Консалтинг ИБ нового уровня

Когда информационная безопасность работает

Консалтинг информационной безопасности нового уровня: современные решения для вашего бизнеса

Наша цель — не просто соблюдение формальных требований, а создание реально функционирующей системы защиты информации, которая будет обеспечивать непрерывность бизнес-процессов и предотвращать возможные угрозы.

Организационные вопросы информационной безопасности

На этом этапе необходимо определить, какие организационные меры будут приняты для обеспечения информационной безопасности в компании. Какие подходы будут выбраны для реализации информационной безопасности. «Шашечки или ехать?».

Бизнес-процессы компании

Необходимо провести анализ бизнес-процессов компании и определить, как они связаны с информационной безопасностью.

Определить верхние уровни рисков, направления развития бизнеса. Провести «симбиоз» бизнес-процессов и информационной безопасности.

Бизнес-процессы компании с точки зрения информационной безопасности

Этот этап включает в себя более детальный анализ бизнес-процессов с учётом требований информационной безопасности. Необходимо определить уязвимости и недостатки каждого процесса и разработать меры и стратегию по их устранению.

Документация в части ИБ (политики, регламенты и пр.)

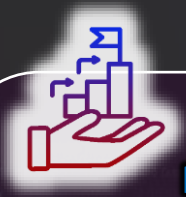
На этом этапе проводится проверка имеющейся документации, выявление недостатков и их исправление, а так же предложения к разработке недостающих документов.

ИТ-архитектура и инфраструктура, её состав

ИТ-инфраструктура компании включает в себя программные и технические компоненты. Необходимо провести аудит этой инфраструктуры и выявить не только уязвимые места, но и корректность конфигураций компонентов, достаточность инфраструктуры для стабильного функционирования бизнеса.

ИБ-архитектура и инфраструктура, её состав

Аналогично ИТ-архитектуре необходимо провести аудит ИБ-инфраструктуры и определить её состав, достаточность и рациональность использования тех или иных систем.



Планы развития информационной безопасности, стратегия ИБ

Стратегия ИБ определяет долгосрочные цели и задачи в области информационной безопасности. Планы развития включают в себя конкретные мероприятия, которые будут реализованы для достижения этих целей.

Взаимодействие и влияние других подразделений на подразделение информационной безопасности

Служба безопасности отвечает за общую безопасность компании, включая физическую охрану, контроль доступа и т.п. Другие подразделения, например, отдел кадров или бухгалтерия, также могут влиять на информационную безопасность, обрабатывая персональные данные сотрудников или финансовые операции. Необходимо проанализировать взаимодействие между этими подразделениями и отделом информационной безопасности.

Что в итоге?

По завершению всех этапов Вы получите структурированный ОТЧЕТ, с выводом информации о текущем состоянии уровня зрелости информационной безопасности и перечнем рекомендаций по оптимизации и конфигурации процессов информационной безопасности, которые нацелены на увеличение уровня зрелости, рациональное и рабочее состояние организационных и программно-аппаратных мер и средств защиты информации:

Оставить заявку

Site: consultib.ru

Email: sale@consultib.ru

Tel./WA: +7 (991) 630-29-12
Telegram: @ConsultIS