Цифровая трансформация ТЭК и кибербезопасность

Новые угрозы и COVID-фактор

26-29 апреля 2021 года в Москве пройдет очередной Национальный нефтегазовый форум. Его участники обсудят широкий круг проблем, касающихся развития глобальной и российской энергетики. Важное место среди основных тем дискуссий займут цифровизация нефтегазового комплекса и вопросы обеспечения безопасности при внедрении цифровых решений. Эта тема стала особенно актуальной на фоне пандемии COVID-19 и широкого распространения формата удаленной работы. Как нефтегазовые компании будут справляться с новыми угрозами? Об этом НГВ беседует с руководителем направления Kaspersky Industrial CyberSecurity в России АЛЕКСЕЕМ ПЕТУХОВЫМ.

Ред.: ***Алексей Владимирович, давайте поговорим о цифровой трансформации ТЭК. Уровень цифровизации предприятий, новые инициативы в области внедрения искусственного интеллекта наверняка влекут за собой и новые информационные угрозы?***

А.П.: Я бы разбил этот вопрос на два: вызовы цифровизации в целом для сферы информационной безопасности (ИБ) и актуальные угрозы сегодняшнего и завтрашнего дня.

В части общих вызовов современности хотелось бы отметить, что информационная безопасность также подвержена проблемам нехватки кадров и отставания технологий, как и другие отрасли. Как и везде, здесь требуется внедрять новые решения: информационные системы, базы знаний, цифровые сервисы и т.д., позволяющие упростить работу специалиста ИБ и при этом повысить ее качество.

Например, цифровые технологии сегодня внедряются зачастую на ходу. Предприятия выбирают объекты, где внедрят их, и вживую смотрят, каким будет результат и как двигаться дальше. То есть классический процесс проектирования выпадает. Это влечет потерю данных о том, что и как внедрено, как настроено. Потом происходит большое проектирование и внедрение хорошо показавших себя технологий, но за время формирования этой большой системы сама инфраструктура предприятия опять меняется. Поэтому идет бесконечный цикл периодического проектирования с низким КПД. Для этого в том числе создаются цифровые двойники или иные информационные системы, позволяющие владеть актуальной информацией и эффективно пользоваться ею для управления изменениями предприятия. В сфере информационной безопасности тоже такие нужны. Необходимо иметь интерактивную информацию о том, что мы защищаем именно сейчас и как реагировать на разные события в области ИБ.

Информационная безопасность также подвержена проблемам нехватки кадров и отставания технологий, как и другие отрасли. Как и везде, здесь требуется внедрять новые решения

Это касается и угроз, которые привносит внедрение систем искусственного интеллекта. Объект (информационная система) меняется гораздо быстрее, чем способна на это реагировать система защиты, и результаты работы ИИ непредсказуемые. Следовательно, создать правила для защиты не всегда возможно.

Если посмотреть на прогнозы компании Gartner «Технологии искусственного интеллекта: на какой стадии находятся и когда они начнут работать продуктивно», то мы увидим, что ИИ внедряется повсеместно и говорить о статичности инфраструктуры сложнее с каждым днем.

Ред.: ***Как, по-вашему, повлияла пандемия на кибербезопасность?***

А.П.: Согласно результатам нашего опроса «Информационная безопасность систем промышленной автоматизации в эпоху цифровой трансформации», пандемия привела к тому, что многие компании изменили формат работы. Так, 53% респондентов подтвердили, что они переводят сотрудников на удаленную работу. Это стало испытанием на прочность для процессов кибербезопасности. В результате 14% организаций заявили, что пересмотрели свои концепции кибербезопасности, и лишь 7% посчитали свои стратегии кибербезопасности достаточными в период пандемии.

Объект (информационная система) меняется гораздо быстрее, чем способна на это реагировать система защиты, и результаты работы ИИ непредсказуемые. Следовательно, создать правила для защиты не всегда возможно

Рост числа сотрудников, работающих удаленно, привел к увеличению количества попыток сканирования промышленных сетей. В результате компании признают недостаточность своих процедур кибербезопасности в чрезвычайных условиях.

