

ОТЧЕТ
по анализу системы менеджмента
«Агентство государственных услуг при Министерстве
Юстиции Республики Узбекистан»
на соответствие требованиям международных стандартов
ISO 9001:2015 и ISO/IEC 27001:2013

C-191-AGU/IMSA-0.825

Заказчик ПРООН

Объекты Существующая практика управления Агентства
диагностического государственных услуг при Министерстве Юстиции Республики
аудита Узбекистан в рамках требований стандартов ISO 9001:2015 и
ISO/IEC 27001:2013 при разработке, внедрении и оказании
государственных услуг

от Исполнителя: Руководитель проекта  Куйлибаев Э.М.

от Заказчика: _____

КОНФИДЕНЦИАЛЬНО

Введение

Целью проведения анализа существующей системы менеджмента «Агентство государственных услуг при Министерстве Юстиции Республики Узбекистан» (далее Агентство) является:

- определение степени соответствия фактически выполняемой деятельности в Агентства, требованиям международных стандартов ISO 9001:2015 Требования к системе менеджмента качества и ISO/IEC 27001:2013 Системы менеджмента информационной безопасности - Требования;
- сбор сведений для планирования дальнейшей реализации проекта по разработке и внедрению интегрированной системы менеджмента (ИСМ);
- сбор сведений для проведения анализа со стороны высшего руководства;
- выявление наиболее проблемных направлений деятельности, которые могли бы негативно повлиять на результаты прохождения сертификации, или на результативность функционирования ИСМ.

Анализ системы менеджмента проводился консультантами ООО «SMS SYSTEMS» Куйлибаевым Э.М. и Ибрагимовым А.А.

Анализ системы менеджмента осуществлялся методом интервьюирования должностных лиц (опросы и беседы) согласно плана аудита. На основании полученных ответов и предоставленной информации определялось насколько имеющаяся документация и практика управления соответствует минимальным требованиям и может быть полезной в достижении успеха реализации проекта.

Проведенный анализ системы менеджмента «Агентство государственных услуг при Министерстве Юстиции Республики Узбекистан» позволяет подвести основные предварительные итоги работы.

Наблюдения, сделанные в ходе проведения диагностического аудита, а также рекомендации по приведению практики осуществления деятельности в соответствие требованиям международных стандартов ISO 9001:2015 и ISO/IEC 27001:2013 приведены в приложении 1 и 2 соответственно.

1. Выводы и предложения по дальнейшей реализации проекта

Сильные стороны

- Состав специалистов, имеющих достаточный опыт и стремящихся к обучению и улучшениям в работе;
- Наличие законодательной базы и возможностей для её развития с целью улучшения качества и увеличения количества предоставляемых услуг;
- Наличие информационно вычислительных мощностей;
- Наличие источников финансирования.

В ходе диагностического аудита выявлены слабые стороны:

- Не определен контекст Агентства;
- В системе управления не применен принцип риск ориентированного мышления.
- Не применен процессный подход и не определены процессы;
- Не определены ключевые показатели результативности;
- Не определены Политика и цели;
- Низкий уровень регламентации деятельности (в основном упор на компетентность сотрудников, что увеличивает человеческий фактор)
- Не определены (документально не установлены) требования к управлению обеспечивающих процессов: управление инфраструктурой, средой для функционирования процессов, коммуникации, управление средствами измерений и т.д;
- Отсутствует заявление о применимости, не определены риски информационной безопасности и отсутствует процесс обработки рисков, направленных на их устранение или смягчение;
- Не обеспечивается системный подход к подготовке персонала;
- Не установлены требования к управлению внутриорганизационными знаниями;
- Отсутствует системный подход к оценке результативности системы менеджмента;
- Не установлен механизм управления несоответствиями.

Слабые стороны и наблюдения, связанные с отдельными видами деятельности подразделений АГУ:

Управление внедрения и развития государственных услуг:

- Отсутствует системный метод к процессу разработки государственных услуг;
- Не ведутся записи по анализу рисков касательно разрабатываемых государственных услуг;
- Нет свидетельств верификации (контроля) и валидации (подтверждения) результатов государственных услуг.
- Не представлены свидетельства управления внешним процессом, участвующим в процессе разработки гос. услуг.

Управление по контролю за оказанием государственных услуг государственными органами и иными организациями:

- Не предоставлены свидетельства по управлению несоответствий, выявляемых при предоставлении государственных услуг;
- Нет записей несоответствий, возникших в прошлом для анализа качества предоставляемых услуг со стороны государственных учреждений и других организаций.

Управление цифровизации государственных услуг:

- Не установлены требования к инфраструктуре;
- Не предоставлены свидетельства контроля за аутсорсинговыми организациями по предоставлению инструментов оказания государственных услуг;

- Нет свидетельств анализа рисков информационной безопасности на всех этапах осуществления деятельности Агентства и её инфраструктуры.

Организационно-аналитический отдел:

- Не установлены требования к инструментам коммуникации;
- Отсутствует системный подход по сбору, анализу и оценке данных о деятельности Агентства.

Отдел связей с общественностью и СМИ:

- Не установлены требования по классификации категорий информации, подлежащей публикации;
- Не установлены требования к порядку публикации данных со стороны Агентства, включая ответственность за предоставление неправильных данных или утечку данных, не подлежащих публикации;
- Не представлены свидетельства сбора данных по требованиям внешних заинтересованных сторон.

Отдел международного сотрудничества:

- Отсутствует системный подход к обращению международным и иностранным организациям со стороны Агентства;
- Не предоставлены свидетельства сбора данных по требованиям внешних заинтересованных сторон.

Отдел материально-технического обеспечения:

- Нет свидетельств проведения контроля закупаемых услуг или материалов;
- Не представлены записи по анализу результативности закупок, включая анализ тенденций деятельности по закупкам.

Отдел кадров:

- Нет системного подхода к обеспечению компетенции персонала;
- Нет свидетельств анализа результативности обучения и контроля соответствия установленных требований к компетенции персонала.

Ознакомившись с текущей организацией деятельности и применяемой практикой управления, предлагаем следующие решения:

1. Определить процессы, установить взаимосвязи показатели результативности процессов;
2. Установить ответственность по процессам за ключевыми должностями в Агентстве. Установить мониторинг результативности ИСМ по ключевым показателем результативности;
3. Закрепить ответственность за контроль и мониторинг ИСМ за организационно-аналитическим отделом;
4. Закрепить ответственность за информационной безопасностью за отделом кибербезопасности и предоставить необходимые полномочия для установления необходимых механизмов обеспечения информационной безопасности;
5. Выделить необходимые ресурсы для обеспечения требований к физической, экономической и информационной безопасности;
6. Разработать необходимые документы по требованиям стандарта ISO/IEC 27001:2013 согласно приложению 3.
7. Определить мероприятия по повышению уровня ответственности и сознательности к управлению информацией со стороны работников;
8. Вовлекать персонал в деятельность по ИСМ посредством целевых семинаров и собраний;
9. Определить мероприятия по внедрению риск-ориентированного мышления в каждую отдельную структуру предприятия. Среди мероприятий установить при вводном обучении для новых сотрудников обучение риск-ориентированному подходу к работе на предприятии;
10. Периодически проверять систему на пригодность и актуальность требований посредством проведения внутренних аудитов, а также проведения анализа результативности со стороны Высшего руководства.

Приложение 1.

**Анализ фактического состояния существующей системы менеджмента
«Агентство государственных услуг при Министерстве Юстиции Республики Узбекистан» по требованиям стандарта ISO 9001:2015**

