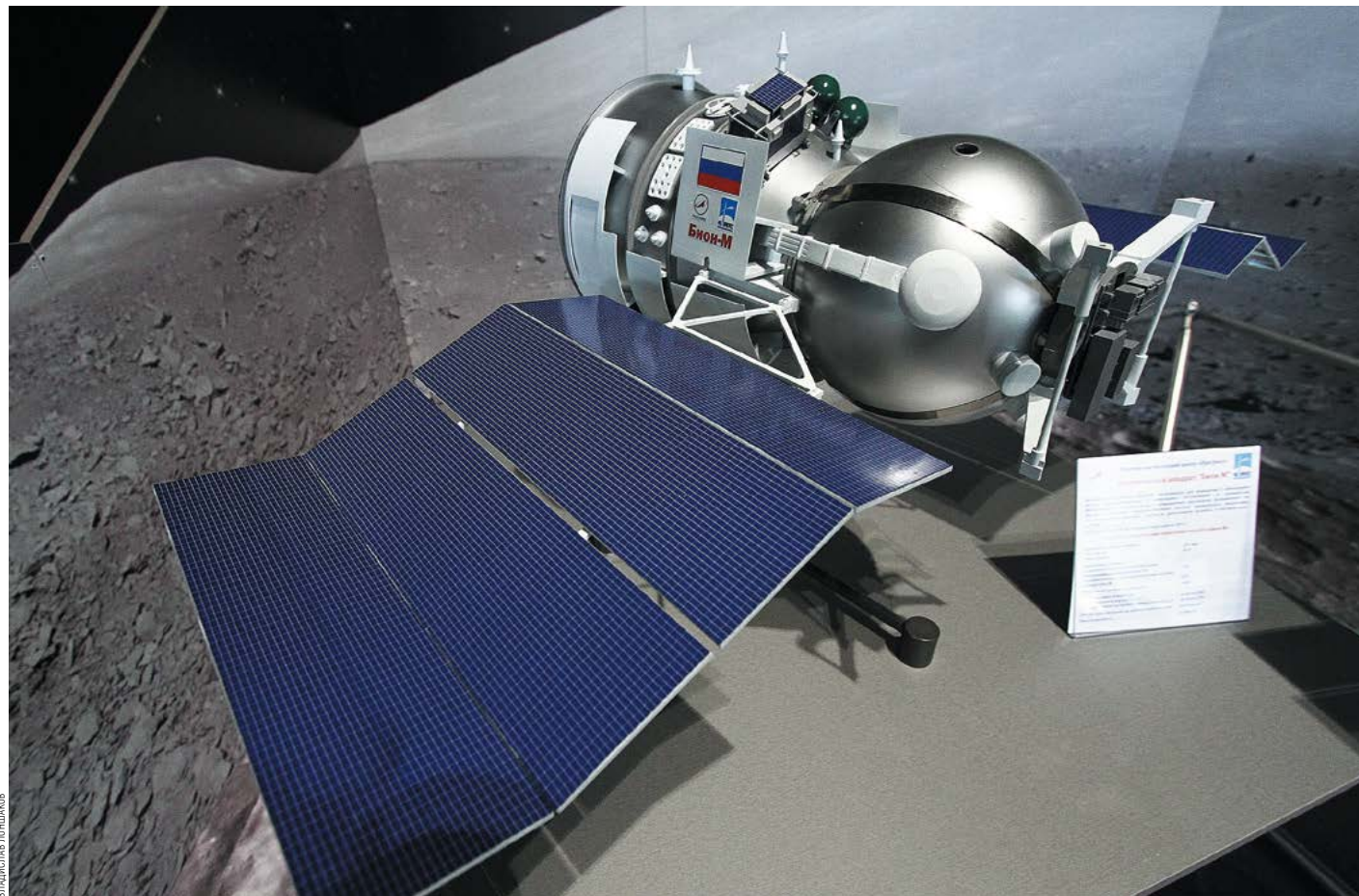


→ **РЫНОЧНЫЕ РЕАЛИИ** Участники рынка технологий для электроэнергетики делят направления работы на несколько типов. Так, в ПАО «Энел Россия» проекты разделяют на три потока: повышение эффективности генерирующего оборудования, цифровизация процессов на производстве и создание цифровой инфраструктуры. Там отмечают, что цифровизация не связана напрямую с модернизацией и обновлением оборудования. «С помощью новых технологий мы повышаем эффективность текущих активов генерации, а также занимаемся оптимизацией производственных и административных процессов на станции», — пояснили в пресс-службе компании. Среди проектов по указанным направлениям в «Энел» называют управление удельным расходом топлива — систему мониторинга характеристик оборудования по потреблению топлива, предиктивную диагностику на основе данных с датчиков паровозовых установок с помощью систем Prism и Predix, цифровое планирование ремонтов и управление отходами. Отдельное внимание уделено кибербезопасности и IT-инфраструктуре. В рамках последней создается глобальное хранилище всех данных (Data Lake). «Все упомянутые выше проекты уже с успехом реализуются на Среднеуральской ГРЭС», — заверили в пресс-службе.

Аналогичное разделение направлений проектов проводят в компании «Сименс». Там среди решений выделяют информационные системы управления, цифровые подстанции, системы автоматизации процессов ликвидации аварий сетей, интеллектуальные системы учета и энергомониторинга. В частности, для управления энергоснабжением компания создает интеллектуальную систему Spectrum Power, которая содержит информацию по перетокам мощности, а также состояние энергетической сети в целом, решения для цифровых подстанций, устройства индикации места повреждения для кабельных и воздушных линий. Кроме того, отметили в пресс-службе «Сименса», у компании существует облачное решение для анализа данных, получаемых от точек коммерческого учета — EnergyIP. Это единая архитектура, связывающая данные от счетчиков с бизнес-процессами компании и рынком электроэнергетики.

