# Методология оценки надежности иерархических информационных систем

Г. П. Акимова[1], А. В. Соловьев[2]

Статья содержит описание разработанной методики оценки надежности иерархических информационных систем на примере Государственной автоматизированной системы Российской Федерации «Выборы». В рамках проделанной работы проведена оценка надежности как отдельных элементов системы, так и системы в целом с указанием степени влияния элементов на общую надежность системы. В статье излагается аналитический подход к оценке надежностных показателей (коэффициента готовности, вероятности безотказной работы за время выполнения основной задачи, коэффициента оперативной готовности). Применяемый подход основан на независимом учете потока отказов (сбоев) за счет различных факторов (технических, программных средств, ошибок оператора), воздействующих на программно-технические средства.

## Обозначения и сокращения

КСА — комплекс средств автоматизации
ПО — программное обеспечение
ПТС — программно-техническое средство
СПО — специальное программное обеспечение
ОПО — общее программное обеспечение
ЗИП — запасные части, инструменты, принадлежности и материалы
ТО — техническое обеспечение
АРМ — автоматизированное рабочее место
ПТК — программно-технический комплекс
РУК — региональный узел коммутации
ТУК — территориальный узел коммутации

[1] 117312, Москва, просп. 60-летия Октября, д. 9, ИСА РАН, galina@cs.isa.ru.
[2] 117312, Москва, просп. 60-летия Октября, д. 9, ИСА РАН, alexsol@cs.isa.ru.

# 1. Основные определения и выбранные показатели надежности

Для больших информационных иерархических территориально-распределенных систем понятие надежности работы системы является одним их определяющих. Это особенно важно, поскольку такие системы нуждаются не только в сопровождении, но и в непосредственном участии человека в технологическом процессе.

Все расчеты производились применительно к государственной автоматизированной системе (ГАС) «Выборы» (далее Система), повлекшее за собой введение некоторых допущений и ограничений, что, впрочем, не умаляет значения работы как таковой.

Определим надежность как свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих ее способность выполнять основное назначение [8] при воздействии неисправностей (отказов и сбоев) технических средств, ошибок в программах и данных, ошибок персонала и пользователей в заданных режимах и условиях эксплуатации при известных характеристиках системы технического обслуживания и ремонта [9].

Надежность системы, как комплексное свойство, включает в себя следующие свойства: безотказность, ремонтопригодность, сохраняемость и долговечность.

Остановимся на оценке двух свойств надежности: безотказность (свойство системы непрерывно сохранять работоспособное состояние в течение некоторого времени) и ремонтопригодность (приспособленность системы к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта).

Введем ряд определений, характеризующих надежность работы автоматизированной распределенной информационной системы в целом.

**Вероятность безотказной работы $P(t)$** — вероятность того, что система будет работоспособна в течение заданного времени работы при заданных условиях эксплуатации. Вероятность безотказной работы — это характеристика безотказности системы. Данный показатель будем применять для оценки безотказности системы во время проведения избирательных кампаний как отрезка времени, когда она используется по своему основному назначению.

**Коэффициент готовности $K_г$** — вероятность того, что система окажется в работоспособном состоянии в произвольный момент времени. Это комплексная характеристика безотказности и ремонтопригодности системы, которая характеризуется показателями ремонтопригодности: $T_о$ — среднее время наработки на отказ и $T_в$ — среднее время восстановления после отказа. Поскольку времени на ремонт отказавших элементов систе-

мы во время проведения избирательных кампаний нет, то этот показатель оценивает вероятность работоспособности Системы в произвольный момент времени, не ограниченный только временем проведения выборов.

**Коэффициент оперативной готовности $K_{о.г.}(t)$** — вероятность того, что система окажется работоспособной в произвольный момент времени, и, начиная с этого момента, будет работоспособной еще в течении заданного времени. $K_{о.г.}(t) = K_г\, P(t)$. Это также комплексная характеристика безотказности и ремонтопригодности системы. В нашем случае $K_{о.г.}(t)$ характеризует вероятность выполнения Системой своей основной задачи во время подведения итогов голосования по избирательным кампаниям с учетом того, что Система будет в работоспособном состоянии в момент начала подведения итогов выборов.

Положим минимальное значение норматива времени, при котором выполняется требование к вероятности своевременной обработки результатов работы системы, равным $t = 69$ часам для расчетов вероятности безотказной работы системы и ее отдельных элементов.

Математический аппарат методики разработан для оценки надежности на основе статистических данных о ремонте программно-технических средств, отказах оборудования каналом связи, сбоях программного обеспечения.

Выбранные модели расчетов надежности дают устойчиво заниженные (пессимистические) оценки надежности.

## 1.1. Понятие отказов и сбоев в ГАС «Выборы»

Определим понятие отказа для системы в целом и для каждого элемента схемы надежности (см. рис. 1).

Поскольку мы рассматриваем сложную территориально-распределенную многофункциональную систему, то у нее кроме состояний «Полная работоспособность» и «Полный отказ» существует множество промежуточных состояний с различными уровнями работоспособности и соответствующими им уровнями эффективности функционирования.

Под состоянием «Полная работоспособность» понимается такое состояние, при котором работоспособны все составные части и компоненты системы.

«Полным отказом» называется состояние, в котором использование системы по назначению становится невозможным или нецелесообразным из-за неисправностей ПТС, линий связи, влияния человеческого фактора. В этом случае восстановление работоспособности может произойти только после выполнения специальных ремонтно-восстановительных работ.

Для системы в целом можно выделить следующие элементы надежности (назовем их элементами надежности верхнего уровня): КСА верхнего

уровня, каналы связи средний — нижний уровень, КСА среднего уровня, каналы связи нижний уровень — средний уровень, КСА нижнего уровня.

На рис. 1 представлена схема надежности системы в целом. Номера на этой схеме служат для определения количества различных КСА и количества каналов связи.

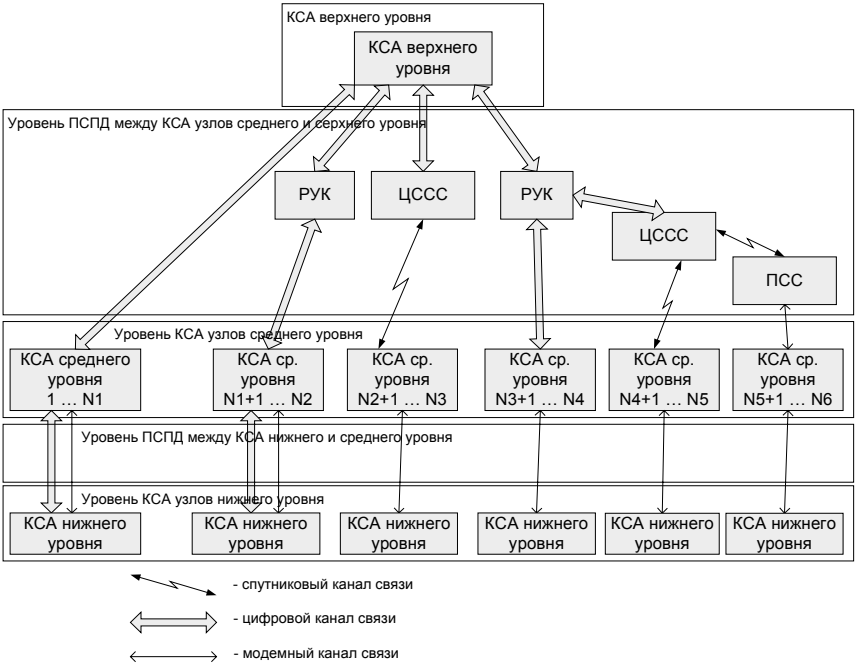


**Рис. 1.** Структурная схема надежности территориально-распределенной иерархической системы

Таким образом, схема надежности системы можно представить в виде графа, в котором узлами являются КСА, а дугами графа — каналы связи. Причем этот граф, не содержащий в себе замкнутых циклов, — не что иное как дерево (или иерархия) с корнем в вершине КСА верхнего уровня (для схемы надежности принимаем допущение, что узлы графа одного уровня между собой не соединены, т. е. горизонтальные связи отсутствуют. Любым подграфом основного графа будет также дерево (например, с корнем в одной вершине КСА среднего уровня). Подобное деление общей схемы на подграфы позволяет оценить вероятность безотказной работы системы в усеченной схеме надежности, например, в нашем случае, когда

выборы проводятся в одном отдельном регионе страны или муниципальном образовании.

Элементы надежности верхнего уровня внутри себя также делятся на отдельные элементы. Подробное деление каждого элемента верхнего уровня на элементы надежности и перечень возможных отказов, приводящих к отказу элемента верхнего уровня, описаны в соответствующих разделах.

Отказы и сбои элементов надежности можно определить в целом следующим образом.

Признаком нарушения функционирования элемента надежности является прекращение решения задачи пользователя или появление не устраняемой (без вмешательства человека) ошибки в результатах ее решения.

