МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ ПО ВЕРОЯТНОСТНОМУ ПРОГНОЗИРОВАНИЮ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ. Часть 2. МОДЕЛИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ «ЧЕРНЫХ ЯЩИКОВ»

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

DOI: 10.21681/2311-3456-2024-6-2-27

Продолжение[4]

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, применимого 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 2-й части работы: *детализировать в интересах вероятностного анализа свойств, характеризующих качество функционирования ИС, общие методические положения, укрупненно изложенные в 1-й части статьи, путем предложения вероятностных моделей, представимых в виде «черных ящиков».*

Методы исследования *включают: методы теории вероятностей, методы системного анализа. В качестве моделируемой системы формально выступают «черные ящики», когда известны исходные данные для моделирования и выходные результаты, но неизвестно внутреннее устройство системы. Получаемые результаты математического моделирования используются в интерпретации к исходной ИС, в интересах которой проводятся соответствующие расчеты.*

Результаты 2-й части работы: *предложены модели, представимые в виде «черных ящиков», для вероятностного анализа составных свойств качества ИС согласно ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы».*

Научная новизна работы: *предлагаемые модели ориентированы на достижение общей цели функционирования ИС различного функционального приложения (сформулированной в 1-й части статьи) – обеспечения надежности и своевременности предоставления необходимой информации, полноты, достоверности и безопасности используемой информации для последующего применения по назначению. Использование моделей позволяет осуществлять оценки по единой вероятностной шкале качества функционирования рассматриваемых системы и ее составных элементов, представимых в виде «черных ящиков».*

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

1. Введение

Методические положения настоящей части статьи предназначены для вероятностного прогнозирования качества функционирования рассматриваемой ИС (далее по тексту – «Системы» с заглавной буквы) с использованием понятия «моделируемой системы». 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. Например, при проведении системного анализа в принимаемых допущениях, ограничениях и предположениях модель может формально описывать процесс, функциональные действия, множество активов и/или выходных результатов или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях.

В 1-й части статьи обоснована актуальность работы, предложен общий подход к вероятностному прогнозированию качества функционирования ИС, основанный на использовании моделей и методов ГОСТ Р 59341. Подход представлен в виде основных методических положений, раскрывающих базовые термины и определения, рассматриваемые объекты

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

4 Часть 1 настоящей работы опубликована в журнале «Правовая информатика», 2024, №3, с. 13–31.

ИС, цель и задачи прогнозирования, принятые предположения, условия и допущения, оцениваемые показатели, перечень вероятностных моделей, порядок проведения моделирования, интерпретация и системный анализ результатов расчетов [1–24]. Тем самым по-крупному описан облик комплексной методики вероятностного прогнозирования качества функционирования ИС, который подлежит наполнению моделями и методами.

В настоящей 2-й части работы общие методические положения 1-й части детализированы путем предложения вероятностных моделей, позволяющих проведение исследований «моделируемых систем» в виде «черного ящика». Это: «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 опасных программно-технических воздействий»; «Модели для оценки защищенности активов от несанкционированного доступа»; «Модели для оценки конфиденциальности используемой информации». Также приводится «Метод использования универсальной вспомогательной модели показателя для определения исходных данных в расчетах», используемый при формировании исходных данных.

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

Тем самым представленные модели охватывают практическое воплощение идеи оценки качества функционирования ИС – см. рис. 1 и пояснения в 1-й части статьи. Во 2-й части статьи также приведены некоторые примеры, иллюстрирующие варианты применения предложенных моделей [1–12, 15–30].

2. Вероятностные модели

2.1. Общие положения по использованию «черных ящиков»

За основу предлагаемого подхода к математическому моделированию с использованием «черных ящиков» принят подход, изложенный в разные годы в приложении к различным системам [2–12, 15–24] и доведенный до реализации на уровне ГОСТ Р 59341. С учетом неопределенностей расчет вероятностных показателей делается в принятых предположениях, условиях и допущениях, описанных в 1-й части статьи.

Предлагаемые математические модели ориентированы на противодействие возможным угрозам качеству функционирования Системы. Перечень возможных разнородных угроз может включать:

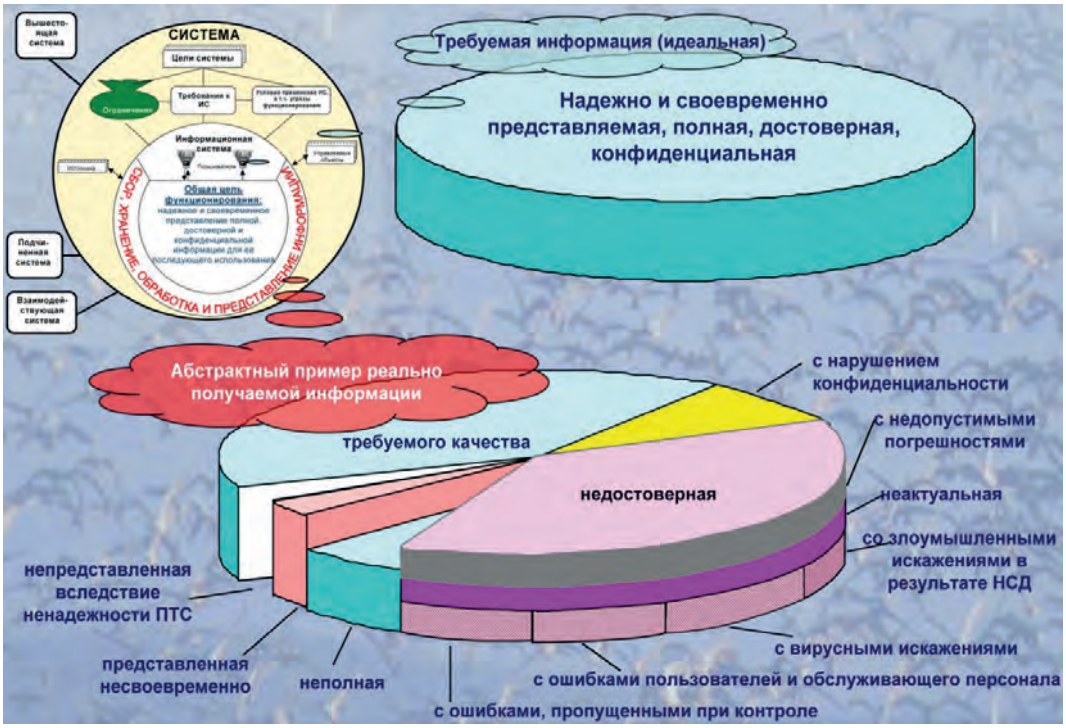


Рис. 1. Абстрактная иллюстрация качества функционирования ИС

- природные и природно-техногенные угрозы – по ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7;
- угрозы со стороны человеческого фактора – по ГОСТ Р МЭК 62508;
- угрозы безопасности информации, качеству программного обеспечения, безопасности оборудования и коммуникаций, используемых в процессе работы – по ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 51583, ГОСТ Р 54124, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994;
- угрозы возникновения ущерба репутации и/или потери доверия к конкретному заказчику или поставщику, системы которого были скомпрометированы;
- прочие соответствующие угрозы качеству функционирования Системы.

Для оценки риска нарушения качества функционирования моделируемой системы (подсистемы, элемента), представимой как «черный ящик», необходимо учитывать, что в общем случае существует зависимость от надежности и своевременности предоставления используемой информации и выполнения операций, полноты оперативного отражения в системе новых объектов и явлений, актуальности обновляемой информации, безошибочности информации после контроля, корректности обработки информации, безошибочности действий пользователей и персонала системы, обеспечения безопасности информации – см. рис. 1. При этом понятие обеспечения безопасности информации включает сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации. Под целостностью моделируемой системы понимается такое состояние моделируемой системы, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза. Полное формализованное описание всех предлагаемых моделей приведено в ГОСТ Р 59341, а ранее – в [2–12, 15–24]. По этой причине для оценки предлагаемых показателей качества функционирования моделируемой системы (подсистемы, элемента) в представляемых ниже в 2.2.–2.12. описаниях и примерах перечисляются лишь необходимые исходные данные. В отдельных случаях даются иллюстративные примеры и методические рекомендации с указанием соответствующих ссылок. Общий порядок проведения моделирования, интерпретации и системного анализа получаемых результатов расчетов приведен в 1-й части статьи.

2.2. Модели для оценки надежности предоставления информации и выполнения операций

Под надежностью предоставления информации в системе и выполнения операций понимается

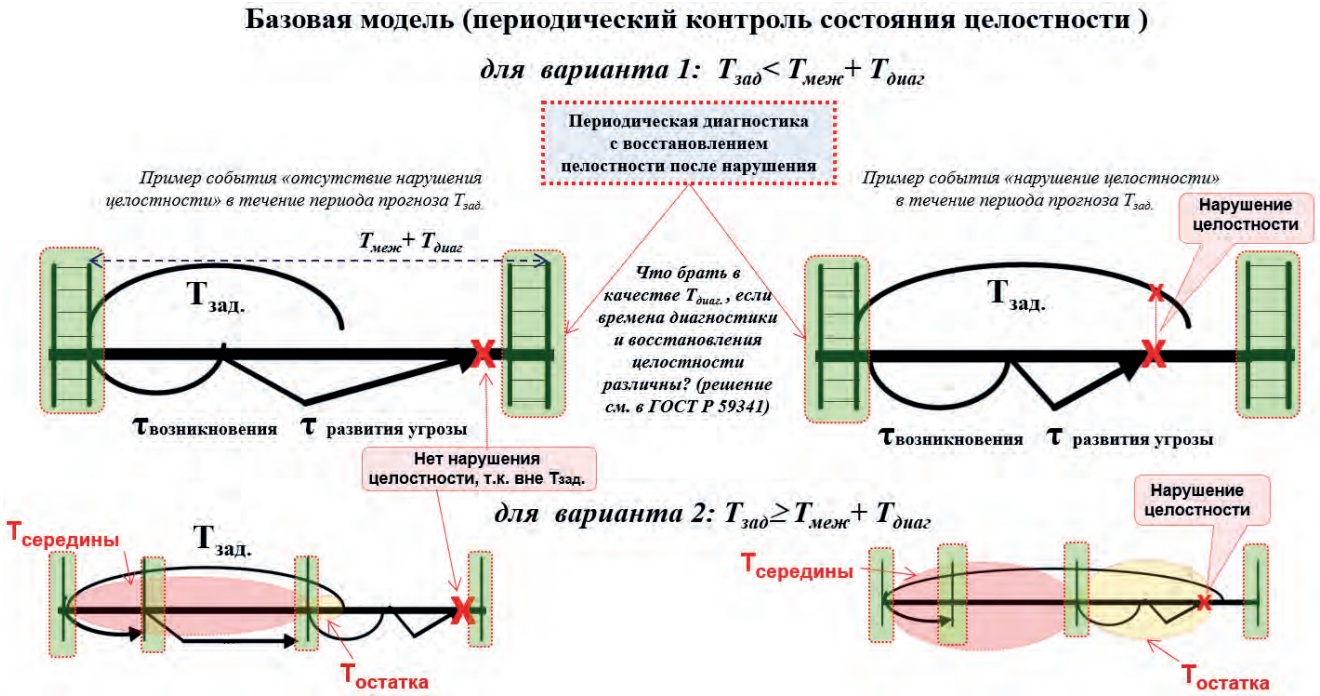


Рис. 2. Примеры элементарных событий, связанных с нарушением целостности моделируемой системы по ГОСТ Р 59341, приложению В.3.2

свойство системы обеспечивать прием, автоматическую обработку запроса или команды и предоставление или принудительную выдачу выходной информации согласно функциональному алгоритму при соблюдении эксплуатационных условий применения и технического обслуживания системы.

Для оценки надежности предоставления информации и выполнения операций в моделируемой системе (подсистеме, элементе) в течение заданного периода прогноза применяются «Модели для оценки надежности предоставления информации» из ГОСТ Р 59341, приложения В.3.2. Примеры рекомендуемой базовой модели в части элементарных событий, связанных с нарушением целостности моделируемой системы, и с привязкой к обозначениям исходных данных в ГОСТ Р 59341 представлены на рис. 2.

В качестве исходных данных для моделирования используются:

σ – частота возникновения источников угроз (например, ведущих к отказам и сбоям программно-технических и технологических средств);

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы;

$T_{\text{меж}}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{\text{диаг}}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{\text{восст}}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

$T_{\text{зад}}$ – задаваемая длительность периода прогноза.

В результате моделирования рассчитываются частные показатели: вероятность $P_{\text{над предст}}(T_{\text{зад}})$ надежного предоставления информации и выполнения операций в системе в течение заданного периода прогноза $T_{\text{зад}}$ и вероятностный показатель надежности предоставления информации и выполнения операций $Z_{\text{над предст}}(T_{\text{зад}})$, учитывающий рассчитываемое значение $P_{\text{над предст}}(T_{\text{зад}})$ и соответствующие условия α из ГОСТ Р 59341, приложения В.3.2. Условие α касается надежности предоставления запрашиваемой или выдаваемой принудительно информации и 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 уровня (это – формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного показателя надежности предоставления информации $Z_{\text{над предст}}(T_{\text{зад}})$

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

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого показателя $[1 - Z_{\text{над предст}}(T_{\text{зад}})]$ в качестве вероятностного выражения риска нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в системе. Его равенство нулю при несущественном ущербе означает пренебрежимо малый риск.

Некоторые возможности применения модели продемонстрированы в 3-й части статьи. С целью избегания трудностей с формированием исходных данных для моделирования ниже излагается метод использования универсальной вспомогательной модели показателя элементарных состояний эксплуатируемой системы.

