Киберзащита критически важных объектов России

17–18 марта в Москве прошла четвертая конференция «Информационная безопасность АСУ ТП критически важных объектов» (ИБ АСУ ТП КВО), организованная Издательским домом «КОННЕКТ». В центре внимания делегатов форума были практические проблемы обеспечения информационной безопасности автоматизированных систем управления (АСУ) технологическими процессами (ТП) критически важных объектов (КВО), вопросы создания защищенных АСУ ТП, перспективы импортозамещения в области создания АСУ ТП и систем защиты информации АСУ ТП. Партнерами конференции в этом году стали компании «АйТи Бастион», УЦСБ, «Инфосистемы Джет», Positive Technologies, ТСС, InfoWatch, которые развернули в фойе форума свои демонстрационные стенды. Информационные спонсоры – профильные журналы «Нефтяное хозяйство», «Нефть России» и информационно-аналитический портал MetalTorg.Ru.

К участию в конференции были приглашены представители органов исполнительной власти, отраслевые регуляторы, предприятия топливно-энергетического комплекса, нефтехимической отрасли, транспортной индустрии, металлургии, машиностроения и оборонно-промышленного комплекса, а также разработчики средств промышленной автоматизации и производители и интеграторы в области защиты информации. На этот раз конференция собрала более 220 делегатов из различных коммерческих компаний, государственных ведомств и научных заведений, которые прослушали свыше 30 докладов и поучаствовали в круглом столе по перспективам импортозамещения в сфере АСУ ТП и средств защиты АСУ ТП для критически важных объектов.

Международные аспекты безопасности

Конференцию открыл **Владислав Шушин, советник Секретариата Организации Договора о коллективной безопасности (ОДКБ)**, который зачитал

Владислав ШУШИН,
советник Секретариата Организации Договора о коллективной безопасности (ОДКБ)

Виктор ГАВРИЛОВ,
главный специалист по ИБ, ФИЦ ИУ РАН

Сергей ГАРБУК,
Фонд перспективных исследований (ФПИ)

приветственное слово **генерального секретаря ОДКБ Николая Бордюжи**. В приветственном слове отмечалось, что сегодня идет сложный процесс сближения международных отношений в такой области информационной безопасности, как совместное противодействие преступности в сфере информационных технологий. В настоящее время в формате Организации Договора о коллективной безопасности проводится активная работа по разработке и формированию практических механизмов сотрудничества на данном направлении. В рамках ОДКБ сформирован Консультационный координационный центр по вопросам реагирования на компьютерные инциденты, который уже приступил к работе. Обеспечение защиты критически важных объектов стран – участниц ОДКБ находится в сфере его интересов.

В конференции впервые приняла участие делегация Республики Беларусь, где также занимаются решением проблем информационной безопасности критически важных объектов информатизации (КВОИ) – именно такой термин используется в законодательной базе нашего соседа. Подробности организации защиты КВОИ в Республике раскрыл **Анатолий Матвеев, начальник отдела Оперативно-аналитического центра при Президенте Республики Беларусь**. Указ Президента Республики Беларусь по КВОИ № 486 был подписан еще 25 октября 2011 г. А 30 марта 2012 г. постановлением Совета Министров Республики Беларусь № 293 «О некоторых мерах по обеспечению безопасности КВОИ» были утверждены и требования по информационной безопасности к этим объектам.

К критически важным объектам информации в Беларуси были отнесены предприятия из таких отраслей, как транспорт, энергетика, ТЭК и водоснабжение. Подробности реализации требований защиты КВОИ на конференции раскрыл **Сергей Стефанович, начальник отдела информационной безопасности Службы безопасности РУП «Белтелеком»**. У этого оператора часть систем была признана как КВОИ со всеми вытекающими последствиями. Компания распределила свои информационные системы по шести классам защиты и обеспечивала для каждого из них соответствующие механизмы защиты. Для наиболее критичных пришлось даже

Виталий ЛЮТИКОВ,
начальник управления ФСТЭК России

использовать метод макетирования, при котором все изменения вначале тестируются на специально построенном макете и только после всесторонней проверки переносятся на боевую систему. Это достаточно дорого в эксплуатации, но зато обеспечивает обновление всего программного обеспечения и исправление, как минимум, обнаруженных уязвимостей. Таким образом, Беларусь продвинулась в части правового обеспечения защиты критической инфраструктуры дальше России.

