УДК 005.6+004.056
DOI 10.53403/9785951505200_578

# АДАПТАЦИЯ И ВНЕДРЕНИЕ СТАНДАРТОВ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА И СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ РФЯЦ-ВНИИЭФ

*Камышева Наталья Сергеевна (NSKamysheva@vniief.ru), Шагаева София Владимировна*

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

В данной работе проведен анализ нормативно-правовой документации, законодательных актов, стандартов отрасли и предприятия, сформированы требования и определены необходимые процедуры. Разработан порядок адаптации стандартов ISO для ИЛ РФЯЦ-ВНИИЭФ, с учетом ориентации на потребителя и построения эффективного взаимодействия со смежными подразделениями института.

**Ключевые слова:** нормативная база, управление предприятием, информационная безопасность, качество представляемых услуг, испытания, сертификация.

# ADAPTATION AND IMPLEMENTATION OF THE STANDARDS OF THE QUALITY MANAGEMENT SYSTEM AND THE INFORMATION SECURITY MANAGEMENT SYSTEM IN THE TESTING LABORATORY OF RUSSIAN FEDERAL NUCLEAR CENTER VNIIEF

*Kamysheva Natalia Sergeevna (NSKamysheva@vniief.ru), Shagaeva Sofia Vladimirovna*

FSUE “RFNC-VNIIEF”, Sarov Nizhny Novgorod region

This work analyzes the regulatory documents, legislative acts, industry and enterprise standards, formulates the requirements and defines the necessary procedures. A procedure has been developed for adapting ISO standards for the Russian Federal Nuclear Center VNIIEF testing laboratory, taking into account customer orientation and building effective interaction with related departments of the institute.

**Key words:** regulatory framework, enterprise management, information security, quality of services provided, testing, certification.

## Введение

Все большее значение приобретает необходимость внедрения эффективных систем управления на предприятиях, которые бы обеспечивали постоянное улучшение многочисленных производственных процессов и как следствие, результатов деятельности. Одним из инструментов эффективного управления в организации является применение Системы менеджмента качества (СМК) и Системы менеджмента информационной безопасности (СМИБ), основанных на потребностях и целях в области качества и информационной безопасности.

Поскольку ФГУП «РФЯЦ-ВНИИЭФ» является аккредитованной испытательной лабораторией (ИЛ РФЯЦ-ВНИИЭФ) в Системах сертификации средств защиты информации ФСТЭК России и Министерства обороны Российской Федерации, качественное и безопасное предоставление услуг по сертификации изделий-ИТ со встроенными механизмами защиты – является приоритетной задачей, стоящей перед предприятием.

Функции ИЛ РФЯЦ-ВНИИЭФ, входящей в состав Института цифровых технологий, возложены на научно-исследовательский отдел разработки решений по информационной безопасности, в котором я являюсь ответственной за управление системами качества и информационной безопасности.

Наиболее применимыми стандартами в области разработки, внедрения, мониторинга и улучшения СМК и СМИБ являются документы Международной Организации по стандартизации (ISO) [3,6], которые являются унифицированными и применимыми к организации любого вида продукции и услуг.

Внедрение эффективной СМК гарантирует потребителю высокое качество товаров и услуг, поэтому прохождение сертификации по [3] может стать серьезным импульсом к увеличению объемов реализации и ускорению развития компании в целом.

В наш информационный век вопросы защиты корпоративных данных и обеспечения бесперебойной работы информационных систем становятся ключевыми для эффективности всей хозяйственной деятельности предприятия [6].

Требования стандартов разделяют информационные ресурсы организации на доступную информацию и конфиденциальную, обеспечивая их безопасность от несанкционированного доступа и неправомерных действий.

С целью соответствия предъявляемым к аккредитованным лабораториям требованиям, на базе стандартов ISO ИЛ РФЯЦ-ВНИИЭФ внедрены, поддерживаются и непрерывно улучшаются процессы СМК и СМИБ. Адаптация и внедрение СМК и СМИБ обеспечивает решение широкого спектра задач, способствует повышению качества оказываемых услуг, а также коррелируется с внутренними регламентирующими документами и стандартами предприятия.