Разделение потока неисправностей на отказы и сбои производится в соответствии со следующими определениями.

Отказом элемента надежности называется событие, состоящее в устойчивом нарушении процесса решения задачи пользователя или из-за отказа какого-либо ПТС, входящего в конфигурацию элемента и не имеющего резерва, или из-за отказа резервированной группы ПТС, или из-за возникновения ошибки, обусловленной конструктивной недоработкой, обесценивающей результат решения задачи пользователя и не устраняемой пользователем с помощью оперативных средств и процедур восстановления работоспособности, указанных в эксплуатационной документации.

Под конструктивной недоработкой понимается не выявленная в процессе отладки и испытаний ошибка, возникшая при конструировании и/или изготовлении составных частей элемента, которая может содержаться в технических средствах, программах, данных, процедурах или эксплуатационной документации.

Сбоем называется событие, состоящее в неустойчивом нарушении процесса решения задачи пользователя или из-за сбоя какого-либо ПТС, входящего в конфигурацию элемента, или из-за отказа ПТС, имеющего резерв, или из-за ошибки оператора (пользователя), или из-за ситуационной ошибки, обусловленной конструктивной недоработкой в ПТС.

При восстановлении функционирования после сбоя допускается не более чем троекратная попытка возобновления решения задачи пользователя с помощью перезапуска вычислительного процесса. В противном случае фиксируется отказ.

При оценке надежности КСА принимаются следующие допущения и ограничения:

- нарушения работоспособности из-за неисправностей (отказов и сбоев) ПТС — события взаимно независимые;
- время между возникновением неисправностей — случайная величина, имеющая экспоненциальное распределение вероятностей;

- время восстановления работоспособности ПТС после неисправностей — случайная величина, имеющая произвольное распределение с известным средним значением.

На стадии эксплуатации в процессе сбора статистических данных должны регистрироваться все неисправности (сбои и отказы), не зависимо от причин их вызвавших. Однако, при расчете статистических значений показателей надежности, в соответствии с действующими государственными стандартами, не учитываются:

- зависимые неисправности;
- неисправности, возможность возникновения которых в будущем предотвращена выполненными доработками (что должно быть подтверждено дальнейшими испытаниями);
- неисправности, появление которых вызвано воздействием внешних факторов, не предусмотренных в технических условиях на программно-технические средства;
- неисправности, вызванные нарушением пользователями или персоналом технического обслуживания и ремонта правил и требований, изложенных в эксплуатационной документации;
- неисправности, возникшие во время проведения планового технического обслуживания, и устраненные к моменту использования КСА по назначению.

Кроме того, в данной методике рекомендовано не учитывать отказы, приводящие к ремонту оборудования, но не приводящие к нарушению выполнения основной задачи (отказы устройств указания, клавиатур, мониторов, принтеров).

В приведенных ниже расчетах не учитывались нарушения работоспособности программного и технического обеспечения (не требующие вмешательства разработчиков или сервисных центров в процесс восстановления функционирования) на время меньшее 0,5 часов.

## 1.2. Математическая модель оценки надежности технического обеспечения

Функционирование технического обеспечения КСА и каналов связи может быть определено согласно [13], как циклическая работа по назначению. Тогда, применительно к выбранным нами показателям надежности, основными можно считать следующие.

1. Коэффициент оперативной готовности

$$K_{\text{о.г}} = K_{\text{г}} P(t), \tag{1.1}$$

где $K_г$ — коэффициент готовности, вероятность того, что изделие будет работоспособно в произвольный момент времени;

$P(t)$ — вероятность безотказной работы при наработке $t = 69$ часов.

2. Среднее время восстановления $T_в$ (по всем видам отказов).

Под безотказной работой понимается способность технического (программного) обеспечения выполнять свои функции даже в условиях отказа (полного или с восстановлением) отдельных частей**.**

Коэффициент готовности определяется как:

$$K_г = \frac{T_0}{T_0 + T_в}, \tag{1.2}$$

где $T_0$ — средняя наработка на отказ (по всем видам отказов).

В свою очередь,

$T_о = \sum_{i=1}^{N} t_i / N$,

$T_в = \sum_{i=1}^{N} t_{i\,пр} / N$,

$t_i$ — $i$-й период времени непрерывной работы системы;

$t_{i\,пр}$ — время простоя системы, вызванное $i$-й неисправностью;

$N$ — количество неисправностей.

Для элемента надежности верхнего уровня $K_г$ рассчитывается как произведение входящих в него одиночных и дублированных программно-технических средств (ПТС)

$$K_г = \prod_j K_{г.птс}^{(j)} \prod_j (1 - (1 - K_{г.птс}^{(j)})^n, \tag{1.3}$$

где $n$ — количество дублированных ПТС.

3. Вероятность безотказной работы системы $P(t)$.

Для элемента надежности верхнего уровня $P(t)$ рассчитывается как произведение входящих в него одиночных и дублированных ПТС

$$P(t) = \prod_j P(t)_{птс}^{(j)} \prod_j (1 - (1 - P(t)_{птс}^{(j)})^n, \tag{1.4}$$

$$P_{птс}^{(j)}(t) = e^{-\lambda_j t}, \tag{1.5}$$

где $P_{птс}^{(j)}(t)$ — вероятность безотказной работы одиночного неремонтируемого ПТС (считаем, что на поведение ремонтных работ во время про-

ведения выборов времени нет, поэтому используются только ЗИП и дублированные ПТС),

$\lambda = 1/T_o$ — интенсивность потока отказов для одного ПТС.

## 1.3. Математическая модель оценки надежности программного обеспечения

Оценка надежности ПО отличается от оценки надежности ТО в первую очередь из-за различия характеристик программного и технического обеспечения. ПО не подвержено износу в отличие от ТО, в общем случае надежность программного обеспечения повышается в зависимости от времени. Всякое программное обеспечение содержит ошибки (дефекты), но если они не проявляются, то оно может работать длительное время достаточно устойчиво. Поэтому его надежность включает в себя понятие устойчивости (программа устойчива к любым внешним воздействиям пользователя, т. е. не разрушается), безотказности (ошибки не влияют на правильность функционирования), безошибочности (количество ошибок со временем уменьшается), безошибочность входных данных (даже безошибочная программа может дать неверный результат при ошибочном наборе входных данных).

Грамотно отлаживаемое программное обеспечение постепенно входит в период стабильности, т. к. интенсивность ошибок в нем должна уменьшаться. Характер зависимости количества дефектов от внесенных изменений должен быть «пилообразный», с общим стремлением графика к нулю.

Характеристики программного обеспечения с точки зрения надежности:

- оно не подвержено износу;
- если обнаруженные в процессе отладки ошибки устраняются, а интенсивность внесения новых ошибок ниже интенсивности устраненных ошибок, то интенсивность отказов ПО уменьшается;
- надежность программ зависит от надежности используемой входной информации, т. к. от значений входного набора данных зависит траектория исполнения программы, если при этом информационное обеспечение само содержит дефекты, то программа выработает неправильный результат, даже при отсутствии программных ошибок;
- если при возникновении ошибок дефекты программного обеспечения не диагностировать и не устранять — ошибки будут носить систематический характер;
- надежность программного обеспечения зависит от области применения; при расширении области применения (функционала системы) показатели надежности могут существенно измениться, но изменение функционала — сравнительно редкая доработка программного обеспечения, и не в каждом пакете обновлений меняется функционал, сле-

довательно, пакет обновлений можно рассматривать, в основном, как исправление известных ошибок.

Все коэффициенты готовности ($K_г$) и вероятности безотказной работы ($P(t)$) в формулах, приведенных ниже для конкретной подсистемы или оборудования, для которого не имеется статистических данных, можно принять равными 1 так, чтобы выполнение расчетов можно было провести без их учета.

С точки зрения оценки надежности программного обеспечения для систем рассматриваемого класса разработана модель (далее Модель) оценки надежности, основанная на моделях Джелинского—Моранды и Шика—Волвертона [1], которая, согласно исследованиям [2], наиболее близко подходит для оценки надежности крупномасштабных программных разработок с продолжительным периодом отладки. Данная Модель учитывает тот факт, что в процессе работы с программой постоянно исправляются ошибки и вносятся новые. Кроме того, она позволяет дать оценку числа оставшихся в программе дефектов. Это важно особенно для систем, которые, практически постоянно, находятся в состоянии отладки. В пользу этого свидетельствует тот факт, что пакеты обновлений математического обеспечения могут поступать 1 раз в 2–3 недели.

Модель основана на допущении, что интенсивность обнаружения ошибок пропорциональна числу ошибок, остающихся по истечении $i - 1$ интервала времени, суммарному времени, уже затраченному на отладку к началу текущего интервала, средней длительности поиска ошибки в текущем $i$-м интервале времени отладки $t_i$ и позволяет оценить вероятность безотказной работы системы и коэффициент готовности. Нужно отметить, что разработанная Модель дает заниженные (пессимистические) оценки надежности.