Однако проблемы с обеспечением безопасности КВОИ по-прежнему остаются. Связано это с тем, что промышленные информационные системы в Беларуси в основном иностранного происхождения и построены из типовых компонентов. Производителям требуется доступ к установленным продуктам для обновления функционала, устранения ошибок и технического обслуживания. Для этого используется либо удаленный доступ, либо подключение компьютеров сотрудников технической службы напрямую к промышленной сети. Сейчас для удобства управления промышленные сети все чаще подключают к корпоративной сети, что позволяет внешним злоумышленникам получить удаленный доступ, в частности, к промышленному сегменту. Причем защита корпоративной сети чаще оказывается более надежной, поскольку в промышленной используются операционные системы и программное обеспечение, которые годами не обновлялись. Антивирусов и других средств защиты в промышленной сети обычно нет, поэтому злоумышленнику достаточно проникнуть внутрь корпоративной сети, а получить затем доступ к промышленной не составляет труда. При этом нет правового регулирования отношений между организациями, эксплуатирующими КВОИ, и разработчиками АСУ ТП в части обеспечения информационной безопасности.

Деятельность ФСТЭК

Тема информационной безопасности критически важных объектов активно развивается последние несколько лет и в России. Связано это с усилением террористической активности радикальных экстремистов в сети Интернет и созданием иностранными государствами киберподразделений своих вооруженных сил. Основными целями обоих формирований могут стать объекты критической инфраструктуры России, выведение из строя которых может нанести вред как российскому государству, так и гражданам. Понимая важность защиты подобных КВО, ФСБ России разработало и внесло в Государственную Думу законопроект «О безопасности критической информационной инфраструктуры Российской Федерации» (ID: 00/04-5890/08-13/20-13-4), который с августа 2013 г. находится на обсуждении в законодательном органе. В то же время ФСТЭК России был подготовлен приказ № 31, который предполагалось использовать в реализации принятого закона и который определяет требования к защите КВО от кибератак. Приказ был принят и вступил в силу еще в 2013 г., но закона, требующего его исполнения, до сих пор нет, поэтому пока он носит только рекомендательный характер.

Как отмечали многие участники конференции, в России остается правовая неопределенность в вопросах регулирования требований к защите критически важных объектов. Федеральное законодательство только формируется, однако на уровне ведомственных актов большое влияние на развитие этой сферы оказал приказ № 31 ФСТЭК, который хоть и является рекомендательным, но уже определил требования к средствам защиты АСУ ТП КВО. «Когда-то в Курчатовском институте дорожки прокладывали там, где сотрудники протоптали

Анатолий МАТВЕЕВ,
начальник отдела Оперативно-аналитического центра при Президенте Республики Беларусь

Сергей СТЕФАНОВИЧ,
РУП «Белтелеком»

Георгий ЦЕДИЛКИН,
компания ANP Ceges Technology

тропинки, – отметил ведущий круглого стола **Виктор Гаврилов, главный специалист по ИБ, ФИЦ ИУ РАН**. – Так и ФСТЭК своим приказом № 31 «протаптывает тропинки» в сфере безопасности АСУ ТП».

Поэтому центральным выступлением конференции был доклад **Виталия Лютикова, начальника управления ФСТЭК России**, посвященный совершенствованию законодательных требований к обеспечению информационной безопасности критически важных объектов со стороны Федеральной службы по техническому и экспортному контролю.

Стенд компании Infowatch

Стенд компании «АйТи БАСТИОН»

Стенд компании «ТСС»

Стенд компании УЦСБ

«За 2015 г. как минимум 15 крупных компаний согласовали свои политики ИБ с ФСТЭК и приступили к реализации требований, заложенных в приказе № 31, – отметил В.С. Лютиков. – В частности, они пересмотрели свои документы по информационной безопасности, а в некоторых случаях выработали даже отраслевые стандарты».

Однако приказ этот создавался два года тому назад, и сейчас настал момент привести его в соответствие с современными реалиями. Поэтому ФСТЭК инициировала процесс подготовки дополнений к приказу № 31, которые будут учитывать текущую ситуацию в сфере информационной безопасности АСУ ТП КВО. Ведомство разрабатывает соответствующий набор дополнений, а в III квартале 2016 г. планируется приступить к его публичному обсуждению. Виталий Сергеевич Лютиков предложил поучаствовать в этом процессе разработчикам АСУ ТП. «Требования по защите автоматизированных систем управления должны формировать сами разработчики АСУ ТП, – отметил он. – Сейчас же ситуация обратная – разработчики средств защиты в инициативном порядке предлагают свои средства защиты, а разработчики АСУ ТП их отвергают».

Кроме того, ожидается дополнение требований к межсетевым экранам в части выделения специального типа МСЭ, который предназначен для работы в сетях АСУ ТП. Предполагается, что такие межсетевые экраны должны поддерживать протоколы, используемые в промышленных сетях, и оказывать минимальное воздействие на технологический процесс. Требования по надежности для подобных средств защиты тоже должны быть на уровне аналогичных показателей АСУ ТП. Такой же дополнительный тип предполагается определить и в готовящемся проекте требований защиты для операционных систем. Для решения задач АСУ ТП предполагается выделить


Дмитрий БЕЗУГЛОВ,
компания «Пластик Энтерпрайз»


Андрей ФРЕЙДМАН,
компания «Науцилус»

Борис ПОЗДНЕЕВ,
ФГБОУ ВОУ «МГТУ «СТАНКИН»

Вячеслав ГРЫЗЛОВ,
Центр автоматизации в энергетике «НИИТеплоприбор»

Олег СЕРДЮКОВ,
компания «Модульные системы «Торнадо»

специальный тип операционных систем реального времени. В будущем ведомство планирует приступить к разработке требований для защиты систем управления производством.

