Надёжность информационных систем. Лекции 4–5. Основные задачи и методы расчёта надёжности

Макаров П. А.

23 октября и 6 ноября 2026 г.

Содержание

1 Классификация задач **1**

2 Методы расчёта **2**
2.1 Аналитические методы 2
2.2 Виды аналитических расчётов для невосстанавливаемых и нерезервированных ИС 11
2.3 Статистические методы и цензурирование 15
2.4 Имитационное (Монте-Карло) моделирование 17

3 Контрольные вопросы и задания **18**

Список литературы **18**

1 Классификация задач

Теория надёжности решает четыре класса задач.

1. **Прогнозирование** — определение показателей надёжности объектов на основе конструктивных, технологических и эксплуатационных данных до их изготовления или ввода в эксплуатацию.

2. **Оценка** — расчёт показателей надёжности по данным испытаний или полевой эксплуатации. Требует статистической обработки.

3. **Контроль** — проверка соответствия показателей надёжности установленным нормам (приёмочные, периодические испытания).

4. **Оптимизация** — выбор параметров системы, структуры резервирования, стратегии технического обслуживания (ТО) для максимизации надёжности при тех или иных ограничениях (на стоимость, массу, габариты и т. п.).

2 Методы расчёта

2.1 Аналитические методы

Основаны на математическом описании структуры ИС и законов распределения вероятности безотказной работы (ВБР).

2.1.1 Прямые формулы

Применимы только для самых простейших конфигураций. К ним относятся последовательное и параллельное соединение элементов системы. В первом случае система находится в рабочем состоянии, только если работают все N её элементов, а значит для ВБР справедливо следующее равенство:

$$P_{\text{sys}} = \prod_{i=1}^{N} P_i. \tag{1}$$

Формула (1) является следствием того, что отказы всех звеньев системы рассматриваются как независимые[1].

При параллельном соединении элементов (которое часто используется при резервировании объектов) система работает, если работает хотя бы один её элемент. Кажущееся логичным на первый взляд суммирование $\sum_{i=1}^{N} P_i$ в данном случае некорректно, т. к. мы имеем дело с *вероятностными величинами*, для которых принципиально невозможно $P_{\text{sys}} > 1$. Поэтому правильная формула для ВБР системы из N параллельно-соединённых элементов выводится через вероятность отказа:

$$Q_{\text{sys}} = \prod_{i=1}^{N} Q_i = \prod_{i=1}^{N} (1 - P_i). \tag{2}$$

Как результат, поскольку $P_{\text{sys}} = 1 - Q_{\text{sys}}$, имеем

$$P_{\text{sys}} = 1 - \prod_{i=1}^{N} (1 - P_i). \tag{3}$$

В частном случае параллельного соединения двух элементов из формулы (3) следует

$$P_{\text{sys}} = P_1 + P_2 - P_1 P_2. \tag{4}$$

2.1.2 Метод декомпозиции

Состоит в разложении системы по главным элементам (pivotal element). Позволяет сводить сложные схемы к комбинациям простых. Формально это

[1] Если это не так, то следует применять более общие формулы для условной вероятности зависимых событий.

приводит к оценке надёжности системы по следующей формуле:

$$P_{\text{sys}} = p_e P_{\text{sys}}\Big|_{e=1} + (1 - p_e) P_{\text{sys}}\Big|_{e=0}, \tag{5}$$

где $P_{\text{sys}}\Big|_{e=1}$ — ВБР системы при условии, что элемент e абсолютно надёжен, т. е. $p_e \equiv 1$ (графически это эквивалентно короткому замыканию контактов элемента e в структурной схеме), а $P_{\text{sys}}\Big|_{e=0}$ — ВБР системы при условии, что элемент e абсолютно ненадёжен ($p_e \equiv 0$). Последнее эквивалентно разрыву цепи в месте элемента e.

Формула (5) является результатом применения закона полной вероятности (law of total probability) к структурной функции надёжности. События «элемент e работоспособен» ($X_e = 1$) и «элемент e отказал» ($X_e = 0$) образуют полную группу несовместных событий. Поэтому вероятность работоспособного состояния системы можно разложить по этому базису:

$$\mathbb{P}\{\text{сист. раб.}\} = \mathbb{P}\{\text{сист. раб.}|X_e = 1)\}p_e + \mathbb{P}\{\text{сист. раб.}|X_e = 0)\}(1 - p_e). \tag{6}$$

Формула (5) позволяет рекурсивно упрощать сложные структуры (мостовые, решётчатые), пока они не сведутся к последовательно-параллельным комбинациям, для которых надёжность считается напрямую. Выбор главного (pivotal) элемента e влияет на скорость сходимости расчётного алгоритма.

Пример

Для мостовой схемы из пяти элементов (см. мост Уитстона на рис. 1(a)) выбор центрального элемента в качестве главного $e = 5$ даёт следующую схему определения надёжности всей системы.