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
4.1	<p>Понимание организации и ее контекста Организация должна выявить внешние и внутренние факторы (обстоятельства) Организация должна осуществлять мониторинг и анализ информации, относящейся к этим внешним и внутренним факторам (обстоятельствам)</p>	<p>Отсутствуют свидетельства что контекст определялся. В беседе с сотрудниками Агентства выявлено, что внешние и внутренние факторы влияющие на деятельность Агентства анализируются специалистами или руководством, в основном при возникновении проблемных ситуаций. Эта работа не систематизирована.</p>	<p>Необходимо определить контекст Агентства с учётом всех внутренних и внешних факторов. Необходимо установить требования по проведению анализа контекста.</p>
4.2	<p>Понимание потребностей и ожиданий заинтересованных сторон Организация должна определить: а) заинтересованные стороны, которые имеют отношение к системе менеджмента качества; б) требования этих заинтересованных сторон, относящиеся к системе менеджмента качества. Организация должна осуществлять мониторинг и анализ информации относительно этих заинтересованных сторон и их соответствующих требований.</p>	<p>Отсутствует описание заинтересованных сторон и анализа их требований. Отсутствует систематизированный анализ заинтересованных сторон, который бы учитывал специфику и особенности деятельности Агентства, и в полной мере учитывал бы требования и ожидания заинтересованных сторон.</p>	<p>Необходимо более тщательно провести анализ заинтересованных сторон и их требований, которые имеют отношение к ИСМ и оказываемым услугам. Необходимо установить требования, для того что бы определение и анализ заинтересованных сторон и их требований применялись систематически, с учётом всех внутренних и внешних заинтересованных сторон и факторов связанных с ними.</p>
4.3	<p>Определение области применения системы менеджмента качества Организация должна определить границы применения системы менеджмента качества, чтобы установить ее область с учетом: а) внешние и внутренние факторы (обстоятельства), указанные в 4.1; б) требования соответствующих заинтересованных сторон, указанные в 4.2; с) продукцию и услуги организации. Информация об области применения системы менеджмента качества организации должна быть доступна, а также поддерживаться в актуальном состоянии в виде документированной информации</p>	<p>Область применения системы менеджмента не определена.</p>	<p>Рекомендуется сформулировать область сертификации в следующем виде: «Оказание государственных услуг физическим и юридическим лицам»</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
4.4.1	<p>Система менеджмента качества и ее процессы Организация должна разработать, внедрить, обеспечить функционирование и постоянно улучшать систему менеджмента качества, включая необходимые процессы а) определить требуемые входы к этим процессам и их ожидаемые выходы Определить последовательность и взаимодействие этих процессов Определить и применять критерии и методы (включая мониторинг, измерения и соответствующие показатели/индикаторы деятельности), необходимые для обеспечения результативного функционирования процессов и управления ими; Определить ресурсы, необходимые для этих процессов, и обеспечить их наличие; Возложить ответственность и предоставить полномочия в отношении этих процессов; Учесть риски и возможности в соответствии с требованиями 6.1 Оценивать эти процессы и вносить какие-либо изменения, необходимые для обеспечения того, чтобы эти процессы достигали желаемые результаты; Улучшать процессы и систему менеджмента качества В том виде и объеме, в котором это необходимо, организация должна: Поддерживать в актуальном состоянии документированную информацию для поддержки функционирования ее процессов Сохранять документированную информацию для обеспечения уверенности в том, что процессы осуществляются так, как было запланировано.</p>	<p>Не применяется процессный подход. Существующая система управления основана на иерархическом подходе сверху вниз, где не учитываются связи и требования внутренних потребителей.</p>	<p>Необходимо определить процессы, их основные входы и выходы, описать взаимодействие этих процессов, установить показатели и критерии результативности этих процессов, кто и когда должен их контролировать.</p> <p>Рекомендуется определить внешние процессы по предоставлению услуг и методы их контроля.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
5.1.1	<p>Лидерство и приверженность</p> <p>Высшее руководство должно демонстрировать свое лидерство и приверженность системе менеджмента качества посредством:</p> <p>Принятия на себя ответственности за результативность системы менеджмента качества</p> <ul style="list-style-type: none"> – Обеспечения того, чтобы в рамках системы менеджмента качества были установлены политика и цели в области качества, и чтобы они были согласованы с ее контекстом и со стратегическим направлением организации; – Обеспечения того, чтобы требования системы менеджмента качества были интегрированы в бизнес-процессы организации; – Поддержки применения процессного подхода и риск-ориентированного мышления; – Обеспечения наличия ресурсов, необходимых для системы менеджмента качества; – Распространения в организации понимания важности результативного менеджмента качества и соответствия требованиям системы менеджмента качества; – Обеспечения того, чтобы система менеджмента качества получала свои желаемые результаты – Вовлечения, направления и поддержки лиц вносящих вклад по обеспечению результативности системы менеджмента качества; – Поддержки улучшений; – Поддержки соответствующих должностных лиц в демонстрации ими лидерства в их зоне ответственности. 	<p>Активное участие персонала Агентства при проведении диагностического аудита свидетельствует о том, что Руководство Агентства обеспечивает понимание работниками важности результативного менеджмента качества и соответствия требованиям системы менеджмента качества.</p> <p>Руководство Агентства способствует вовлечению персонала в разработку и внедрение ИСМ, с целью дальнейшего улучшения результативности системы и деятельности Агентства в целом.</p> <p>Не определены политика и цели в области качества.</p> <p>Требования системы менеджмента качества не интегрированы в бизнес процессы предприятия.</p> <p>Не внедрен процессных подход и риск-ориентированное мышление.</p>	<p>Для полного соответствия требованиям стандарта в отношении лидерства (ведущей роли) Руководства Агентства, необходимо задокументировать его стремления и намерения в улучшении системы менеджмента, и принятые в этом отношении обязательства. Для этого Определить Стратегические направления Агентства, отразить их в Политике в области качества, разработать Цели в области качества (см. пункт 6.2.1).</p>
5.1.2	<p>Ориентация на потребителей</p> <p>Высшее руководство должно демонстрировать свое лидерство и приверженность в отношении ориентации на потребителей и посредством обеспечения того, чтобы:</p> <p>Требования потребителей, а также применимые законодательные и нормативные правовые требования были выявлены, поняты и постоянно выполнялись</p> <p>Риски и возможности, которые могут влиять на соответствие продукции и услуг и на способность повышать степень удовлетворенности потребителей, были определены и рассмотрены;</p> <p>В центре внимания находилось повышение степени удовлетворенности потребителей.</p>	<p>Нет свидетельств того, что целенаправленно применяется изучение рисков и возможностей, которые могут влиять на соответствие услуг, для повышения степени удовлетворенности потребителей.</p>	<p>Необходимо создать механизм обратной связи, а также использования информации, получаемой от потребителей с целью улучшения качества предоставляемой продукции (услуги).</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
5.2.1	<p>Разработка политики в области качества Высшее руководство должно разработать, внедрить и поддерживать политику в области качества, которая должна:</p> <ul style="list-style-type: none"> a) соответствовать намерениям организации и ее контексту и поддерживать ее стратегическое направление, b) создавать основу для установления целей в области качества, c) включать обязательство соответствовать применимым требованиям, d) включать обязательство постоянно улучшать систему менеджмента качества. 	<p>Политика в области качества не разработана.</p>	<p>Необходимо разработать документ «Политика в области качества». Документ должен соответствовать всем требованиям раздела 5.2.1 стандарта ISO 9001:2015.</p>
5.2.2	<p>Доведение политики в области качества Политика в области качества должна:</p> <ul style="list-style-type: none"> a) быть доступной и поддерживаться в актуальном состоянии в виде документированной информации; b) быть доведена до сведения сотрудников организации, понята ими и применяться в организации; c) быть доступной подходящим способом для соответствующих заинтересованных сторон. 	<p>Политика не разработана, соответственно, пока не может быть доведена до персонала.</p>	<p>Необходимо определить результативный механизм доведения Политики до всего персонала Агентства. Обеспечить понимание её сущности. Также необходимо определить каким образом Политика в области качества будет доступна для заинтересованных сторон.</p>
5.3	<p>Организационные роли, ответственность и полномочия Высшее руководство должно обеспечить, чтобы ответственность и полномочия для соответствующих ролей были распределены, доведены и понятны в организации. Высшее руководство должно распределить ответственность и полномочия:</p> <ul style="list-style-type: none"> a) за обеспечение соответствия системы менеджмента качества требованиям настоящего международного стандарта; b) за обеспечения достижения процессами намеченных выходов; c) за предоставление отчетности высшему руководству по показателям функционирования системы менеджмента качества и возможностям по улучшению (см. 10.1); d) за обеспечение распространения и поддержки в организации ориентации на потребителей, e) за сохранение целостности системы менеджмента качества при планировании и внесении в нее изменений. 	<p>Имеется штатное расписание и орг. структура. Имеются должностные инструкции.</p>	<p>Руководство Агентства должно обеспечить чтобы были чётко определены ответственность и полномочия персонала по каждому бизнес процессу для результативного функционирования процессов. При разработке процедур ИСМ и документов по процессам ИСМ, будут определены и описаны функции каждого подразделения и/или работника в том или ином направлении деятельности.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
6.1.1	<p>Действия по реагированию на риски и возможности При планировании системы менеджмента качества организация должна учитывать факторы, указанные в 4.1, и требования, указанные в 4.2, а также определять риски и возможности, в отношении которых необходимы действия по реагированию, чтобы:</p> <ul style="list-style-type: none"> a) обеспечивать уверенность в том, что система менеджмента качества может достигать желаемых результатов; b) повышать желательные эффекты; c) предотвращать или снижать нежелательные эффекты; d) достигать улучшения. 	<p>Не установлен порядок определения рисков и возможностей, методы их снижения и оценки результативности проведенных мероприятий.</p>	<p>Выполнение требования данных пунктов связаны с выполнением требования определять контекст Агентства (см пункт 4). Необходимо определить механизм выявления рисков и возможностей, связанных с внешними и внутренними факторами (которые будут выявлены при определении контекста организации), в том числе рисков и возможностей связанных с процессами ИСМ. Необходимо определить механизм отслеживания изменений, которые могут повлиять на степень управляемости рисков и возможностей. Необходимо определить механизм планирования проведения и оценки результативности предпринятых в отношении рисков и использования возможностей.</p>
6.1.2	<p>Организация должна планировать:</p> <ul style="list-style-type: none"> a) действия по реагированию на эти риски и возможности; b) то, как она будет: <ul style="list-style-type: none"> 1) интегрировать и внедрять действия в процессы ее системы менеджмента качества (см. 4.4); 2) оценивать результативность этих действий. 		
6.2.1	<p>Цели в области качества и планирование их достижения Организация должна установить цели в области качества для соответствующих функций, уровней и процессов, необходимых для системы менеджмента качества. Цели в области качества должны:</p> <ul style="list-style-type: none"> a) быть согласованными с политикой в области качества; b) быть измеримыми; c) учитывать применимые требования; d) иметь отношение к обеспечению соответствия продукции и услуг и повышению степени удовлетворенности потребителей; e) подлежать мониторингу; f) доводиться до сведения персонала; g) пересматриваться по мере необходимости. <p>Организация должна поддерживать документированную информацию о целях в области качества в актуальном состоянии.</p>	<p>Есть план работы по годам и стратегия + постановления правительства и президента. (цели и стратегические направления). Отсутствует (не разработан) документ Цели в области качества.</p>	<p>На основе утвержденной политики, разработанной руководством (см. пункт выше), должны быть разработаны конкретные измеримые цели и задачи на конкретный срок с указанием конкретных исполнителей. Для каждой цели необходимо разработать план мероприятий с указанием ответственных и сроков. Сроки выполнения должны быть конечными. Необходимо определить кто и когда должен проводить мониторинг выполнения целей.</p>
6.2.2	<p>При планировании деятельности по достижению целей в области качества организация должна определить:</p> <ul style="list-style-type: none"> a) что должно быть сделано; b) какие для этого требуются ресурсы; c) кто за все это ответственен; d) когда все это должно быть завершено; e) каким образом будут оцениваться полученные результаты. 		

