


# Низкий баррель — не помеха

Несмотря на нестабильные котировки цен на нефть на мировом рынке в 2016 году, отраслевые компании продолжают поддерживать и даже наращивать инвестиции в технологии защиты своих объектов. Чтобы оправдать возросшие ожидания заказчиков, игрокам рынка систем безопасности необходимо следовать за основными трендами. В их числе — продвинутые компетенции в сфере кибербезопасности, многофункциональность систем, контроль за внутренними процессами, повышение уровня организационной культуры на промышленных предприятиях.

 Текст: Екатерина Покровская

**Low Barrel Is not a Problem for Security. The development of global industrial security market. Trends and problems / By Ekaterina Pokrovskaya**

Despite unsustainable oil prices in 2016, industrial companies continue to increase their investments in security technologies. But their requirements for technologies and equipment become tougher. That's why suppliers and manufactures need to provide additional functions and quality.

## БАРЕЛЬ ПАДАЕТ, ИНВЕСТИЦИИ РАСТУТ

В феврале 2016 года цена на нефть достигла минимума за последние 12 лет, упав ниже отметки 27 долларов за баррель. Несмотря на то что с тех пор его стоимость подросла до 50 долларов, это все равно в два раза ниже котировок 2014 года, когда цена за баррель на рынке равнялась 100 долларам.

Однако падение стоимости «черного золота» практически не отразилось на объемах инвестиций компаний ТЭК в технологии безопасности. Как отмечает Рассел Ост, управляющий вертикальной интеграцией глобальных нефтегазовых проектов компании Pelco by Schneider Electric, величина инвестиций соответствует реально занимаемой доле компании на рынке. «По мере того как растут запасы нефти и газа, компании этой отрасли будут продолжать вкладывать деньги в инфраструктуру безопасности и делать капитальные вложения. Хотя делается это без особого энтузиазма. Труднее всех пришлось компаниям, которые находятся в государственной собственности», — считает эксперт.

По оценкам агентства MarketsandMarkets, сильно выросли инвестиции в безопасность на рынках Центральной Азии, Африки, Латинской Америки — регионах, где мишенью террористов часто являются нефтегазовые объекты. В агентстве также подчеркивают, что США займут самую большую долю на рынке решений безопасности для нефтегазовой промышленности.

«Многие компании значительно урезали бюджеты, что усложняет масштабный выпуск на рынок продукции визуального наблюдения, основанной на облачных технологиях, — комментирует Джереми Бернارد из Osprey Informatics. — Тем не менее экономический спад также обусловил появление новых возможностей в двух направлениях. Во-первых, отмечается увеличение воровства на нефтяных промыслах, что подстегивает спрос на бюджетные системы видеонаблюдения. Во-вторых, заказчики стремятся сэкономить на операционных расходах с помощью технологий, которые позволяют управлять большим количеством активов с участием меньшего количества персонала».

«В то время как темпы добычи нефти снизились, спрос на нефтепродукты и продукцию газопереработки продолжает расти. Поэтому у производителей по всему миру сохраняется необходимость защищать свои инвестиции в производственные активы», — сказал Рассел Ост.

По словам Амита Маттатия, президента и исполнительного директора компании Orgal Optronic Industries, даже во время экономического спада в нефтегазовой промышленности безопасность остается приоритетным направлением для компаний из-за растущих угроз терроризма, пиратства и саботажа.

Аналитики MarketsandMarkets подтверждают эти высказывания. По их прогнозам, объем мирового рынка технологий и услуг безопасности в нефтегазовом секторе к 2020 году увеличится до 33,9 млрд долларов, а среднегодовой прирост оценивается на уровне 5,2%. Для сравнения: в 2015 году объем рынка составил около 26,3 млрд долларов.

## ШАГАЯ В НОГУ С ТРЕНДОМ

Концепция интернета вещей (англ. — *Internet of Things, IoT*) за последние несколько лет стала очень популяр-

на в промышленном применении, равно как и концепции больших данных и облачных вычислений. Применительно к технологиям безопасности эти тенденции усваиваются медленнее по причине высоких затрат и опасений компаний, связанных с информационной безопасностью данных.

«Мы рассматриваем видеонаблюдение в нефтегазовой индустрии как ключевой элемент продвижения технологий интернета вещей. Машинное зрение — также важная часть современных технологий для эффективного анализа активов и деятельности предприятия. Наша компания активно использует эту технологию во многих текущих проектах наших заказчиков», — отмечает Джереми Бернارد.

Рассел Ост убежден, что заказчикам необходимо обеспечивать не только безопасность периметра удаленных объектов, но и безопасность инфраструктуры внутри него. «Это нужно, чтобы быстрее и эффективнее предотвращать, реагировать и расследовать инциденты, связанные с нарушением правил безопасности самими сотрудниками предприятий», — считает он.

