$ — вероятность нарушения специфических требований к ИС (ниже – на примере требований по защите информации) в течение периода прогноза $T_{зад}$, рассчитывается с использованием «Модели для оценки защищенности системы от опасного программно-технического воздействия», «Модели для оценки защищенности активов от несанкционированного доступа», «Модели для оценки конфиденциальности используемой информации» [2].

Вероятность нарушения основных свойств качества функционирования ИС $R_{осн}(T_{зад})$ в течение периода прогноза определяется как дополнение до единицы вероятности того, что обеспечена надежность и своевременность предоставления запрашиваемой или выдаваемой принудительно информации, полнота, достоверность используемой информации и безошибочность действий пользователей и персонала (учитывая возможные ограничения на расчетные вероятностные показатели), т. е., как обобщенный показатель риска нарушения основных свойств качества функционирования ИС, $R_{осн}(T_{зад})$, учитывающий при необходимости структурную сложность составных компонентов, может быть рассчитан по формуле:

$$R_{осн}(T_{зад}) = 1 - Z_{над\,предст}(T_{зад}) \cdot Z_{своевр} \cdot Z_{полн} \cdot Z_{акт} \cdot \cdot Z_{безош} \cdot Z_{корр} \cdot Z_{чел}(T_{зад}), \quad (7)$$

где $Z_{над\,предст}(T_{зад})$ — вероятностный индикатор надежности предоставления информации, учитывающий вероятность надежного предоставления информации в системе в течение заданного периода прогноза $T_{зад}$ и соответствующие условия α; $Z_{своевр}$ — вероятностный индикатор своевременности обработки запросов, учитывающий относительную долю своевременно обработанных в системе запросов и соответствующие условия α; $Z_{полн}$ — вероятностный индикатор полноты оперативного отражения в системе новых объектов и явлений, учитывающий вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений, и соответствующие условия α; $Z_{акт}$ — вероятностный индикатор актуальности информации в системе, учитывающий вероятность сохранения актуальности информации на момент ее использования и соответствующие условия α; $Z_{безош}$ — вероятностный индикатор безошибочности информации в системе, учитывающий вероятность отсутствия ошибок в информации после ее контроля и соответствующие условия α; $Z_{корр}$ — вероятностный индикатор корректности обработки информации в системе, учитывающий вероятность получения корректных результатов обработки информации и соответствующие условия α; $Z_{чел}(T_{зад})$ — вероятностный индикатор безошибочных действий пользователей и персонала системы, учитывающий вероятность безошибочных действий пользователей и персонала в течение заданного периода прогноза и соответствующие условия α.

В частном случае рассматриваемого разделения свойств на основные и специфические вероятность нарушения специфических требований к ИС (на примере требований по защите информации) в течение периода прогноза $R_{специф}(T_{зад})$ применяются модели угроз безопасности используемой информации для учета защищенности от опасных программно-технических воздействий, от НСД, сохранения конфиденциальности информации (при необходимости применяется аналитическая адаптация моделей). При этом вероятность $R_{специф}(T_{зад})$ с учетом возможных ущербов может рассматриваться как обобщенный показатель риска нарушения специфических свойств качества функционирования ИС (дополнительно к основным). Учитывая при необходимости структурную сложность составных компонентов, показатель $R_{специф}(T_{зад})$ может быть определен по формуле:

$$R_{специф}(T_{зад}) = 1 - P_{возд}(T_{зад}) \cdot P_{НСД}(T_{зад}) \cdot P_{конф}(T_{конф}), \quad (8)$$

где $P_{возд}(T_{зад})$ — вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $T_{зад}$; $P_{НСД}(T_{зад})$ – вероятность обеспечения защищенности активов системы от НСД в течение заданного периода прогноза $T_{зад}$ (или без привязки к этому периоду – $P_{НСД}$); $P_{конф}(T_{конф})$ — вероятность сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $T_{конф}$ (период $T_{конф}$ может играть роль периода прогноза $T_{зад}$).

5. Пример оценки надежности функционирования сложной системы

Развивая примеры из 2-й части статьи [2], рассмотрим функционирование системы дистанционного контроля (СДК) на гипотетичном предприятии опасного производства, например, угольной шахты, где контролируемые в режиме реального времени действия людей и оборудования происходят во взрывоопасных условиях, когда требуются обязательные вентиляция и дегазация эксплуатационной среды. СДК включает в свой состав контролируемые комплекс главных вентиляторных установок (ГВУ), комплекс модульных дегазационных установок (МДУ) и газоотсасывающую установку. Оценивается вероятность надежного предоставления информации и выполнения операций в СДК в течение заданного периода прогноза $P_{над\,предст}(T_{зад})$, а также вероятностный индикатор надежности предоставления

Рис. 4. Моделируемая система, логически структурированная до составных объектов анализа, охваченных функциональными возможностями СДК

информации $Z_{\text{над предст}}(T_{\text{зад}})$ для оценки обобщенного и интегрального показателей качества функционирования СДК.

Объектами анализа в примере являются комплекс ГВУ, комплекс МДУ и газоотсасывающая установка, охваченные функциональными возможностями СДК и являющиеся источниками информации для последующей обработки и использования по назначению (см. структуру сложной моделируемой системы на рис. 4).

Надежность предоставления используемой информации определяется надежностью функционирования средств СДК совместно с контролируемым оборудованием. Это означает, что надежность предоставления информации в СДК должна быть выше, чем надежность функционирования контролируемого оборудования.

Логическая интерпретация событий для моделируемой системы следующая: надежность функционирования моделируемой системы обеспечена, когда обеспечена надежность функционирования объектов, охваченных функциональными возможностями СДК:

- «И» ГВУ (в том числе ГВУ 1 «И» ГВУ 2), имеющих различное местоположение в комплексе ГВУ и отличающихся характеристиками по безотказности;
- «И» МДУ (в том числе «И» МДУ 1, «И» МДУ 2, «И» МДУ 3), также имеющих различное местоположение в комплексе МДУ и отличающихся характеристиками по безотказности;
- «И» газоотсасывающей установки.

