Конкурентоспособные услуги на основе новейших международных стандартов

Принято считать XX век веком индустрии, а XXI век – веком услуг и информационных технологий. Это, прежде всего, связано с революционными изменениями в методах деятельности – в переходе от медленных процессов обработки информации к компьютерам и Интернету. В наше время колоссальный объем информации можно уместить на небольших портативных устройствах, а многоядерные микропроцессоры способны обработать такой ранее немыслимый информационный поток, как видео в формате высокого разрешения. А мобильная связь стала повсеместна и общедоступна даже для малообеспеченных слоев общества. С другой стороны, произошло перенасыщение мировых рынков материальными товарами, но одновременно открылись колоссальные возможности в области услуг. Особенно это касается услуг в области информационных технологий, где рынок продолжает расти. Но, к сожалению, качество и своевременность услуг улучшается не так быстро, как хотелось бы. Если качество материальных товаров проверяется достаточно легко и точно, то качество услуг проверить очень сложно или поздно, когда уже трудно что-либо исправить. Наиболее действенный инструмент – это выбор надежных и зарекомендовавших себя поставщиков услуг. В качестве критерия все чаще используют такой инструмент, как сертификация на соответствие международным стандартам. Для информационных технологий это прежде всего стандарты серии ИСО/МЭК 20000 и ИСО/МЭК 27001.

В Казахстане уже несколько организаций, являющихся поставщиками услуг, внедрили и сертифицировали систему менеджмента услуг и систему менеджмента информационной безопасности на соответствие международным стандартам ИСО/МЭК 20000-1 и ИСО/МЭК 27001. Такие сертификаты являются веским аргументов при выборе поставщиков услуг на тендерах и конкурсах.

Все больше заказчиков в своих требованиях указывают на необходимость предоставления сертификатов на системы менеджмента. Ведь качество и своевременность услуг, например, в области информационных технологий,

становятся все более критичными для непрерывности бизнеса. Прерывание информационной услуги (сервиса) может привести к остановке бизнеса, что сулит для заказчика не только прямые финансовые потери, но и ухудшение имиджа и доверия потребителей. В наше время в условиях сильнейшей конкуренции нельзя игнорировать репутационные риски. Управлять такими рисками легче всего через закупку услуг у сертифицированных поставщиков.

Вместе с новыми информационными технологиями появились новые проблемы и новые виды преступности, то есть новые угрозы информационной безопасности. Это компьютерные вирусы, «трояны», хакеры, промышленный шпионаж, кража информации, воровство ноу-хау, террор, шантаж, вооруженные ограбления и тому подобное. Источниками этих угроз могут быть информационные сети и системы, сотрудники, поставщики, потребители, финансовые организации и государственные учреждения. Слабая защита также является постоянным источником угроз безопасности. В результате возможна потеря ценного конкурентного преимущества, утечка информации личного характера, кража клиентской базы данных и прямые финансовые потери. Кроме того, компания теряет свой имидж из-за неспособности защитить конфиденциальную информацию, предоставленную ему клиентом. В наихудшем случае возможна и утечка государственных секретов.

Очевидно, что задача по обеспечению качества услуг и информационной безопасности является одной из приоритетных для современной организации. От успешного решения этой задачи зависит устойчивость и конкурентоспособность организации, а также ее репутация. Необходимо заметить, что решение такой задачи не может быть частичным, оно должно быть комплексным. Услуга должна комплексно учитывать все аспекты: качество, время, риски, безопасность и прочие. Такое комплексное решение возможно только посредством СИСТЕМНОГО ПОДХОДА.

К счастью, появились международные стандарты, включая ИСО/МЭК 20000-1:2011 «Информационные технологии. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг» и ИСО/МЭК 27001:2013 «Информационные технологии. Системы информационной безопасности. Требования». На основе этих стандартов можно создать интегрированную систему менеджмента, включающую в себя качество услуг и информационную безопасность. Эти стандарты основаны на общих принципах разработки международных стандартов и имеют структуры, которые обеспечивает максимально легкое их совместное использование. Кроме того, часто эти стандарты используются совместно с другими стандартами на системы менеджмента, такие как ИСО 9001 «Системы менеджмента качества. Требования» или ИСО 14001 «Системы экологического менеджмента. Требования и руководство по применению».