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
6.3	<p>Планирование изменений В тех случаях, когда организация выявляет необходимость в изменениях системы менеджмента качества, эти изменения должны осуществляться на плановой основе (см. 4.4). Организация должна учесть:</p> <ul style="list-style-type: none"> a) цели изменений и их потенциальные последствия; b) сохранения целостности системы менеджмента качества; c) наличие ресурсов; d) распределение или перераспределение ответственности и полномочий. 	<p>Так как система ещё не разработана и не описана, не установлены требования (или порядок) как необходимо действовать в случае если появится необходимость изменить ИСМ.</p>	<p>Необходимо определить механизм изменения ИСМ, т.е как необходимо действовать в случае если появится необходимость изменить ИСМ: кто может инициировать внесение изменений в ИСМ, какие моменты необходимо проверить, кто будет анализировать, и кто принимать решения и т.п. (Примечание: данный момент будет отражен при описании процесса, связанного с планированием ИСМ.)</p>
7.1.1	<p>Ресурсы Организация должна определить и предоставить ресурсы, необходимые для разработки, внедрения, обеспечения функционирования и постоянного улучшения системы менеджмента качества. Организация должна учесть:</p> <ul style="list-style-type: none"> a) возможности и ограничения имеющихся внутренних ресурсов; b) потребности, которые должны быть удовлетворены за счет внешних поставщиков. 	<p>Обеспечение необходимыми ресурсами не планируется и не систематизирована. Необходимые ресурсы обеспечиваются по потребности.</p>	<p>При описании процессов ИСМ по каждому бизнес процессу определить ресурсы, необходимые для выполнения работ процесса. Осуществлять периодический анализ достаточности ресурсов на основании информации, предоставленной от руководителей процессов, и принимать решение об их выделении на анализе со стороны высшего руководства. Стандарт ISO 9001:2015 под ресурсами понимает людские ресурсы, инфраструктуру и производственную среду. К финансовым ресурсам стандарт требований не предъявляет.</p>
7.1.2	<p>Человеческие ресурсы Организация должна определить и обеспечить наличие лиц, необходимых для результативного внедрения ее системы менеджмента качества, а также для обеспечения функционирования и управления ее процессами.</p>	<p>Необходимый персонал определен в штатном расписании.</p>	<p>Для внедрения ИСМ рекомендуется приказом определить рабочую группу по внедрению ИСМ. Также после определения процессов ИСМ издать приказ о процессах ИСМ, в котором для каждого процесса назначить руководителя.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
7.1.3	<p>Инфраструктура Организация должна определить, обеспечить и поддерживать инфраструктуру для функционирования ее процессов с целью достижения соответствия продукции и услуг.</p> <p>Примечание. Инфраструктура может включать: а) здания и соответствующие сооружения б) оборудование, включая аппаратную и программную часть; в) транспортные ресурсы; г) информационные и коммуникационные технологии.</p>	<p>Не определен порядок управления инфраструктурой. Отсутствуют требования к планированию и выполнению обслуживанию имеющегося оборудования, компьютерной и оргтехники. Работа ведется по осмотру зданий и территории, но нет записей. Нет инструкций для обслуживания оборудования и других элементов инфраструктуры.</p>	<p>Необходимо определить действия, направленные на поддержание инфраструктуры в рабочем состоянии. Необходимо документально установить общий порядок учета объектов инфраструктуры, распределения ответственности, требования к планированию работы по их поддержанию, а для каждого объекта определить конкретные действия с учетом руководств по эксплуатации, и степень насколько ими необходимо управлять, с учетом способности влиять на ИСМ.</p>
7.1.4	<p>Среда для функционирования процессов Организация должна определить, обеспечить и поддерживать в рабочем состоянии среду, необходимую для функционирования ее процессов для достижения соответствия продукции и услуг.</p> <p>Примечание. Пригодная среда может быть комбинацией человеческих и физических факторов, таких, как: а) социальные (например, отсутствие дискриминации, спокойная атмосфера, бесконфликтность); б) психологические (например, снижение стрессовых ситуаций, предотвращение морального истощения, защита от проявления эмоций); в) физические (например, температура, тепла, влажности, освещения, вентиляции, гигиены, шума)</p>	<p>Общая температура и влажность в помещениях обеспечивается в нормальных условиях. В серверных комнатах установлены системы кондиционирования воздуха. Не определен порядок управления средой для функционирования процессов.</p>	<p>Рекомендуется разработать процесс управления средой для управления средой для функционирования предоставления услуг и выполнению деятельности, связанных с предоставлением услуг.</p>
7.1.5.1	<p>Ресурсы для мониторинга и измерений Организация должна определить и предоставить ресурсы необходимые для обеспечения достоверности и признаваемости результатов, когда мониторинг или измерения используются для верификации соответствия продукции или услуг требованиям.</p> <p>Организация должна обеспечить, что предоставленные ресурсы: а) были пригодны для конкретных видов осуществляемой деятельности по мониторингу и измерениям; б) поддерживались в рабочем состоянии для обеспечения постоянной пригодности их назначения.</p> <p>Организация должна сохранять соответствующую документированную информацию в качестве доказательства пригодности ресурсов для целей мониторинга и измерений.</p>	<p>Используются различные информационные системы для мониторинга статусов предоставления услуг и выполнения заданий по планам и мероприятиям. Нет свидетельств управления информационных систем и обеспечения их пригодности для мониторинга и измерений. Что необходимо предпринять для поддержания работоспособности приложения и отсутствия проблем и ошибок приложений. Постоянные</p>	<p>Необходимо систематизировать работу по поддержанию информационных систем в работоспособном состоянии и постоянном их улучшении. Рекомендуется создать поддерживающий процесс управления инфраструктурой. Определить элементы инфраструктуры и контролировать их работоспособное состояние.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
7.1.5.2	<p>Прослеживаемость измерений В тех случаях, когда прослеживаемость измерений является требованием или рассматривается организацией в качестве существенного обстоятельства при предоставлении доказательств признаваемости результатов измерений, измерительное оборудование должно быть:</p> <p>а) верифицировано и/или прокалибровано, через установленные интервалы или перед его применением, по отношению к стандартам измерений, имеющим прослеживаемость к международным или национальным измерительным стандартам; в случае, когда такие стандарты отсутствуют, основа, используемая для калибровки или верификации, должна фиксироваться и сохраняться в качестве документированной информации;</p> <p>б) идентифицировано в целях возможности установления его статуса;</p> <p>в) защищено от регулировок, поломок или повреждений, которые могли бы сделать недействительными его статус калибровки и последующие результаты измерений.</p> <p>В тех случаях, когда обнаруживается, что измерительное оборудование непригодно для применения по своему назначению, организация должна определить, не повлияло ли это отрицательно на признаваемость результатов выполненных ранее измерений, и осуществить, при необходимости, соответствующие действия.</p>	<p>обновления и работа по усовершенствованию ИС.</p>	
7.1.6	<p>Внутрифирменные знания Организация должна определить знания, необходимые для функционирования ее процессов и для достижения соответствия продукции и услуг Эти знания должны поддерживаться на соответствующем уровне и быть доступными в необходимом объеме. При рассмотрении вопросов, касающихся изменений потребностей в знаниях или тенденций в таких изменениях, организация должна рассмотреть имеющиеся у нее знания и определить, каким образом она будет приобретать или получит доступ к необходимым дополнительным знаниям и необходимому обновлению своих знаний.</p>	<p>Внутрифирменными знания Агентства не находятся под управлением.</p>	<p>Необходимо определить, что является базой знаний. Необходимо определить каким образом будет формироваться и управляться эти знания. Необходимо определить доступ к этим знаниям.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
7.2	<p>Компетентность Организация должна:</p> <p>а) определить необходимую компетентность лиц(а), осуществляющих(его) под ее управлением работу, которая влияет на показатели функционирования и результативность системы менеджмента качества;</p> <p>б) обеспечить, чтобы эти лица были компетентны на основе соответствующего образования, подготовки или опыта;</p> <p>в) где это возможно, осуществлять действия по приобретению необходимой компетентности и оценивать результативность предпринятых действий;</p> <p>г) сохранять соответствующую документированную информацию, как свидетельство компетентности.</p>	<p>Требования к компетентности персонала определены в должностных инструкциях. Ведется работа по повышению квалификации персонала. Но нет планов по обучению персонала.</p> <p>Существует система повышения квалификации юристов, но нет системного подхода к обеспечению требуемой компетенции работников Агентства и центров гос. услуг. Соответственно нет системы оценки знаний после обучения кроме аттестации, которая ещё не производилась.</p>	<p>Необходимо проанализировать ДИ на предмет адекватности описания функциональных обязанностей. Проверить установленные в ДИ требования к образованию, подготовке и опыту.</p> <p>Необходимо систематизировать процесс подготовки и повышения квалификации персонала.</p>
7.3	<p>Осведомленность Организация должна обеспечить, чтобы лица, работающие под управлением организации, были осведомлены:</p> <p>а) о политике в области качества;</p> <p>б) о соответствующих целях в области качества;</p> <p>в) об их вкладе в обеспечение результативности системы менеджмента качества, включая выгоды от улучшения показателей их деятельности;</p> <p>г) о последствиях несоответствий требованиям системы менеджмента качества.</p>	<p>Так как ИСМ не внедрена, отсутствует порядок осведомления персонала об их вкладах в системы предприятия, и о выгодах от улучшения их показателей.</p>	<p>Необходимо определить и задокументировать каким образом будет обеспечиваться осведомленность сотрудников относительно всех моментов, причисленных в пункте 7.3 стандарта.</p> <p>Рекомендуется при внедрении и после спланировать и проводить периодические внутренние семинары для работников, на которых в понятной для них форме освещать вопросы по данной тематике.</p>
7.4	<p>Коммуникация Организация должна определить внутреннюю и внешнюю коммуникацию, относящуюся к системе менеджмента качества, включая:</p> <p>а) то, по каким вопросам будет осуществляться коммуникация;</p> <p>б) когда будет осуществляться коммуникация;</p> <p>в) с кем будет осуществляться коммуникация;</p> <p>г) каким образом будет осуществляться коммуникация;</p> <p>д) кто будет осуществлять коммуникацию.</p>	<p>Частично внутренняя коммуникация определена в должностных инструкциях. Отсутствует документальное определение видов коммуникации, а также распределение ответственности за внешнюю коммуникацию.</p>	<p>Необходимо определить порядок осуществления внутренних и внешних коммуникаций.</p> <p>Необходимо определить ответственность и полномочия по видам коммуникации с внешними сторонами, например, с потребителями, заинтересованными сторонами и внутри предприятия.</p> <p>Рекомендуется установить порядок коммуникации по вопросам ИСМ, а также по взаимодействию с внешними заинтересованными сторонами.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
7.5.1	<p>Документированная информация Система менеджмента качества организации должна включать:</p> <ul style="list-style-type: none"> a) документированную информацию, требуемую настоящим международным стандартом; b) документированную информацию, определенную организацией как необходимую для обеспечения результативности системы менеджмента качества. 	<p>Так как ИСМ не внедрена, отсутствует систематизация документированной информации ИСМ Агентства.</p>	<p>Необходимо разработать процедуру по управлению документированной информацией.</p>
7.5.2	<p>Создание и актуализация При создании и актуализации документированной информации организация должна подходящим образом обеспечить:</p> <ul style="list-style-type: none"> a) ее идентификацию и описание (например, путем указания ее заголовка, даты, авторов или учетного номера); b) ее форматирование (например, язык изложения, версия программного обеспечения, требования к графическим изображениям) и установление соответствующих носителей (например, бумажный, электронный носитель); c) проведение анализа и утверждения информации с точки зрения ее пригодности и адекватности. 	<p>Не определен порядок разработки, согласования и утверждения внутренних документов. Нет четкого определения ответственных за разработку, согласование и утверждение отдельных видов документов.</p>	<p>Разработать процедуру управления документированной информацией. Важно:</p> <ul style="list-style-type: none"> - ориентировать систему управления документацией на большее применение электронных документов, в том числе ведение записей. - исключать дублирование документов; - стремиться оптимизировать по количеству документов и объем содержащихся в документах данных.
7.5.3.1	<p>Управление документированной информацией Документированная информация, требуемая системой менеджмента качества и настоящим международным стандартом, должна находиться под управлением для обеспечения того, что она:</p> <ul style="list-style-type: none"> a) доступна и пригодна для применения в тех случаях, где и когда она необходима; b) адекватно защищена (например, от потери конфиденциальности, ненадлежащего использования или потери целостности). 	<p>Документированная информация управляется посредством информационной системы EDO.</p>	<p>Рекомендуется определить порядок управления документированной информацией. Необходимо классифицировать всю требуемую документированную информацию. Определить требований к доступу к определенным документам для определенных пользователей.</p>
7.5.3.2	<p>Для управления документированной информацией организация должна в том объеме, в котором это приемлемо, рассмотреть следующее:</p> <ul style="list-style-type: none"> a) распространение, доступа к ней, поиск и использования; b) хранения и защита, включая сохранение читабельности; c) управление изменениями (например, управление версиями); d) сроки хранения и порядок уничтожения. <p>Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и функционирования системы менеджмента качества, должна быть подходящим образом идентифицирована и находиться под управлением. Документированная информация, фиксируемая и сохраняемая как свидетельство соответствия, должна быть защищена от непредумышленных изменений.</p>		