В свою очередь, каждая из ГВУ (т. е. ГВУ 1 и ГВУ 2) находится в работоспособном состоянии (т.е. признается функционирующей надежно), если «ИЛИ» вентилятор 1, «ИЛИ» вентилятор 2 находится в работоспособном состоянии (это достигается резервированием вентиляторов). Каждая из МДУ (т.е. МДУ 1 и МДУ 2) находится в работоспособном состоянии (т. е. признается функционирующей надежно), если «ИЛИ» насос 1, «ИЛИ» насос 2 в их составе находится в работоспособном состоянии (это достигается резервированием насосов). В МДУ 3 резервный насос отсутствует (см. рис. 4).

Исходные данные для моделирования отражены в таблице 1, для их определения может быть использована универсальная вспомогательная модель показателя (УВМП), рассмотренная в [2] – см. также ГОСТ Р 59349 «Системная инженерия. Защита информации в процессе системного анализа».

Моделирование осуществлено с использованием рекомендаций раздела 2 и «Модели для оценки

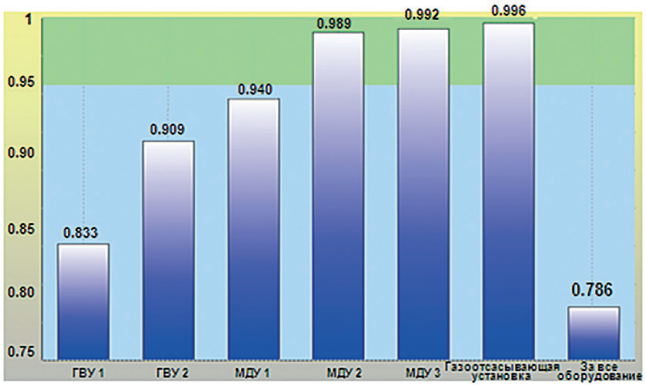

Рис. 5. Оценки для вероятности надежного предоставления информации в СДК в течение месяца за все оборудование и поэлементно: за ГВУ 1, 2, МДУ 1, 2, 3 и газоотсасывающую установку

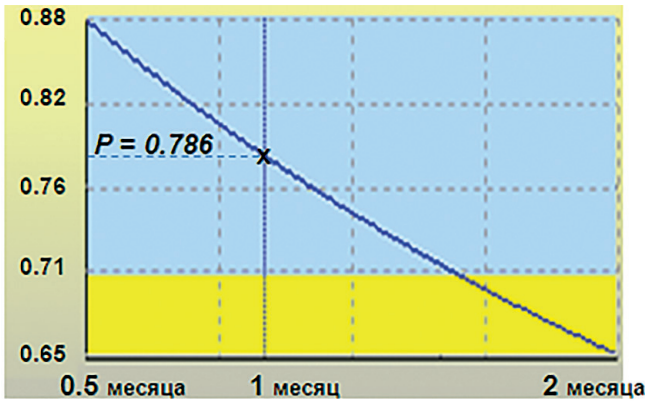

Рис. 6. Зависимость вероятности надежного предоставления информации в СДК (за все оборудование) от периода прогноза длительностью от 0,5 месяца до 2 месяцев

Таблица 1.

Исходные данные для моделирования

Исходные данные	Значения и комментарии					
	Комплекс ГВУ		Комплекс МДУ			Газоотсасывающая установка
	ГВУ 1 (для каждого вентилятора)	ГВУ 2 (для каждого вентилятора)	МДУ 1 (для каждого насоса)	МДУ 2 (для каждого насоса)	МДУ 3	
σ – частота возникновения источников угроз (например, выхода значений контролируемых параметров за границы рабочего диапазона)	1 раз в месяц	1 раз в 2 мес. (т. е. безотказность каждого вентилятора в 2 раза выше по сравнению с ГВУ 1)	1 раз в 3 мес. (т. е. безотказность каждого насоса в 3 раза выше по сравнению с ГВУ 1)	1 раз в 6 мес. (т. е. безотказность каждого насоса в 2 раза выше по сравнению с МДУ 1)	1 раз в год (т. е. в 4 раза выше по сравнению с МДУ 1)	1 раз в 2 года (т. е. в 24 раза выше по сравнению с ГВУ 1 и в 8 раз выше по сравнению с МДУ 1)
β – среднее время развития угроз с момента возникновения источников угроз до нарушения (например, выхода значений контролируемых параметров за границы нормативного диапазона)	30 минут (оценка среднего времени до возгорания метана после отказа ГВУ, МДУ или газоотсасывающей установки)					
$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики	5 минут (с учетом переключения внимания диспетчера на выполнение разных функций)					
$T_{диаг}$ – среднее время диагностики	1 минута (включая необходимую отдачу распоряжений)					
$T_{восст}$ – среднее время восстановления после выявления нарушений	20 минут (оценка среднего времени реакции ответственного лица на сигналы СДК о предпосылках возникновения опасных ситуаций)					
$T_{зад}$ – задаваемая длительность периода прогноза	1 месяц (период времени, в течение которого возможно принятие упреждающих мер, направленных на поддержание рисков в допустимых пределах)					

надежности предоставления информации и выполнения операций» [2].

Системный анализ результатов расчетов показал, что при ориентации на надежность функционирования всех составных элементов моделируемой системы (ГВУ 1, 2, МДУ 1, 2, 3 и газоотсасывающей установки) нижняя оценка вероятности надежного предоставления информации в СДК в течение месяца за все оборудование равна $P_{над\ предст}(T_{зад}) = 0{,}786$ (см. рис. 5).