ИСО/МЭК 20000-1 и ИСО/МЭК 27001, как и прочие международные стандарты на системы менеджмента, применяют широко известный цикл PDCA (см. рисунок 1) для постоянного улучшения и адаптации системы менеджмента:

Plan – разработайте систему менеджмента, которую затем установите, например, посредством утверждения и рассылки процедур и планов.

Do – внедрите систему менеджмента и обеспечьте ее функционирование, например, посредством распределения полномочий и четкой постановки целей и задач.

Check – регулярно проводите мониторинг и анализ системы менеджмента, например, через плановые и внеплановые аудиты, через анализы со стороны руководства.

Act – при необходимости адаптируйте и улучшайте систему менеджмента, например, через корректирующие и предупреждающие действия.

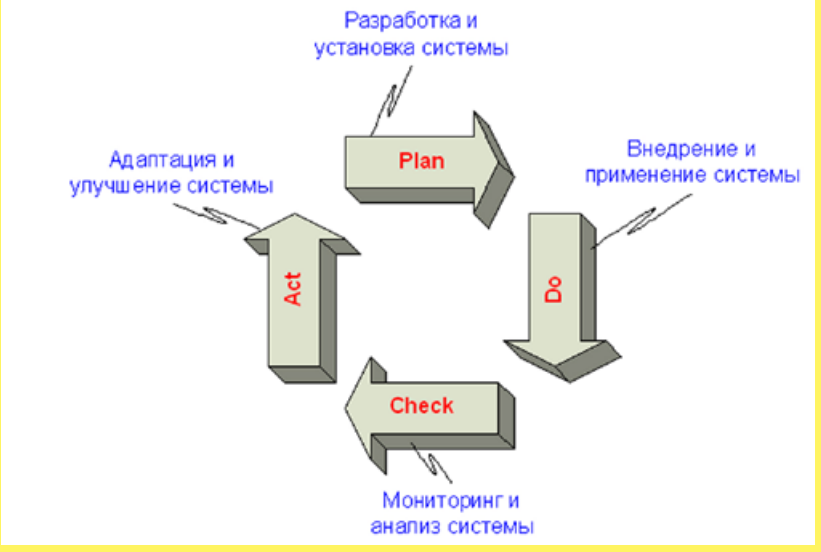


Рисунок 1. Цикл PDCA

Важнейшей концептуальной основой системы менеджмента является риск-менеджмент. Для банков и организаций в некоторых других отраслях это вполне знакомый термин. Обычно под риск-менеджментом понимают управление рисками, включая их опреде-ление, оценку и принятие мер для их исключения или снижения до минимума. Собственно говоря, риск – это сочетание вероятности возникновения события (инцидента) и последствия этого.

Например, компьютерная система организации может легко быть инфицирована компьютерным вирусом, а последствия этого могут вылиться в остановку бизнес-процессов и вытекающие из этого значительные финансовые потери. Поэтому вирусная атака связана с очень высоким риском и обязательно необходима соответствующая защита с помощью организационных, программных и технических средств.

Часто риски оценивают в денежном эквиваленте. Это позволяет оценить эффективность инвестиций в информационную безопасность организации. Как правило, инвестиции в информационную безопасность окупаются стабильностью или устойчивостью организации, большим доверием клиентов.

Международные стандарты серии ИСО/МЭК 20000 и ИСО/МЭК 27001 являются документами, в которых сконцентрирована лучшая международная практика, достигнутая в области менеджмента информационных технологий. Как это принято в ИСО (Международная организация по стандартизации) и МЭК (Международный электротехнический комитет), к разработке новых международных стандартов привлекается широкий круг заинтересованных организаций и экспертов посредством технических комитетов. Данные стандарты были разработан в ОТК 1 (объединенный технический комитет) «Информационные технологии».

Международные стандарты серии ИСО/МЭК 20000 и ИСО/МЭК 27001 интегрируют в себе оба метода – PDCA и риск-менеджмент. Это позволяет построить максимально результативную систему менеджмента. Методы риск-менеджмента непосредственно встроены в цикл PDCA с целью их применения при разработке, мониторинге, поддержании и постоянном улучшении системы менеджмента. ИСО/МЭК 20000 и ИСО/МЭК 27001 предоставляют рабочую структуру для применения лучшей международной практики в области систем менеджмента, то есть для понимания того, где те или иные средства управления (инструменты) могут быть применены.

