

Review



«Интерес к низкоуглеродным решениям будет расти»

Стремясь к повышению энергоэффективности, российские компании нефтегазового сектора постепенно устанавливают на своих объектах оборудование, позволяющее обеспечить снижение выбросов CO₂. Baker Hughes обязалась достигнуть нулевых выбросов к 2050 году, поэтому активно предлагает решения, направленные на их сокращение. О том, почему в России этот процесс идет инерционно и какие решения для повышения энергоэффективности и снижения выбросов существуют в энергетике, «Б» рассказала президент Baker Hughes в регионе Россия и СНГ **Елена Акольцева**.

— экология —

— Чем обусловлено намерение Baker Hughes стать более «зеленой» компанией? — Население планеты растет, растет и потребность в энергии, что, в свою очередь, оказывает влияние на окружающую среду. Мы считаем изменение климата наиболее серьезной глобальной проблемой и уверены, что вместе с остальными участниками энергетической отрасли должны активно участвовать в ее решении.

В январе этого года мы заявили, что к 2030 году снизим выбросы на 50%, а к 2050-му достигнем нулевого уровня выбросов. В принципе мы это делаем уже десять лет — для нас это не новость. И у нас хорошие результаты: с 2012 года мы сократили выбросы углерода на 34% посредством консолидации наших производственных объектов, оптимизации логистики, внедрения энергоэффективных процессов. Например, со следующего года для 170 производственных объектов мы будем закупать 100% электроэнергии на свои нужды от ВИЭ, что за десять лет позволит сократить выбросы на 1,2 млн тонн в CO₂-эквиваленте.

Мы также готовы помочь нашим заказчикам достичь нулевого уровня выбросов к 2050 году. Речь идет о том, что наши продукты и услуги будут обеспечивать нулевой уровень выбросов при их использовании на производственных объектах.

— В этом году вы провели ребрендинг, став «зелеными» не только фирмально, но и буквально? — Да, в связи со снижением доли GE в капитале Baker Hughes, а GE соотрапу — ниже 50%, мы сменили



ЕЛЕНА АКОЛЬЦЕВА, ПРЕЗИДЕНТ БАКЕР ХАУГЕС В РЕГИОНЕ РОССИЯ И СНГ

название на Baker Hughes и обновили логотип. Нашим основным цветом стал зеленый, что символизирует нашу приверженность «зеленым» технологиям.

— Представляется, что при вашей совместной работе с клиентами — нефтегазовыми компаниями — наибольшая часть выбросов приходится на их деятельность, не на вашу. Где та ниша, где вы можете снизить выбросы на ваших сервисах? — На нефтегазовую отрасль приходится чуть меньше 10% мировых выбросов, или около 4,4 млрд тонн в год по всему миру. Наибольшая доля выбросов приходится на добычу — примерно 60%. Около 30% приходится на переработку, остальное — транспортровка.

Наша энергоэффективная технология позволяет операторам ускорить процесс строительства скважин и ввода их в эксплуатацию. Например, в процессе добычи наши электрические погружные насосы потребляют меньше энергии, а ре-

жим их работы можно оптимизировать цифровыми средствами. В зависимости от источника энергии, используемого для погружных насосов, мы добиваемся снижения до 15% вредных выбросов в атмосферу.

— Помимо снижения выбросов путем сокращения энергопотребления оптимизация также возможна, например, благодаря переводу на попутный нефтяной газ (ПНГ) установок для гидроразрыва пласта (ГРП). Насколько сильно все эти меры сказываются на рентабельности бизнеса? — Применение мобильных газовых турбин в качестве источника электроэнергии вместо обычных дизельных приводов для технологического оборудования ГРП является прорывом в области добычи трудноизвлекаемых запасов, повышающим экологическую безопасность и операционную эффективность разработки.

Да, естественно, есть инвестиции в само технологическое изменение, но помимо того, что мы улучшаем эффективность работы оборудования, мы также оптимизируем количество задействованной техники — такому типу оборудования требуются меньше пространства на месторождении. Благодаря применению новой технологии сокращаются сопутствующие затраты на логистику.