## Анализ нормативно-правовой и отраслевой базы

К общей нормативно-правовой базе относятся:

– действующее законодательство Российской Федерации в части защиты информации, организации договорной и экономической деятельности;

– указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ по вопросам информационных технологий, обеспечения безопасности информации;

– государственные стандарты ЕСКД, ЕСПД, ЕСТД;

– комплексы стандартов на автоматизированные системы, информационные технологии и системы менеджмента качества испытательных лабораторий, стандарты в области разработки безопасного программного обеспечения;

К отраслевой базе относятся:

– приказы и указания руководства Государственной корпорации по атомной энергии «Росатом» и директора РФЯЦ-ВНИИЭФ;

– инструкции по безопасному функционированию РФЯЦ-ВНИИЭФ, защиты государственной и коммерческой тайны, персональных данных, служебной информации ограниченного распространения, интеллектуальной собственности РФЯЦ-ВНИИЭФ;

– правила внутреннего трудового распорядка РФЯЦ-ВНИИЭФ;

– правила и нормы охраны труда и окружающей среды, техники безопасности, промышленной санитарии, пожарной безопасности;

– положения планово-экономической деятельности отдела и института в целом.

Требования к ИЛ предъявляются в следующих документах:

– в нормативной и методической документации по вопросам сертификации средств защиты информации по линии ФСТЭК России, Минобороны РФ;

– в документах системы менеджмента качества ИЛ и РФЯЦ-ВНИИЭФ;

– в документах системы менеджмента информационной безопасности ИЛ и РФЯЦ-ВНИИЭФ;

– в положениях действующих соглашений о намерениях и конфиденциальности;

– в положениях действующих договоров и дополнительных соглашений;

– во внутренних приказах и указаниях подразделения и института.

## Формирование требований

### *Требования к СМК ИЛ РФЯЦ-ВНИИЭФ*

Требования к СМК ИЛ РФЯЦ-ВНИИЭФ устанавливаются [1].

[1] учитывает последние разработки в области информационных технологий, технические изменения, содержит обновленную терминологию, а также внедряет процессный подход.

### *Нормативные документы СМК*

Достижение точных и надежных результатов лабораторных исследований всегда являлось предметом повышенного внимания со стороны государственных, общественных и частных организаций. На сегодняшний день существует много наработок в области регулирования системы качества ИЛ. Они выражаются в виде нормативных документов различного уровня: международные и национальные стандарты, правила аккредитации, постановления надзорных органов, лучшие практики, типовые решения и т. п.

### *Структура документации СМК*

Структура документации СМК [3], представляет собой иерархическую систему взаимосвязанных документов. Часть этих документов в явном виде оговорена в стандарте, другая часть подразумевается. Поэтому структура СМК имеет «постоянную» составляющую, определенную стандартом и «переменную» составляющую, зависящую от конкретной организации.

«Постоянная» составляющая структуры документации СМК:

– Политика в области качества;

– Цели в области качества;

– Руководство по качеству;

– Шесть обязательных процедур СМК;

– Записи по качеству.

«Переменная» составляющая структуры в стандарте: – Как правило, к этим документам относятся различные планы, карты или схемы процессов, рабочие инструкции, отчетные формы, договора, нормативные документы, накладные и пр. То есть можно считать, что под эту «переменную» составляющую подпадает практически вся документация организации.

**Политика в области качества** – это один из стратегических документов организации. В этом документе определяются основные принципы работы и развития ее системы управления в области качества. Как правило, политика в области качества представляет собой декларативный документ. Однако, каждая декларация, заявленная в политике, должна «раскладываться» на конкретные цели, планы и действия по реализации указанных деклараций. Отсюда появляется и прямая связь политики в области качества с целями в области качества.

**Цель в области качества** – это документ, в котором организация устанавливает, задачи по достижению конкретных результатов в области качества. Задачи в области качества направлены на реализацию политики в области качестваи и имеют конкретные показатели, которые можно измерить и достигнуть в ограниченные периоды времени.

**Руководство по качеству** представляет собой документ, описывающий всю СМК организации, а точнее то, каким образом организована СМК, какую структуру она имеет, какова структура документации СМК.

Стандарт [6] требует от организации разработать и внедрить **6 обязательных процедур СМК**:

– управление документацией – процедура предназначена для формализации документационного обеспечения организации. Данная процедура регламентирует вопросы создания, анализа, и проверки документов до начала их официального использования в организации, актуализации и пересмотра документов уже используемых в организации, правила обозначения документов и идентификации каких-либо изменений в действующих документах. Кроме того, в процедуре управления документацией необходимо четко определить правила распространения документов в организации и правила изъятия, либо явной идентификации устаревшей документации. В процедуре обязательно необходимо отразить и порядок идентификации и обращения с документами внешнего происхождения, например, нормативными документами, стандартами, договорами заказчиков и пр.;