Кроме того, руководителям организаций следует признать, что система менеджмента будет результативной и эффективной при условии вовлечения всех структурных подразделений и всех работников. Этот подход, основанный на общих организационных рисках, отражен в другом стандарте серии ИСО/МЭК 27002:2013 «Информационные технологии – Методы обеспечения безопасности – Практические правила менеджмента информационной безопасностью». Новейшие принципы безопасности OECD (Организация по экономическому сотрудничеству и развитию) требуют создания «культуры безопасности» внутри организации.

Далее, международные стандарты серии ИСО/МЭК 20000 и ИСО/МЭК 27001 предо-ставляют средства для внедрения результативной системы менеджмента, соответствующей организационным целям и потребностям бизнеса. Ядро этой системы менеджмента должно также соответствовать существующим и потенциальным угрозам безопасности, техническим и технологическим требованиям, возможностям информационных систем и бизнес-процессов, законодательным и нормативным требованиям и контрактным требованиям.

Применение международных стандартов серии ИСО/МЭК 20000 и ИСО/МЭК 27001 позволяет получить следующий ряд преимуществ:

– конкурентное преимущество на тендерах/конкурсах, где в технических условиях требуется наличие сертификатов на соответствующие системы менеджмента;

– демонстрация того, что системы и процессы организации находятся на достаточном уровне зрелости и обеспечивают надлежащее качество и безопасность;

– обеспечение качества, непрерывности и информационной безопасности для клиентов, что жизненно важно для ведения организацией успешного бизнеса;

– передача на аутсорсинг процессов без ущерба для качества, непрерывности и ин-формационной безопасности как организации, так и ее клиентов;

– снижение рисков организации и ее клиентов, что в целом способствует устойчивому развитию.

Организации, прошедшие сертификацию по ИСО/МЭК 20000-1 и ИСО/МЭК 27001, прежде всего видят пользу от этой сертификации в

расширении портфеля сертификатов, что непосредственно влияет на имидж организации как преуспевающей и современной.

ИСО/МЭК 27001 применим для любых видов деятельностей, для любых типов и размеров организаций. Наибольшей популярностью стандарт ИСО/МЭК 27001 пользуется в следующих отраслях:

– телекоммуникация;
– банковская деятельность и финансы;
– страхование;
– информационные технологии;
– здравоохранение;
– государственные услуги;
– коммунальные услуги;
– розничная торговля;
– образование;
– службы по чрезвычайным ситуациям;
– силовые структуры;
– производство;
– транспортные компании;
– поставщики услуг.

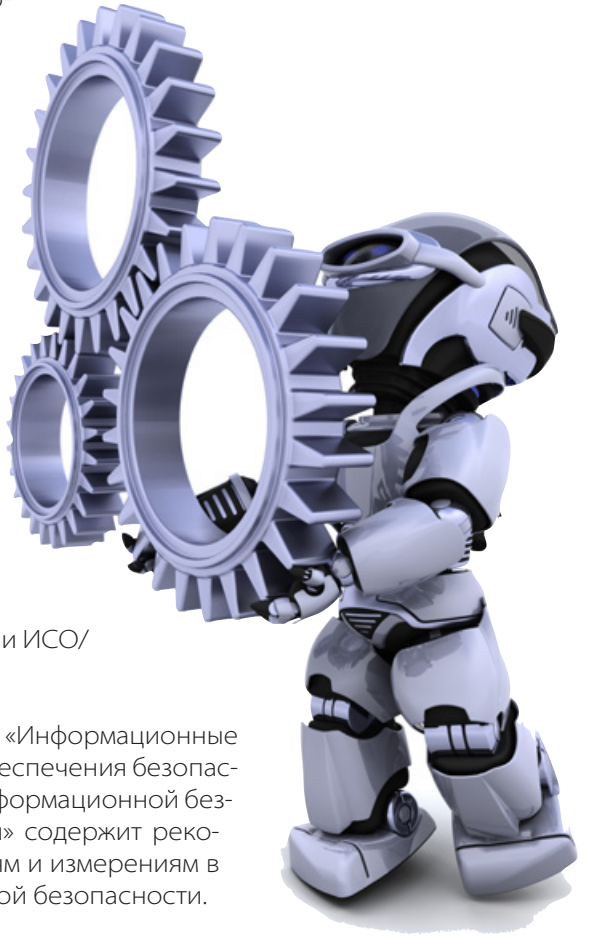
Стандарт ИСО/МЭК 20000 изначально разрабатывался для отраслей, применяющих информационные технологии. Но тем не менее в нем нет запретов на более широкое применение. Есть уже практический опыт применения этого стандарта для телекоммуникационных услуг.

