ИНЖЕНЕРНАЯ ШКОЛА
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И РОБОТОТЕХНИКИ

ТОМСКИЙ
ПОЛИТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ

Безопасность, надежность киберфизических систем, методы оценки и управления риском

Лектор: Ефремов Александр Александрович,
ст. преподаватель ОАР ИШИТР

Томск, 2024

Контактная информация

ЕФРЕМОВ Александр Александрович

Старший преподаватель,
Отделение автоматизации и робототехники,
ИШИТР

Ауд. 112а, 10к.
email: *alexyefremov@tpu.ru*

Структура курса

Лекции:	16 часов	8 баллов
Лабораторные:	16 часов	40 баллов
Практики:	16 часов	16 баллов
ИДЗ:		16 баллов
Промежуточный контроль: экзамен		20 баллов

Лекция 1

Основные понятия и определения.

Лекция 1

Киберфизическая система (КФС) — это система, состоящая из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое.

В КФС обеспечивается тесная связь и координация между вычислительными и физическими ресурсами.

Компьютеры осуществляют мониторинг и управление физическими процессами с использованием такой петли обратной связи, где происходящее в физических системах оказывает влияние на вычисления и наоборот.

Основные составляющие КФС описываются следующим образом:

- **Физический уровень** относится к материальным объектам.
- **Цифровой уровень** охватывает компьютерные алгоритмы, протоколы обработки информации и системные данные, хранящиеся в облаке.
- **Интерфейс цифрового и физического уровней** реализуется путем развертывания датчиков и механизмов управления.
- **Интерфейс взаимодействия человека и КФС** – напр. SCADA.

Эффективность функционирования КФС в значительной степени зависит от надежности как отдельных устройств, входящих в систему, так и элементов, обеспечивающих взаимодействие между этими устройствами.

Недостаточная надежность элементов и устройств не только приводит к значительным простоям системы, но и удорожает стоимость ее эксплуатации.

Кроме того, отказы КФС могут привести к аварийным ситуациям, последствия которых могут быть катастрофическими.

Основными причинами, определяющими повышенное внимание к проблемам надежности, являются:

- повышение сложности устройств и появление сложных систем;
- более медленный рост уровня надежности комплектующих элементов по сравнению с ростом числа элементов в устройствах и системах;
- повышение важности выполняемых элементами и устройствами функций и, как следствие этого, повышение требований к их надежности;
- усложнение условий эксплуатации систем.

Лекция 1

Теория надежности

- устанавливает закономерности возникновения отказов и восстановления работоспособности системы и её элементов,
- рассматривает влияние внешних и внутренних воздействий на процессы в системах,
- создаёт основы расчёта надёжности и предсказания отказов,
- изыскивает способы повышения надёжности при конструировании и изготовлении систем и элементов, а также способы сохранения надёжности при эксплуатации.

Лекция 1

Теория надежности изучает:

- критерии и количественные характеристики надежности;
- методы анализа надежности элементов и систем;
- методы синтеза элементов и систем с заданной надежностью;
- методы повышения надежности элементов и систем на этапах их проектирования и эксплуатации;
- методы испытания элементов и систем на надежность.

Надежностью называется свойство объекта выполнять и сохранять во времени заданные функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортировки.

Термин *«надежность»* часто смешивается с термином *«безопасность»*. Оба этих понятия связаны с анализом работоспособности и отказов технических объектов, изучением их причин и развития.

Однако если надежность системы по определению предполагает только возможность выполнения заданных функций, то безопасность связана с возможностью нанесения ущерба другим объектам, окружающей среде и людям.

Для оценки эффективности управления можно ввести понятие «риск» как меру опасности при разной стратегии управления системами, включая риск при отсутствии управления.

Риск – мера опасности, характеризующая возможность причинения ущерба и его тяжесть. Предполагается, что можно оценить масштаб ущерба – его тяжесть.

В целом понятия «риск» и «опасность» близки.
Чаще всего риск выступает как характеристика действия (рискованные действия), а опасность – как характеристика состояния объекта (опасный фактор).

Управление риском подразумевает анализ риска, оценку риска и контроль риска.

Анализ и оценка риска включают идентификацию опасностей, оценку вероятности событий и оценку последствий.

Контроль риска предполагает определения приемлемого риска и сравнительную оценку вариантов и/или альтернатив посредством мониторинга и анализа решений.
Контроль риска также включает предотвращение отказов (аварий) и уменьшение их последствий.

Элементы и системы, с точки зрения надёжности, могут находиться в пяти состояниях: исправном, неисправном, работоспособном, неработоспособном, предельном.

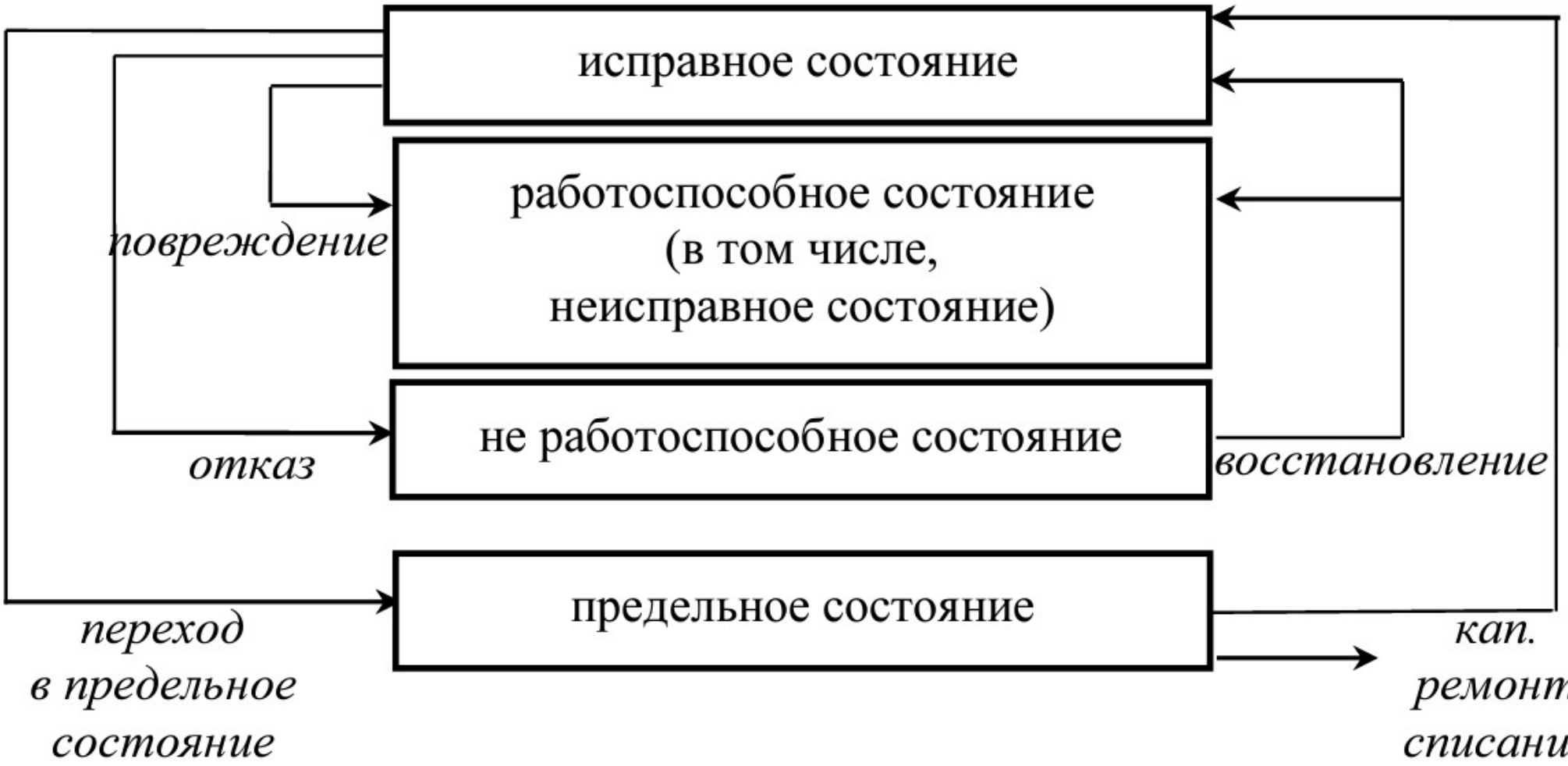
Исправное состояние – это состояние объекта, при котором он соответствует всем требованиям нормативно-технической и (или) конструкторской (проектной) документации.