– управление записями о качестве – это процедура, которая регламентирует порядок обращения с документальными свидетельствами работы СМК. Процедура управления записями о качестве должна содержать правила идентификации записей и средства управления записями (например, делать записи можно на бумаге, можно в электронной системе), порядок хранения, защиты и восстановления записей о качестве в случае их повреждения. Кроме того, необходимо определить сроки хранения и порядок изъятия и уничтожения записей о качестве;

– управление несоответствующей продукцией – это процедура, которая определяет, кто и как должен действовать, если в ходе работы организации возникли несоответствия. Под несоответствующей продукцией в стандарте понимается не только продукция, но и услуги, и другие результаты работы. Например, результатом работы договорного отдела является договор, тогда в процедуре управления несоответствующей продукцией необходимо определить какие несоответствия могут возникать в договоре, и как необходимо действовать при обнаружении несоответствий;

– проведение внутренних аудитов – в данной процедуре необходимо определить порядок организации внутренних аудитов, требования к аудиторам, методы, критерии, частоту и область применения аудитов. Также, необходимо определить состав документации, которая разрабатывается при проведении аудита и порядок обработки результатов аудита;

– корректирующих действий – эта процедура должна регламентировать порядок проведения работ по устранению несоответствий, связанных с продуктами (услугами) организации, процессами и системой качества. Порядок проведения корректирующих действий должен предусматривать анализ выявленных несоответствий, установление причин их возникновения, разработку действий по устранению несоответствий, запись результатов предпринятых действий и анализ результатов предпринятых действий;

– предупреждающих действий – если процедура проведения корректирующих действий определяет, как должна действовать организация после возникновения несоответствий, то данная процедура должна определять действия для предотвращения возникновения несоответствий. В процедуре необходимо определить методы определения возможных несоответствий, порядок разработки действий по недопущению возникновения несоответствий, порядок ведения записей результатов предпринятых действий и анализ результатов выполнения предупреждающих действий.

## Требования к СМИБ

Требования к СМИБ отражены в [6–12].

Как известно, внедрение и содержание информационных систем, обеспечивающих управление предприятием и взаимодействием между различными подразделениями, требует существенных инвестиций. Большой ущерб наносит и доступ к корпоративной информации посторонних лиц. Именно поэтому наличие продуманной системы информационной защиты ИЛ представляется обязательным условием ее стабильного развития и ключевым элементом безопасности организации в целом.

В то же время внедрение систем по стандарту [3] позволяет ИЛ стать более прозрачной, обеспечивает эффективность информационного взаимодействия с партнерами и способствует развитию и расширению коммерческой деятельности. Корпоративные информационные ресурсы становятся более понятными, доступными и востребованными для сотрудников, благодаря чему существенно возрастает результативность их деятельности.

## Адаптация и внедрение СМК и СМИБ

Сложность систем требует, чтобы все элементы работали правильно, а их взаимодействие было скоординировано. Основная цель СМК и СМИБ ИЛ – гарантировать точность, надежность и своевременность представления результатов испытаний, анализа, исследований или тестирования.

***Структура СМК и СМИБ***

Несмотря на то, что существуют различные типы ИЛ и каждая из них работает в своей области деятельности, структура СМК и СМИБ ИЛ является единой. Она включает в себя элементы, присущие

любой лаборатории от самой маленькой до большого лабораторного центра. Эти основные элементы представляют собой совокупность скоординированных мероприятий, которые служат основой для управления качеством и информационной безопасностью.

Структура СМК и СМИБ ИЛ включает в себя:

– организационную систему. Для того чтобы создать эффективную СМК и СМИБ, в ИЛ должна быть выстроена четкая организационная система, определяющая права, обязанности и полномочия сотрудников, а также их взаимодействия. Она необходима для управления ИЛ, работы механизмов мониторинга и контроля деятельности;

– персонал. Наиболее важным лабораторным ресурсом является квалифицированный и мотивированный на хорошую работу персонал. СМК охватывает многие элементы учета и управления персоналом, а также способствует поощрению и мотивации сотрудников;

– оборудование. В ИЛ применяется много видов различного оборудования, и каждая единица оборудования должна эксплуатироваться, обслуживаться и применяться правильно. Грамотно выстроенная СМК и СМИБ ИЛ гарантирует, что для работы выбирается подходящее оборудование, оно правильно установлено, работает в соответствии с требуемыми условиями, а обслуживание и управление производится своевременно и в полном объеме;

– закупки. Управление поставками различного рода расходных материалов часто является сложной задачей. Они всегда должны быть доступны и пригодны для работы. Излишние запасы могут приводить к увеличению издержек и снижению качества. Процедуры СМК позволяют гарантировать, что все применяемые расходные материалы хорошего качества, а их хранение и использование выполняется таким образом, чтобы сохранять целостность и надежность;

