Обеспечение безопасности функционирования энергетической инфраструктуры на этапе цифровизации

В энергокомплексе наступает новая эпоха – цифровая. Энергетические сети дополняются новыми цифровыми интеллектуальными возможностями. В этих "разумных" сетях все чаще используются датчики, интеллектуальные приборы учета, цифровые средства управления и аналитические инструменты, обеспечивающие автоматизацию, мониторинг и контроль двусторонней передачи энергии на всех этапах – от электростанции до бытовой розетки. Цель всех этих изменений – оптимизация производительности сети, предотвращение перебоев в энергоснабжении в автоматическом режиме, более быстрое восстановление подачи электроэнергии и предоставление пользователям возможности управлять потреблением энергии – вплоть до работы на уровне отдельных приборов, подключенных к сети. В свою очередь, технологические достижения и рост цен на электроэнергию изменяют коллективный облик потребителей, превращая их из пассивных плательщиков в хорошо информированных заказчиков, которые заботятся об окружающей среде и хотят влиять на принятие решений, связанных с использованием энергии.

От аналоговых сигналов к цифровизации энергетики – новые возможности и новые вызовы

С появлением технологий, делающих возможным создание "разумных" энергетических сетей, энергокомпании будут предоставлять потребителям необходимую информацию и средства управления, с помощью которых они смогут изменять свою модель поведения и сокращать расход электроэнергии.

С оснащением мира энергетики новейшими интеллектуальными техническими средствами, находящимися в тесном взаимодействии друг с другом, начнет генерироваться колоссальный объем данных различного формата (рис. 1): записи камер наблюдения, информация с датчиков в энергетических системах, "умных" домах. Все эти необработанные данные будут поступать с огромной скоростью в системы обработки данных.

Вместе с этим мы столкнемся и с целым рядом трудностей: различными темпами трансформации бизнеса и технологий, необходимостью серьезных вложений в модернизацию производства, несовершенством законодательной базы, требованиями безопасности инфраструктуры на уровне стыковки физических и кибернетических систем и многими другими.

Новые аналитические инструменты помогут извлекать полезные знания из огромного потока данных. Станут очевидными закономерности, взаимосвязи и резкие отклонения, скрытые в этих огромных массивах разнородных данных. С помощью сложных математических моделей и мощнейших вычислительных систем можно будет оценить накапливаемую в мире энергетики информацию и начать на практике прогнозировать и предупреждать изменения в наших энергетических системах, и не только в сетях. Так выглядят перспективы разумной – включающей и интеллектуальные сети – цифровой энергетики, которая в конечном итоге поможет повысить качество жизни каждого жителя.

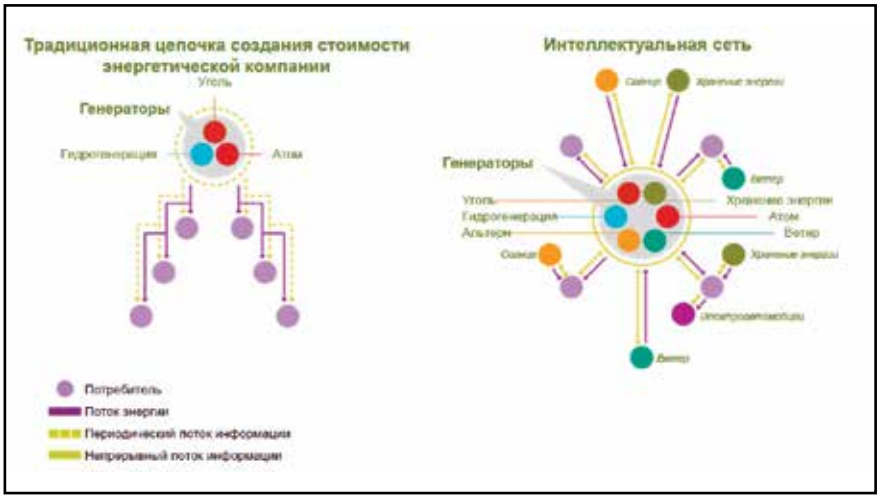

Рис. 1

Вместе с тем, использование новых цифровых технологий ведет в том числе и к возникновению новых, ранее не встречающихся угроз. Например, недавно службы кибербезопасности нескольких распределительных энергосистем в США зафиксировали попытку проникновения в цифровые сети передачи данных, связывающие приборы контроля потребления электроэнергии. При самом негативном сценарии развития событий это могло привести к масштабному отключению

и усложнению процесса восстановления энергоснабжения целых регионов.