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.1	<p>Планирование деятельности и управление ею Организация должна планировать и внедрять процессы (см. 4.4), необходимые для выполнения требований к поставке продукции и предоставлению услуг и для реализации действий, определенных в разделе 6, а также управлять этими процессами посредством:</p> <p>а) определения требований к продукции и услугам; б) установления критериев: 1) для процессов; 2) для приемки (одобрения) продукции и услуг; в) определения ресурсов, необходимых для достижения соответствия требованиям к продукции и услугам; г) управления процессами в соответствии с установленными критериями; д) определения, ведения и сохранения документированной информации в объеме, необходимом: 1) для обеспечения уверенности в том, что процессы осуществляются так, как было запланировано; 2) для демонстрации соответствия продукции и услуг требованиям к ним. Выходные данные такого планирования должны подходить для деятельности организации. Организация должна управлять запланированными изменениями и анализировать последствия незапланированных изменений, предпринимая, при необходимости, действия по смягчению любого негативного влияния. Организация должна обеспечить, чтобы аутсорсинговые процессы находились под управлением (см. 8.4).</p>	<p>Не применен процессный подход. Не применен риск ориентированный подход.</p>	<p>Рекомендуется с учетом требования п.7.4 и 6.1 составить краткие инструкции или планы работ, в которых четко прописать последовательность действий, кто должен осуществлять, какие входные данные нужны и от кого, чем необходимо руководствоваться (ссылки на внутренние и внешние требования), кому в каком виде передается результат действий. Также такие описания могут быть в документах по процессам. Более точно будет определено в ходе разработки процессных документов.</p>
8.2.1	<p>Коммуникация с потребителями Коммуникация с потребителями должна охватывать:</p> <p>а) предоставление информации, относящейся к продукции и услугам; б) обращение с запросами, контрактами или заказами, включая их изменения; в) получение от потребителей обратной связи относительно продукции и услуг, включая их жалобы; г) обращение с собственностью потребителей или управление ею; д) установление специфических требований, относящихся к действиям в непредвиденных обстоятельствах, когда это уместно.</p>	<p>Делается опрос населения (самостоятельно и аутсорсинг) занимается отдел СМИ. Не установлен порядок выявления первичных требований потребителя; Нет свидетельств установления и применения механизма получения обратной связи от конечных потребителей относительно удовлетворенности получаемой услугой.</p>	<p>Задokumentировать требования к осуществлению коммуникации с потребителями по всем возможным направлениям (см. также п.8.1 и 7.4), в том числе определить механизм обратной связи.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.2.2	<p>Определение требований, относящихся к продукции и услугам При определении требований к продукции и услугам, которые будут предлагаться потенциальным потребителям, организация должна обеспечить, чтобы:</p> <p>а) требования к продукции и услугам были определены, включая:</p> <p>1) все применимые законодательные и нормативные правовые требования;</p> <p>2) те, которые рассматриваются организацией как необходимые,</p> <p>б) она могла удовлетворить требования к предлагаемым ею продукции и услугам.</p>	<p>Делается опрос населения (самостоятельно и аутсорсинг) занимается отдел СМИ. В центрах гос. услуг есть автоматическая система обратной связи по оценке уровня сервиса оператора с помощью метода 5 бальной оценки (смайлики). Отсутствует механизм определения требований потребителей.</p>	<p>Необходимо разработать механизм определения требований, относящихся к предоставляемым услугам.</p>
8.2.3.1	<p>Анализ требований, относящихся к продукции и услугам Организация должна быть уверена, что она способна выполнить требования к продукции и услугам, которые будут предложены потребителям. До того, как организация примет на себя обязательство поставить потребителю продукцию и услуги, она должна провести анализ, охватывающий:</p> <p>а) требования, установленные потребителями, включая требования, относящиеся к поставке и деятельности после поставки;</p> <p>б) требования, не заявленные потребителями, но необходимые для обеспечения, установленного или, если это известно, предполагаемого использования;</p> <p>в) требования, установленные организацией;</p> <p>г) законодательные и нормативные правовые требования, применимые к продукции и услугам;</p> <p>д) требования контракта или заказа, отличающиеся от тех, которые были выражены первоначально. Организация должна обеспечить, чтобы требования контракта или заказа, отличающиеся от ранее выраженных, были разрешены. В тех случаях, когда потребители не представляют документально оформленных требований, их требования должны быть подтверждены организацией до того, как они будут приняты к исполнению.</p>	<p>Собирают жалобы и обращения посредством телеграм ботов, телефоны доверия (1148) для улучшения предоставления существующих гос. услуг. Отсутствует механизм определения требований потребителей.</p>	<p>Необходимо определить, как проводить анализ, кто должен участвовать, кто может принимать решения по тем или иным вопросам. Что необходимо рассмотреть при таком анализе.</p>
8.2.3.2	<p>Организация в том объеме, насколько это применимо, должна фиксировать и сохранять документированную информацию, касающуюся:</p> <p>а) результатов анализа;</p> <p>б) всех новых требований к продукции и услугам.</p>	<p>Отсутствует механизм определения требований потребителей.</p>	<p>Необходимо определить в какой форме будут фиксироваться результаты такого анализа.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.2.4	<p>Изменения требований к продукции и услугам В тех случаях, когда требования к продукции и услугам изменились, организация должна обеспечить, чтобы в соответствующую документированную информацию были внесены необходимые изменения, а заинтересованный персонал был поставлен в известность об этих изменениях.</p>	<p>Отсутствует механизм определения требований потребителей.</p>	<p>Необходимо определить механизм реагирования на изменения, для того чтобы обеспечить чтобы они были своевременно доведены до соответствующих лиц, и вовремя применены.</p>
8.3.1	<p>Проектирование и разработка продукции и услуг Организация должна разработать процесс проектирования и разработки, который приемлем для обеспечения последующего создания продукции и услуг, внедрить его и обеспечить его функционирование.</p>	<p>Существуют требования к разработке порядка предоставления услуг.</p>	<p>Необходимо определить и внедрить процесс проектирования и разработки услуг.</p>
8.3.2	<p>Планирование проектирования и разработки При определении стадий и средств управления проектированием и разработкой, организация должна рассматривать:</p> <ul style="list-style-type: none"> a) характер, продолжительность и сложность деятельности по проектированию и разработке; b) требуемые стадии процесса, включая применимые действия по анализу проектирования и разработке; c) требуемые действия в отношении верификации и вариации проектирования и разработки; d) ответственность и полномочия, связанные с процессом проектирования и разработки; e) внутренние и внешние ресурсы, необходимые для проектирования и разработки продукции и услуг; f) необходимость в управлении взаимодействиями между персоналом, участвующим в процессе проектирования и разработки; g) необходимость вовлечения потребителей и пользователей в процесс проектирования и разработки; h) требования для последующего производства продукции и услуг; i) уровень управления процессом проектирования и разработки, ожидаемый потребителями и другими соответствующими заинтересованными сторонами; j) документированную информацию, необходимую для демонстрации выполнения требований к проектированию и разработке. 	<p>Не предоставлены свидетельства планирования разработки регламентов государственных услуг.</p>	<p>Необходимо определить строгую отчетность по каждому этапу разработки порядка предоставления услуг учитывая все возможные этапы и верификации разработки.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.3.3	<p>Входные данные для проектирования и разработки Организация должна определить требования, имеющие важное значение для конкретного вида проектируемых и разрабатываемых продукции и услуг. Организация должна учесть:</p> <ul style="list-style-type: none"> a) функциональные и эксплуатационные требования; b) информацию, полученную из предыдущей аналогичной деятельности по проектированию и разработке; c) законодательные и регламентирующие требования; d) стандарты или своды практик, которые организация обязалась применять; e) потенциальные последствия отказов, связанных с характеристиками продукции и услуг. <p>Входные данные должны быть адекватны целям проектирования и разработки, а также быть полными и непротиворечивыми. Противоречия по входным данным проектирования и разработки должны быть разрешены. Организация должна сохранять документированную информацию по входным данным проектирования и разработки.</p>	<p>Не систематизированы требования по определению входных данных для разработки и проектирования.</p>	<p>Определить порядок выявления всех входных данных для разработки и проектирования и их документирования.</p>
8.3.4	<p>Средства управления проектированием и разработкой Организация должна применять средства управления процессом проектирования и разработки для обеспечения того, что:</p> <ul style="list-style-type: none"> a) результаты, которые должны быть достигнуты, определены; b) проведен анализ для оценки способности результатов проектирования и разработки выполнить требования; c) проведена верификация в целях обеспечения соответствия выходных данных проектирования и разработки входным требованиям к проектированию и разработке; d) проведены валидации в целях обеспечения того, что готовая продукция и услуги отвечают требованиям к установленному применению или намеченному использованию; e) предприняты необходимые действия по проблемам, выявленным в ходе деятельности по анализу, верификации и валидации; f) документированная информация об этих действиях сохранена. <p>ПРИМЕЧАНИЕ Анализ, верификация и валидация проектирования и разработки имеют четкие цели. Они могут выполняться по отдельности или совместно, насколько это применимо к продукции и услугам организации.</p>	<p>Не определены средства и методы разработки и проектирования.</p>	<p>Определить форму(ы) записей и для обеспечения фиксирования результатов по каждому этапу разработки.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.3.5	<p>Выходные данные проектирования и разработки Организация должна обеспечить, чтобы выходные данные проектирования и разработки:</p> <ul style="list-style-type: none"> a) соответствовали входным требованиям; b) были адекватными для последующих процессов производства продукции и предоставления услуг; c) содержали требования к мониторингу и измерению, насколько это приемлемо, а также критерии приемки или ссылки на них; d) определяли характеристики продукции и услуг, которые имеют важное значение для их предназначения, безопасного и надлежащего предоставления. <p>Организация должна сохранять документированную информацию по выходным данным проектирования и разработки.</p>	<p>Не определены выходные данные для разработки и проектирования.</p>	<p>Определить форму(ы) записей и для обеспечения фиксирования результатов проверки выходных данных, по требованиям данного пункта..</p>
8.3.6	<p>Изменения проектирования и разработки Организация должна идентифицировать, анализировать и управлять изменениями, сделанными во время или после проектирования и разработки продукции и услуг, в той степени, которая необходима для обеспечения исключения негативного влияния на соответствие требованиям.</p> <p>Организация должна сохранять документированную информацию по:</p> <ul style="list-style-type: none"> a) изменениям проектирования и разработки; b) результатам действий по анализу; c) санкционированию изменений; d) действиям, предпринятым для предотвращения неблагоприятного влияния. 	<p>Не ведутся записи по управлению изменением при проектировании и разработке порядка предоставления государственных услуг.</p>	<p>Определить форму(ы) записей и для обеспечения фиксирования записей об изменениях при разработке, так чтобы обеспечить возможность прослеживания этих изменений.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.4.1	<p>Управление внешне поставляемыми процессами, продукцией и услугами</p> <p>Организация должна обеспечить, чтобы поставляемые ей извне процессы, продукция и услуги соответствовали требованиям.</p> <p>Организация должна определить методы управления, которые должны быть применены к внешне поставляемым процессам, продукции и услугам, когда:</p> <p>а) продукция и услуги от внешних поставщиков предназначены для включения в состав собственной продукции и услуг организации;</p> <p>б) продукция и услуги предоставляются потребителю(ям) напрямую внешним поставщиком по поручению (от имени) организации;</p> <p>в) процесс или часть процесса осуществляются внешним поставщиком на основе решения организации.</p> <p>Организация должна определить и применять критерии для оценки, выбора, мониторинга показателей деятельности и переоценки внешних поставщиков на основе их способности осуществлять процессы или поставлять продукцию и услуги в соответствии с установленными требованиями. Организация должна сохранять документированную информацию об этих видах деятельности и всех необходимых действиях, являющихся следствием оценки.</p>	<p>Используется заявление на имя руководства. Есть сметы для одобрения потребностей. Выбор поставщиков и закупка осуществляется посредством платформы D-xarid. Входной контроль осуществляется заявителем. Возможны прямые закупки в период пандемии.</p>	<p>Доработать и документировать механизм осуществления закупок, включая планирование, выбор, оценку и переоценку поставщиков по установленным критериям, а также способы документирования результатов оценки и всех необходимых действий, вытекающих из оценки.</p> <p>Также определить и задокументировать требования к выбору субподрядных организаций (в случае если потребуются передача части деятельности на аутсорсинг).</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.4.2	<p>Вид и степень управления Организация должна обеспечить, чтобы поставляемые извне процессы, продукция и услуги не оказывали негативного влияния на способность организации постоянно поставлять своим потребителям соответствующую продукцию и услуги. Организация должна:</p> <ul style="list-style-type: none"> a) обеспечить, чтобы внешне поставляемые процессы находились под управлением ее системы менеджмента качества; b) определить методы управления, которые предполагает применить как к внешнему поставщику, так и к результатам (выходам) его деятельности; c) принять во внимание: <ul style="list-style-type: none"> 1) степень потенциального влияния внешне поставляемых процессов, продукции и услуг на способность организации постоянно обеспечивать выполнение требований потребителя и применимых законодательных и нормативных правовых требований; 2) результативность методов управления, применяемых внешним поставщиком; d) определить деятельность по верификации или иные действия, необходимые для обеспечения того, что внешне поставленные процессы, продукция и услуги соответствуют требованиям. 	<p>Не установлены требования к управлению процессами, переданными для выполнения подрядчикам.</p>	<p>Необходимо более подробно установить требования к управлению закупкам, и внешне поставляемым процессам с учетом того насколько они могут влиять на качество и своевременность предоставления услуг.</p>
8.4.3	<p>Информация для внешних поставщиков Организация должна обеспечить адекватность требований прежде, чем они будут доведены до сведения внешнего поставщика. Организация должна довести до сведения внешних поставщиков свои требования, касающиеся:</p> <ul style="list-style-type: none"> a) процессов, продукции и услуг, которые должны быть поставлены; b) получения одобрения: <ul style="list-style-type: none"> 1) продукции и услуг; 2) методов, процессов и оборудования; 3) выпуска продукции или оказания услуг; c) компетентности персонала, включая необходимую квалификацию; d) взаимодействий внешнего поставщика с организацией; e) управления и мониторинга показателей деятельности внешнего поставщика, которые будут применяться организацией; f) деятельности по верификации или валидации, которые организация или ее потребитель собираются осуществлять на месте выполнения работ внешним поставщиком. 	<p>Информация для закупок заполняется заявлением руководителю Агентства. Отсутствует конкретная форма заявки с указанием требований к качеству, срокам и условиям поставок. Ввиду этого не ведется анализ заявок.</p>	<p>Рекомендуется определить и установить требования к указанию в заявке подробных характеристик к закупаемым материалам. Ввести систему анализа заявок в виде электронного журнала заявок и поставок с указанием целей закупок (категорий) для удобства анализа.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.5.1	<p>Управление производством продукции и предоставлением услуг Организация должна осуществлять производство продукции и предоставление услуг в управляемых условиях. Управляемые условия в той степени, насколько это применимо, должны включать:</p> <p>а) наличие документированной информации, устанавливающей:</p> <ol style="list-style-type: none"> 1) характеристики продукции, которая должна быть произведена, услуг, которые должны быть предоставлены, или деятельности, которая должна быть осуществлена; 2) результаты, которые должны быть достигнуты; <p>б) наличие и применение пригодных ресурсов для осуществления мониторинга и измерений;</p> <p>в) осуществление на соответствующих стадиях деятельности по мониторингу и измерениям, чтобы верифицировать, что управление процессами или их результатами (выходами) осуществляется в соответствии с критериями, а также что продукция и услуги соответствуют критериям их приемки;</p> <p>г) использование соответствующей инфраструктуры и среды для функционирования процессов;</p> <p>д) назначение компетентных лиц, включая любую требуемую квалификацию;</p> <p>е) проведение валидации и периодической перевалидации способности достигать запланированных результатов у всех тех процессов производства продукции и предоставления услуг, конечные результаты (выходы) которых не могут быть верифицированы последующим мониторингом или измерениями;</p> <p>ж) осуществление действий по предупреждению ошибок, связанных с человеческим фактором;</p> <p>з) осуществление выпуска, поставки и деятельности после поставки.</p>	<p>Существуют регламенты оказания услуг. Отсутствуют инструкции и скрипты для оказания услуг для операторов. Для мониторинга используется информационные системы ЕПИГУ, Регистрация бизнеса, Электронные цифровые подписи. Мониторинг предоставления государственных услуг осуществляют управление контроля за предоставлением государственных услуг государственными органами и другими организациями и отдел контроля за деятельностью центров государственных услуг. Нет единого подхода к инфраструктуре и среде для функционирования процессов. Нет риск ориентированного подхода при разработке гос. услуг учитывающего влияние человеческого фактора. История предоставления гос. услуг сохраняется. Отсутствуют требования по деятельности после предоставления гос. услуг.</p>	<p>Необходимо установить требования к предоставлению государственных услуг в плане организации и обеспечения ресурсами. Необходимо создать механизм оценки влияния человеческого фактора на все процессы, связанные с разработкой и предоставлением государственных услуг. Также необходимо разработать требования к деятельности после предоставления государственных услуг.</p>
8.5.2	<p>Идентификация и прослеживаемость Организация должна применять подходящие способы идентификации выходов в тех случаях, когда необходимо обеспечить соответствие продукции и услуг. Организация должна по ходу производства продукции и предоставления услуг идентифицировать статус выходов по отношению к требованиям, относящимся к мониторингу и измерениям. Организация должна управлять уникальной идентификацией выходов, когда прослеживаемость является требованием, а также сохранять документированную информацию, необходимую для обеспечения прослеживаемости</p>	<p>Существует идентификация всех входов и выходов посредством привязки к номеру заявки для получения гос. услуг. Однако идентификация осуществляется в различных информационных системах.</p>	<p>Необходимо установить требования к идентификации всех выходов при предоставлении гос. услуг и учитывать эти требования при разработке, цифровизации, внедрении, предоставлении гос. услуг и их мониторинге.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.5.3	<p>Собственность, принадлежащая потребителям или внешним поставщикам Организация должна проявлять заботу о собственности потребителей или внешних поставщиков, когда она находится под управлением организации или используется ею. Организация должна идентифицировать, верифицировать, сохранять и защищать собственность потребителей или внешних поставщиков, предоставленную для использования организацией или включения в состав выпускаемой организацией продукции и предоставляемых услуг. В тех случаях, когда предоставленная потребителями или внешними поставщиками собственность была утеряна, повреждена или признана не пригодной для использования, организация должна уведомить об этом потребителей или внешних поставщиков, а также сохранять документированную информацию о том, что произошло.</p>	<p>Отсутствие требований по отношению к собственности потребителей. Информационная система хотя и обеспечивает идентификацию и верификацию собственности потребителей, но также имеет риски потери конфиденциальности ввиду наличия уязвимостей в инфраструктуре Агентства, региональных управлений и центров государственных услуг. Отсутствует механизм и ресурсы для информирования потребителей о потери конфиденциальности или сохранности собственности потребителей.</p>	<p>Создать требования по управлению собственностью потребителей, а также механизма уведомления при потери конфиденциальности и сохранности.</p>
8.5.4	<p>Сохранение Организация должна обеспечить сохранность выходов во время производства продукции и предоставления услуг в той степени, в которой это будет необходимо для обеспечения соответствия требованиям.</p>	<p>Сохранность выходов обеспечивается идентификацией заявок в информационной системе.</p>	<p>Необходимо задокументировать требования к сохранности и механизм его обеспечения.</p>
8.5.5	<p>Деятельность после поставки Организация должна выполнить требования к деятельности после поставки, связанной с продукцией и услугами. При установлении объема требуемой деятельности после поставки организация должна рассмотреть: а) законодательные и нормативные правовые требования; б) потенциально возможные нежелательные последствия, связанные с ее продукцией и услугами; в) особенности продукции и услуг, способы их использования и предполагаемое «время жизни»; г) требования потребителей; д) обратную связь с потребителями.</p>	<p>В настоящее время деятельность после поставки не предусмотрена.</p>	<p>Рекомендуется определить необходимость определения деятельности после поставки</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.5.6	<p>Управление изменениями</p> <p>Организация должна проводить анализ изменений в создании продукции и предоставлении услуг, и управлять ими в том объеме, который необходим для сохранения постоянного соответствия требованиям.</p> <p>Организация должна сохранять документированную информацию о результатах анализа изменений, о лицах, санкционировавших изменение, и о всех необходимых действиях, являющихся следствием анализа.</p>	<p>Требования к управлению изменений при предоставлении государственных услуг не регламентированы.</p>	<p>Необходимо определить механизм реагирования на изменения требований к предоставлению государственных услуг. Необходимо определить кто и как получает информацию, как согласовываются эти изменения, какие дополнительные согласования необходимы, как об этих изменениях своевременно информировать необходимый персонал (тех, кто должен учесть эти изменения).</p>
8.6	<p>Выпуск продукции и предоставление услуг</p> <p>На соответствующих стадиях организация должна осуществлять запланированные мероприятия по верификации того, что требования к продукции и услуге были выполнены.</p> <p>Передача продукции и услуг потребителям не должна осуществляться до тех пор, пока все запланированные мероприятия не будут осуществлены с положительными результатами, если на иное не будет получено согласие соответствующих уполномоченных лиц и/или органов и, где это возможно, потребителей.</p> <p>Организация должна сохранять документированную информацию о выпуске продукции и предоставлении услуги. Документированная информация должна включать:</p> <ul style="list-style-type: none"> a) доказательства соответствия критериям приемки; b) прослеживаемость лиц(а), санкционировавших(его) выпуск продукции и предоставление услуги. 	<p>Хотя во многих услугах присутствует этап контроля перед предоставлением услуг, данный этап не регламентирован.</p>	<p>Необходимо определить механизм контроля предоставления услуг и интегрировать данный механизм в процесс разработки регламентов.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.7.1	<p>Управление несоответствующими выходами</p> <p>Организация должна обеспечить, чтобы выходы, несоответствующие требованиям, были идентифицированы и находились под управлением для предотвращения их непредназначенного использования или поставки.</p> <p>Организация должна осуществить соответствующие действия, исходя из характера несоответствия и его влияния на соответствие продукции и услуг. Это должно относиться также к несоответствующей продукции и услугам, выявленным после поставки продукции, в ходе или после оказания услуг.</p> <p>Организация должна поступать с несоответствующими выходами одним или несколькими из указанных ниже способов:</p> <ul style="list-style-type: none"> a) осуществить коррекцию; b) изолировать, сдерживать, возвращать или приостанавливать поставку продукции и оказание услуг; c) информировать потребителя; d) получить разрешение на признание соответствия на основе разрешения на отклонение <p>В тех случаях, когда несоответствующий выход подвергся коррекции, его соответствие требованиям должно быть верифицировано.</p>	<p>Есть отдел контроля за деятельностью центров общественного обслуживания.</p> <p>Есть график мониторинга работы центра гос. услуг посредством использования метода «таинственный потребитель» - программа выявления несоответствий со стороны таинственного подставного потребителя.</p> <p>Документально не описан порядок управления несоответствующим выходом.</p>	<p>Необходимо разработать процедуру управления несоответствующими выходами.</p>
8.7.2	<p>Организация должна сохранять документированную информацию, которая:</p> <ul style="list-style-type: none"> a) описывает несоответствие; b) описывает осуществленные действия; c) описывает полученные разрешения на отклонение; d) указывает полномочное лицо и/или орган, принявшее решение об осуществлении действий в отношении несоответствия. 	<p>Не определен порядок ведения записей при управлении несоответствующей продукцией (или её составляющими, в том числе связанными с нарушениями технологии производства продукции).</p>	

