Игорь ДУША

«От импортозамещения в сфере безопасности к технологиям проактивного реагирования»

Повышенный спрос на базовые продукты информационной безопасности, регламентированные нормативными актами, обусловлен импортозамещением зарубежных решений и требованиями регуляторов. Однако защита от кибератак становится еще более актуальной на фоне растущей активности злоумышленников, поэтому руководители предприятий пересматривают свое отношение к вопросам ИБ. Компании стремятся не просто мигрировать на российские решения, а усовершенствовать технологии проактивного реагирования на угрозы. При внедрении продуктов и процессов ИБ на промышленных предприятиях важно учитывать их особенности. О представленных на рынке ИТ-продуктах и трудностях, с которыми сталкиваются заказчики при внедрении ИБ-платформ, в интервью журналу Connect рассказал директор портфеля решений экосистемы в области информационной безопасности НОТА КУПОЛ Игорь Душа.

– В чем специфика реализации проектов по внедрению средств ИБ на промышленных предприятиях?

– Особенности реализации подобных проектов схожи с внедрением любых технологий автоматизации в промышленных компаниях. Они обусловлены прежде всего продолжительным жизненным циклом производства, а также длительной эксплуатацией любых решений в промышленности. Это касается как оборудования автоматизации, общесистемного ПО, например, операционных систем (ОС), так и других средств, в том числе предназначенных для обеспечения информационной безопасности.

Программно-технические комплексы и программное обеспечение со временем устаревают и снимаются с поддержки производителем. В таких условиях обнаруженные уязвимости, известные злоумышленникам, невозможно устранить путем обычного обновления систем. Более того, зачастую не удается модернизировать только один компонент системы автоматизации (например, обновление ПО SCADA), так как его замена или обновление может потянуть за собой необходимость замены общесистемного ПО, а вслед за ними – инструментов автоматизации, ОС и даже парка аппаратных средств.

В текущих условиях доступ к техподдержке ряда ИТ-решений, в том числе в сфере сетевой безопасности, также может быть существенно ограничен. Еще одна особенность заключается в том, что инвазивные мероприятия по внедрению средств ИБ зачастую возможны только в рамках «технологических окон» – специально выделяемого времени, когда оборудование не используется активно для проведения работ. Это позволяет свести к минимуму непредвиденные риски остановки производства.

– Какие условия должны соблюдаться для обеспечения безопасной разработки средств промышленной автоматизации?

– Условия предусмотрены нормативными документами: госстандартами и приказами ФСТЭК России. Критерии безопасной разработки ПО для объектов КИИ указаны в п. 29.3 Приказа ФСТЭК России № 239. В частности, ПО должно проходить статический и динамический анализ, а для ИТ-продуктов необходимо сформировать модель угроз и осуществить проверку безопасности.

В проектах промышленной автоматизации особое внимание уделяют надежности любых внедряемых средств. Ее расчет для ИТ-систем – отдельное и достаточно сложное направление, особенно если необходимо учитывать возможные риски ИБ. Одно из перспективных направлений – применение методов формальной верификации, подразумевающей математическое доказательство

соответствия требованиям. Пока метод является предметом обсуждений внутри профессионального сообщества, однако через пять-десять лет формальная верификация трансформируется в инструмент, доступный на практике. Сегодня есть практические примеры расчета функциональной надежности, но даже они относительно редко учитывают риски ИБ ввиду особой сложности.

– В отличие от разрабатываемых инструментов, возможности экосистемы продуктов НОТА КУПОЛ уже доступны на рынке. Для каких сегментов промышленности она предназначена?

– При разработке экосистемы НОТА КУПОЛ учитывалась специфика различных отраслей, в том числе промышленных предприятий, заинтересованных в автоматизации ИБ-процессов и управлении ими. На данный момент на рынке представлено не так много средств, предназначенных для обеспечения контроля безопасности и управления инфраструктурой крупных территориально разделенных предприятий. Еще меньше – комплексов, которые в автоматизированном режиме позволяют оценить состояние безопасности ИТ-инфраструктуры и контролировать все внешние каналы коммуникации и уязвимости.

– Расскажите, как выполняемые функции связаны с особенностями защиты промышленных предприятий?

– В сетях общего пользования вновь найденные уязвимости ПО чаще всего устраняются обновлением ПО. В промышленности это не всегда возможно. Чтобы исключить угрозы эксплуатации уязвимостей на промышленных предприятиях, требуется принять компенсирующие меры защиты, которые не позволят злоумышленникам использовать эту уязвимость. Один из вариантов – установить дополнительную политику на имеющееся средство защиты, например, межсетевой экран или IPS. При этом нужно понимать, что вектор для эксплуатации уязвимости будет закрыт, а новая политика не навредит бизнес-процессам.

Когда политик безопасности в ведении специалиста ИБ на всех средствах защиты менее ста, ими легко управлять, а когда их сотни, а в некоторых случаях тысячи или сеть распределена, – необходимы специальные средства автоматизации. Именно такие инструменты мы разработали – НОТА КУПОЛ. Документы и НОТА КУПОЛ. Управление.

– При обсуждении задач ИБ часто речь идет о возможностях внешнего воздействия на информационные системы. Однако большую опасность представляют и внутренние угрозы, например, манипуляции параметрами технологического процесса в целях хищения. Какие варианты защиты и профилактики доступны российским предприятиям?