Узким местом является надежность функционирования главной вентиляторной установки ГВУ 1 – вероятность надежного функционирования в течение месяца составила 0,833. Такое сравнительно низкое значение объясняется тем, что при прочих равных условиях наработка вентиляторов ГВУ 1 на отказ составляет 1 месяц, что в разы меньше аналогичной наработки на отказ для вентиляторов ГВУ 2, насосов модульных дегазационных установок МДУ 1, 2, 3 и газоотсасывающей установки.

В свою очередь, анализ зависимости вероятности надежного предоставления информации в СДК от периода прогноза (см. рис. 6) позволяет обосновать рекомендацию: сроки планирования и реализации мер, связанных с поддержанием надежности функционирования средств СДК не должны превышать двух недель, при этом среднее время диагностики с использованием СДК должно быть не более 1 мин, а среднее время реакции ответственного лица на сигналы СДК о предпосылках возникновения опасных ситуаций не должно превышать 20 мин. В этом случае вероятность надежного предоставления информации превысит 0,88, что более чем в 7 раз превысит вероятностное значение риска нарушения надежности [0,88 / (1 – 0,88) ≈ 7,3].

Рис. 7. Моделируемая система для оценки защищенности СДК от опасного программно-технического воздействия

Для расчета интегрального риска при ограничениях на вероятность надежного предоставления информации в СДК не ниже 0,95 индикатор надежности предоставления информации в течение месяца $Z_{\text{над предст}}(T_{\text{зад}})$ также будет равен $P_{\text{над предст}}(T_{\text{зад}}) = 0{,}786$, т.е. $Z_{\text{над предст}}(T_{\text{зад}}) = 0{,}786$. Более того, учитывая математическую идентичность моделей для оценки надежности предоставления информации и безошибочности действий пользователей и персонала системы, отслеживающего состояние оборудования, не перегружая работу подобными расчетами, по аналогии положим, что вероятностный индикатор безошибочных действий пользователей и персонала системы $Z_{\text{чел}}(T_{\text{зад}})$ при расчете обобщенного показателя положим равным 0,786.

6. Пример оценки защищенности сложной системы от опасных программно-технических воздействий

Пример демонстрирует подход к оценке вероятности отсутствия опасного программно-технического воздействия на СДК в течение заданного периода прогноза $P_{\text{возд}}(T_{\text{зад}})$. Объектами анализа являются программное обеспечение и информационные массивы СДК, используемые при мониторинге функционирования комплекса ГВУ, комплекса МДУ и газоотсасывающей установки. Согласно модели угроз безопасности информации, принятой руководством предприятия, для СДК моделируемый сценарий предполагает маскировку опасных программно-технических воздействий под обычные отказы оборудования. Структура моделируемой системы для оценки защищенности СДК от опасных программно-технических воздействий представлена на рис. 7. Она логически связана со структурами, представленными на рис. 4, однако все аспекты зависимости рассматриваются на уровне активов, представимых как «черные ящики».

Исходные данные для оценки вероятности отсутствия опасного программно-технического воздействия на СДК представлены в таблице 2.

Остальные исходные данные аналогичны данным из таблицы 1:

- среднее время между окончанием предыдущей и началом очередной диагностики $T_{\text{меж}}$ составляет 5 мин с учетом переключения внимания диспетчера на выполнение разных функций;
- среднее время диагностики $T_{\text{диаг}}$ = 1 мин, включая необходимую отдачу распоряжений;
- среднее время восстановления после выявления нарушений $T_{\text{восст}}$ = 20 мин (это среднее время

Таблица 2.

Исходные данные для оценки защищенности СДК от опасных программно-технических воздействий

Исходные данные	Значения и комментарии					
	Программное обеспечение и информационные массивы СДК, используемые при мониторинге функционирования предприятия					
	Комплекс ГВУ		Комплекс МДУ			Активы газоотсасывающей установки
	Активы ГВУ 1	Активы ГВУ 2	Активы МДУ 1	Активы МДУ 2	Активы МДУ 3	
σ – частота возникновения источников угроз	1 раз в месяц	1 раз в 2 мес. (т. е. безотказность каждого вентилятора в 2 раза выше по сравнению с ГВУ 1)	1 раз в 3 мес. (т. е. безотказность каждого насоса в 3 раза выше по сравнению с ГВУ 1)	1 раз в 6 мес. (т. е. безотказность каждого насоса в 2 раза выше по сравнению с МДУ 1)	1 раз в год (т. е. в 4 раза выше по сравнению с МДУ 1)	1 раз в 2 года (т. е. в 24 раза выше по сравнению с ГВУ 1 и в 8 раз выше по сравнению с МДУ 1)
β – среднее время развития угроз с момента возникновения источников угроз до нарушения	1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток)					

переинсталляции программного обеспечения и восстановления информационных массивов);

- задаваемая длительность периода прогноза $T_{зад}$ = 1 мес.

Моделирование осуществлено по этим исходным данным с использованием рекомендаций раздела 2 и «Модели для оценки защищенности системы от опасных программно-технических воздействий» [2].

Системный анализ результатов расчетов показал, что при ориентации на противодействие составных элементов моделируемой системы опасным компьютерным воздействиям оцениваемая вероятность отсутствия опасного программно-технического воздействия на каждый из активов в течение месяца будет не ниже 0,998 (см. рис. 8). По этому показателю защищенности все активы СДК в моделируемых условиях приблизительно равнопрочны.

В свою очередь анализ зависимости вероятности отсутствия опасного программно-технического воздействия от периода прогноза (см. рис. 9) позволил установить: в условиях примера защищенность программного обеспечения и информационных массивов СДК будет обеспечена в течение периода до 2 месяцев с вероятностью не ниже 0,992.