Вероятность безотказной работы определяется как:

$$P(t) = \exp(-(K_{JM}(E_0 - M))\, t/2), \qquad (1.6)$$

где

$K_{JM}$ — коэффициент пропорциональности;

$E_0$ — количество ошибок в начале отладки;

$M$ — полное количество временных интервалов, на каждом из которых обнаружена хотя бы одна ошибка. В нашем случае оно равно количеству обнаруженных ошибок, т. к. принимается допущение, что на каждом временном интервала произошла одна ошибка.

Средняя наработка между обнаруженными ошибками:

$$T = \sqrt{\left(\pi / \left(2\left(K_{JM}\left(E_0 - M\right)\right)\right)\right)}.$$

Для оценки параметров модели $K_{JM}$ и $E_0$ необходимо решить систему уравнений (решается итерационно, затем округляется $E_0'$ и получается $E_0$):

$$\begin{cases} K_{JM} = M / \left( \left( \sum_{i=1}^{M} (t_i) \right) \left( E'_0 + 1 - \left( \sum_{i=1}^{M} (i \cdot t_i) / \sum_{i=1}^{M} (t_i) \right) \right) \right), \\ E'_0 = M / \left( \sum_{i=1}^{M} \left( 1 / \left( E'_0 - i + 1 \right) \right) \right) + \sum_{i=1}^{M} (i \cdot t_i) / \sum_{i=1}^{M} t_i - 1. \end{cases}$$

Коэффициент готовности определяется как

$$K_{\text{г по}} = T_{\text{о по}} / (T_{\text{о по}} + T_{\text{в по}}),$$

где

$T_{\text{о по}}$ — среднее время наработки на отказ ПО,
$T_{\text{в по}}$ — среднее время восстановления ПО после отказа,
$K_{\text{г по}}$ — коэффициент готовности ПО (оценивается по подсистемам);

$$T_{\text{о по}} = \sum_{i=1}^{M} (t_i) / M, \qquad T_{\text{в по}} = \sum_{i=1}^{M} \left( t_{\text{i пр}} \right) / M,$$

$t_i$ — $i$-й период времени непрерывной работы ПО;
$t_{i\,\text{пр}}$ — время простоя системы, вызванное $i$-й ошибкой.

Оценка остаточного количества ошибок ПО:

$$E_{\text{ост}} = E_0 - M.$$

## 2. Схема надежности ПТС

Для каждого элемента надежности верхнего уровня, определенного в п. 1.1, составим свою схему надежности. Сначала определим порядок расчетов элементов надежности для КСА всех уровней.

На каждом уровне расчета надежности под элементом надежности будем понимать: техническое обеспечение, отдельные подсистемы ОПО и СПО для расчета надежности внутри АРМ, АРМ целиком для расчета надежности внутри КСА, КСА соответствующего уровня для расчета надежности системы в целом.

### 2.1. Схема надежности ПТС КСА нижнего уровня

Для ПТС КСА нижнего уровня приведем схему расчета надежности, подробно выделив схему расчета для программного и технического обеспечения, с разбивкой (по возможности) по подсистемам.

Введем ряд допущений. Пусть имеется 2737 КСА нижнего уровня, состоящий из практически одинаковых АРМ1 и АРМ2 (сервер БД и АРМ пользователя одновременно), оснащенных ПО. Элементами надежности схемы будем считать отдельные подсистемы ОПО и СПО, проявление отказов для которых может быть однозначно установлено. Вводить более мелкое деление на элементы представляется не целесообразным, т. к. может внести путаницу при определении задачи, в процессе решения которой наступил отказ (или сбой). АРМ1 и АРМ2 практически дублируют друг друга.

Для примера предположим, что не все узлы нижнего уровня однородны, и на 153 из 2737 КСА нижнего уровня дополнительно стоят одинаковые АРМ пользователей АРМ3, АРМ4 (9 из 153 узлов), АРМ5 (2 из 9 узлов).

Надежность АРМ1 можно выразить формулой:

$$K_{\text{г АРМ1}} = K_{\text{г опо}} K_{\text{г поиб}} K_{\text{г спо}} K_{\text{г то}}, \qquad (2.1)$$

где

$K_{\text{г опо}}$ — коэффициент готовности ОПО АРМ1,

$K_{\text{г поиб}}$ — коэффициент готовности системы безопасности АРМ1,

$K_{\text{г спо}}$ — коэффициент готовности СПО АРМ1,

$K_{\text{г то}}$ — коэффициент готовности ТО АРМ1.

Если допустить, что АРМ2 все-таки полностью дублирует АРМ1, и решение задачи пользователя в случае отказа АРМ1 можно возобновить на АРМ2, то получим, что общая надежность ПО нижнего уровня выражается формулой (она справедлива по крайней мере для 2584 КСА нижнего уровня):

$$K_{\text{г н.у.}} = K_{\text{г ск}} (1 - (1 - K_{\text{г АРМ1}})^2), \qquad (2.2)$$

где $K_{\text{г ск}}$ — коэффициент готовности сетевого коммутатора.

Учтем влияние на надежность ПО нижнего уровня дополнительно установленных АРМ3, АРМ4, АРМ5. С точки зрения решаемой задачи АРМ3 не является дублирующим звеном для АРМ1 и АРМ2, но, в то же время, выход из строя АРМ3 скажется на скоростных характеристиках ввода исходных данных, а, следовательно, косвенно все же снизит надежность.

Надежность АРМ3 можно оценить формулой:

$$K_{\text{г АРМ3}} = K_{\text{г опо}} K_{\text{г поиб}} K_{\text{г то}},$$

где $K_{\text{г то}}$ — коэффициент готовности технического обеспечения АРМ3.

Для общего случая надежность группы одинаковых и взаимозаменяемых АРМ3–АРМ5 оценивается по формуле:

$$K_{\text{г АРМ3-5}} = 1 - (1 - K_{\text{г АРМ3}})^n,$$

где $n = [1, 3]$.

Если предположить, что работа во время избирательной кампании равномерно распределена по всем АРМ КСА нижнего уровня, и выход из строя одного из них снижает скорость работы на определенный процент, что является критичным для выполнения поставленной задачи, то влияние АРМ3–АРМ5 на общую надежность программного обеспечения нижнего уровня можно выразить следующим образом:

$$K_{\text{г н.у.}} = K_{\text{г ск}} ((1 - (1 - K_{\text{г АРМ1}})^2) (1 - (1 - K_{\text{г АРМ3}})^n)), \qquad (2.3)$$

где $n = 1$ для 144 узлов $n = 2$ для 7 узлов, $n = 3$ для 2 узлов.

Определим отказы одного КСА нижнего уровня, работающего в режиме проведения выборов. Отказом для этого уровня можно считать отказ (устойчиво проявляемую неисправность) группы резервируемых ПТС АРМ1 и АРМ2, на которых находится БД или отказ сетевого коммутатора. В свою очередь отказ АРМ1 (АРМ2) — это отказ ТО компьютера одного АРМ, или отказ ОПО АРМ, или отказ СПО АРМ, или отказ подсистемы безопасности одного АРМ. Дополнительно для крупных узлов нижнего уровня с дополнительно установленными АРМ3, АРМ4, АРМ5 отказ этой группы резервируемых АРМ будут означать, что требование своевременности решения основной задачи системой не будет выполнено (в нашем случае это своевременность ввода протоколов участковых избирательных комиссий с результатами голосования, а, следовательно, и их отправки на следующий уровень иерархии системы). Отказом, также, можно считать отключение электропитания во время работы системы.

Теперь оценим схему учета общей надежности программного обеспечения КСА нижнего уровня в целом. Будем при этом исходить из предположения, что полный отказ системы в целом наступает с выходом из строя всех КСА нижнего уровня одновременно (такое состояние системы делает невозможным подсчет результатов голосов с помощью Системы). В то же время, выход из строя полностью одного или нескольких КСА нижнего уровня приводит к частичной потере работоспособности, но не к отказу системы в целом. Полное множество КСА нижнего уровня представляет собой непересекающиеся множества ПТС этих КСА.

Поскольку элементы множества КСА нижнего уровня являются практически типовыми (т. е. представляют собой монотонную структуру с точки зрения теории множеств) и не пересекаются между собой, то можно получить итоговую надежность, как сумму функций надежности $F(A_i, K_{\text{г}i})$, где $A_i$ — весовой коэффициент $i$-го элемента на множестве всех элементов нижнего уровня, $K_{\text{г}i}$ — коэффициент готовности (надежность) $i$-го элемента. Тогда итоговая надежность выражается формулой $K_{\text{г н.у.}} = \sum_{i=1}^{N} F\left(A_i, K_{ri}\right)$, где $N$ — количество элементов нижнего уровня.