2.3. Метод использования универсальной вспомогательной модели показателя для определения исходных данных в расчетах

Для расчета разных по смысловому пониманию показателей могут быть использованы одни и те же математические модели. Например, упомянутые выше в 2.2. «Модели для оценки надежности...» из ГОСТ Р 59341, приложения В.3.2, применимы для анализа безошибочности действий пользователей и персонала системы, а также для анализа защищенности системы от опасных программно-технических воздействий в течение заданного периода прогноза – см. в том же стандарте приложения В.3.8, В.3.9. В качестве исходных выступают те же данные для моделирования (адаптированные по контексту), обозначаемые одинаковым образом как σ, β, $T_{\text{меж}}$, $T_{\text{диаг}}$, $T_{\text{восст}}$, $T_{\text{зад}}$.

В общем случае, если для таких исходных данных, как $T_{\text{меж}}$ и $T_{\text{диаг}}$ на практике не возникает каких-либо трудностей, а $T_{\text{зад}}$ задается аналитиком, то для определения σ, β, $T_{\text{восст}}$ может возникать вопрос – откуда их брать? В этом случае рекомендуется использование универсальной вспомогательной модели показателя (УВМП) – см., например, ГОСТ Р 59349 «Системная инженерия. Защита информации в процессе системного анализа». Дело в том, что в любой момент времени у ответственных лиц, принимающих решение, должно быть формальное представление о том, какое состояние эксплуатируемой системы «приемлемо», а какое «неприемлемо» и требует управляющей реакции для улучшения. То есть в каждый отчетный момент времени по каждому из критичных показателей (или по их совокупности) можно с однозначной уверенностью определить, что его (их) значения находятся в состоянии, которое может быть

охарактеризовано как «Приемлемое» или «Приемлемое с отклонением» (когда требуются определенные организационные или обычные технические усилия по улучшению значения показателя) или как «Неприемлемое» состояние (когда требуются кардинальные решения по восстановлению условий и/или ресурсов, которые в существующем виде уже не обеспечивают требуемый уровень качества функционирования системы или в ближайшее время при бездействии не будут его гарантировать) – см. рис. 3.

Состояния «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» – это элементарные состояния, в которые может переходить во времени каждый из учитываемых показателей, используемых при моделировании. Под приемлемыми условиями и/или ресурсами системы понимается такое ее состояние (характеризуемое этими условиями и ресурсами), при котором обеспечивается достижение целей функционирования системы. Такое состояние называют состоянием целостности системы.

Рис. 3. Элементарные состояния контролируемого показателя УВМП во времени и временные исходные данные для моделирования

Из фрагмента состояний на рисунке 3 частота возникновения источника угроз для моделируемой системы $\sigma = 1 / [(\tau_{возн.1} + \tau_{возн.2} + \tau_{возн.3} + \tau_{возн.4}) / 4]$, среднее время развития угроз с момента возникновения источника угроз до нарушения нормальных условий функционирования моделируемой системы $\beta = (\tau_{разв.1} + \tau_{разв.2} + \tau_{разв.3} + \tau_{разв.4} + \tau_{разв.5}) / 5$, среднее время восстановления нарушаемой целостности моделируемой системы $T_{восст} = (\tau_{восст.1} + \tau_{восст.2} + \tau_{восст.3}) / 3$, где $\tau_{возн.i}$ – i-й интервал времени между возникновениями источника угроз, $\tau_{разв.j}$ – j-й интервал времени развития угроз с момента возникновения источника угроз до нарушения нормальных условий, $\tau_{восст.m}$ – m-й интервал времени восстановления нарушаемой целостности.

Значения σ, β, $T_{восст}$, получаемые по результатам анализа данных мониторинга (или их пересчета на уровне УВМП), являются исходными данными для формального описания моделируемой системы с учетом возможности прогнозирования динамики разнородных событий. Роль в УВМП каждого из учитываемых критичных показателей сводится к их количественным значениям при формировании значений исходных данных σ, β, $T_{восст}$ для последующего моделирования.

Примечание. Этот способ также применим для случая, когда в качестве критичного показателя выступает неколичественная оценка состояния с градациями «Приемлемое», «Приемлемое с отклонением», «Неприемлемое», что аналогично понятиям «допустимого», «значимого» и «критического» рисков, используемых для экспертных оценок.

Учитывая математическую идентичность моделей для оценки надежности предоставления информации, безошибочности действий пользователей и персонала системы, а также защищенности системы от опасных воздействий в течение заданного периода прогноза, некоторые возможности моделирования приведены в 3-й части статьи с использованием понятий сложной «моделируемой системы».

2.4. Модели для оценки своевременности предоставления информации и выполнения операций

2.4.1. Общее

Под своевременностью предоставления требуемой информации в системе понимается свойство системы обеспечивать предоставление запрашиваемой или выдаваемой принудительно (автоматически) выходной информации в задаваемые сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы. Аналогичное определение – в приложении к выполнению операций.

Для оценки своевременности предоставления информации и выполнения операций в моделируемой системе достаточно высокую степень адекватности обеспечивают модели и методы теории массового обслуживания. В реальности могут использоваться различные технологии обслуживания. Например, это бесприоритетное и приоритетное обслуживание одним или несколькими приборами, многофазное обслуживание, обслуживание в режиме разделения времени и т.п. Для оценки некоторых из этих технологий при различного рода ограничениях уже существуют методические разработки, в том числе в приложении к анализу вычислительных систем и сетей. Применительно к системам массового обслуживания с ожиданием термин «технология обслуживания» совпадает с термином «дисциплина обслуживания» или «технология диспетчеризации», определяющим

порядок выборки очередного запроса из буфера для обработки на приборе – см., например, характерные свойства технологий в примере 1-й части статьи, описывающем динамический метод рациональной диспетчеризации запросов различной срочности. Под запросами понимаются не только запросы пользователей на получение выходных документов, но и задачи на пересылку файлов или ввод информации в базу данных (БД), а также некоторые технологические операции по управлению вычислительным процессом, администрированию доступа к передающей среде в компьютерных сетях, обеспечению безопасности информации и пр.

В общем случае процессы предоставления информации и выполнения операций формализуются как процессы массового обслуживания потоков запросов в надежно функционирующих системах с ожиданием и буфером бесконечного объема [3–13, 19–21] – см. рис. 4.

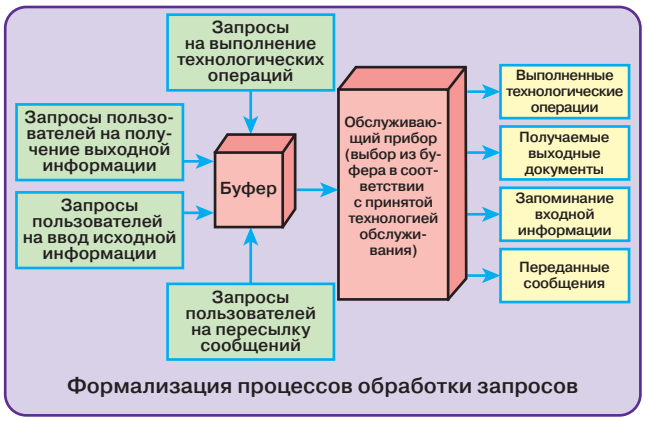


Рис. 4. Пример формального описания процессов обработки запросов

Требования к своевременности обработки запросов определяются формально с помощью следующих критериев.

Определение критерия 1 (оценка по среднему времени обработки). Обработка запросов i–го типа считается выполненной в срок, если среднее время их обработки $T_{\text{полн}.i1}$ с учетом задержек в очередях не превышает заданного уровня $T_{\text{зад}..i}$, т.е. если $T_{\text{полн}.i1} \le T_{\text{зад}..i}$.

Определение критерия 2 (оценка по вероятности своевременной обработки). Обработка запросов i–го типа считается выполненной в срок, если вероятность своевременной обработки $P_{\text{св}\,i}(T_{\text{зад}\,i})$ за время $T_{\text{зад}..i}$ не ниже заданной вероятности $P_{\text{св. зад}.i}$, т.е. $P_{\text{св}\,i}(T_{\text{зад}\,i}) = P(t_{\text{полн}.i} \le T_{\text{зад}..i}) \ge P_{\text{св.зад}.i}$, где случайная величина $t_{\text{полн}.i}$ характеризует полное время обработки запросов i–го типа с учетом задержек в очередях. Критерий 2 задает более жесткие временные рамки и используется для компьютерных систем жесткого реального времени (как правило, при этом $T_{\text{зад}.i} \ge 0{,}8$).

Для каждого из значимых типов обрабатываемой информации с привязкой к выполняемым функциональным задачам, источникам и получателям информации требования к своевременности обработки запросов в системе указываются в форме одного из двух упомянутых выше критериев своевременности 1 или 2.

В результате расчетов оцениваются такие показатели, как вероятность своевременной обработки запросов i-го типа в системе $P_{\text{св}\,i}(T_{\text{зад}\,i})$ и, исходя из них – относительная доля своевременно обработанных в системе запросов $C_{\text{своевр}}$, для которых выполняются требования к своевременности.

Вероятность своевременной обработки запросов определяется с использованием табулируемой неполной гамма-функции:

$$P_{\text{св}\,i}(T_{\text{зад}\,i}) = \int_0^{\theta_i} \exp(-\tau)\,\tau^{\gamma_i}\,d\tau/\Gamma(\gamma_i), \qquad (2)$$

где $\Gamma(\gamma) = \int_0^{\infty} \exp(-\tau)\,\tau^{\gamma}\,d\tau$ – гамма-функция,

$$\gamma_i = \frac{T_i}{\sqrt{|\,T_{i2} - T_i^2\,|}},\ \theta_i = T_{\text{зад}\,i} \cdot \frac{\gamma_i^2}{T_i};$$

γ_i, θ_i – рассчитываемые параметры неполной гамма-функции; T_i, и $\sqrt{|\,T_{i2} - T_i^2\,|}$ – соответственно среднее время и среднеквадратичное отклонение времени реакции системы при обработке запросов i-го типа (т. е. полного времени пребывания на обработке с учетом ожидания в очередях), T_{i2} – второй момент времени реакции. Чаще в качестве исходных данных формируют целиком именно среднеквадратичное отклонение, не опускаясь до отдельных измерений второго момента. В свою очередь, упомянутые значения T_i, и $\sqrt{|\,T_{i2} - T_i^2\,|}$ сами могут быть получены в результате математического моделирования – см., например, приемлемые модели в [2, 4–6, 15–23]. Поскольку полностью детерминированный режим поступления и обработки из рассмотрения исключен, то среднеквадратичные отклонения никогда не обращаются в 0 (т.е. отсутствуют случаи деления на 0).

Относительная доля своевременно обработанных в системе запросов $C_{\text{своевр}}$ охватывает лишь те типы запросов, для которых выполнены требования заказчика, этот показатель вычисляют по формуле

$$C_{\text{своевр}} = \frac{\sum_{i=1}^{I} \lambda_i\, P_{\text{св}\,i}(T_{\text{зад}\,i})[Ind(\alpha_1) + Ind(\alpha_2)]}{\sum_{i=1}^{I} \lambda_i} \qquad (3)$$

где λ_i – частота поступления на обработку запросов i-го типа; критерии α своевременности обработки каждого типа запросов устанавливают 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 определяют одним из условий α_1 или α_2:

α_1 – условие, когда для i-го типа запросов задан критерий 1 своевременности по среднему времени обработки (реакции системы) и $T_i \le T_{\text{зад } i}$.

α_2 – условие, когда для i-го типа запросов задан вероятностный критерий 2 своевременности и $P_{\text{св } i}(T_{\text{зад } i}) \ge P_{\text{св зад } i}$.

В общем случае расчетные показатели $P_{\text{св } i}(T_{\text{зад } i})$ зависят не только от частоты поступления различных запросов на обслуживание и времени их обслуживания, но и от использования конкретных технологий диспетчеризации (обслуживания) запросов и критериев своевременности (см. пример в 1-й части статьи).

Для оценки интегрального риска рассчитывается $Z_{\text{своевр}}$ – вероятностный показатель своевременности обработки запросов, учитывающий относительную долю своевременно обработанных в системе запросов $C_{\text{своевр}}$, и соответствующие условия α из ГОСТ Р 59341, приложения В.3.3.

2.4.2. Пример для оценки своевременности

Настоящий пример поясняет логику подхода к оценке относительной доли своевременно обработанных запросов лишь тех типов, для которых выполняются требования по своевременности $C_{\text{своевр}}$ согласно ГОСТ Р 59341. Пример призван продемонстрировать извлечение прагматических эффектов от применения предложенного подхода не только для решения корпоративных проблем с использованием ИС, но и для выработки научно обоснованных подходов к решениям задач по оптимизации функционирования и совершенствованию ИС межгосударственного значения. В настоящем примере область исследования охватывает острую проблематику обеспечения доверия к информационному обслуживанию пользователей с использованием распределенных реестров, основанных на блокчейн-технологии. Сами сообщения могут иметь произвольную природу, в частности, иметь технологический, информационный, финансовый, управленческий характер. При этом основным требованием к информационным сообщениям выступает требование наличия биективного отображения с элементом блокчейн-записей (реестровых записей).

Например, в инфраструктуре КНР используется национальная блокчейн-платформа «Xinghuo» («Искра», разработчик – компания Буби)[5], обеспечивающая единую среду взаимодействия государственных и частных организаций. На сегодняшний день она насчитывает около 20 опорных узлов и более 40 региональных блокчейн-хабов, включая отраслевые. Кроме того, сформированы шлюзы для доверенного обмена данными с рядом стран (Казахстан, Филиппины, Малайзия) Пример взаимодействия, основанный на цифровых сертификатах, представлен на рис. 5.

