Внедрение и сертификация СМИБ

написано GlobalTrust.ru | 20.08.2023

Что такое система менеджмента информационной безопасности?

Менеджмент информационной безопасности — 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/IEC 27001, система менеджмента информационной безопасности (СМИБ) — 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.

Цели сертификации системы менеджмента информационной безопасности

Для подтверждения соответствия существующей в организации системы управления информационной безопасностью требованиям международного стандарта ISO/IEC 27001, а также ее адекватности существующим бизнес

рискам используется процедура добровольной сертификации.

Под сертификацией СМИБ организации по требованиям международного стандарта ISO/IEC 27001 понимается комплекс организационно-технических мероприятий, проводимых независимыми экспертами, в результате которых, посредством специального «Сертификата соответствия», подтверждается наличие и надлежащее функционирование всех рекомендуемых Стандартом механизмов контроля, применимых в данной организации. Целью работ по сертификации также является совершенствование СУИБ организации в соответствии с рекомендациями стандарта ISO/IEC 27001.

Преимущества сертификации

Сертификация полностью оправдывает вложенные в эту процедуру средства и время. В результате организации получают ряд неоспоримых преимуществ:

- Происходит официальная регистрация СУИБ организации в реестре авторитетных органов, таких как служба аккредитации Великобритании (UKAS), что укрепляет имидж компании, повышает интерес со стороны потенциальных клиентов, инвесторов, кредиторов и спонсоров
- В результате успешной сертификации расширяется сфера деятельности компании за счет получения возможности участия в тендерах и развития бизнеса на международном уровне

Процедура сертификации оказывает серьезное мотивирующее и мобилизующее воздействие на персонал компании: повышается уровень осведомленности сотрудников, эффективнее выявляются и устраняются недостатки и несоответствия в системе управления информационной безопасностью, что в перспективе означает для организации снижение среднестатистического ущерба от инцидентов безопасности, а также сокращение накладных расходов на эксплуатацию информационных систем. Вполне возможно, наличие сертификата позволит застраховать информационные риски организации на более выгодных условиях.

Как свидетельствует текущая практика, расходы на сертификацию в большинстве случаев несопоставимо малы в сравнении с затратами

организации на обеспечение информационной безопасности, а получаемые преимущества многократно их компенсируют.

Внедрение СМИБ и подготовка к сертификации

Создание и эксплуатация СМИБ требует применения такого же подхода, как и любая другая система менеджмента. Используемая в ISO/IEC 27001 для описания СМИБ процессная модель предусматривает непрерывный цикл мероприятий: планирование, реализация, проверка, действие (ПРПД).

Процесс внедрения СМИБ и подготовка к сертификации включает в себя ряд последовательных этапов.

Этап 1. Инициирование процедуры сертификации

- Определение и документирование границ проведения обследования и сертификации, наиболее критичных для организации бизнес процессов и информационных подсистем
- Подготовка интервью с сотрудниками организации
- Подготовка исходных данных для проведения обследования
- Планирование ресурсов и сроков проведения работ
- Заключение договоров, разработка технического задания и планов работ по аудиту, подготовке и проведению сертификации

Этап 2. Оценка текущего состояния СУИБ и анализ расхождений

- Сбор и анализ исходных данных по объекту обследования
- Сбор и анализ действующих организационно-распорядительных документов по обеспечению информационной безопасности
- Проведение интервью с сотрудниками организации, отвечающими за обеспечение информационной безопасности, с использованием специально разработанных опросных листов
- Определение и документирование статуса механизмов контроля, определяемых Стандартом
- Определение применимости конкретных механизмов безопасности,

описанных в Стандарте, в данной организации
- Определение действующей законодательной базы применимой к деятельности организации
- Подготовка отчетных документов по результатам обследования, содержащий оценку степени несоответствия СМИБ организации требованиям Стандарта (Отчет о расхождениях)

Этап 3. Оценка рисков

- Анализ информационных, программных и технических ресурсов организации, оценка их стоимости, построение модели ресурсов
- Идентификация угроз и уязвимостей, оценка вероятности осуществления угроз и величины уязвимостей, разработка модели угроз и модели нарушителя безопасности
- Оценка величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость
- Определение комплекса механизмов безопасности, адекватных существующим рискам
- Идентификация механизмов контроля, применимых в данной организации, и дополнительных механизмов контроля, необходимых для минимизации рисков

Этап 4. Подготовка программы совершенствования СУИБ

- Разработка программы совершенствования СУИБ и устранения существующих недостатков
- Разработка детального плана мероприятий по реализации программы и подготовке к сертификации
- Выделение ресурсов для внедрения недостающих механизмов контроля

Этап 5. Внедрение механизмов контроля, необходимых для обеспечения соответствия ISO/IEC 27001

- Разработка политики информационной безопасности организации

- Разработка и внедрение недостающих документов по обеспечению информационной безопасности, доработка действующей документации (инструкций, процедур, регламентов, политик, стандартов и т.п.)
- Определение и документирование организационной структуры управления информационной безопасностью (назначение ответственных, распределение ролей)
- Устранение недостатков и несоответствий, выявленных на этапе оценки текущего состояния
- Проектирование и внедрение недостающих механизмов контроля организационного и программно-технического уровня
- Проведение мероприятий по обучению сотрудников организации вопросам применения ISO/IEC 27001

Этап 6. Подготовка финального аудита

- Подготовка всей необходимой документации по СМИБ
- Выбор органа сертификации и заключение с ним соглашения на проведение сертификации

Процедура сертификации системы менеджмента информационной безопасности

Процедура сертификации по стандарту ISO/IEC 27001 выполняется органом сертификации, имеющим соответствующую аккредитацию включает в себя следующие этапы:

- Обращение в орган по сертификации и заполнение заявки на сертификацию
- Предоставление и согласование калькуляции работ по сертификации
- Назначение команды аудиторов
- Предварительная оценка (опционально)
- Сертификационный аудит (включает 2 фазы)

- Регистрация СМИБ и выдача сертификата соответствия

Действительность вашего сертификата, который остается в силе на протяжении трех лет, подтверждается посредством выполнения программы визитов Последующей Периодической Оценки. По итогам трёхгодичного цикла Ваш сертификат будет продлен при условии положительных результатов ре-сертификационного аудита.

Наш опыт создания систем менеджмента информационной безопасности

Мы были одной из первых российских компаний, которые еще в 2004 году стала проводить работы по внедрению процессов менеджмента информационной безопасности и их аудиту в соответствии с требованиями британского стандарта BS 7799. Начиная с 2005 года GlobalTrust готовит первые российские компании к сертификации по требованиям британских и международных стандартов BS 7799/ISO 27001. Нами накоплен уникальный опыт в области аудита безопасности, оценки рисков, внедрения механизмов управления безопасностью и подготовки к сертификации по международным стандартам.

Работы по созданию систем управления информационной безопасностью и их подготовке к сертификации проводятся GlobalTrust по согласованной с российским отделением BSI MS методологии в полном соответствии с требованиями международных стандартов серии ISO/IEC 27000.

Заказ услуг

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму