

# КОНВЕРГЕНТНЫЙ ПОДХОД В ОЦЕНКЕ ЭФФЕКТИВНОСТИ КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ИТ-ПОДРАЗДЕЛЕНИЯ

Худяков Д.С., Неизвестный С.И.

Финансовый университет при Правительстве Российской Федерации, Москва, Россия  
DSKhudyakov2021@edu.fa.ru, SINEizvestny@fa.ru

*Аннотация.* Конвергентные технологии начинают проявлять себя в качестве основных направлений развития, при этом многочисленные исследования подчеркивают потенциальные преимущества, связанные с внедрением этих технологий. Одним из главных преимуществ конвергентных технологий в управлении крупномасштабными информационными системами является повышение качества их планирования и управления.

*Ключевые слова:* конвергентный подход, эффективность ИТ, оценка эффективности.

## Введение

Радикальные изменения в образе жизни, порожденные развитием и масштабным распространением информационных технологий, привели к изменению парадигмы всего общества. Человеческая деятельность последних лет сопряжена с активной эксплуатацией информационных технологий, средств роботизации и автоматизации производства. Осуществляется генерация продуктов конвергенции, направленных на цифровую трансформацию бизнеса. Стремительный прогресс, невозможный без оперативного реагирования на постоянно трансформирующиеся турбулентные условия, требует решения новых проблем, главная из которых – конвергенция узкоспециализированных решений и средств информационных технологий с инструментами, применяемыми в других отраслях промышленности и сферах деятельности. Именно это явление поставлено во главу угла всех нынешних преобразований и инноваций.

Термины «Конвергентное мышление» и «Дивергентное мышление» были введены в 1956 году Дж. П. Гилфордом, американским психологом [1]. Данные термины не антонимичны друг другу, а представляют собой два противоположных конца одного спектра. Конвергентное мышление характеризует собой процесс поиска решения проблемы среди знакомых и конкретных вариантов. Напротив, дивергентное мышление предполагает нестандартный, творческий подход поиска решения, основанного на генерировании новых идей и оригинальных методик. Дивергентный подход помогает генерировать множество разнообразных концепций и вариантов действия. Конвергентный подход направлен на поиск лучшего решения, основанного на синергии объединения. В его основе – определение общих свойств систем разных типов и классов, а также их составных элементов. Технологии, базирующиеся на конвергентном подходе, могут быть весьма продуктивны для ИТ-подразделения, когда требуется выработка конкретных инструментов и методов [2, 3]. Ряд исследований подтверждает, что выработка гибких и адаптируемых решений по осуществлению и управлению цифровизацией бизнеса с использованием конвергентного подхода реальна и вполне может привести к положительным результатам [4-9]. Но, конечно, все зависит индивидуально. Каждый конкретный успешный случай зависит от контекста ситуации, в которой применялся конвергентный подход. Большую роль играет опыт руководства, а самое главное желание и умение эффективно внедрять новые методики, подходы и инструменты.

Важно понимать точное определение понятия «Конвергенция», т.к. в разных странах смысл данного термина имеет нюансы. При этом, данный термин не совсем точно отображает изменения в организации бизнеса, порожденные недавней ИТ-парадигмой. Даже учитывая, что в некоторых сферах экономики и промышленности конвергенция ИТ существует, а в некоторых нет, выстроить четкое понимание текущей ситуации достаточно трудно. Помимо этого, нынешние условия ведения бизнеса способствуют возникновению новой проблемы – конвергенции между технологиями и даже различными отраслями промышленности. Во многих сферах экономики резко выросло число требований, предъявляемых к конвергенции ИТ. Возникла потребность в алгоритме для выведения индекса конвергенции ИТ. Его задача – систематически и всесторонне отображать реальную ситуацию конвергенции ИТ между различными сферами и отраслями экономики, чтобы предоставить возможность объективного сравнения.