Разработчики АСУ ТП

Следует отметить, что, по словам **Георгия Цедилкина, генерального директора ANP Ceges Technology**, в России есть собственные АСУ ТП, которые по функционалу не уступают иностранным аналогам, но проигрывают им в удобстве. Аналогичное мнение высказал **Дмитрий Безуглов, старший инженер-программист компании «Пластик Энтерпрайз»**: «Российские АСУ ТП работают не хуже иностранных, если их правильно настроить. Вот только Siemens достаточно установить, и он будет работать, а российские продукты надо еще суметь правильно настроить». Таким образом, у российских АСУ ТП есть достаточный функционал, но сопровождение этих решений, их внедрение и техническое обслуживание до сих пор не устраивают промышленные компании.

В конференции приняли участие разработчики как минимум четырех российских решений: «Квинт», Phocus, «Торнадо» и «Оператор». Они рассказали о совершенствовании своих продуктов в части обеспечения информационной безопасности. Так, **Вячеслав Грызлов, директор Центра автоматизации в энергетике «НИИТеплоприбор»**, разработчика АСУ ТП «Квинт», рассказал о планах создания новой версии системы «Квинт-8», в которой уже будут интегрированы механизмы информационной безопасности. Работа над новой версией должна быть завершена к 2020 г. На начальном этапе решение будет тестироваться совместно со сторонней системой защиты одного из российских разработчиков, но в окончательной версии механизмы защиты планируется встроить в саму АСУ ТП. Причем планируется создать и среду моделирования АСУ ТП, которая позволит решать, в частности, вопросы информационной безопасности: управляющее воздействие вначале можно проверить на модели, а затем исполнить на реальном оборудовании.

О подходах к обеспечению безопасности в АСУ ТП Phocus рассказал на конференции **Андрей Фрейдман, заместитель директора ООО «Науцилус»**. По его мнению, отказ от Windows на промышленном оборудовании сейчас является насущной необходимостью. В качестве альтернативы предлагается строить АСУ ТП на операционной системе QNX, для которой есть реализация и для российских процессоров «Эльбрус», разработанная компанией «Встраиваемые системы». Таким образом, Phocus позволяет построить АСУ ТП полностью на российском оборудовании – начиная от процессора и заканчивая собственно системой управления технологическими процессами. Видимо, этого достаточно для информационной безопасности промышленных объектов под ее управлением.

Подход компании «Модульные системы «Торнадо», которую на конференции представлял **генеральный директор Олег Сердюков**, аналогичен: создать собственный программно-аппаратный комплекс и полностью защитить его от внешних информационных воздействий. Все изменения, вносимые в работу АСУ ТП, считать за вредоносные и блокировать – это так называемая концепция «темного щита». Изменения можно вносить только в ходе регламентных работ под строгим контролем и тут же включать «темный щит». Понятно, что ни о каком удобстве эксплуатации и обслуживания в данном случае говорить не приходится.

Сергей ТРУШКИН,
советник Rusal Global Management B.V.

Владислав ПУГАЧЕВ,
ПАО «Северсталь»

Практика защиты

Исполнение требований регуляторов вызывает определенные вопросы в применении к конкретному предприятию. В частности, о некоторых из них рассказал **Сергей Трушкин, советник Rusal Global Management B.V**. Он отметил, что на крупном промышленном предприятии существует не одна система АСУ ТП, а до 50 различных систем, которые связаны с производством не только основных продуктов, но и сопутствующих компонентов, энергетикой, логистикой и выполнением других самых разнообразных задач. Сформировать для всех единые требования к безопасности удается не всегда: приходится каждую систему рассматривать в отдельности и принимать решения по защите каждой из них индивидуально. Сергей Борисович привел статистику по источникам возникновения рисков ИБ. Оказалось, что большая их часть – 56% – относится к обслуживающему персоналу и пользователям АСУ ТП, 18% – к разработчикам, 14% – к иностранным спецслужбам и конкурентам и только 12% – к внешним хакерам и другим злоумышленникам. В результате концепция «темного щита» и перехода на российские разработки не способна снизить более половины рисков.

Таким образом, для улучшения защиты нужно вначале навести порядок внутри предприятия с учетом того, что наиболее острые проблемы возникают при взаимодействии служб ИТ и АСУ ТП. Первые умеют работать в основном с типовыми и хорошо известными наборами продуктов, в то время как вторые не хотят устанавливать в свои промышленные системы никаких дополнительных элементов, которые не связаны с основным технологическим процессом. Для разрешения конфликтов и обеспечения конструктивного взаимодействия этих служб было принято решение сформировать специальный центр компетенции по проблеме обеспечения безопасности АСУ ТП, который является отдельной структурной единицей и отвечает за взаимодействие служб эксплуатации, обслуживания, разработки и модернизации АСУ ТП в целях повышения защищенности всех промышленных информационных систем от постороннего кибервоздействия.