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
9.1.1	<p>Мониторинг, измерения, анализ и оценка Организация должна определить: а) что необходимо подвергать мониторингу и измерениям; б) методы мониторинга, измерений, анализа и оценки, необходимые для обеспечения достоверности их результатов; в) когда должны проводиться мониторинг и измерения; г) когда результаты мониторинга и измерений должны быть проанализированы и оценены. Организация должна оценивать показатели функционирования и результативность системы менеджмента качества. Организация должна сохранять соответствующую документированную информацию, служащую свидетельством полученных результатов.</p>	<p>Ведется мониторинг выполнения планов, установленных в законодательстве. Не все процессы подвергаются мониторингу и анализу. Не установлен порядок проведения мониторинга, измерения, анализа и оценки данных. Не установлено что будет подвергаться мониторингу, частота проведения и ответственность.</p>	<p>Необходимо определить: что и когда будет подвергаться мониторингу и измерениям в деятельности Агентства, в том числе что и когда из полученных данных необходимо анализировать и на каком уровне, для того чтобы подтверждать, что все запланированные действия выполняются, а в случае отклонения вовремя реагировать на них и предотвращать негативное влияние на достижение главных результатов. Это касается и основных процессов и управленческих бизнес процессов, также для бизнес процессов необходимо установить показатели и критерии к их результативности.</p>
9.1.2	<p>Удовлетворенность потребителей Организация должна проводить мониторинг восприятия потребителями того, в какой степени удовлетворены их потребности и ожидания. Организация должна определить методы получения, мониторинга и анализа этой информации.</p>	<p>Существует инструмент оценки операторов путем 5 бальной оценки. Нет установленных требований к мониторингу удовлетворенности заказчиков.</p>	<p>Необходимо определить методы получения обратной связи, для осуществления мониторинга информации об удовлетворенности потребителя, а также методы использования данной информации, определяющие определение корректирующих и предупреждающих действий для постоянного улучшения.</p>
9.1.3	<p>Анализ и оценка Организация должна анализировать и оценивать соответствующие данные и информацию, получаемую в ходе мониторинга и измерений. Результаты анализов должны быть использованы для оценки: а) соответствия продукции и услуг; б) степени удовлетворенности потребителей; в) показателей и результативности системы менеджмента качества г) успешности планирования; д) результативности действий по реагированию на риски и возможности; е) показателей деятельности внешних поставщиков; г) необходимости улучшений системы менеджмента качества.</p>	<p>Не полностью определен порядок проведения мониторинга, измерения, анализа и оценки данных. (Что будет подвергаться мониторингу, частота проведения и ответственность.) так как процессный подход не внедрен, не применяется анализ и оценка результативности процессов. Не выявлено свидетельств того, что анализируются результаты действий, предпринятых в отношении рисков.</p>	<p>Организация должна определить механизм сбора и анализа данных для оценки результативности ИСМ. При этом необходимо обеспечить, чтобы анализировались все данные перечисленные в пункте 9.1.3 стандарта.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
9.2.1	<p>Внутренний аудит Организация должна проводить внутренние аудиты через запланированные интервалы времени для получения информации о том, является ли система менеджмента качества:</p> <p>а) соответствующей</p> <p>1) собственным требованиям организации к своей системе менеджмента качества;</p> <p>2) требованиям настоящего международного стандарта;</p> <p>б) результативно внедренной и функционирующей.</p>	<p>Отсутствуют свидетельства проведения внутреннего аудита ИСМ</p>	<p>Необходимо разработать документированную процедуру по проведению внутренних аудитов ИСМ Агентства. Далее на основании данной процедуры планировать, организовать и проводить внутренние аудиты. Для проведения самих аудитов необходимо обучить внутренних аудиторов из числа сотрудников Агентства, которые будут составлять группу внутреннего аудита.</p>
9.2.2	<p>Организация должна:</p> <p>а) планировать, разрабатывать и поддерживать программу(ы) аудита, включая частоту, методы ответственности, требования к планированию, и отчетности), которые должны учитывать важность выбранных для проверки процессов, изменения, влияющие на организацию, и результаты предыдущих аудитов;</p> <p>б) для каждого аудита устанавливать критерии и области;</p> <p>в) отбирать аудиторов и проводить аудит так, чтобы была обеспечена объективность и беспристрастность процесса аудита;</p> <p>г) обеспечить, чтобы результаты аудитов были доведены до сведения соответствующих руководителей;</p> <p>д) осуществлять соответствующие коррекции и корректирующих действий без необоснованной задержки;</p> <p>е) сохранять документированную информацию как свидетельства реализации программы аудита и результаты аудита.</p>	<p>Не определен порядок планирования и проведения аудита, в том числе распределение ответственности за разработку плана, программы, составление отчета об аудите. (см. подпункт а) пункта 9.2.2))</p>	<p>Необходимо разработать документированную процедуру по проведению внутренних аудитов ИСМ Агентство. Далее на основании данной процедуры планировать, организовать и проводить внутренние аудиты. Для проведения самих аудитов необходимо обучить внутренних аудиторов из числа сотрудников Агентства, которые будут составлять группу внутреннего аудита.</p>
9.3.1	<p>Анализ со стороны руководства Высшее руководство должно через установленные периоды времени проводить анализ системы менеджмента качества организации, чтобы обеспечить ее сохраняющуюся пригодность, адекватность и результативность, а также связь со стратегическим направлением организации.</p>	<p>Каждый квартал создаются отчеты из системы для предоставления отчетности высшему руководству по результатам работы системы гос. услуг.</p>	<p>Необходимо определить деятельность в отношении анализа со стороны высшего руководства. Определить порядок проведения, периодичность проведения, необходимый перечень входных данных для анализа со стороны высшего руководства, при которых анализ считается полноценным и может проводиться, минимальный состав решений, которые необходимо принимать по результатам таких анализов.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
9.3.2	<p>Входные данные для анализа со стороны руководства Анализ со стороны руководства должен планироваться и проводиться, принимая во внимание:</p> <ul style="list-style-type: none"> а) статус действий, осуществляемых по итогам предыдущих анализов со стороны руководства; б) изменения во внешних и внутренних факторах, касающихся системы менеджмента качества; в) информацию о показателях и результативности системы менеджмента качества, включая тенденции, относящиеся: <ul style="list-style-type: none"> 1) к удовлетворенности потребителей и обратной связи от соответствующих заинтересованных сторон; 2) к степени достижения целей в области качества; 3) к показателям процессов и к соответствию продукции и услуг; 4) к несоответствиям и корректирующим действиям; 5) к результатам мониторинга и измерений; 6) к результатам аудитов; 7) к показателям деятельности внешних поставщиков; г) адекватность выделенных ресурсов; д) результативность действий, предпринятых в ответ на риски и возможности (см. 6.1); е) возможности для улучшения. 	<p>Не представлены данные проведения анализа функционирования ИСМ.</p>	<p>Необходимо определить четкую форму отчетности и сбора входных данных для анализа со стороны руководства. Данные могут собираться и анализироваться в несколько этапов.</p>
9.3.3	<p>Результаты (выходы) анализа со стороны руководства Результаты (выходы) анализа со стороны руководства должны включать решения и действия, относящиеся:</p> <ul style="list-style-type: none"> а) к возможностям для улучшения; б) ко всем необходимым изменениям системы менеджмента качества; в) к потребностям в ресурсах. <p>Организация сохранять документированную информацию, служащую свидетельством результатов анализа со стороны руководства.</p>	<p>Не представлены данные.</p>	<p>Рекомендуем оформлять решения протоколом или приказами, содержащими решения в отношении выходных данных указанных в пункте 9.3.3</p>
10.1	<p>Улучшение Организация должна определять и отбирать возможности для улучшения и осуществлять необходимые действия для выполнения требований потребителей и повышения их удовлетворенности. Это должно включать:</p> <ul style="list-style-type: none"> а) улучшение продукции и услуг в целях выполнения требований, равно как и в целях учета будущих потребностей и ожиданий; б) коррекцию, предупреждение или снижение влияния нежелательных воздействий; в) улучшение показателей и повышение результативности системы менеджмента качества. 	<p>Работа по улучшению ведется, но не носит систематизированный характер, и не основана на анализе контекста, анализе результативности ИСМ, на анализе удовлетворенности потребителей.</p>	<p>Реализация данного пункта обеспечивается выполнением требований целого ряда пунктов стандарта, в том числе требований к планированию деятельности с учетом рисков, установлению мониторинга и измерений, анализа данных о функционировании ИСМ, анализе удовлетворенности потребителей.</p>