**РЕГИОНАЛЬНАЯ ЦИФРОВИЗАЦИЯ** По данным Свердловскстата, в 2018 году объем обеспечения электрической энергией, газом и паром по УрФО превысил 700 млрд руб., на 3% увеличив показатели 2017 года. При этом на Свердловскую область пришлось 33,1% общего объема рынка. Доля УрФО в общероссийском показателе по этому виду экономической деятельности составила 12,7%. В первом квартале 2019 года объемы выросли на 5,8% по сравнению с аналогичным периодом 2017 года — до 220,3 млрд руб.



ЭНЕРГЕТИКИ СЛЕДЯТ ЗА РАБОТОСПОСОБНОСТЬЮ СЕТЕЙ С ПОМОЩЬЮ КОСМИЧЕСКИХ ТЕХНОЛОГИЙ

По мнению участников рынка, энергосистема Свердловской области — одна из крупнейших в России. При этом, по их словам, структура электропотребления региона неоднородна, поскольку в ней доминируют предприятия металлургического и горнодобывающего комплексов, транспорт ресурсов, научно-исследовательские организации и коммунальное хозяйство. В перспективе до 2023 года эксперты прогнозировали умеренный рост потребления до 1% в год на фоне отсутствия планов по вводу крупных генерирующих мощностей.

Между тем «Россети Урал» уже разработали модель цифровизации электросетевого комплекса в соответствии с единой концепцией развития «Россетей». Представить дорожную карту планируется на «Иннопроме-2019». Осенью прошлого года в компании сообщали, что под цифровизацией подразумевают создание высокоавтоматизированной сети, наблюдаемость и управляемость которой будут обеспечены цифровыми системами связи.

«Мы начинаем не с нуля: в компании уже реализован ряд инновационных проектов. В итоге то, что сегодня звучит как фантастика, уже к 2030 году должно стать реальностью», — уверен генеральный директор «Россетей Урал» Сергей Дреговаль.