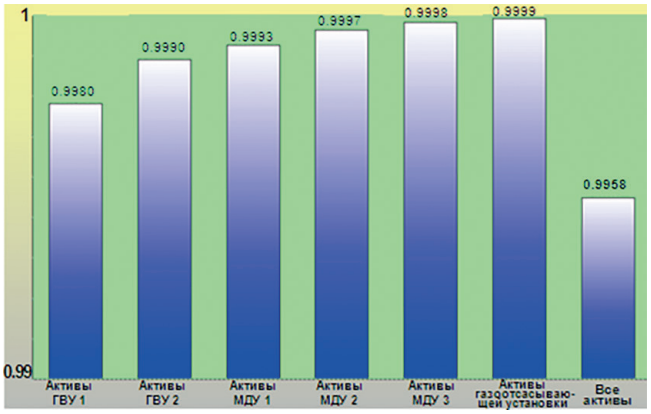

Рис. 8. Оценки вероятности отсутствия опасного программно-технического воздействия в течение месяца

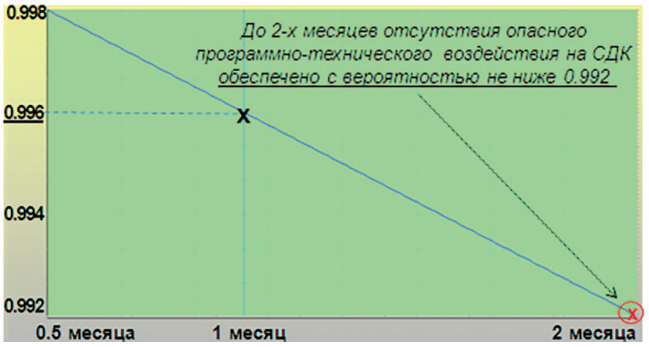

Рис. 9. Зависимость вероятности отсутствия опасного программно-технического воздействия на все активы от периода прогноза длительностью от 0.5 месяца до 2 месяцев

Для определенности при расчете обобщенного показателя с учетом требований по защите информации использована достигаемая вероятность отсутствия опасного программно-технического воздействия на СДК в течение месяца $P_{возд}(T_{зад}) = 0{,}996$.

7. Пример расчета обобщенных и интегрального рисков

Пример демонстрирует подход к прогнозированию обобщенных $R_{осн}(T_{зад})$ и $R_{специф}(T_{зад})$ и интегрального рисков $R_{интегр}(T_{зад})$ по формулам соответственно (7), (8) и (6) с учетом рассмотренных примеров в [2] и выше в разделах 5, 6.

С использованием результатов расчетных примеров получаются следующие окончательные результаты оценки для периода прогноза $T_{зад}$ = 1 мес:

- обобщенный показатель по формуле (7) – вероятность $R_{осн}(T_{зад})$ нарушения основных свойств качества функционирования ИС в течение периода прогноза без учета специфических требований (в примерах – без учета требований по защите информации [2])

$$R_{осн}(T_{зад}) = 1 - Z_{над\ предст}(T_{зад}) \cdot Z_{своевр} \cdot Z_{полн} \cdot Z_{акт} \cdot Z_{безош} \cdot$$
$$\cdot Z_{корр} \cdot Z_{чел}(T_{зад}) = 1 - 0{,}786 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 0{,}786 \approx 0{,}382;$$

Примечание. По результатам расчетов в примерах 2-й части статьи [2] значения индикаторов $Z_{своевр}$, $Z_{полн}$, $Z_{акт}$, $Z_{безош}$, $Z_{корр}$ были приравнены 1, это означает, что условия своевременности предоставления информации, полноты, актуальности, безошибочности и корректности используемой информации выполнены, т.е. соответствующие угрозы качеству информации для рассматриваемой системы несущественны, имеющие место риски пренебрежимо малы;

- обобщенный показатель по формуле (8) – вероятность $R_{специф}(T_{зад})$ нарушения специфических требований к ИС в течение периода прогноза (на примере требований по защите информации с детализацией защищенности от опасных программно-технических воздействий и НСД, сохранения конфиденциальности информации [2])

$$R_{специф}(T_{зад}) = 1 - P_{возд}(T_{зад}) \cdot P_{НСД}(T_{зад}) \cdot P_{конф}(T_{конф}) =$$
$$= 1 - 0{,}996 \cdot 0{,}9975 \cdot 0{,}9993 = 0{,}0072;$$

- интегральный показатель по формуле (6) – с учетом возможного ущерба интегральный риск нарушения качества функционирования ИС с учетом специфических требований $R_{интегр}(T_{зад})$(в примерах – требований по защите информации)

$$R_{интегр}(T_{зад}) = 1 - [1 - 0{,}382]\ [1 - 0{,}0072] \approx 0{,}387.$$

Вывод: уровень риска нарушения специфических требований по защите информации при функционировании СДК в течение одного месяца (0,0072) в 54 раза меньше по сравнению с интегральным

риском (0,387). Качество используемой информации в СДК (полнота, актуальность, безошибочность и корректность используемой информации) – на приемлемом уровне. Главное узкое место – неудовлетворительная надежность оборудования предприятия, выявленная при системном анализе надежности предоставления информации в СДК, и принятая по аналогии с этими результатами опасность «человеческого фактора».

Тем самым в рамках примеров продемонстрированы способы разностороннего вероятностного прогнозирования качества функционирования ИС с использованием предложенных методических положений.

8. О применении результатов вероятностного прогнозирования качества функционирования ИС к решению задач системного анализа

Основной целью применения предложенных методических положений является получение объективных результатов количественного прогноза качества функционирования ИС для решения следующих задач системного анализа (в т.ч. в приложении к Системам более высоких уровней, включающих ИС в свой состав):

- задачи 1-го типа: прогнозирования значений показателей (в т.ч. рисков), интерпретации и анализа получаемых результатов, включая сравнение прогнозируемых значений показателей с допустимым уровнем на предмет выполнения задаваемых ограничений;
- задачи 2-го типа: обоснования допустимых рисков;
- задачи 3-го типа: определения существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на свойства рассматриваемой Системы (и/или ее элементов);
- задачи 4-го типа: определения и обоснования в жизненном цикле Системы упреждающих мер противодействия угрозам и условий снижения рисков или удержания рисков в допустимых пределах, обеспечивающих желаемые свойства рассматриваемой Системы (и/или ее элементов) при задаваемых ограничениях в задаваемый период прогноза;
- задачи 5-го типа: обоснования предложений по обеспечению и повышению качества функционирования рассматриваемой Системы (и/или ее элементов).