В настоящий момент развитие новых видов угроз в сфере ИКТ для бизнеса энергетических компаний нарастает лавинообразным образом. Это связано, с одной стороны, с высокой скоростью разработки новых видов атак киберпреступности, так как эта деятельность становится все более выгодной для правонарушителей. С другой стороны, современные энергетические компании вынуждены все более активно внедрять новые виды сервисов, непосредственно связанных с применением передовых информационных технологий. Скорость изменения ИТ-ландшафта компаний ведет к резкому росту новых векторов угроз и ко все большему влиянию отдельных ИТ-сервисов на общий бизнес компании.

В таких обстоятельствах существующие решения, предназначенные для оперативного реагирования на инциденты в области безопасности не в состоянии гибко изменяться и масштабироваться под новые задачи и угрозы. И это значит, что разрыв между уровнем защиты и уровнем угроз серьезно растет. Новые реалии требуют расследования инцидентов и реакции на них не в рамках нескольких месяцев, как это было еще недавно, а в пределах часов и минут, а также гибкой адаптации под новые векторы атак, постоянного учета изменения ИТ-ландшафта.

Таким образом, энергетические компании стоят на пороге новых, комплексных и масштабных вызовов, которые требуют немедленных действий.

Основные вызовы обеспечения безопасности инфраструктуры энергетических компаний

При обеспечении безопасности критической инфраструктуры энергетических компаний необходимо обратить особое внимание на 10 основных вызовов времени.

Вызов 1. Использование нетрадиционных возобновляемых источников энергии

Интегрирование возобновляемых источников энергии (вода, ветер, солнце) с традиционной сетью потребует использования распределенных сетей сенсоров, в том числе погодных датчиков, усложненной схемы учета сигналов и передачи данных в компьютерные системы. В свою очередь это неизбежно приведет к усложнению контроля за безопасностью сетевой и энергетической инфраструктуры.

Вызов 2. Усложнение топологии сетей передачи данных

Сети передачи данных энергетических (прежде всего – распределительных) сетевых компаний, как правило, имеют сложную топологию. Для доступа к основным узлам подобной сети требуется идентификация и обеспечение безопасности основных приложений. Подчас нестыковки и уязвимости в системах идентификации в узлах сетей могут стать дополнительными факторами рисков, поскольку в каждом из подобных узлов могут скрываться уязвимости и существовать возможности для проникновения. Ввиду этого целесообразно строить защиту сети передачи данных энергетических компаний не как единого шлюза, а как сети распределенных узлов.

Вызов 3. Необходимость следовать усложняющимся требованиям регулирующих органов

Энергетические компании всегда функционировали в партнерстве с государственными органами, федеральными, региональными и местными администрациями. С учетом того, что регуляторная среда и сегодня остается достаточно комплексной, многоуровневой и разветвленной, в эпоху постепенной цифровизации необходимо ожидать дальнейшего усложнения требований регуляторов к обеспечению кибербезопасности критической инфраструктуры энергетических компаний, что требует соответствующих проактивных действий по формированию стандартов безопасности, желательно перекрывающих требования регуляторов.

Вызов 4. Достижение эффекта "Интернета доверия"

Интеллектуальная активно-адаптивная сеть построена на принципах использования Интернета вещей (Internet of Things, IoT) – целой инфраструктуры сенсоров, которые размещены во всех ключевых узлах интеллектуальной сети. Сенсоры и средства передачи и обмена данными могут стать мишенью для потенциальных атак злоумышленников. И чем больше сенсоров используется, тем больше должно быть уверенности в их безопасном функционировании. Как же превратить Интернет вещей в "Интернет доверия"? Очевидно, что необходимы новые подходы и решения, такие например, как "брокеры доверия", которые позволяют обеспечивать безопасное инкорпорирование данных, получаемых с сенсоров из контуров, расположенных вне традиционных SCADA-систем диспетчерского управления и сбора данных.

