

УДК 330.131.7:658.513:004.05

Д.А. Бахвалов, Е.Н. Савчик

ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», Красноярск, email: baherus@mail.ru, savchik_elena@mail.ru

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА ИТ-КОМПАНИИ НА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Ключевые слова: система менеджмента качества, риск, риск-ориентированный подход, методы риск-менеджмента, информационная безопасность.

В данной статье обоснована актуальность совершенствования системы менеджмента качества компании, предоставляющей услуги в области информационных технологий на основе риск-ориентированного подхода. Рассмотрены вопросы реализации риск-ориентированного подхода, включая практическое применение методов управления рисками на примере анализа процесса обеспечения работоспособности ИТ-оборудования одной из компаний, а также разработана методика оценки рисков информационной безопасности. Применение данных методов позволило разработать рекомендации по улучшению деятельности компании, как в области качества, так и безопасности информационных систем, используемых для обеспечения системы менеджмента качества.

D.A. Bakhvalov, E.N. Savchik

Reshetnev Siberian State University of Science and Technology, Krasnoyarsk territory, email: baherus@mail.ru, savchik_elena@mail.ru

IMPROVING THE IT COMPANY'S QUALITY MANAGEMENT SYSTEM BASED ON A RISK-BASED APPROACH

Keywords: quality management system, risk, risk-oriented approach, risk management methods, information security.

This article substantiates the relevance of improving the quality management system of a company providing information technology services based on a risk-based approach. The issues of implementing a risk-based approach, including the practical application of risk management methods on the example of analyzing the process of ensuring the operability of IT equipment of one of the companies, are considered, and a methodology for assessing information security risks is developed. The application of these methods allowed us to develop recommendations for improving the company's activities, both in the field of quality and security of information systems used to ensure a quality management system.

Мировой опыт показывает, что конкурентоспособность национальной экономики в целом связана с развитием информационных технологий. В настоящее время развитие большинства отраслей непосредственно связаны с внедрением информационных технологий. С каждым годом информационные технологии открывают все более широкие перспективы для повышения эффективности бизнеса и качества жизни граждан.

Цифровизация способствует минимизации человеческого фактора, автоматизирует рутинные процессы и помогает принимать важные управленческие решения на основе анализа больших данных. Можно утверждать, что информационные технологии являются ведущей сферой для развития любого бизнеса. Для решения многих проблем в компа-

нии внедряются информационные технологии, которые требуют специальных знаний и постоянного внимания. Рост числа ИТ-компаний объясняется растущим многообразием спроса на ИТ-услуги, а также сложностью используемых корпоративных ИТ-систем, которые требуют больших затрат на установку, интеграцию, а также обучение и обслуживание [1].

При этом необходимо отметить, что в связи с изменениями рыночных условий для организаций ИТ-отрасли возрастает неопределенность и неуверенность в достижении желаемых результатов, что приводит к возникновению рисков и непредвиденных потерь. С целью исключения данных ситуаций многие организации внедряют систему менеджмента качества, основу которой составляют

процессный и риск-ориентированный подходы. При внедрении системы менеджмента качества главной задачей является сделать так, чтобы система обеспечила слаженную работу и привела к безошибочному процессу оказания информационно-технологических услуг, тем самым способствуя повышению эффективности и качеству предоставляемых услуг, а также улучшению управляемости и контроля за процессами. Но чтобы система менеджмента качества оставалась эффективной и результативной необходимо ее постоянное совершенствование с учетом быстро меняющихся внешних и внутренних факторов, ключевыми из которых являются высокая конкуренция и завышенные требования потребителей. В таких условиях компании, которые не могут предложить своим клиентам качественные продукты или услуги, рискуют оказаться не конкурентоспособными.

Цель исследования

Целью данной работы является разработка рекомендаций по совершенствованию системы менеджмента качества компании, оказывающей услуги в области информационных технологий на основе применения методов риск-ориентированного подхода.

Материалы и методы исследования

При проведении данного исследования были рассмотрены научные труды российских и зарубежных ученых в области менеджмента качества и применения риск-ориентированного подхода, нормативно-законодательная база в данной области, а также аналитические материалы, предоставленные одной из компаний, оказывающей услуги в области информационных технологий. Авторами использованы как общенаучные, так и специальные исследовательские подходы и методы, в том числе: наблюдение; описание; системный, логический и статистический анализ; систематизация; метод экспертных оценок и др.