В России на данный момент около 100 флотов ГРП, большинство из которых в качестве источника энергии используют дизельные двигатели. Переход на газ позволит сократить выбросы в атмосферу на 24% в год и снизить топливные расходы на 90%.

— Какими еще средствами вы собираетесь достичь «нулевых» выбросов? — За счет всего комплекса продуктов и услуг и совместной работы с заказчиком. Например, определение утечек метана, который наносит большой вред окружающей среде, чем углекислый газ. У нас есть цифровое решение Lumen, которое позволяет обнаруживать утечки метана при помощи наземных датчиков, используемых для таких объектов, как станции газораспределения, или на месторождениях. Или при помощи дронов, обследующих протяженные или труднодоступные участки, такие как трубопроводы, намного быстрее человека. Кроме этого мы предлагаем нашим заказчикам решение Flare IQ, предназначенное для оптимизации работы факельных установок, которое позволяет подобрать оптимальный процесс горения и значительно уменьшить вредные выбросы.



Применение дронов позволяет быстрее и экономичнее обследовать протяженные участки трубопроводов

— Ваши цифровые решения в основном предназначены для клиентов или для оптимизации ваших собственных процессов? — И то и другое. Есть программа цифровизации и для клиентов, и для нас самих. Этим летом было создано совместное предприятие VNC3.ai по разработке решений на базе техно-

логий искусственного интеллекта для нефтегазовой отрасли. И всего за три месяца было разработано первое приложение VNC3 Reliability, которое заблаговременно предупреждает о возможных простоях технологического оборудования и рисках, связанных с технологическими процессами, способствуя повышению производительности, эффективности и безопасности.

— На ваш бизнес цифровых решений приходится примерно десятая доля выручки компании. За какое время удалось увеличить эту долю до такого уровня и продолжит ли она расти? — Необходимо понимать, что после слияния Baker Hughes и GE Oil & Gas в июле 2017-го прошло немного времени и как независимая компания мы впервые представили консолидированные финансовые результаты за 2018 год. Вы правы, на цифровые решения приходится чуть больше 10% заказов и выручки всего Baker Hughes. Цифровые решения являются для нас сегодня приоритетными, мы активно развиваем это направление. Так, например, в ноябре Baker Hughes, C3.ai и Microsoft создали альянс для внедрения ре-

шений искусственного интеллекта VNC3.ai на базе Microsoft Azure.

Основной целью является минимизация выбросов, уменьшение времени простоя оборудования, повышение эффективности и надежности всего технологического процесса в целом, и наши цифровые решения в этом помогают.

— Предлагаете ли вы технологии по уменьшению выбросов российским клиентам? Не секрет, что российские компании довольно спокойно относятся к проблеме выбросов. Насколько подобные сервисы востребованы? — За пределами России стремление компаний к сокращению выбросов действительно выражено гораздо ярче. В этом году Россия присоединилась к Парижскому соглашению по климату, и декарбонизация постепенно становится трендом и у нас. Интерес к низкоуглеродным решениям будет расти, и мы хотим, в том числе совместно с другими участниками рынка, внедрять эти продукты и услуги в нашей стране, и мы сейчас активно работаем в этом направлении.

— Ваши цифровые решения в основном предназначены для клиентов или для оптимизации ваших собственных процессов? — И то и другое. Есть программа цифровизации и для клиентов, и для нас самих. Этим летом было создано совместное предприятие VNC3.ai по разработке решений на базе техно-

логий искусственного интеллекта VNC3.ai на базе Microsoft Azure.

Основной целью является минимизация выбросов, уменьшение времени простоя оборудования, повышение эффективности и надежности всего технологического процесса в целом, и наши цифровые решения в этом помогают.

— Предлагаете ли вы технологии по уменьшению выбросов российским клиентам? Не секрет, что российские компании довольно спокойно относятся к проблеме выбросов. Насколько подобные сервисы востребованы? — За пределами России стремление компаний к сокращению выбросов действительно выражено гораздо ярче. В этом году Россия присоединилась к Парижскому соглашению по климату, и декарбонизация постепенно становится трендом и у нас. Интерес к низкоуглеродным решениям будет расти, и мы хотим, в том числе совместно с другими участниками рынка, внедрять эти продукты и услуги в нашей стране, и мы сейчас активно работаем в этом направлении.