Неисправное состояние – это состояние объекта, при котором он не соответствует хотя бы одному из требований нормативно-технической и (или) конструкторской (проектной) документации.

Работоспособное состояние – это состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и (или) конструкторской (проектной) документации.

Неработоспособное состояние – это состояние объекта, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствуют требованиям нормативно-технической и (или) конструкторской (проектной) документации.

Предельное состояние – это состояние объекта, при котором его дальнейшая эксплуатация или восстановление работоспособного состояния недопустимо или нецелесообразно.


исправное состояние
работоспособное состояние
(в том числе,
неисправное состояние)
не работоспособное состояние
предельное состояние
повреждение
отказ
восстановление
переход
в предельное
состояние
кап.
ремонт
списание

Как видно из рисунка, только в двух состояниях, исправном и работоспособном, система может выполнять свои функции. Поэтому, с позиций теории надёжности все элементы и системы могут находиться в двух состояниях: работоспособном и неработоспособном.

Переход из одного состояния в другое происходит в результате событий, называемых отказом и повреждением.

Повреждение – это событие, заключающееся в нарушении исправного состояния объекта при сохранении его работоспособного состояния.

Отказ – это событие, заключающееся в нарушении работоспособного состояния системы.

Виды отказов

Ресурсный отказ – отказ, в результате которого объект достигает предельного состояния.

Независимый отказ (первичный отказ) – это отказ, не обусловленный другими отказами.

Зависимый отказ (вторичный отказ) – это отказ, обусловленный другими отказами.

Внезапный отказ – это отказ, характеризующийся скачкообразным изменением значений одного или нескольких параметров объекта.

Виды отказов

Постепенный отказ – это отказ, возникший в результате постепенного изменения значений одного или нескольких параметров объекта.

Сбой – это самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора.

Перемежающийся отказ – это многократно возникающий самоустраняющийся отказ одного и того же характера.

Явный отказ – отказ, обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования при подготовке объекта к применению или в процессе его применения по назначению.

Виды отказов

Скрытый отказ – отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый при проведении технического обслуживания или специальными методами диагностики.

Конструктивный отказ – отказ, возникший по причине, связанной с несовершенством или нарушением установленных правил и (или) норм проектирования и конструирования.

Виды отказов

Производственный отказ – отказ, возникший по причине, связанной с несовершенством или нарушением установленного процесса изготовления или ремонта, выполняемого на ремонтном предприятии.

Эксплуатационный отказ – отказ, возникший по причине, связанной с нарушением установленных правил и (или) условий эксплуатации.

Деградационный отказ – отказ, обусловленный естественными процессами старения, изнашивания, коррозии и усталости при соблюдении всех установленных правил и (или) норм проектирования, изготовления и эксплуатации.

Безотказность – свойство системы или элемента непрерывно сохранять работоспособность в течение некоторого времени или некоторой наработки.

Долговечность – свойство объекта сохранять работоспособное состояние до наступления предельного состояния при установленной системе технического обслуживания и ремонта.

Ремонтопригодность – свойство объекта, заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путём технического обслуживания и ремонта.

Надежность – свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования.

Надёжность является комплексным свойством, которое, в зависимости от назначения объекта и условий его применения, может включать безотказность, долговечность, ремонтопригодность или определённые сочетания этих свойств.

Например, для неремонтируемых объектов основным свойством является безотказность. Для ремонтируемых объектов одним из важнейших свойств, входящих в определение надёжности, может быть ремонтопригодность.

ПОКАЗАТЕЛИ НАДЕЖНОСТИ

Определение количественных характеристик или показателей надёжности необходимо для того, чтобы:

- учитывать надежность элементов и устройств при их применении в различных системах;
- формулировать требования по надежности к проектируемым устройствам или системам;
- сравнивать различные варианты построения системы;
- рассчитывать необходимый комплект запасных частей и принадлежностей (ЗИП) для восстановления систем, сроки их службы.

ПОКАЗАТЕЛИ НАДЕЖНОСТИ

Показатель надежности – это количественная характеристика одного или нескольких свойств, составляющих надежность объекта.

Различают единичные, комплексные, расчётные, экспериментальные, и эксплуатационные показатели надежности.

Единичный показатель надежности – это показатель надежности, характеризующий одно из свойств, составляющих надежность объекта.

Комплексный показатель надежности – это показатель надежности, характеризующий несколько свойств, составляющих надежность объекта.

Поскольку отказы элементов являются случайными событиями, то *теория вероятностей и математическая статистика* являются основным аппаратом, используемым при исследовании надежности, а сами характеристики надежности должны выбираться из числа показателей, принятых в теории вероятностей.

Все показатели надёжности могут определяться ***аналитически*** по формулам, полученным на основе теории вероятности, и по результатам испытаний или наблюдений, т. е. ***в виде статистических оценок*** показателей надежности, полученным на основе методов математической статистики.

Будем считать, что отказ объекта – это случайное событие.

Наработка (время) до отказа – непрерывная случайная величина X, распределенная в соответствии с некоторым распределением $F_X(t)$.

Функция $F_X(t)$ называется ***вероятностью отказа*** и представляет собой функцию распределения случайной величины:

$$F_X(t) = \Pr\{X \le t\}$$

Свойства: $F_X(0) = 0$;

$F_X(\infty) = 1$;

$F_X(t)$ не убывает на всей числовой прямой.

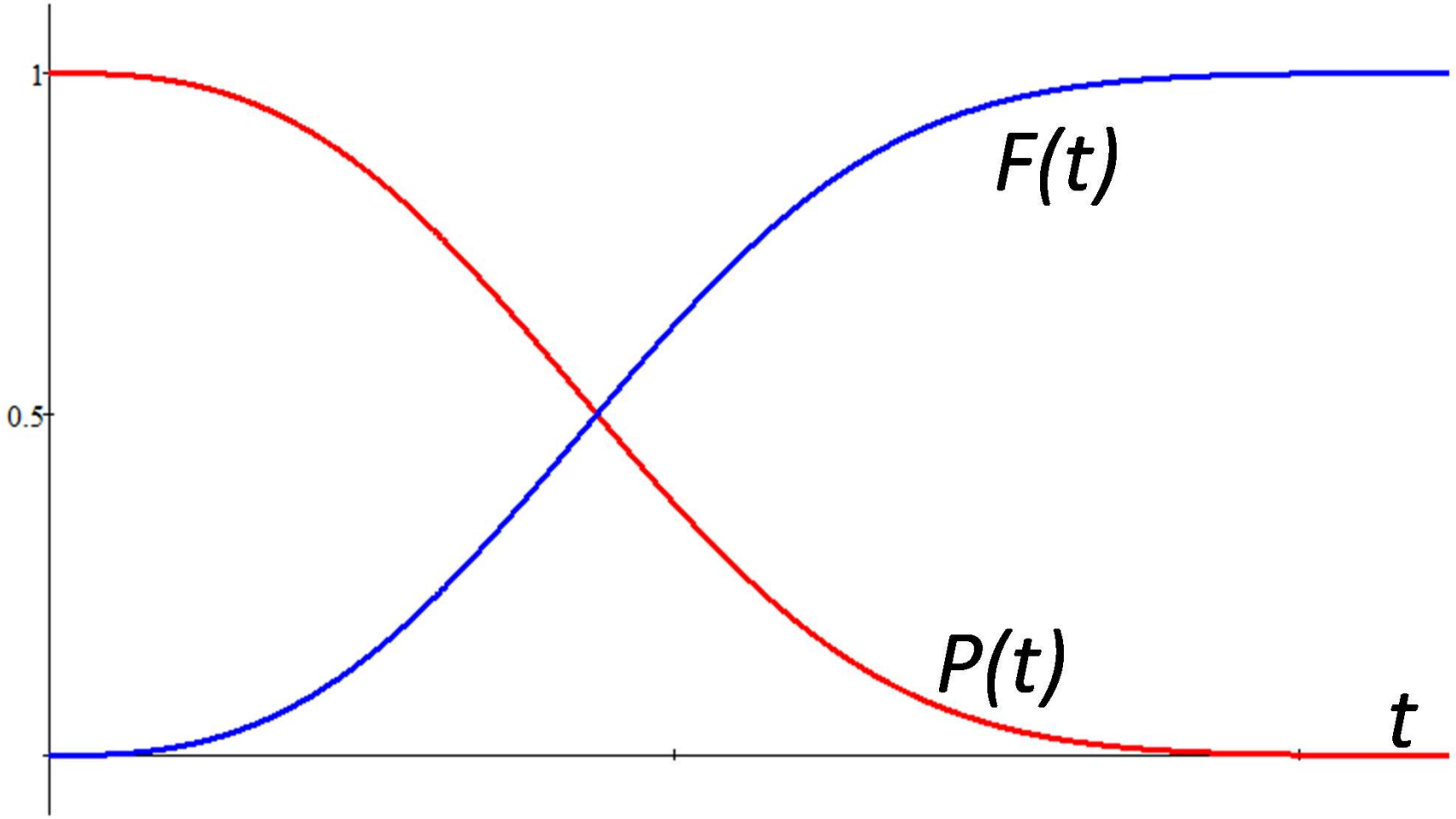
Вероятность безотказной работы – вероятность того, что в пределах заданной наработки на отказ (в заданном интервале времени $[0; t]$) отказ объекта не возникнет.