Стандарты серии ИСО/МЭК 20000 и ИСО/МЭК 27001 достаточно гибки, чтобы их можно было использовать для интеграции как между собой, так и с уже существующими системами менеджмента, а также для интеграции в любые существующие методики риск-менеджмента. Например, такие процедуры, как управление записями, управление документами, управление внутренними аудитами, корректирующие и предупреждающие действия могут быть общими для всех систем менеджмента.

Как и при применении ИСО 9001, применяя ИСО/МЭК 20000-1 и ИСО/МЭК 27001, организация может разработать, внедрить и сертифицировать свою систему менеджмента на соответствие этим международным стандартам. Общая динамика роста сертификатов по ИСО/МЭК 20000 и ИСО/МЭК 27001 свидетельствует о том, что данные стандарты являются настоящими бестселлерами и их авторитет очень высок. Несомненно, этому также способствует все большее преобладание в деятельности нематериальных активов над материальными, то есть информационной над физической составляющей продукции. Текущий финансовый кризис еще раз подтвердил значимость информации в наше время и тяжесть последствий от ошибок в области информационной безопасности.

Кроме упомянутых выше стандартов ИСО/МЭК 27001 и ИСО/МЭК 27002 в серию стандартов по информационной безопасности уже вошли также следующие стандарты:

ИСО/МЭК 27000:2012 «Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь». Данный стандарт содержит общие сведения и терминологию по информационной безопасности, так же как стандарт ИСО 9000, предоставляет общие положения и словарь для системы менеджмента качества.



ИСО/МЭК 27003:2010 «Информационные технологии – Методы обеспечения безопасности – Руководящие указания по внедрению системы менеджмента информационной безопасности». Данный стандарт содержит руководящие указания для внедрения СМИБ на основе стандартов серии ИСО/МЭК 27000.

ИСО/МЭК 27004:2009 «Информационные технологии – Методы обеспечения безопасности – Менеджмент информационной безопасности – Измерения» содержит рекомендации по показателям и измерениям в области информационной безопасности.

ИСО/МЭК 27005:2011 «Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности». Как было отмечено выше, риск-менеджмент является ядром стандартов серии ИСО 27000, и поэтому был опубликован дополнительный стандарт касательно управления рисками безопасности.

ИСО/МЭК 27006:2011 «Информационные технологии – Обеспечение безопасности – Требования к органам, осуществляющим аудит и сертификацию систем информационной безопасности». Данный стандарт необходим аккредитованным органам для предоставления услуг по аудиту и сертификации систем информационной безопасности. Следует также опираться на стандарты ИСО/МЭК 17021:2011 «Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента» и ИСО 19011:2011 «Руководящие указания по аудиту систем менеджмента».

ИСО/МЭК 27007:2011 «Информационные технологии – Методы обеспечения безопасности – Руководящие указания по аудиту систем менеджмента информационной безопасности».

ИСО/МЭК ТО 27008:2011 «Информационные технологии – Методы обеспечения безопасности – Руководство для аудиторов средств управления информационной безопасностью».

ИСО/МЭК 27010:2012 «Информационные технологии – Методы обеспечения безопасности – Менеджмент информационной безопасности для межотраслевых и межорганизационных коммуникаций».

ИСО/МЭК 27011:2008 «Информационные технологии – Методы обеспечения безопасности – Руководящие указания по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».

ИСО/МЭК 27013:2012 «Информационные технологии – Методы обеспечения безопасности – Руководство по интегрированному внедрению ИСО/МЭК 27001 и ИСО/МЭК 20000-1».

ИСО/МЭК 27014:2013 «Информационные технологии – Методы обеспечения безопасности – Управления информационной безопасностью».

ИСО/МЭК ТО 27015:2012 «Информационные технологии – Методы обеспечения безопасности – Руководящие указания для менеджмента информационной безопасности финансовых услуг».