— Ваши цифровые решения в основном предназначены для клиентов или для оптимизации ваших собственных процессов? — И то и другое. Есть программа цифровизации и для клиентов, и для нас самих. Этим летом было создано совместное предприятие VNC3.ai по разработке решений на базе техно-

логий искусственного интеллекта VNC3.ai на базе Microsoft Azure.

Основной целью является минимизация выбросов, уменьшение времени простоя оборудования, повышение эффективности и надежности всего технологического процесса в целом, и наши цифровые решения в этом помогают.

— Предлагаете ли вы технологии по уменьшению выбросов российским клиентам? Не секрет, что российские компании довольно спокойно относятся к проблеме выбросов. Насколько подобные сервисы востребованы? — За пределами России стремление компаний к сокращению выбросов действительно выражено гораздо ярче. В этом году Россия присоединилась к Парижскому соглашению по климату, и декарбонизация постепенно становится трендом и у нас. Интерес к низкоуглеродным решениям будет расти, и мы хотим, в том числе совместно с другими участниками рынка, внедрять эти продукты и услуги в нашей стране, и мы сейчас активно работаем в этом направлении.

— Ваши цифровые решения в основном предназначены для клиентов или для оптимизации ваших собственных процессов? — И то и другое. Есть программа цифровизации и для клиентов, и для нас самих. Этим летом было создано совместное предприятие VNC3.ai по разработке решений на базе техно-

логий искусственного интеллекта VNC3.ai на базе Microsoft Azure.

Основной целью является минимизация выбросов, уменьшение времени простоя оборудования, повышение эффективности и надежности всего технологического процесса в целом, и наши цифровые решения в этом помогают.

— Предлагаете ли вы технологии по уменьшению выбросов российским клиентам? Не секрет, что российские компании довольно спокойно относятся к проблеме выбросов. Насколько подобные сервисы востребованы? — За пределами России стремление компаний к сокращению выбросов действительно выражено гораздо ярче. В этом году Россия присоединилась к Парижскому соглашению по климату, и декарбонизация постепенно становится трендом и у нас. Интерес к низкоуглеродным решениям будет расти, и мы хотим, в том числе совместно с другими участниками рынка, внедрять эти продукты и услуги в нашей стране, и мы сейчас активно работаем в этом направлении.

энергетика

Взлом и проникновение

— информационные технологии —

«Если говорить об уязвимостях, то основные компоненты, уязвимости которых эксплуатируются хакерами, — это промышленное оборудование, системы АСУ ТП, различные контроллеры, — отмечает Илья Шаленков. — Сами уязвимости в общей массе весьма типичны: SQL-инъекции, внедрение вредоносных команд, раскрытие информации, небезопасная конфигурация оборудования, некорректная реализация контроля доступа и т. п. Распространена ситуация, когда устройства напрямую подключены к сети Интернет. Специализированные поисковые системы (например, Shodan, Censys) фиксируют более 200 тыс. компонентов АСУ ТП, которые доступны из глобальной сети, чему способствует распространение концепции IIoT (промышленного интернета вещей — Industrial Internet of Things) в различных отраслях, в том числе в электроэнергетике».

Существует множество примеров специализированных вредоносных программ, спроектированных непосредственно для причинения вреда энергосистеме. Мы рассмотрим наиболее известные из них.

Что зло имеет предложить

В 2010 году были обнаружены и описаны червь Stuxnet, поражающий АСУ ТП и изначально созданный для воздействия на ядерную программу Ирана. Stuxnet поразила производственное по обогащению урана в иранском городе Натанз, отключив 1368 центрифуг из 5000, и распространился по всему миру. Специалисты относят Stuxnet к кибероружию в силу высокой стоимости разработки и ориентированности на конкретную технологическую конфигурацию иранской площадки. Хотя Stuxnet впервые привлек к себе внимание в 2010 году, обнаруживались и более ранние и примитивные образцы.

