Комплексные услуги

Стоимость и сроки реализации работ определяются спецификой проекта в каждом конкретном случае и формируются на базе согласованного с Заказчиком технического задания.

Мы предлагаем провести комплексную разработку и внедрение системы безопасности информации Вашей компании для достижения максимальной отдачи с вложенных в безопасность стредств.

Примерная схема работ, по этапам:

- Предварительное обследование, заключения договора;
- Полное обследование, составление технического задания на систему защиты информации;
- Подбор и закупка оборудования, программного обеспечения с экономическим обоснованием выбора;
- Составление документации: политики безопасности, инструкций, модели угроз безопасности, документов по защите персональных данных, других видов профессиональных тайн;
- Внедрение оборудования и программного обеспечения, настройка, тестирование;
- Обучение сотрудников, подписание сотрудниками документов, регламентирующих ответственность, тестовая эксплуатация системы;
- Введение в эксплуатацию системы, настройка, доводка по пожеланиям сотрудников заказчика;
- Обслуживание оборудования и программного обеспечения, контроль соблюдения режима безопасности, реагирование и расследование инцидентов безопасности, донастройка и изменение параметров системы с учётом изменений в бизнес процессах или законодательстве.

При разработке комплексного решения мы максимально подгоняем условия под клиента, подбирая оптимальную защиты от актуальных угроз, комбинируя средства защиты информации со средствами физической защиты и наблюдения для достижения наилучшего эффекта.

Описание

Информационная безопасность, как и любая деятельность связанная с безопасностью, значительно выигрывает от комплексного подхода, стандартизации и тщательного контроля.

Грубо можно разделить создание системы безопасности информации на три этапа:

- Планирование
- Внедрение
- Контроль/настройка

Все этапы одинаково важны для эффективной защиты. Часто в сфере информационных технологий бывает следующая картина: начинает создавать инфраструктуру один подрядчик, далее

принимает дела другой, при расширении привлекают третьего и так далее. В результате заказчик имеет лишние операционные расходы, завышенные сроки, отсутствие или некачественно составленную техническую документацию, избыточность инфраструктуры, дорогое обслуживание и слабый контроль за системой. Поскольку защита информации тесно связана с информационными технологиями, то и занимаются ей зачастую одни и те же сотрудники. Так что нередки случаи когда системные администраторы не знают настроек безопасности ранее установленного оборудования или пароли утеряны. В сетевое оборудование могут быть подключены чужие, бесхозные линии связи, устройства, через которые злоумышленники могут месяцами следить за деятельностью компании. Нагромождение программных продуктов даёт внутренние сбои и простои сервисов. Средства контроля доступа настраиваются периодически, при возникновении инцидента. Уволенные сотрудники сохраняют привелегии в ответственных системах, для сохранения возможности доступа к старым файлам или просто "по тому что забыли отключить". Особенно опасен такой подход при точечной модернизации устройств в сети и недостаточно ответственной настройки систем информационной безопасности под новые параметры. Отсюда возникают ситуации когда новые устройства получают ничем не ограниченные права доступа к информации в сети. Обнаруживается это, как правило, после инцидента безопасности.