1. При $X_5 = 1$ схема сводится к двум последовательно соединённым блокам, в каждом из которых элементы соединены параллельно (рис. 1(b)). Применение формул (3) и (1) при этом даёт

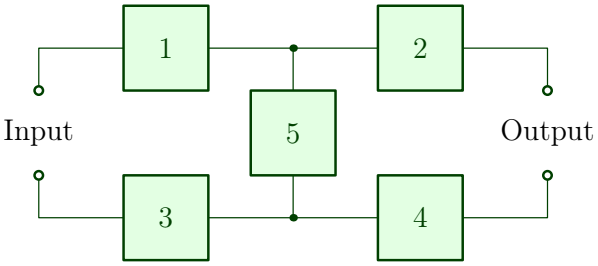
$$P_{\text{sys}}\Big|_{e=1} = (P_1 + P_3 - P_1P_3) \cdot (P_2 + P_4 - P_2P_4). \tag{7}$$

2. При $X_5 = 0$ схема распадается на две параллельно-соединённые ветви, каждая из которых представляет собой последовательное соединение элементов (рис. 1(c)). Используя формулы (1) и (3) в этом случае, получаем

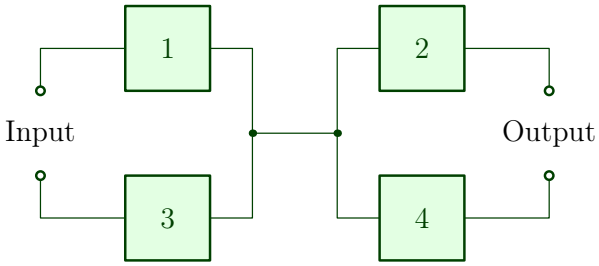
$$P_{\text{sys}}\Big|_{e=0} = P_1P_2 + P_3P_4 - P_1P_2P_3P_4. \tag{8}$$

3. Окончательно, подставляя в (5) полученные на предыдущих этапах промежуточные результаты (7) и (8), и считая $p_e = P_5$, получаем

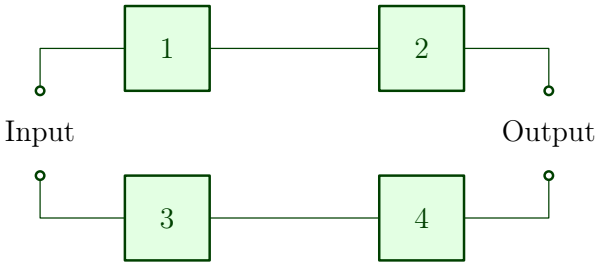
$$\begin{aligned} P_{\text{sys}} = {} & P_5(P_1 + P_3 - P_1P_3)(P_2 + P_4 - P_2P_4) + \\ & + (1 - P_5)(P_1P_2 + P_3P_4 - P_1P_2P_3P_4). \end{aligned} \tag{9}$$



(a) Исходная расчётная схема



(b) $X_5 = 1$



(c) $X_5 = 0$

Рис. 1: Применение метода декомпозиции для мостовой схемы из пяти элементов

Сравнение надёжности мостовой схемы, вычисленное в соответствии с (9), с надёжностью последовательной (1) и параллельной (3) схем наглядно представлено на рис. 2.

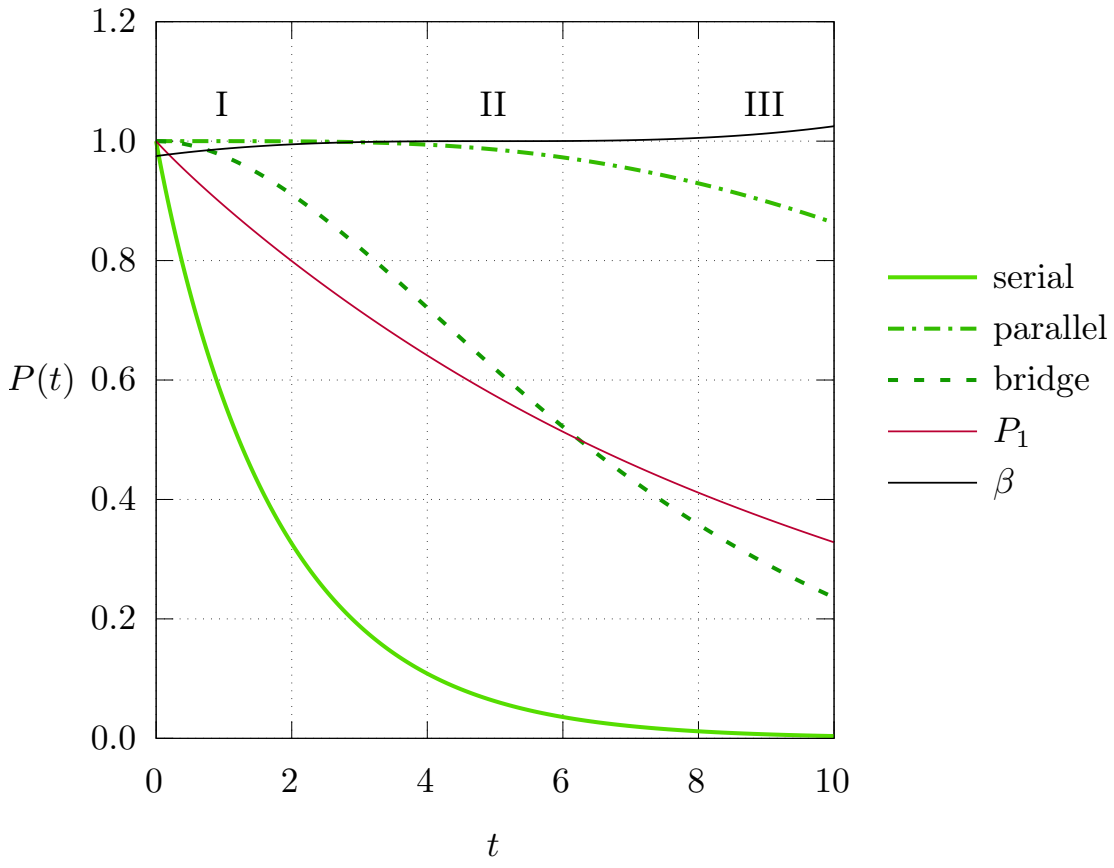


Рис. 2: Сравнение ВБР для различных схем включения пяти одинаковых элементов, работающих согласно модели Вейбулла при $t_0 = 9$

Мостовая схема (или схема с перекрёстной связью) в теории надёжности ИС описывает ситуации, когда имеются две основные параллельные ветви объектов, но между ними присутствует «перемычка», позволяющая системе перераспределить нагрузку или обойти отказ, не требуя полного дублирования каждого компонента. При этом «элементами» $1-5$ на схеме рис. 1(а) могут быть не только физические детали, но и сетевые соединения, логические пути или каналы связи. Приведём несколько конкретных реализаций мостовой схемы.