Вызов 5. Обеспечение комплексной кибербезопасности

Энергетические компании в отношении доступа к их критической инфраструктуре требуют комплексных мер кибербезопасности. Например, создания архитектуры управления доступом и авторизацией, которая обеспечивает безопасность за пределами ввода обычных логинов и паролей. Комплексная безопасность требует использования технологий динамической смены паролей доступа при истечении заданных интервалов времени, интегрированного отзыва паролей и логинов, предупреждений о событиях, связанных с попыткой несанкционированного использования логинов и паролей. Эти технологии существуют и используются, но настало время для их обязательного повсеместного применения, а также использования новейших достижений в области информационной

безопасности, например технологий блокчейна для дополнительной верификации.

Вызов 6. Координирование работы все большего числа систем

Чем сложнее ландшафт используемых энергетическими компаниями систем, тем более комплексным становится вопрос обеспечения кибербезопасности. Компании в энергетике уже приступают к использованию систем с элементами искусственного интеллекта, автоматически принимающих решения, найденные при применении алгоритмов для распределенных (мультиагентных) систем. Мы закономерным образом переходим от умной системы управления критической инфраструктурой к более умной и далее к самой умной. Но как минимизировать угрозы асинхронного принятия решений, влияющих на кибербезопасность, когда, например, система рекомендует решение, которое на локальном уровне может быть корректным, но способно привести к уязвимостям на уровне взаимодействия систем? Например, при атаке на один из узлов трансформаторной подстанции распределительной сети система безопасности может рекомендовать временное блокирование этого узла, что в свою очередь может вызвать перегрузку всей сети и, как следствие, к веерному отключению по всей системе. Что и может быть целью злоумышленников. Поэтому с точки зрения обеспечения кибербезопасности необходимо рассматривать не только безопасность отдельных систем, узлов, элементов, но и практики взаимодействия функционирующих систем класса SCADA, MES, ERP, BI и так далее друг с другом.

Вызов 7. Сложный, многоуровневый ИТ-ландшафт

Современные энергетические компании все более и более широко используют самые передовые технологии – облачные сервисы (инфраструктура как услуга, вычислительные ресурсы, клиентские сервисы и так далее), услуги по управлению кибербезопасностью инфраструктуры, что в свою очередь ведет к новым вызовам в области обеспечения безопасности. Соответственно, встает задача корректной адресации рисков при использовании передовых технологий. Одним из рекомендуемых способов ее решения является синхронизация облачных сервисов с обеспечением их комплексной безопасности.

Вызов 8. Обеспечение интегрированной безопасности критической инфраструктуры на стыке физической и кибербезопасности

Меры по обеспечению киберзащиты, безусловно, очень важны. Однако они могут дать необходимый эффект только в сочетании с эффективной физической безопасностью. Для получения наибольшего эффекта от комплексных решений на стыке физической и кибербезопасности рекомендуется, например, расширить возможности сотрудников служб, обеспечивающих физическую безопасность инфраструктуры, средствами интеллектуального видеораспознавания, соединенными с системами кибербезопасности.

Вызов 9. Обеспечение регулярного мониторинга угроз и связанных с ними рисков

Динамическая, постоянно меняющаяся природа угроз требует постоянного совершенствования и систем предупреждения. Процедуры в компании должны обеспечивать четкое следование принципам обеспечения кибербезопасности всеми взаимодействующими департаментами – ИТ, безопасности, закупок и так далее – для согласования понимания всеми участниками, кто и за что отвечает.