Как сообщала в своем обзоре червя компания Symantec, он обладает возможностью поражать АСУ ТП, меняя код на программируемых логических контроллерах (ПЛК). Вредоносное ПО вмешивается в информационный поток между ПЛК Simatic S7 и рабочими станциями SCADA WinCC (все это — оборудование Siemens). По данным «Лаборатории Касперского», на закрытые объекты ядерной программы Ирана он попал че-

рез зараженные организации, с которыми эта программа взаимодействует, — трех вендоров промышленных систем, поставщика комплектующих и разработчика центрафта.

Одним из старейших инструментов, впервые описанным в 2007 году, является троян BlackEnergy. С годами он эволюционировал из простого DDoS-трояна в сложное вредоносное ПО с компонентом, имеющим возможность заражать SCADA (появился в версии 2), ICS-CERT США указывало на уязвимость к BlackEnergy человеко-машинного интерфейса (ЧМИ) GE Cimplicity, Advantech/Broadwin WebAccess и Siemens WinCC. BlackEnergy 3, не затрагивавшая ЧМИ, но внедрявшаяся в SCADA, использовалась для атаки на оборудование «Прикарпатьеобленерго», оставившей Ивано-Франковск и половину области без света на несколько часов, а также других предприятий украинской энергетики 23 декабря 2015 года.

Следующим шагом эволюции является Industroger, который позволяет контролировать устройства релейной защиты и автоматики (РЗА) на подстанциях. Этот сложный и высокоадаптивный инструмент стал первой вредоносной программой, разработанной непосредственно для атаки на электросетевую комплекс. 17 декабря 2016 года Industroger вывел из строя на час энергoinфраструктуру Киева. Как сообщал в описании Industroger Антон Черепанов из ESET, «те, кто стоит за Win32/Industroger, имеют глубокое понимание промышленных систем управления, и в первую очередь промышленных протоколов и протоколов связи в электроэнергетике». «Более того, — продолжает он, — маловероятно, что кто бы то ни было мог написать и протестировать подобное ПО, не имея доступа к специализированному оборудованию, используемому в целевой промышленной среде».

Industroger поддерживает четыре промышленных протокола, описанных в стандартах МЭК 60870-5-101 (протокол, предназначенный для передачи сигналов телемеханики в систему диспетчерского и автоматизированного технологического управления электроэнергетическими объектами (АСУ) по сетям передачи данных RS-232/485), МЭК 60870-5-104 (то же самое по протоколу TCP/IP), МЭК-61850 (сети и системы связи на подстанциях) и OLE for Process Control Data Access (OPC DA) — интерфейс для управле-

ния обменом данными в реальном времени с различными системами управления производственными процессами. Также создатели Industroger заложили в него инструмент для осуществления DoS-атаки по конкретной линейке цифровых устройств релейной защиты — Siemens Siprotec.

Плодится и усложняется

Эволюция вредоносного ПО продолжается, потенциальный размах причиняемого ущерба растет. В 2017 году на нефтехимическое производство в Саудовской Аравии была проведена атака при помощи вируса Triton, поражающего систему противоаварийной защиты Triconex компании Schneider Electric и маскирующегося под легальное ПО. Отличительной особенностью конкретного применения было создание аварийной обстановки, прямо угрожающей жизни людей.

В марте 2019 года DoS-атака вызвала сбой в работе электростанции, зарегистрированный Западным координационным советом по вопросам электричества (Western Electricity Coordinating Council), которому подведомственна энергосистема ряда районов штатов Калифорния, Юта и Вайоминг. В конце октября Индия признала факт атаки хакерской группировки Lazarus на инфраструктуру АЭС «Куданкулам». Впрочем, Nuclear Power Corporation of India Limited объявила, что хотя в административной сети были обнаружены вредоносные программы, она была «изолирована от критической внутренней системы». Троян Dtrack, проникший в систему, мог использоваться как для целей шпионажа, так и в качестве носителя других вредоносных программ. А буквально в минувшую пятницу мэрия Нового Орлеана ввела в городе режим ЧС из-за кибератаки на муниципальную сеть.