Физический уровень: Система питания серверной стойки. В высоконадёжных ЦОД каждый сервер или стойка подключается к двум независимым вводам питания, но между ними есть автоматический выключатель связи (Bus Tie).

- Input — городская электрическая сеть / генераторы.
- 1 — ввод питания от электрического щита A (кабель + автомат).
- 2 — блок распределения питания PDU A (Power Distribution Unit).
- 3 — ввод питания от щита B (резервный кабель + автомат).
- 4 — блок распределения питания PDU B.
- 5 — межсекционный выключатель (Bus Tie Breaker) между PDU A и PDU B.
- Output — серверы.

Такой мост работает по следующему алгоритму.

- При $X_5 = 1$ (выключатель 5 замкнут): PDU A и PDU B объединены в одну шину. Если отключается ввод A (элемент 1), то серверы продолжают питаться через ввод B по резервной линии: $3 \to 5 \to 2$.
- При $X_5 = 0$ (выключатель 5 разомкнут/сломан) секции изолированы. Если отключается ввод A, то серверы на PDU A обесточиваются, даже если ввод B (элемент 3) и PDU B (элемент 4) работают.

Вывод: Элемент 5 (перемычка) критически важен при учёте плавной деградации системы. Его надёжность должна быть максимальной, так как он является «спасательным кругом» для обеих цепей питания серверов.

Сетевой уровень: Сеть хранения данных (SAN — Storage Area Network) с Multipath I/O. Сервер подключён к массиву дисков (реализующему SAN) через два независимых адаптера HBA (Host Bus Adapter) и два коммутатора (FS — Fabric Switch), чтобы исключить единую точку отказа.

- Input — сервер (приложение).
- 1 — HBA-порт 1 и кабель до коммутатора 1.
- 2 — коммутатор FS 1.

- 3 — HBA-порт 2 и кабель до коммутатора 2.
- 4 — коммутатор FS 2.
- 5 — магистральный кабель ISL (Inter-Switch Link), соединяющий коммутаторы FS 1 и FS 2.
- Output — контроллеры SAN и дисковый массив.

Если ISL разорван, то сеть «рассыпается» на два изолированных острова. Так, отказ HBA-порта 1 означает полную потерю доступа к дискам через коммутатор 1, даже если FS 2 исправен.

Логический уровень: Микросервисная архитектура с fallback-маршрутизацией. Представим систему обработки платежей, где важно не потерять транзакцию, если отказал один из микросервисов.

- Input — API-шлюз (получает запрос от клиента).
- 1 — канал связи с микросервисом A (основной процессинг).
- 2 — микросервис A.
- 3 — канал связи с микросервисом B (резервный процессинг / асинхронная очередь).
- 4 — микросервис B.
- 5 — общая шина данных / кэш (например, Redis или Kafka), куда оба микросервиса могут писать и читать состояние.
- Output — успешная транзакция.

Как работает данный мост:

- При $X_5 = 1$ кэш / шина работает, а значит если микросервис A (элемент 2) “упадёт”, то API-шлюз через микросервис B (4) и общую шину (5) сможет получить доступ к временному кэшу состояний микросервиса A (2) и завершить транзакцию.
- При $X_5 = 0$ кэш / шина недоступны. В этом случае микросервисы полностью изолированы друг от друга: падение микросервиса A (1 или 2) ведёт к отказу всей системы для части пользователей, так как микросервис B не сможет “подхватить” его незавершённые сессии.

Главные выводы по рассмотренному примеру. Мостовая схема наглядно иллюстрирует одну из теорем теории надёжности, которую можно сформулировать так: *Перекрёстное резервирование повышает надёжность системы, но создаёт новые точки уязвимости.*

Действительно, как видно из рис. 3, наличие перемычки 5 существенно увеличивает общую ВБР P_{sys}, однако если надёжность P_5 самой перемычки

