Леонид УХЛИНОВ:

«Система защиты не должна искажать характеристик работы АСУ ТП»

За последнее время российские законодатели существенно обновили правовые акты, связанные со сферой информационных технологий. Одной из важнейших тем здесь, безусловно, является безопасность работы автоматизированных систем управления технологическими процессами критически важных объектов (АСУ ТП КВО). Эти вопросы будут обсуждаться на конференции «Информационная безопасность АСУ ТП критически важных объектов», организованной Издательским домом «КОННЕКТ».
В преддверии нашего форума мы решили побеседовать с Леонидом Михайловичем Ухлиновым, вице-президентом АО НИП «Информзащита», руководителем одного из ведущих системных интеграторов в области ИБ.

– Каково, по вашим оценкам, положение отрасли информационной безопасности в российской и мировой экономике? Какие новые тенденции помогают АО НИП «Информзащита» продвигаться на этом высококонкурентном рынке?

– Отрасль информационной безопасности за последние пять лет получила достаточно серьезное развитие, причем как в мире, так и в Российской Федерации. В первую очередь необходимо отметить,

что существенно повысилась интеллектуальная составляющая всех систем автоматизации. Автоматизация бизнес-процессов, роботизация, применение искусственного интеллекта, внедрение Интернета вещей – все эти новые технологии требуют параллельного развития средств информационной безопасности.

Сегодня возрастает понимание руководителями компаний необходимости внедрения решений по информационной безопасности как инструментов, которые защищают сам бизнес, а не только информационные системы. Кроме того, идет активное развитие нормативной базы, причем можно наблюдать параллельное развитие как международных норм по информационной безопасности, так и национальных законов и подзаконных актов, которые регламентируют все аспекты информационной безопасности в России.

Следование всем этим тенденциям и определяет ближайшие перспективы развития для «Информзащиты», поскольку наша компания – довольно специализированное предприятие. Мы работаем на рынке уже 25 лет и занимаемся исключительно вопросами информационной безопасности. Именно в этой сфере компания располагает всеми необходимыми компетенциями.

Одно из важнейших для компании направлений развития – Security Operations Center (IZ:SOC), причем развиваем его в сторону SOCaaS (Security Operations Center as a Service – «SOC как услуга»). Мы создали у себя один из лучших в России центров управления безопасностью. Помимо мощной технической инфраструктуры и целого ряда уникальных методик, в «Информзащите» собрался уникальный коллектив, который способен решать задачи по мониторингу инцидентов информационной безопасности, проведению расследований этих инцидентов и выработке рекомендаций для наших клиентов, каким образом им в дальнейшем избежать утечки информации либо других киберугроз.

Мы формировали свой продуктовый портфель в течение длительного времени и сегодня можем позволить себе участие в комплексных проектах под ключ.

Мы создали у себя один из лучших в России центров управления безопасностью.

– Какие новые продукты появились в ассортименте вашей компании за прошедшие два года? Чем вы руководствуетесь при наполнении продуктового портфеля?

– Прежде всего потребностями рынка и теми запросами, которые получаем от заказчиков. Мы формировали свой продуктовый портфель в течение длительного периода времени и сегодня можем позволить себе участие в комплексных проектах под ключ.

Сегодня мы готовы предоставить заказчику систему управления ролевыми моделями, в которую входит все, что связано с регламентацией доступа к ресурсам предприятия, к функциям информационных систем, включая контроль деятельности администраторов информационной безопасности.

Еще одна интересная новинка – система управления безопасностью конфигураций. Как мы знаем, любая информационная система не является неким фиксированным продуктом, который не меняется после ввода в эксплуатацию. Изменению подвержены все системы, в том числе и системы защиты, поэтому отслеживание конфигураций, тех или иных угроз и формирование понимания новых киберугроз, связанных с изменением конфигураций, становится важной задачей, особенно для людей, которые занимаются развитием ИТ-инфраструктуры и систем безопасности.

За последнее время АО НИП «Информзащита» также разработала новые решения в области платформы безопасной аутентификации и авторизации пользователей. Естественно, эти решения в большей степени интересны для таких сфер, как облачные структуры, облачные конфигурации. В ближайшее время будем выводить эти решения на рынок.

Перспективной новинкой является автоматизация деятельности органа криптозащиты, который имеется в любой серьезной организации, располагающей криптографическими системами защиты информации как каналов передачи данных, так и внешних носителей. Автоматизация всей деятельности по управлению ключами, по регистрации устройств, по взаимодействию с регуляторами, отслеживание временных интервалов по смене ключей – все это покрывается нашим новым решением. Мы создали его с использованием ресурсов центра разработки программного обеспечения компании.

Все перечисленные направления в АО НИП «Информзащита» развиваются с целью усилить наши конкурентные преимущества на рынке информационной безопасности.

– По мнению многих экспертов, главным драйвером развития рынка ИБ сейчас является Закон № 187-ФЗ «О безопасности КИИ». Вы согласны с этим утверждением? Какие услуги АО НИП «Информзащита» предлагает в помощь клиентам по реализации требований названного закона?