«Несмотря на то что сфера электроэнергетики не является самой близкой к живым деньгам, как, например, банковская сфера, внимание хакеров к этой области из года в год растет и киберинциденты в ней происходят все чаще, — говорит Илья Шаленков. — В последние пять-семь лет появилось несколько хакерских группировок, специализирующихся на ней (например, APT33 — Elfint Team, APT34 — Helix Kitten, Berserk Bear), что свидетельствует о повышении интереса к этой отрасли. В нашей стране она не яв-

ляется самой IT-зависимой, однако усложнение технологий в ней происходит достаточно быстро, чему нельзя не уделять повышенное внимание с точки зрения кибербезопасности и киберустойчивости».

Нужно понимать, отмечает господин Шаленков, что мотивация атакующих отрасль электроэнергетики отличается от мотивации обычных хакеров, которых интересует в первую очередь быстрая монетизация своих усилий: «Профиль хакеров, орудующих в этой отрасли, в основном такой — это либо кибертеррористы, либо хактивисты. При этом они могут быть state-sponsored, если речь идет о причинении вреда со стороны одного государства другим. Порог входа для злоумышленников в этой отрасли существенно выше: используется сложное специализированное оборудование и программное обеспечение, что требует от хакеров существенно больших затрат как времени, так и материальных ресурсов».

Вместе с тем актуальной остается проблема эволюционного отставания, вызванного стандартизованностью и зарегулированностью, систем обмена данными в промышленной среде от вредоносного ПО. Как замечал в 2017 году руководитель отдела кибербезопасности АСУ ТП «ДиалогНаука» Дмитрий Ярушевский, на турнире по кибербезопасности «Лаборатории Касперского» по взлому цифровой подстанции в 2015 году и по деградации энергоснабжения города в 2016-м большинству участников было менее 25 лет, опыта работы в электроэнергетике и глубоких познаний в области АСУ ТП и РЗА они не имели, однако задачи решили успешно. В 2017 году молодым участникам турнира понадобилось менее семи часов, чтобы с нуля взломать цифровую подстанцию НПС. На то, чтобы проникнуть в технологическую сеть предприятия, победителю, по оценкам жюри, не хватило 10–15 минут.

Энергетический отклик

Одновременно с необходимостью совершенствовать свои системы информационной безопасности с целью ответа на вызовы непрерывно эволюционирующих киберугроз компании энергосектора РФ сталкиваются со все ужесточающимися требованиями законодательства в сфере кибербезопасности. Именно из-за масштабов возможных по-

следствий государства относят сферу энергетике к критически важной, а информационную инфраструктуру, задействованную в функционировании этих сфер, — к критической информационной инфраструктуре, поясняет Илья Шаленков. «Законодательство в этой части некоторое время назад начало активно развиваться в нашей стране, что показывает серьезное отношение к проблеме на уровне государства», — заключает он.

Вступивший в силу 1 января 2018 года закон о безопасности критической информационной инфраструктуры (КИИ, 187-ФЗ) требует от компаний провести категорирование объектов КИИ, проанализировать уязвимости и оценить потенциальный ущерб от киберинцидентов. Также субъекты КИИ должны подключиться к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и передавать туда данные об инцидентах. С начала года, говорил в середине ноября замначальника Центра ФСБ Игорь Качалин, Национальный координационный центр по компьютерным инцидентам выявил 3 тыс. инцидентов. После категорирования компаниям нужно будет принять целый комплекс мер, оговоренных ФСТЭК, связанных с обеспечением информационной безопасности значимых объектов КИИ — это следует сделать до 2022 года.

Эти сроки могут вызвать затруднения у компаний энергетического сектора, в силу того что на рынке, как правило, работают очень крупные структуры. «Вне зависимости от масштаба субъекта КИИ есть сроки, которые обозначены регулятором и поддержаны Минэнерго, в которые от нас ожидают, что мы приведем все свои значимые объекты КИИ к требованиям ФСТЭК, — говорит на конференции «Промышленная кибербезопасность-2019» замначальника отдела АСЗИ «Транснефти» Дмитрий Ли. — Это немного пугает ввиду того, что сроки достаточно сжатые. Потому что, по нашей оценке, это потребует существенных инвестиций и финансовых, и временных. Нужно подходить дифференцированно». Впрочем, директор департамента оперативного контроля и управления в электроэнергетике Минэнерго Евгений Грабчак ответил, что если компании не будут успевать, то сроки будут скорректированы.