## 1. Конвергенция как одна из тенденций цифровизации

Современные тенденции применения конвергентного подхода в области цифровизации подразумевают анализ различных исследований и понимание самого понятия «Конвергенция» в

разных странах. Без этого вывести определение термина «Конвергенция ИТ», а также осуществить разработку системы индексации конвергенции ИТ невозможно. А без системы индексации невозможно объективно проанализировать степень конвергенции ИТ. Эмпирическим путем установлено, что результаты применения конвергентного подхода тесно взаимосвязаны с жизнью человека и его безопасностью. Результаты применения конвергенции оказывают существенное влияние на производственные отрасли промышленности, т.к. несут в себе более фундаментальные функции, к которым относятся: управление целеполаганием, управление стратегией, управление интеграцией, рост качества и объемов производства. Все это свидетельствует о продуктивности конвергенции ИТ не только в краткосрочной, тактической плоскости, но и в стратегической. Другими словами, осуществляется анализ глобальных трендов цифровизации и в первую очередь – конвергенции ИТ, пропорционально значимости процесса в отрасли [10-14].

Тенденции роста применения конвергентных технологий наблюдаются и в сфере искусственного интеллекта [15, 16], информационной и кибербезопасности, в формулировке и конкретизации задач для отделов ИТ и информационной безопасности, а также метриках, используемых для этих целей [17-20].

В целях оценки методологического применения конвергенции применяется уже упомянутый ранее индекс конвергенции. Он представляет собой скорость и порядок сходимости, что дает необходимые данные для применения итерационных подходов при реализации проекта объединения различных методов, инструментов и средств, направленных на создание конкретных процессов цифровизации. Высокий порядок сходимости означает, что потребуется меньшее число итераций для выведения и реализации результативного процесса цифровизации. Однако, по асимптотическому поведению последовательности нельзя со стопроцентной уверенностью судить о той или иной конечной части последовательности. Существует множество методов, позволяющих увеличить скорость сходимости последовательности конвергенции. Таким образом, появляется возможность преобразования исходной последовательности в аналогичную, но сходящуюся в тот же «предел» гораздо быстрее. Такие методы в общем известны, как «последовательное ускорение». Главной его целью является преобразование последовательности с целью снижения организационных, методических и прочих затрат и ресурсов.

## **2. Конвергентный подход при оценке эффективности крупномасштабных информационных систем**

Крупномасштабные информационные системы представляют собой сложные и трудноанализируемые структуры. Их эффективность определить достаточно сложно. Чем система крупнее, тем больше в ней элементов и взаимосвязей между ними. Больше объектов для анализа и больше вероятность ошибок. Какого-то универсального подхода для анализа эффективности ИТ вообще и крупномасштабных информационных систем в частности нет. В этом случае следует рассматривать информационные системы не как единое целое, а как совокупность элементов – ИТ-процессов. ИТ-процессы подойдут для этого лучше всего, так как информационные системы различны по своим программно-аппаратным, функциональным и структурным характеристикам. Требуется оценить эффективность ИТ-процессов, из которых состоит анализируемая крупномасштабная информационная система.

Анализ существующих подходов к оценке эффективности ИТ-процессов позволил установить, что конвергентные технологии наиболее применимы для высокоуровневой модели ИТ-процессов, предлагаемой сводом знаний COBIT 5 (Control Objectives for Information and Related Technology) [21]. Данный свод знаний представляет собой руководство по управлению информационными и смежными с ними технологиями. COBIT 5 является хорошим пособием для проведения аудита ИТ, так как содержит описание типовых целей и задач по управлению средствами ИТ, схемы и модели типовых ИТ-процессов. Главное, что есть в COBIT 5 – высокоуровневая модель эталонных ИТ-процессов. Всего составителями COBIT 5 выделено 37 ИТ-процессов.

Однако COBIT 5 не является стандартом. Выделенные 37 ИТ-процессов это модель идеального ИТ-отдела, оптимум, к которому надо стремиться. Но при этом помнить об индивидуальности каждого конкретного случая. Для конкретного ИТ-отдела реализация всех 37 ИТ-процессов может не иметь смысла и принести больше вреда, чем пользы. Руководство ИТ-отдела должно четко понимать, какие из 37 ИТ-процессов COBIT 5 действительно необходимы ИТ-отделу и бизнесу.

Помимо определения необходимых ИТ-процессов не менее значительна проблема четко выделить уже имеющиеся ИТ-процессы. В большинстве случаев ИТ-процесс, прописанный в COBIT, может существовать и давать конечный результат, но являться частью более крупного процесса, а не самостоятельным элементом. Это усложняет выделение входов и выходов ИТ-процесса, установку его

границ так, как того требует COBIT. Более того, стремление сделать все строго по COBIT может привести к сбоям в работе уже отлаженных процессов. На практике не всегда ИТ-процесс следует достаточно жёстко обособлять от других – это может оказать негативный эффект на конечный продукт ИТ-процесса. Именно поэтому эталонная модель COBIT 5 является не готовым решением по формированию структуры ИТ-отдела, а лишь шаблоном, базовой точкой, с которой следует начинать аналитику имеющихся ИТ-процессов.