Пункт ISO 9001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
10.2.1	<p>Несоответствия и корректирующие действия При появлении несоответствий, включая все те, о которых стало известно из жалоб, организация должна:</p> <p>а) отреагировать на несоответствие и, в том виде, как это подходит:</p> <p>1) осуществить действия по управлению несоответствием и по его коррекции;</p> <p>2) предпринять действия в отношении последствий несоответствия;</p> <p>б) оценить необходимость в действиях по устранению причин(ы) несоответствия с тем, чтобы они(о) не повторились или не возникли где-нибудь в другом месте, на основе:</p> <p>1) анализа несоответствия;</p> <p>2) установления причин возникновения несоответствия;</p> <p>3) выяснения того, нет ли аналогичного несоответствия еще где-то или не может ли оно потенциально возникнуть еще где-то;</p> <p>с) осуществить все необходимые действия;</p> <p>д) проанализировать результативность каждого осуществленного корректирующего действия;</p> <p>е) уточнить, при необходимости, риски и возможности, выявленные в ходе планирования;</p> <p>ф) внести, при необходимости, изменения в систему менеджмента качества.</p> <p>Корректирующие действия должны соответствовать степени влияния выявленных несоответствий.</p>	<p>Не определен порядок управления несоответствиями, проведения корректирующих действий и анализа результативности этих действий.</p>	<p>Необходимо определить требования к управлению несоответствиями и корректирующими действиями.</p>
10.2.2	<p>Организация должна сохранять документированную информацию, служащую свидетельством:</p> <p>а) характера несоответствий и всех последующих действий, связанных с ними;</p> <p>б) результатов всех корректирующих действий.</p>	<p>Не установлены требования к ведению записей в отношении характера несоответствий, проведения корректирующих действий.</p>	<p>Необходимо установить требования к ведению записей в отношении несоответствий, проведения корректирующих действий. Определить форму записей, и ответственного(ых) за ведение записей.</p>
10.3	<p>Постоянное улучшение Организация должна постоянно повышать пригодность, адекватность и результативность системы менеджмента качества. Организация должна рассмотреть результаты анализов и оценки, а также выходные данные анализа со стороны руководства для установления того, имеются ли потребности или возможности, которые должны быть рассмотрены в качестве составной части деятельности по постоянному улучшению.</p>	<p>Работа по улучшению ведется, но не носит постоянный и систематизированный характер, основанный на полном анализе результативности ИСМ.</p>	<p>Реализация данного пункта обеспечивается выполнением требований целого ряда пунктов стандарта, в том числе требований к планированию деятельности с учетом рисков, установления мониторинга и измерений, анализа данных о функционировании ИСМ.</p>

Приложение 2.

Анализ фактического состояния существующей системы менеджмента
«Агентство государственных услуг при Министерстве Юстиции Республики Узбекистан» по требованиям стандарта ISO/IEC 27001:2013

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
4 Организационный контекст			
4.1	Понимание организации и её контекста Организация должна определить внешние и внутренние факторы, касающиеся её деятельности и влияющие на её способность достигать запланированного результата(ов) своей системы менеджмента информационной безопасности.	Нет свидетельств определения внешних и внутренних факторов.	Установить механизм определения внешних и внутренних факторов, касающихся деятельности и влияющих на способность достигать запланированных результатов СМИБ.
4.2	Понимание потребностей и ожиданий заинтересованных сторон Организация должна определить следующее: а) Заинтересованные стороны, имеющие отношение к системе менеджмента информационной безопасности, и б) Требования этих заинтересованных сторон, относящиеся к информационной безопасности.	Нет свидетельств определения заинтересованных сторон и их требований.	Установить механизм определения заинтересованных сторон и их требований, имеющие отношение к СМИБ.
4.3	Определение области применения системы менеджмента информационной безопасности Организация должна определить границы и применимость системы менеджмента информационной безопасности для установления её области применения. При определении этой области организация должна учитывать следующее: а) внешние и внутренние факторы описанные в п. 4.1 б) требования, описанные в п. 4.2, и; в) взаимосвязь и зависимость между деятельностью, осуществляемой организацией, и деятельностью других организаций. Область распространения должна быть доступна в виде документально оформленной информации.	Область распространения не определена и не задокументирована.	Определить область распространения СМИБ учитывая внешние и внутренние факторы и требования заинтересованных сторон и взаимосвязи с другими организациями. Задокументировать область распространения в Политики в области СМИБ.
4.4	Система менеджмента информационной безопасности Организация должна разработать, внедрить, поддерживать и непрерывно улучшать систему менеджмента информационной безопасности в соответствии с требованиями настоящего Международного Стандарта.	Система менеджмента информационной безопасности не разработана.	Необходимо определить процессы системы менеджмента и разработать необходимую документированную информацию для её внедрения, поддержания и постоянного улучшения СМИБ.

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
5. Лидерство			
5.1	<p>Лидерство и приверженность Высшее руководство демонстрирует свою руководящую роль и приверженность в отношении СМИБ посредством:</p> <p>a) обеспечения разработки политики в области информационной безопасности, целей в области информационной безопасности и их совместимости со стратегическим направлением организации;</p> <p>b) обеспечения интеграции требований к системе менеджмента информационной безопасности в процессы организации;</p> <p>c) обеспечения наличия необходимых ресурсов для системы менеджмента информационной безопасности;</p> <p>d) информирования о важности результативного менеджмента информационной безопасности и соответствия требованиям к системе менеджмента информационной безопасности;</p> <p>e) обеспечения достижения запланированного результата(ов) системой менеджмента информационной безопасности;</p> <p>f) направления и поддержки сотрудников во внесении их вклада в результативность системы менеджмента информационной безопасности;</p> <p>g) мотивации постоянного улучшения; и</p> <p>h) поддержки других управленческих ролей для демонстрации лидерства в рамках их сферы ответственности.</p>	<p>Высшее руководство приняло решение по разработке и внедрению требований международных стандартов включая ISO/IEC 27001:2013.</p>	<p>Необходимо установить полномочия и определить необходимые ответственности по обеспечению выполнения требований международных стандартов и её постоянного улучшения.</p>
5.2	<p>Политика Высшее руководство должно разработать политику в области информационной безопасности, которая:</p> <p>a) соответствует цели организации;</p> <p>b) содержит цели в области информационной безопасности (см. 6.2) либо определяет основу для установления целей в области информационной безопасности;</p> <p>c) включает в себя приверженность выполнению применимых требований в отношении информационной безопасности; и</p> <p>d) включает в себя приверженность непрерывному улучшению системы менеджмента информационной безопасности;</p> <p>Политика в области информационной безопасности должна быть:</p> <p>e) оформлена документально;</p> <p>f) доведена до сведения персонала организации; и</p> <p>g) доступна для заинтересованных сторон, при необходимости.</p>	<p>В организации отсутствует Политика в области СМИБ.</p>	<p>Необходимо разработать и оформить Политику в области ИБ, которая содержит в себе основу для установления целей в области ИБ. Довести до сведения персонала и создать механизм доступа для всех заинтересованных сторон.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
5.3	<p>Организационные обязанности, ответственность и полномочия Высшее руководство должно обеспечить, что ответственность и полномочия сотрудников, связанных с информационной безопасностью, были определены и доведены до сведения.</p> <p>Высшее руководство должно определить ответственность и полномочия по:</p> <p>а) обеспечению соответствия системы менеджмента информационной безопасности требованиям настоящего Международного Стандарта; и</p> <p>б) отчётности о функционировании системы менеджмента информационной безопасности для высшего руководства.</p>	<p>Существует отдел кибербезопасности. Для каждого отдела разработаны положения о подразделении. Для каждой должности разработаны должностные инструкции, в которых установлены права и ответственности.</p> <p>Не установлены ответственность и полномочия по обеспечению соответствия СМИБ.</p> <p>Не установлены ответственность и полномочия по отчетности о функционировании СМИБ для высшего руководства</p>	<p>Пересмотреть положения о подразделении и должностные инструкции после разработки документации СМИБ для актуализации ответственности и полномочий касательно обеспечения результативного функционирования СМИБ.</p> <p>Определить представителя руководства по СМИБ.</p> <p>Распределить ответственность и полномочия для сбора данных о функционировании СМИБ для высшего руководства.</p>
6. Планирование			
6.1. Действия по обработке рисков и возможностей			
6.1.1	<p>При планировании мероприятий в рамках системы менеджмента информационной безопасности организация должна учитывать факторы, описанные в п. 4.1 и требования, описанные в п.4.2, а также определить риски и возможности, которые необходимо рассматривать для:</p> <p>а) обеспечения способности системы менеджмента информационной безопасности достигать запланированного результата(ов);</p> <p>б) предотвращения или сокращение возникновения нежелательных результатов; и</p> <p>с) достижения непрерывного улучшения (совершенствования).</p> <p>Организация должна планировать:</p> <p>д) действия по работе с данными рисками и возможностями; и</p> <p>е) каким образом:</p> <p>1) интегрировать и внедрять действия в процессы своей системы менеджмента информационной безопасности; и</p> <p>2) оценивать результативность данных действий.</p>	Отсутствует процесс обработки рисков, направленных на их устранение или смягчение.	Необходимо определить процесс управления рисками. Необходимо определить мероприятия для устранения или смягчения рисков, имеющих отношение к ИБ.
6.1.2	<p>Оценка рисков информационной безопасности Организация должна определить и применять процесс оценки рисков информационной безопасности, который:</p> <p>а) устанавливает и поддерживает критерии рисков информационной безопасности, включающие в себя:</p> <p>1) критерии принятия рисков; и</p>	Отсутствует процесс обработки рисков, направленных на их устранение или смягчение.	Необходимо определить процесс управления рисками. Необходимо определить мероприятия для устранения или смягчения рисков, имеющих отношение к ИБ.