– Борьба с внешними угрозами – сложная задача, но в большинстве случаев требует универсальных подходов. Это объясняется тем, что киберпреступники нередко используют типовые векторы атак, направленные, в основном, на внешний контур организации. К наиболее распространенным методам относятся фишинг, социальная инженерия. Когда речь идет о компрометации периметра и действиях злоумышленника внутри производственной инфраструктуры, характер угроз зависит непосредственно от предприятия и отрасли. Это могут быть манипуляции с целью хищения ресурсов в обход средств учета, а также кража важной информации: документов, списков заказчиков, прайс-листов.

Для защиты и профилактики внутренних угроз сотрудникам ИБ-подразделений и отделов по предотвращению экономических преступлений следует использовать комплексный подход, сочетающий организационные и технические меры. В перечень управленческих инструментов входят обучение персонала, соблюдение правил информационной и экономической безопасности. В политиках организации должны быть отражены юридические последствия несоответствия установленным регламентам. Другие эффективные методы – обучение способам обнаружения и профилактики нарушений.

При разработке экосистемы НОТА КУПОЛ учитывалась специфика различных отраслей, в том числе промышленных предприятий, заинтересованных в автоматизации ИБ-процессов и управлении ими.

В числе технических средств стоит отметить, например, DLP-системы, инструменты обезличивания данных, обеспечивающие сохранность персональных данных в отдельных сценариях. В отдельных отраслях применяются специальные технологии, например, системы на базе ИИ, которые помогают обнаруживать мошеннические действия. Они используются, например, в банковской отрасли, нефтехимии.

– Какие проекты, реализованные вашей компанией за последнее время, вы хотели бы отметить и почему?

– Недавно мы завершили внедрение модуля НОТА КУПОЛ. Документы

на крупном производственном предприятии. Проект был реализован с учетом требований 187-ФЗ. Установка инструментов позволила автоматизировать различные процессы – от инвентаризации активов до разработки документации по присвоению класса защищенности КИИ. Работа предусматривала участие в эксплуатации продуктов не только специалистов по ИБ, но и топ-менеджеров. Благодаря этому руководители смогут оценивать риски и особенности исполнения задач по информационной безопасности, а в дальнейшем – использовать данные из программного комплекса для принятия стратегических решений.

На одном из нефтехимических предприятий мы провели пилотную эксплуатацию модуля HOTA КУПОЛ. Управление для организации сетевой инфраструктуры, включающей более 400 межсетевых экранов. Это позволило автоматизировать систему, а также предоставило заказчику удобный аналитический инструмент для работы с большим количеством правил и политик безопасности. Важным фактором стало то, что платформа заменила собой зарубежное решение, которое не имело аналогов на российском рынке.

– С какими трудностями сталкиваются промышленные предприятия при внедрении средств ИБ?

– Рынок российских решений динамично развивается, но импортозамещение в сфере информационной безопасности – долгий процесс, и пока еще не все сегменты обеспечены отечественным аналогами в полной мере. Это создает определенные сложности для предприятий.

При выборе решения следует учитывать экспертизу вендора или интегратора. Необходимость разобраться в предлагаемых системах и выбрать подходящую может стать вызовом для организации. Для внедрения ИБ-средств на промышленных предприятиях требуются высококвалифицированные специалисты. Дефицит кадров на российском рынке пока не позволяет удовлетворить потребности производств в найме сотрудников, которые обеспечат эффективную реализацию проектов.

При выборе решения следует учитывать экспертизу вендора или интегратора.

– Как вы оцениваете попытки участников рынка объединиться для создания продукта, способного стать базовым в той или иной индустрии? Есть успешные примеры реализации такого подхода?

– Производственные компании активно и часто обсуждают между собой возможности взаимодействия. Наряду с этим крупные ИБ-игроки стремятся создавать свои экосистемы продуктов, охватывающие широкий спектр задач. Объединение всех функций в рамках одного сервиса – непростая задача, поэтому востребованность узкоспециализированных решений сохранится. Возможна и совместная эксплуатация нескольких продуктов, что даст дополнительную ценность в виде повышенных технических параметров решений. Наша компания, в частности, ориентируется именно на автоматизацию эксплуатации уже существующих СЗИ и поэтому активно развивает взаимодействие с производителями. Разрабатывая методы автоматизации, мы стремимся к технологическому партнерству с поставщиками средств защиты, в частности межсетевых экранов, как фокусных на текущий момент.

– Какие технологии для обеспечения ИБ производственных площадок сейчас наиболее востребованы?

– Востребованы достаточно простые инструменты и технологии, перечень которых предусмотрен требованиями регулятора. К ним относятся средства антивирусной защиты, межсетевые экраны, механизмы обнаружения вторжений, SIEM-системы. Крупные производственные объединения, которые давно внедрили базовый набор инструментов, сосредоточены на импортозамещении ранее применяемых зарубежных технологий. Лишь небольшая доля предприятий внедряет дополнительные средства ИБ или исследует возможности новых перспективных продуктов. Однако это довольно крупные предприятия, поэтому рынок в этом направлении уже развивается.

– А какие технологии в сфере ИБ вы считаете наиболее интересными для промышленных предприятий?

– Системы для автоматизации процессов ИБ, технологии ИИ, упрощающие, например, выявление новых угроз. Такие продукты еще не так широко распространены на российском рынке. Однако импортозамещение близится к завершению, одновременно повышается зрелость процессов, формируется культура информационной безопасности. Промышленные предприятия хорошо осознают актуальность этих проблем. Им интересны продукты, которые не просто помогают соблюдать требования регулятора, но и решают задачи безопасности на более высоком уровне.

На мой взгляд, совсем скоро произойдет переход от базовых ИБ-инструментов к продвинутым средствам автоматизации – мониторингу, XDR-, NSPM-системам. Инструментарий, который уже тестируют некоторые заказчики, в перспективе будет востребован и промышленными предприятиями. ■