Одной из наиболее сложных практических задач обеспечения безопасности АСУ ТП является проведение аудита информационной безопасности. Связано это с тем, что остановка промышленного оборудования сопряжена с большими расходами для предприятия, так что технологические окна для обслуживания оборудования очень маленькие и провести в них полноценный аудит безопасности не всегда удается. Тем не менее требование по внутреннему аудиту есть в приказе № 31 ФСТЭК, поэтому проводить его приходится. В частности, опытом внутренних проверок поделился **Владислав Пугачев, старший менеджер Управления обеспечения ИБ СОБ ПАО «Северсталь»**. Он рассказал о проведении внутреннего теста на проникновение в систему управления шахтной печью из резерва. Сотрудники компании сумели за пять часов проникнуть в систему управления печью и даже немного «поуправлять» ею. Она была выключена, поэтому никаких убытков от этой атаки предприятие не понесло, но, по оценкам Владислава Владимировича, стоимость простоя основного агрегата в АСУ ТП в течение часа обходится предприятию в 300 тыс. руб.

Более подробно о методике проведения аудита и выявления различных направлений политики безопасности на промышленном предприятии рассказал в своем докладе **Александр Севостьянов, начальник отдела защиты информации СЭБ ПАО «Трубная металлургическая компания»**. Он, в частности, рекомендовал выявлять несанкционированные точки доступа Wi-Fi и 3G-модемы, разбираться и наказывать сотрудников, которые допустили подобные нарушения требований безопасности. При этом посетовал, что до сих пор не разработаны эффективные и безопасные средства аудита, такие как антивирусы. По его словам, даже промышленный антивирус Лаборатории Касперского вызвал у них в компании остановку прокатного стана. Он же отметил, что системы контроля могут следить не только за информационной системой, но и за самими сотрудниками в целях предотвращения воровства дорогих расходных материалов. Для этого хорошо подходит система видеонаблюдения с функциями видеоанализа,

которая может проследить за перемещением сотрудников по цеху.

О внедрении подобной системы видеонаблюдения за сотрудниками рассказал Дмитрий Валерьевич Безуглов. Его компания «Пластик Энтерпрайз» занимается производством технической химии – порохов и боеприпасов. Производство опасное, поэтому часто возникают нештатные ситуации. Для их предотвращения была разработана система видеонаблюдения, которая интегрирована с системой АСУ ТП для выявления ситуаций, опасных для жизни обслуживающего персонала, и для снабжения сотрудников инструкциями на случай нештатной ситуации. В системе, в частности, использовался антивирус Dr.Web, также в промышленной сборке, который не вызывал никаких нареканий в процессе достаточно длительной эксплуатации. Таким образом, для обеспечения информационной безопасности АСУ ТП необходимы качественные специализированные решения.

Средства защиты АСУ ТП

Российский рынок средств защиты АСУ ТП сейчас активно развивается. На нем появляются новые классы решений, которые разработаны специально для защиты промышленных систем. На конференции были представлены российские разработки подобных инструментов защиты. В частности, **Сергей Гарбук, заместитель генерального директора Фонда перспективных исследований (ФПИ)**, предложил использовать для выработки инструментов защиты промышленных сетей методы эмуляции технологического процесса. В таком случае безопасность той или иной команды вначале проверяется на симуляторе и только потом выполняется в реальной промышленной системе. Этот метод используют, в частности, в «Белтелекоме» при макетировании изменений. В качестве среды для симуляции ФПИ предлагает разрабатываемую среду «Гербарий», для которой уже есть модели промышленных контроллеров, различных датчиков и исполнительных устройств, что позволяет быстро собрать из необходимых компонентов макет промышленной системы. Он может быть использован не только для проверки безопасности команд, но и для обучения операторов АСУ ТП правильной реакции на информационные угрозы.

Еще один метод проверки правильности средств защиты предложил на конференции **Виталий Промыслов, ведущий научный сотрудник ИПУ им. В.А. Трапезникова РАН**. Им и его коллегами разработан специальный сервис, который дает возможность проверить модель доступа к данным, используемую в организации. Сейчас существует только демонстрационная модель сервиса по адресу OMOLE.WS, позволяющая описать права доступа вручную и проверить пути наследования и делегирования прав для конкретных пользователей и групп. Сервис обеспечивает возможность моделировать распределение прав доступа на всех

Александр СЕВОСТЬЯНОВ,
ПАО «Трубная металлургическая компания»

Виталий ПРОМЫСЛОВ,
ИПУ им. В.А. Трапезникова РАН

этапах жизненного цикла информационной системы, позволяя заранее определить для каждого участника минимальный набор необходимых прав. На конференции была представлена работа по применению указанного сервиса для оценки соответствия требованиям безопасности МАГАТЭ для защиты АЭС. Следует отметить, что именно ИПУ РАН в свое время разработал АСУ ТП «Оператор» для управления атомными электростанциями, в которой еще в 1980-х гг. были предусмотрены механизмы информационной защиты.