В большинстве случаев процессную модель COBIT следует использовать для выделения и формализации собственных ИТ-процессов, которые будут коррелировать с ИТ-процессами COBIT. Один ИТ-процесс может включать в себя прямо или косвенно несколько ИТ-процессов COBIT. Например, условный процесс «Обеспечение бесперебойного функционирования информационных систем и технического оборудования» включает в себя элементы таких ИТ-процессов COBIT 5, как [22]:

- EDM03. Обеспечение оптимизации рисков;
- EDM04. Обеспечение оптимизации ресурсов;
- APO05. Управление портфелем инвестиций;
- APO06. Управление бюджетом и затратами;
- APO07. Управление персоналом;
- APO09. Управление соглашениями об услугах;
- APO10. Управление подрядчиками;
- APO11. Управление качеством;
- APO12. Управление рисками;
- BAI04. Управление доступностью и мощностью;
- BAI09. Управление активами.
- DSS01. Управление эксплуатацией;
- DSS02. Управление запросами на обслуживание и инцидентами;
- DSS03. Управление проблемами;
- DSS04. Управление непрерывностью.

Если брать все эти процессы в чистом виде оценка:

1. Затруднительна, т.к. ИТ-процессы не выражены в явном виде.
2. Длительна, т.к. потребуются вместо условного одного ИТ-процесса оценивать 10-15.
3. Некорректна, т.к. вместо одного реального будет осуществляться оценка нескольких косвенно существующих ИТ-процессов.

### **3. Оценка эффективности элементов крупномасштабных информационных систем**

Для оценки эффективности ИТ-процессов, как элементов крупномасштабной информационной системы, можно воспользоваться качественными или количественными методами. Однако, с точки зрения конвергенции, лучше всего для этой цели подойдет ГОСТ Р ИСО/МЭК 15504 [23, 24]. Данный стандарт рекомендован составителями COBIT 5, как наиболее структурированный инструмент для оценки эффективности.

Основной методики ГОСТ 15504 является утверждение, что каждый процесс имеет один из пяти уровней эффективности. Каждому уровню соответствует набор атрибутов с критериями для определения степени их выполнения. Уровень считается достигнутым, если все атрибуты на нем выполняются более чем на 50%. Источниками информации для определения критериев могут служить результаты ежегодно проводимого аудита, а также экспертное мнение работников, задействованных в оцениваемом ИТ-процессе.

Методика ГОСТ 15504 достаточно универсальна, но не лишена недостатков. Так, алгоритм расчета выполнения атрибута включает нормализацию входных данных по каждому критерию, суммирование значений и выведение среднего значения по атрибуту, путем расчета среднего арифметического. Такой подход не берет в расчет отрицательные эффекты от «недобора» или «перебора» при определении эффективности определенного критерия [25].

Для устранения данного явления требуется обратиться к теории систем и системного анализа, а конкретно к понятию диссенергии. Диссенергия подразумевает уменьшение эффективности системы при наличии негативной эмерджентности – системного эффекта – проявляющейся в отрицательном воздействии элементов системы друг на друга. Отрицательные воздействия при оценке эффективности определяются путем четкого определения оптимального значения, а также какой результат оценки будет недобором или перебором, относительно оптимального значения.

Необходимо сформировать три кортежа данных (во всех случаях  $i = 1, \dots, n$ , где  $n$  – количество рассматриваемых критериев):

- $A = \{Ai\}$  – нижний допустимый предел;
- $B = \{Bi\}$  – верхний допустимый предел;
- $V = \{Vi\}$  – значения, определяемые в процессе анализа критериев.

Далее необходимо провести расчет оценочных характеристик. Берется в расчет «полезная часть» оценки. Для этого частный коэффициент эффективности (PCEi) или нормализованная оценка критерия суммируется «как есть». После этого требуют проверки три условия:

1. Результаты оценки находятся в рамках оптимального интервала. В этом случае оценка считается оптимальной и частный критерий неэффективности учитываться не будет ( $PCi = 0$ ).