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	<p>2) критерии осуществления оценки рисков информационной безопасности;</p> <p>б) обеспечивает достоверные, актуальные и сопоставимые результаты периодического проведения оценки рисков информационной безопасности;</p> <p>с) определяет риски информационной безопасности:</p> <p>1) применение процесса оценки рисков информационной безопасности для идентификации рисков, связанных с нарушением конфиденциальности, целостности и доступности информации в рамках системы менеджмента информационной безопасности; и</p> <p>2) идентификация владельцев рисков;</p> <p>д) анализирует риски информационной безопасности:</p> <p>1) оценка потенциальных последствий, которые могут возникнуть в результате материализации рисков, определённых в п.6.1.2 с) 1);</p> <p>2) оценка реальной вероятности возникновения рисков, определённых в п.6.1.2 с) 1); и</p> <p>3) определение уровней рисков;</p> <p>е) оценивает риски информационной безопасности:</p> <p>1) сравнение результатов анализа рисков с критериями рисков, установленных в п. 6.1.2 а); и</p> <p>2) устанавливает приоритеты, анализируемых рисков, для последующей обработки рисков.</p> <p>Организация должна сохранять документально оформленную информацию о процессе оценки рисков информационной безопасности.</p>		
6.1.3	<p>Обработка рисков информационной безопасности</p> <p>Организация должна определить и применять процесс обработки рисков информационной безопасности, который позволяет:</p> <p>а) выбрать соответствующий вариант обработки рисков информационной безопасности с учётом результатов оценки рисков;</p> <p>б) определить все средства управления, которые необходимы для внедрения выбранного варианта(ов) обработки рисков информационной безопасности;</p>	<p>Отсутствует процесс обработки рисков, направленных на их устранение или смягчение. Отсутствует заявление о применимости. Не назначены ответственные по управлению рисками (владельцы рисков).</p>	<p>Необходимо определить процесс управления рисками. Необходимо определить мероприятия для устранения или смягчения рисков, имеющих отношение к ИБ. Разработать заявление о применимости. Назначить ответственные по управлению рисками (владельцев рисков).</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	<p>с) сравнить средства управления, определённые выше в п. 6.1.3 b), со средствами управления в Приложении А и убедиться, что необходимые средства управления не пропущены (включены)</p> <p>d) разработать Заявление о Применимости, которое содержит необходимые средства управления (см. п.6.1.3 b) и с)) и обоснование применения, внедрённых либо не внедрённых, а также обоснования исключений средств управления из Приложения А;</p> <p>e) разработать план обработки рисков информационной безопасности; и</p> <p>f) получить от владельца рисков одобрение плана обработки рисков информационной безопасности и принятие остаточных рисков информационной безопасности.</p> <p>Организация должна сохранять документально оформленную информацию о процессе обработки рисков информационной безопасности.</p>		
6.2	<p>Цели в области информационной безопасности и планирование их выполнения</p> <p>Организация должна установить цели в области информационной безопасности для соответствующих должностных обязанностей и на соответствующих уровнях. Цели в области информационной безопасности должны:</p> <p>a) соответствовать политике в области информационной безопасности;</p> <p>b) быть измеримыми (если применимо);</p> <p>c) учитывать применимые требования информационной безопасности и результаты оценки рисков и обработки рисков;</p> <p>d) доводиться до сведения; и</p> <p>e) обновляться при необходимости.</p> <p>Организация должна сохранять документально оформленную информацию о целях в области информационной безопасности. При планировании способов достижения целей в области информационной безопасности организация должна определить:</p> <p>f) что должно быть выполнено;</p> <p>g) какие ресурсы потребуются;</p> <p>h) кто будет ответственным;</p> <p>i) когда действия будут завершены; и</p> <p>j) как будут оцениваться результаты.</p>	<p>Существуют общие планы работ на год. Установленные мероприятия</p> <p>Существуют планы работ и назначенные задания посредством информационной системы.</p>	<p>Разработать цели в области ИБ соответствующие требованиям международного стандарта ISO/IEC 27001:2013</p> <p>Рекомендуется дополнительно отслеживать статус выполнения целей посредством выполнения мероприятий в информационной системе.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
7. Поддержка			
7.1	<p>Ресурсы Организация должна определить и выделить ресурсы, необходимые для разработки, внедрения, поддержания и непрерывного улучшения системы менеджмента информационной безопасности.</p>	Необходимые ресурсы выделяются, но нет системного подхода к управлению ресурсами.	Рекомендуется создать процесс управления ресурсами.
7.2	<p>Компетентность Организация должна:</p> <p>a) определить необходимую компетентность сотрудника(ов), выполняющего контролируемую работу, которая может повлиять на эффективность информационной безопасности;</p> <p>b) обеспечить наличие у таких сотрудников компетенции на основе соответствующего образования, подготовки или опыта;</p> <p>c) где применимо, предпринять действия для достижения необходимой компетентности и оценить результативность предпринятых действий; и</p> <p>d) сохранять соответствующую документально оформленную информацию в качестве свидетельств компетентности;</p>	Персонал Агентства подбирается с учётом требований к должности, также существует система набора на должность. Существуют курсы повышения квалификации юристов. Отсутствует системный подход к выявлению потребности в обучении персонала. Аттестация персонала не осуществлялась.	Рекомендуется создать механизм управления компетенцией персонала с учетом приобретенных знаний и требований к выполняемой деятельности. С учетом минимальных требований пересмотреть деятельность по поиску и набору новых сотрудников.
7.3	<p>Осведомлённость Сотрудники, осуществляющие работу в рамках организационного управления, должны быть осведомлены о следующем:</p> <p>политика в области информационной безопасности;</p> <p>собственный вклад в результативность системы менеджмента информационной безопасности, в том числе преимуществ улучшения эффективности информационной безопасности; и</p> <p>последствиях несоблюдения требований в области применения системы менеджмента информационной безопасности.</p>	Не ведется работа по повышению осведомленности персонала о вкладе в результативность СМИБ ввиду того, что СМИБ ещё не разработана и не внедрена.	Необходимо создать механизм внутренней коммуникации для осведомленности персонала по требованиям стандарта.
7.4	<p>Обмен информацией Организация должна определить необходимость ведения внутреннего и внешнего обмена информацией, связанной с системой менеджмента информационной безопасности, в том числе:</p> <p>a) на какой предмет обмениваться информацией;</p> <p>b) когда осуществлять обмен информацией;</p> <p>c) с кем осуществлять обмен информацией;</p> <p>d) кто должен осуществлять обмен информацией; и</p>	Есть внутренняя система для оповещений заданий и обратной связи по выполняемой работе. Также ведется обмен информацией с внешними организациями. Отсутствует анализ того, какая информация может быть передана и кому.	Рекомендуется создать механизм управления коммуникацией и её методов для обеспечения информационной безопасности. Рекомендуется классифицировать информацию по уровню конфиденциальности и пригодности.