На конференции были представлены и коммерческие продукты, которые специально разрабатывались для защиты АСУ ТП. Так, одним из производителей средств защиты для АСУ ТП является компания Positive Technologies, которая представила на конференции свой новый продукт для защиты промышленных сетей – Industrial Security Incident Manager (ISIM). О его функциональных возможностях рассказал **Олег Матыков, менеджер по продуктам Positive Technologies**. Продукт занимается сбором событий, которые происходят в промышленной сети, их анализом и выявлением признаков нападения. Продукт позволяет обнаружить попытки эксплуатации уязвимостей в промышленном оборудовании, несанкционированные действия администратора, нарушение логики технологического процесса и распределенные по времени атаки. ISIM также можно использовать для проведения расследования и ретроспективного анализа изменений в промышленном сегменте сети. При этом он может располагаться за пределами промышленного сегмента и получать необходимые для работы сведения через так называемый диод данных, который обеспечивает однонаправленную передачу информации. Такие диоды рекомендуется использовать в промышленных системах, чтобы средства мониторинга не оказывали влияния на технологический процесс.

О своем продукте на конференции рассказал и представитель Уральского центра систем безопасности (УЦСБ), где был разработан аналогичный инструмент для мониторинга промышленного сегмента АСУ ТП под названием DATAPK. **Николай Домуховский, главный инженер департамента системной интеграции УЦСБ**,

Олег МАТЫКОВ,
компания Positive Technologies

Николай ДОМУХОВСКИЙ,
компания УЦСБ

Александр НОВОЖИЛОВ,
компания «АйТи Бастион»

Даниил ТАМЕЕВ,
компания «Инфосистемы Джет»

Константин ЗДИРУК,
МГТУ им. Н.Э. Баумана

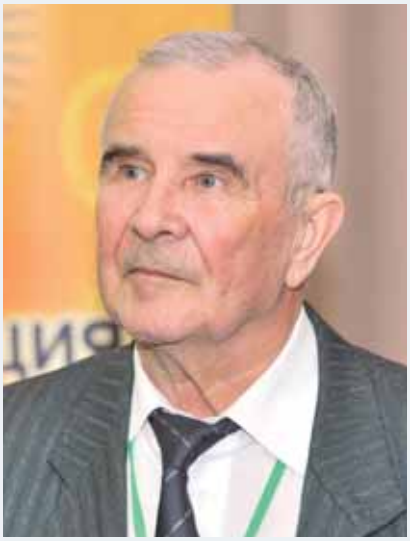
Андрей КОРНЕЕВ,
Центр проблем энергетической безопасности института США и Канады РАН

отметил, что сейчас промышленные системы бывают трех типов: изолированные, контролируемые и интегрированные. В первом случае сетевое взаимодействие только однонаправленное, во втором – строго ограничено рамками корпоративной сети, в третьем – полностью интегрировано, в частности, с Интернетом с применением необходимых средств защиты и контроля. Во всех трех типах Николай Домуховский предложил использовать DATAPK для анализа информационных потоков в промышленной сети, выявления событий, связанных с безопасностью, управления конфигурациями устройств сети и контроля соответствия требованиям регуляторов. Отдельно рекомендуется установить специализированное устройство защиты Check Point 1200R Rugged Appliance, которое будет выявлять попытки проведения сетевых атак.

Для случаев контролируемого и интегрированного подключения промышленного сегмента **генеральный директор «АйТи Бастион» Александр Новожилов** рекомендует использовать инструмент контроля за действиями пользователей. Инструмент позволяет контролировать действия производителей АСУ ТП и сотрудников их партнеров, которые занимаются техническим сопровождением промышленных решений, а также действия собственных администраторов и операторов АСУ ТП, что дает возможность в случае возникновения проблем проанализировать действия обслуживающего персонала и выявить те из них, которые привели к проблеме. Это позволяет быстро выявить причину проблем и оперативно устранить ее, а также провести расследование действий персонала и наказать виновных. Компания предлагает продукт такого класса под названием AdminBastion, который к тому же сертифицирован ФСТЭК на отсутствие недекларированных возможностей по классу НДВ4.

Впрочем, универсального решения проблем обеспечения безопасности АСУ ТП КВО на конференции предложено не было, причем неоднократно заявлялось, что такового и не может быть в принципе, поскольку все технологические процессы разные и защищать их нужно по-разному. Поэтому важная роль в защите промышленных систем отводится системному интегратору, сотрудники которого могут подобрать

Вадим ПОДОЛЬНЫЙ,
АО «Русатом автоматизированные системы управления»



Анатолий АЛПЕЕВ,
ФБУ «НТЦ по ядерной и радиационной безопасности»

необходимый набор компонентов, интегрировать их между собой, настроить под особенности конкретного технологического процесса и даже сопровождать построенную систему защиты. О возможностях системного интегратора рассказал на конференции **Даниил Тамеев, руководитель направления по работе с ПиТЭК Центра информационной безопасности компании «Инфосистемы Джет»**. Он предложил два подхода к процессу обеспечения ИБ АСУ ТП – стратегический и оперативный. В первом случае интегратор проводит полное обследование информационной системы заказчика, моделирует угрозы, выбирает средства защиты и выполняет их внедрение с последующей аттестацией. Во втором – решает самые насущные проблемы безопасности: организует контроль доступа, установку обновлений, защиту периметра и выявление целевых атак. При этом оптимально, чтобы организация, эксплуатирующая КВО, запускала оба процесса параллельно, поскольку стратегический решает проблемы долго, но гарантированно, а оперативный – быстро исправляет наиболее очевидные проблемы. Оба процесса нужны и важны.

Значимым компонентом обеспечения безопасности КВО является подготовка кадров. В управлении техническими процессами важно, чтобы специалисты были компетентными и могли правильно и своевременно принимать решения. Для этого их нужно обучить не только знаниям, но и умениям быстро выходить из кризисных ситуаций. О методиках такого обучения рассказал на конференции **Андрей Корнеев, руководитель Центра проблем энергетической безопасности института США и Канады РАН**. Он, в частности, предложил использовать для обучения операторов критически важных объектов методы контраварийного управления, в процессе которых моделируются критические ситуации. Такие методы используют для обучения операторов АСУ ТП управлению технологическим оборудованием, однако при этом зачастую не моделируются критические ситуации, связанные с информационной безопасностью. Поэтому в программы контраварийной подготовки операторов промышленных систем следует включать и критические ситуации, связанные с атаками хакеров или иностранных спецслужб на системы управления.

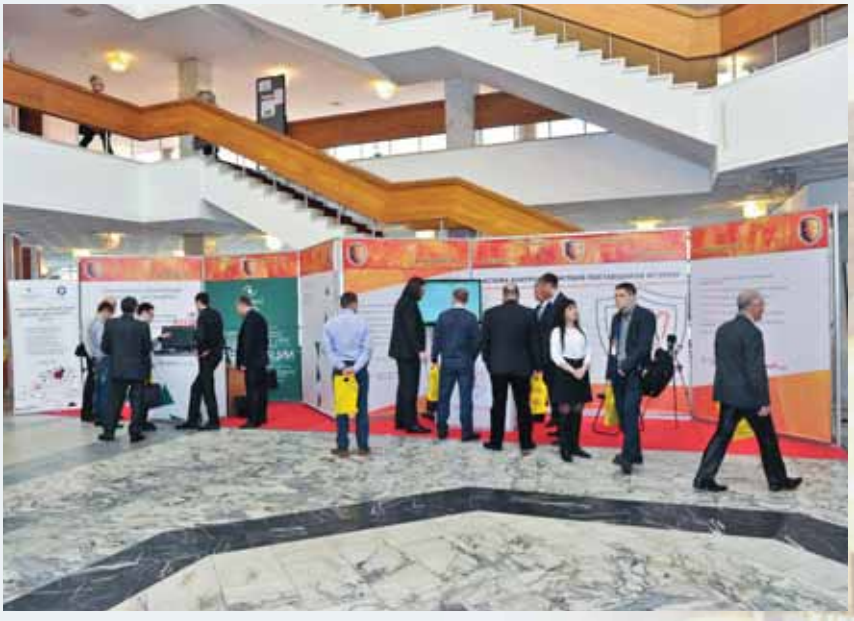
Защита импортозамещения

Важной темой в области защиты АСУ ТП является импортозамещение. Как отметил Сергей Владимирович Гарбук, сейчас в российских системах управления технологическими процессами до 80% оборудования иностранного происхождения, что не позволяет оценить его надежность при обслуживании критически важных объектов. Поэтому операторам КВО следует постепенно переходить на более доверенные решения, которые, как уже было отмечено, в России есть.

Споры на конференции вызвала сама концепция доверенного программного обеспечения. В частности, **Константин Здирук, доцент кафедры «Защита информации» Московского государственного технического университета им. Н.Э. Баумана**, отметил, что оценивать доверие к программному обеспечению по его владельцу неправильно, поскольку на свободном рынке владелец может и поменяться. Лучше оценивать уровень доверия по автору, степени контроля исходного кода и полной документации в соответствии с ГОСТом. Для этого в Университете была сформирована среда разработки, в которой автор кода фиксируется, код проверяется и для него готовится полная документация. Это позволило сформировать так называемый фонд экстремальных технологий, где есть примеры абсолютно доверенных программ.