Результаты исследований и их обсуждение

Проведя анализ открытых источников рассматриваемых вопросов развития системы менеджмента качества в орга-

низации, нами определены следующие ключевые цели ее совершенствования:

- улучшение качества услуг, что приводит к удовлетворенности клиентов и повышению их лояльности;
- снижение затрат за счет выявления неэффективных процессов и их устранения;
- укрепление репутации, что способствует получению положительных отзывов от заказчиков;
- соблюдение стандартов, в том числе отраслевых, что может быть необходимо для работы с некоторыми заказчиками;
- улучшение производительности путем оптимизации бизнес-процессов, что способствует повышению эффективности работы и увеличению прибыли.

В целом, совершенствование системы менеджмента качества направлено на повышение конкурентоспособности компании с учетом как тенденций рынка информационных услуг, так и требований потребителей, что является первоочередным с точки зрения обеспечения качества.

На сегодняшний день любая ИТ-компания с целью улучшения системы менеджмента качества может реализовать следующие направления [2]:

- постоянно анализировать и улучшать процессы на основе современных методов управления качеством, в т.ч. риск-менеджмента, чтобы выявлять проблемы и недостатки в системе управления;
- проводить регулярные внутренние аудиты системы менеджмента качества для выявления проблем и недостатков;
- обучать персонал организации новым методам и технологиям управления качеством услуг;
- проводить опросы потребителей и получать обратную связь о качестве продукции или услуг;
- участвовать в отраслевых конференциях и семинарах для обмена опытом и получения новых знаний по управлению качеством;
- внедрять различные международные и национальные стандарты в области систем менеджмента, учитывающих отраслевую специфику.

Так, для компаний, оказывающих услуги в области информационных технологий, может быть актуальным

внедрение следующих нормативных документов [3]:

– ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Данный стандарт устанавливает требования к системе менеджмента информационной безопасности и помогает организациям разработать и реализовать политику безопасности информации.

– ГОСТ Р ИСО/МЭК 20000-1-2021 «Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов». Этот стандарт устанавливает требования к системе менеджмента сервисов и помогает организациям улучшить качество своих услуг, а также повысить удовлетворенность клиентов.

Кроме того, существуют множество и других нормативных документов, которые могут быть использованы с целью совершенствования системы менеджмента качества организации, оказывающей услуги в области информационных технологий. Некоторые из них устанавливают требования к качеству программного обеспечения, другие – к безопасности информации и защите персональных данных.

При этом, любая компания при внедрении нововведений и поддержании системы менеджмента качества в рабочем состоянии должна учитывать внешние и внутренние факторы, а также управлять рисками во избежание неблагоприятных для себя последствий. Поэтому, одним из направлений улучшения деятельности может быть ориентация на более детальное рассмотрение рисков и определения технологий их идентификации и оценки, т.е. внедрение риск-ориентированного подхода.

Для достижения стратегических целей, принятия оптимальных решений и повышения эффективности деятельности в области управления рисками компании могут использовать ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» [4], а также ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска» [5,6].

Реализация риск-ориентированного подхода может включать следующие элементы:

– Оценка рисков. Компания может проводить регулярную оценку рисков, связанных с ее деятельностью, чтобы определить потенциальные угрозы и возможности для улучшения.

– Разработка стратегии управления рисками. На основе результатов оценки рисков, компания может разработать стратегию управления рисками, которая поможет ей снизить вероятность возникновения проблем и минимизировать их последствия. Эта стратегия может включать в себя различные меры, такие как создание процедур безопасности данных, обучение персонала и т.д.

– Мониторинг и анализ. Компания может проводить регулярный мониторинг и анализ рисков, чтобы оценить эффективность своих мер по управлению рисками и внести корректировки при необходимости.

– Участие персонала. Компания может вовлекать свой персонал в процесс управления рисками, обучая их, как распознавать и предотвращать потенциальные угрозы. Например, она может проводить тренинги, чтобы повысить осведомленность персонала и снизить риск возникновения проблем.