При решении задач 1-го типа прогнозирование рисков используют для формального решения задач системного анализа, связанных с ранним распознаванием и оценкой развития предпосылок к нарушению качества и/или безопасности Системы. В зависимости от целей решаемых задач прогнозируемый риск связывают с заранее определенным периодом прогноза (например, на час, сутки, неделю, месяц), с возможными сценариями возникновения и развития угроз, ожидаемых для этого периода. Для прогнозирования рисков при решении поставленных задач должны быть: определены потенциально существенные угрозы или условия, для которых при том или ином развитии событий возможно негативное воздействие на Систему (и/или ее элементы); реализованы сбор и обработка исходных данных, обеспечивающих применение моделей и методов; предусмотрены способы использования результатов математического моделирования.

При решении задач 2-го типа допустимые риски рассматриваются в качестве количественных норм эффективности мер противодействия угрозам. Значения допустимых рисков определяют применительно к расчетным показателям рисков в условиях возможных угроз в задаваемом периоде прогноза. Возможно обоснование допустимых рисков по прецедентному принципу или с использованием ориентации на риски, свойственные системе-эталону, которая выбирается в качестве аналога для моделируемой Системы.

Методы количественного обоснования допустимых рисков по прецедентному принципу должны предусматривать формирование статистики по состоявшимся фактам. В результате моделирования применительно к условиям различных произошедших событий формируют базу знаний, устанавливающую соответствие расчетных значений прогнозируемых рисков тем реальным событиям, которые состоялись и оказались свойственными этим ситуациям. Соответствие устанавливают по журналам регистрации инцидентов нарушений качества и/или безопасности системы). Учитывают собираемую статистику, из нее выбирают прецеденты нарушений. Расчетные значения рисков, свойственные состоявшимся нарушениям, определяют как недопустимые, а меньшие по сравнению с недопустимыми определяют как допустимые. Во множестве расчетных значений допустимых рисков выбирают максимальное значение, отвечающее задаваемым условиям функционирования системы. Его признают в качестве допустимого по факту прецедента. Это значение допустимого риска устанавливают в качестве нормы эффективности мер противодействия угрозам по прецедентному принципу и используют для формального решения задач системного анализа (например, по ГОСТ Р 59991).

При решении задач 3-го типа определение существенных угроз и условий выполняют с использованием прогнозирования рисков в случае необходимости учета различного рода неопределенностей

для Системы. При задаваемых условиях угроза признается существенной, если для нее расчетное значение риска при осуществлении возможных сценариев может превышать установленное значение соответствующего допустимого риска. При полном перечне существенных угроз рассматриваемые условия признаются существенными (применительно к конкретной угрозе или когда само условие как таковое представляет собой угрозу), если для них расчетные значения рисков превышают установленные значения допустимых рисков.

При решении задач 4-го типа с использованием моделирования обеспечивается поддержка принятия решений, связанных с определением и обоснованием упреждающих мер противодействия угрозам и условий снижения рисков или удержания рисков в допустимых пределах при задаваемых ограничениях и обеспечением баланса по критерию «эффективность — стоимость». При недопустимых значениях прогнозируемых рисков и/или при наступлении реальных нарушений должны быть выявлены их причины и определены меры для целенаправленного планового восстановления качества функционирования Системы на уровне рисков, не превышающих допустимые.

При решении задач 5-го типа на этапах создания или модернизации или развития Системы поддержки принятия решений по обоснованию предложений по повышению ее качества функционирования и/или безопасности должна быть основана на изучении значений расчетных показателей рисков при сроке прогноза от нескольких месяцев до нескольких лет. Возможности реализации этих предложений подлежат учету в долгосрочных планах организаций, отвечающих за создание и сопровождение Системы.

9. О формировании облика комплексной методики вероятностного прогнозирования качества функционирования ИС

В результате детализации предложенного стандартизованного подхода к прогнозированию качества функционирования ИС в работе раскрыты базовые термины и определения, рассматриваемые объекты ИС, принятые предположения, условия и допущения, возможные цели и задачи, подлежащие решению с применением результатов вероятностного прогнозирования, оцениваемые показатели, непосредственно приемлемые вероятностные модели, порядок проведения моделирования, интерпретация результатов расчетов на различных прикладных примерах и некоторые вопросы системного анализа в обеспечение качества и безопасности функционирования ИС.

За основу предлагаемого подхода к моделированию принят подход, изложенный в разные годы в приложении к различным системам и доведенный до реализации на уровне ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы», ГОСТ Р 59991-2022 «Системная инженерия. Системный анализ процесса управления рисками для системы».

Предложенные показатели обобщенных и интегрального рисков нарушения качества функционирования ИС позволяют оценить способность ИС обеспечить надежность и своевременность предоставления, полноту, достоверность и безопасность используемой информации и, при необходимости, дополнительных специфических требований. Обобщенные и интегральный риски могут быть использованы для сравнения весомости прогнозируемых частных рисков, выявления явных и скрытых угроз и поддержки принятия решений для задач системного анализа.

Тем самым в совокупности в результате исследований созданы основные компоненты облика комплексной методики вероятностного прогнозирования качества функционирования ИС, применимые системными аналитиками в интересах обеспечения качества и безопасности, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле ИС.

Заключение (по работе в целом)

1. Предложен системный подход к вероятностному прогнозированию качества функционирования ИС, основанный на использовании моделей и методов ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы» и ориентированный на достижение общей цели функционирования ИС различного функционального приложения – цели обеспечения надежности и своевременности предоставления необходимой информации, полноты, достоверности и безопасности используемой информации для последующего применения по назначению.