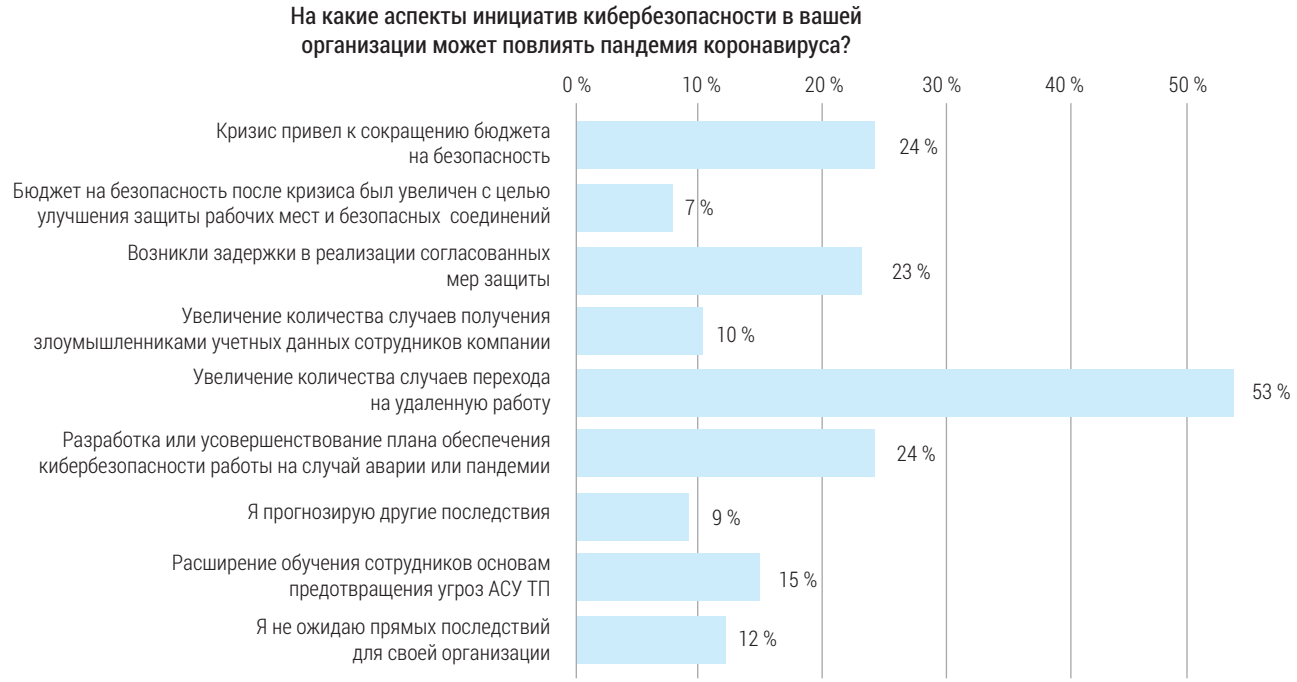
Еще одной примечательной особенностью стало то, что всего 24% респондентов согласились с необходимостью пересмотра внутренних процессов обеспечения безопасности во время пандемии. Аналогично лишь 15% предлагали своим сотрудникам специальное обучение основам безопасной работы из дома. Это говорит о том, что подавляющее большинство респондентов не видело необходимости ни в изменении процессов обеспечения безопасности, ни в организации дополнительного обучения для своих сотрудников во время пандемии *(см. «Результаты опроса…»)*.

Ред.: ***Какие основные пробелы существуют сегодня при реализации мер обеспечения кибербезопасности объектов ТЭК?***

А.П.: В первую очередь я бы выделил человеческий фактор, который включает в себя ряд аспектов:

Во-первых, достаточно низкий уровень грамотности в информационной безопасности (ИБ), затрудняющий проработку вопросов ИБ как на верхнем уровне принятия решений, так и на уровнях детализации данных решений и их реализации. Например, часто на предприятиях считают, что любое окно с логином и паролем

РЕЗУЛЬТАТЫ ОПРОСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»



Q10 — Последствия пандемии (во всем мире), 606 ответов от 337 участников опроса.
Вариант «Воздержался от ответа» исключен.

невозможно обойти в принципе, а значит и усиливать меры ИБ тоже не стоит. Специалист же информационной безопасности обозначит несколько проблемных мест. Первое – необходимость определить устойчивость данного окна авторизации к взлому. Второе – возможность воздействовать на систему, не авторизуясь в ней, а прямо через поля логин и пароль («SQL-инъекции»). И эти вопросы обязательно необходимо исследовать применительно к каждой системе и IT/OT-инфраструктуре в целом. Из-за этого зачастую строятся огромные MES, цифровые, автоматизированные и информационные системы, почти не защищенные в части ИБ. А если все построено так, что окно авторизации легко можно обойти, то, когда вопрос «всплывет», затраты на защиту системы могут быть значительными.

Во-вторых, обеспечение информационной безопасности – это процесс, который включает в себя технические и человеческие ресурсы. Система информационной безопасности по сути должна пронизывать действия всех сотрудников, работающих с АСУ ТП, ИТ-ресурсами. Даже для маленького производства требуется несколько человек, которые создали бы эту систему. Но найти сотрудников, способных создать и поддерживать такую систему, достаточно сложно, особенно учитывая необходимость значительных инвестиций на первых этапах.

В-третьих, достаточно резкий скачок, который происходит последние пару лет между тем временем, когда отсутствие системы ИБ приносило неощутимый для предприятий ущерб, и сегодняшним миром, когда вредоносное ПО или компьютерная атака могут нарушить деятельность предприятия на дни, недели, месяцы. Требуются значительные инвестиции, что делает ИБ, скажем прямо, неадекватным для многих руководителей на первый взгляд. Но это так. Слишком долго ИБ не уделялось достаточного внимания.

Рост числа сотрудников, работающих удаленно, привел к увеличению количества попыток сканирования промышленных сетей. В результате компании признают недостаточность своих процедур кибербезопасности

Но популярность и грамотность в части ИБ растет: вузы все активнее готовят специалистов, добавляют минимальные курсы по ИБ в свои программы; многие специалисты из АСУ ТП и ИТ переходят в ИБ; государственные структуры, например ФСТЭК, ФСБ и Минэнерго, ведут системную работу с предприятиями, поэтому, надеюсь, ситуация в ближайшие пару лет изменится в лучшую сторону.