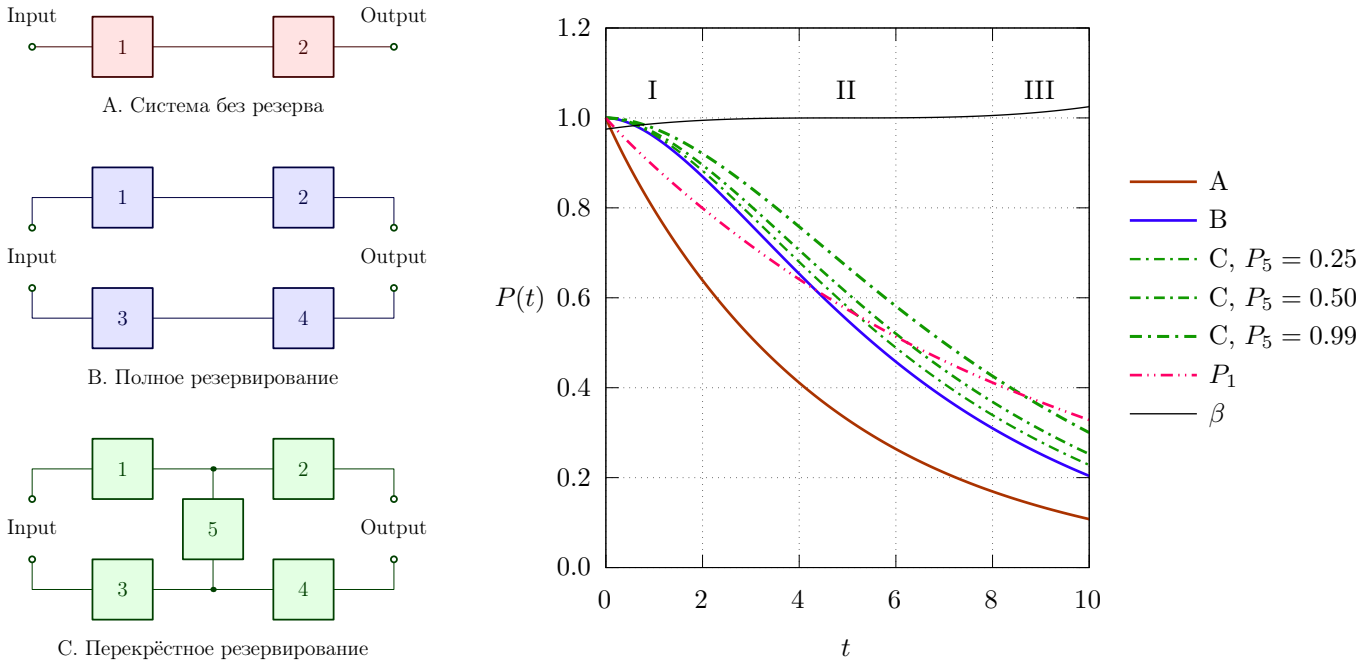


Рис. 3: Иллюстрация справедливости теоремы о перекрёстном резервировании для случая одинаковых элементов $1-4$ ($P(t) = \exp(t/t_0)^\beta$, $t_0 = 9$) и перемычки со стационарной надёжностью $P_5 = \text{const}$

низкая, то вся система фактически деградирует до простого параллельно-последовательного соединения, и преимущества моста теряются. В связи с этим в IT при построении мостовых схем (например, при настройке ISL в SAN или Bus-Tie в силовой электронике) элемент 5 часто сам делают логически избыточным (например, прокладывают два ISL-кабеля вместо одного).

2.1.3 Граничные оценки

Дают диапазон значений $P_{\text{low}} \leqslant P_{\text{sys}} \leqslant P_{\text{up}}$ в тех случаях, когда точное решение получить затруднительно. Оценки P_{low} и P_{up} строятся по минимальным путям и минимальным сечениям (или срезам).

Опр. 1. ***Минимальный путь / Minimal path*** **:** Это минимальный набор элементов, одновременная работа которых гарантирует, что система работоспособна.

Примечание: Минимальность здесь означает, что если убрать из этого набора хоть один элемент, то система становится неработоспособной.

Главное свойство: Система работает тогда и только тогда, когда работает хотя бы один минимальный путь (фактически, мы рассматриваем систему как параллельное соединение путей и связываем их надёжности логической операцией дизъюнкция).

Опр. 2. ***Минимальное сечение (или срез) / Minimal cut*** **:** Это минимальный набор элементов, одновременный отказ которых гарантирует неработоспособность системы.

Примечание: При этом реализуется логика операции конъюнкция для отказа системы.

Главное свойство: Система отказывает тогда и только тогда, когда отказывает хотя бы одно минимальное сечение.

Почему оценки P_{low} и P_{up} вообще возникают? Мы знаем, что

$$\mathbb{P}\{\text{сист. раб.}\} = \mathbb{P}\left\{\text{работоспособно } \bigcup_k j_k\right\} = P\left(\bigcup_k X_k\right), \tag{10}$$

однако пути j_k в общем случае пересекаются, так как могут содержать одинаковые элементы[2]. Следовательно события X_k (состоящие в том, что путь j_k работоспособен), вероятность исхода которых мы оцениваем в правой части равенства (10), **зависимы** (иногда говорят, что события X_k **положительно скоррелированы**). Формулы полного сложения вероятностей для зависимых событий достаточно громоздкие и сложные, а для больших систем их вообще крайне затруднительно получить. Именно поэтому и придуманы граничные оценки, опирающиеся на «пессимистичные» допущения, с помощью которых сложную систему с пересечениями можно заменить более простой.

Строгие (структурные) оценки

При таком подходе делаются максимально пессимистичные допущения, полностью игнорирующие избыточность системы.

1. **Нижняя оценка (пессимистичный взгляд на успех).** Система точно работает, только если работают все минимальные пути одновременно (если хоть один путь не работает, система может отказать, поэтому мы перестраховываемся).
$$P_{\text{low}} = \prod_k P(j_k). \tag{11}$$

2. **Верхняя оценка (пессимистичный взгляд на отказ).** Система точно откажет, только если откажут все минимальные сечения одновременно.
$$Q_{\min} = \prod_k Q(s_k). \tag{12}$$
Следовательно
$$P_{\text{up}} = 1 - Q_{\min} = 1 - \prod_k Q(s_k). \tag{13}$$

[2]Так, например, элемент 1 есть и в пути j_1, и в пути j_3.

Граничные оценки на примере моста Уитстона

Выпишем для изображённого на рис. 1(а) моста Уитстона все минимальные пути, минимальные сечения[3], а также соответствующие им ВБР и вероятности отказов. Сформируем из полученных данных таблицу 1.

