**Управления информационной безопасностью**

Управление информационной безопасностью — это циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

Согласно ISO 27001, система управления информационной безопасностью (СУИБ) — это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». Система управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO 27001 для **описания СУИБ процессная модель предусматривает непрерывный цикл мероприятий**:

* планирование,
* реализация,
* проверка,
* действие (ПРПД).

Процесс непрерывного совершенствования обычно требует первоначального инвестирования: документирование деятельности, формализация подхода к управлению рисками, определение методов анализа и выделение ресурсов. Эти меры используются для приведения **цикла в действие**. Они не обязательно должны быть завершены, прежде чем будут активизированы стадии пересмотра.

**На стадии планирования** обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются рисков информационной безопасности, предлагается соответствующий план обработки этих рисков. В свою очередь, на **стадии реализации** внедряются принятые решения, которые были определены на стадии планирования. **На стадиях проверки и действия** усиливают, исправляют и совершенствуют решения по безопасности, которые уже были определены и реализованы.

Проверки могут проводиться в любое время и с любой периодичностью в зависимости от конкретной ситуации. В некоторых системах они должны быть встроены в автоматизированные процессы с целью обеспечения немедленного выполнения и реагирования. Для других процессов реагирование требуется только в случае инцидентов безопасности, когда в защищаемые информационные ресурсы были внесены изменения или дополнения, а также когда произошли изменения угроз и уязвимостей. Необходимы ежегодные или другой периодичности проверки или аудиты, чтобы гарантировать, что система управления в целом достигает своих целей.

**Назначение серии стандартов ГОСТ Р ИСО/МЭК 27000-27006**

**Семейство стандартов СМИБ предназначено для помощи организациям любого типа и величины в реализации и функционировании СМИБ.**

Семейство стандартов СМИБ содержит стандарты, которые:

* определяют требования к СМИБ и к сертификации таких систем;
* содержат прямую поддержку, детальное руководство и/или интерпретацию полных процессов «План (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA) и требования;
* включают в себя специальные руководящие принципы для СМИБ;
* руководят проведением оценки соответствия СМИБ.

Глоссарий терминов и определений, приведённый в этом международном стандарте:

* охватывает термины и определения, в большинстве случаев используемые в семействе стандартов СМИБ;
* не охватывает все термины и определения, применяемые в семействе стандартов СМИБ;
* не ограничивает семейство стандартов СМИБ в определении терминов для своего использования.

**ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология,** представляет обзор систем менеджмента информационной безопасности, которые составляют предмет семейства стандартов СМИБ, а также даёт определения терминов.

**ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования,** предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасности и ее контроля, которые могут быть использованы организациями в соответствии с установленными целями и задачами обеспечения информационной безопасности.

**ГОСТ Р ИСО/МЭК 27002-2007 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности,**устанавливает руководящие и общие принципы начинания, реализации, поддержания в рабочем состоянии и улучшения управления защитой информации в организации. Этот международный стандарт может служить в качестве практического руководства по разработке организационных стандартов защиты и практик эффективного управления защитой, а также для того, чтобы помочь создать доверие в межорганизационной деятельности.

**ГОСТ Р ИСО/МЭК 27003 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.** В данном международном стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения системы менеджмента информационной безопасности (СМИБ) соответствии со стандартом ISO/IEC 27001:2005. В нем описывается процесс определения и разработки СМИБ, от запуска до составления планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СМИБ, определяется проект внедрения СМИБ (упоминается в данном международном стандарте, как проект СМИБ), и представлены рекомендации по планированию проекта СМИБ, в результате которого получается конечный план внедрения СМИБ.  
Данный международный стандарт предназначен для использования организациями, применяющими СМИБ. Он применяется ко всем типам организаций (например, коммерческим предприятиям, правительственным органам, некоммерческим организациям) любых размеров. Сложность структуры и риски каждой организации уникальны, и на внедрение СМИБ будут влиять ее особые требования. Небольшие организации могут посчитать, что действия, указанные в данном международном стандарте, применимы к ним и могут быть упрощены. Крупным организациям или организациям со сложной структурой для эффективного выполнения действий, указанных в данном международном стандарте, может потребоваться  
многоуровневая система организации или управления. Однако в обоих случаях соответствующие действия можно планировать, применяя данный международный стандарт. В данном международном стандарте приведены рекомендации и разъяснения; в нем не указано  
никаких требований.  
Данный международный стандарт предназначен для использования в сочетании с ISO/IEC 27001:2005 и ISO/IEC 27002:2005, но не предназначен для изменения или сокращения требований, указанных в ISO/IEC 27001:2005, или рекомендаций, приведенных в  
ISO/IEC 27002:2005. Предъявление требований на соответствие данному международному стандарту не применяется.

**ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения,** содержит рекомендации по разработке и использованию измерений и мер измерения для проведения оценки эффективности реализованной системы менеджмента информационной безопасности, а также мер и средств контроля и управления или их групп ИСО/МЭК 27001.

Эффективно реализованная программа измерений позволит укрепить доверие заинтересованных сторон к результатам измерений, а также даст возможность заинтересованным сторонам применять меры измерений для непрерывного улучшения информационной безопасности и СМИБ.

Накопленные результаты измерений позволят следить за прогрессом в достижении целей информационной безопасности за некоторый период времени в интересах реализации процесса непрерывного совершенствования СМИБ организации.

**ГОСТ Р ИСО/МЭК 27005-2008 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности** обеспечивает рекомендации для менеджмента рисков информационной безопасности, которые включают информацию и менеджмент рисков безопасности технологий телекоммуникации. Эти рекомендации предназначены, чтобы помочь реализовать достаточную информационную безопасность, основанную на подходе менеджмента рисками.

Этот международный стандарт является применимым ко всем типам организаций (например, коммерческие предприятия, правительственные агентства, некоммерческие организации), которые намереваются осуществлять менеджмент рисками, ставящими под угрозу информационную безопасность организации.

**ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности** устанавливает требования к органам, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности, и способствует проведению аккредитации органов сертификации.  
Любой орган, осуществляющий сертификацию СМИБ, должен продемонстрировать в плане компетентности и надежности свое соответствие требованиям к органу, осуществляющему сертификацию СМИБ.  
Настоящий документ может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки или других процессов аудита.