– Закон № 187-ФЗ «О безопасности КИИ», безусловно, драйвер развития рынка информационной безопасности, но я бы не сказал, что главный, поскольку он охватывает лишь критическую информационную инфраструктуру, не покрывая остальных аспектов информационной безопасности.

А разве программа цифровой трансформации экономики России не является мощнейшим драйвером ИБ? Этот национальный проект охватывает все сферы экономики страны. Забыть о кибербезопасности при переходе на цифровые технологии означает забыть об эффективности трансформации. Рынок намного сложнее, и мы видим гораздо больше потребностей в области информационной безопасности, чем в сфере критической инфраструктуры.

Если просмотреть все подзаконные акты, которые изданы регуляторами по реализации Закона № 187-ФЗ, то мы увидим, что все начинается с аудита ИТ-инфраструктуры и ресурсов, с категоризации, с выявления критичных ресурсов по защите информации, затем уже дело доходит до создания систем защиты, их внедрения и обслуживания. АО НИП «Информзащита» предоставляет заказчикам полный спектр услуг – от тестов на проникновение и выявление возможных каналов утечки, создания моделей угроз до проектирования и внедрения систем защиты, а также их обслуживания.

– На каком этапе сейчас находится реализация требований Закона № 187-ФЗ в российской промышленности? Как вы оцениваете уровень защищенности российских промышленных предприятий по результатам проделанной работы?

– Работа по реализации требований находится на начальном этапе. Закон № 187-ФЗ принят два года назад, но сегодня выполнены работы в основном по категорированию объектов критической инфраструктуры. Дальнейшая работа, как правило, упирается в сложно решаемую проблему: предприятию необходим бюджет, причем достаточно большой, для того, чтобы система защиты соответствовала той категории, которую определили на начальном этапе работ.

На мой взгляд, настал момент перейти от желания выполнить все требования закона с минимальными затратами к обеспечению реальной безопасности критической инфраструктуры предприятия. Просто отчитаться перед ФСТЭК в том, что категорирование завершено и что-то сделано в области разработки моделей угроз, – это лишь самое начало процесса. Главная задача – создать систему защиты, которая будет соответствовать современным технологиям. Зачастую компании, которые работают на этом рынке, указывают в своих материалах следующее: «Мы обеспечим выполнение текущих требований регулятора». Это неправильно! Наша компания стоит на других позициях: «Мы обеспечиваем безопасность критической инфраструктуры, а не только оформляем необходимые документы и формуляры для регулятора».

> Главная задача – создать систему защиты, соответствующую современным технологиям.

До выхода Закона № 187-ФЗ уровень информационной безопасности предприятий был гораздо ниже сегодняшнего. Однако требуемый уровень безопасности объектов критической инфраструктуры еще не достигнут – мы только на пути к этому.

– Переходя к более узкой тематике АСУ ТП: насколько проекты в области информационной защиты промышленных сетей востребованы сейчас на российском рынке? Для каких АСУ ТП особенно сложно организовать полноценную защиту?

– Безопасность АСУ ТП обсуждается с момента появления таких систем, хотя повышенное внимание к этому сектору стало уделяться в последние пять лет. Особенность всех проектов, связанных с безопасностью АСУ ТП, заключается в том, что для построения их защиты необходимо привлекать специалистов исключительно по АСУ ТП, поскольку в этих системах применяются внутренние технологические протоколы.

Особенности обычных информационных систем всем хорошо известны, и все они давно уже стандартизованы. Конечно, стандартизация существует и в секторе АСУ ТП, однако протоколы разные, потому и последовательность применения средств защиты, и их состав значительно отличаются от того, что имеется для обычных ИС.

Ключевая особенность этих проектов заключается в следующем: необходимо сохранить все характеристики работы АСУ ТП при внедрении средств защиты. Поясню на простом примере: в информационных системах, если мы поставим межсетевой экран, который будет генерировать задержку доставки пакета до рабочего места клиента длительностью 2–3 секунды, никто этого просто не заметит. А теперь представьте себе систему управления ядерного реактора: задержка в долю секунды при поднимании и опускании стержней может привести к катастрофе планетарного масштаба. Поэтому система защиты не должна искажать характеристик работы АСУ ТП как объекта

защиты. Мы должны обеспечить минимальное вмешательство в работу оборудования при сохранении максимального контроля над безопасностью объекта.

Не все способны выполнить такую ювелирную работу: специалист по информационной безопасности не всегда в деталях и тонкостях понимает функционал той или иной системы управления. Поэтому мы создали в своей компании Центр промышленной безопасности, в который набрали специалистов по АСУ ТП – уникальных экспертов, в том числе из числа наших «воспитанников». Это результат сотрудничества «Информзащиты» с российскими вузами, с производителями АСУ ТП, со многими вендорами на российском рынке.