Таблица 1: Данные для граничных оценок надёжности моста Уитстона

k	j_k	$P(j_k)$	s_k	$Q(s_k)$
1	$1 \to 2$	P_1P_2	$\{1,3\}$	$(1-P_1)(1-P_3)$
2	$3 \to 4$	P_3P_4	$\{2,4\}$	$(1-P_2)(1-P_4)$
3	$1 \to 5 \to 4$	$P_1P_4P_5$	$\{1,5,4\}$	$(1-P_1)(1-P_4)(1-P_5)$
4	$3 \to 5 \to 2$	$P_2P_3P_5$	$\{3,5,2\}$	$(1-P_2)(1-P_3)(1-P_5)$

Используя содержимое третьей и пятой колонок таблицы 1 в формулах (11) и (13), рассчитаем оценки надёжности для нескольких вариантов схем. Вычисленные значения представим в таблице 2.

Таблица 2: Результаты строгих оценок для нескольких мостовых систем

Type	P_i	P_{sys}	P_{low}	P_{up}
A	$\{P_i\}_1^5 = 0.5$	0.5	0.001	0.999
B	$\{P_i\}_1^4 = 0.5$, $P_5 = 0.9$	0.55	0.003	0.999
C	$\{P_i\}_1^4 = 0.9$, $P_5 = 0.5$	0.972	0.108	0.999
D	$\{P_i\}_1^5 = 0.9$	0.978	0.349	0.999

Вывод: Как видно из таблицы 2, полученные нами оценки верны (истинные вероятности P_{sys}, вычисленные согласно точной формуле (9) действительно лежат в интервале $P_{\text{sys}} \in [P_{\text{low}}, P_{\text{up}}]$), однако они чрезвычайно широкие. Поэтому на практике используются другие методы, дающие более точные (узкие) границы. К их числу относятся: «инженерные» оценки, основанные на неравенстве Буля; формула включений-исключений; метод непересекающихся путей и т. п.

2.1.4 Булевы методы

Для определения надёжности сложных систем используют алгебру логики. При этом для системы строится **функция работоспособности (структурная функция)** $\phi(\mathbf{X})$ — булева функция, ставящая в соответствие вектору состояний элементов системы $\mathbf{X} = (X_1, \ldots, X_N) = \{0,1\}^N$ состояние работоспособности

[3]Для их определения полезно задать вопрос: *"Что нужно сломать, чтобы изолировать вход системы от её выхода?"*

системы (1 – работоспособное состояние, 0 — отказ)

$$\phi(\mathbf{X}) : \{0,1\}^N \to \{0,1\}. \tag{14}$$

Надёжность системы при этом выражается через математическое ожидание функции работоспособности

$$P_{\text{sys}} = \mathbb{M}[\phi(\mathbf{X})] = \sum_{\mathbf{x}} \phi(\mathbf{x}) \prod_{i=1}^{N} p_i^{x_i}(1-p_i)^{1-x_i}. \tag{15}$$

Для понимания смысла формулы (15) необходимо определиться со всеми принятыми в ней обозначениями.

1. Так, $\mathbf{X} = (X_1, \ldots, X_N)$ — это вектор состояний элементов системы. Каждый X_i — это случайная величина, принимающая значение 1 (элемент работает) или 0 (отказ элемента).

2. $\mathbf{x} = (x_1, \ldots, x_N)$ — это конкретная реализация состояния элементов системы, например, $(1, 0, 1, 1, 0)$. Если в системе N элементов, то всего таких состояний 2^N.

3. $\phi(\mathbf{x})$ — функция работоспособности. Для конкретного сценария $\mathbf{x}$ она возвращает 1, если система в этом случае работает, и 0, если система не работоспособна.

4. $\prod p_i^{x_i}(1-p_i)^{1-x_i}$ — это вероятность того, что реализуется именно сценарий $\mathbf{x}$ при условии, что элементы отказывают независимо.

5. $\sum\limits_{\mathbf{x}}$ — перебор всех 2^N возможных сценариев, в процессе которого вероятность каждого сценария умножается на его «вес» $\phi(\mathbf{x}) = \{0,1\}$, и суммирование всех этих значений.

Пример. Веб-кластер для работы которого требуются:

- одно хранилище данных S;
- приложение A_1 на сервере 1 или приложение A_2 на сервере 2;
- каждому серверу необходима своя подсистема питания B_1, B_2.

Функция работоспособности в этом случае:

$$\phi(\mathbf{X}) = S \wedge ((B_1 \wedge A_1) \vee (B_2 \wedge A_2)). \tag{16}$$

Перечислим только те сценарии, которые соответствуют единичным значениям функции (16) и вычислим соответствующие вероятности их реализации. Представим эти данные в таблице 3. Итоговый результат для ВБР рассматриваемого веб-кластера согласно (15) определяется при этом суммой всех элементов последнего столбца данной таблицы.

Булевы методы эффективны при автоматизации расчётов надёжности. Наиболее часто встречаются два следующих варианта.

Таблица 3: Работоспособные конфигурации и их вероятности для функции (16)

S	A_1	B_1	A_2	B_2	$P_{\mathbf{x}}$
1	1	1	1	1	$P_S P_{A1} P_{B1} P_{A2} P_{B2}$
1	1	1	1	0	$P_S P_{A1} P_{B1} P_{A2} (1 - P_{B2})$
1	1	1	0	1	$P_S P_{A1} P_{B1} (1 - P_{A2}) P_{B2}$
1	1	1	0	0	$P_S P_{A1} P_{B1} (1 - P_{A2})(1 - P_{B2})$
1	1	0	1	1	$P_S P_{A1} (1 - P_{B1}) P_{A2} P_{B2}$
1	0	1	1	1	$P_S (1 - P_{A1}) P_{B1} P_{A2} P_{B2}$
1	0	0	1	1	$P_S (1 - P_{A1})(1 - P_{B1}) P_{A2} P_{B2}$

- Метод непересекающихся путей (SDP — Sum of Disjoint Products). Основывается на представлении $\phi(\mathbf{X})$ в виде суммы непересекающихся произведений. Позволяет вычислять ВБР как обычную сумму, избегая формулы включения-исключения для условной вероятности зависимых событий.