Вызов 10. Проблема слишком большого объема данных и их некорректности

Конечно, на первый взгляд, чем больше данных, получаемых, например, с сенсоров – тем лучше. До тех пор, пока злоумышленники не попытаются атаковать вашу сеть передачи данных, объединяющую сенсоры и системы аналитики. Некачественные или незащищенные данные (которые могут быть искажены в результате атак злоумышленников) в состоянии вызвать неправильные действия операторов и диспетчеров сетевого комплекса. Как предотвратить подобные проблемы? В случае данных, получаемых с сенсоров, раннее предупреждение об атаках злоумышленников могут обеспечить улучшенные алгоритмы их обработки, а также использование аналитических систем нового поколения, включающих в себя когнитивные возможности. Необходимы и инструменты комбинированной разработки и тестирования.

Резюмируя вышеизложенное, необходимо отметить, что в век неуклонного перехода к цифровым технологиям многочисленнее вызовы, встающие перед энергетическими компаниями, диктуют потребность в новых знаниях, компетенциях и партнерстве с ведущими в мире разработчиками систем противодействия атакам злоумышленников на критически важную инфраструктуру энергетики.

IBM: услуги по обеспечению безопасности критической инфраструктуры энергетических компаний

В целях эффективного предотвращения угроз для критической инфраструктуры энергетических компаний IBM предлагает разработанный компанией подход к построению системы комплексной безопасности и оперативного реагирования – ЦОР (Центр оперативного реагирования).

ЦОР по своей сути – это не просто технологическое решение, такое как SIEM-система (Security information and event management). SIEM – это объединение в одном двух терминов, обозначающих область применения программного обеспечения: SIM (Security information management) – управление информационной безопасностью и SEM (Security event management) – управление

событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлена приложениями, приборами или услугами и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.

Рис. 2

ЦОР в понимании IBM – это организационная единица подразделения информационной безопасности, объединяющая в себе сотрудников, процессы и технологии, которая предназначена для получения ситуационной осведомленности о текущих и новых угрозах и реагирования на них в соответствии с установленными приоритетами.

С точки зрения процессов ЦОР – это:

- ***ранняя идентификация и быстрое разрешение инцидентов*** до того, как данные инциденты окажут влияние на инфраструктуру компании;
- ***устранение инцидентов*** до момента нанесения ими значительного ущерба компании, как прямого, так и опосредованного, например в виде репутационных потерь;
- как следствие двух первых пунктов – ***минимизация финансовых потерь***, в том числе связанных с введением нового поколения сервисов и услуг.

Основными функциями ЦОР IBM является сбор и учет максимального количества информации с применением современных аналитических средств. Как правило, функционал традиционных ЦОР ограничивается только сбором журналов функционирования различных ИТ-систем и средств информационной безопасности. Но для учета современных реалий этой информации недостаточно. Расширенный диапазон анализируемой информации в ЦОР IBM и применение всего спектра автоматизированной аналитики для анализа данной информации в реальном времени позволяет перейти от пассивного уровня расследования инцидентов к оперативному и даже проактивному предупреждению угроз (рис. 2).

ЦОР IBM нового поколения – это новейшая инфраструктура, предназначенная для наблюдения за инцидентами безопасности и реагирования на них. Эксперты и разработчики систем энергетических компаний смогут воспользоваться самыми современными и инновационными инструментами в соответствии с выработанными процедурами для управления угрозами и снижения уровня риска.

Это позволит проактивно отвечать на любые незаконные действия, противоречащие корпоративной политике безопасности в реальном времени. ЦОР обычно функционирует круглосуточно в режиме 24x7 и может стать критически важным элементом инфраструктуры энергетической компании.

Остановимся более подробно на архитектурном подходе к построению ЦОР IBM нового поколения.

Структурно архитектура ЦОР нового поколения гораздо шире тех, которые построены в соответствии с традиционными подходами. Если традиционные ЦОР работают только со структурированными данными в рамках так называемых SIEM-систем, то ЦОР IBM нового поколения обогащает собираемую информацию данными из неструктурированных и полуструктурированных источников (в том числе видео- и аудиоисточников), внутренних справочников и баз данных, систем противодействия мошенничеству. Также предусматривается подключение к международным базам знаний и сведений о текущих угрозах и атаках, появляющихся в мире.