– Сотрудничество с партнерами. Организация может сотрудничать с партнерами и поставщиками, чтобы убедиться, что они также принимают меры по управлению рисками.

В связи с тем, что для IT-компаний одним из ключевых факторов является работоспособность оборудования, то было принято решение рассмотреть различные методы управления рисками [5] и определить возможность их применения с целью анализа отказов оборудования в одной из компаний, оказывающих услуги в области информационных технологий.

Так, нами был применен метод «Анализ дерева отказов (FTA)» (рис. 1), который показал основные риски отключения серверного оборудования:

1) Отсутствует питание из-за отключения электроэнергии.

2) Недоступность сервера в локальной сети по причинам:

– высокая нагрузка на сервер;

– сбой сетевой карты;

– сбой работы маршрутизатора (отсутствует питание, ошибка компонентов, сбой программной части).

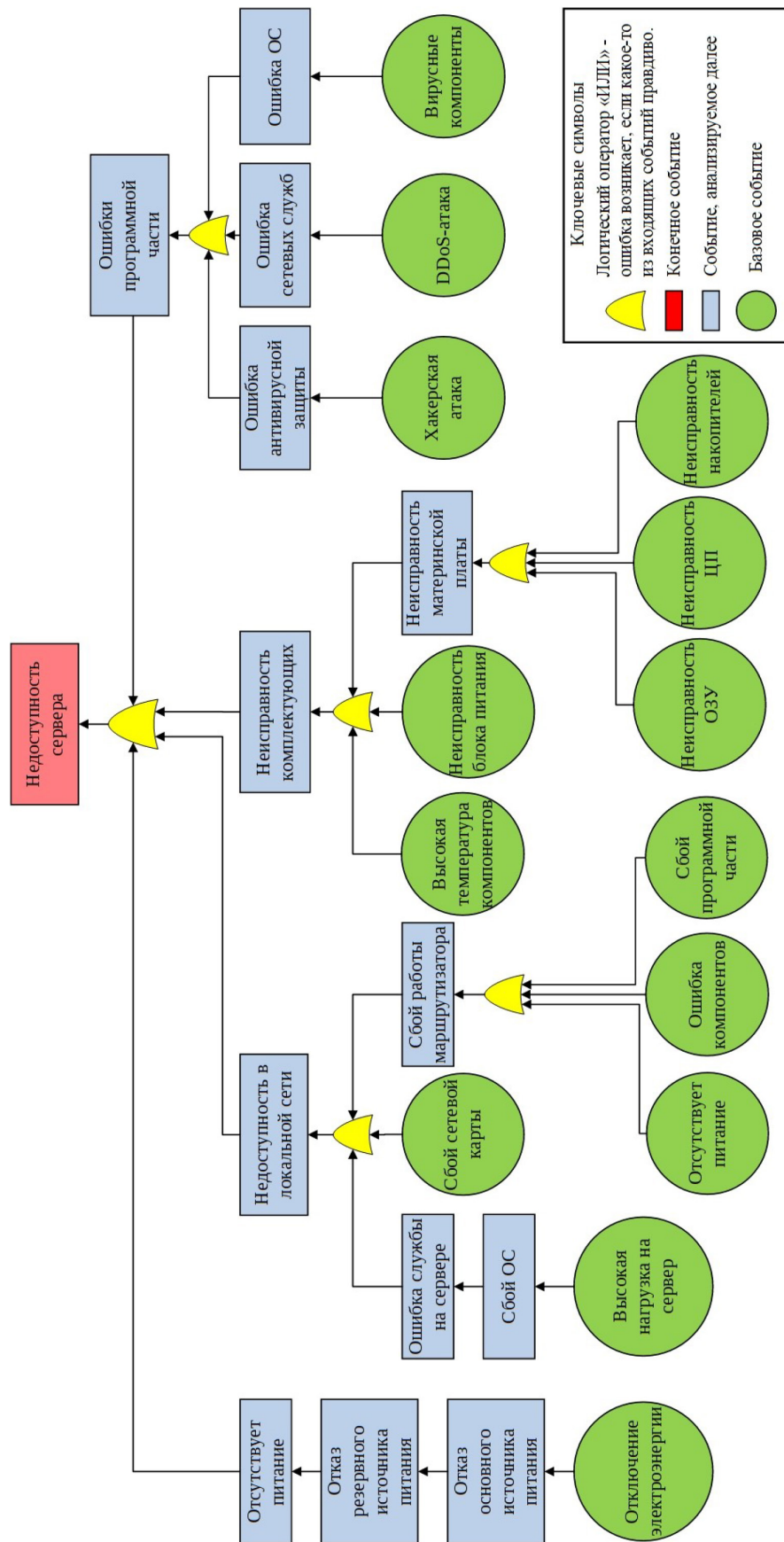


Рис. 1. FTA – анализ недоступности сервера

3) Неисправность комплектующих: высокая температура компонентов; неисправность блока питания; неисправность материнской платы (оперативной памяти, центрального процессора или накопителей).

4) Ошибка программного обеспечения на сервере:

- ошибка антивирусной защиты из-за хакерской атаки;
- ошибка сетевой службы из-за DDoS-атак;
- ошибка операционной системы из-за вирусного заражения сервера.

В связи с этим, было рекомендовано компании обратить внимание на выявленные риски при мониторинге серверного оборудования, а также выполнять периодическое обслуживание программных и аппаратных компонентов серверного оборудования.

В результате FTA-анализа также установлено, что для компании являются важными вопросы идентификации и оценки рисков, связанных с информационной безопасностью, поэтому нами разработана соответствующая методика.

При этом методика по оценке рисков информационной безопасности является необходимым инструментом для эффективного управления безопасностью информации в любой компании. Без такой методики невозможно оценить уровень рисков и принять необходимые меры для защиты информации.

Основная задача методики – обеспечение прозрачности и объективности при оценке рисков. Она позволяет получить четкое представление о том, какие угрозы существуют, каковы вероятности их возникновения и какой ущерб может быть нанесен компании. Это позволяет принимать взвешенные решения по управлению рисками и выбирать оптимальные меры безопасности.