2. Результаты оценки выше верхнего допустимого предела ( $Vi > Bi$ ). В этом случае:

$$PCi = (Bi - Vi) * k, \quad (1)$$

где  $k$  – количество критериев, зависимых от рассматриваемого. Коэффициент считается зависимым, если коэффициент его корреляции относительно анализируемого критерия больше или равен 0,5.

3. Результаты оценки ниже нижнего допустимого предела ( $Vi < Ai$ ). В этом случае:

$$PCi = (Vi - Ai) * k. \quad (2)$$

Коэффициент  $k$  в данном случае позволяет распределить негативное влияние недобора (или перебора) оценки эффективности по всем критериям, зависимым от анализируемого. Таким образом, полученное отрицательное значение вычитается из оценок всех зависимых критериев [25].

Когда рассчитаны все оценочные характеристики для всех анализируемых критериев  $n$ , необходимо учесть их положительные и негативные эффекты. Для этого воспользуемся формулой (3):

$$EA = \frac{\sum_{i=1}^n (PCEi + PCi)}{n}, \quad (3)$$

где  $EA$  – оценка эффективности.

Таким образом, появляется возможность уточнить результаты оценки по ГОСТ 15504.

#### 4. Интерпретация результатов оценки эффективности ИТ-процессов

Оценив эффективность отдельных ИТ-процессов крупномасштабной информационной системы, нельзя говорить в целом о ее эффективности. Как уже было сказано выше, простое среднее арифметическое, полученное путем суммирования оценок ИТ-процессов и поделенное на их число, не может являться надежным результатом. Говорить об уровне эффективности всей системы, исходя из уровня наименее эффективных ее элементов еще более некорректно. Из ряда полученных оценок эффективности следует вывести интегральный показатель эффективности.

ИТ-процессы не равнозначны между собой по степени критичности и своему влиянию на эффективность информационной системы в целом. Единичный отказ одного ИТ-процесса станет для системы фатальным, а регулярные сбои в другом ИТ-процессе нет. Поэтому требуется проранжировать ИТ-процессы по степени критичности.

Введем понятие Инцидент. Под этим термином следует понимать сбой в работе процесса, отклонение от выполнения стандартного алгоритма действий. Для анализа Инцидентов используем подход FMEA (Failure Mode and Effects Analysis, анализ видов и последствий отказов). Его суть заключается в определении критических этапов процесса с целью управления качеством продукции. С точки зрения конвергенции, он идеально подходит, т.к. универсален и может использоваться для анализа любых процессов.

Подход FMEA описан в ГОСТ Р 27.303-2021 Надежность в технике. Анализ видов и последствий отказов [26]. FMEA позволяет рассчитать ранг приоритетности риска. Для этого необходимы три показателя:

- **Значимость** – степень катастрофичности последствий Инцидента для конечного продукта процесса. Оценивается от 1 (влияния нет), до 10 (запланированный результат невозможен);
- **Вероятность** – частота проявления Инцидентов и вероятность их повторения. Оценивается от 1 (нулевая вероятность) до 10 (вероятность более 10%);
- **Обнаружение** – уровень контролируемости Инцидентов, их своевременного обнаружения. Оценивается от 1 (гарантированное обнаружение) до 10 (обнаружение последует только после негативных последствий).

Расчёт ранга приоритетности риска (RPN) осуществляется по формуле (4):

$$RPN = S * O * D, \quad (4)$$

где S — Severity/Значимость,  
 O — Occurrence/Вероятность  
 D — Detection/Обнаружение

Теоретически, RPN может принимать значения на интервале от 0 до 1000, но показатель выше 125-130 уже свидетельствует о наличии высокой угрозы, исходящей от Инцидента.

Анализ требует разделения ИТ-процесса на подпроцессы, в рамках которого определяются возможные Инциденты и их потенциальные причины. Для каждого Инцидента определяются значимость, вероятность и обнаружение. После по формуле (4) рассчитывается RPN каждого Инцидента.