5 Информационное сообщение о платформе: https://wap.cinn.cn/p/303392.html

Рис. 5. Интеграционное решение для реализации международной платформенной торговли Китай-Малайзия

Особенностью построения подобного рода сложных ИС является неотчуждаемость информации от ее создателя, при этом обеспечивается возможность проверки достоверности сведений для произвольного сообщения, в том числе за счет одновременного хранения нескольких его копий на распределенных узлах. Принцип организации блокчейн-сетей не обязательно реализуется на основе подтверждения работы, однако для ряда случаев его применение, несмотря на высокую энергозатратность, является безальтернативным.

Что может быть известно о рассматриваемой Системе опорных узлов и региональных блокчейн-хабов гипотетической информационной среды взаимодействия государственных и частных организаций при ее создании, модернизации и развитии? Стараясь не перегружать статью техническими деталями, полагаем, что известно следующее: по условиям функционирования Системы в период наивысшей нагрузки все множество запросов (технологических, информационных, финансовых, управленческих и др.), связанных с предоставлением необходимой информации и выполнением операций в каждом из опорных узлов и региональных блокчейн-хабов рассматривается как самостоятельная «моделируемая Система» с исходными информационными данными, подразделяется на 4 типа. Это могут быть запросы, каждый из которых может быть обработан в режиме распараллеливания процессов обработки. Для примера, предположим, что запросы 1-го типа ($i = 1$) поступают в среднем через 4 секунды (т.е. частота поступления на обработку запросов 1-го типа $\lambda_1 = 0{,}25$ сек$^{-1}$), 2-го типа – через 5 секунд (т.е. $\lambda_2 = 0{,}2$ сек$^{-1}$), 3-го типа – через 6 секунд ($\lambda_3 = 0{,}167$ сек$^{-1}$), 4-го типа – через 7 секунд ($\lambda_4 = 0{,}143$ сек$^{-1}$). При этом, учитывая повышенные требования к надежности всей информационной среды, задаваемые требованиями бизнес-сообщества, выглядят следующим образом: риск несвоевременной обработки запросов не должен превышать 10^{-6} при том, что предельная длительность обработки запросов 1-го типа не должна превышать 64 секунд, 2-го типа – 96 секунд, 3-го типа – 164 секунд, 4-го типа – 180 секунд. Дополнительно с учетом собираемой статистики положим, что соотношения средних времен обработки запросов 1:2:3:4-го типов в автономном режиме (т.е. без очередей) составляет приблизительно 3:4:6:10.

Главные практические задачи для каждого из опорных узлов и региональных блокчейн-хабов гипотетичной информационной среды взаимодействия государственных и частных организаций (наподобие приведенной на рис. 5 интеграционной среды), подлежащих разрешению с использованием предлагаемой «Модели для оценки своевременности предоставления информации и выполнения операций», формулируются в виде четырех вопросов:

1. Сколько серверов необходимо для своевременной обработки всех запросов, поступающих в «моделируемую Систему»?
2. Как изменятся требования к количеству серверов, необходимых для своевременной обработки запросов в «моделируемой Системе», при смягчении требований к допустимому риску несвоевременной обработки запросов с уровня 10^{-6} до уровня 0.05?
3. Какое количество серверов необходимо иметь для обеспечения гарантированной своевременности обработки запросов при некоторой фиксированной степени распараллеливания процессов в их обработке в «моделируемой Системе» и заданных ограничениях?
4. Как оптимизировать степень распараллеливания процессов при обработке запроса каждого типа в «моделируемой Системе», чтобы избежать излишних затрат и при этом обеспечить требуемую своевременность? (т.е. как определить рациональное число параллельно выполняемых заданий для обработки запроса каждого типа?)

Методические рекомендации по приемлемым подходам к решению сформулированных выше задач с использованием предложенной в 2.4.1 «Модели...» состоят в следующем.

В качестве объектов анализа выступают технологии диспетчеризации и временные задержки при обработке запросов в «моделируемой Системе» (см. 1-ю часть статьи, где показано, что эффекты могут быть достигнуты за счет рациональной динамической настройки параметров технологий диспетчеризации ограничений в специфических условиях ограничений на своевременность обработки запросов различных типов). Каждый из опорных узлов и региональных блокчейн-хабов рассматривается как самостоятельная «моделируемая Система» с исходными информационными потоками, обеспечивающая предоставление необходимой информации и выполнение операций.

Применяя модель 2.4.1., предлагается вариант решения 1-й задачи.

Сначала требования бизнес-сообщества к своевременности обработки запросов переформулируются к виду критерия 2, рекомендуемому ГОСТ Р 59341, а именно:

- время обработки запросов 1-го типа не должно превышать 64 сек. с вероятностью не ниже 0,999999, т.е. задается условие $P(t_{\text{полн.1}} \le 64 \text{ сек.}) \ge 0{,}999999$;
- время обработки запросов 2-го типа не должно превышать 96 сек. с вероятностью не ниже

0,999999, т.е. задается условие $P(t_{\text{полн.2}} \le 96 \text{ сек.}) \ge \ge 0{,}999999$;

- время обработки запросов 3-го типа не должно превышать 164 сек. с вероятностью не ниже 0,999999, т.е. задается условие $P(t_{\text{полн.3}} \le 164 \text{ сек.}) \ge \ge 0{,}999999$;
- время обработки запросов 4-го типа не должно превышать 180 сек. с вероятностью не ниже 0,999999, т.е. задается условие $P(t_{\text{полн.3}} \le 180 \text{ сек.}) \ge \ge 0{,}999999$.

Здесь случайная величина $t_{\text{полн.}i}$ характеризует полное время обработки запросов i–го типа с учетом задержек в очередях, а допустимая вероятность «успеха» 0,999999 получается как дополнение допустимого риска 10^{-6} до 1, т.е. 0,999999 = 1 – 10^{-6}.

Решение задачи будем искать на множестве четырех технологий диспетчеризации, описанных в 1-й части статьи, где разъяснены свойства этих технологий относительно задержек в очередях и возможности извлечения эффектов при решении задачи повышения пропускной способности компьютерной сети путем максимизации своевременно обработанных в системе запросов. Краткая характеристика сравниваемых технологий диспетчеризации: технология 1 заключается в бесприоритетном обслуживании запросов (БПО) в порядке «первый пришел — первый обслужился»; технология 2 заключается в обслуживании запросов с относительными приоритетами (ОП); технология 3 заключается в обслуживании запросов с абсолютными приоритетами с дообслуживанием с прерванного места (АП); технология 4 заключается в пакетном обслуживании запросов с естественным формированием пакетов и относительными приоритетами внутри пакета (Пак.).

Для этих технологий значения среднего времени T_i и среднеквадратичного отклонения времени обработки запросов i-го типа в системе $\sqrt{|T_{i2} - T_i^2|}$ и, соответственно, $P_{\text{св }i}(T_{\text{зад }i})$ по формуле (2) рассчитываются с помощью моделей массового обслуживания, подробно описанных в [2, 4–6, 15–23].

Результаты расчетов показали, что только для 4-й технологии пакетной обработки (Пак.) требования по своевременности обработки всех типов запросов будут выполнены с вероятностью не ниже 0,999999 (i-й тип – это i-й приоритет внутри пакета) – см. рис. 6.

При этом среднее время обработки запросов 1-го типа составит 3.84 сек. (с учетом задержек в очередях) при максимально задаваемой длительности 64 сек., 2-го типа – 4,91 сек. при максимально задаваемой длительности 96 сек., 3-го типа – 6,33 сек. при максимально задаваемой длительности 164 сек., 4-го типа – 8,50 сек. при максимально задаваемой длительности 180 сек. А относительная доля своевременно обработанных в системе запросов, для которых выполнены требования бизнес-сообщества $C_{\text{своевр}}$, составит в процентном выражении более 99,9999 %. Такой эффект достигается, когда исходные средние времена обработки запросов в автономном режиме (т.е. без очередей) составляют: по 1-му типу – не более 0.6 сек. (сравните: с очередями среднее время обработки составит 3,84 сек.); по 2-му типу – не более 0,8 сек. (с очередями 4,91 сек.); по 3-му типу – не более 1,2 сек. (с очередями 6,33 сек.); по 4-му типу – не более 2,0 сек. (с очередями 8,50 сек.)

Таким образом, в результате моделирования принципиально найдено решение 1-й задачи. Т.е. ответ на 1-й вопрос «Сколько серверов необходимо для своевременной обработки всех запросов поступающих в «моделируемую Систему»?» таков: «Серверов необходимо столько, чтобы после распараллеливания процессов времена обработки запросов в автономном режиме составляли: по 1-му типу (приоритету) – не более 0,6 сек.; по 2-му типу – не более 0,8 сек.; по 3-му типу – не более 1,2 сек.; по 4-му типу – не более 2,0 сек. При этом должна применяться технология пакетной обработки запросов с естественным формированием пакетов и относительными приоритетами внутри пакета.

По 2-й задаче (вопрос: Как изменятся требования к количеству серверов, необходимых для своевременной обработки запросов в «моделируемой Системе», при смягчении требований к допустимому риску несвоевременной обработки запросов с уровня 10^{-6} до уровня 0,05? Т.е. смягчение требований к допустимому риску – в 50000 раз!). Для критерия 2, рекомендуемого ГОСТ Р 59341, требования стали такими (вероятность «успеха» 0,95 задается как дополнение до 1 допустимого риска 0.05):

- время обработки запросов 1-го типа не должно превышать 64 сек. с вероятностью не ниже 0,95, т.е. задается условие $P(t_{\text{полн.1}} \le 64 \text{ сек.}) \ge 0{,}95$;

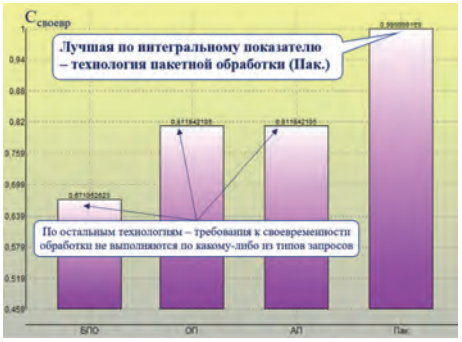


Рис. 6. Относительная доля своевременно обработанных в системе запросов, для которых выполнены требования бизнес-сообщества $C_{\text{своевр}}$ при допустимом риске 10^{-6}

- время обработки запросов 2-го типа не должно превышать 96 сек. с вероятностью не ниже 0,95, т.е. задается условие $P(t_{\text{полн.2}} \le 96 \text{ сек.}) \ge 0{,}95$;
- время обработки запросов 3-го типа не должно превышать 164 сек. с вероятностью не ниже 0,95, т.е. задается условие $P(t_{\text{полн.3}} \le 164 \text{ сек.}) \ge 0{,}95$;
- время обработки запросов 4-го типа не должно превышать 180 сек. с вероятностью не ниже 0,95, т.е. задается условие $P(t_{\text{полн.4}} \le 180 \text{ сек.}) \ge 0{,}95$.

При приблизительно задаваемом соотношении средние времена обработки запросов подбирались так, чтобы хотя бы для одной из рассматриваемых технологий диспетчеризации все видоизмененные требования к своевременности выполнялись.

По результатам расчетов по интегральному показателю $C_{\text{своевр}}$ опять оказывается лучшей технология пакетной обработки (Пак.) – см. рис. 7.

Рис. 7. Относительная доля своевременно обработанных в системе запросов, для которых выполнены требования бизнес-сообщества $C_{\text{своевр}}$ при допустимом риске 0,05

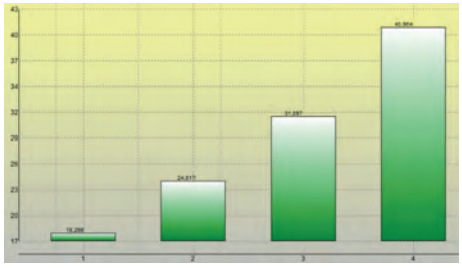


Рис. 8. Средние времена обработки запросов 1–4-го типов в секундах (с учетом очередей)

При этом по сравнению с допустимым риском 10^{-6} с учетом задержек в очередях среднее время обработки запросов 1-го типа составит 18,30 сек. (т.е. возрастет в 4,8 раза), 2-го типа – 24,02 сек. (возрастет в 4,9 раза), 3-го типа – 31,10 сек. (возрастет в 4,9 раза), 4-го типа – 40,96 сек. (возрастет в 4,8 раза) – см. рис. 8. А относительная доля своевременно обработанных в системе запросов, для которых выполнены заданные требования бизнес-сообщества, $C_{\text{своевр}}$ составит в процентном выражении 97,51 %. Такой эффект при решении задачи 2 достигается, когда исходные средние времена обработки запросов в автономном режиме (т.е. без очередей) составляют: по 1-му типу – не более 0,67 сек. (сравните: для задачи 1 – 0,6 сек. при допустимом риске 10^{-6}); по 2-му типу – не более 0,96 сек. (для задачи 1 – 0,8 сек.); по 3-му типу – не более 1,46 сек. (для задачи 1 – 1,2 сек.); по 4-му типу – не более 2,42 сек. (для задачи 1 – 2,0 сек.). Это очень несущественное смягчение требований к производительности серверов при смягчении требований к допустимому риску несвоевременной обработки запросов с уровня 10^{-6} до уровня 0,05, т.е. в 50000 раз (!).

Таким образом, в результате моделирования принципиально найдено решение 2-й задачи. Т.е. ответ на 2-й вопрос таков: «Серверов необходимо столько, чтобы после распараллеливания процессов времена обработки запросов в автономном режиме составляли: по 1-му типу – не более 0,67 сек.; по 2-му типу – не более 0,96 сек.; по 3-му типу – не более 1,46 сек.; по 4-му типу – не более 2,42 сек.». При этом был выявлен важный скрытый эффект: смягчение допустимого риска с высокого уровня 10^{-6} до 0,05 (применимого для обычных ИС организационного типа) приведет лишь к послаблениям по производительности обслуживающих серверов на 10–20 %. Т.е. способ снизить затраты на производительность и количество серверов путем смягчения допустимых рисков несвоевременной обработки запросов до уровня 0,05 является абсолютно бесперспективным.