С точки зрения Системы в целом, выход из строя КСА, обслуживающего большое количество избирателей, более критичен, чем выход из строя КСА, обслуживающего меньшее количество избирателей. Поэтому в общей схеме надежности добавим весовой коэффициент ($A_i$), учитывающий (примерно) количество избирателей, обслуживаемых данным элементом нижнего уровня.

С учетом введенной неоднородности узлов (в нашем случае в зависимости от количества избирателей), итоговая формула запишется как:

$$K_{\text{г н.у.}} = \sum_{i=1}^{M} F\left(A_i, K_{ri}\right),$$

где $M$ — количество множеств одинаковых узлов КСА.

Для Системы в целом получим, согласно формулам (2.1) и (2.2):

$$\begin{aligned} K_{\text{г н.у.}} = {} & (A_1 K_{\text{г кс}} (1 - (1 - K_{\text{г АРМ1}})^2)) + \quad (A_2 K_{\text{г кс}} (1 - (1 - K_{\text{г АРМ1}})^2)) + \\ & + (A_3 K_{\text{г кс}} ((1 - (1 - K_{\text{г АРМ1}})^2) K_{\text{г АРМ3}}) + \\ & + (A_4 K_{\text{г кс}} ((1 - (1 - K_{\text{г АРМ1}})^2) (1 - (1 - K_{\text{г АРМ3}})^2)) + \\ & + (A_5 K_{\text{г кс}} ((1 - (1 - K_{\text{г АРМ1}})^2) (1 - (1 - K_{\text{г АРМ3}})^3)). \end{aligned} \qquad (2.4)$$

Должно строго выполняться условие $A_5 + A_4 + A_3 + A_2 + A_1 = 1$.

Вычисленные значения весовых коэффициентов:

$$A_5 = 0{,}005, \quad A_4 = 0{,}013, \quad A_3 = 0{,}16, \quad A_2 = 0{,}22, \quad A_1 = 0{,}602.$$

Для расчета влияния одного конкретного КСА на общую надежность всей Системы устанавливается весовой коэффициент, равный проценту обслуживаемых им избирателей. Это необходимо для оценки степени влияния отказа отдельного КСА нижнего уровня на общую надежность Системы в целом.

Аналогично коэффициенту готовности рассчитывается и вероятность безотказной работы $P(t)$ путем произведения показателей $P(t)$ соответствующих элементов схемы надежности (аналогично формуле (2.4)).

Отказ всей системы, с точки зрения возможности проведения подсчета голосов с её использованием, наступит после выхода из строя ВСЕХ КСА нижнего уровня системы. Выход из строя одного КСА будет считаться частичным отказом (или отказом одного КСА), но не отказом всей системы.

## 2.2. Схема надежности ПТС КСА среднего уровня

Для ПТС КСА среднего уровня приведем схему расчета надежности, подробно выделив схему расчета для программного обеспечения, с разбивкой по подсистемам.

Согласно рис. 1 в системе имеется 89 КСА среднего уровня. Считаем, что схема всех КСА типовая и состоит из АРМ сервера, АРМ1 СПО и четырех АРМ2–10 для ввода данных, которые при необходимости дублируют друг друга. Тогда схему надежности можно представить следующими формулами:

$K_{\text{г АРМ2-10}} = 1 - (1 - K_{\text{г АРМ2}})^4$ , надежность одного узла:

$$K_{\text{г ср.у. } i} = K_{\text{г сервер}}\, K_{\text{г АРМ1}}\, K_{\text{г АРМ2-10}}\, K_{\text{г ск}}{}^2, \qquad (2.5)$$

где $K_{\text{г ск}}$ — коэффициент готовности сетевых коммутаторов (соединены последовательно).

Определим отказы одного КСА, работающего в режиме проведения выборов. Отказом в таком случае можно считать отказ сервера, или АРМ1, или резервируемой группы АРМ2–АРМ10, или одного из двух сетевых коммутаторов. В свою очередь, отказ сервера — это отказ ТО компьютера сервера, или отказ ОПО сервера, или отказ СПО сервера, или отказ системы безопасности сервера. Аналогично для АРМ1–АРМ10 отказом каждого из этой группы АРМ считаем отказ ТО (компьютеры), или отказ ОПО, или отказ системы безопасности для случая, когда СПО находится на сервере. Отказом можно также считать отключение электропитания.

Теперь приведем интегральную оценку надежности множества элементов среднего уровня, руководствуясь соображениями, изложенными для интегральной оценки надежности множества элементов нижнего уровня (см. п. 2.1).

Поскольку элементы множества являются практически типовыми (т. е. представляют собой монотонную структуру с точки зрения теории множеств) и не пересекаются между собой, то можно получить итоговую надежность как сумму функций надежности $F(B_i, K_{\text{г}i})$, где $B_i$ — весовой коэффициент $i$-го элемента на множестве всех элементов среднего уровня, $K_{\text{г}i}$ — коэффициент готовности (надежность) $i$-го элемента. Тогда итоговая надежность всего множества выражается формулой:

$$K_{\text{г ср.у.}} = \sum_{i=1}^{N} F\left(B_i, K_{ri}\right),$$

где $N$ — количество узлов среднего уровня.

Бесспорно, что полным отказом системы, является выход из строя всех 89 элементов среднего уровня. Выход из строя одного элемента не является, в общем случае, отказом всей системы в целом

Поскольку считаем, что все элементы имеют одинаковое техническое и программное оснащение, то степень влияния одного отдельно взятого элемента на общую надежность Системы определяется количеством избирателей, обслуживаемых данным элементом среднего уровня. Степень

влияния $i$-го элемента на общую надежность системы в целом можно выразить весовым коэффициентом:

$$B_i = \text{Изб}_i / \sum_{i=1}^{89} \text{Изб}_i,$$

где $\text{Изб}_i$ — количество избирателей в $i$-м субъекте РФ.

При этом должно строго выполняться условие $\sum_{i=1}^{89} B_i = 1$.

Тогда общую надежность всего множества можно выразить формулой:

$$K_{\text{г ср.у.}} = \sum_{i=1}^{89} \left( B_i, K_{\text{г ср.у.}i} \right). \qquad (2.6)$$

Аналогично коэффициенту готовности рассчитывается и вероятность безотказной работы $P(t)$ путем произведения показателей $P(t)$ соответствующих элементов схемы надежности.

### 2.3. Схема надежности ПТС КСА верхнего уровня

Работоспособность КСА верхнего уровня является важнейшим, с точки зрения надежности, звеном общей схемы надежности системы в целом, т. к. отказ приводит к отказу всей системы в целом, а, следовательно, к надежности должны предъявляться наиболее высокие требования.

Общая схема надежности КСА верхнего уровня представлена ниже:

$$K_{\text{г в.у.}} = K_{\text{г сегм. пспд}} K_{\text{г сегм. крипто}} K_{\text{г ЭП}} K_{\text{г сегм. серверов}} \times \\ \times K_{\text{г сои}} K_{\text{г сегм. админ.}} K_{\text{г сегм. польз.}} \qquad (2.7)$$

Определим отказ для верхнего уровня во время работы системы как отказ сегмента каналов связи, или отказ сегмента криптозащиты, или отказ сегмента электронной почты (если он присутствует в системе), или отказ сегмента серверов, или отказ системы представления информации (если таковая присутствует в системе), или отказ сегментов администраторов и пользователей.

## 3. Схема надежности каналов связи

Для учета надежности территориально-распределенной информационной системы, невозможно не учитывать надежность каналов связи и относящегося к ним оборудования и ПО подсистемы ПСПД. При этом необходимо учесть, что отказы всех каналов связи, связывающих узлы нижнего и

среднего уровня, будут равнозначны выходу из строя всех узлов нижнего уровня, выход из строя каналов связи, соединяющих узлы среднего и верхнего уровня, будет равнозначен выходу из строя всего узла среднего уровня (а значит и всех подчиненных ему узлов нижнего уровня).

Наконец, полным отказом Системы, бесспорно, считается выход из строя всех каналов связи между всеми узлами нижнего уровня и всеми узлами среднего уровня, или выход из строя всех каналов связи между всеми узлами среднего и верхнего уровня.

От работы ПСПД зависит возможность выполнения информационной системой поставленной задачи в указанный временной промежуток.

## 3.1. Схема надежности каналов связи между узлами нижнего и среднего уровней

Своевременное получение достоверных данных из КСА узлов нижнего уровня является той отправной точкой, которая является базовой для всех процедур, производимых в рамках рассматриваемой информационной системы. Безусловно, работу каналов связи можно заменить путем использования человеческого труда — передачу данных производить на дисках, в бумажном виде, каким-либо еще способом. Однако, если говорить об автоматизированной системе, то рассмотреть надежность системы передачи данных на узлы нижнего уровня необходимо. Пусть по своему составу все множество ПСПД узлов нижнего уровня делится на 2 однородных подмножества: с модемной связью и с цифровыми каналами связи.