Вадим Подольный, заместитель технического директора АО «Русатом автоматизированные системы управления», доверенными считает системы, разработанные под собственным контролем и по собственному заказу. В частности, компания разрабатывает собственные программные решения для АСУ ТП атомных станций на российском аппаратном обеспечении. «Мы не хотим делиться секретами того, что происходит в наших технологических сетях, с разработчиками иностранного оборудования», – пояснил свою позицию Вадим Павлович Подольный.

В то же время **Анатолий Алпеев, ведущий научный сотрудник ФБУ «Научно-технический центр по ядерной и радиационной безопасности»**, вообще не доверяет программируемым контроллерам, поскольку их показатели надежности могут измениться после перепрошивки. Более надежными являются непрограммируемые контроллеры, поведение которых можно хорошо исследовать и предсказать, однако их функционал ограничен. Поэтому системы управления современными критически важными объектами



он предлагает строить как из программируемых контроллеров, которые будут решать задачи управления и удобства эксплуатации, так и из непрограммируемых, которые будут автоматически защищать от аварийных ситуаций и опасных режимов эксплуатации технологического оборудования.

Финальный круглый стол

Заключительным аккордом конференции стал круглый стол, где основной тематикой было импортозамещение, но речь шла и о бизнесе российских разработчиков АСУ ТП. Отмечалось, что нормативные требования никогда не могут работать как драйвер развития рынка, особенно требования по безопасности – это скорее ограничения, которые российским разработчикам реализовать зачастую даже сложнее, чем иностранным. Поэтому российскому государству нужно не просто регулировать рынок решений АСУ ТП, но стимулировать его развитие.

В частности, Георгий Цедилкин отметил, что российские разработчики не могут конкурировать с иностранными именно по бюджетам на поддержку, и в этом им должно помочь государство – наладить техническое сопровождение решений. По его словам, сейчас государство даже дает кредиты для промышленных организаций на проведение модернизации, и было бы правильно при такой модернизации за государственный счет переходить именно на российские решения и разработки. Это связано с тем, что пока российские разработчики АСУ ТП не готовы конкурировать с иностранными на рыночных условиях – требуются определенные преференции от государства.

У российских разработчиков существует и проблема доверия – промышленные предприятия просто не очень доверяют российским разработчикам АСУ ТП и используют их в основном для автоматизации некритических технологических процессов. Если бы государство взяло на себя ответственность за реализацию нескольких крупных промышленных проектов на российском оборудовании и программном обеспечении, то это могло бы изменить отношение и коммерческих промышленных компаний к российским АСУ ТП, а сами разработчики смогли бы отладить свои производственные процессы.

В целом конференция прошла в дружественной обстановке, которая позволила обсудить насущные проблемы и выработать новые подходы к решению стоящих задач. ■

РЕЗОЛЮЦИЯ

Четвертой конференции «Информационная безопасность АСУ ТП критически важных объектов»

17–18 марта в г. Москва состоялась четвертая конференция «ИБ АСУ ТП КВО». В ее работе приняли участие 215 человек. В течение двух дней было заслушано 32 доклада и сообщения, проведен круглый стол по вопросам импортозамещения в сфере АСУ ТП и средств защиты АСУ ТП КВО.

По итогам работы конференции сформулированы следующие предложения и рекомендации.

Общие подходы

- Признать, что риски целенаправленных атак на АСУ ТП КВО возрастают с каждым годом. Необходимые предпосылки для этого (кадры, технические возможности и мотивация) в целом сформировались. Зачастую не требуется высокая квалификация исполнителя, а необходимые инструменты проведения атаки имеются в свободном доступе.
- С учетом наличия тесной связи информационной и промышленной безопасности АСУ ТП признать сложность задачи разработки типовых требований безопасности для всех отраслей промышленности. Рекомендовать учитывать отраслевую специфику при разработке требований к ИБ АСУ ТП. Отметить, что использование типовых решений защиты ограничивает возможности использования АСУ ТП.
- Признать основополагающим принципом защиты АСУ ТП отсутствие (или минимизацию присутствия) воздействия средств защиты информации непосредственно на технологический процесс. Рекомендовать разработчикам и интеграторам средств защиты руководствоваться этим принципом при построении системы защиты АСУ ТП.
- Признать неприемлемой сложившуюся практику замалчивания и крайне медленного исправления ошибок и уязвимостей в программном коде АСУ ТП мировых лидеров.
- Признать, что существующие АСУ ТП часто работают под управлением устаревших операционных систем с большим количеством известных уязвимостей.