– процессы. Стабильность процессов ИЛ зависит от факторов, которые играют важную роль в обеспечении качества и информационной безопасности. Эти факторы включают в себя: методы организации работы, управление, контроль и мониторинг деятельности, сбор, обработку и систематизацию данных, верификацию и валидацию процессов;

– информацию, документы и данные (документацию лаборатории). Главным продуктом работы ИЛ является информация. Она может быть представлена в виде отчетов, заключений, результатов тестов и пр. Информацией необходимо управлять, чтобы обеспечить ее точность, достоверность и конфиденциальность в отношении третьих лиц. Вместе с тем информация должна быть доступна сотрудникам ИЛ для выполнения работы;

– нештатные ситуации (риски и возможности). Нештатная ситуация – это ошибка или событие, которое не было запланировано в работе. СМК ИЛ необходима для выявления этих проблем или событий, выработки действий по снижению их негативного влияния (или усилению положительного эффекта) и принятия мер, чтобы нештатные ситуации не повторялись;

– оценку работы. Процесс оценки – это инструмент для изучения работы ИЛ и сравнения достигнутых показателей с нормативными требованиями или другими лабораториями. Оценка может быть внутренней (выполняется собственным персоналом) или внешней (проводится сторонней организацией). Стандарты СМК и СМИБ являются важной частью процесса оценки и выступают ориентирами для лаборатории;

– улучшение (совершенствование деятельности). Одной из задач СМК и СМИБ ИЛ является постоянное улучшение процессов. СМК и СМИБ позволяют это делать на систематической основе;

– обслуживание заказчиков (клиентов). В лабораторной практике часто случаются ситуации, когда интересы заказчика упускаются из виду. ИЛ в первую очередь является организацией, которая предоставляет услуги, поэтому важно, чтобы заказчики получали именно ту услугу, которая им нужна. Руководителям ИЛ необходимо точно понимать, кто является ее заказчиком (клиентом), оценить его потребности и свои возможности и выстроить систему обратной связи с заказчиками;

– надежность и безопасность. СМК и СМИБ ИЛ включают в себя множество факторов обеспечения надежности и безопасности. Они позволяет избежать нежелательных последствий от опасностей и рисков, связанных с помещениями ИЛ, применяемым оборудованием, материалами и реагентами, вредными выбросами (отходами), условиями труда сотрудников и пр.

В СМК и СМИБ все аспекты лабораторной деятельности имеют ключевое значение для достижения точности, надежности и своевременности результатов измерения, анализа, тестирования и исследования. Внедрение данных систем не может гарантировать безошибочную работу ИЛ, но они позволяет достигнуть стабильных и повторяемых результатов деятельности.

***Внедрение СМК и СМИБ ИЛ***

Чтобы достичь необходимого уровня компетентности, в ИЛ необходимо реализовать все элементы структуры СМК и СМИБ. Сделать это за короткий срок и сразу невозможно. Поэтому СМК и СМИБ ИЛ строится поэтапно. Процесс внедрения, как правило, разделяется на несколько ключевых шагов. Такой подход позволяет постепенно реализовать все требования нормативных документов, расширяя область действия СМК и СМИБ на все большее число процессов ИЛ.

Процесс внедрения СМК ИЛ может быть разделен на четыре этапа:

– стандартизация основных процессов. На этом этапе устанавливаются требования к процессам, разрабатывается порядок их выполнения и осуществляется реализация процессов. Действия по выполнению процессов «стандартизуются». В первую очередь стандартизуются процессы, без которых невозможно обеспечить адекватные и безопасные услуги для заказчиков;

– создание системы контроля и прослеживаемости работ. Основное внимание на данном этапе уделяется вопросам контроля и гарантий качества. Эффективно контролировать работы можно только в том случае, если ИЛ в состоянии проследить все этапы создания, передачи и изменения информации, сопровождающей процессы. На данном этапе разрабатываются и стандартизуются механизмы контроля основных процессов и связанных с ними процессов обеспечения;

– стандартизация управления ИЛ. Система качества оказывает влияние не только на основные процессы ИЛ и методы контроля, но также и на порядок управления, и структуру. Этот этап позволяет создать адекватные механизмы управления работами ИЛ и выстроить оптимальную структуру;

– создание системы непрерывного совершенствования работы. Данный этап завершает построение системы качества ИЛ. Он включает в себя разработку методов улучшения работы. К таким методам относятся: работа с жалобами, управление несоответствиями и рисками, повышение квалификации персонала, внешние и внутренние аудиты и пр.