2. Раскрыты базовые термины и определения, рассматриваемые объекты ИС, принятые предположения, условия и допущения, возможные цели и задачи, подлежащие решению с применением результатов вероятностного прогнозирования, оцениваемые показатели, непосредственно приемлемые вероятностные модели, порядок проведения моделирования, интерпретация результатов расчетов на различных прикладных примерах и некоторые вопросы системного анализа в обеспечение качества и безопасности функционирования ИС.

3. Предложены вероятностные модели, позволяющие проведение исследований «моделируемых

систем» в виде «черного ящика»: «Модель для оценки надежности предоставления информации и выполнения операций»; «Модель для оценки своевременности предоставления информации и выполнения операций»; «Модель для оценки полноты используемой информации»; «Модель для оценки актуальности используемой информации»; «Модель для оценки безошибочности информации после контроля»; «Модель для оценки корректности информации после обработки»; «Модель для оценки безошибочности действий пользователей и персонала»; «Модель для оценки защищенности системы от опасных программно-технических воздействий»; «Модель для оценки защищенности активов от несанкционированного доступа»; «Модель для оценки конфиденциальности используемой информации». Разъяснено применение предложенного «Метода использования универсальной вспомогательной модели показателя для определения исходных данных в расчетах».

Рассмотрены методы учета дополнительных специфических требований и сложности моделируемой системы, методы оценки обобщенных и интегрального показателей качества функционирования ИС. Предложенные модели и методы проиллюстрированы примерами вероятностного прогнозирования качества функционирования ИС для простой (в виде «черного ящика») и сложной структуры, в т.ч. применительно к гипотетической системе дистанционного контроля, функционирующей в опасном производстве.

4. Раскрыты возможности применения предложенного подхода к решению следующих задач системного анализа: для прогнозирования значений показателей, интерпретации и анализа получаемых результатов, включая сравнение прогнозируемых значений показателей с допустимым уровнем на предмет выполнения задаваемых ограничений; обоснования допустимых рисков; определения существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на свойства рассматриваемой системы; определения и обоснования в жизненном цикле системы упреждающих мер противодействия угрозам и условий снижения рисков или удержания рисков в допустимых пределах, обеспечивающих желаемые свойства рассматриваемой системы при задаваемых ограничениях; обоснования предложений по обеспечению и повышению качества функционирования рассматриваемой системы.

5. В результате проведенных исследований созданы методические положения, формирующие основные компоненты облика комплексной методики вероятностного прогнозирования качества функционирования ИС согласно ГОСТ Р 59341-2021. Использование предложенных методических положений призвано помочь системным аналитикам сформировать облик разносторонней комплексной методики вероятностного прогнозирования, применимый в интересах обеспечения качества и безопасности, обоснования допустимых рисков, выявления существенных угроз и поддержки принятия научно обоснованных системных решений для упреждающего противодействия угрозам в жизненном цикле конкретной ИС.

Литература

1. Костогрызов А. И., Нистратов А. А. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 1. Общий подход // Правовая информатика, 2024, № 3, с. 13–31.
2. Костогрызов А. И., Нистратов А. А., Голосов П. Е. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 2. Моделирование с использованием «черных ящиков» // Вопросы кибербезопасности, 2024, № 6 (65), с. 3–25.
3. Vasilyev V. I., Vulfin A. M., Chernyakhovskaya L. R. Cybersecurity Risk Analysis of Industrial Automation Systems on the Basis of Cognitive Modeling Technology), Chapter 2 in «Digital Forensic Science» / Eds.: S. Shetty, P. Shetty / IntechOpen Pub., London, UK, 2019. ISBN: 978-1-83880-260-8; eBook (PDF) ISBN: 978-1-83968-742-6. DOI: 10.5772/intechopen.78450.
4. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, combinatorics and control./ Intech Open, 2020, pp. 3–34. – URL: https://www.intechopen.com/books/probability-combinatorics-and-control.
5. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In «Safety and Reliability of Systems and Processes», Gdynia Maritime University, 2020. pp. 153–174.
6. Golosov P. E., Gostev I. M. Optimization of the Distribution of Hash Calculation Tasks Flow at a Priori Given Complexity / Информационные технологии. 2021. No 5. P. 242–248.
7. Cognitive security modeling of biometric system of neural network cryptography / A. M. Vulfin, V. I. Vasilyev, A. D. Kirillova, A. V. Nikonov // Proceedings of the Information Technologies and Intelligent Decision-Making Systems (ITIDMS2021), (January 20, 2021). CEUR. –2021. – Vol. 2843.
8. Berkholts V. V., Vulfin A. M., Frid A. I. Telemetry data integrity monitoring system // IOP Conf. Series: Materials Science and Engineering, 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation. - 2021. – Vol. 1069. – 012003.
9. Network traffic analysis based on machine learning methods / A. M. Vulfin, V. I. Vasilyev, V. E. Gvozdev, K. V. Mironov, O. E. Churkin // International Scientific and Practical Conference «Information Technologies and Intelligent Decision-Making Systems». – Journal of Physics: Conference Series. – 2021. – Vol. 2001. – 012017.

10. Нистратов А.А. Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 1. Математические модели и методы // Системы высокой доступности. 2021. Т. 17 № 3, с. 16–31, Часть 2. Программно-технологические решения. Примеры применения // Системы высокой доступности. 2022. Т. 18 № 2, с. 42–57.
11. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии //Вопросы кибербезопасности. 2022, №6 (52), с.71–82.
12. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis – New Insights. IntechOpen, 2023, pp. 73–105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments.
13. Гостев И.М., Голосов П.Е. Анализ эффективности облачной вычислительной системы, обслуживающей поток заданий с директивными сроками выполнения при множественных отказах серверов // Программная инженерия. 2023. Том 14, № 6. С. 278–284. DOI: 10.17587/prin.14.278-284.
14. Голосов П.Е., Гостев И.М. Анализ эффективности имитационных моделей облачных вычислений с использованием элементов искусственного интеллекта / Радиотехнические и телекоммуникационные системы. М. 2023. № 2. С. 29–39.
15. Костогрызов А.И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, № 3. С. 114–133.
16. Костогрызов А.И. Моделирование процесса выявления закладок при тестировании программного обеспечения систем с искусственным интеллектом после машинного дообучения // INSiDE Защита информации. 2023, № 5. С. 28–35.
17. Костогрызов А.И., Нистратов А.А. Методический подход к вероятностному прогнозированию и сравнению качества функционирования систем в условиях неопределенности // Надежность. 2024. № 1. С. 10–24.
18. Костогрызов А.И. Подход к интервальной оценке системных рисков при неполноте данных о кратности резервирования в подсистемах. 2-я Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2024». 22-23 октября 2024 г. Москва. М.: НИЯУ МИФИ, 2024. С. 14–17.
19. Andrey Kostogryzov. Probabilistic predicting the risks of system integrity violation in the absence of complete data on subsystems reservation multiplicity. IEEE. Published in: 2024 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC). 29–31 October 2024. DOI: 10.1109/MoNeTec60984.2024.10768172.
20. Костогрызов А.И. Вероятностное моделирование системы защиты духовно-нравственных ценностей Часть 1. Общий подход // Системы высокой доступности. 2024. Том 20. № 2, с.40–55. Часть 2. Примеры прогнозирования рисков // Системы высокой доступности. 2024. Том 20. № 3, с.37–50.

METHODOLOGICAL PROVISIONS ON PROBABILISTIC PREDICTION OF INFORMATION SYSTEMS OPERATION QUALITY. Part 3. MODELING OF COMPLEX SYSTEMS. INTEGRAL ANALYSIS

Kostogryzov A.I.[4], Nistratov A.A.[5], Golosov P.E.[6]

Keywords: *probability, model, prediction, risk, system, system analysis, threat.*

Objective: *the purpose of the entire work is to help system analysts involved in assessing the quality of information systems (IS) operation during their creation, operation, modernization, development, to form the appearance of a comprehensive probabilistic prediction methodology applicable in the interests of ensuring quality and safety, justifying acceptable risks, identifying significant threats and supporting the adoption of scientifically rational system decisions to proactively counter threats in IS life cycle. The purpose of the 3rd part of the work is to complete the detailing of the general methodological provisions on the probabilistic prediction of the quality of IS operation quality (taking into account the enlarged description of the approach in the 1st part of the article [1] and the presentation of the basics of detailing modeling using «black boxes» in the 2nd part of the article [2]) by proposing:*

- *the formalization of complex modeled systems consisting of parallel-sequential structures formed from «black boxes» and combined using logical connections «AND», «OR»;*
- *the methods of system analysis of the IS operation quality;*
- *the main components of the appearance of a comprehensive methodology for the probabilistic predicting IS operation quality, used by system analysts in the interests of ensuring quality and safety, justifying acceptable risks, identifying significant threats and supporting the adoption of scientifically based system decisions to proactively counter threats in the life cycle of specific IS.*

4 Andrey I. Kostogryzov, Dr.Sc, of Technical Sciences, Professor, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences, Moscow. Russia. E-mail: Akostogr@gmail.com
5 Andrey A. Nistratov, Ph.D., Federal Research Center «Informatics and Control» of the Russian Academy of Sciences, Moscow. Russia. E-mail: Andrey.nistratov@gmail.com
6 Pavel E. Golosov., Ph.D., Director of the Institute of Social Sciences of the Russian Academy of National Economy and Public Administration (RANEPA), Moscow. Russia. E-mail: pgolosov@gmail.com

Research methods include: *methods of probability theory, methods of system analysis. The modeled system is formally represented by «black boxes» and complex systems in the form of parallel-sequential structures formed from «black boxes» combined using logical connections «AND», «OR». The obtained results of mathematical modeling are used in the interpretation of the original IS, in the interests of which the corresponding calculations are carried out.*

The result of the work as a whole is: *based on the research results presented in [1, 2], methodological provisions have been created that form the main components of the appearance of a complex methodology for probabilistic prediction of IS operation quality in accordance with GOST R 59341-2021 «System engineering. Protection of information in system information management process». The use of the proposed methodological provisions is intended to help system analysts form the appearance of a versatile complex methodology of probabilistic prediction, applicable in the interests of ensuring quality and safety, justifying acceptable risks, identifying significant threats and supporting the adoption of scientifically sound system decisions to proactively counter threats in the life cycle of specific IS.*

Scientific novelty of the work: *with the widespread introduction of modern information technology tools and systems, the problems associated with a comprehensive study of the IS operation quality remain acutely relevant. Despite the fact that many system engineering standards have appeared that recommend the use of probabilistic system analysis for various types of systems, in practice, the formation of a set of techniques applicable to predicting quality measures, justifying acceptable risks, identifying significant threats and supporting the adoption of scientifically sound system decisions in IS life cycle causes practical difficulties for system analysts. These difficulties and the use of subjective assessments are related not only to the versatility of the very concept of IS operation quality, but also to the complexity of mathematical formalization, taking into account the specifics of each system. As a result, many important aspects are beyond the analyst's field of consideration, specific quality measures turn out to be incommensurable on a single quantitative scale, and the inverse analytical tasks of proactive threat management in IS life cycle and constituent elements are not solved. I.e., in practice, there is a contradiction between the needs for system analysis of IS and the possibilities for solving urgent problems of system analysis. To overcome this contradiction, the proposed methodological provisions formulate the general purpose of IS operation in various areas applications – to ensure the reliability and timeliness of providing the necessary information, completeness, validity and safety of the information used for subsequent intended use. The main proposed components of the complex methodology of probabilistic prediction of IS operation quality have determined the scientific novelty of this work, focused precisely on achieving this general formulated goal of IS operation.*