Методика также помогает определить наиболее уязвимые места в системе, что позволяет сосредоточить усилия на защите именно этих участков. Она также позволяет определить эффективность принятых мер по уменьшению рисков, что дает возможность корректировать стратегию безопасности в соответствии с изменением условий.

Для понимания возникновения рисков информационной безопасности создаем рабочую группу, в которую входят:

- начальник отдела информационных технологий;
- руководители сервисных центров;
- специалист службы информационной безопасности;
- инициативные сотрудники сервисного центра.

При оценке рисков информационной безопасности рабочая группа определила показатели и по результатам работы была собрана статистика защищенности устройств и определено количество сотрудников, которые предупреждают возникновение рисков информационной безопасности (табл. 1).

Таблица 1

Статистика информационной защищенности организации

Наименование показателя статистики	Текущий показатель	Необходимый показатель
Установленных лицензий антивирусного программного обеспечения	8956	9996
Успешно отраженных компьютерных атак	43	45
Количество специалистов, подготовленных по образовательным программам в области ИБ	12	15
Уровень соответствия паролей сотрудников стандартам безопасности	15224	16250
Количество защищенных устройств сети компании	821	955

Для расчета безопасности компании произведем расчет пяти показателей:

1) Соотношение количества установленных лицензий антивирусного программного обеспечения к общему количеству рабочих мест сотрудников компании определяется по формуле (1):

$$P_1 = \frac{W_1}{W_s} = \frac{8956}{9996} = 0,86. \quad (1)$$

где P_1 – соотношение количества установленных лицензий антивирусного программного обеспечения к общему количеству рабочих мест сотрудников компании, пункты;

W_1 – количество установленных лицензий антивирусного программного обеспечения, единиц;

W_s – общее количество рабочих мест сотрудников, единиц.

2) Соответствие количества успешно отраженных компьютерных атак к общему количеству компьютерных атак определяется по формуле (2):

$$P_2 = \frac{A_s}{A_q} = \frac{43}{45} = 0,96. \quad (2)$$

где P_2 – уровень соответствия количества успешно отраженных компьютерных атак к общему количеству компьютерных атак, пункты;

A_s – количество успешно отраженных компьютерных атак, единиц;

A_q – общее количество компьютерных атак, единиц.