После внедрения всех элементов СМК (на основе выбранного стандарта), лаборатория может пройти аккредитацию по международной или национальной системе. Многие ИЛ рассматривают аккредитацию в качестве конечной цели внедрения системы качества. Однако такой подход является неправильным, с точки зрения конкуренции на рынке лабораторных услуг. СМК ИЛ должна постоянно поддерживаться в работоспособном состоянии и совершенствоваться, чтобы ИЛ имела возможность гарантировать своим заказчикам качество услуг, а также сохранять аккредитацию.

Для того чтобы можно было успешно внедрить и обслуживать функциональную СМК был разработан порядок адаптации стандартов ISO для ИЛ.

Важно также:

– чтобы старший руководящий состав принимал участие и вносил свой вклад в проект;

– чтобы были предоставлены соответствующие человеческие ресурсы и адекватное количество времени для того, чтобы разработать, модифицировать и внедрить необходимые процедуры, протоколы и письменные инструкции;

– чтобы была обеспечена соответствующая финансовая поддержка (например, чтобы покрыть расходы на калибровки/услуги, предоставленные третьими сторонами, закупить оборудование и эталонные материалы для внутренних проверок в рамках контроля качества, принять участие в схемах межлабораторных сравнений и покрыть расходы на ежегодную оценку);

– чтобы при обнаружении пробелов в знаниях лаборатории или ее понимании требований системы качества, использовались услуги соответствующих третьих сторон (например, органа по аккредитации, курсов обучения, специалистов), чтобы устранить эти недостатки и укрепить базу технических знаний лаборатории;

– чтобы весь персонал был полностью проинструктирован и принимал участие в разработке новых систем (например, об основах проекта, зачем необходима аккредитация, как она может помочь им, его роли в разработке и внедрении систем и т. п.);

– обеспечить, чтобы внедряемые системы отвечали необходимым требованиям и были легкодоступными для понимания пользователей;

– чтобы персонал прошел полное обучение с целью обеспечить, чтобы он понимал и компетентно выполнял свои обязанности на требуемом уровне и в соответствии с документально подтвержденными инструкциями;

– проводить регулярную оценку/мониторинг операций лаборатории, протоколов и деятельности персонала с целью обеспечить, чтобы деятельность постоянно выполнялась правильно/в соответствии с письменными процедурами, а также, чтобы замеченные проблемы/несоответствия были правильно устранены.

## Заключение

В заключение следует отметить важность наличия в организации внедренной и адаптированной СМК, выстроенной в соответствии с требованиями стандарта ISO 9001, и завоевывающей всемирные позиции СМИБ. Сегодня лидером рынка станут те организации, которые отслеживают не только показатели качества продукции и услуг, но и уровни конфиденциальности, целостности и доступности обрабатываемой информации.

Стоит отметить, что эффективным инструментом управления СМК и СМИБ является прогнозирование и оценка рисков, что требует грамотного подхода и использования лучших международных практик. Совместная адаптация и внедрение СМК и СМИБ поможет решить широкий спектр задач для любой отрасли промышленности или торговли, что в свою очередь приведет к качественному повышению уровня оказываемых услуг.

На сегодняшний день в ИЛ РФЯЦ-ВНИИЭФ запущен процесс актуализации СМК в соответствии с требованиями [1] и была проведена подготовка для успешного прохождения инспекционного контроля от ФСТЭК России, который прошел в марте 2021 году.

В частности, было выполнено:

– актуализация руководства по качеству, обновление политики качества;

– внесение изменений в имеющий комплект документации и разработка дополнительных процедур;

– оптимизация процессов работы ИЛ.

Переход ИЛ РФЯЦ-ВНИИЭФ на стандарт [1] считается еще одним доказательством готовности выполнить требования стандарта в конкретных условиях того или иного проекта. Так, в 2015 году ИЛ РФЯЦ-ВНИИЭФ получила аттестат аккредитации в системе сертификации средств защиты информации от ФСТЭК России, а в 2021-м подтвердили его. Прохождение инспекционного контроля по новой

версии стандарта помогло увеличить эффективность работы ИЛ и позволило соответствовать высоким требованиям заказчиков.

### Список литературы


1. ГОСТ ISO/IEC 17025-2019. Общие требования к компетентности испытательных и калибровочных лабораторий.
2. ГОСТ Р ИСО 9000-2015. Системы менеджмента качества. Основные положения и словарь.
3. ГОСТ Р ИСО 9001-2015. Системы менеджмента качества. Требования.
4. СТП А 40.4480-2008.Система менеджмента качества. Руководство по качеству.
5. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
6. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
7. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
8. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.
9. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
10. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
11. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
12. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.