V конференция

«Информационная безопасность АСУ ТП КВО»

Рабочие моменты обеспечения безопасности АСУ ТП

В середине марта в Конгресс-центре МТУСИ прошла пятая, юбилейная конференция «Информационная безопасность АСУ ТП КВО», в которой приняли участие ФСТЭК России и другие регуляторы, представители предприятий топливно-энергетического комплекса, химической промышленности, транспорта, металлургии, машиностроения, оборонно-промышленного комплекса, ЖКХ и других отраслей, а также разработчики средств промышленной автоматизации, производители и интеграторы в области защиты информации. Промышленность представляли руководители служб ИТ, ИБ и АСУ ТП.

В центре внимания пятой конференции были обмен практическим опытом в области защиты информации в АСУ ТП, начало работы системы СОПКА по защите критически важных информационных инфраструктур, поиск диалога между эксплуатантами АСУ ТП на реальном производстве и специалистами в области ИБ. Последняя тема прошла красной нитью через все мероприятие и стала ключевой в связи с множеством вопросов, возникающих у подразделений АСУ к опыту и компетенциям ИБ-компаний и собственной службы обеспечения информационной безопасности.

Всего в мероприятии приняли участие 257 человек, выступили 30 докладчиков, которые обсуждали темы «Методы, технологии и техника защиты АСУ ТП» и «Опыт разработки и эксплуатации АСУ ТП». Причем оказалось, что программа второго дня привлекла даже больше слушателей, поскольку рассматривались проблемы внедрения средств защиты АСУ ТП. В конце второго дня состоялся круглый стол по теме «В поиске диалога. Позиции специалистов по ИБ и специалистов по внедрению и эксплуатации АСУ ТП». Выступающие были условно поделены на «асушников» и «безопасников», которые задавали друг другу неудобные вопросы. В результате длительного обсуждения пришли к выводу, что на промышленных предприятиях вполне возможна организация бесконфликтного взаимодействия между специалистами, обеспечивающими функционирование АСУ ТП, и сотрудниками, ответственными за информационную безопасность.

Мероприятие было организовано Издательским домом «КОННЕКТ». «Золотым» партнером конференции выступила компания «АйТи БАСТИОН». Партнеры конференции: «ЭЛВИС-ПЛЮС», Positive Technologies, «Газинформсервис», «Информзащита», КРОК, ГК InfoWatch, «КВМ технологии». Все они имели стенды на выставке, где демонстрировали свои решения и проекты. В частности, ГК InfoWatch и «Информзащита» привезли модели АСУ ТП с реальным технологическим оборудованием. Партнерами второго дня стали компании «ИнфоТеКС», СИБ, НТЦ «Станкоинформзащита», РНТ.

Законодательные требования

Центральным выступлением конференции стал доклад **заместителя начальника управления ФСТЭК России Елены Борисовны Торбенко**, которая раскрыла подробности о готовящихся изменениях в приказ № 31 ФСТЭК России о разработке методических материалов по организации защиты АСУ ТП, а также о подготовке требований безопасности для СУБД и систем управления информационными потоками. Регулятор планирует привести свои требования в соответствие с выпущенными со дня его опубликования документами. Проект новых требований был выставлен на всеобщее обсуждение ранее – все, кто хотел высказать свои замечания, мог это сделать на портале обсуждения законодательных актов. Сейчас проект уже снят с обсуждения, и по его результатам готовится новая версия с учетом поступивших замечаний.

Кроме того, ФСТЭК собирается выпустить методические рекомендации по применению требований приказа № 31 для защиты систем АСУ ТП. Как пояснила Елена Торбенко, это будет подробное

разъяснение по реализации мер защиты информации, изложенных в приказе, в том числе с учетом их применимости на различных уровнях АСУ ТП. Таким образом, ФСТЭК, уточняя требования по безопасности, рассчитывает более точно соответствовать особенностям промышленных систем, чтобы не мешать их работе.

В этом году законодатели активизировали деятельность по законопроекту о защите критической информационной инфраструктуры (КИИ). Предполагается, что уполномоченный орган построит систему ГосСОПКА, которая будет обеспечивать защиту информационной инфраструктуры, в частности критически важных объектов. Поскольку требования закона будут обязательными, то в результате предприятия, которые эксплуатируют объекты КИИ, должны будут построить собственные центры реагирования на компьютерные инциденты и интегрировать их с государственной системой ГосСОПКА. Таким образом, будет построена распределенная система киберзащиты критических для российского государства предприятий. В частности, в докладе **заместителя директора дирекции безопасности ФГУП «ЗащитаИнфоТранс» Алексея**

Виктор ГАВРИЛОВ,
ФИЦ ИУ РАН

Елена ТОРБЕНКО,
заместитель начальника управления ФСТЭК России

Игоревича Пятигорского было подробно рассмотрено построение отраслевого центра ГосСОПКА для Министерства транспорта Российской Федерации. Под защитой отраслевого центра Минтранса будут пять государственных систем: система обеспечения транспортной безопасности (ЕГИС ОТБ), стык с информационной системой «Розыск-Магистраль» МВД России (СС РМ), система мониторинга объектов транспортной инфраструктуры (ССТМК), координационный центр Минтранса (КЦ) и система регулирования транспорта (АСУ ТК). Для этих систем будет построен центр оперативного управления информационной безопасностью (SOC) и организовано его взаимодействие с аналогичными центрами самой ГосСОПКА.