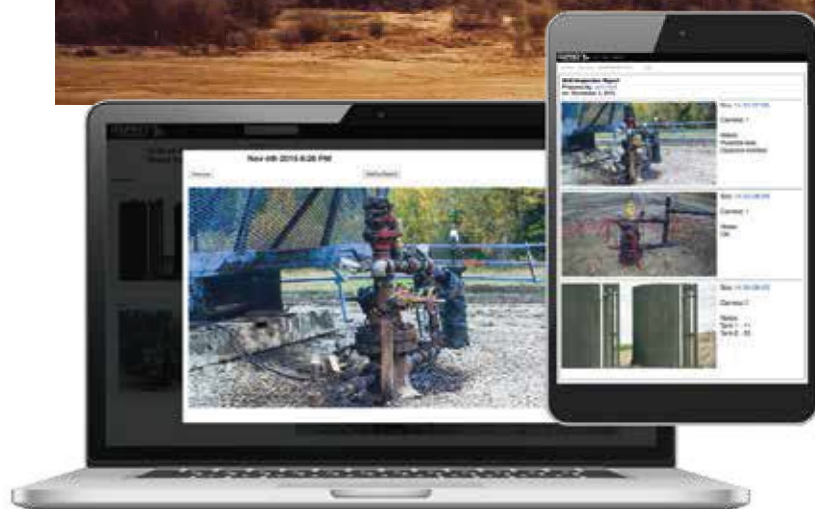
## Падение стоимости «черного золота» практически не отразилось на объемах инвестиций компаний ТЭК в технологии безопасности

Амит Маттатия отметил резкий скачок спроса на высокочувствительные неохлаждаемые системы мониторинга для обнаружения угроз на промышленных объектах и трубопроводах. По его словам, они постепенно вытесняют с рынка дорогие и нуждающиеся в частом техническом обслуживании охлаждаемые системы. «Промышленности нужны технологии, рассчитанные на большие площади, с минимумом техобслуживания и по доступной цене», — комментирует Маттатия.

## ХАКЕР ПРОМЫШЛЕННОГО МАСШТАБА

Рост спроса на новые технологии среди промышленных компаний вызвал повышенное внимание к ним со стороны киберпреступников. По мнению аналитиков исследовательского агентства MarketsandMarkets, этот фактор является одним из основных драйверов рынка оборудования и услуг для нефтегазового сектора. Бывший глава американского Агентства национальной безопасности генерал Кит Александер неоднократно выступал с заявлениями, что электрические сети, нефтеперерабатывающие заводы и электростанции считаются главными мишенями кибертеррористов. По данным некоторых исследований, к 2018 году нефтегазовой промышленности потребуется инвестировать 2 млрд долларов на обеспечение информационной безопасности.

Тем не менее существует мнение, что к вопросу серьезности проблемы кибербезопасности в нефтегазовом секторе остаются глухи. «Кибербезопасности в нефтегазовом секторе должно отводиться такое же внимание, как и к безопасности в целом. В промышленной безопасности компании имеют более четкий и действенный контроль, чем в информационном



пространстве. Поэтому оно не рассматривается компаниями наравне с мерами по физической защите промышленных объектов, — рассказывает Чарльз Дробни, президент и исполнительный директор компании Globalogix. — Руководство часто просто отказывается признать наличие риска и факторов уязвимости». Дробни полагает, что шансы масштабного внедрения систем многоуровневого контроля за информационным пространством предприятий пока невелики. По мнению специалиста, такая ситуация будет сохраняться до тех пор, пока какая-нибудь крупная нефтегазовая компания не подвергнется серьезной кибератаке с существенными последствиями.

### БОЛЬШЕ, ЧЕМ БЕЗОПАСНОСТЬ

Видеонаблюдение является ключевым компонентом любой системы безопасности, в том числе в нефтегазовой промышленности. Однако, как и в других отраслях, возможность применения камеры в целях помимо безопасности делает этот товар более привлекательным с точки зрения продаж.

«Мы продолжаем работать с нашими заказчиками, чтобы подвести технико-экономическое обоснование систем видеонаблюдения в сферах, отличных от безопасности. Например, использование систем видеонаблюдения для удаленного мониторинга за объектом в целях сокращения рутинных обходов скважин и управления отчетностью об исполнении работ подрядчиком, — рас-

сказывает Джереми Бернارد. — Мы также инвестируем в исследования и разработки, чтобы расширить спектр применения наших систем и модифицировать их с учетом требований пользователей во всей организации — от главы отдела безопасности до оператора на объекте нефтяного промысла. Более тесное вовлечение в процесс разработки разного круга пользователей придаст системе большую ценность и уменьшает текучесть заказов покупателей».