После найденных решений для 1-й и 2-й задач становятся понятными возможные подходы к решениям по 3-й и 4-й задачам.

Поставленный вопрос по 3-й задаче примера: «Какое количество серверов необходимо иметь для обеспечения гарантированной своевременности обработки запросов при некоторой фиксированной степени распараллеливания процессов в их обработке в «моделируемой Системе» и заданных ограничениях? Предлагаемый подход к решению 3-й задачи таков: «Гарантии должны быть связаны с задаваемой вероятностью своевременной обработки (не менее 0,999999, что эквивалентно допустимому риску 10^{-6}) и применением пакетной технологии диспетчеризации. Для искомого ответа достаточно оценить, сколько серверов при распараллеливании процессов обеспечат временные требования к обработке запросов в автономном режиме, обоснованные выше при исследованиях по вопросам 1 и 2. Если решение приемлемо при существующих ограничениях, следует остановиться, т.е. ответ найден. Если ожидаемые затраты и условия неприемлемы (т.к. производительные серверы – это суть затраты денег, энергии и пр.), это означает, что требования при задаваемых ограничениях невыполнимы, т.е. в принятой постановке вопроса задача не имеет решения».

Поставленный вопрос по 4-й задаче: «Как оптимизировать степень распараллеливания процессов при обработке запроса каждого типа в Системе, чтобы избежать излишних затрат и при этом обеспечить требуемую своевременность?». Понимая, что в общем случае алгоритмическое выполнение программы обработки запросов состоит из составных распараллеливаемых заданий, предлагаемый подход к решению 4-й задачи следующий: «Оптимизация должна заключаться в формальном решении такой постановки задачи: для задаваемой вероятности своевременной обработки не менее 0,999999 определить такое минимальное число составных распараллеливаемых заданий, при котором на выделенном множестве серверов с принятой пакетной технологией диспетчеризации будут обеспечены следующие временные характеристики обработки запросов после распараллеливания (на незагруженных серверах при отсутствии очередей): по 1-му типу (приоритету) – не более 0,6 сек.; по 2-му типу – не более 0,8 сек.; по 3-му типу – не более 1,2 сек.; по 4-му типу – не более 2,0 сек. При этом предполагается наличие иных задаваемых ограничений (стоимостных, технических, ресурсных, климатических и пр.)».

Примечание. Для других технологий диспетчеризации решения рассмотренных в 2.4.2. задач 1–4 будут иными.

2.5. Модели для оценки полноты используемой информации

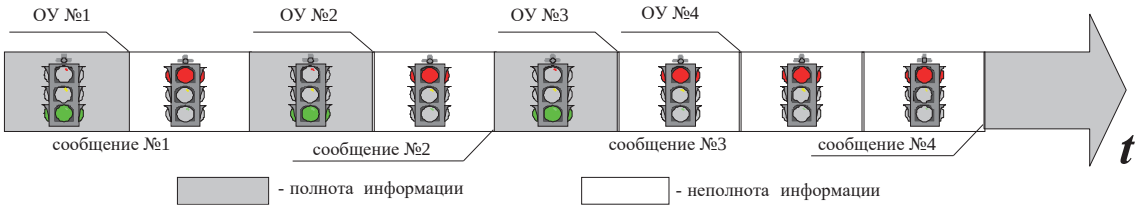
2.5.1. Общее

Под полнотой выходной информации в системе понимается свойство выходной информации отражать состояния всех требуемых объектов учета предметной области системы. Слагается из полноты реализации функций системы, полноты ввода первоначальной информации и полноты оперативного отражения объектов учета в системе.

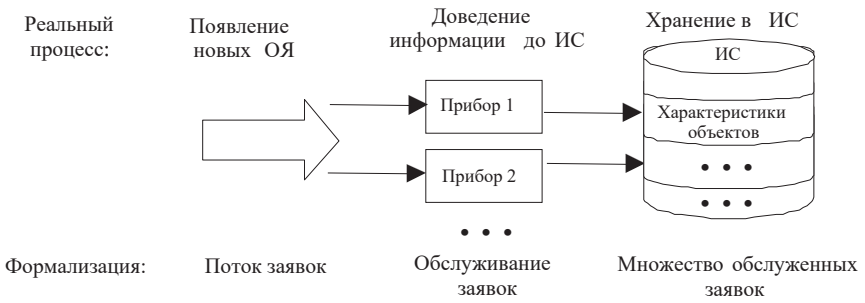
Анализ функционирования ИС показывает, что при решении некоторых задач нередко оказывается необходимым учет множества объектов и явлений, первоначальное возникновение которых в реальности имеет случайный характер. Примерами такого рода задач служат задачи слежения за состоянием местности в условиях чрезвычайной ситуации (например, пожара или наводнения), учета грузов на таможне и др. Выходную информацию будем называть полной, если в ней отражены состояния всех существующих в реальности объектов учета и явлений, необходимых для эффективного выполнения должностными лицами ИС своих функциональных обязанностей. Необходимо отличать полноту представляемой информации от ее достоверности: полнота относится лишь к вновь появляющимся объектам учета и явлениям, а достоверность – как к новым, так и к уже отраженным в ИС. Следовательно, информация может быть полной, но недостоверной.

Сущность влияния неполноты информации на принятие решения состоит в невозможности учета всех объектов учета и явлений (ОУ), характеризующих формальное состояние реальной действительности и влияющих на принимаемые решения. В результате логика принятия решения может оказаться неадекватной в сложившейся ситуации, т.е. решение может оказаться просто неверным – см. рис. 9.

Под полнотой оперативного отражения объектов учета в системе понимается свойство системы



а) Процессы появления новых объектов учета (ОУ) и доведения информации о них до ИС



б) Моделирующая система массового обслуживания M/G/∞.

Рис. 9. Формализация процессов отражения в ИС информации о новых появляющихся объектах учета

отражать требуемые состояния реально существующих объектов учета, в том числе впервые появляющихся в процессе функционирования системы и подлежащих учету в системе согласно ее функциональному назначению. Для оценки полноты оперативного отражения в системе новых объектов и явлений применяется «Модель для оценки полноты оперативного отражения в системе новых объектов и явлений (ОЯ)» из ГОСТ Р 59341, приложения В.3.4. Облик рекомендуемой базовой модели массового обслуживания M/G/∞ с привязкой к обозначениям исходных данных в ГОСТ Р 59341 представлен на рис. 9б. При использовании этой модели отсутствие очереди означает, что все объекты, подлежащие учету, отражены в базе данных ИС.

В качестве исходных данных для моделирования используются:

λ — частота появления новых ОУ в процессе функционирования системы;

$T_{\text{база данных}}$ — среднее время подготовки, передачи и ввода новых ОУ в БД системы.

В результате моделирования рассчитываются частные показатели: вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{\text{полн}}$ и вероятностный показатель полноты оперативного отражения в системе новых объектов и явлений $Z_{\text{полн}}$, учитывающий эту вероятность и соответствующие условия α из ГОСТ Р 59341, приложения В.3.4.

2.5.2. Пример для оценки полноты

Этот пример демонстрирует подход к оценке полноты оперативного отражения объектов учета в такой ИС, как система дистанционного контроля (СДК) гипотетичной угольной шахты – см. подробнее ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов».

Объектами анализа являются информационные сообщения, впервые поступающие в базу данных (БД), и технологии сбора таких данных от источников в режиме реального времени функционирования СДК угольной шахты. Требования заказчика сформулированы следующим образом: должна быть обеспечена полнота отражения информации в СДК обо всех реальных событиях и явлениях, в частности, вероятность того, что в СДК полностью отражены состояния всех реально существующих критичных объектов и явлений (это – условия α по ГОСТ Р 59341):

- для чрезвычайных происшествий, угрожающих безопасности людей и среды их обитания, должна быть не ниже 0,98;
- для оперативной информации об обстановке (в т. ч. по условиям функционирования шахты) – не ниже 0,95;
- для статистической информации при управлении СДК – не ниже 0,9;
- для команд и приказов с условиями их выполнения – не ниже 0,95.

Положим, согласно выданным главному конструктору СДК постановкам функциональных задач и принятым неблагоприятным сценарием возникновения и развития возможных аварийных ситуаций установлена ожидаемая частота появления новых объектов учета:

- для информации о чрезвычайных происшествиях – до трех раз в сутки (расчетные варианты $i = 1, 2, 3$);
- для оперативной информации об обстановке – в среднем до одного раза в час ($i = 4, 5, 6$);
- для статистической информации при управлении СДК – 2 раза в неделю ($i = 7, 8, 9$);
- для единожды вводимой информации (команд и приказов с условиями их выполнения) – 6 раз в сутки ($i = 10$).

Для проведения требуемых оценок технические решения главного конструктора в части сбора информации описаны следующими исходными данными, позволяющими охарактеризовать существенные различия в среднем времени подготовки, передачи и ввода новых объектов учета в БД СДК (именно для анализа этих различий анализируемые варианты снабжены индексом $i = 1,\ldots,10$).

Для информации о чрезвычайных происшествиях предусмотрена ее подготовка человеком. При этом для детальной информации и ее визуального контроля подготовка занимает в среднем 20 мин ($i = 1$), для детальной информации с программным контролем – 10 мин ($i = 2$), для укрупненной информации – до 5 мин ($i = 3$).

Для оперативной информации об обстановке возможна подготовка ее человеком с визуальным контролем в среднем около 20 мин ($i = 4$) либо с программным контролем до 10 мин ($i = 5$), а для некоторых видов информации, формируемой с помощью автоматических датчиков, в среднем за 30 с ($i = 6$). Т. е. результаты для $i = 4$ характеризуют существующую систему ручного контроля на местах, а результаты для $i = 5, 6$ характеризуют СДК.

Для статистической информации возможна подготовка информации человеком в течение 20 мин ($i = 7$), для детальной информации с программным контролем – до 10 мин ($i = 8$), для укрупненной информации с программным контролем – до 5 мин ($i = 9$).

Для команд и приказов информация готовится человеком в среднем в течение 5 мин ($i = 10$).

Согласно предложенным техническим решениям предусмотрены:

– передача информации от источников по телефону за среднее время до 10 мин ($i = 1, 4, 7$) или

автоматизированно с использованием СДК – до 1 мин (i = 2, 3, 5, 6, 8, 9, 10);
- ввод поступившей информации в БД за среднее время человеком от 1 мин (i = 4) до 10 мин (i = 1, 2, 5, 7, 8) или автоматически в СДК за 20 с (i = 3, 6, 9, 10).

С использованием модели 2.5.1. осуществлена количественная оценка полноты оперативного отражения в СДК состояния всех реально существующих критичных объектов и явлений. Результаты расчетов для сравнения вариантов приведены на рисунке 10.

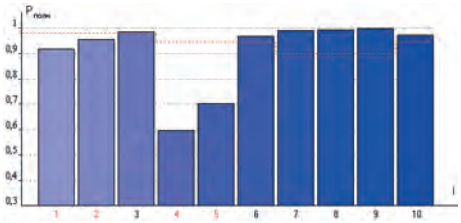


Рис. 10. Сравнительные оценки вариантов по вероятности того, что в СДК полностью отражены состояния всех реально существующих критичных объектов и явлений

Анализ результатов расчетов показывает (см. рис. 10):

- для информации о новых чрезвычайных происшествиях требованиям заказчика удовлетворяет лишь вариант оперативного обнаружения и подготовки укрупненной информации у источника с программным контролем, передачей через СДК с автоматическим вводом в БД (i = 3);
- для оперативной информации об обстановке требованиям заказчика отвечает лишь вариант с автоматическими датчиками СДК (i = 6). При этом другие варианты обнаружения и подготовки информации в течение 10–20 мин и длительного ввода ее в БД при передаче сколь угодно быстро не позволят обеспечить требуемую полноту оперативного отражения информации;
- для статистической информации при управлении СДК (i = 7, 8, 9) любой способ обнаружения и подготовки информации человеком, передачи любым из выбранных способов обеспечит полноту оперативного отражения в БД информации о реальных объектах учета и явлениях. Это объясняется относительной редкостью появления новой статистической информации;
- требуемая полнота оперативного отражения в системе реальных команд и приказов, поступающих через средства связи СДК (i = 10), будет обеспечена, что гарантируется быстротой передачи.

По результатам системного анализа сделан вывод: из множества сравниваемых технических решений лишь варианты 3, 6–10 отвечают задаваемым требованиям. Их реализация позволит обеспечить выполнение изначальных требований заказчика. Вместе с тем, заказчик, осознавая привычность работы в условиях неполноты информации на шахте, а также дороговизну технических изменений в проекте, вполне может согласиться на снижение изначальных требований к полноте оперируемой информации до такого уровня, что предъявляемые условия α по результатам моделирования выполняются. Эти результаты будут учтены при расчете интегрального риска в 3-й части статьи, где используется значение вероятностного показателя полноты оперативного отражения в системе новых объектов и явлений $Z_{\text{полн}}$, учитывающего рассчитываемое значение $P_{\text{полн}}$ и соответствующие условия α из ГОСТ Р 59341, приложения В.3.4 по допустимой вероятности того, что в СДК полностью отражены состояния всех реально существующих критичных объектов и явлений. Поскольку все требования к полноте оперируемой информации выполнены, в примере 3-й части статьи соответствующий показатель $Z_{\text{полн}}$ полагается равным 1.