В своем выступлении **заместитель начальника отдела БРИС белорусской компании ОАО «АГАТ – системы управления» Андрей Анатольевич Обухович** рассказал о реализации требований защиты критически важных объектов на территории Республики Беларусь. Там требования основаны на «Общих критериях» (ISO 15408) и ISO 27001, но, в отличие

Президиум

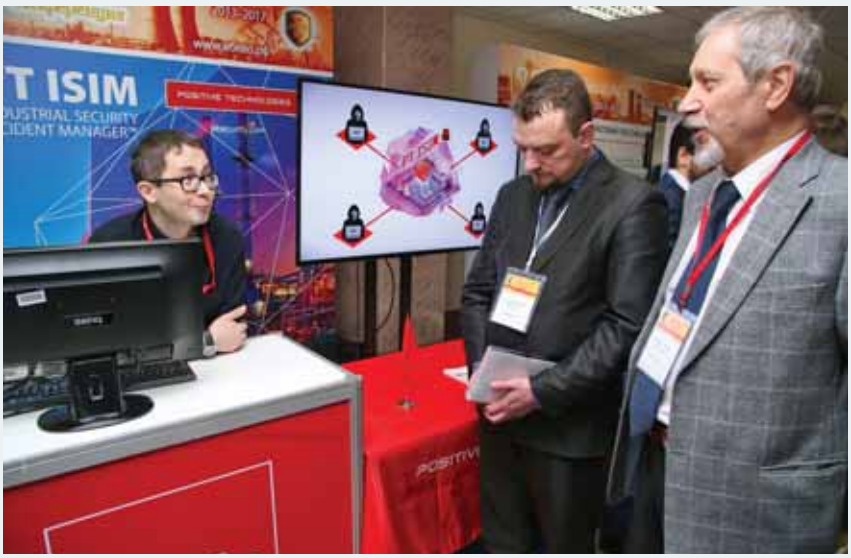
Александр НОВОЖИЛОВ, *«АйТи БАСТИОН» у стенда компании*

от России, они изначально были обязательными. Правда, безопасность АСУ ТП оценивается не в целом по единому шаблону, а с точки зрения влияния на различные аспекты человеческой деятельности. Например, проект, о котором рассказал Андрей Анатольевич, оценивался по влиянию на экологию. В результате рассматривались только те угрозы, которые приводят к выбросу вредных веществ, – защита от подобных угроз является обязательной. А вот если в результате атаки будет просто остановлено производство, то такие угрозы блокировать не обязательно.

Обзор международных стандартов в целом выполнил **сотрудник СПИИРАН Илья Иосифович Лившиц**, который отметил, что международные стандарты, такие как «Общие критерии» и ISO 27001, прописаны достаточно подробно, признаны на территории России и поэтому могут быть использованы для заполнения неопределенностей российской законодательной базы. Однако у нас существует примат локального законодательства: если требования международных стандартов противоречат указаниям российских регуляторов, предпочтение должно быть отдано российским документам. Впрочем, процессы, построенные по лучшим международным практикам, достаточно легко адаптировать к российским требованиям, хотя оборудование, используемое для защиты, может значительно отличаться – российские акты требуют сертификации оборудования по российским критериям, а международные рекомендуют собственную систему сертификации.

На конференции часто возникал вопрос об эффективности средств защиты. Дело в том, что эффективность защиты можно посчитать только как предотвращенный ущерб. В то же время реальных крупных аварий по причине атаки на информационную систему в России пока не было зафиксировано. Поэтому многие специалисты по АСУ ТП, да и руководители промышленных предприятий говорят: «Инцидентов не было, ущерб не посчитан, следовательно, оценить эффективность работы средств защиты и вычислить экономические показатели такого проекта для обоснования невозможно». В то же время Илья Лифшиц уверяет, что может на основе международного опыта и стандартов оценить и обосновать экономическую эффективность проекта по защите АСУ ТП. Впрочем, не всегда нужно экономически обосновывать внедрение средств защиты. В соответствии со ст. 217 ч. 2 УК РФ «Нарушение правил безопасности на взрывоопасных объектах» возникновение инцидентов, в том числе информационной безопасности, может привести к уголовному преследованию ответственного лица – генерального директора или руководителя службы ИБ. Именно поэтому приказ № 31 ФСТЭК России является просто рекомендацией для ответственного лица, чтобы оно могло доказать, что сделало все возможное для предотвращения аварии.

