



IT-аутсорсинг систем информационной безопасности

Разглашение корпоративной тайны предприятия, утечка стратегически важных сведений конкурентам, распространение конфиденциальных данных в сети Интернет – все это может нанести существенный ущерб состоянию бизнеса. В связи с этим исключительно важное значение приобретает обеспечение и поддержка информационной безопасности IT-инфраструктуры.

Другие услуги Бизнес-консультирования



IT-аутсорсинг систем информационной безопасности от FTL Company Ltd. – это не только текущая поддержка и профилактика, но и оперативное восстановление IT-инфраструктуры после попыток взлома или вирусных атак. Мы гарантируем Вам бесперебойное функционирование программного обеспечения и оборудования на Вашем предприятии, даже если предстоит проведение длительных технических работ.

FTL Company Ltd. предоставляет широкий спектр услуг по внедрению и техническому сопровождению систем информационной безопасности. Вам гарантирована высокая стабильность и надежность функционирования программного обеспечения и оборудования, которое мы обслуживаем.

Деятельность специалистов по защите конфиденциальных данных предприятия-заказчика складывается из следующих этапов:

1. Разработка, поддержка и регулярное обновление системы антивирусной защиты. IT-специалисты FTL Company Ltd. обеспечат эту систему актуальными базами данных, а также настройками сканирования оборудования и другими опциями, которые соответствуют конкретным требованиям Вашей IT-инфраструктуры.
2. Защита всех составляющих IT-инфраструктуры от несанкционированного доступа. Как правило, в условиях офиса для пользователей, занимающих разные должности, исходя из политики информационной безопасности, устанавливаются разные права доступа к программам и оборудованию. Наши IT-инженеры работают таким образом, чтобы все эти требования были соблюдены, но не в ущерб эффективности работы офиса в целом.
3. Система «Антиспам», или защита почтового сервиса предприятия от нежелательных писем. В рамках этой услуги специалисты FTL Company Ltd. устанавливают для почтовых ящиков пользователей параметры, касающиеся того, какие письма могут поступать на электронный адрес, а какие следует задержать в разделе «Спам», чтобы не перегружать почтовый сервер и корпоративную сеть в целом.
4. Использование специализированных решений для защиты бизнес приложений, баз данных, web-порталов, систем резервного копирования, защиты от утечки конфиденциальных данных (DLP), систем предупреждения и предотвращения вторжения (IDS/IPS, HIPS, DDoS), шифрование данных и др.

Помните, что для успешного бизнеса безопасность играет ключевую роль, поэтому конфиденциальности и сохранению корпоративной тайны на предприятии необходимо уделять максимум внимания. Аутсорсинг IT-инфраструктуры от FTL Company Ltd. всегда к Вашим услугам!



www.ftl.ua
+380 (44) 538-13-00



©2020 FTL Company Ltd.

Информация, приведенная в данном документе, может быть изменена без предварительного уведомления. Ничто в настоящем документе не должно толковаться как составляющее дополнительную гарантию. Компания FTL не несет ответственности за технические или редакционные ошибки или упущения, содержащиеся в настоящем документе.