### 3.1.1. Надежность ПСПД узлов нижнего уровня с модемной связью

Пусть ПСПД, в данном случае, будет содержать резервируемый модем и не резервируемый канал связи до узла среднего уровня. Оценка надежности такой ПСПД проводится следующим образом

$$K_{\text{г пспд н.у. 1}} = K_{\text{г ккс}} \left(1 - (1 - K_{\text{г модем}})^2\right), \qquad (3.1)$$

где

$K_{\text{г ккс}}$ — коэффициент готовности коммутируемого канала связи, причем в канал связи включено так же оборудование промежуточных узлов (точки) связи и физические линии связи (типа точка — точка);

$K_{\text{г модем}}$ — коэффициент готовности модема (резервируемый).

Определим отказ для одного канала модемной связи. Отказом будем считать выход из строя модемного (коммутируемого) канала связи или выход из строя резервируемой группы модемов.

### 3.1.2. Надежность ПСПД узлов нижнего уровня с цифровым каналом связи

Пусть ПСПД содержит маршрутизатор, скоростной модем и цифровой не резервируемый канал связи. В случае отказа оборудования цифрового канала, его функции резервируются коммутируемым каналом связи, включающем не резервируемый модем и не резервируемый канал связи до узла среднего уровня.

Тогда коэффициент готовности для ПСПД с цифровым каналом связи определяется по формуле

$$K_{\text{г пспд н.у. 2}} = 1 - ((1 - (K_{\text{г кс}} K_{\text{г cisco}} K_{\text{г смодем}})) \times \\ \times (1 - (K_{\text{г ккс}} K_{\text{г модем}}))), \quad (3.2)$$

где

$K_{\text{г кс}}$ — коэффициент готовности цифрового канала связи,

$K_{\text{г cisco}}$ — коэффициент готовности маршрутизатора,

$K_{\text{г смодем}}$ — коэффициент готовности скоростного модема,

$K_{\text{г ккс}}$ — коэффициент готовности коммутируемого канала связи,

$K_{\text{г модем}}$ — коэффициент готовности модема.

Определим отказ для одного канала цифровой связи. Отказом будем считать выход из строя резервируемой группы ПТС цифровой связи (отказ цифрового канала связи, или маршрутизатора, или скоростного модема) и группы ПТС резервной аналоговой связи (выход из строя модемного канала связи, или выход из строя модема).

Оценим общую надежность ПСПД между узлами нижнего и среднего уровня. Для этого необходимо ввести весовые коэффициенты, отражающие процентное соотношение (например, процент обслуживаемых избирателей) ПСПД КСА нижнего уровня с цифровыми каналами связи и модемными каналами связи.

Надежность ПСПД КСА нижнего уровня можно выразить следующей формулой:

$$K_{\text{г пспд н.у.}} = C_1 K_{\text{г пспд н.у. 1}} + C_2 K_{\text{г пспд н.у. 2}}, \quad (3.3)$$

где

$C_1$ — процент избирателей, обслуживаемых с помощью модемных каналов связи;

$C_2$ — процент избирателей, обслуживаемых с помощью цифровых каналов связи.

## 3.2. Схема надежности ПСПД каналов связи между узлами среднего и верхнего уровней

Важность надежной работы системы передачи данных на среднем уровне определяется тем, что отказ в ее работе может привести к невы-

полнению основной задачи информационной системы. Пусть, по своему составу все множество ПСПД узлов среднего уровня также делится на два однородных подмножества: ПСПД с системой спутниковой связи и ПСПД с цифровыми каналами связи.

### 3.2.1. Надежность ПСПД узлов среднего уровня с цифровым каналом связи

Пусть большинство ПСПД КСА среднего уровня оборудовано цифровыми высокоскоростными каналами связи.

Схема подсистемы передачи данных включает следующее оборудование. Не резервируемый цифровой канал связи, маршрутизатор для связи с цифровым каналом, дублируемый в случае отказа маршрутизатором коммутируемого канала связи, два коммутатора локальной вычислительной сети, дублирующие друг друга в случае отказа, не дублируемый криптошлюз и не резервируемый сервер электронной почты, резервируемый скоростной модем.

В соответствии со схемой КСА узла среднего уровня, при оценке надежности необходимо учитывать следующие показатели:

$K_{\text{г кс}}$ — коэффициент готовности канала связи;

$K_{\text{г cisco}}$ — коэффициент готовности маршрутизатора (резервируемый);

$K_{\text{г коммутатор лвс}}$ — коэффициент готовности коммутатора локальной вычислительной сети;

$K_{\text{г криптошлюз}}$ — коэффициент готовности криптошлюза;

$K_{\text{г эп}}$ — коэффициент готовности сервера электронной почты,

$K_{\text{г смодем}}$ — коэффициент готовности скоростных модемов.

Тогда коэффициент готовности для общего случая определяется по формуле

$$K_{\text{г пспд ср.у. ц}} = K_{\text{г кс}} \left(1 - (1 - K_{\text{г cisco}})^2\right) \left(1 - (1 - K_{\text{г коммутатор лвс}})^2\right) \times \\ \times K_{\text{г криптошлюз}} K_{\text{г эп}} \left(1 - (1 - K_{\text{г смодем}})^2\right). \qquad (3.4)$$

Определим отказ ПСПД от одного узла среднего уровня до узла верхнего уровня, оборудованного цифровой линией. Отказом будем считать отказ цифрового канала связи, или криптошлюза, или сервера электронной почты, или резервированной группы из 2-х маршрутизаторов, или отказ резервированной группы коммутаторов локальной вычислительной сети, или выход из строя резервированных групп скоростных модемов.

### 3.2.2. Надежность ПСПД узлов среднего уровня со спутниковым каналом связи

При оценке ПСПД, оснащенной системой спутниковой связи, отдельно необходимо рассмотреть ситуацию, когда сама система спутниковой

связи находится в разных помещениях с узлом среднего уровня и имеет физическое соединение с помощью линии связи.

Пусть согласно имеющейся конфигурации КСА узла со спутниковой системой связи при оценке надежности работы подсистемы передачи данных необходимо учитывать следующие показатели:

$K_{\text{г кс}}$ — коэффициент готовности канала связи,

$K_{\text{г cisco}}$ — коэффициент готовности маршрутизатора,

$K_{\text{г коммутатор лвс}}$ — коэффициент готовности коммутатора локальной вычислительной сети,

$K_{\text{г криптошлюз}}$ — коэффициент готовности криптошлюза,

$K_{\text{г эп}}$ — коэффициент готовности сервера электронной почты,

$K_{\text{г cisco тук}}$ — коэффициент готовности маршрутизатора,

$K_{\text{г смодем}}$ — коэффициент готовности модема,

$K_{\text{г ср.у.-псс}}$ — коэффициент готовности физической соединительной линии (между узлом и ПСС),

$K_{\text{г модема сс}}$ — коэффициент готовности модема спутниковой связи (ПСС и ЦССС),

$K_{\text{г псс-цссс}}$ — коэффициент готовности канала связи между ПСС и ЦССС,

$K_{\text{г цссс-тук}}$ — коэффициент готовности физической соединительной линии между ЦССС и ТУК.

Тогда коэффициент готовности для ПСПД со спутниковой связью в общем случае определяется по формуле

$$K_{\text{г пспд ср.у. сс}} = K_{\text{г кс}} \left(1 - (1 - K_{\text{г cisco}})^2\right) \left(1 - (1 - K_{\text{г коммутатор лвс}})^2\right) \times$$
$$\times K_{\text{г криптошлюз}} K_{\text{г эп}} K_{\text{г cisco тук}} \left(1 - (1 - K_{\text{г смодем}})^2\right)^3 \times$$
$$\times K_{\text{г ср.у.-псс}} K_{\text{г модема сс}} K_{\text{г псс-цссс}} K_{\text{г цссс-тук}}. \qquad (3.5)$$

Определим отказ ПСПД одного узла среднего уровня, оборудованного системой спутниковой связи и работающей в режиме проведения выборов. Отказом будем считать отказ каналов связи ЦССС — узел верхнего уровня, узел среднего уровня — ПСС, ПСС — ЦССС, ЦССС — ТУК, ТУК — узел верхнего уровня (см. рис. 1), или криптошлюза, или сервера электронной почты, или резервированной группы из двух маршрутизаторов, или отказ резервированной группы коммутаторов локальной вычислительной сети, или выход из строя резервированных групп скоростных модемов узла среднего уровня, ПСС или ТУК, или маршрутизатора ТУК, или спутниковых модемов узла среднего уровня и ЦССС. Отказом можно считать отключение электропитания на промежуточных передающих узлах коммутации (ТУК, ПСС, ЦССС).

В итоге, можно оценить общую надежность ПСПД между узлами среднего и верхнего уровня. Для этого необходимо ввести весовые коэф-

фициенты, отражающие процентное соотношение (например, количество обслуживаемых избирателей) ПСПД между узлами среднего и верхнего уровней с цифровыми каналами связи и системой спутниковой связи.

Надежность ПСПД можно выразить следующей формулой:

$$K_{\text{г пспд н.у.}} = D_1 K_{\text{г пспд ср.у. ц}} + D_2 K_{\text{г пспд ср.у. сс}}, \quad (3.6)$$

где

$D_1$ — процент избирателей, обслуживаемых с помощью цифровых каналов связи;

$D_2$ — процент избирателей, обслуживаемых с помощью системы спутниковой связи.

## 4. Учет влияния человеческого фактора на надежность Системы

Человек, как звено системы (системный администратор СА, оператор), обладает следующими свойствами: способность к адаптации, способность к утомлению, способность к отдыху, возможность совершения ошибки, способность принимать решения, способность запоминания информации, способность переносить информационную перегрузку [6].

Например, учет такой характеристики, как способность к утомлению осуществляется следующим образом. При работе в благоприятных условиях, средняя выработка в последние часы падает на 6–7 % на каждый час удлинения рабочего дня сверх 6 часов (т. е. за 7-й час производительность составляет 94 %, за 8-й — 88 %, за 9-й — 81 % и т. д.). Большое влияние на утомляемость оказывает эмоциональное возбуждение. Так, работа, выполняемая с интересом, утомляет меньше, чем скучная монотонная работа.

Степень влияния на надежность системы человеческого фактора можно оценить по вероятности проявления ошибок в процессе ручного ввода данных. Ошибка системного администратора всегда связана с неверной интерпретацией поступивших и анализируемых им данных. Считается, что для сложных технических приборов и сложных компьютерных задач вероятность ошибки может достигать 15 %, для простых технических устройств и несложных компьютерных задач вероятность ошибки составляет от 1 % до 5 % [6].

Безошибочность действий системного администратора (оператора) зависит от многих факторов:

- дефицит времени (частота совершения ошибок при обработке информации является логарифмической функцией скорости поступления информации);

- перегрузка информацией (количество ошибок возрастает при перегрузке, в частности, при увеличении числа источников информации);
- степень подготовки (более подготовленные специалисты совершают меньше ошибок);
- психологические особенности человека;
- «сенсорный голод» (увеличение частоты ошибок при длительном выполнении монотонной работы из-за малой нагрузки органов чувств).

Важную роль в уменьшении ошибок играет степень подготовленности оператора. Считается [6], что в процессе обучения частота ошибок имеет тенденцию к уменьшению, причем эту зависимость можно аппроксимировать формулой:

$$q = q_c + (q_0 - q_c)\exp(-n/N),$$

где

$q$ — частота ошибок после обучения;

$q_0$ — начальное значение частоты ошибок (до обучения);

$q_c$ — установившееся стационарное значение частоты ошибок (для обученных СА);

$n$ — накопленная сумма операций ввода, выполненных СА в предыдущих циклах обучения (работы);

$N$ — «постоянная обучения», характеризующая продолжительность обучения СА.

При $n = N$ разность $q_0 - q_c$ уменьшается на 63 %. Считается, что значение $q_c$ достигается через 4–5 $N$ (для нашего случая — это 4–5 тренировок работы с Системой). При этом, если обозначить за $n_1$ — количество вводов информации, при котором выполняется $q = q_c$, то:

$$N = -((\lg e)/(\lg(q_0 - q_c)))\, n_1$$

По экспериментальным данным [7], полученным при отработке операторами зрительных сигналов, вычислены следующие значения перечисленных выше параметров:

$q_0 = 0{,}27$ (новички, не умеющие работать с Системой),

$q_c = 0{,}018$ (СА, прошедшие 4 и более тренировок),

Совсем не обученных с системой операторов нет, поэтому считаем, что процент ошибок $q_0 = 0{,}27$ в нашем случае не достигается.

Тогда коэффициент учета ошибок этапа ручного ввода можно вычислить по формуле:

$$K_{\text{рв}} = 1 - q = \left(\sum_{i=1}^{N_{\text{н.у.}}} (1 - q_i)\right)/N_{\text{н.у.}}, \qquad (4.1)$$

где

$K_{рв}$ — коэффициент учета влияния ошибок этапа ручного ввода (оценивается для каждого ручного процесса отдельно, если процессы последовательные, коэффициенты перемножаются, т. е. $K_{рв} = \Pi_{i=1}^{M} K_{рв\,i}$, где $M$ — количество последовательных процессов ручного ввода),

$N_{н.у.}$ — количество операторов, по которым собрана статистика об ошибках.

Вероятность появления ошибки оператора существенно зависит от скорости поступления информации. Согласно [6], вероятность проявления ошибки в зависимости от скорости поступления информации $V$ (бит/с) можно представить следующей формулой:

$$q_{рв} = 9{,}7\ 10^{-4}\ V^{1{,}77}.$$

Проведем оценочные расчеты для определения вероятности появления ошибки оператора Системы. Допустим, что протокол одной избирательной кампании содержит 20 числовых полей по 4 цифры каждая (каждая цифра — байт информации) и 5 информационных полей по 50 символов каждое (каждый символ — байт). Тогда информационное содержание одного протокола равно 2640 бит. Пусть скорость набивания протокола составляет в среднем 5 минут (300 секунд). Допустим, что половина этого времени уходит на чтение, а половина на ввод данных в Систему. Тогда скорость поступления информации к оператору равна 17,6 бит/с (это высокая нагрузка, нормальная лежит в пределах 8–15 бит/с), $q_{рв} = 0{,}15$ или вероятность безошибочной работы $P_{рв} = 0{,}85$, что соответствует проценту ошибок при работе со сложными техническими устройствами и программами [6]. Примем это значение за нижнюю границу $К_{рв}$. Тогда $К_{рв}$ будет лежать в диапазоне от 0,85 до 0,982.

Если предположить, что 10 % операторов впервые участвуют в выборах, и тем самым они не подготовлены, еще 10 % прошли недостаточную тренировочную подготовку, а остальные 80 % имеют достаточную компьютерную и тренажерную подготовку (участие как минимум в 4–5 выборах или тренировках), то $K_{рв} = 0{,}2 \times 0{,}85 + 0{,}8 \times 0{,}982 = 0{,}9556 \approx 0{,}96$.

Ошибка оператора в общем случае не приводит к отказу на отдельном КСА, она характеризует только увеличение времени ввода в систему на $1/K_{рв}$. Теперь оценим степень влияния ошибок операторов на отказ одного КСА. Такой ошибкой может быть:

- принципиальная невозможность ввода протокола из-за неверно подготовленного описателя протокола;
- накопление такого количества ошибок ввода, исправление которых не позволит выдержать требование своевременности отправки результатов голосования;

- возникновение такого отказа в системе, на который реакция оператора оказалась неверной (неверная или запоздалая диагностика неисправности) и восстановление ТО/ПО превысило отведенный резерв времени на подведение итогов голосования;
- «выход из строя» системного администратора, делающий невозможным выполнение работ по вводу данных;
- нехватка памяти при вводе информации в БД по причине ошибок администрирования или нехватка дискового пространства, что делает невозможным дальнейший ввод информации.

При вводе данных в систему, осуществляются логические проверки на соответствие, вычисляются контрольные соотношения. Поэтому часть ошибок отсекается с помощью проверок, т. е. коэффициент $K_{\text{рв}} \approx 0{,}96$ влияет на увеличение времени ввода из-за повторного выполнения работы [11]. Считаем, что при повторном выполнении работы происходит полная проверка данных неправильно введенного протокола и исправление ошибок. При этом при исправлении ошибок оператор допускает новые, не выявляемые логическими проверками, ошибки с той же вероятностью 0,96.

В этих предположениях составим таблицу работы оператора в зависимости от времени.

**Таблица 1**

| | **Время работы (часы работы)** | | | | | |
|---|---|---|---|---|---|---|
| | **1–6** | **7** | **8** | **9** | **10** | **11** |
| Производительность (% от нормы) | 1 | 0,94 | 0,88 | 0,81 | 0,74 | 0,67 |
| Процент ошибок | 0,96 | 0,9 | 0,85 | 0,78 | 0,71 | 0,64 |
| Реальное время ввода с учетом повторных работ (часов) | 6,25 | 1,11 | 1,18 | 1,28 | 1,4 | 1,56 |
| Достоверность результатов ввода (процент ошибок с учетом логических проверок и повторного ввода) | 0,999 | 0,996 | 0,994 | 0,991 | 0,988 | 0,985 |
| Верхняя граница достоверности | 0,9995 | 0,998 | 0,997 | 0,995 | 0,993 | 0,991 |
| Нижняя граница достоверности | 0,997 | 0,993 | 0,991 | 0,987 | 0,983 | 0,979 |

Средняя «достоверность» информации при вводе данных итоговых протоколов получается равной 0,995 (или количество недостоверной информации по предварительной оценке составляет не более 0,5 % от обще-

го количества введенной в БД Системы информации, или $r = 5$ ошибок на $n = 1\ 000$ вводов данных).

$$0{,}985 <= K_{\text{рв}} <= 0{,}999.$$

Если ввести доверительный интервал с квантилями уровня 90 % распределения Фишера [14] (квантили уровня 90–95 % выбираются для случая, когда возникают сомнения в выполнении гипотезы, принятой для оценки уровня достоверности), получим верхнюю и нижнюю оценки средней достоверности введенной информации по формулам (для $K_{\text{рв}} = 0{,}995$)

$$K_{\text{рв}}\hat{} = 1 - 1/(1 + (n - r + 1)\,(z(0.9,\, 2r + 2,\, 2r)/r)) = 0{,}998,$$
$$K_{\text{рв}}\tilde{} = 1 - 1/(1 + (n - r)/(z(0.9,\, 2r,\, 2r)\,(r + 1))) = 0{,}992$$

Данные, рассчитанные по этим формулам, занесем в табл. 1 (см. 2 последние строки).