На этом метод FMEA оканчивается, но его можно продолжить и получить RPN для всего процесса [27]. Для расчета RPN процесса (RPN<sub>проц</sub>) из ряда значений ряда RPN Инцидентов (RPN<sub>инци</sub>) требуется ввести коэффициент значимости i-го Инцидента для каждого подпроцесса K<sub>i</sub>. При этом для каждого подпроцесса  $\sum K_i = 1$ . Расчет критичности подпроцесса будем вести по форме (5):

$$RPN_{\text{подпроц}} = \sum_{i=1}^m RPN_{\text{инци}_i} K_i, \quad (5)$$

где RPN<sub>подпроц</sub> – степень критичности подпроцесса,  
 RPN<sub>инци</sub> – степень критичности инцидента,  
 K – коэффициент значимости инцидента,  
 m – количество инцидентов для данного подпроцесса.

Затем аналогичным образом вводим коэффициент значимости j-го подпроцесса K<sub>j</sub> с тем же условием  $\sum K_i = 1$ . Далее по формуле (6) определяем степень критичности процесса в целом:

$$RPN_{\text{проц}} = \sum_{j=1}^n RPN_{\text{подпроц}_j} K_j, \quad (6)$$

где RPN<sub>проц</sub> – степень критичности процесса в целом,  
 RPN<sub>подпроц</sub> – степень критичности подпроцесса,  
 K – коэффициент значимости подпроцесса,  
 n – количество подпроцессов (этапов) для данного процесса.

Получившиеся значения для наглядности можно расположить на шкале RPN от 0 до 125 с шагом в 25 единиц. Эту шкалу можно рассматривать с двух позиций:

1. Шкала критичности, демонстрирующая, какие ИТ-процессы при наступлении Инцидентов будут нести больше негативных последствий, а какие меньше.

2. Шкала эффективности анализируемой крупномасштабной информационной системы, отображающая уровень ее общей эффективности. Для этого необходимо увязать результаты оценки степени критичности каждого процесса с оценкой их эффективности. Определим, что вероятность наступления Инцидентов в конкретном ИТ-процессе стремится к нулю, если эффективность данного ИТ-процесса составляет не менее 50% (то есть третий уровень эффективности по ГОСТ 15504). Если данному условию будут соответствовать все ИТ-процессы на том или ином отрезке шкалы степени критичности, то данный отрезок (уровень) считается безопасным. В таком случае данный уровень критичности можно рассматривать как уровень эффективности всей крупномасштабной информационной системы в целом.

## 5. Заключение

В настоящее время появилось много разнообразных методологий, средств, инструментов цифровизации, построения крупномасштабных информационных систем и платформ. Но единого подхода и универсальных инструментов, подходящих на все случаи, до сих пор не создано. Тем не менее, анализ имеющихся тенденций цифровизации демонстрирует высокую эффективность применения конвергентных технологий.

Проблема определения оптимального методологического инструментария в ИТ становится особенно актуальной в эпоху перехода к цифровому обществу. Примеры применения конвергентного подхода, предложенные в этой статье, позволяют гармонически сочетать лучшие методы и средства, как для грамотного построения крупномасштабных информационных систем, так и для управления ее отдельными элементами – ИТ-процессами.

Для более оперативной реализации процесса оценки эффективности крупномасштабных информационных систем необходимо синергетически объединять «классические» методы, инструменты с «гибкими», основываясь на конвергентном подходе. При этом должны адаптироваться наборы метрик оценки эффективности процессов цифровизации и средства конвергенции всех процедур, вовлеченных в данный процесс.

Как показано в данной работе, реализацией данных мер можно существенно повысить качество оценки эффективности крупномасштабных информационных систем, что в перспективе позволит повысить и качество их управления.