Вероятность безотказной работы дополняет вероятность отказа до 1:

$$F_X(t) = \Pr\{X \le t\} \qquad P(t) = \Pr\{X > t\}$$
$$F_X(t) + P(t) = 1$$

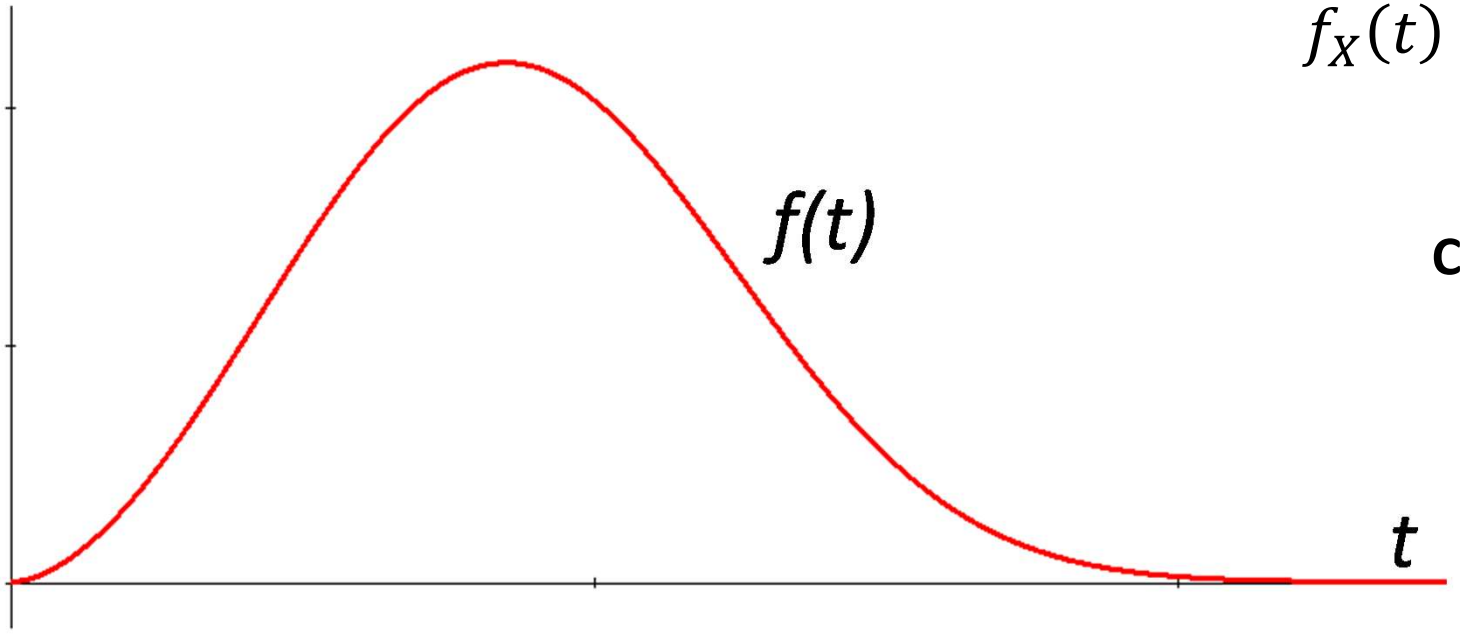
$P(t)$ - функция вероятности безотказной работы (функция ВБР).

Свойства: $P(0) = 1$;
$P(\infty) = 0$;
$P(t)$ не возрастает на всей числовой прямой.


1
0.5
F(t)
P(t)
t

Для непрерывной случайной величины с функцией распределения $F_X(t)$ можно определить функцию плотности распределения $f_X(t)$, которая в теории надежности называется *частотой отказов*.

$$f_X(t) = \frac{dF_X(t)}{dt} = -\frac{dP(t)}{dt}$$



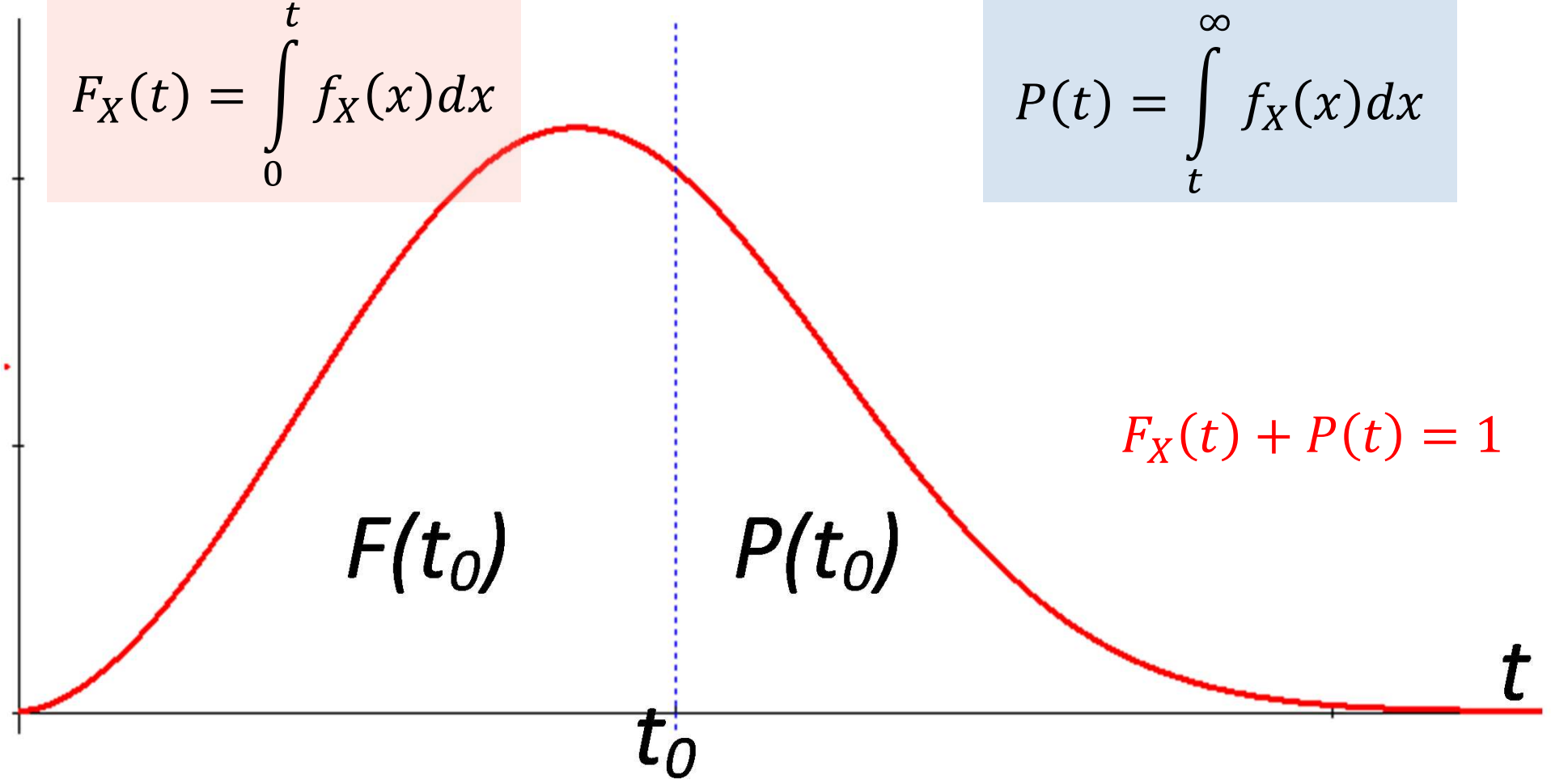
Свойства:

$$f_X(t) \geq 0;$$

$$\int_0^{\infty} f_X(t)dt = 1.$$

$$F_X(t) = \int_0^t f_X(x)dx$$

$$P(t) = \int_t^\infty f_X(x)dx$$



$$F_X(t) + P(t) = 1$$

Интенсивность отказов – это условная плотность распределения вероятности времени безотказной работы для момента времени t, при условии, что до момента времени t отказ объекта не произошел.

$$h(t) = \frac{f_X(t)}{P(t)}$$

Так как $\mathrm{P}(t) \leq 1$, то, очевидно, всегда выполняется соотношение

$$h(t) \geq f_X(t)$$

Функцию ВБР можно выразить через интенсивность отказов следующим образом:

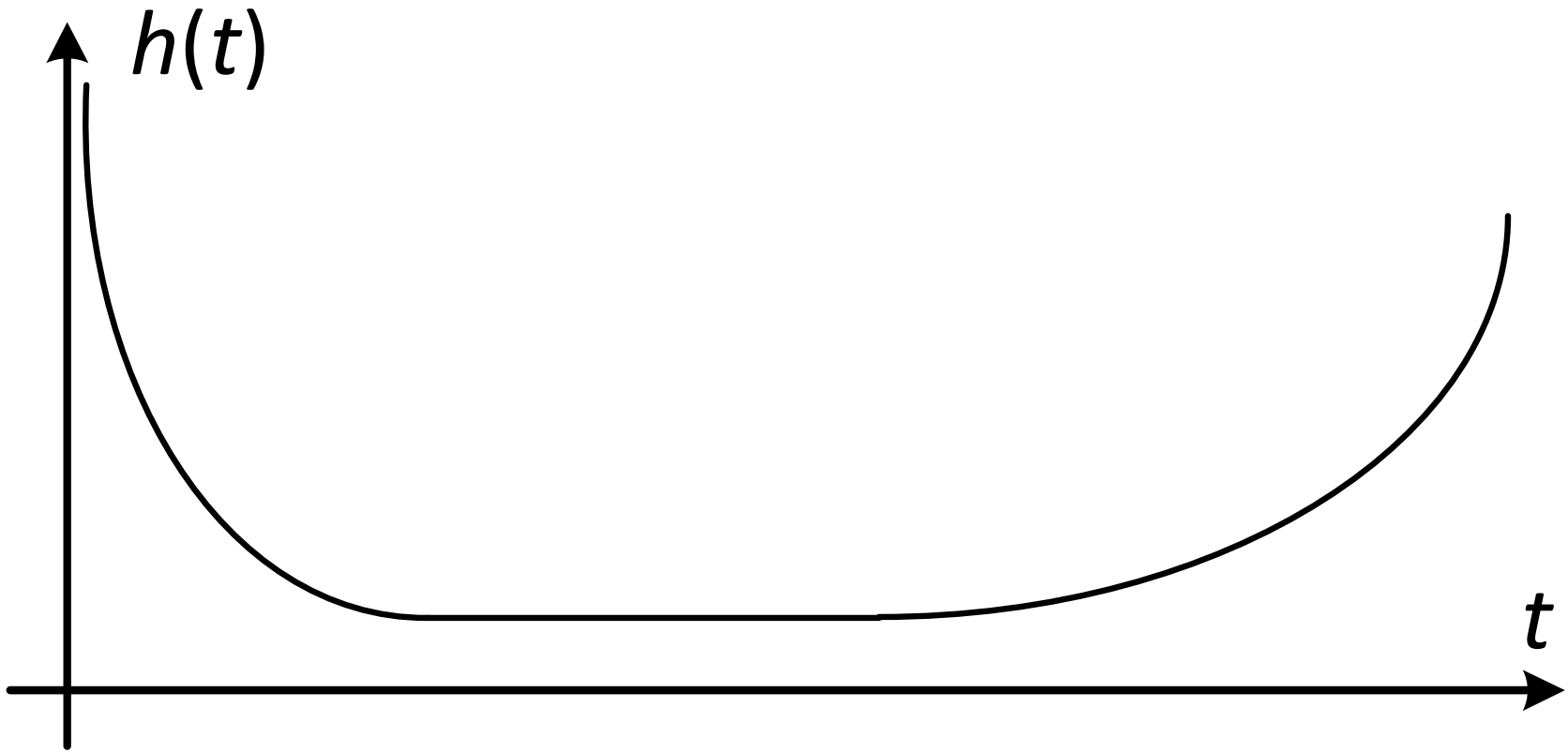
$$P(t) = e^{-\int_0^t h(x)dx}$$

Можно отметить различие между величинами $f_X(t)$ и $h(t)$.

Вероятность $f_X(t)dt$ характеризует вероятность отказа системы или элемента за интервал времени $(t, t + dt)$, взятых произвольным образом из группы таких же систем или элементов, причем *неизвестно, в каком состоянии (работоспособном или неработоспособном) находится элемент или система*.

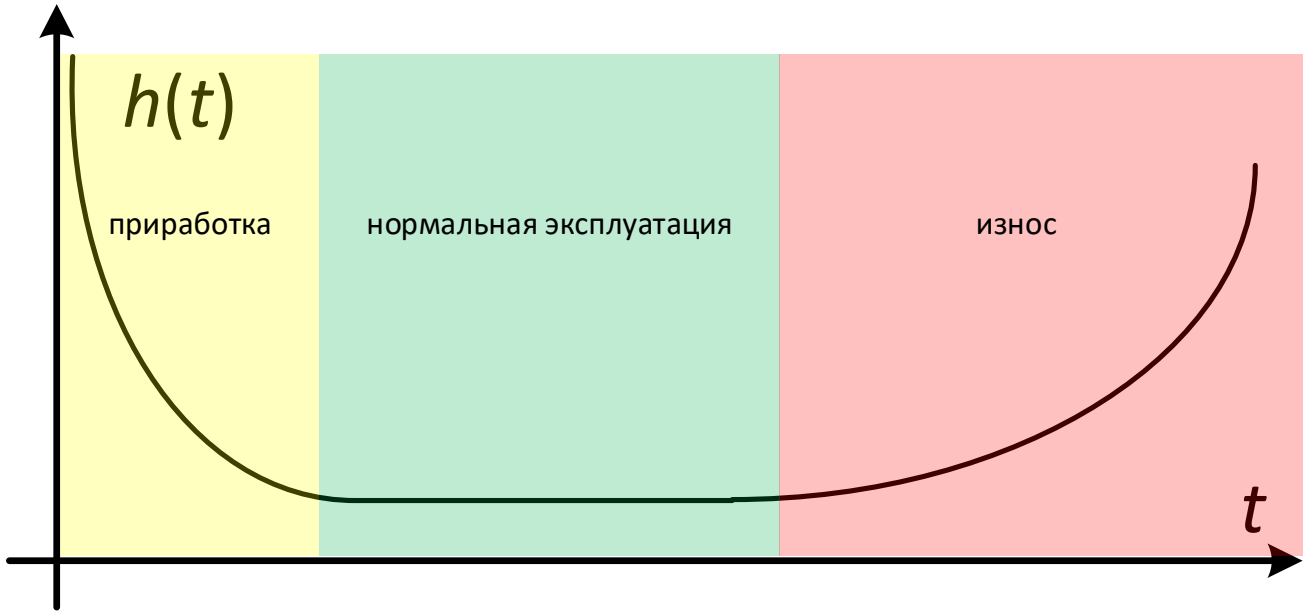
Вероятность $h(t)dt$ характеризует вероятность отказа системы или элемента за интервал $(t, t + dt)$, взятых из группы элементов или систем, *которые остались работоспособными к моменту времени* t.