ИСО/МЭК ТО 27019:2013 «Информационные технологии – Методы обеспечения безопасности – Руководящие указания по менеджменту информационной безопасности на основе ИСО/МЭК 27002 для систем контроля процессов в энергетической отрасли».

Следующие стандарты находятся в стадии разработки и подготовки к публикации:

ИСО/МЭК 27009 «Информационные технологии – Методы обеспечения безопасности – Использование и применение ИСО/МЭК 27001 для отрасли/услуг, аккредитованных третей стороной».

ИСО/МЭК 27016!!Проект!!! «Информационные технологии – Методы обеспечения без-опасности – Менеджмент информационной безопасности – Экономика организации».

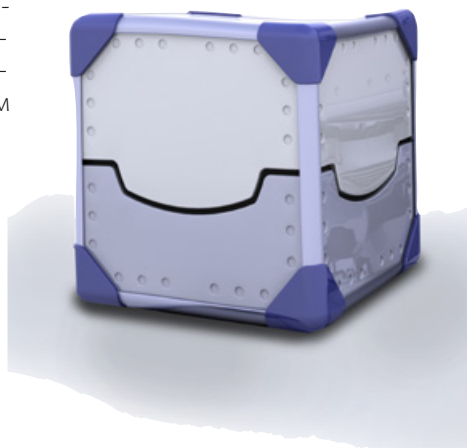
ИСО/МЭК 27017 «Информационные технологии – Методы обеспечения безопасности – Практические правила по средствам управления для «облачных» вычислительных сервисов на основе ИСО/МЭК 27002».

ИСО/МЭК 27018 «Информационные технологии – Методы обеспечения безопасности – Практические правила по средствам управления защитой данных в общедоступных вычислительных сервисах».

Стандарт ИСО/МЭК 20000 состоит из нескольких частей. Чаще всего используется первая часть этого стандарта ИСО/МЭК 20000-1, которая содержит требования и по которой проводится сертификация системы менеджмента услуг. Другие части этого стандарта:

ИСО/МЭК 20000-2:2012 «Информационная технология. Менеджмент услуг. Часть 2. Руководство по применению систем менеджмента услуг».

ИСО/МЭК ТО 20000-3:2012 «Информационные технологии. Менеджмент услуг.



Часть 3. Руководство по определению области применения и применимости ИСО/МЭК 20000-1».

ИСО/МЭК ТО 20000-4:2010 «Информационные технологии. Менеджмент услуг. Часть 4: Стандартная модель процесса».

ИСО/МЭК ТО 20000-5:2010 «Информационные технологии. Менеджмент услуг. Часть 5: Примерный план реализации ИСО/МЭК 20000-1».

Следующие части находятся в стадии разработки и подготовки к публикации:

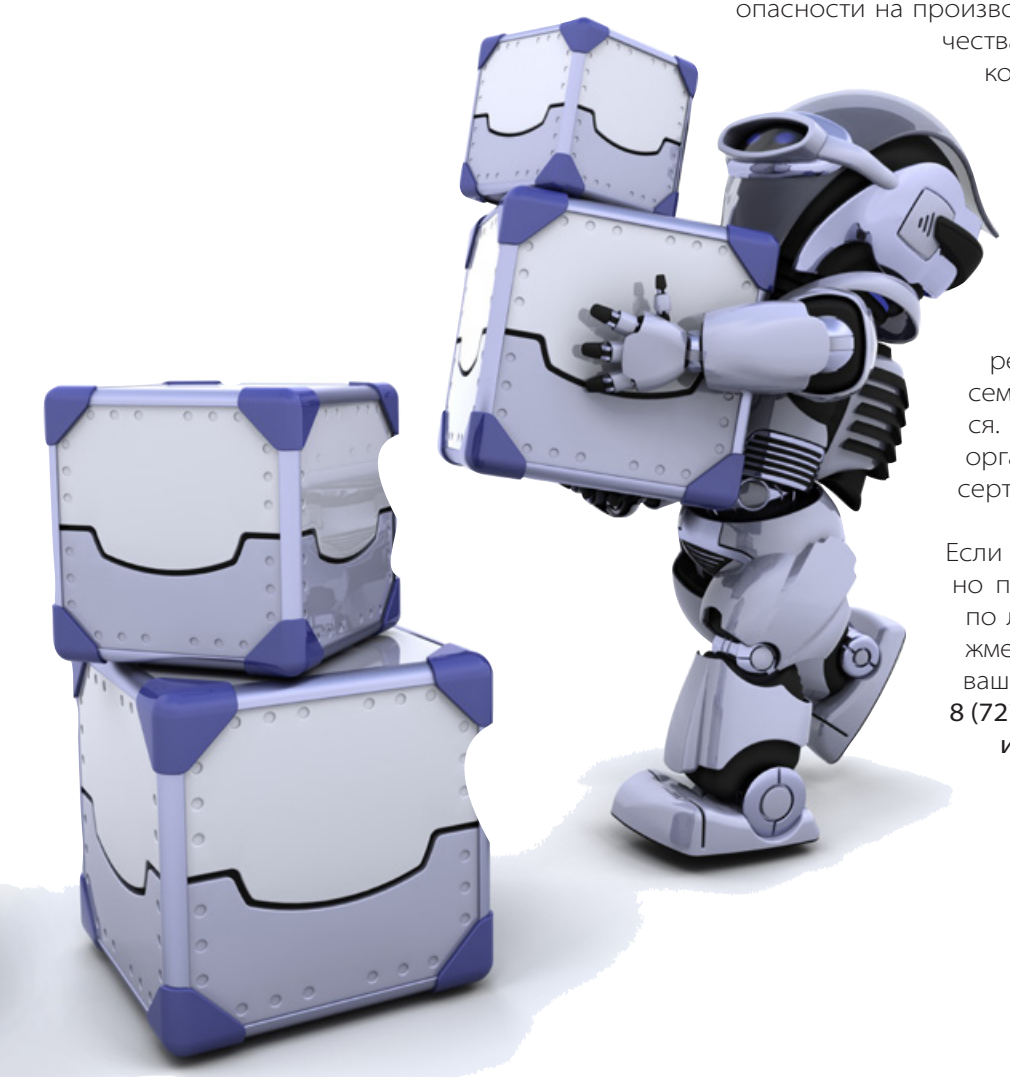
ИСО/МЭК 20000-7 «Информационные технологии. Менеджмент услуг. Часть 7. Руководство по применению ИСО/МЭК 20000-1 для «облака».

ИСО/МЭК 20000-10 «Информационные технологии. Менеджмент услуг. Часть 10. Концепция и терминология».

ИСО/МЭК 20000-11 «Информационные технологии. Менеджмент услуг. Часть 11. Руководство по взаимосвязи ИСО/МЭК 20000-1:2011 с концепциями менеджмента услуг».

Приступить к внедрению систем менеджмента можно, например, воспользовавшись услугами наших консультантов, обладающих соответствующей подготовкой и знаниями, подтвержденными международными сертификатами. Например, Казахстанская организация качества имеет более 700 успешно внедренных проектов в области систем менеджмента на территории Республики Казахстан.

Казахстанская организация качества с 1 сентября 2005 года является членом EFQM (Европейский фонд управления качеством). Казахстанская организация качества одной из первых казахстанских консалтинговых компаний в 2005 году успешно прошла процедуру международной сертификации системы менеджмента качества на соответствие требованиям международных стандартов ИСО 9001, 14001 и OHSAS 18001 и получила сертификат соответствия единого международного образца IQNet. Кроме того, Казахстанская организация качества разработала десятки СТ РК – стандартов Республики Казахстан, включая стандарты по качеству и безопасности на производстве. Казахстанская организация качества является также членом технического комитета ТК 54 «Системы менеджмента качества».



Казахстанская организация качества организует большое количество бизнес-семинаров по системам менеджмента как для специалистов, так и для высшего руководства. Эти семинары посетили более 25 000 слушателей из всех регионов Казахстана. Темы и программы семинаров постоянно совершенствуются. Например, проводятся семинары для орга-низаций, которые уже внедрили и сертифицировали системы менеджмента.

Если у вас возникнут вопросы касательно процедур внедрения и сертификации по любым стандартам на системы менеджмента, то мы будем рады ответить на все ваши вопросы **по телефонам:**
8 (727) 2-60-87-68, 2-60-87-69
или по электронной почте
kok@kok.kz.

Сауле Шокаева, консультант