С точки зрения непосредственно внутреннего устройства ЦОР, он, как уже указывалось, подразделяется на три основных направления – технологии, люди и процессы (рис. 3). В каждом из этих направле-

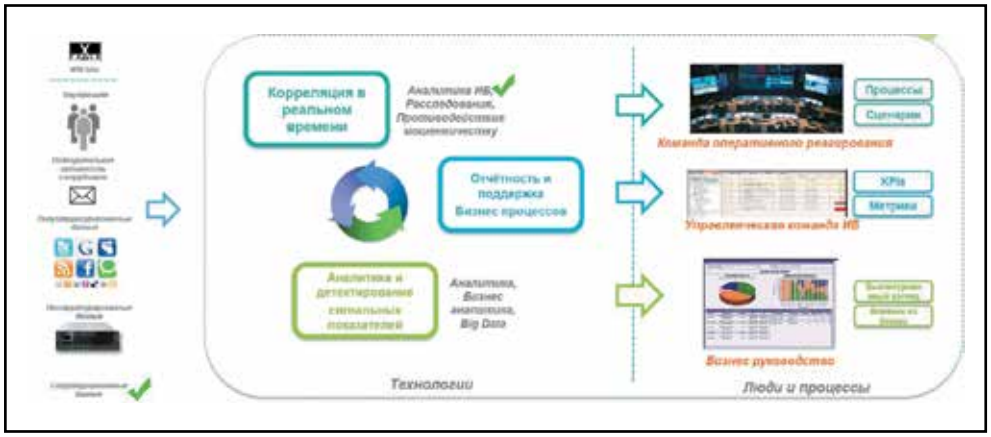

Рис. 3

ний есть ключевые моменты, от которых зависит качественный скачок в направлении построения зрелого ЦОР. Средства аналитики совместно с иными аналитическими средствами, включая бизнес-аналитику и анализ больших данных, наличие соответствующего уровня поддержки бизнес-процессов работы с инцидентами и отчетности всех уровней используются на уровне контроля технологий. Для уровня контроля людей и процессов ключевым фактором является создание единой интегрированной (с возможностью территориального распределения) команды оперативного реагирования с разработанными процессами и сценариями реагирования на различные уровни инцидентов.

Какие же основные преимущества получают энергетические компании от построения ЦОР IBM?

Прежде всего – это проактивный мониторинг угроз, повышение осведомленности персонала, снижение времени обнаружения инцидента с нескольких часов до минут и хорошо обоснованное выстраивание операций по дальнейшему снижению рисков и соответствующих затрат, повышение общего уровня кибербезопасности. Немаловажным моментом является также возможность получения экспертизы мирового уровня по управлению борьбой с киберугрозами в отрасли, позволяющей лучше контролировать все направления безопасности компании.

Александр Соковнин, директор по развитию бизнеса в электроэнергетике и ЖКХ, компания IBM в России и СНГ

НОВОСТИ

EcoStruxure Maintenance Advisor – комплексное решение для повышения эффективности предприятий

Новая разработка Schneider Electric – ПО EcoStruxure Maintenance Advisor со встроенным модулем EcoStruxure Condition Advisor, которое устраняет разрыв между процессами эксплуатации и обслуживания производственных активов, обеспечивая превентивное обслуживание и поддержку принятия решений для эксплуатации всех производственных активов предприятия. В процессе задействованы компоненты систем управления EcoStruxure Foxboro DCS, EcoStruxure Hybrid DCS, интеллектуальные полевые устройства, приводы и широкий спектр другого оборудования для системы автоматизации.

Предоставляя оперативные данные, требующие принятия решений, аналитическую информацию о нештатных ситуациях и условиях работы оборудования, эти продукты позволяют специалистам принимать более понятные, четкие и упреждающие решения по техническому обслуживанию и эксплуатации, повышая тем самым надежность и рентабельность работы предприятия. Благодаря мобильным устройствам и параметрам рабочего процесса, доступным с помощью единого унифицированного интерфейса EcoStruxure Maintenance Advisor, персонал предприятия может быстро реагировать на возникающие события, находясь в любом месте производственной площадки.