Для большинства физических систем (в том числе технических) кривая интенсивности отказов выглядит как U-образная кривая:



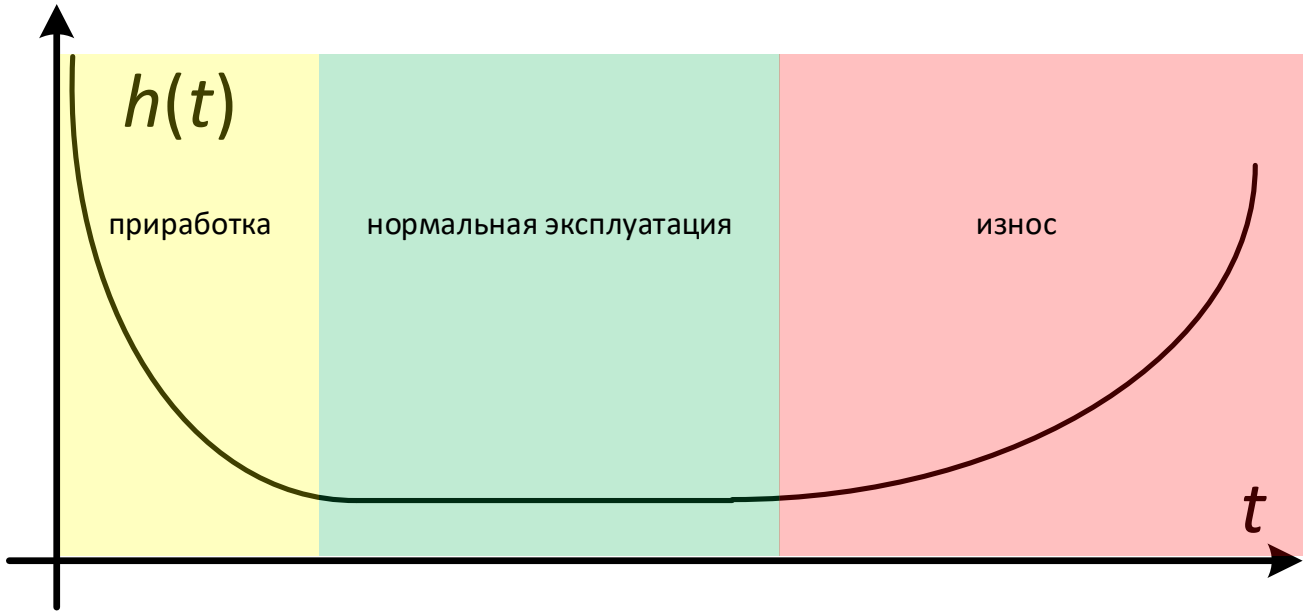
В соответствии с формой кривой интенсивности отказов можно выделить три периода жизненного цикла изделия:

- период приработки;
- период нормальной эксплуатации;
- период износа.



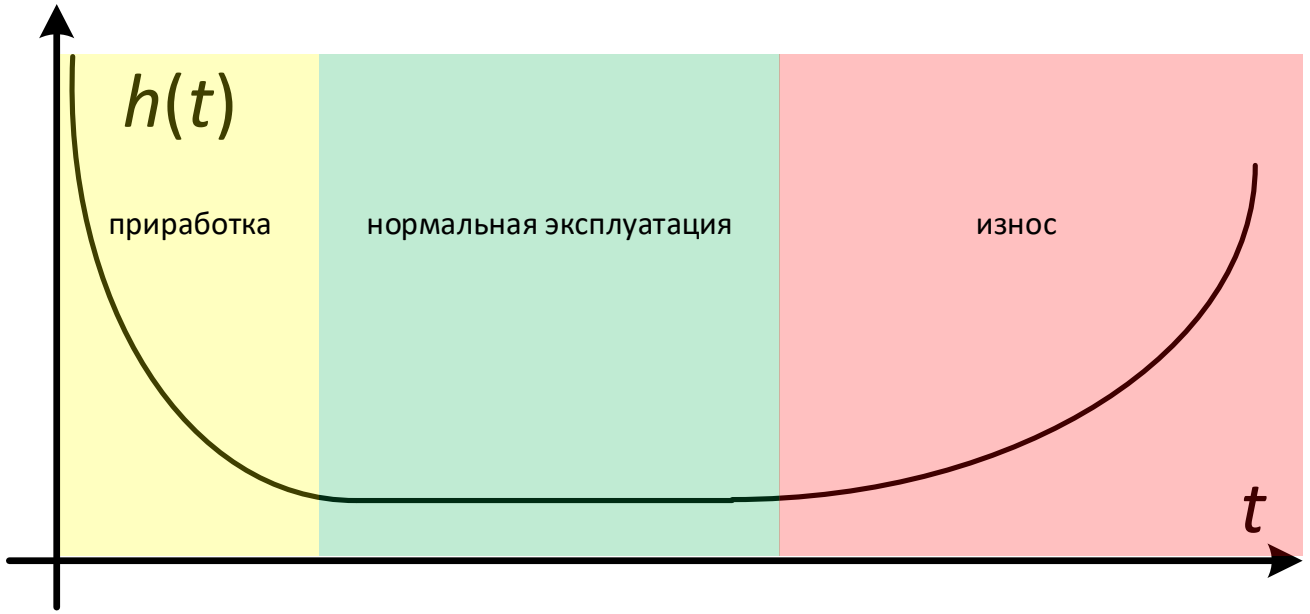
В период приработки интенсивность отказов *высока и уменьшается* с течением времени. На этом участке выявляются грубые дефекты производства объекта.

Для устройств и систем длительность этого участка составляет десятки, иногда сотни часов.



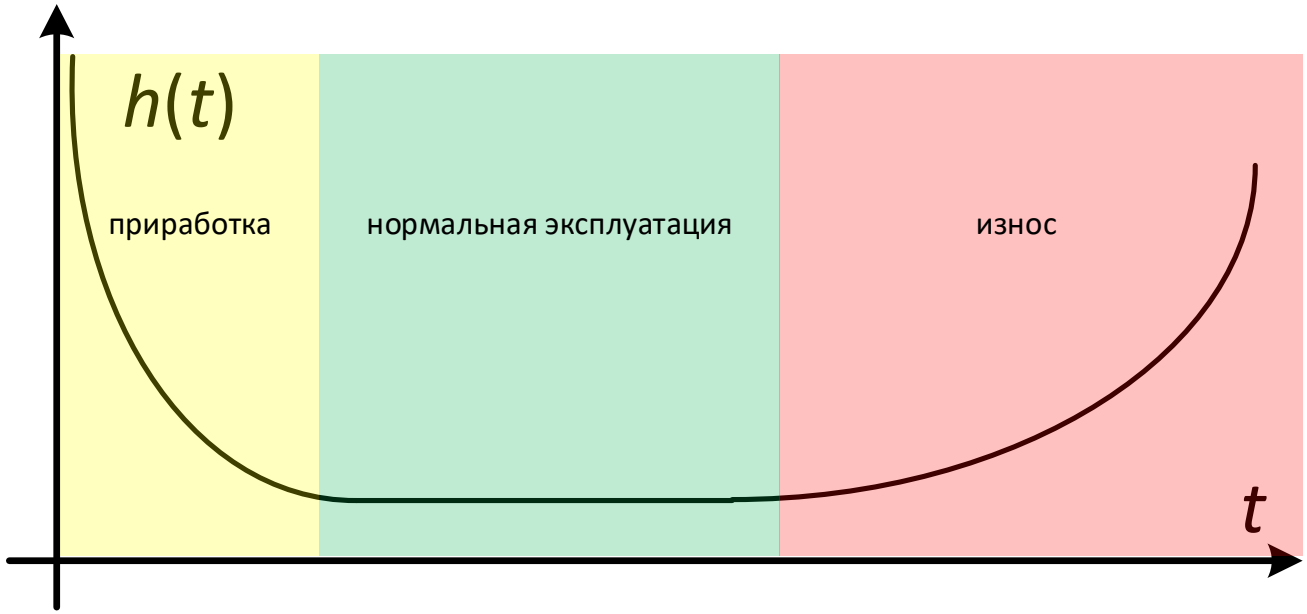
В период нормальной эксплуатации интенсивность отказов имеет *приблизительно постоянное значение*.