Очевидно, что возникновение отказа под влиянием человеческого фактора происходит гораздо реже, чем простое проявление ошибки ввода данных. Степень влияния ошибки оператора на отказ КСА нижнего уровня можно характеризовать:

$$1 > K_{\text{са}\,P(t)} \geq K_{\text{рв}}.$$

Таким соотношением мы оценили влияние человеческого фактора на ввод итоговых протоколов во время проведения выборов. Примем вероятность возникновения отказов при этом за верхнюю границу $K_{\text{рв}}$ , таким образом,

$$K_{\text{са}\,P(t)} = 0{,}999.$$

Этот коэффициент влияет на вероятность безотказной работы $P(t)$ во время проведения выборов и может быть учтен только для нижнего уровня. Кроме того, данная оценка влияния человеческого фактора на надежность узла нижнего уровня является явно заниженной относительно истинного значения.

Оценим влияние коэффициента учета человеческого фактора $K_{\text{са}}$ на надежность системы в межвыборный период с учетом времени восстановления

$$K_{\text{са в.у.}} \approx 0{,}9995, \qquad K_{\text{са ср.у.}} \approx 0{,}995, \qquad K_{\text{са н.у.}} \approx 0{,}995.$$

Тогда влияние человеческого фактора на коэффициент готовности системы в целом можно грубо оценить как:

$$K_{\text{са}} = K_{\text{са в.у.}}\, K_{\text{са ср.у.}}\, K_{\text{са н.у.}} \approx 0{,}99.$$

$K_{са} = 0{,}99$ (будем считать нижней границей влияния человеческого фактора на надежность системы в целом, причем оценена она для межвыборного периода, т. е. будет влиять на коэффициент готовности и коэффициенты оперативной готовности системы в целом и отдельных уровней КСА).

Отдельное место в решении вопроса учета влияния человеческого фактора на надежность работы системы занимает наличие средств защиты программных продуктов от воздействий извне.

$$K_{защ} = (\alpha_{атак} K_{г\ атак} + \alpha_{вир} K_{г\ вир} + \\ + \alpha_{дост} K_{г\ дост} + \alpha_{восст} K_{г\ восст})/\Sigma\ \alpha, \qquad (4.2)$$

$K_{защ}$ — коэффициент учета человеческого фактора подсистемы защиты ПО при вмешательстве извне,

$\alpha_{атак}$ — коэффициент учета атак извне на систему (Internet и др.), например, число в диапазоне [0, 1] (весовой коэффициент), назначаемое из соображений важности данного показателя,

$K_{г\ атак}$ — коэффициент готовности подсистемы отражения атак на систему (может рассчитываться на основании статистики простоев, сбоев и отказов, вызванных последствиями успешных атак извне),

$\alpha_{вир}$ — коэффициент учета вирусных атак на систему,

$K_{г\ вир}$ — коэффициент готовности антивирусных подсистем (может рассчитываться на основании статистики простоев, сбоев и отказов, вызванных последствиями «успешных» вирусных атак), отличается от $K_{г\ атак}$, так как чисто технически это 2 разных потока возможных отказов,

$\alpha_{дост}$ — коэффициент учета несанкционированного доступа к системе,

$K_{г\ дост}$ — коэффициент готовности подсистем предотвращения несанкционированных доступов (может рассчитываться на основании статистики простоев, сбоев и отказов, вызванных последствиями несанкционированного доступа),

$\alpha_{восст}$ — коэффициент учета восстановления системы,

$K_{г\ восст}$ — коэффициент готовности подсистемы восстановления данных (может рассчитываться на основании статистики простоев, вызванных процедурой восстановления),

$\Sigma\ \alpha$ — сумма всех коэффициентов $\alpha_I$ формулы.

$$\alpha_I = A_I/\Sigma_{I=1}^{n} A_I, \quad (\alpha_1 = \alpha_{атак}, \alpha_2 = \alpha_{вир} \text{ и т. д.}),$$

где

$A_I$ — экспертная оценка важности $I$-го показателя,

$n$ — количество учитываемых показателей.

Тогда, учитывая формулы (4.1) и (4.2) можно модифицировать формулы (2.4), (2.6), (2.7) с учетом влияния человеческого фактора:

$$K_{\text{г н.у.}} = K_{\text{са н.у.}}\, K_{\text{защ н.у.}}\, ((A_1\, K_{\text{г ск}}\, (1 - (1 - K_{\text{г АРМ1}})^2)) + \\ + (A_2\, K_{\text{г ск}}\, (1 - (1 - K_{\text{г АРМ1}})^2)) + \\ + (A_3\, K_{\text{г ск}}\, ((1 - (1 - K_{\text{г АРМ1}})^2)\, K_{\text{г АРМ3}}) + \\ + (A_4\, K_{\text{г ск}}\, ((1 - (1 - K_{\text{г АРМ1}})^2)\, (1 - (1 - K_{\text{г АРМ3}})^2)) + \\ + (A_5\, K_{\text{г ск}}\, ((1 - (1 - K_{\text{г АРМ1}})^2)\, (1 - (1 - K_{\text{г АРМ3}})^3))), \quad (4.3)$$

$$K_{\text{г ср.у.}} = K_{\text{са ср.у.}}\, K_{\text{защ ср.у.}} \sum_{I=1}^{89} (B_I\, K_{\text{защ}}\, K_{\text{г ср.у. }I}), \quad (4.4)$$

$$K_{\text{г в.у.}} = K_{\text{са в.у.}}\, K_{\text{защ в.у.}}\, K_{\text{г сегм. пспд}}\, K_{\text{г сегм. крипто}}\, K_{\text{г ЭП}} \times \\ \times K_{\text{г сегм. серверов}}\, K_{\text{г сои}}\, K_{\text{г сегм. админ.}}\, K_{\text{г сегм. польз.}}\, K_{\text{защ}}\,. \quad (4.5)$$

## 5. Схема надежности системы в целом

Согласно схеме, представленной на рис. 1, исходя из предположения равнозначности понятия полного отказа системы в целом, можно составить общую схему надежности системы, выразив ее, согласно последовательной схеме включения всех элементов схемы надежности, следующей формулой (согласно формулам (2.4) или (4.3), (2.6) или (4.4), (2.7) или (4.5), (3.3), (3.6)):

$$K_{\text{г Системы}} = K_{\text{г в.у.}}\, K_{\text{г пспд ср.у.}}\, K_{\text{г ср.у.}}\, K_{\text{г пспд н.у.}}\, K_{\text{г н.у.}}. \quad (5.1)$$

Аналогично коэффициенту готовности ($K_{\text{г Системы}}$) рассчитывается и вероятность безотказной работы $P(t)_{\text{Системы}}$ путем произведения показателей $P(t)$ соответствующих элементов схемы надежности.

Формула (5.1) дает упрощенный расчет надежности. Для более точного расчета необходимо учесть, что отказ одного КСА среднего уровня и его каналов связи с нижним уровнем равнозначен отказу всех входящих в него элементов нижнего уровня и связывающих их каналов связи. Для более точного расчета нужна информация о количестве элементов в каждом звене среднего уровня и о процентном количестве избирателей данного элемента системы.

Исходя из этого, итоговая формула оценки надежности запишется в виде:

$$K_{\text{г Системы}} = K_{\text{г в.у.}} \sum_{i=1}^{89} (B_i\, K_{\text{г пспд ср.у. }i}\, K_{\text{г ср.у. }i} \times \\ \times (\sum_{j=1}^{N\text{н.у.}i} A_{ij}\, K_{\text{г пспд н.у. }ij}\, K_{\text{г н.у. }ij})), \quad (5.2)$$

где $B_i = \text{Изб}_i / \sum_{i=1}^{89} \text{Изб}_i$ ($\text{Изб}_i$ — количество избирателей, обслуживаемых $i$-м КСА среднего уровня, причем $\sum_{i=1}^{89} B_i = 1$) — процент избирателей, обслуживаемых в $i$-м КСА среднего уровня;

$A_{ij}$ = Изб$_{ij}$/Изб$_{i_}$ процент избирателей, обслуживаемых $j$-м элементом нижнего уровня в $i$- среднем звене ($\sum_{j=1}^{N\text{н.у.}i} A_{ij} = 1$);

$N_{\text{н.у.}i}$ — количество элементов нижнего уровня в $i$-м среднем звене.