- Диаграммы бинарных решений (BDD — Binary Decision Diagrams).

2.2 Виды аналитических расчётов для невосстанавливаемых и нерезервированных ИС

Обзор основных аналитических методов, применимых для произвольных систем в общем случае, приведён нами в разделе 2.1. Здесь же мы рассмотрим чуть более подробно главные виды расчёта характеристик надёжности самых простых объектов — нерезервированных ИС, состоящих из невосстанавливаемых подсистем, соединённых последовательно.

Очевидно, что отказ такой системы наступает при отказе любой из её подсистем. При расчёте надёжности таких ИС предполагают, что отказы всех их элементов являются случайными и независимыми событиями. Тогда ВБР системы равна произведению ВБР её элементов, как это и предполагалось в (1). Так как ВБР элементов $P_i(t)$ можно выразить через интенсивность их отказов $\lambda_i(t)$, то расчётные формулы для ВБР устройства при последовательном соединении элементов можно записать следующим образом:

$$P_{\text{sys}}(t) = \exp\left[-\sum_{i=1}^{N} \int_0^t \lambda_i(t_1)\,\mathrm{d}t\right]. \tag{17}$$

Выражение (17) наиболее общее. Оно позволяет определить ВБР системы до первого отказа при любом законе изменения интенсивности отказов с наработкой. На практике интенсивность отказов часто является постоянной величиной (для периода нормальной эксплуатации $\lambda_i = \text{const}$), поэтому ВБР описывается

экспоненциальным распределением

$$P_{\text{sys}}(t) = e^{-\lambda_{\text{sys}} t} = e^{-t/T_{\text{sys}}}, \quad T_{\text{sys}} = \frac{1}{\lambda_{\text{sys}}}, \tag{18}$$

где

$$\lambda_{\text{sys}} = \sum_{i=1}^{N} \lambda_i, \tag{19}$$

а плотность распределения наработки системы на отказ (частота отказов)

$$f_{\text{sys}}(t) = \lambda_{\text{sys}}\, e^{-\lambda_{\text{sys}} t}. \tag{20}$$

Более того, на практике очень часто приходится вычислять характеристики высоконадёжных систем. При этом произведение $\lambda_{\text{sys}}\, t \ll 1$, а $P_{\text{sys}}(t) \approx 1$. В этом случае, используя разложение в ряд Тейлора и ограничиваясь первыми несколькими слагаемыми, с высокой степенью точности можно пользоваться приближенными формулами

$$P(t) \approx 1 - \lambda_{\text{sys}}\, t, \qquad Q(t) \approx \lambda_{\text{sys}}\, t, \qquad f_{\text{sys}}(t) \approx \lambda_{\text{sys}}\, (1 - \lambda_{\text{sys}} t)\,. \tag{21}$$

Вычисление количественных характеристик надёжности по приближенным формулам (21) не даёт больших ошибок для систем, ВБР которых $P_{\text{sys}} > 0.9$, т. е. для $\lambda_{\text{sys}}\, t \leqslant 0.1$.

Далее, в зависимости от полноты учёта факторов, влияющих на работу ИС, различают прикидочный, ориентировочный и окончательный расчёты надёжности.

2.2.1 Прикидочный расчёт надёжности (метод подсчёта элементов)

Прикидочный расчёт применяется после получения технического задания (ТЗ) на этапе эскизного проектирования системы и основывается на следующих допущениях.

- Все элементы системы равнонадёжны: $\lambda_i = \lambda_{\text{eq}}$;
- Интенсивности отказов не зависят от времени: $\lambda_{\text{eq}} = \text{const}$;
- Отказ любого элемента приводит к отказу всей системы.

В этом случае результирующая интенсивность отказов:

$$\lambda_{\text{sys}} = N \lambda_{\text{eq}}, \tag{22}$$

где N — общее число элементов.

Основные адекватные сценарии применения прикидочного расчёта надёжности следующие.

1. **Раннее концептуальное проектирование:** Проверка требований заказчика по надёжности системы, выдвинутых в ТЗ на её проектирование. По-сути, это очень грубая оценка порядка величин («бюджетирование надёжности») на этапе выбора архитектуры, когда точных данных о компонентах ещё нет.

2. **Сравнительный анализ надёжности отдельных вариантов системы:** Оценка относительной надёжности двух разных архитектурных решений при использовании одной и той же упрощённой модели (важна разница между вариантами, а не абсолютное значение).

3. **Расчёт нормативных данных по надёжности отдельных подсистем.** При этом рассматриваются только простые, нерезервированные аппаратные узлы: схемы, где нет ECC, резервирования или микрокода, и отказ любого элемента действительно ведёт к отказу всей подсистемы (например, простой аппаратный watchdog-таймер на базовой логике или цепь аварийного отключения).

4. **Определение минимально допустимого уровня надёжности элементов проектируемой системы.** Необходимо для формального соблюдения консервативных стандартов: некоторые нормы требуют такого подхода именно для получения гарантированно пессимистичной (и поэтому «безопасной» с точки зрения сертификации) оценки.

Прикидочный расчёт надёжности позволяет судить о принципиальной возможности обеспечения требуемой надёжности объекта, однако применять его следует крайне осторожно с учётом всех его слабых сторон.