Длительность этого участка для современных элементов, устройств и систем составляет тысячи и десятки тысяч часов.



В период износа из-за усиления процессов старения элементов интенсивность отказов начинает *возрастать*.

Момент начала этого участка может служить временем, при достижении которого объекты должны сниматься с эксплуатации или ставиться на капитальный ремонт.



Математическое ожидание (среднее значение) непрерывной случайной величины X представляет собой ее первый начальный момент:

$$E[X] = \int_{-\infty}^{\infty} t f_X(t) dt$$

В теории надежности математическое ожидание времени до отказа (времени безотказной работы) называют средним временем безотказной работы (средней наработкой до отказа).

Учитывая, что $t > 0$,

$$T_{cp} = E[X] = \int_{0}^{\infty} t f_X(t) dt = \int_{0}^{\infty} P(t) dt$$

	$P(t)$	$F(t)$	$f(t)$	$h(t)$	T_{cp}
$P(t) =$		$1 - F(t)$	$\int_t^{\infty} f(t)dt$	$e^{-\int_0^t h(t)dt}$	
$F(t) =$	$1 - P(t)$		$\int_0^t f(t)dt$	$1 - e^{-\int_0^t h(t)dt}$	
$f(t) =$	$-P'(t)$	$F'(t)$		$-\left[e^{-\int_0^t h(t)dt}\right]'$	
$h(t) =$	$\frac{-P'(t)}{P(t)}$	$\frac{F'(t)}{1 - F(t)}$	$\frac{f(t)}{\int_t^{\infty} f(t)dt}$		
$T_{cp} =$	$\int_0^{\infty} P(t)dt$	$\int_0^{\infty} \big(1 - F(t)\big)dt$	$\int_0^{\infty} tf(t)dt$	$\int_0^{\infty} e^{-\int_0^t h(t)dt}d\tau$	

Статистические оценки показателей надежности

Вероятность отказа и ВБР:

$$\hat{F}_X(t) = \frac{n(t)}{N_0}; \qquad \hat{P}(t) = \frac{N_0 - n(t)}{N_0};$$

Частота отказов:

$$\hat{f}(t) = \frac{n(\Delta t)}{N_0 \cdot \Delta t};$$

где N_0 - число изделий, поставленных на испытание или на эксплуатацию;

$n(t)$ - число изделий, отказавших в течение времени t;

$n(\Delta t)$ - число отказавших изделий в интервале времени $\left(t - \frac{\Delta t}{2}; t + \frac{\Delta t}{2}\right]$;

Δt – ширина интервала.

Статистические оценки показателей надежности

Интенсивность отказов:

$$\hat{h}(t) = \frac{n(\Delta t)}{N_{cp} \cdot \Delta t};$$

Средняя наработка до отказа:

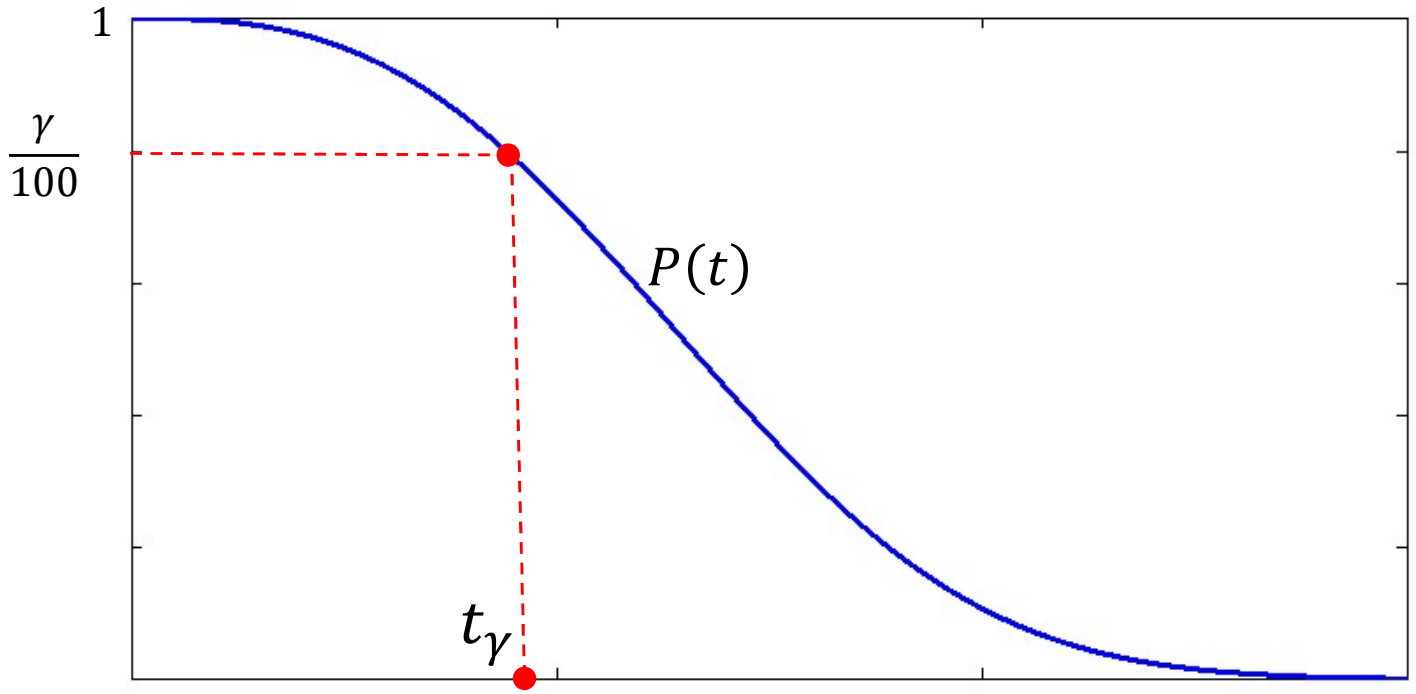
$$\hat{T}_{cp} = \frac{1}{N_0} \sum_{i=1}^{N_0} t_i ;$$

где $N_{cp} = \frac{1}{2}(N_a + N_b)$ - среднее число изделий, исправно работающих на интервале $(a; b]$;

t_i - время безотказной работы i-го изделия.

Гамма-процентная наработка до отказа – это наработка, в течении которой отказ объекта не возникнет с вероятностью γ, выраженной в процентах, то есть:

$$P(t_\gamma) = \frac{\gamma}{100}$$



Средняя остаточная наработка до отказа – это ожидаемая наработка до отказа, вычисленная для объекта, работоспособного в момент времени t.

$$\mu(t) = \frac{1}{P(t)} \int_t^\infty P(\tau) d\tau = -t + \frac{1}{P(t)} \int_t^\infty \tau \cdot f(\tau) d\tau$$

Вероятность отказа объекта на интервале $[t; t + \Delta t]$ при условии, что до момента времени t отказ не произошел, определяется как

$$F_{\Delta t}(t) = \frac{F(t + \Delta t) - F(t)}{1 - F(t)}.$$

Заметьте, что $F_\infty(t) = \frac{F(\infty) - F(t)}{1 - F(t)} = \frac{1 - F(t)}{1 - F(t)} = 1$.

Как следует из определений показателей надёжности для их расчёта необходимо знание закона или функции распределения ***времени безотказной работы объекта***, которое является случайной величиной.

Функция распределения времени безотказной работы объекта $F_X(t)$, определяющая вероятность отказа, может быть определена по статистическим данным, полученным при испытании или при наблюдении за объектом.

Однако, на стадии проектирования объектов таких статистических данных нет, поэтому, обычно, выдвигается и обосновывается гипотеза о функции распределения времени безотказной работы, которая затем должна проверяться после производства и в процессе эксплуатации объекта.

Время до отказа для элементов устройств или систем является непрерывной случайной величиной, которая характеризуется некоторым законом распределения.

Поскольку истинное распределение может быть неизвестно, для практических целей предполагается, что время до отказа распределено в соответствии с неким известным законом распределения, который используется в качестве **вероятностной модели надежности (ВМН)** объекта или системы.