2.6. Модели для оценки актуальности используемой информации

2.6.1. Общее

Под актуальностью информации понимается свойство безошибочной информации отражать текущее состояние прикладной области системы со степенью приближения, достаточной для получения на ее основе достоверной выходной информации в интересах конечного пользователя. Рассогласование реальной и хранимой в БД информации вызвано устареванием информации в результате какого-либо значимого изменения до следующего обновления этого изменения в БД – см. рис. 11. Т.е. актуальность характеризует старение информации во времени.

Для оценки актуальности обновляемой информации применяется «Модель для оценки актуальности обновляемой информации» из ГОСТ Р 59341, приложение В.3.5.

В качестве исходных данных используются:

ξ — среднее время между значимыми изменениями реальной информации относительно информации, хранимой в системе (т. е. ξ^{-1} — частота значимого изменения);

$T_{\text{база данных}}$ – среднее время подготовки, передачи и ввода в БД данных от источников;

q – среднее время между соседними обновлениями данных (т. е. q^{-1} – частота обновления данных) в системе при обновлении ее по регламенту;

В результате моделирования рассчитываются частные показатели: вероятность сохранения актуальности информации на момент ее использования $P_{\text{акт}}$

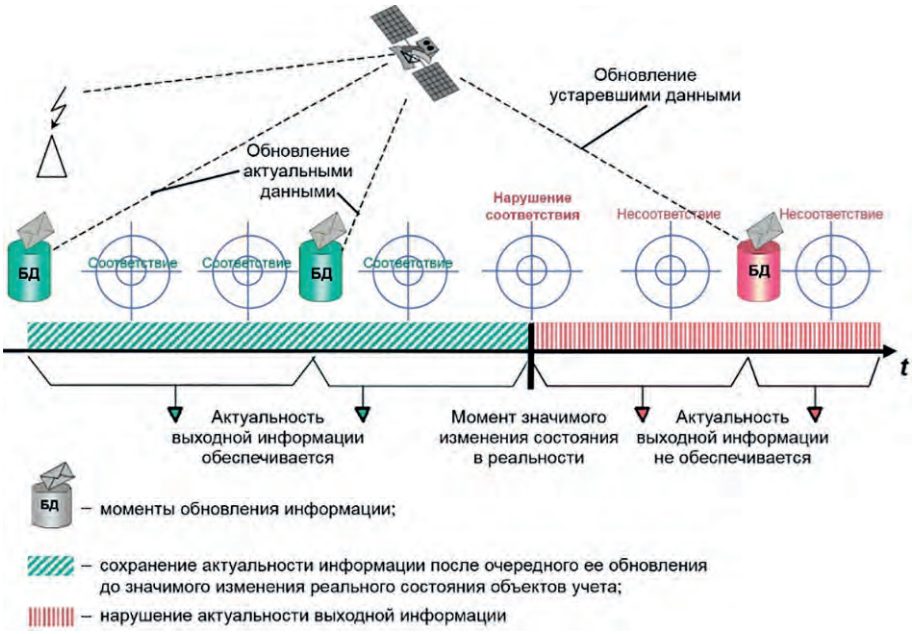


Рис. 11. Иллюстрация формирования актуальности выходной информации

и вероятностный показатель актуальности информации в системе $Z_{акт}$, учитывающий и соответствующие условия α из ГОСТ Р 59341, приложения В.3.5.

2.6.2. Пример для оценки актуальности

Важной практической задачей при создании и организации эффективного функционирования СДК является определение научно обоснованного периода обновления данных о состоянии параметров контролируемого оборудования и среды эксплуатации угольной шахты (например, давления, температуры, напряжения, загазованности и др.). С одной стороны, обновление данных по мере значимого изменения состояния оборудования необходимо для обеспечения достоверности информации с последующим ее применением по назначению. С другой стороны, слишком частое обновление этих данных необоснованно перегружает каналы связи и компьютерную память, приводит к программным сбоям, создает недопустимые временные задержки, может рассинхронизировать информационные процессы в СДК, нарушая тем самым режим реального времени функционирования самой СДК и лишая необходимой информационно-аналитической поддержки должностных лиц в процессе управления информацией на шахте. Учитывая результаты примера 2.5.2. о достижимости полноты отражения оперативной информации об обстановке с вероятностью не ниже $P_{полн} = 0{,}95$, задача формализована главным конструктором следующим образом: определить такой рациональный период обновления информации в СДК, при котором актуальность используемой информации будет не ниже, чем 0,95.

Анализ совокупности обновляемой информации при круглосуточной загрузке оборудования позволил выявить два варианта условий:

- обычные условия загрузки оборудования, характеризуемые частотой значимого изменения состояния оборудования 36 раз в сутки;
- условия наивысшей загрузки, возникающие для некоторого оборудования случайным образом (например, для вентиляторных установок или модульных дегазационных установок при повышенных скоплениях на местах газа метана), продолжающиеся несколько часов в сутки и характеризуемые частотой значимого изменения состояния оборудования 3 раза в час.

Среднее время съема, передачи и ввода в БД СДК телеметрических данных от оборудования составляет в среднем 16 с. Еще несколько секунд уходит на аналитическую обработку и доведение результатов обработки до пользователей. Это означает, что обновление чаще 25–30 с нецелесообразно из-за перегрузки и вычислительной неспособности своевременно обработать такую часто обновляемую информацию от сотен источников.

Моделирование для определения искомого периода обновления информации в СДК осуществлено по этим исходным данным с использованием модели 2.6.1. Сравнительные результаты расчетов приведены на рисунках 12–15.

Анализ результатов расчетов показывает, что для обеспечения актуальности информации в СДК с вероятностью не ниже 0,95, период обновления может быть выбран следующим образом: для обычных

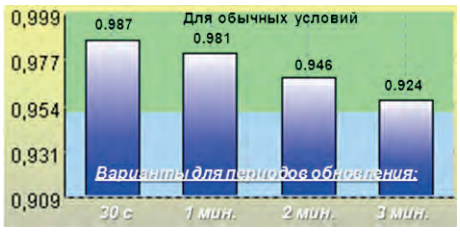


Рис. 12. Вероятность сохранения актуальности информации для обычных условий загрузки оборудования

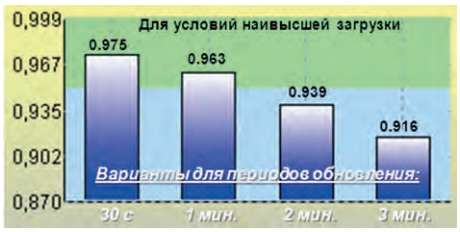


Рис. 13. Вероятность сохранения актуальности информации для условий наивысшей загрузки оборудования

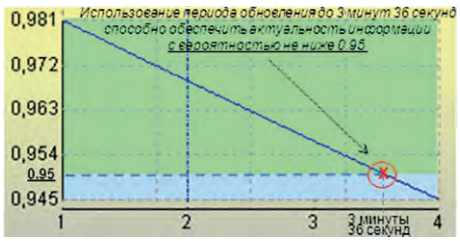


Рис. 14. Зависимость вероятности сохранения актуальности информации для обычных условий загрузки оборудования от периода обновления (в минутах)

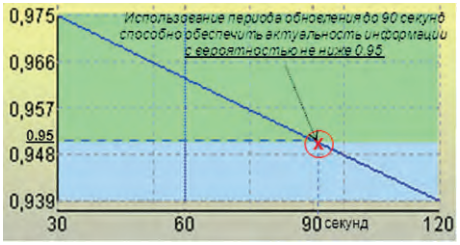


Рис. 15. Зависимость вероятности сохранения актуальности информации для условий наивысшей загрузки оборудования от периода обновления (в секундах)

условий загрузки оборудования – до 3 мин 36 с; для условий наивысшей загрузки – до 90 с. В результате системного анализа определено: из соображений недопущения вычислительной перегрузки СДК наиболее рациональным в условиях неопределенности функционирования шахты признан период обновления информации в СДК, равный 90 с.

Для определенности при расчете интегрального риска нарушения реализации процесса управления информацией системы в части 3 статьи использована достигаемая вероятность сохранения актуальности информации $P_{акт} = 0{,}95$. Эти результаты будут учтены при определении значения вероятностного показателя $Z_{акт}$, учитывающего условия и соответствующие им α из ГОСТ Р 59341, приложения В.3.5. Поскольку все требования к актуальности оперируемой информации выполнены, в примере 3-й части статьи этот показатель $Z_{акт}$ полагается равным 1.

2.7. Модели для оценки безошибочности информации после контроля

2.7.1. Общее

Под безошибочностью информации понимается свойство информации не иметь явных или скрытых ошибок и/или искажений. Понятие ошибки должно быть определено в эксплуатационной документации для каждой конкретной задачи ИС в зависимости от целевого назначения информации.

Модель процессов анализа каких-либо объектов (например, информации, образцов материала, событий, результатов работы и др.) поясним на примере.

Модель может использоваться для оценки безошибочности информации в результате контроля и для оценки корректности информации в результате ее обработки.

Определение: информация считается безошибочной в результате контроля, если в процессе контроля до истечения заданного срока контроля все наличествующие ошибки выявлены (и, соответственно, исправлены) и новые ошибки не внесены.

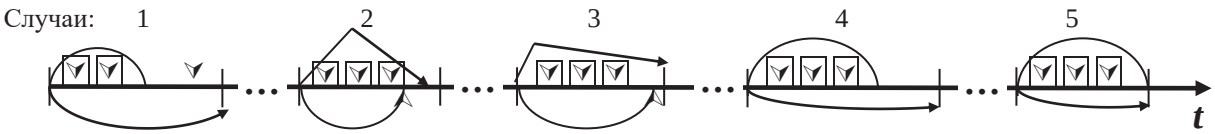
Определение: информация считается корректно обработанной, если в процессе ее анализа до истечения заданного срока обработки все принципиальные моменты учтены и алгоритмические ошибки не допущены.

Поскольку содержание модели для оценки корректности информации в результате ее обработки отличается лишь формулировкой исходных данных, приведенных в подразделе 2.8., то ниже ограничимся изложением содержания модели в приложении к контролю информации. Суть формализации отражена на рис. 16:

Случаи 1, 2, 3 характеризуют наличие ошибок после контроля, для случаев 4, 5 безошибочность после контроля обеспечена.

Случай 1 – наработка на ошибку или допустимое время контроля истекли раньше, чем закончился проверяемый документ, и после этого осталась хотя бы одна наличествующая ошибка. Ошибки контроля 1-го рода при этом не допускались.

Случай 2 – допустимое время контроля истекло раньше, чем закончился проверяемый документ, однако в непроверенной части ошибок не осталось. Вместе с тем, во время работы были допущены ошибки контроля 1-го рода.



- наличие изначальной ошибки в проверяемом документе;
- выявленная и исправленная ошибка;
- ошибка, случайно внесенная контролером (ошибка контроля 1-го рода);
- минимальное из двух времен:
а) периода непрерывной работы контролера (например, для контролера-человека по истечении этого периода следует восстановительный отдых, для программных средств контроля - время их непрерывного использования);
б) времени реального контроля документа, определяемого его объемом и скоростью контроля;
- задаваемое допустимое время контроля (истекает в момент пересечения оси *t* со стрелкой);
- минимальное из двух времен:
а) времени наработки контролера на ошибку, по истечении которого наличествующая ошибка пропускается (ошибка контроля 2-го рода);
б) задаваемого допустимого времени контроля;
- время до свершения первой ошибки контроля 1-го рода.

Рис. 16. Иллюстрация формальных процессов контроля безошибочности информации (фрагмент)

Случай 3 – допустимое время контроля не истекло раньше, чем закончился проверяемый документ, вследствие чего все изначальные ошибки выявлены и исправлены. Вместе с тем, во время работы были допущены ошибки контроля 1-го рода.

Случаи 4 и 5 — все ошибки выявлены и исправлены, и новые не внесены. При этом случай 4 аналогичен случаю 2, а случай 5 — случаю 3 с тем отличием, что ошибки 1-го рода не были допущены.

Для оценки безошибочности информации после контроля применяется «Модель для оценки безошибочности информации после контроля» из ГОСТ Р 59341, приложение В.3.6.

В качестве исходных данных используются:

V – объем контролируемой информации;

μ – доля первоначальных ошибок в контролируемой информации в объеме V (до контроля), т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν – средняя скорость контроля информации;

n — частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки);

$T_{нар}$ – среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной (для программно-технических средств — это время наработки на отказ);

$T_{непр}$ – период непрерывной работы контролера;

$T_{зад}$ – задаваемое время на контроль информации.

В результате моделирования рассчитываются частные показатели: вероятность отсутствия ошибок в информации после ее контроля $P_{безош}$ и вероятностный показатель безошибочности информации в системе $Z_{безош}$, учитывающий и соответствующие условия α из ГОСТ Р 59341, приложения В.3.6.

2.7.2. Пример для оценки безошибочности

Объектами анализа являются информационные ресурсы, вводимые в СДК, и технологии контроля их безошибочности. При проектировании СДК необходимо обосновать технологию контроля информации, обеспечивающую безошибочность входной информации. Требования заказчика сформулированы следующим образом: используемые технологии контроля входной формализованной и неформализованной информации должны обеспечивать ее безошибочность, в частности, вероятность отсутствия ошибки во входном сообщении, вводимом в БД СДК, должна быть не ниже 0,95, при этом допустимое время контроля не должно превышать 10 мин для графических документов и входных обобщенных документов до 10000 знаков и 1 ч для детальных документов объемом до 50000 знаков.

Для проведения требуемых оценок технические решения главного конструктора в части контроля информации описаны следующими исходными данными, позволяющими охарактеризовать существенные различия в рассматриваемых вариантах технологий контроля (именно для анализа этих различий анализируемые варианты снабжены индексом $i = 1,\ldots,10$). Согласно постановкам функциональных

задач информация, подлежащая контролю, обладает следующими характеристиками: средний объем коротких документов составляет в среднем 20 контролируемых объектов для графической информации (расчетные варианты $i = 1, 2$), 10000 текстовых знаков для обобщенных документов ($i = 3, 4, 7–10$) и 50000 знаков для детальных документов ($i = 5, 6$).

