

МОДЕЛЬ БЕЗОПАСНОСТИ В НЕФТЕГАЗОВОЙ ОТРАСЛИ



Евгений ПИТОЛИН,
управляющий директор
Kaspersky
в Казахстане, Центральной Азии и Монголии

050010, Республика Казахстан,
г. Алматы, Казыбек би, 20а (Медеуский район)

Разработка стратегии защиты от киберугроз для нефтегаза – непростая задача, особенно для его промышленных систем и интернета вещей. В процессах проектирования, разработки, интеграции, использования и сопровождения таких систем принимает участие большое количество сторон.

Оценка рисков, связанных с атаками, у разных участников отличается, при этом безопасность для бизнеса определенных игроков может быть как отрицательным стимулом (увеличение времени выхода на рынок для продукта из-за необходимости реализовать требования безопасности), так и положительным (безопасный продукт – это еще и конкурентное преимущество с точки зрения маркетинга).

ПОЧЕМУ И ЗАЧЕМ НУЖНА МОДЕЛЬ ЗРЕЛОСТИ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Так, производители продуктов для автоматизации технологического процесса до сих пор пытаются переложить ответственность за обеспечение безопасности своих продуктов на клиентов, утверждая, что их продукт должен быть использован в изолированной (от интернета, от офисной сети и т. д.) среде. При этом они упорно игнорируют объективную реальность, в которой большинство предприятий в погоне за увеличением эффективности своей работы оказываются не в состоянии эти требования выполнить.

Читайте далее в журнале «Нефть и газ», №5, 2019 год