References

1. Kostogryzov A.I., Nistratov A.A. Metodicheskie polozhenija po verojatnostnomu prognozirovaniju kachestva funkcionirovanija informacionnyh sistem. Chast' 1. Obshhij podhod // Pravovaja informatika, 2024, № 3. S. 13–31. (in Russian).
2. Kostogryzov A.I., Nistratov A.A., Golosov P.E. Metodicheskie polozhenija po verojatnostnomu prognozirovaniju kachestva funkcionirovanija informacionnyh sistem. Chast' 2. Modelirovanije s ispolzovaniem «chernich jashikov». Voprosy kiberbezopasnosti, 2024, № 6, S. 3–25. (in Russian).
3. Vasilyev V.I., Vulfin A.M., Chernyakhovskaya L.R. Cybersecurity Risk Analysis of Industrial Automation Systems on the Basis of Cognitive Modeling Technology), Chapter 2 in «Digital Forensic Science» / Eds.: S. Shetty, P. Shetty / IntechOpen Pub., London, UK, 2019. ISBN: 978-1-83880-260-8; eBook (PDF) ISBN: 978-1-83968-742-6. DOI: 10.5772/intechopen.78450.
4. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, combinatorics and control./ IntechOpen, 2020, pp. 3–34. – URL: https://www.intechopen.com/books/probability-combinatorics-and-control.
5. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In «Safety and Reliability of Systems and Processes», Gdynia Maritime University, 2020. pp. 153–174.
6. Golosov P.E., Gostev I.M. Optimization of the Distribution of Hash Calculation Tasks Flow at a Priori Given Complexity / / Informacionnye Tehnologii. 2021. No 5. P. 242–248.
7. Cognitive security modeling of biometric system of neural network cryptography / A.M. Vulfin, V.I. Vasilyev, A.D. Kirillova, A.V. Nikonov // Proceedings of the Information Technologies and Intelligent Decision-Making Systems (ITIDMS2021), (January 20, 2021). CEUR. – 2021. – Vol. 2843.
8. Berkholts V.V., Vulfin A.M., Frid A.I. Telemetry data integrity monitoring system // IOP Conf. Series: Materials Science and Engineering, 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation. – 2021. – Vol. 1069. – 012003.
9. Network traffic analysis based on machine learning methods / A.M. Vulfin, V.I. Vasilyev, V.E. Gvozdev, K.V. Mironov, O.E. Churkin // International Scientific and Practical Conference «Information Technologies and Intelligent Decision-Making Systems». – Journal of Physics: Conference Series. – 2021. – Vol. 2001. – 012017.
10. Nistratov A.A. Analytical prediction of the integral risk of violation of the acceptable performance of the set of standard processes in a life cycle of highly available systems. Part 1. Mathematical models and methods. Highly Available Systems. 2021. V. 17. № 3. P. 16–31. Part 2. Software-technological solutions. Examples. Highly Available Systems. 2022. V. 18. № 2. P. 42–57. (in Russian).
11. Kostogryzov A.I. O modelyah i metodah veroyatnostnogo analiza zashchity informacii v standartizovannyh processah sistemnoj inzhenerii. Voprosy kiberbezopasnosti. 2022. № 6(52). S. 71–82 (in Russian).
12. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis – New Insights. Intech Open, 2023, pp. 73–105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments.

13. Gostev I. M., Golosov P. E. Analiz jeffektivnosti oblachnoj vychislitel'noj sistemy, obsluzhivajushhej potok zadanij s direktivnymi srokami vypolnenija pri mnozhestvennyh otkazah serverov // Programmnaja inzhenerija. 2023. Tom 14, № 6. S. 278–284. DOI: 10.17587/prin.14.278-284. (in Russian).
14. Golosov P. E., Gostev I. M. Analiz jeffektivnosti imitacionnyh modelej oblachnyh vychislenij s ispol'zovaniem jelementov iskusstvennogo intellekta / Radiotehnicheskie i telekommunikacionnye sistemy. M. 2023. № 2. S. 29–39. (in Russian).
15. Kostogryzov A. I. Podchod k verojatnostnomu prognozirovaniju zaschiscennosti reputacii «feikovich» ugroz b publichnom prostranstve. Voprosy kiberbezopasnosti. 2023. № 3. S. 114–133 (in Russian).
16. Kostogryzov A. I. Modelirovanie processa vijavlenija zakladok pri testirovanii programmnogo obespechenija system s iskusstvennim intellektom posle mashinnogo doobuchenija // INSiDE Zashita informacii. 2023, № 5. S. 28–35 (in Russian).
17. Kostogryzov A. I., Nistratov A. A. Methodological approach to probabilistic prediction and comparison of systems operation quality under conditions of uncertainty. Dependability. 2024; 1: 10–24. (in Russian).
18. Kostogryzov A. I. Podchod k intervalnoi ozenke systemnich riskov pri nepolnote dannich o kratnosti rezervirovanija v podsystemach. 2-ja Vserossiiskaja nauchno-technicheskaja konferencija «Kibernetika i informacionnaja besopasnost «KIB-2024». 22-23.10. Moskva. NIJAU MIFI, 2024. S. 14–17. (in Russian).
19. Andrey Kostogryzov. Probabilistic predicting the risks of system integrity violation in the absence of complete data on subsystems reservation multiplicity. IEEE. Published in: 2024 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC). 29–31 October 2024. DOI: 10.1109/MoNeTec60984.2024.10768172.
20. Kostogryzov A. I. Probabilistic modeling the protection system of spiritual and moral values. Part 1. The general approach. Highly Available Systems. 2024. V. 20. № 2. P. 40–55. Part 2. The risks prediction examples. Highly Available Systems. 2024. V. 20. № 3. P. 37–50. (in Russian).