В качестве ВМН можно использовать любое непрерывное распределение, для которого ***носителем*** является положительная числовая полуось:

$$supp(X) = [0; \infty)$$

В теории надежности часто используются следующие распределения (вероятностные модели надежности):

- экспоненциальное распределение;
- распределение Вейбулла;
- распределение Рэлея;
- логнормальное распределение.

Нормальное распределение (распределение Гаусса) используется реже; обычно в случаях, когда $F_X(0) \approx 0$.

Экспоненциальная модель надежности

$$F_X(t) = 1 - e^{-\lambda t}; \qquad f_X(t) = \lambda e^{-\lambda t};$$

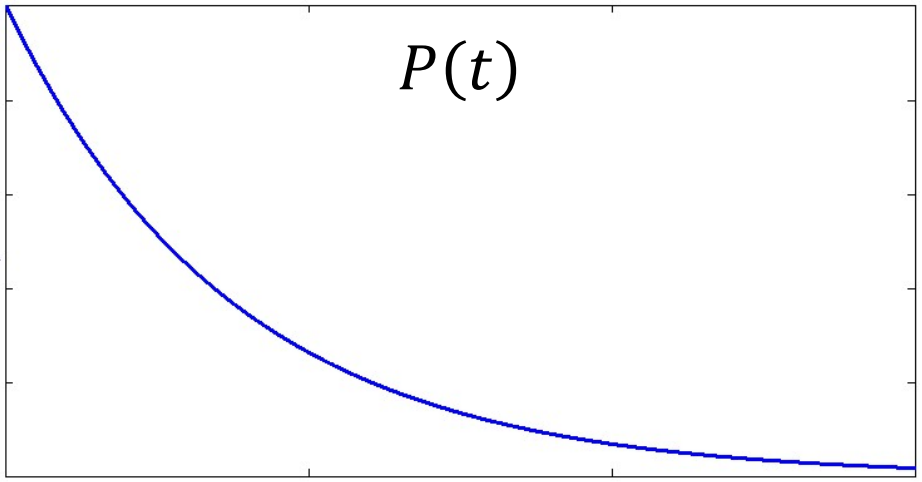
$$P(t) = 1 - F_X(t) = e^{-\lambda t};$$

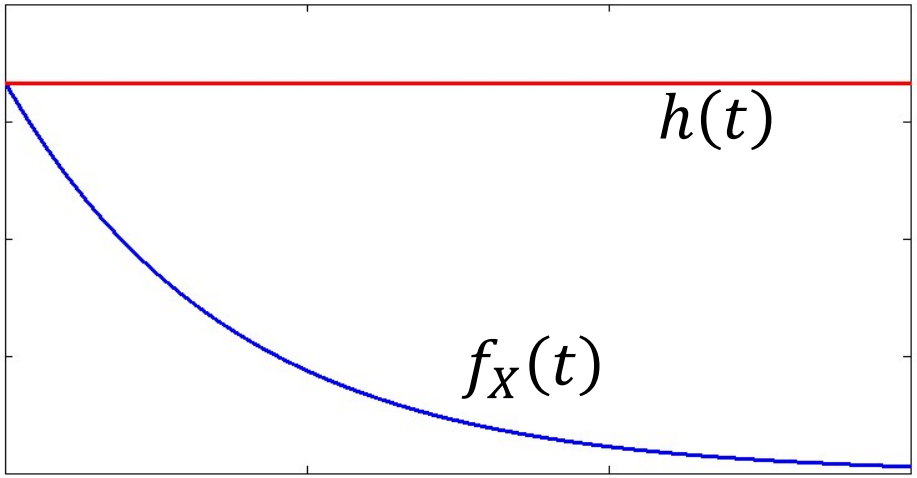
$$h(t) = \frac{f_X(t)}{P(t)} = \lambda = const.$$

$$T_{cp} = \int_0^\infty P(t)dt = \frac{1}{\lambda};$$

где $t \geq 0$, а $\lambda > 0$ – параметр распределения.

Экспоненциальная модель надежности





Экспоненциальная модель надежности

Недостатки:

- $h(t) = const$ означает, что экспоненциальная модель надежности не подходит для моделирования отказов в периодах приработки и износа. Более того, модель подразумевает, что объект не «стареет».

Достоинства:

- Простота расчетов;
- Многие современные электронные компоненты действительно могут демонстрировать постоянную интенсивность отказов в течении долгого времени.

Модель надежности Рэлея

$$F_X(t) = 1 - e^{-\frac{t^2}{2\sigma^2}}; \qquad f_X(t) = \frac{t}{\sigma^2} e^{-\frac{t^2}{2\sigma^2}};$$

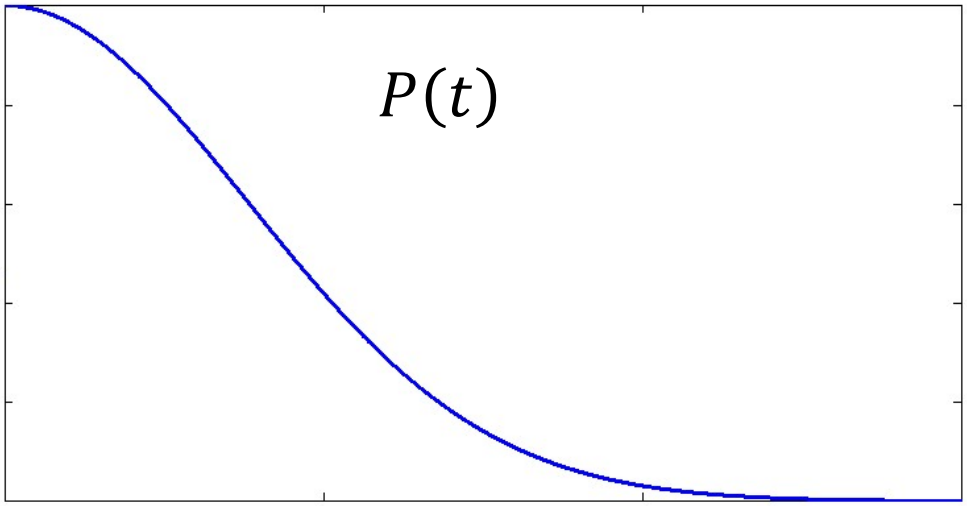
$$P(t) = 1 - F_X(t) = e^{-\frac{t^2}{2\sigma^2}};$$

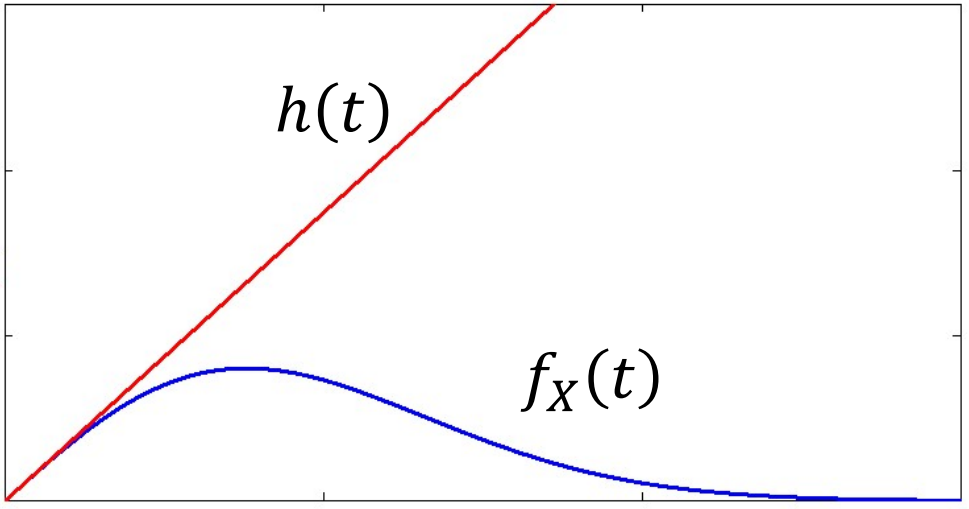
$$h(t) = \frac{f_X(t)}{P(t)} = \frac{t}{\sigma^2}.$$

$$T_{cp} = \int_0^\infty P(t)dt = \sqrt{\frac{\pi}{2}}\sigma;$$

где $t \geq 0$, а $\sigma > 0$ – параметр распределения.