Новый компонент программного обеспечения EcoStruxure Condition Advisor с поддержкой протокола OPC DA позволяет осуществлять в режиме реального времени автоматический мониторинг состояния любого совместимого с OPC DA оборудования, например интеллектуальных электронных устройств, пускателей и приводов электродвигателей. Эта возможность дополняет существующие модули Condition Advisor, которые контролируют состояние полевых устройств, работающих по технологиям Fieldbus Foundation, HART и Profibus.

Хосе Бономо, вице-президент по управлению технологическими процессами компании Schneider Electric, отмечает: "Впервые предлагая рынку новые возможности в едином решении, мы помогаем клиентам повысить эффективность работы предприятий и увеличить производственные мощности в такой степени, чтобы обеспечить полную и измеряемую окупаемость инвестиций уже через три месяца после внедрения. При правильном применении эти решения помогут преобразовать автоматизацию технологических процессов в механизмы увеличения прибыльности".

Перед сотрудниками промышленных предприятий традиционно стоит задача по повышению эффективности производственных операций, что приводит к преждевременному износу оборудования, увеличению количества и продолжительности простоев. Более надежные архитектуры на базе Промышленного Интернета вещей (IIoT), являющиеся неотъемлемой частью платформы EcoStruxure компании Schneider Electric, открывают специалистам промышленных предприятий широчайшие возможности для оперативного контроля, повышения окупаемости и обеспечения надежности функционирования производственных фондов.

EcoStruxure – это открытая системная архитектура и платформа компании Schneider Electric, основанная на Промышленном Интернете вещей. С помощью подключенных полевых устройств, средств обеспечения контроля, обработки и сбора данных, применения специализированных приложений, средств аналитики и обслуживания архитектура EcoStruxure предлагает масштабируемое решение и обеспечивает высокий уровень кибернетической безопасности для каждого производственного участка.

Возможность комбинации решений компании Schneider Electric и систем управления других производителей позволяет пользователям отслеживать и диагностировать состояние широкого спектра производственных активов в режиме реального времени, что может максимально увеличить время бесперебойной работы, минимизировать эксплуатационные расходы и затраты на обслуживание, повысить безопасность для персонала. Понятные предупреждения сообщают о текущем состоянии данного производственного актива, критичности условий работы, дают четкие рекомендации, что уменьшает время реакции обслуживающего персонала.

В настоящее время программное обеспечение EcoStruxure Maintenance Advisor и EcoStruxure Control Advisor доступны для предприятий перерабатывающих и гибридных отраслей промышленности.

ПЕТЕРБУРГСКАЯ ТЕХНИЧЕСКАЯ ЯРМАРКА

ufi Approved Event

20–22 марта 2018

Санкт-Петербург
ЭКСПОФОРУМ

ТЕМАТИКА ВЫСТАВОЧНОЙ ЭКСПОЗИЦИИ:

- Обработка металлов (MP expo)
- Машиностроение
- Металлургия. Литейное дело
- Крепёж. Метизы. Инструмент
- Автоматизация промышленных предприятий

NEW! Пластмассы, каучуки, РТИ

NEW! Автокомплект. Автосервис

NEW! Подъемно-транспортное оборудование

NEW! Охрана труда и средства индивидуальной защиты

БИРЖА ДЕЛОВЫХ КОНТАКТОВ

Выставка «Высокие технологии. Инновации. Инвестиции (Hi-Tech)»

ВАШ СТЕНД ПО СПЕЦИАЛЬНОЙ ЦЕНЕ – ptfair.ru

ОРГАНИЗАТОР:

РЕСТЭК® Выставочное объединение

СВЯЖИТЕСЬ С НАМИ:

+7 (812) 320 96 76, 320 80 94
ptcomp@restec.ru

ГЕНЕРАЛЬНЫЙ ИНФОПАРТНЕР:

Станочный парк