2.2.2 Ориентировочный расчет надежности

Применяется после разработки электрических схем. Ориентировочный расчёт надёжности учитывает влияние только количества и типов применённых элементов и основывается на следующих допущениях:

- все элементы данного типа равнонадёжны, т. е. величины интенсивности отказов λ_i для этих элементов одинаковы;

- все элементы работают в номинальном (нормальном) режиме ($\lambda_i = \lambda_{0i}$), предусмотренном техническими условиями;

- интенсивности отказов всех элементов не зависят от времени, т.е. в течение срока службы у элементов, входящих в изделие, отсутствует старение и износ, следовательно, $\lambda_{0i}(t) = \text{const}$;

- отказы элементов изделия являются событиями случайными и независимыми;

- все элементы изделия работают одновременно.

Для определения надёжности изделия необходимо знать:

1. типы элементов, входящих в систему, и число элементов каждого типа;
2. величины интенсивности отказов элементов λ_i, входящие в изделие;
3. вид соединения элементов.

Таким образом, при ориентировочном расчёте надёжности достаточно знать структуру системы, номенклатуру применённых элементов и их количество.

2.2.3 Окончательный расчёт надёжности

Окончательный расчёт надёжности выполняется тогда, когда известны реальные режимы работы всех элементов после испытания макетов и основных подсистем объекта в лабораторных условиях. Элементы объекта обычно находятся в различных режимах работы, отличающихся от номинального. Это влияет на надёжность как системы в целом, так и отдельных её составляющих.

Выполнение окончательного расчёта надёжности возможно только при наличии данных о параметрах нагрузки отдельных элементов и при наличии моделей зависимости интенсивности отказов элементов от потребляемой ими электрической мощности, температуры окружающей среды и других существенных факторов, т. е. для окончательного расчёта необходимо знать зависимости

$$\lambda_i = \lambda_i(T_0, K, v, \varphi, \dots), \tag{23}$$

где T_0 — температура окружающей среды, K — электрическая нагрузка, а v и φ — параметры механических и климатических воздействий.

Во многих случаях удаётся сводить (24) к следующей форме

$$\lambda_i = \alpha_i \prod_j k_i^{(j)} \lambda_{0i}, \tag{24}$$

где $\alpha = \alpha(T_0, K)$ — поправочный коэффициент, учитывающий температуру и электрическую нагрузку, а $k^{(j)} = k^{(j)}(v, \varphi)$ — поправочные коэффициенты, учитывающие механические и климатические воздействия.

Для современных полупроводниковых компонентов (CPU, NVMe, DDR5) зависимости $\alpha_i(T_0, K)$ опираются на соответствующие физико-технологические модели [1; 2]: например, интенсивность отказов SSD экспоненциально растёт с температурой по закону Аррениуса (25), а для CPU критичным фактором является не столько температура, сколько *электромиграция* (так называемый *электронный ветер*) в транзисторах при высоких K.

Закон Аррениуса, в частности, может быть представлен в следующем виде

$$\lambda_{\text{SSD}}(T_0) = \exp\left[\frac{E_a}{k_B}\left(\frac{1}{T_{\text{ref}}} - \frac{1}{T_0}\right)\right], \tag{25}$$

где $E_a \approx 0.7$ эВ — энергия активации, k_B — постоянная Больцмана, $T_{\text{ref}} = 313$ K (40 °C), T_0 — рабочая температура.

2.3 Статистические методы и цензурирование

В реальных условиях испытания часто прерываются, что приводит к **цензурированным данным**.

Цензурирование (censoring) в теории надёжности — это ситуация в которой точное время безотказной работы объекта t_i не наблюдается в полном объёме (для всех элементов выборки), но известно, что t_i превышает некоторый порог наблюдения t_c. Формально, для i-го элемента наблюдается пара (t_i, δ_i), где

$$\delta_i = \begin{cases} 1, & \text{если отказ зафиксирован в момент } t_i, \\ 0, & \text{если элемент работал до } t_c \text{ и был изъят из испытаний.} \end{cases}$$

При $\delta_i = 0$ известно лишь, что $t_i \geqslant t_c$.

Различают следующие типы цензурирования.

- **Тип I (по времени).** Испытания останавливаются в фиксированный момент $T_{\max}$. Число отказавших элементов n известно, остальные $N_0 - n$ объектов на момент $T_{\max}$ — работоспособны.
- **Тип II (по числу отказов).** Испытания останавливаются после возникновения d отказов.
- **Случайное/прогрессивное.** Объекты могут выходить из выборки в случайные моменты по причинам, не связанным с отказами (плановое ТО, обновление парка, вывод из эксплуатации, потеря связи с объектами и т. п.).

Рассмотрим классическую задачу теории надёжности — определение точечной интенсивности отказов $\widehat{\lambda}$ при цензурировании данных первого и второго типа. Поскольку в обоих случаях мы не наблюдаем полные данные об отказах, прямое вычисление $\lambda(t)$ при этом невозможно. Вместо этого используются приближённые параметрические и непараметрические (основанные на оценке кумулятивной интенсивности) подходы.

Остановимся только на одном параметрическом подходе — **методе максимального правдоподобия**, который состоит в следующем.

1. Предполагается, что ВБР подчиняется некоторому параметрическому распределению $P(t;\theta)$ с параметрами θ (например, распределению Вейбулла или экспоненциальному).
2. Для данной схемы цензурирования определяется функция правдоподобия $L(\theta)$.
3. Из условия максимальности

$$\frac{\partial}{\partial\theta} \ln L(\theta) = 0 \tag{26}$$

находятся оценки параметров $\widehat{\theta}$.

4. Точечная интенсивность вычисляется по теоретической формуле для выбранного распределения при найденных на предыдущем этапе параметрах $\widehat{\lambda}(t) = \lambda(t; \widehat{\theta})$.

Функция правдоподобия $L(\theta)$ имеет следующий вид.