3) Анализ численности специалистов, подготовленных по образовательным программам в области информационной безопасности, осуществляется по формуле (3):

$$P_3 = \frac{S_f}{S_p} = \frac{12}{15} = 0,8. \quad (3)$$

где P_3 – соотношение количества фактически подготовленных специалистов по образовательным программам в области информационной безопасности, с плановым количеством подготовленных специалистов, пункты;

S_f – количество фактически подготовленных специалистов по образовательным программам в области информационной безопасности, единиц;

S_p – количество подготовленных специалистов по образовательным программам в области информационной безопасности по плану, единиц.

4) Уровень соответствия паролей сотрудников компании стандартам информационной безопасности организации, осуществляется по формуле (4):

$$P_4 = \frac{P_s}{P_q} = \frac{15224}{16250} = 0,93. \quad (4)$$

где P_4 – соотношение количества сотрудников компании, пароли которых соответствуют стандартам информационной безопасности к общему количеству сотрудников организации, пункты;

P_s – количество сотрудников компании, пароли которых соответствуют стандартам информационной безопасности, единиц;

P_q – общее количество сотрудников компании, единиц.

5) Оценка защищенности сети компании определяется по формуле (5):

$$P_5 = \frac{N_s}{N_q} = \frac{821}{955} = 0,86. \quad (5)$$

где P_5 – соотношение количества настроенных сегментов сети к их общему количеству, пункты;

N_s – количество настроенных сегментов сети, единиц;

N_q – общее количество сегментов сети, единиц.

Количественная интегральная оценка эффективности управления рисками информационной безопасности рассчитывается как сумма пяти вышеуказанных критериев, по формуле (6):

$$I = P_1 + P_2 + P_3 + P_4 + P_5 = 0,86 + 0,96 + 0,8 + 0,93 + 0,86 = 4,41. \quad (6)$$

Управление рисками признается высокоэффективным при получении значения интегральной оценки (I) от 4,5 до 5 баллов, эффективным – от 4 до 4,4 баллов, низкоэффективным при получении менее 4 баллов.

По результатам анализа информационной безопасности объекта исследования было получено значение равное 4,41 баллов, что говорит об эффективной работе в области риск-менеджмента. Но также стоит отметить, что компании есть куда развиваться. Основные проблемы выявлены в результате анализа численности специалистов информационной безопасности и при оценке защищенности сети организации.

Кроме того, установлено, что основные риски при работе с оборудованием связаны также с процессом «Настройка оборудования удаленного рабочего места». Поэтому, необходимо идентифицировать и выполнить оценку уровня рисков данного процесса. Для этого были определены факторы (тяжесть последствий и вероятности возникновения) и проведена их оценка по шкале от 1 до 3 (табл. 2).

Таблица 2

Оценка уровня рисков процесса «Настройка оборудования удаленного рабочего места»

Риск	Тяжесть последствий	Вероятность возникновения	Уровень риска
Неисправен монитор	1	1	1
Неисправна периферия	1	3	3
Неисправность маршрутизатора	3	1	3
Неисправность кабеля – удар электрическим током	3	1	3
Возгорание блока питания	3	1	3
Неисправность чипсета	2	3	6
Ошибка при вводе пароля	1	1	1
Установка по PXE не запускается из-за недоступности SCCM	3	1	3
Доменное имя создано в некорректном каталоге AD	3	1	3
Выбрана неправильная сборка ОС	1	1	3
Ошибка при указании доменного имени	1	3	3
Запуск ОС не выполняется из-за недоступного драйвера на чипсет оборудования	3	1	3
Неисправный накопитель (HDD или SSD) на ПК	3	2	6
Установлено не разрешенное ПО	3	3	9
Установочный файл не запускается	1	1	1
Не доступен сервер для активации специального ПО	3	2	6
Устаревший установочный файл для установки ПО	1	1	1
Риск вирусного заражения при установке специализированного ПО	3	2	6
Установлено старое антивирусное ПО	3	1	3
Отсутствует модуль TPM на ПК	3	1	3
Неконкретно настроена служба шифрования данных	3	1	3
Не удастся расшифровать накопитель информации	3	2	6
Шкала оценки			
Тяжесть последствий, балл	Незначительная (1)	Умеренно значимая (2)	Серьезная (3)
Вероятность возникновения, балл	Маловероятно (1)	Вероятно (2)	Высокая вероятность (3)
Уровень риска, балл	Приемлемый (1,2)	Оправданный (3,4)	Недопустимый (6,8,9)