К этому времени компания намерена поэтапно вводить в строй интеллектуальные системы учета, совершенствовать оперативно-технологическое управление, работать над созданием единых IT-продуктов. Предполагается, все это повысит эффективность работы электросетей. В итоге энергетики должны прийти к «умной, активно-адаптивной» сети, которой потребуются минимальное время реагирования на аварийные ситуации и оперативный ввод резерва. Длительность отключений и их частота должны снизиться в пять-восемь раз.

Кроме того, в Свердловской области энергетики установят более 28,5 тыс. интеллектуальных приборов учета в 106 населенных пунктах. Устройства размещают на опорах линий электропередачи, а потребитель полу-

чит к ним дистанционный доступ. В компании полагают, что проект повысит качество и надежность электроснабжения, поскольку новый прибор не поддерживает несанкционированное подключение, избавит потребителя от обязанности самостоятельно снимать показания, повысит точность определения объема оказанных услуг. Инвестиции оцениваются более чем в 900 млн руб., предполагаемый срок окупаемости составит 4,2 года. Обойтись без начального вложения средств филиала поможет механизм энергосервисных контрактов.

Сейчас в регионе уже есть пилотные проекты. Так, «Сименс» имеет опыт поставок силового оборудования для современных подстанций, например поставка ячеек 35kV (КРУЭ-8DA10) для подстанции «Верхняя Сысерть». Помимо этого, «Сименс» ведет переговоры по пилотному проекту цифровизации сетей Екатеринбурга. «Предлагается создать концепцию внедрения цифровых решений для оценки технического и экономического эффекта от цифровых технологий», — рассказали в компании.

## ХАКЕРЫ ПОЛЕЗЛИ В СЕТИ

За последние годы серьезно вырос процент кибератак на электроэнергетику, которая относится к объектам критической информационной инфраструктуры (КИИ), отметил гендиректор «Ростелеком-Solar» Игорь Ляпунов. По его данным, в абсолютных значениях оно выросло в два-три раза за последний год. «В прошлом году была большая атака с использованием уязвимостей в устройствах Cisco. При этом плотность атак на объекты КИИ была в 10–15 раз выше других», — сообщил господин Ляпунов. В связи с этим меняется профиль атак, отмечают в компании. Так, при атаке на банк сначала идет долгое исследование периметра, получение точек присутствия, а дальше — за 2–3 часа быстрая атака, незамаскированная и лобовая, поясняет господин Ляпунов. «В случае атак на объекты КИИ цель злоумышленника — не моментальное действие, а получение точки присутствия, возможности контроля. Он ведет аккуратную, многомесячную атаку на систему, постепенно получая присутствие в разных сегментах. В большинстве случаев это очень скрытый инструментарий: бесфайловые вирусы, жизнь зловредов в оперативной памяти компьютера, практически без каких-то следов в файловых системах и почти без следов в сети», — рассказывает Игорь Ляпунов. Это накладывает серьезные ограничения на возможность выявления таких видов атак.

При этом атаки на объекты КИИ, в отличие от простых, относительно дешевых фишинговых атак, прицельно создают коллективы по 20–30 человек. «Это очень дорого — написать такой инструментарий и реализовать такую атаку, а прямой монетизации там нет вообще», — отмечает господин Ляпунов. По его словам, в даркнете деятельность злоумышленников разграничена: «Одни пишут зловреды, другие их распространяют, третьи уже делают атаки, четвертые, имея точки присутствия в инфраструктурах, ей управляют».

Сейчас защита электроэнергетики — большое направление работы компаний, занимающихся информационной безопасностью. «Мы проводим анализ ПО или оборудования на предмет уязвимости. Если находим, работаем с вендорами по устранению, информируем ФСТЭК и работаем с потребителями информационных систем, чтобы реализовывать компенсирующие меры на уязвимости, которые находим», — пояснил господин Ляпунов.



ХАКЕРЫ СТАЛИ ЧАЩЕ СОВЕРШАТЬ НАПАДЕНИЯ НА КИИ