Мы имеем большое наследие еще со времен СССР, когда АСУ ТП создавались на заводах местными специалистами – эти люди ушли, документации на предприятиях нет, и сегодня никто не знает, на каких принципах работают их системы автоматизации. Прежде чем заниматься защитой информации в такой среде, приходится изучать оборудование предприятия, выяснять, как именно работает АСУ ТП.

– Какие рекомендации можно дать компаниям, которые в процессе категорирования обнаружили у себя значимые объекты КИИ? Какие механизмы защиты им стоит внедрить в первую очередь?

– Исходя из опыта реализации таких проектов, хотелось бы особо выделить один из механизмов – сегментацию объектов информационной инфраструктуры по уровню защищенности. Речь идет об изоляции объектов с необходимостью наиболее высокой степени защиты и о выделении демилитаризованных зон.

Второй важный аспект – мониторинг работоспособности ИТ-инфраструктуры, той инфраструктуры, которая обеспечивает работоспособность и реализацию всех бизнес-процессов, а также мониторинг событий информационной безопасности, включая реагирование на инциденты и оперативное расследование инцидентов. Все это требует создания SOC.

Далее, обязательно создание службы информационной безопасности либо, если это невозможно по ряду причин (отсутствие бюджета, невозможность расширения штатной структуры), заключение

сервисного договора на обслуживание, аутсорсинг со специализированными организациями.

– Какие проекты по внедрению российских продуктов были для вашей компании наиболее поучительны? Как вы оцениваете уровень зрелости российских промышленных предприятий по реализации проектов в области информационной безопасности?

– Нам, разумеется, больше всего интересны комплексные проекты. Мы должны учитывать существующий ландшафт информационной безопасности. Когда мы приходим в какую-то компанию или крупную структуру, обычно там присутствуют средства защиты как от российских, так и от зарубежных вендоров, и нам доставляет особое удовольствие показать по завершении проекта заказчику, что мы сохранили его инвестиции в имеющиеся средства защиты, добавив к ним лишь те функции, которые были ему максимально необходимы для обеспечения безопасности. Понятно, что каждого заказчика волнует эффективность потраченных денег, и в этом отношении мы придерживаемся строгих принципов: заказчик не должен слышать от нас, что все, что у него было раньше, нужно снести и построить новую систему с нуля. Мы стараемся по максимуму сохранить все, что было, и добавить наши новые знания, новые возможности. Именно в этом мы видим свое конкурентное преимущество.

Что же касается уровня зрелости российских промышленных предприятий, то сейчас информационная безопасность там гораздо выше, чем несколько лет назад. За последние годы, что отрадно отметить, заметно выросла компетенция заказчиков: все видят необходимость внедрения решений ИБ, понимают терминологию, у большинства заказчиков выделены специалисты, которые занимаются защитой информационных ресурсов.

> Нам удалось создать коллектив единомышленников, которые способны решать любые задачи.

– Насколько в целом успешной, на ваш взгляд, оказалась стратегия импортозамещения в области информационной безопасности? Остались ли области, где российских продуктов по-прежнему не хватает?

– Традиционно наши отечественные разработчики были сильны в средствах криптозащиты, поскольку российская криптография базируется на мощной математической школе. Если вы сегодня посмотрите публикации форумов по криптографии, то найдете множество российских трудов, которые легли в основу тех или иных решений, – это и криптографические протоколы, и квантовая криптография, и многое другое.

Однако все, что касается решений, связанных с интеллектуальным насыщением систем защиты (не просто зашифровать данные, а сделать систему управляемой, адаптивной, провести интеграцию средств выявления инцидентов со средствами решения инцидентов), то наши зарубежные коллеги стали заниматься этими вопросами раньше. Мы на сегодняшний день еще не достигли такого состояния, когда можно было бы говорить о 100%-ном замещении всех средств защиты.

> Безопасность промышленных систем мы рассматриваем в качестве одного из перспективных направлений роста нашего бизнеса.

– В каком направлении планирует развиваться ваша компания в области защиты промышленных систем? Как будет совершенствоваться ассортимент используемых вами продуктов и развиваться партнерская политика?

– Прежде всего я хотел бы сказать, что безопасность промышленных систем мы рассматриваем в качестве одного из перспективных направлений роста нашего бизнеса. Три года назад был создан Центр промышленной безопасности, и сегодня он уже вышел на хорошие объемы заказов. Но самое главное – нам удалось создать коллектив единомышленников, которые способны решать любые задачи, в том числе связанные с защитой АСУ ТП в сложных условиях производства.

Мы делаем большие инвестиции тестовую базу: сегодня у нас более 150 стендов, на которых можно смоделировать любую систему и любую ситуацию, связанную с управлением производственными процессами. Наша компания ориентируется на более глубокое партнерство с производителями технологий и программного обеспечения, анализирует интересные тренды на производстве, в частности внедрение робототехники.

Таким образом, будущее АО НИП «Информзащита» – повышение интеллектуальной составляющей проектов. ■