- **Цензурирование по времени:**

$$L_I(\theta) = \prod_{i=1}^{n} f(t_i; \theta) \cdot \prod_{j=1}^{N_0 - n} P(T_{\max}; \theta). \tag{27}$$

- **Цензурирование по числу отказов:**

$$L_{II}(\theta) = \prod_{i=1}^{d} f(t_i; \theta) \cdot \prod_{j=1}^{N_0 - d} P(t_d; \theta). \tag{28}$$

Для экспоненциального распределения $P(t; \theta = \lambda) = e^{-\lambda t}$ и, поскольку

$$f(t) = -\frac{\mathrm{d}P}{\mathrm{d}t} = \lambda\, e^{-\lambda t},$$

имеем

$$L_I(\lambda) = \lambda^n \exp\left[-\lambda \left(\sum_{i=1}^{n} t_i + (N_0 - n) T_{\max}\right)\right], \tag{29}$$

$$L_{II}(\lambda) = \lambda^d \exp\left[-\lambda \left(\sum_{i=1}^{d} t_i + (N_0 - d) t_d\right)\right]. \tag{30}$$

Условие (26) при этом даёт

$$\frac{\partial \ln L_I(\lambda)}{\partial \lambda} = \frac{n}{\widehat{\lambda}_I} - \left(\sum_{i=1}^{n} t_i + (N_0 - n) T_{\max}\right) = 0, \tag{31}$$

$$\frac{\partial \ln L_{II}(\lambda)}{\partial \lambda} = \frac{d}{\widehat{\lambda}_{II}} - \left(\sum_{i=1}^{d} t_i + (N_0 - d) t_d\right) = 0. \tag{32}$$

И окончательно, для точечной оценки интенсивности отказов получаем

$$\widehat{\lambda}_I = \frac{n}{\sum\limits_{i=1}^{n} t_i + (N_0 - n) T_{\max}}, \tag{33}$$

$$\widehat{\lambda}_{II} = \frac{d}{\sum\limits_{i=1}^{d} t_i + (N_0 - d) t_d}. \tag{34}$$

Игнорирование цензурирования приводит к искажённым оценкам величин λ, $MTTF$ и т. п.

Также на практике часто необходимо определять доверительные интервалы тех или иных статистических величин. Доверительным интервалом называют интервал $[x_L, x_U]$, накрывающий истинное значение величины x с заданной доверительной вероятностью $1-\alpha$ (обычно 0.9 или 0.95) $P(x_L \leqslant x \leqslant x_U) = 1-\alpha$. Доверительный интервал строится через χ^2-распределение (частный случай гамма-распределения).

Так, для экспоненциального закона сумма n независимых времён наработки до отказа имеет распределение $\Gamma(n, \lambda)$. Суммарная наработка при этом описывается статистической величиной $2\lambda T_{\text{sum}}$, которая подчиняется распределению χ^2 с $2n$ степенями свободы ($2\lambda T_{\text{sum}} \sim \chi^2_{2n}$). Поэтому для интенсивности отказов имеем

$$\frac{\chi^2_{\alpha/2,2n}}{2T_{\text{sum}}} \leqslant \lambda \leqslant \frac{\chi^2_{1-\alpha/2,2n}}{2T_{\text{sum}}}. \tag{35}$$

Квантили $\chi^2_{\alpha/2,2n}$ и $\chi^2_{1-\alpha/2,2n}$ определяются из специальных таблиц либо при помощи аппроксимаций (Корниша — Фишера, Голдштейна и др.) или специализированных библиотек (в частности, библиотека `scipy` для языка Python предоставляет для этого функцию `stats.chi2.ppf()`)

Зная границы доверительного интервала интенсивности отказов (35) можно рассчитать доверительные интервалы и других величин. В частности,

$$MTTF_L = \frac{1}{\lambda_U}, \quad MTTF_U = \frac{1}{\lambda_L} \tag{36}$$

и

$$P_L(t) = \exp(-\lambda_U t), \quad P_U(t) = \exp(-\lambda_L t). \tag{37}$$

2.4 Имитационное (Монте-Карло) моделирование

Общий алгоритм моделирования.

1. Генерация времени отказа каждого элемента системы по заданному закону.
2. Проверка состояния работоспособности системы по структурной схеме. Если произошёл отказ системы — фиксация времени отказа.
3. Многократное «проигрывание» жизненного цикла системы ($N \sim 10^4 - 10^6$).
4. Оценка показателей надёжности системы $P(t)$, $MTTF$, K_g (и других) как выборочных статистических средних.

Точность оценки $\sim 1/\sqrt{N}$.
Применяется в следующих случаях.

- При сложных зависимостях между элементами системы.

- Для нестационарных или неэкспоненциальных законов распределения.
- При наличии восстановлений, приоритетов ремонта, ограниченных ресурсов.

3 Контрольные вопросы и задания

1. Какие приближенные формулы используются при расчёте наработки на отказ и частоты отказов?
2. На каких допущениях основывается прикидочный расчёт надёжности?
3. В каких случаях используется ориентировочный расчёт?
4. При каком методе расчёта надёжности учитываются режимы работы элементов ИС?
5. Что такое коэффициент нагрузки?
6. В каких условиях метод Монте-Карло предпочтительнее аналитического расчёта?

Список литературы

1. *Pecht M.* Product Reliability, Maintainability, and Supportability Handbook. — 2rd Edition. — Boca Raton : CRC Press, 2009. — P. 480. — DOI: 10.1201/9781420009897.
2. *Modarres M.*, *Kaminskiy M. P.*, *Krivtsov V.* Reliability Engineering and Risk Analysis: A Practical Guide. — 3rd Edition. — Boca Raton : CRC Press, 2016. — P. 522.