Для оценки безошибочности информации в СДК технические решения главного конструктора предусматривают осуществление лишь визуального контроля всей информации. С применением настоящей методики осуществляется количественная оценка ожидаемой безошибочности используемой информации и выявление необходимости создания вспомогательных средств программного контроля и обоснования системных требований к ним.

По результатам сравнения с аналогами установлено, что частота ошибок в документах может составлять одну ошибку на 100 графических объектов ($i = 1, 2$), одну ошибку на 100 знаков ($i = 3, 5, 7, 8$) или 200 знаков ($i = 4, 6$) неформализованной информации. В результате натурных экспериментов и сравнения с аналогами установлено, что технология контроля информации характеризуется следующими исходными данными:

- скорость контроля равна 20 объектам в минуту для графической информации ($i = 1, 2$), 2000 табличным знакам в минуту ($i = 3–6$) без программной поддержки и 6000 знакам в минуту (i = 7–10) с использованием средств программного контроля;
- частота ошибок контроля 1-го рода составляет одну ошибку на 100 мин работы для высококвалифицированного контролера ($i = 1, 3, 5$) и одну ошибку на 50 мин для контролера средней квалификации ($i = 2, 4, 6$). Кроме того, при поддержке программными средствами контроля частота ошибок 1-го рода может быть снижена на порядок, т. е. для высококвалифицированного контролера она составит одну ошибку на 16 ч ($i = 7, 9$), а для контролера средней квалификации – одну ошибку на 8 ч ($i = 8, 10$) работы;
- среднее время наработки на ошибку 2-го рода соответственно составляет 1 ч для высококвалифицированного контролера ($i = 1, 3, 5, 7, 9$) и 40 мин для среднеквалифицированного ($i = 2, 4, 6, 8, 10$) контролера;
- среднее непрерывное время работы человека-контролера составляет 45 мин ($i = 1–10$), после чего следует необходимое восстановление концентрации внимания (вплоть до смены контролера);
- на однократный контроль короткого и обобщенного документа отводится в среднем 10 мин ($i = 1–4, 7–10$), а на однократный контроль детального документа – 1 ч ($i = 5, 6$).

При моделировании предусмотрено использование повторного визуального контроля ($i = 9, 10$), причем в качестве исходной доли ошибок после первого контроля выступают результаты расчетов по настоящей методике соответственно для вариантов $i = 7$ и $i = 8$.

С использованием модели В.3.6 по этим исходным данным проведена количественная оценка безошибочности информации после контроля. Сравнительные результаты расчетов приведены на рисунках 17 и 18.

Рис. 17. Вероятность отсутствия ошибок в информации без контроля для 10 вариантов сравнения

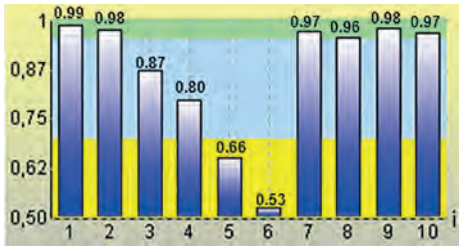


Рис. 18. Вероятность отсутствия ошибок в информации после контроля для 10 вариантов сравнения

Анализ результатов расчетов показывает:

- для коротких графических документов вероятность отсутствия ошибок после контроля специалистом средней и высокой квалификации превышает 0,98, причем она по-прежнему будет удовлетворять требованиям при возможном увеличении среднего объема контролируемой информации до 40 объектов ($i = 1, 2$);
- для документов объемом 10000–50000 знаков ($i = 3–6$) ошибки без контроля неизбежны. При контроле без поддержки программными средствами вероятность отсутствия ошибок ниже требуемой (от 0,53 до 0,87) независимо от квалификации проверяющих;
- применение поддерживающих программных средств контроля ($i = 7, 8$) позволяет повысить вероятность отсутствия ошибок в документах объемом 10000 знаков до уровня 0,96–0,97;
- применение повторного визуального контроля с использованием программных средств ($i = 9, 10$)

оказывается избыточным как для высококвалифицированных, так и среднеквалифицированных контролеров по сравнению с вариантами $i = 7, 8$.

Вывод: для выполнения заданных требований выявлена объективная необходимость разработки специальных программных средств поддержки контроля информации в СДК. Рекомендации: основными требованиями к разработке этих программных средств, а в последующем – и для эксплуатационной документации должны быть:

- требования к скорости контроля – не ниже 20 графических объектов в минуту и 6000 текстовых знаков в минуту;
- требования к допустимой частоте ошибок первого рода – не чаще одной ошибки за 500 мин работы;
- требования к допустимой наработке до первого пропуска ошибки – в среднем не менее 40 мин;
- регламентация времени работы человека-контролера, в частности непрерывное время контроля не должно превышать 45 мин.

Поскольку все требования к безошибочности информации в системе после контроля выполнены, в примере 3-й части статьи показатель $Z_{\text{безош}}$ полагается равным 1.

2.8. Модели для оценки корректности информации после обработки

2.8.1. Общее

Под корректностью обработки информации в системе понимается свойство системы обеспечивать получение правильных согласованных результатов или эффектов обработки информации. Информация считается корректно обработанной, если в процессе ее анализа до истечения заданного срока обработки все принципиальные моменты учтены и алгоритмические ошибки не допущены. Требуемая корректность обработки информации программно-аналитическими средствами в системе и выходной информации от системы пользователями обеспечивается на основе применения эффективных способов анализа информации (как с использованием, так и без использования прикладного программного обеспечения), позволяющих учесть важную для принятия решения информацию и не допустить алгоритмических ошибок при анализе всего объема информации. Корректность в обработке информации является следствием приемлемого соотношения между объемом анализируемой информации, частью важной для принятия решения информации, подлежащей учету, скоростью анализа информации, частотой ошибок аналитика, длительностью его непрерывной работы и ограничениями на допустимое время обработки.

Формализация процессов обработки информации в системе полностью аналогична формализации для модели 2.7.1. с точностью до переопределений исходных данных. Для оценки корректности обработки информации применяется «Модель для оценки корректности обработки информации» из ГОСТ Р 59341, приложение В.3.7.

В качестве исходных данных используются:

V – объем информации, подлежащий обработке (анализу);

μ – часть важной для принятия решения информации, которая должна быть объективно использована при обработке (анализе) информации объема V, т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

v – скорость обработки (анализа);

n – частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной);

$T_{\text{нар}}$ – среднее время наработки на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это аналог ошибки контроля 2-го рода);

$T_{\text{непр}}$ – период непрерывной работы аналитика (в качестве аналитика могут выступать программно-аналитические средства или пользователь системы);

$T_{\text{зад}}$ – задаваемое время на обработку (анализ) информации.

В результате моделирования рассчитываются частные показатели: вероятность получения корректных результатов обработки информации $P_{\text{корр}}$ и вероятностный показатель корректности обработки информации в системе $Z_{\text{корр}}$, учитывающий и соответствующие условия α из ГОСТ Р 59341, приложения В.3.7.

2.8.2. Пример для оценки корректности

Объектами анализа являются информационные активы СДК и технологии их обработки по назначению. При проектировании СДК главный конструктор оценивает целесообразность разработки вспомогательных экспертных систем для обработки информации. Заказчик использует настоящую методику для количественной оценки ожидаемой корректности обработки информации в режиме реального времени функционирования СДК, а главный конструктор – для дальнейшего выявления рациональных технических способов удовлетворения требований технического задания. Согласно постановкам функциональных задач аналитики (операторы) анализируют те же объемы информации, что и в примере 2.7.2., но уже с целями подготовки и принятия прагматических решений по обеспечению промышленной безопасности на предприятии. Для проведения требуемых оценок с учетом существенных различий в рассматриваемых вариантах технологий обработки информации

анализируемые варианты по-прежнему снабжены индексом $i = 1,...,10$. Т. е. обобщенная информация характеризуется объемом до 20 объектов ($i = 1, 2$), а детальная информация – объемом до 10000 знаков ($i = 3, 4, 7–10$) и до 50000 знаков ($i = 5, 6$). При анализе информации осуществляется не контроль, а семантическая обработка аналитиком. Примером малого объема анализируемой информации может служить обобщенное состояние контролируемых объектов на электронной карте с использованием мнемосхем.

Примером большего объема анализируемой информации может служить детальная информация о состоянии контролируемого оборудования шахты. Таковых объектов учета для СДК, охватывающих несколько шахт, могут быть тысячи и десятки тысяч.

Пусть в обобщенной информации малого объема (i = расчетные варианты 1, 2) вся информация является принципиальной, в детальной (для $i = 3–10$) процент принципиальной информации не превышает 50 %. В обязанности аналитика (оператора) входят корректные выделение и осмысление этой информации в режиме реального времени для последующего использования ее по назначению. Требуемый уровень корректности обработки информации по выбранному вероятностному показателю – не ниже 0,95.

В результате натурных экспериментов и сравнения с аналогами установлено, что технология обработки информации характеризуется следующими исходными данными. Скорость обработки информации составляет 20 объектов в минуту для аналитика как высокого ($i = 1, 3, 5, 7, 9$), так и среднего уровня квалификации ($i = 2, 4, 6, 8, 10$) и 2000 знаков в минуту для оператора-аналитика ($i = 3–5$). Использование специальной экспертной системы автоматической обработки данных (целесообразность создания которой оценивается Главным конструктором, $i = 6–10$) позволяет повысить скорость обработки детальной информации аналитиком до 6000 знаков в минуту. Частота ошибок анализа 1-го рода, среднее время наработки на алгоритмическую ошибку и непрерывное время работы человека (аналитика, оператора) сохраняются теми же, что и в примере 5 для контроля информации. Допустимое время оперативной обработки информации объемом 10000 знаков составляет 10 мин для $i = 1–4, 7, 8$, при детальной аналитической обработке документов объемом 50000 знаков – до одного часа ($i = 5, 6$).

Моделирование осуществлено по этим исходным данным с использованием рекомендаций 2.8.1. – см. результаты расчетов на рис. 19, 20.

Анализ обобщенных результатов расчетов показывает:

- вероятность получения корректных результатов обработки обобщенной информации составляет 0,96–0,97 для аналитика как среднего, так и высокого уровня квалификации ($i = 1, 2$) из-за сравнительно небольшого объема анализируемой информации. Часть неучтенной информации не превысит 5 %;
- для документов объемом 10000 знаков за счет применения специальной экспертной системы ($i = 7, 8$) корректность обработки информации оператором как среднего, так и высокого уровня квалификации составит 0,96–0,97 ($i = 7, 8$) против 0,80–0,88 (для $i = 3, 4$), характерных для варианта обработки информации без ее использования. При этом часть неучтенной информации составит для $i = 7, 8$ лишь 1,5–2.2 % против 6,2–10,1 % для $i = 3, 4$;
- для документов объемом 50000 знаков применение оператором экспертной системы ($i = 6$) позволит повысить вероятность корректной обработки до уровня 0,81 против 0,66 без ее использования ($i = 5$), но для корректности обработки информации этого явно недостаточно;
- использование в автоматическом режиме специальной экспертной системы обеспечит корректность обработки лишь на уровне 0.58–0,59 ($i = 9, 10$), что объясняется слабой производительностью применяемых программно-технических средств, не позволяющих за одну минуту автоматически обработать весь объем принципиальной информации. Часть неучтенной информации превысит 20 %.

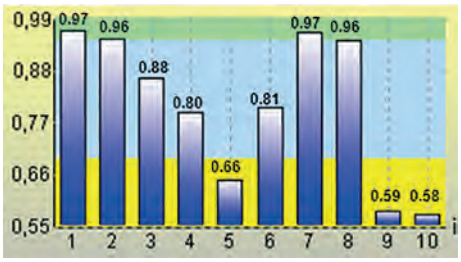


Рис. 19. Вероятность получения корректных результатов обработки информации для 10 вариантов сравнения

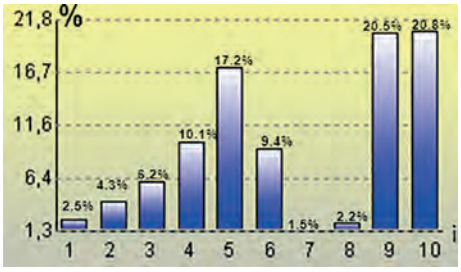


Рис. 20. Часть принципиальной информации, не учтенная в процессе обработки для 10 вариантов сравнения

Учитывая потенциальные возможности специальной экспертной системы поддержки принятия решений и ее осуществимость, при расчете интегрального риска в примере 3-й части статьи использован вероятностный коэффициент корректности обработки информации в системе $Z_{\text{корр.}} = 1$.

2.9. Модели для оценки безошибочности действий пользователей и персонала

Модель позволяет оценить воздействие «человеческого фактора» на уровне вероятности безошибочных действий пользователей и персонала системы в течение заданного периода прогноза $P_{\text{чел}}(_{\text{Тзад}})$.

Требуемая безошибочность действий пользователей и персонала системы в течение заданного времени обеспечивается на основе профессионального отбора, специальной подготовки пользователей и обслуживающего персонала системы, реализации и использования эффективных средств программной поддержки. Безошибочность является следствием приемлемого соотношения между частотой возможных ошибок, временем их обнаружения и исправления.

Для оценки безошибочности действий пользователей и персонала системы в течение заданного периода прогноза применяются одноименные модели из ГОСТ Р 59341, приложения В.3.8.

В качестве исходных данных используются:

σ – частота возникновения источников угроз из-за «человеческого фактора»;

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы;

$T_{\text{меж}}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{\text{диаг}}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{\text{восст}}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

$T_{\text{зад}}$ – задаваемая длительность периода прогноза.