## Литература

1. Гилфорд Дж. Три стороны интеллекта // Психология мышления; под ред. А.М. Матюшкина. М.: Прогресс, 1965, 456 с.
2. Неизвестный С.И., Неизвестный Н.С., Шецуков М.А. Применение конвергентных технологий ИТ-подразделения в программах проектов высокой неопределенности целеполагания. Особенности процесса целеполагания // Управление проектами и программами. – М.: 2019. – № 4 (60). – С.290-299.
3. Неизвестный С.И. Конвергентные технологии развития методологий ИТ-подразделения проектами. М.– С.-Пб.: «Нестор-История», 2019, 352 с.
4. Yoo T., Chang H. The IT convergence framework design in the internet of things environment. EURASIP Journal on Wireless Communications and Networking volume 2013, No. 53. URL: <https://jwcn-urasipjournals.springeropen.com/articles/10.1186/1687-1499-2013-53> (дата обращения: 24.03.2023).
5. Kubiliusa K, Mishurab Y: The rate of convergence of Hurst index estimate for the stochastic differential equation // Stochastic Processes and their Applications. 2012, 122(11):3718-3739. DOI: 10.1016/j.spa.2012.06.011
6. Yeon S-J, Hwang S-h: A digital convergence maturity model: the relative importance of factors // Communications in Computer and Information Science. 2011, 264: 316-323. DOI: 10.1007/978-3-642-27210-3\_42
7. Kim Y, Kang J, Na Y, Chang H: Study on development of appraisal business performance indicator // Lecture Notes in Electrical Engineering. 2012, 164: 417-423. DOI: 10.1007/978-94-007-4516-2\_42
8. Jack SL, Anderson AR: The effects of embeddedness on the entrepreneurial process // Journal of Business Venturing. 2002, 17(5), 467-487. DOI: 10.1016/S0883-9026(01)00076-3
9. Shalaby M, El-Kassas S: Applying Scrum framework in the IT service support domain // Journal of Convergence. 2012, 3(1), 21-28.
10. Dowrick St., Bradford J.D. Globalization and Convergence. Globalization in Historical Perspective. USA: University of Chicago Press, 2003. URL: <http://www.nber.org/books/bord03> (дата обращения: 23.03.2023).
11. Халин В. Г., Чернова Г.В. Цифровизация и ее влияние на современную экономическую конвергенцию — методологический аспект // Управленческое консультирование. 2020. – № 8. – С. 78–87. DOI: 10.22394/1726-1139-2020-8-78-87
12. Кузнецова Н. П., Писаренко Ж.В., Чернова Г.В. Финансовая конвергенция как механизм повышения конкурентоспособности субъектов финансового рынка // Финансы и кредит. 2015. – № 46(670). – С. 10–23.
13. Чернова Г.В., Писаренко Ж.В., Кузнецова Н. П. Факторы, предпосылки и параметры финансовой конвергенции // Страховое дело. 2017. – № 3 (288). – С. 3–14.
14. Чернова Г.В., Халин В.Г., Калайда С.А. Бизнес-модель предпринимательской деятельности в условиях межсегментной экономической конвергенции // Экономика и предпринимательство. 2020. – № 5 (118). – С. 691—694.
15. Хель И. Искусственный интеллект плюс конвергенция: пять ожидаемых прорывов. Hi-News, 22/04/2019. URL: <https://hi-news.ru/research-development/iskusstvennyj-intellekt-plyus-konvergenciya-pyat-ozhidaemyx-proryvov.html> (дата обращения: 24.03.2023).
16. Внутских А.Ю., Железняк В.Н. Концепции конвергентных технологий и искусственного интеллекта: философские альтернативы // Вестник Вятского государственного университета. 2013. – № 4-1. – С.6-10.
17. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества. М.: Стандартинформ, 2006.
18. ГОСТ Р ИСО 19011:2011. Руководящие указания по проведению аудитов систем менеджмента. М.: Стандартинформ, 2013.
19. ISO/IEC 27000:2014. Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization, 2014. 31 p.
20. Лившиц И.И., Лонцих П.А. Формирование метрик для измерения результативности систем менеджмента информационной безопасности // Вестник ИрГТУ. – 2016. – № 5 (112). – С.65-72.
21. COBIT Process Assessment Model (PAM): Using COBIT 5, 2013. 144 p. ISBN 978-1-60420-264-9.
22. Худяков Д.С. Оценка эффективности ИТ-отдела и её влияние на разработку ИТ-стратегии // Самоуправление. 2022. – № 4 (132). – С.139-142.
23. ГОСТ Р ИСО / МЭК 15504-2—2009 «Информационные технологии. Оценка процессов. Часть 2. Проведение оценки».
24. ГОСТ Р ИСО / МЭК 15504-3—2009 «Информационные технологии. Оценка процессов. Часть 3. Руководство по проведению оценки».
25. Ханькин А.И., Яковлева С.С. Математическая модель оценки эффективности бизнес-процесса как один из методов системного анализа // Экономика и социум. 2016. №3(22). – С. 1981 -1983.
26. ГОСТ Р 27.303-2021 Надежность в технике. Анализ видов и последствий отказов
27. Новиков В.А., Гришин А.И. FMEA-анализ критичности процесса «Техническое обслуживание технологического оборудования»// Компетентность. 2012. № 6. – С. 37- 41.