Модель надежности Рэлея





Модель надежности Рэлея

Недостатки:

- Линейное возрастание интенсивности отказов означает, что модель надежности Рэлея не подходит для моделирования отказов в периоде приработки.

Достоинства:

- Относительная простота;
- Некоторые механические и электромеханические компоненты могут иметь возрастающую интенсивность отказов, сходную по форме с линейной зависимостью.

Модель надежности Вейбулла

$$F_X(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}}; \qquad f_X(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} \cdot e^{-\left(\frac{t}{\eta}\right)^{\beta}};$$

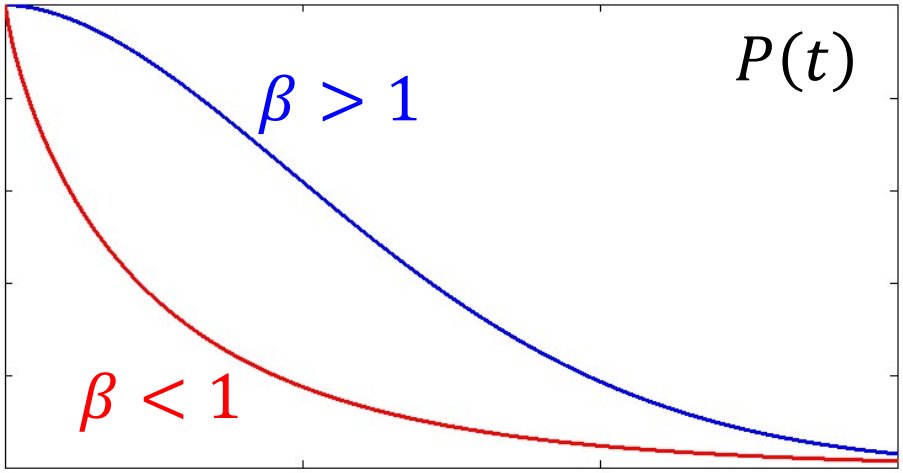
$$P(t) = 1 - F_X(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}}; \qquad h(t) = \frac{f_X(t)}{P(t)} = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta-1}.$$

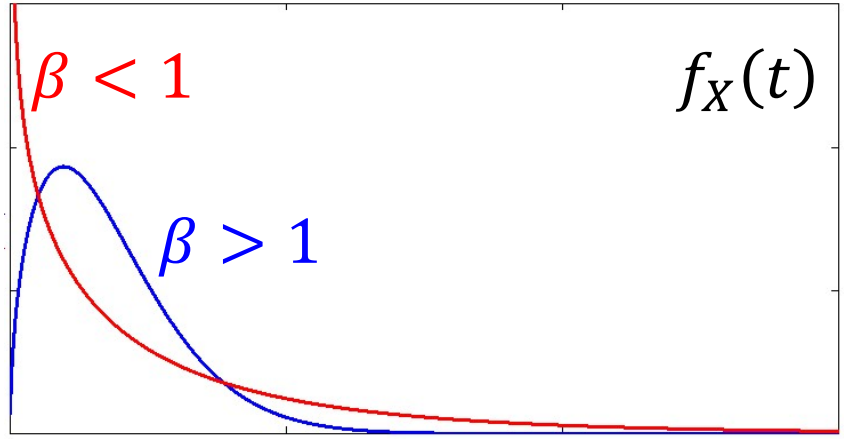
$$T_{cp} = \int_0^{\infty} P(t)dt = \eta \cdot \Gamma\left(1 + \frac{1}{\beta}\right);$$

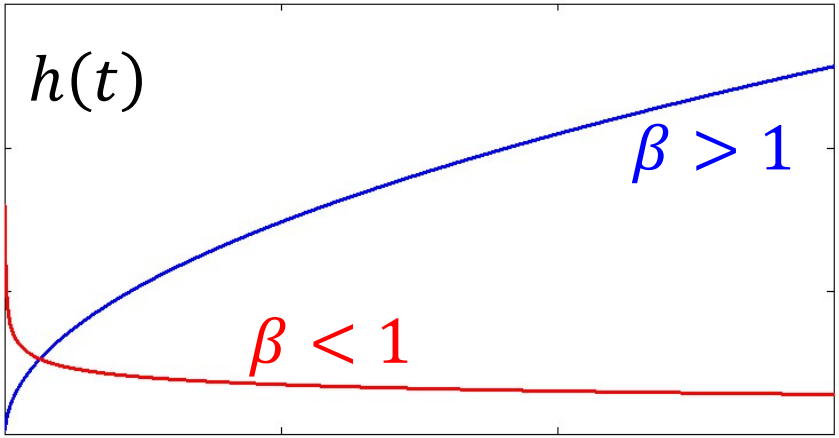
где $t \geq 0$, а$\beta, \eta > 0$ – параметры распределения;

$\Gamma(x)$ - гамма-функция.

Модель надежности Вейбулла







Модель надежности Вейбулла

Достоинства:

- Гибкость модели – возможность получать разные формы кривой интенсивности в зависимости от значения параметра β;
- Относительная простота.

Недостатки:

- Относительная сложность – при расчетах появляется необходимость рассчитывать значение гамма-функции.

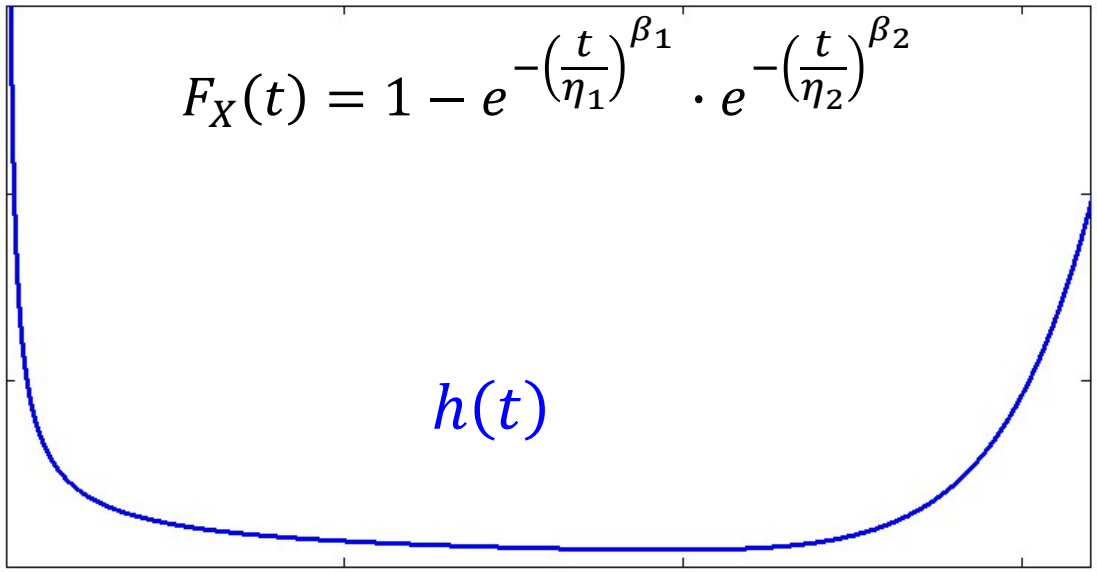
Модель надежности Вейбулла

Следует отметить, что экспоненциальное распределение и распределение Рэлея являются частными случаями распределения Вейбулла:

при $\beta = 1$: $F_X(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^1} = 1 - e^{-\frac{1}{\eta}t} = 1 - e^{-\lambda t}$ $\left(\frac{1}{\eta} = \lambda\right)$

при $\beta = 2$: $F_X(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^2} = 1 - e^{-\frac{t^2}{\eta^2}} = 1 - e^{-\frac{t^2}{2\sigma^2}}$ $(\eta^2 = 2\sigma^2)$

Формы кривой интенсивности отказов, близкие к U-образной кривой, возможно получить, если использовать в качестве вероятностной модели надежности более сложные распределения, с бóльшим числом параметров, в том числе различные комбинации простых распределений.



Недостатком такого подхода является повышение сложности модели, и следовательно, расчетов показателей надежности.