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	е) процесс, с помощью которого должен осуществляться обмен информацией.		
7.5 Документированная информация			
7.5.1	<p>Общие требования Система менеджмента информационной безопасности организации должна включать в себя следующее:</p> <p>а) документально оформленную информацию (документированная информация), которая требуется согласно настоящему Международному Стандарту; и</p> <p>б) документально оформленную информацию, определённую организацией, как необходимую для результативности системы менеджмента информационной безопасности.</p>	<p>Документированная информация, используемая в Агентстве, имеет различные формы и содержания.</p> <p>Нет установленных требований к тому какие документы требуются для выполнения деятельности Агентства.</p>	<p>Необходимо определить порядок управления документированной информацией, в которой определить документацию и формы записей, необходимую для деятельности Агентства.</p>
7.5.2	<p>Создание и обновление При создании и обновлении документированной информации организация должна обеспечить соответствующие:</p> <p>а) идентификацию и описание (например, название, дата, автор или ссылочный номер);</p> <p>б) формат (например, язык, программная версия, графическое оформление) и носитель (например, бумажная, электронная); и</p> <p>с) анализ и утверждение на предмет пригодности и достаточности.</p>	<p>Документированная информация, используемая в Агентстве, имеет различные формы и содержания.</p> <p>Нет установленных требований к тому как должны быть оформлены документы и формы записей.</p>	<p>Необходимо определить порядок управления документированной информацией, в которой определить требования к созданию и актуализации документированной информации.</p>
7.5.3	<p>Управление документированной информацией Необходимо осуществлять управление документированной информацией, которая требуется системой менеджмента информационной безопасности и настоящим Международным Стандартом, чтобы обеспечить:</p> <p>а) её наличие и пригодность для применения на месте и в момент её необходимости; и</p> <p>б) её адекватную защиту (например, от нарушения конфиденциальности, неправильного использования или нарушения целостности).</p> <p>Для управления документированной информацией, организация должна обеспечить следующие виды деятельности, по необходимости:</p> <p>с) распространение, доступ, восстановление и использование;</p> <p>д) хранение и сохранение, в том числе сохранение удобочитаемости;</p> <p>е) управление изменениями (например, управление версиями); и</p>	<p>Документированная информация, используемая в Агентстве, имеет различные формы и содержания.</p> <p>Нет установленных требований к управлению внешней и внутренней документированной информации в плане проверки её пригодности, обеспечения защиты, обеспечения доступа, хранению, актуализации и уничтожению</p>	<p>Необходимо определить порядок управления документированной информацией, в которой определить требования к управлению внешней и внутренней документированной информации согласно требованиям стандарта.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	<p>f) хранение и уничтожение. Документально оформленная информация внешнего происхождения, определённая организацией как необходимая для планирования и функционирования системы менеджмента информационной безопасности должна быть надлежащим образом идентифицирована и управляема.</p>		
8 Функционирование			
8.1	<p>Планирование и управление операциями Организация должна осуществлять планирование, внедрение и управление процессами, необходимыми для соответствия требованиям информационной безопасности и внедрения действий, определённых в п.6.1. Также организация должна внедрить планы для достижения целей в области информационной безопасности, определённые в п.6.2.</p> <p>Организация должна хранить документально оформленную информацию в объёме, позволяющем убедиться в том, что процессы выполнены, как запланировано.</p> <p>Организация должна осуществлять управление запланированными изменениями и анализ последствий неплановых изменений с принятием действий для снижения их негативного воздействия, если необходимо.</p> <p>Организация должна обеспечить определение и управление процессами, переданными на аутсорсинг.</p>	<p>Деятельность в Агентстве управляется на основе принятых законодательных и нормативных требований. Не определены процессы жизненного цикла предоставления государственных услуг.</p> <p>Ведутся записи по отчётности выполненной деятельности. Не полностью установлены требования к объёму осуществляемых записей по результатам выполняемой деятельности.</p> <p>Изменения вносятся в порядке её надобности, но не систематично.</p> <p>Основная часть предоставляемых государственных услуг осуществляют сторонние государственные организации. Деятельность по мониторингу и контролю за этими организациями и результатами их деятельности осуществляется выделенным подразделением.</p>	<p>Необходимо определить все процессы жизненного цикла предоставления государственных услуг.</p> <p>Определить необходимую форму отчетности результатов деятельности по всем процессам жизненного цикла предоставления государственных услуг.</p> <p>Определить порядок внесения изменений в процессы.</p> <p>Рекомендуется установить критерии контроля для всех процессов передаваемых сторонним организациям, дающие объемлющий вид о результативности деятельности всех организаций осуществляющие процессы, которые были переданы в качестве аутсорсинга.</p>
8.2	<p>Оценка рисков информационной безопасности Организация должна осуществлять оценку рисков информационной безопасности с запланированной периодичностью или при предположении, или в случае значительного изменения с учётом критериев, установленных в п. 6.1.2 а).</p> <p>Организация должна хранить документально оформленную информацию о результатах оценки рисков информационной безопасности.</p>	<p>Существует общее понимание о требованиях к информационной безопасности. Ведется работа по обеспечению информационной безопасности. Не ведется оценка рисков информационной безопасности. Нет системного подхода к устранению критических уязвимостей по информационной безопасности.</p>	<p>Необходимо осуществлять оценку рисков информационной безопасности с запланированной периодичностью. Необходимо определить порядок проведения такой оценки и распределить ответственности и полномочия выполнения деятельности по обеспечению информационной безопасности. Необходимо вести и сохранять записи результатов такой деятельности.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
8.3	<p>Обработка рисков информационной безопасности Организация должна внедрить план обработки рисков информационной безопасности.</p> <p>Организация должна хранить документально оформленную информацию о результатах обработки рисков информационной безопасности.</p>	Не осуществляется обработка рисков информационной безопасности.	Необходимо определить план мероприятий для снижения рисков информационной безопасности.
9 Оценка результативности			
9.1	<p>Мониторинг, измерение, анализ и оценка Организация должна проводить оценку эффективности информационной безопасности и результативности системы менеджмента информационной безопасности. Организация должна определить:</p> <p>а) что необходимо подвергнуть мониторингу и измерению, в том числе процессы и средства управления информационной безопасностью;</p> <p>б) методы мониторинга, измерения, анализа и оценки, насколько это применимо, чтобы обеспечить достоверность результатов;</p> <p>с) когда должны проводиться мониторинг и измерение;</p> <p>д) кто должен осуществлять мониторинг и измерение;</p> <p>е) когда должны проводиться анализ и оценка результатов мониторинга и измерения; и</p> <p>ф) кто должен осуществлять анализ и оценку таких результатов.</p> <p>Организация должна хранить соответствующую документально оформленную информацию в качестве свидетельства результатов мониторинга и измерения.</p>	<p>Ведется работа по мониторингу выполнений назначенных заданий. Для этого выделен специальный отдел мониторинга и анализа. Не установлены все требований к тому что необходимо подвергать мониторингу, с какой периодичностью, не определены методы мониторинга для обеспечения достоверности результатов.</p> <p>Осуществляется анализа деятельности отделов по результатам их отчетности.</p> <p>Данная деятельность не систематизирована и не направлена на улучшение результативности процессов.</p>	<p>Рекомендуется определить все критерии для мониторинга с установлением периодичности их мониторинга, определить доступные и пригодные методы мониторинга. Также систематизировать деятельность по анализу и оценке деятельности процессов, на основе собранных данных по мониторингу и результатов деятельности Агентства. Необходимо установить требований к документированию деятельности по мониторингу и измерениям.</p>
9.2	<p>Внутренний аудит Организация должна с запланированной периодичностью осуществлять внутренние аудиты для получения информации о том, что система менеджмента информационной безопасности:</p> <p>а) соответствует:</p> <p>1) собственным требованиям организации к своей системе менеджмента информационной безопасности</p> <p>2) требованиям ИСО/МЭК 27001 – 2013</p> <p>б) результативно внедрена и поддерживается</p> <p>Организация должна:</p>	<p>Существует механизм внутреннего контроля по отслеживанию выполнения заданий.</p> <p>Отсутствует механизм контроля за результативностью СМИБ.</p>	<p>Необходимо разработать порядок внутреннего контроля.</p> <p>Необходимо установить ответственность за обеспечение выполнения деятельности по внутреннему контролю и подготовки сводных результатов контроля.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	<p>с) планировать, разработать, внедрить и поддерживать программу(ы) аудита, в том числе периодичность, методы, ответственность, требования по планированию и отчетность. Программа(ы) аудита должна учитывать значимость соответствующих процессов и результаты предыдущих аудитов;</p> <p>d) определить критерии и область для каждого аудита;</p> <p>е) подбирать аудиторов и осуществлять аудиты, обеспечивая объективность и беспристрастность процесса аудита;</p> <p>ф) обеспечить предоставление отчетов по результатам аудита руководству, на соответствующих уровнях; и</p> <p>g) хранить документально оформленную информацию в качестве свидетельств программы/программ аудита и результатов аудитов.</p>		
9.3	<p>Анализ со стороны руководства Высшее руководство должно осуществлять анализ системы менеджмента информационной безопасности организации с запланированной периодичностью, чтобы обеспечить непрерывность её пригодности, адекватности и результативности.</p> <p>При анализе со стороны руководства должно учитываться следующее:</p> <p>a) статус действий по результатам предыдущих анализов со стороны руководства;</p> <p>b) изменения внешних и внутренних факторов, связанных с системой менеджмента информационной безопасности;</p> <p>с) обратная информация по показателям информационной безопасности, в том числе тенденции в области:</p> <p>1) несоответствий и корректирующих действий;</p> <p>2) результатов мониторинга и измерения;</p> <p>3) результатов аудитов; и</p> <p>4) выполнения целей в области информационной безопасности;</p> <p>d) обратная связь с заинтересованными сторонами;</p> <p>е) результаты оценки рисков и статус плана обработки рисков;</p> <p>ф) возможности для постоянного улучшения;</p> <p>Выходные данные по анализу со стороны руководства должны включать в себя решения, связанные с возможностями непрерывного улучшения и любых необходимых изменениях в системе менеджмента информационной безопасности.</p>	<p>Отчетность по работе анализируется высшим руководством и принимаются решения касательно деятельности Агентства.</p> <p>Отчетность по работе не содержит всех требований по данному пункту. Отсутствует системный подход по сбору данных и создании отчетов.</p>	<p>Рекомендуется установить порядок проведения анализа со стороны руководства, учитывая все требования данного пункта стандарта.</p>

Пункт ISO/IEC 27001	Требование / документированные процедуры	Анализ фактического состояния, наблюдения	Рекомендации
	Организация должна хранить документально оформленную информацию в качестве свидетельства результатов анализа со стороны руководства.		
10 Улучшение			
10.1	<p>Несоответствия и корректирующие действия При выявлении несоответствия организация должна:</p> <p>a) реагировать на несоответствия и, насколько применимо:</p> <p>1) предпринимать меры по контролю мероприятий по устранению и корректировке; и</p> <p>2) снижать уровень ущерба или последствий несоответствий;</p> <p>b) оценить необходимость действий для устранения причины несоответствия, с целью предотвратить его повторное возникновение за счёт:</p> <p>1) анализа несоответствия;</p> <p>2) определения причин несоответствия; и</p> <p>3) определения наличия или возможности возникновения аналогичного несоответствия;</p> <p>c) внедрить все необходимые действия;</p> <p>d) проанализировать результативность всех предпринятых корректирующих действий; и</p> <p>e) если необходимо, внести изменения в систему менеджмента информационной безопасности.</p> <p>Корректирующие действия должны соответствовать уровню ущерба или последствий результатам выявленных несоответствий.</p> <p>Организация должна хранить документально оформленную информацию в качестве свидетельства:</p> <p>f) характера несоответствий и последующих предпринятых действий; и</p> <p>g) результатов корректирующих действий.</p>	<p>В ходе выполнения работ выявляются несоответствия и предпринимаются меры по их устранению.</p> <p>Отсутствует свидетельства по определению причин несоответствий и мероприятий по их устранению.</p>	<p>Необходимо создать порядок управления несоответствиями, в котором установить ответственность и полномочия по решению несоответствий.</p>
10.2	<p>Непрерывное улучшение Организация должна постоянно улучшать пригодность, адекватность и результативность системы менеджмента информационной безопасности.</p>	<p>Работа по улучшению ведется, но не носит постоянный и систематизированный характер, основанный на полном анализе результативности ИСМ.</p>	<p>Реализация данного пункта обеспечивается выполнением требований целого ряда пунктов стандарта, в том числе требований к планированию деятельности с учетом рисков, установления мониторинга и измерений, анализа данных о функционировании ИСМ.</p>

Приложение 3.

Документированная информация СМИБ	Пункт ISO/IEC 27001:2013
Определение контекста	4.1
Внешние и внутренние аспекты	4.2
Заинтересованные стороны, которые имеют отношение к СМИБ	4.3
Границы СМИБ	4.3
Области применения/распространения СМИБ	
Политика в области СМИБ	5.2
Цели СМИБ	6.2
Процедура оценки рисков	6.1.2
План оценки и обработки рисков	6.1.3.e
Отчет по оценке и обработке рисков	8.2, 8.3
Заявление о применимости	6.1.3.d
Процедура управления документированной информацией ИСМ	7.5.3
Набор политик (политика) в области ИБ	A.5.1
<ul style="list-style-type: none"> • Политика в области информационной безопасности • Политика для мобильных устройств (A.6.2.1) • Политика при дистанционной работе (A.6.2.2) • Политика контроля доступом (A.9.1.1) • Политика по использованию, защите и использованию криптографических ключей в рамках всего их жизненного цикла (A.10.1.1, A.10.1.2) • Политика чистого рабочего стола и экрана (A.11.2.9) • Политика резервного копирования информации, ПО и образов систем (A.12.3.1) • Политика безопасности при разработке ПО и систем (A.14.2.1) • Политика ИБ при взаимоотношении с поставщиками (A.15.1.1) 	
Реестр активов	A.8.1.1
Определение владельцев активов	A.8.1.2
Правила допустимого использования активов	A.8.1.3
Правила/схема маркировки информации	A.8.2.2
Процедура управления активами	A.8.2.3
Процедура управления съемными носителями информации	A.8.3.1
Формализованный процесс регистрации пользователя и отмены регистрации	A.9.2.1
Формализованный процесс инициализации доступа	A.9.2.2
Формализованный процесс управления аутентификацией пользователей для доступа к конфиденциальной информации	A.9.2.3
Процедура управления паролями	A.9.4.3
Процедуры для работы в зонах безопасности	A.11.1.5
Процедуры эксплуатации	A.12.1.1
Процедуры контроля установки ПО на ОС	A.12.5.1
Правила, регулирующие установку программного обеспечения пользователями	A.12.6.2
Процедуры и процедуры передачи информации	A.13.2.1
Трудовой договор, включающих ответственность по ИБ NDA (Соглашения о неразглашении или конфиденциальности)	A.7.1.2, A.13.2.4
Процедуры управления изменениями	A.14.2.2

C-191-AGU/IMSA-0.825

Документированная информация СМИБ	Пункт ISO/IEC 27001:2013
Принципы инжиниринга безопасных систем	A.14.2.5
Процедуры для обеспечения результативной и упорядоченной реакции на инциденты информационной безопасности	A.16.1.1
Процедуры и средства контроля для обеспечения требуемого уровня непрерывности информационной безопасности во время неблагоприятной ситуации	A.17.1.2
Перечень законодательных требований	A.18.1.1