Формулу (5.2) можно упрощенно представить в виде

$$K_{\text{г Системы}} = K_{\text{г в.у.}} \sum_{i=1}^{89} \times$$
$$\times (B_i K_{\text{г пспд ср.у. } i} K_{\text{г ср.у. } i} (\sum_{j=1}^{N\text{н.у.}i} K_{\text{г пспд н.у. } ij} K_{\text{г н.у. } ij})/N_{\text{н.у.}i}). \qquad (5.3)$$

Формулы (5.2), (5.3) позволяют учесть взаимное влияние среднего и нижнего уровня системы. По данным формулам можно рассчитать надежность системы в случае проведения выборов в одном элементе среднего уровня или даже нижнего уровня. В этом случае получим формулу (5.4)

$$K_{\text{г Системы}} = K_{\text{г пспд ср.у. } i} K_{\text{г ср.у. } i} (\sum_{j=1}^{N\text{н.у.}i} K_{\text{г пспд н.у. } ij} K_{\text{г н.у. } ij})/N_{\text{н.у. } i}. \qquad (5.4)$$

## 5.1. Оценка верхней и нижней границы показателей надежности на основе имеющихся статистических данных отказов ТО, ПО и каналов связи

### 5.1.1. Оценка показателей надежности в условиях неполных статистических данных

Порой анализ накопленной статистики отказов оборудования за год не позволяет сделать вывод о полноте этих данных, но даже в этих условиях на основании неполных данных можно оценить надежность системы в целом и оценить верхнюю и нижнюю границы надежности.

Для неполных статистических данных оценить границы надежности можно следующим образом. Нижняя граница оценивается, исходя из соображений, что предоставленная статистика отражает полную картину отказов в системе в целом, и все остальное оборудование работает не лучше того, по которому предоставлена статистика. Верхняя граница оценивается из соображений, что оборудование, по которому нет статистики отказов, работает абсолютно исправно (вероятность безотказной работы принимаем за 1).

## 5.2. Оценка границ показателей надежности на основе оценки стационарного ординарного потока отказов простейших элементов схемы надежности всех уровней

В данном случае под простейшими элементами схемы надежности будем понимать элементы схем надежности отдельных КСА и каналов связи всех уровней.

### 5.2.1. Характеристика потока отказов элементов схемы надежности

Анализ накопленной статистики отказов показал, что наступление нескольких отказов одного и того же оборудования на малом промежутке времени — событие крайне редкое. Более 95 % отказов технического оборудования происходило однократно в течение года. Из этого следует вывод, что поток отказов можно принять за стационарный и однородный.

### 5.2.2. Схема оценки границы показателей надежности снизу

При произвольном числе отказов вероятность того, что ПТС сохранит достаточную работоспособность для выполнения работы в срок, есть вероятность, что текущее чистое время восстановления (исключая время, когда нет отказов) не превысит резерв времени, отведенный для восстановления отказов. Эта вероятность для *j*-го вида отказов определяется соотношением:

$$P^{(J)}_{во.птс}(T) \geq \sum_{k=1}^{\infty}(1-\sum_{j=0}^{k-1} e^{-\mu_j(T_{пр.в\,j})}\frac{(\mu_j T_{пр.в\,j})^j}{j!})e^{-\lambda_j(T-T_{пр.в\,j})}\frac{(\lambda_j(T-T_{пр.в\,j}))^k}{k!}, \tag{5.5}$$

где $\mu = 1/T_в$ — интенсивность восстановления, зависящая от среднего времени восстановления $T_в$ (этот закон широко используется в теории массового обслуживания),

$\lambda$ — интенсивность отказов в единицу времени, связанная с наработкой на отказ $T_0$ соотношением $\lambda = 1/T_0$,

$k$ — количество отказов,

$j$ — вид отказов,

$T$ — время работы (48 или 69 часов),

$T_{пр.в.}$ — предельно допустимое время восстановления (на интервале работы оборудования $T$).

### 5.2.3. Схема оценки границы показателей надежности сверху

Формула (5.5) дает нижнюю границу вероятности безотказной работы в условиях восстановления отказов ПТС, так как исключает случаи, когда время восстановления меньше $T_{пр.в.j}$. Поэтому в формуле (5.5) применен знак $\geq$. С другой стороны, заменяя в этом выражении интервал чистой работы на интервале времени $T$, получаем верхнюю границу для этой вероятности:

$$P^{(J)}_{во.птс}(T) \leq \sum_{k=1}^{\infty}(1-\sum_{j=0}^{k-1} e^{-\mu_j(T_{пр.в\,j})}\frac{(\mu_j T_{пр.в\,j})^j}{j!})e^{-\lambda_j(T)}\frac{(\lambda_j(T))^k}{k!}, \tag{5.6}$$

где $\mu = 1/T_в$ — интенсивность восстановления, зависящая от среднего времени восстановления $T_в$ (этот закон широко используется в теории массового обслуживания),

$\lambda$ — интенсивность отказов в единицу времени, связанная с наработкой на отказ $T_0$ соотношением $\lambda = 1/T_0$,

$k$ — количество отказов,

$j$ — вид отказов,

$T$ — время работы (48 или 69 часов),

$T_{\text{пр.в.}}$ — предельно допустимое время восстановления (на интервале работы оборудования Т).

#### 5.2.4. Схема расчета границ показателей надежности

По формулам (5.5 и 5.6) производится расчет для каждого ПТС, затем расчет для каждого уровня иерархии схемы надежности Системы, а потом вычисляется итоговая оценка. Данный расчет позволит более точно вычислить границы надежности, но само проведение расчета достаточно трудоемко. Примем время работы $T$ при расчетах за 48 (или 69) часов. Для нашего случая $k$ будет равно 1, $j$ следует принять равным 1 (так как виды отказов мы не дифференцируем), $T_{\text{пр.в.}}$ равным 4 часа.

## Заключение

Приведенный в работе методологический подход к оценке надежности разработан специально для расчета надежности государственной автоматизированной системы «Выборы». Однако, предложенный метод разбиения иерархической системы на уровни, подсчет показателей надежности внутри уровня с последующей последовательной интеграцией полученных результатов на все вышестоящие уровни иерархии, может быть применен для любых человеко-машинных территориально-распределенных информационных систем, построенных по иерархическому принципу.

Проведенные по методике оценочные расчеты показали, что применение предложенной технологии позволяет получить достаточно точные оценки показателей надежности.

Отличительной чертой предлагаемой методики является учет влияния человеческого фактора при оценке надежности работы автоматизированной информационной системы в целом. При этом, следует отметить, что в расчетах удалось получить скорее оценку снизу влияния человеческого фактора на надежность в виду недостаточности исходных данных, что, однако, не умаляет проведенных теоретических исследований.

## Литература


1. *Черкесов Г. Н.* Надежность аппаратно-программных комплексов. СПб.: Питер, 2005. С. 393–395.
2. *Sukert C. A.* An investigation of software reliability models // Proc. Annual Reliability and Maintainability Symp. 1977. P. 478–484.
3. Выборы Президента Российской Федерации. Электоральная статистика. М.: Весь мир, 2004. С. 99.
4. Выборы Депутатов Государственной Думы Федерального собрания Российской федерации. М.: Весь мир, 2004. С. 29.
5. *Кривулец В. Г., Полесский В. П.* Квазиупаковочные оценки характеристик надежности сетей // Передача информации в компьютерных сетях. Информационные процессы. 2001. Т. 1. № 2. С. 126–146.
6. *Дружинин Г. В.* Человек в моделях технологий. Часть I: Свойства человека в технологических системах. М.: МИИТ. 1996. 124 с.
7. *Цибулевский И. Е.* Ошибочные реакции человека-оператора. М.: Сов. радио, 1979. 208 с.
8. Федеральный закон от 10 января 2003 г. № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации “Выборы”».
9. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. М.: Изд-во стандартов, 1989. 36 с.
10. Проект закона «О внесении изменений и дополнений в законодательные акты Российской Федерации» в части изменений Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», в частности статья 81.
11. *Дружинин Г. В.* Надежность автоматизированных производственных систем. М.: Энергоатомиздат, 1986. 480 с. ил.
12. Государственная автоматизированная система Российской Федерации «Выборы». Проектная оценка надежности, ИРЦВ.42 5100 5.013.Б1. ФГУП НИИ «Восход», 2004, 48 с.
13. Надежность в технике. Состав и общие правила задания требований по надежности. ГОСТ 27.003-90. М.: Изд-во стандартов, 1990. 27 с.
14. *Болшев Л. Н., Смирнов Н. В.* Таблицы математической статистики. М.: Наука, 1983. 416 с.