### КОГДА РУКОВОДСТВУ НЕ ВСЕ РАВНО

Немаловажным фактором обеспечения высокого уровня безопасности на нефтегазовых предприятиях является информированность сотрудников о правилах безопасности и следование установленному порядку работы с оборудованием. Нарушение различных норм и требований работниками нефтегазовых промыслов в последние годы стало одной из наиболее распространенных причин снижения уровня промышленной безопасности.

Как считает Оуэн Чепэлл, технический директор компании Cresent, специализирующейся на консалтинге в сфере промышленной безопасности, оценка рисков и выявление опасностей должны стать приоритетными вопросами для компаний нефтегазовой отрасли. Именно отсутствие своевременных мер по предотвращению тех или иных инцидентов, по мнению Чепэлл, лежит в основе происшествий.

Отключение оборудования, критически важного для обеспечения безопасности без оценки рисков и формального разрешения, а также вскрытие защитных оболочек без использования средств контроля — именно эти два серьезных нарушения, по убеждению Чепэлл, необходимо устранить для повышения уровня промышленной безопасности. Среди других факторов, влияющих на уровень защищенности объекта: выход оборудования из строя, некачественное выявление рисков, несоблюдение регламента по безопасности, экстремальные условия работы и нарушение защитных мероприятий.

«Подобная череда нелепых происшествий стала причиной взрыва на тexasском НПЗ компании British Petroleum в 2005 году. Катастрофа случилась именно



потому, что отдельные нарушения в области промышленной безопасности стали считаться нормой», — комментирует Чепэлл.

При этом значительную роль в системе промышленной безопасности на объектах играет человеческий фактор. А именно — позиция руководства по вопросам нарушений и его стремление соблюдать установленные нормы, поскольку все элементы безопасности находятся в прямой зависимости от степени эффективности управления.

По оценкам вице-президента нефтесервисной компании Afterburner Эндрю Динджи, только 20% происшествий в нефтегазовой отрасли вызваны отказами оборудования, остальные 80% — человеческим фактором.

«Все дело только в руководстве — оно становится одной из причин аварии, если способствует формированию такого климата на предприятии, когда сотрудник боится сообщить о возникновении нештатной ситуации или любых отклонениях от нормы. Как правило, такого сотрудника автоматически считают виновником аварий», — поясняет Динджи. Эксперт уточняет, что топ-менеджмент нефтегазовых предприятий постоянно находится под давлением из-за необходимости выполнять поставленные перед ними задачи по реализации проектов. Это, в свою очередь, становится причиной невнимательности к деталям, которые напрямую влияют на уровень безопасности.

### ЗОЛОТАЯ СЕРЕДИНА

Как подчеркивает Эндрю Динджи, компаниям нужно соблюдать золотую середину между основной деятельностью и безопасностью. «Следует поддерживать производство на уровне, необходимом для обеспечения рентабельности предприятия. Но при этом организация контроля рисков и технологической безопасности должна обеспечивать равновесный уровень показателей безопасности и охраны труда. Ни один из этих факторов не должен иметь приоритет перед другим».

» Только 20% происшествий в нефтегазовой отрасли вызваны отказами оборудования, остальные 80% — человеческим фактором.

**Эндрю Динджи,**  
вице-президент, Afterburner

Одним из эффективных средств поддержания безопасности Динджи называет включение в перечень контрольных вопросов в отношении безопасности самопроверку исполнителя. В настоящее время такой подход используется компанией British Petroleum для работы на промыслах в сложных условиях.

В статье использованы материалы  
с сайта [asmag.com](http://asmag.com)



Организатор



31 МАРТА 2017 МОСКВА  
[www.chatbotconf.ru](http://www.chatbotconf.ru)  
#ChatBotConfRU

31 марта 2017 года в Москве состоится международная конференция ChatBot Conference. Событие будет посвящено теме чат-ботов – актуальному тренду, который скоро вытеснит бизнес-приложения и станет намного популярнее соцсетей.

Чат-боты – это функциональные программы-собеседники, которые общаются с пользователем на его языке и выполняют просьбы. Бот позволяет узнать интересующие новости, прогноз погоды, курс валют, подобрать подходящие билеты, музыку, литературу, совершить онлайн-покупки, вызвать такси и многое другое.

На конференции ChatBot Conference будут обсуждаться вопросы разработки и применения чат-ботов в бизнесе. Участники события – ведущие отечественные и зарубежные эксперты – ознакомят слушателей с уже существующими решениями и на примерах успешных кейсов расскажут, как использовать ботов на практике.

Конференция ChatBot Conference будет полезна владельцам бизнеса, руководителям и топ-менеджерам компаний, SMM-специалистам, online- и offline-предпринимателям, разработчикам, HR-специалистам, представителям сферы образования, государственным деятелям, основателям стартапов и инвесторам.

**РЕГИСТРИРУЙТЕСЬ И ПРИХОДИТЕ!**