Нормативно-правовые аспекты

- Признать отсутствие системного нормативного правового регулирования сферы информационной безопасности АСУ ТП. Необходимо скорейшее принятие Федерального закона «О безопасности критической информационной инфраструктуры РФ» как первоосновы системного подхода в указанном вопросе.
- Поддержать работу ФСТЭК России в части подготовки нормативно-методических документов по информационной безопасности АСУ ТП.
- Рекомендовать предприятиям, операторам критически важных объектов, интенсифицировать работу по реализации приказа № 31 ФСТЭК России.
- Рекомендовать промышленным компаниям, которые не имеют критически важных объектов, также учитывать рекомендации приказа № 31 ФСТЭК России по защите АСУ ТП.
- Рекомендовать компаниям – лицензиатам ФСТЭК России по технической защите информации и компаниям, специализирующимся в области разработки и проектирования АСУ ТП, активнее участвовать в разработке проектов нормативно-методических документов по защите информации и защите систем управления технологическими процессами.

- Рекомендовать операторам КВО при моделировании угроз и оценке рисков учитывать степень доверия к программному и аппаратному обеспечению. Для оценки степени доверия можно использовать такие критерии, как авторство разработки, наличие полной документации в соответствии с ГОСТ ЕСПД и контроль процессов разработки и сертификации уполномоченным государственным органом (ФСТЭК, Минобороны, ФСБ РФ).
- Рекомендовать операторам КВО во взаимодействии со ФСТЭК России, ФСБ России и отраслевыми регуляторами инициировать проработку и реализацию инициатив обмена информацией в области безопасности АСУ ТП, создание центров обмена и анализа информации в области безопасности, центров реагирования на инциденты безопасности и т. п. структур в рамках групп предприятий, вертикально интегрированных объединений, секторов и отраслей промышленности.
- Признать неприемлемой сложившуюся практику, при которой оператор КВО умышленно занижает классность объекта и, как следствие экономит на системе защите АСУ ТП, в том числе на этапе моделирования закладывая в модель угроз наиболее простые типы атак.
- Признать обязательным проведение аудита информационной безопасности во время тестового режима работы АСУ ТП до ее ввода в эксплуатацию
- Рекомендовать службам безопасности на постоянной основе производить мониторинг и инвентаризацию АРМ оператора АСУ ТП. Сложившаяся практика самовольного установления на АРМ оператора непредусмотренного ПО, открытие портов, подключение непредусмотренных регламентом роутеров несут серьезные риски. В качестве эффективной меры борьбы предлагается немедленное изъятие подобных ПК.
- При проведении аудита защищенности АСУ ТП КВО, ввиду отсутствия возможности останова работы технологического оборудования, рекомендовать использовать метод делегации прав на проверку непосредственно персоналу – операторам АСУ ТП.
- Признать необходимость контраварийной подготовки обслуживающего персонала критически важных объектов и дополнить ее базовыми сведениями о защите информации АСУ ТП.
- Рекомендовать операторам КВО интенсифицировать процесс повышения квалификации в области защиты АСУ ТП, в первую очередь среди операторов АСУ ТП.

Поддержка российских разработчиков

- Признать, что на российском рынке не в полной мере представлены все необходимые продукты для защиты АСУ ТП. Рекомендовать разработчикам средств защиты определиться с перспективными технологиями защиты АСУ ТП и включить их в свои планы разработки новых продуктов.
- Признать важность процесса импортозамещения для обеспечения безопасности АСУ ТП КВО. Отметить, что на текущий момент подавляющее большинство внедренных АСУ ТП имеет иностранное происхождение, степень доверия к которому довольно низка в условиях международных санкций.
- Отметить сложность и наличие рисков быстрого перехода на российские аналоги. Учесть тот факт, что иностранные производители имеют большой опыт работы и сопровождения АСУ ТП.
- Рекомендовать отдавать предпочтение российским доверенным продуктам АСУ ТП на новых объектах и при модернизации устаревших при условии качественного сопровождения их со стороны производителей.
- Поддержать инициативу Фонда перспективных исследований по разработке интегрированной инструментальной среды разработки АСУ ТП в качестве одного из возможных вариантов консолидации усилий отечественных разработчиков АСУ ТП. Рекомендовать разработчикам АСУ ТП принять участие в этом проекте.
- Признать, что практика удаленного подключения специалистов производителя промышленного оборудования к АСУ ТП на территории России несет дополнительные риски информационной безопасности. Рекомендовать при невозможности полностью изжить подобную практику ограничить подключение только гарантийным сроком.
- Призвать зарубежных производителей промышленного оборудования начать активное взаимодействие с отечественными разработчиками средств защиты АСУ ТП в части тестирования и гарантирования заказчику безопасности использования продуктов на собственном технологическом оборудовании. Отметить, что за последнее время ряд иностранных производителей приступили к подобному сотрудничеству.
- Рекомендовать производителям промышленного контроллерного оборудования, разработчикам программного обеспечения АСУТП на их основе и средств защиты АСУ ТП усилить совместную работу в целях создания новых или модернизации уже имеющихся инструментов защиты технологических процессов. ■