В результате моделирования рассчитываются частные показатели: вероятность безошибочных действий пользователей и персонала системы в течение заданного периода прогноза $P_{\text{чел}}(_{\text{Тзад}})$ и вероятностный показатель безошибочности действий пользователей и персонала системы в течение заданного периода прогноза $Z_{\text{чел}}(_{\text{Тзад}})$, учитывающего и соответствующие условия α из ГОСТ Р 59341, приложения В.3.8.

Учитывая математическую идентичность моделей для оценки надежности предоставления информации и безошибочности действий пользователей и персонала системы, некоторые сравнительные возможности моделирования приведены в 3-й части статьи с использованием понятий сложной «моделируемой системы».

2.10. Модель для оценки защищенности системы от опасных программно-технических воздействий

Для оценки безопасности информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий применяется «Модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий» из ГОСТ Р 59341, приложение В.3.9.2.

В качестве исходных данных используются:

σ – частота возникновения источников угроз в виде источников опасных программно-технических воздействий, ведущих к нарушению безопасности информации;

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (т.е. выполняемого процесса или защищаемых активов, используемых при выполнении процесса) в результате опасных программно-технических воздействий;

$T_{\text{меж}}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{\text{диаг}}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{\text{восст}}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

$T_{\text{зад}}$ – задаваемая длительность периода прогноза.

В результате моделирования рассчитывается частный показатель: вероятность отсутствия опасного программно-технического воздействия на систему $P_{\text{возд}}(T_{\text{зад}})$ в течение заданного периода прогноза $T_{\text{зад}}$.

Учитывая математическую идентичность моделей для оценки надежности предоставления информации, безошибочности действий пользователей и персонала системы с моделью для оценки защищенности системы от опасных программно-технических воздействий, некоторые сравнительные возможности моделирования приведены в 3-й части статьи с использованием понятий сложной «моделируемой системы».

2.11. Модели для оценки защищенности активов от несанкционированного доступа (НСД)

2.11.1. Общее

Настоящая вероятностная модель справедлива для оценки защищенности ресурсов без учета периода их объективной ценности, т.е. лишь исходя из реализуемой технологии защиты. Другими словами, защищаемые ресурсы полагаются априори ценными в течение бесконечного периода времени.

Построение вероятностного пространства для оценки отсутствия воздействий в результате НСД осуществляется в предположении реализации в системе

элементов защиты ресурсов от потенциального нарушителя. В приложении к ИС защищаемыми являются в первую очередь информационные и программные ресурсы. Однако, модель является более общей, в качестве защищаемых могут выступать людские, материальные, финансовые и др. ресурсы согласно вербальной модели угроз (см. также сайт ФСТЭК России https://bdu.fstec.ru/).

Для доступа к хранимым в системе ресурсам выстраивается последовательность преград от злоумышленника с тем, чтобы допущенный пользователь, зная и реализуя алгоритм преодоления этих преград, мог решать свои задачи в установленном штатном режиме. В качестве нарушителя рассматривается лицо, не посвященное в тайну преодоления защитных преград. Вскрывая каким-либо доступным образом алгоритм преодоления преград, злоумышленник вполне может получить доступ к ресурсам системы.

Рассматривается наиболее тяжелый режим функционирования системы защиты в ожидании постоянной угрозы ее вскрытия. Нарушитель в состоянии проникнуть в систему лишь при условиях, что

- во-первых, ему станет известна система защиты в части, необходимой для достижения его целей;
- во-вторых, он успеет получить доступ к информационным и/или программным ресурсам системы до того, как эта система защиты видоизменится (после чего перед нарушителем возникнет проблема повторного преодоления защитных преград).

При моделировании действия «умного» нарушителя, оснащенного возможными высокотехнологичными средствами вскрытия системы зашиты, могут быть охарактеризованы лишь большей скоростью преодоления защитных преград.

Для оценки безопасности информации в части защищенности активов от НСД применяется одноименная модель из ГОСТ Р 59341, приложения В.3.9.3.

Таблица 1.

Характеристики сценария угроз НСД и системы защиты

Преграда	Частота смены значения параметра преграды	Среднее время преодоления преграды нарушителем	Возможный способ преодоления преграды
1. Охраняемая территория со сменой охраны	через 2 ч	30 мин	Скрытое проникновение на территорию
2. Пропускная система на объект СДК (в т. ч. доступ к рабочим местам пользователей со сменой службы контроля)	через 1 сут	10 мин	Подделка документов, сговор, обман
3. Электронный ключ для включения компьютера	через 5 лет (наработка до замены)	1 нед	Кража, принудительное изымание ключа, сговор
4. Пароль для входа в систему	через 1 мес	1 мес	Подсматривание, принудительное выпытывание, сговор, подбор пароля
5. Пароль для доступа к программным устройствам	через 1 мес	10 сут	Подсматривание, принудительное выпытывание, сговор, подбор пароля
6. Пароль для доступа к требуемой информации	через 1 мес	10 сут	Подсматривание, принудительное выпытывание, сговор, подбор пароля
7. Зарегистрированный внешний носитель информации для записи	через 1 год	1 сут	Кража, принудительная регистрация, сговор
8. Подтверждение подлинности пользователя в процессе сеанса	через 1 мес	1 сут	Подсматривание, принудительное выпытывание, сговор
9. Телемониторинг	через 5 лет (наработка до замены)	2 сут	Имитация неисправности, ложные ролики, маскировка под персонал, сговор
10. Шифрование информации со сменой ключей	через 1 мес	2 года	Расшифровка, сговор

В качестве исходных данных используются:

M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

f_m – среднее время между соседними изменениями параметров защиты m-й преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-й преграды.

В результате моделирования рассчитывается частный показатель: вероятность обеспечения защищенности активов системы от НСД – $P_{\text{НСД}}$..

2.11.2. Пример для оценки защищенности от НСД

Пример демонстрирует подход к оценке вероятности обеспечения защищенности активов СДК от несанкционированного доступа $P_{\text{НСД}}$.

Объектами анализа являются информационные и программные ресурсы СДК для построения на шахте эффективной защиты от НСД.

Анализируются возможности и целесообразность создания 10 преград для защиты от НСД. На основании вербальной модели угроз в таблице отражены предполагаемые характеристики сценария угроз НСД и системы защиты информации.

Моделирование осуществлено по этим исходным данным с использованием рекомендаций 2.11.1. Результаты расчетов отражены на рисунке 21.

Анализ полученных результатов расчета показывает следующее.

Первые 3 преграды преодолеваются с вероятностью около 0,745. Использование сменяемых паролей один раз в месяц для 4, 5 и 6 преград позволяет в три раза поднять защищенность с 0,255 до 0,872. Однако общая защищенность системы после введения первых шести преград остается слабой (0,872).

Введение 7, 8, 9 преград практически бесполезно, т.к. не обеспечивает заметного повышения защищенности системы для заданных значений исходных данных (0,877 по сравнению с 0,872).

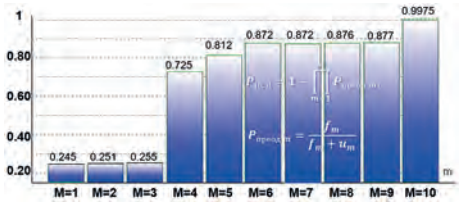


Рис. 21. Рост вероятности обеспечения защищенности активов СДК от НСД с увеличением количества и качества преград, m = 1,..., M

Использование криптографических средств защиты (10-я преграда) позволяет более существенно повысить защищенность информационных ресурсов от НСД – до уровня 0,9975. Это в 399 раз превышает вероятностный риск преодоления преград в системе защиты от НСД [0,9975/(1–0,9975)].

Для определенности при расчете интегрального риска с учетом требований по защите информации от НСД в примере 3-й части статьи использована достигаемая вероятность обеспечения защищенности активов СДК от НСД $P_{\text{НСД}} = 0{,}9975$.

2.12. Модели для оценки конфиденциальности используемой информации

2.12.1. Общее

Требуемая конфиденциальность информации обеспечивается на основе реализации мероприятий, гарантирующих защищенность информационных ресурсов системы от НСД до истечения периода объективной конфиденциальности (ПОК) данной информации. Моделируемые случаи соотношения между временем смены значений параметров преград системы защиты и их расшифровки (вскрытия) и периодом объективной конфиденциальности информации для одной преграды приведены на рисунке 22.

Случай 1 – НСД осуществлен до истечения ПОК. Случай 2 – НСД осуществлен после истечения ПОК. Случай 3 – НСД не состоялся. Случай 4 – НСД осуществлен, и период объективной ценности ресурсов

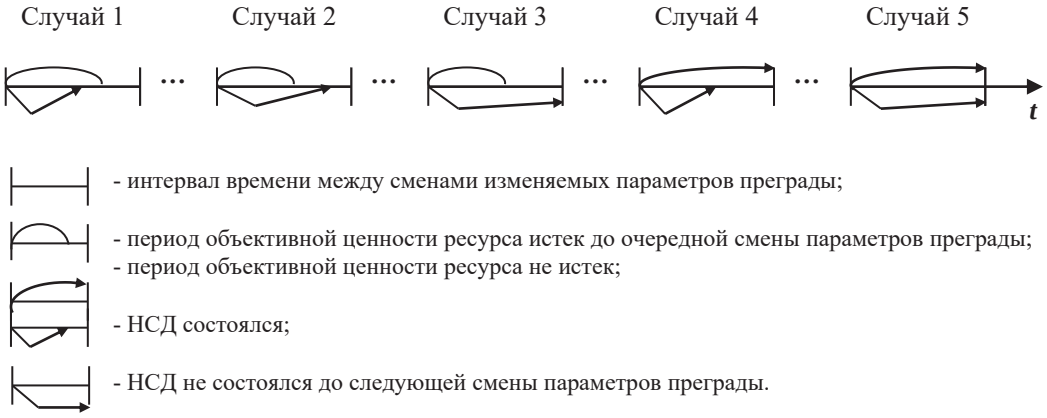


Рис. 22. Формализация процессов НСД с учетом ценности ресурсов

дольше, чем время между соседними сменами параметров системы защиты. Случай 5 – параметры системы защиты сменились раньше, чем истек ПОК и осуществлен НСД (для нарушителя требуется повторное преодоление преграды).

Для оценки безопасности информации в части сохранения конфиденциальности используемой информации применяются «Модель для оценки сохранения конфиденциальности используемой информации» из ГОСТ Р 59341, приложение В.3.9.3.

В качестве исходных данных используются:

M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

f_m – среднее время между соседними изменениями параметров защиты m-й преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-й преграды;

$T_{\text{конф}}$ – период объективной конфиденциальности используемой информации.

В результате моделирования рассчитывается частный показатель: вероятность сохранения конфиденциальности используемой информации $P_{\text{конф}}(T_{\text{конф}})$ в течение периода объективной конфиденциальности $T_{\text{конф}}$ (период $T_{\text{конф}}$ может играть роль периода прогноза $T_{\text{зад}}$).

2.12.2. Пример для оценки конфиденциальности используемой информации

Пример демонстрирует подход к оценке вероятности сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $P_{\text{конф}}(T_{\text{конф}})$.

Объектами анализа являются те же информационные и программные ресурсы СДК при тех же используемых преградах системы защиты от НСД. Дополнительно учтена длительность периода объективной конфиденциальности информации, характеризующего ценность ресурса. С учетом того, что большинство примеров в 3-й части статьи ориентированы на период прогноза 1 мес, в настоящем примере роль периода объективной конфиденциальности информации играет именно этот период прогноза. Характеристики десяти преград те же, что и в примере 2.11.2.

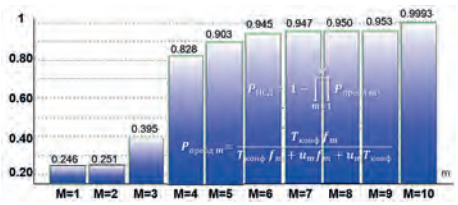


Рис. 23. Рост вероятности сохранения конфиденциальности используемой информации с увеличением количества и качества преград, m = 1,..., M

Моделирование осуществлено по исходным данным таблицы заданием $T_{\text{конф}}$ = 1 мес и использованием рекомендаций 2.12.1. Результаты расчетов отражены на рисунке 23.

Системный анализ полученных результатов расчета показывает следующее.

Использование первых 6 преград (охрана, пропускной режим, электронный ключ и различные системы паролей) обеспечит конфиденциальность информации с вероятностью не выше 0,945.

Использование всех 10 преград обеспечит требуемую конфиденциальность информации в системе: 0,9993, что более, чем в 1400 раз превышает вероятностный риск нарушения конфиденциальности информации [0,9993/(1— 0,9993)]. В условиях примера это может рассматриваться как более обоснованное значение показателя эффективности защиты информации.

Для определенности при расчете интегрального риска в 3-й части статьи использована достигаемая вероятность сохранения конфиденциальности используемой информации в течение месяца $P_{\text{конф}}(T_{\text{конф}}) = 0{,}9993$.

Выводы по 2-й части работы

1. Методические положения 1-й части статьи детализированы путем предложения следующих вероятностных моделей, позволяющих проведение исследований «моделируемых систем» в виде «черного ящика»: «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 опасных программно-технических воздействий»; «Модели для оценки защищенности активов от несанкционированного доступа»; «Модели для оценки конфиденциальности используемой информации». Также разъяснен предложенный «Метод использования универсальной вспомогательной модели показателя для определения исходных данных в расчетах».
2. Использование некоторых возможностей предложенных моделей продемонстрировано на примерах:

➢ оценки своевременности предоставления информации и выполнения операций в приложении

к решению практических задач, связанных с производительностью опорных узлов и региональных блокчейн-хабов гипотетичной информационной среды взаимодействия государственных и частных организаций;

- оценки и обеспечения полноты и актуальности используемой информации, безошибочности информации после контроля, корректности обработки информации, защищенности ресурсов ИС от НСД и сохранения конфиденциальности используемой информации в приложении к системе дистанционного контроля гипотетичной угольной шахты.