В результате оценки были выявлены недопустимые риски процесса и с целью уменьшения их влияния на процесс были предложены рекомендации по предотвращению:

1) Для предотвращения риска «Установлено неразрешенное ПО» рекомендуется выполнять мониторинг установленного программного обеспечения и стандартизировать приобретение нового.

2) Чтобы избежать риска «Неисправность чипсета на материнской плате», рекомендуется выполнять закупку оборудования у проверенных поставщиков.

3) Чтобы свести к минимуму частоту появления риска «Неисправный накопитель (HDD или SSD) на ПК» необходимо проводить мониторинг работы накопителей, а впоследствии нахождения ошибок проводить плановую замену оборудования.

4) Для недопущения риска «Не доступен сервер для активации специального ПО» рекомендуется назначить ответственного за мониторинг доступности сервера специального программного обеспечения.

5) Для уменьшения влияния риска «Вирусное заражение при установке специализированного ПО» необходимо создать облачную песочницу для проверки запускаемых пакетов.

6) Для уменьшения влияния риска «Не удастся расшифровать накопитель информации» на процесс необходимо выполнить синхронизацию серверов шифрования данных и настроить репликации с общего репозитория для хранения ключей.

Все эти рекомендации помогут снизить влияния рисков на процесс и улучшить качество оказания услуг.

Выводы

Предлагаемые методы идентификации и оценки рисков могут применяться различными компаниями, оказывающими услуги в области информационных технологий при совершенствовании процессов системы менеджмента качества. А учитывая активное развитие технологий в данной сфере, можно сказать, что внедрение риск-ориентированного подхода будет не только мерой для поддержания стабильности в организации, но и отправной точкой для развития индустрии в целом. Также, необходимо отметить, что внедрение риск-ориентированного подхода в деятельность компании любой сферы экономической деятельности – это действенный инструмент повышения эффективности и обеспечения устойчивого положения на рынке.

Библиографический список

1. Махницкий Д.П. Общий центр обслуживания как инструмент повышения эффективности работы федеральных органов исполнительной власти Российской Федерации // Государственное и муниципальное управление. 2018. № 1. С. 111-115.
2. Бгашев М.В., Хамид К.А. Проблемы вовлечения персонала в процессе совершенствования системы менеджмента качества промышленных предприятий // Промышленность: экономика, управление, технологии. 2021. № 4. С. 22-28.
3. Логинова А.О. Обзор нормативно-правовых источников и практик управления инцидентами информационной безопасности // Вестник СибГУТИ. 2021. № 1. С. 50-59.
4. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство = Risk management. Principles and guidelines: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 10 декабря 2019 г. N 1379-ст: дата введения 2020-03-01/ подготовлен некоммерческим партнерством «Русское Общество Управления Рисками» (НП «РусРиск»), 2019. [Электронный ресурс]. URL: <https://docs.cntd.ru/doc-ument/1200170125> (дата обращения 20.12.2023).
5. ГОСТ Р 58771-2019. Менеджмент риска. Технологии оценки риска: Risk management. Risk assessment technologies: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию

и метрологии от 17 декабря 2019 г. N 1405-ст: дата введения 2020-03-01/ разработан некоммерческим партнерством «Русское Общество Управления Рисками» (НП «РусРиск»), 2020. [Электронный ресурс]. URL: <https://docs.cntd.ru/document/1200170253> (дата обращения 20.12.2023).

6. Бахвалов Д.А., Савчик Е.Н. Риск-ориентированный подход в системе менеджмента качества IT-компаний // Актуальные проблемы авиации и космонавтики: сб. материалов IX Междунар. науч.-практ. конф., посвящ. Дню космонавтики (10–14 апреля 2023 г., Красноярск): в 3 т. Т. 2. Красноярск, 2023. С. 1089-1091.