Демонстрация оценок других свойств, характеризующих качество функционирования ИС с помощью предложенных моделей, охватывающих понятия сложной «моделируемой системы», будет проведена в 3-й части статьи.

(Окончание статьи следует в №1–2025 журнала «Вопросы кибербезопасности»)

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., Петухов А. В., Щербина А. М. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа. М.: Изд. «Вооружение. Политика. Конверсия», 1994. 278 с.*
3. *Костогрызов А. И., Липаев В. В. Сертификация качества функционирования автоматизированных информационных систем. – М. Изд. «Вооружение, политика, конверсия», 1996. 278 с.*
4. *Костогрызов А. И., Нистратов Г. А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. – М. Изд. «Вооружение, политика, конверсия», 2004, 2-е изд. 2005. 395 с.*
5. *Костогрызов А. И., Степанов П. В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. «Вооружение, политика, конверсия», 2008. – 404 с.*
6. *A. Kostogryzov, A. Nistratov, G. Nistratov SOME APPLICABLE METHODS TO ANALYZE AND OPTIMIZE SYSTEM PROCESSES IN QUALITY MANAGEMENT («Некоторые прикладные методы для анализа и оптимизации системных процессов в управлении качеством») // InTech, 2012, ISBN979-953-307-778-8, 2012, pp. 127–196. http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management*
7. *Абросимов Н. В., Алешин А. В., Махутов Н. А. и др. /Под ред. Махутова Н. А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, 936 с.*
8. *Абросимов Н. В., Махутов Н. А. и др. / Под ред. Махутова Н. А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность. М.: МГОФ «Знание», 2018, 1016 с.*
9. *Probabilistic modeling in system engineering (Вероятностное моделирование в системной инженерии). InTechOpen, Edited by A. Kostogryzov, 2018, 279 p. URL: http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering*
10. *A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems (Вероятностные методы для когнитивного решения некоторых задач в системах искусственного интеллекта). Probability, combinatorics and control./ IntechOpen, 2020, pp. 3–34. URL: https://www.intechopen.com/books/probability-combinatorics-and-control*
11. *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.*
12. *Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Вероятностное упреждающее моделирование для оценок рисков в сложных системах). 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. *Хинчин А. Я. Работы по математической теории массового обслуживания. – М.: изд-во Физ. мат. лит., 1963.*
14. *Григолионис В. О сходимости сумм ступенчатых процессов к пуассоновскому // Теория вероятности и ее применения. Т.8, 1963, №2.*
15. *Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. М.: Наука. 1987.*
16. *Матвеев В. Ф., Ушаков В. Г. Системы массового обслуживания. М.: МГУ, 1984.*
17. *Костогрызов А. И., Назаров Л. В. Пакетная обработка требований в системе с относительным приоритетом// Изв. АН СССР сер. Техническая кибернетика. 1981, №3, С. 183–187.*
18. *Балыбердин В. А. Методы анализа мультипрограммных систем. – М. Радио и связь, 1982. – 152 с.*
19. *Балыбердин В. А. Оценка и оптимизация характеристик систем обработки данных. – М.: Радио и связь, 1987. 176 с.*
20. *Костогрызов А. И., Матвеев В. Ф. Анализ применения комбинированной дисциплины обслуживания в системах реального времени // Изв. АН СССР сер. Техническая кибернетика. 1986, №6, С. 79–84.*
21. *Костогрызов А. И. Пакетная обработка заявок в режиме равномерного разделения процессора с прерыванием // Изв. АН СССР сер. Техническая кибернетика. 1987, №4, С. 88–93.*
22. *Костогрызов А. И. Класс приоритетных дисциплин с комбинированием принципов обслуживания в порядке приоритета и пакетной обработки заявок. Анализ их свойств и возможностей применения в АСУ// Анализ стохастических систем методами исследования операций и теории надежности. К.: Ин-т кибернетики им. В. М. Глушкова АН УССР, 1987. С. 52–55.*
23. *Безкоровайный М. М., Костогрызов А. И., Львов В. М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. М.: Изд. «Вооружение. Политика. Конверсия», 2002. 304 с.*
24. *Kostogryzov A., Atakishchev O., Nistratov A., Nistratov G., Klimov S., Grigoriev L. The method of rational dispatching a sequence of heterogeneous repair works // Energetica. 2017. Vol.63, No 4, P. 154–162.*
25. *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*

26. 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.
27. Golosov P. E., Ronzhin A. F. Approaches to execution of sets of tasks with random processing time in coherent computational systems / Proceedings of the International Conference on Modern stochasticity: theory and applications. Kyiv. 10–14.09.2012. С. 33.
28. Lyu, Siwei & Farid, Hany. (2005). How Realistic is Photorealistic?. Signal Processing, IEEE Transactions on. 53. 845–850. 10.1109/TSP.2004.839896.
29. Rahmouni, Nicolas & Nozick, Vincent & Yamagishi, Junichi & Echizen, I. (2017). Distinguishing computer graphics from natural images using convolution neural networks. 1–6. 10.1109/WIFS.2017.8267647.
30. 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.

METHODOLOGICAL PROVISIONS ON PROBABILISTIC PREDICTION OF INFORMATION SYSTEMS OPERATION QUALITY. Part 2. MODELING USING «BLACK BOXES»

Kostogryzov A. I[6], Nistratov A. A.[7], Golosov P. E.[8]

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 2nd part of the work is to detail, in the interests of probabilistic analysis of the properties characterizing information systems operation quality, the general methodological provisions (summarized in the 1st part of the article), by proposing probabilistic models represented in the form of «black boxes».*

Research methods include: *methods of probability theory, methods of system analysis. Formally, «black box» acts as a modeled system when the initial data for modeling and output results are known, but the internal detail structure of the system is unknown. 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.*

Results of the 2nd part are: *models presented in the form of «black boxes» are proposed for the probabilistic analysis of the composite properties of the IS quality according to GOST R 59341-2021 «System engineering. Protection of information in system information management process».*

Scientific novelty: *The proposed models are aimed at achieving the general purpose of IS operation in various functional applications – to ensure the reliability and timeliness of providing the necessary information, completeness, validity and security (the purpose is formulated in the 1st part of the article). The use of models makes it possible to carry out assessments on a single probabilistic scale of IS operation quality under consideration and its constituent elements, represented as «black boxes».*

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

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.
2. Kostogryzov A. I., Petuhov A. V., Shherbina A. M. Osnovy ocenki, obespechenija i povyshenija kachestva vyhodnoj informacii v ASU organizacionnogo tipa. M.: Izd. «Vooruzhenie. Politika. Konversija», 1994. 278 s.
3. Kostogryzov A. I., Lipaev V. V. Sertifikacija kachestva funkcionirovanija avtomatizirovannyh informacionnyh sistem. – M. Izd. «Vooruzhenie, politika, konversija», 1996. 278 s.
4. Kostogryzov A. I., Nistratov G. A. Standartizacija, matematicheskoe modelirovanie, racional'noe upravlenie i sertifikacija v oblasti sistemnoj i programmnoj inzhenerii. – M. Izd. «Vooruzhenie, politika, konversija», 2004, 2-e izd. 2005. 395 s.
5. Kostogryzov A. I., Stepanov P. V. Innovacionnoe upravlenie kachestvom i riskami v zhiznennom cikle sistem – M.: Izd. «Vooruzhenie, politika, konversija», 2008. – 404 s.
6. A. Kostogryzov, A. Nistratov, G. Nistratov SOME APPLICABLE METHODS TO ANALYZE AND OPTIMIZE SYSTEM PROCESSES IN QUALITY MANAGEMENT («Nekotorye prikladnye metody dlja analiza i optimizacii sistemnyh processov v upravlenii kachestvom») // InTech,

6 Andrey I. Kostogryzov, Dr.Sc., Professor, Chief Researcher, Federal Research Center «Informatics and Control» of the Russian Academy of Sciences. Moscow, Russia. E-mail: Akostogr@gmail.com
7 Andrey A. Nistratov, Ph.D., Senior researcher, Federal Research Center «Informatics and Control» of the Russian Academy of Sciences. Moscow, Russia. E-mail: Andrey.nistratov@gmail.com
8 Pavel E. Golosov, Ph.D., Director of the Institute of Social Sciences of the Russian Academy of National Economy and Public Administration, Moscow, Russia. E-mail: pgolosov@gmail.com

2012, ISBN979-953-307-778-8, 2012, pp. 127–196. http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
7. Abrosimov N. V., Aleshin A. V., Mahutov N. A. i dr. /Pod red. Mahutova N. A./ Bezopasnost' Rossii. Pravovye, social'no-jekonomicheskie i nauchno-tehnicheskie aspekty. Nauchnye osnovy tehnogennoj bezopasnosti. M.: MGOF «Znanie», 2015, 936 s.
8. Abrosimov N. V., Mahutov N. A. i dr. / Pod red. Mahutova N. A./ Bezopasnost' Rossii. Pravovye, social'no-jekonomicheskie i nauchno-tehnicheskie aspekty. Tehnogennaja, tehnologicheskaja i tehnosfernaja bezopasnost'. M.: MGOF «Znanie», 2018, 1016 s.
9. Probabilistic modeling in system engineering (Verojatnostnoe modelirovanie v sistemnoj inzhenerii). InTechOpen, Edited by A. Kostogryzov, 2018, 279 p. URL: http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering
10. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems (Verojatnostnye metody dlja kognitivnogo reshenija nekotoryh zadach v sistemah iskusstvennogo intellekta). Probability, combinatorics and control./ IntechOpen, 2020, pp. 3-34. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
11. Nistratov A. A. Analiticheskoe prognozirovanie integral'nogo riska narushenija priemlemogo vypolnenija sovokupnosti standartnyh processov v zhiznennom cikle sistem vysokoj dostupnosti. Chast' 1. Matematicheskie modeli i metody // Sistemy vysokoj dostupnosti. 2021. T. 17 № 3, s. 16–31, Chast' 2. Programmno-tehnologicheskie reshenija. Primery primenenija // Sistemy vysokoj dostupnosti. 2022. T. 18 № 2, s. 42–57
12. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Verojatnostnoe uprezhdajushhee modelirovanie dlja ocenok riskov v slozhnyh sistemah). 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. Hinchin A. Ja. Raboty po matematicheskoj teorii massovogo obsluzhivanija. – M.: izd-vo Fiz. mat. lit., 1963.
14. Grigolionis V. O shodimosti summ stupenchatyh processov k puassonovskomu // Teorija verojatnosti i ee primenenija. T. 8, 1963, № 2.
15. Gnedenko B. V., Kovalenko I. N. Vvedenie v teoriju massovogo obsluzhivanija. M.: Nauka. 1987.
16. Matveev V. F., Ushakov V. G. Sistemy massovogo obsluzhivanija. M.: MGU, 1984.
17. Kostogryzov A. I., Nazarov L. V. Paketnaja obrabotka trebovanij v sisteme s otnositel'nym prioritetom // Izv. AN SSSR ser. Tehnicheskaja kibernetika. 1981, №3, S.183–187.
18. Balyberdin V. A. Metody analiza mul'tiprogrammnyh sistem. – M. Radio i svjaz', 1982. – 152 s.
19. Balyberdin V. A. Ocenka i optimizacija harakteristik sistem obrabotki dannyh. – M.: Radio i svjaz', 1987. 176 s.
20. Kostogryzov A. I., Matveev V. F. Analiz primenenija kombinirovannoj discipliny obsluzhivanija v sistemah real'nogo vremeni // Izv. AN SSSR ser. Tehnicheskaja kibernetika. 1986, № 6, S.79–84.
21. Kostogryzov A. I. Paketnaja obrabotka zajavok v rezhime ravnomernogo razdelenija processora s preryvaniem // Izv. AN SSSR ser. Tehnicheskaja kibernetika. 1987, № 4, S.88–93.
22. Kostogryzov A. I. Klass prioritetnyh disciplin s kombinirovaniem principov obsluzhivanija v porjadke prioriteta i paketnoj obrabotki zajavok. Analiz ih svojstv i vozmozhnostej primenenija v ASU// Analiz stohasticheskih sistem metodami issledovanija operacij i teorii nadezhnosti. K.: In-t kibernetiki im. V.M.Glushkova AN USSR, 1987. S. 52–55
23. Bezkorovajnyj M.M., Kostogryzov A.I., L'vov V.M. Instrumental'no-modelirujushhij kompleks dlja ocenki kachestva funkcionirovanija informacionnyh sistem KOK. M.: Izd. «Vooruzhenie. Politika. Konversija», 2002. 304 s.
24. Kostogryzov A., Atakishchev O., Nistratov A., Nistratov G., Klimov S., Grigoriev L. The method of rational dispatching a sequence of heterogeneous repair works // Energetica. 2017. Vol.63, No 4, P. 154–162
25. 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.
26. 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.
27. Golosov P. E., Ronzhin A. F. Approaches to execution of sets of tasks with random processing time in coherent computational systems / Proceedings of the International Conference on Modern stochasticity: theory and applications. Kyiv. 10–14.09.2012. S. 33
28. Lyu, Siwei & Farid, Hany. (2005). How Realistic is Photorealistic?. Signal Processing, IEEE Transactions on. 53. 845–850. 10.1109/TSP.2004.839896.
29. Rahmouni, Nicolas & Nozick, Vincent & Yamagishi, Junichi & Echizen, I.. (2017). Distinguishing computer graphics from natural images using convolution neural networks. 1–6. 10.1109/WIFS.2017.8267647.
30. 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.