Впрочем, не всегда инциденты информационной безопасности выглядят как атаки хакеров. Тот же Stuxnet приводил к выводу из строя оборудования, и только



Стенд компании Positive Technologies

через некоторое время обнаружилось, что это была кибератака. По мнению **независимого эксперта Вадима Павловича Подольного**, при расследовании аварии на Нововоронежской АЭС, которая произошла 10 ноября 2016 г., не исследовали вопросы именно информационной безопасности. Тогда сгорел статор генератора АЭС, что потребовало его замены и привело к простою станции в течение 75 дней. Кроме того, ресурс топливных элементов был израсходован напрасно. Ущерб значительный, причем по аналогии со Stuxnet и центрифугами велика вероятность атаки через информационную систему. Дело в том, что такая авария не случается «сразу» – замыкание витков обмотки происходит постепенно, что должны были зафиксировать средства мониторинга состояния. Однако данных из АСУ ТП представлено и исследовано не было. Записи системы мониторинга промышленной сети, а таковые уже созданы некоторыми российскими разработчиками средств защиты, позволили бы разобраться в том, что происходило в момент аварии и не было ли воздействия на систему извне.

Другой пример привел в своем докладе **главный руководитель проектов по информационной безопасности компании КРОК Павел Луцик**. Он рассказал, как

Стенд компании «ЭЛВИС ПЛЮС»

на одном нефтеперерабатывающем заводе с помощью продукта «Лаборатории Касперского» удалось выявить мошенничество персонала с переливом и воровством нефти. Для этого было использовано средство мониторинга KICS for Nodes, с помощью которого можно контролировать параметры технологического процесса и поднимать тревогу, если они выходят за допустимые границы. «И при этом еще есть руководители производственных предприятий, которые по-прежнему считают, что русская рулетка абсолютно безопасна», – отметил Павел Луцик.

Георгий ЦЕДИЛКИН,
ANP Ceges Technology

Илья ЛИВШИЦ,
сотрудник СПИИРАН

Алексей ПЯТИГОРСКИЙ,
ФГУП «ЗащитаИнфоТранс»

Андрей ОБУХОВИЧ,
ОАО «АГАТ – системы управления» (Беларусь)

Стенд компании Газинформсервис

Вадим ПОДОЛЬНЫЙ,
независимый эксперт

Павел ЛУЦИК,
компания КРОК

Практика защиты АСУ ТП

Наибольший интерес вызвали на конференции доклады российских операторов критически важных объектов. В частности, об особенностях проведения аудита информационной безопасности рассказали представители ГМК «Норильский никель» и ПАО ТМК, практические аспекты организации защиты АСУ ТП раскрыли представители ООО «ТиссенКрупп Индастриал Солюшнс (РУС)», ЕВРАЗ, ГУП «Водоканал Санкт-Петербурга». Следует отметить, что в соответствии с требованиями приказа № 31 ФСТЭК, прежде чем внедрять средства защиты, необходимо провести аудит защищенности АСУ ТП, затем оценить угрозы, установить необходимый уровень защищенности и только после этого можно заниматься внедрением инструментов защиты. То есть предварительные действия по реализации требований занимают значительное время, поэтому, как отметил Павел Луцик, «большинство компаний в России, относящихся к КВО, находятся на первых трех этапах процедуры, прописанной в приказе № 31 ФСТЭК. До собственно внедрения средств обеспечения безопасности пока дошли единицы».

Именно поэтому доклады **специалиста управления защиты ИТ-инфраструктуры из ГМК «Норильский никель» Алексея Сергеевича Мартынцева и начальника отдела защиты информации СЭБ ПАО ТМК Александра Владимировича Севостьянова** вызвали живую дискуссию. В частности, по словам Алексея Сергеевича Мартынцева, «информационной безопасностью АСУ ТП в «Норникеле» занимались специалисты по АСУ ТП. Причем, не имея квалификации в информационной безопасности, они интуитивно делали все правильно. В то же время после проведения аудита информационной безопасности на предприятии в течение года стратегия защиты промышленных систем была полностью пересмотрена». Аудит проводился в два этапа: документарная проверка наличия всех необходимых процессов, людей требуемой квалификации и принятых локальных юридических актов; инструментальная проверка конфигурационных файлов всего коммуникационного и технологического оборудования с выявлением слабых конфигураций и неисправленных уязвимостей в компонентах АСУ ТП. При этом проверялись не все 600 промышленных систем, принадлежащих «Норникелю», а наиболее критические из них. По мнению Мартынцева, окончательное внедрение средств защиты ограничено нечеткими требованиями регуляторов, но он надеется, что в этом году проблема будет решена.

Проблемы аудита информационной безопасности отметил Александр Владимирович Севостьянов, который выделил четыре точки сопротивления: нежелание персонала, обслуживающего АСУ ТП; недостаточная квалификация аудиторов в проверке именно промышленных систем; длительное ожидание технологических окон – аудит проводился на неработающем оборудовании; неопределенные риски – сложно подсчитать потенциальный ущерб. При этом аудиторы не хотят брать на себя риски возможного ущерба от проведения исследования, поскольку он может быть достаточно большим. Тем не менее «Трубной металлургической компании» удалось подписать с аудиторами договор, при котором они обязались выплатить 5% ущерба в случае задержек запуска технологического процесса по вине аудиторов.

На конференции выступил представитель критически важного объекта, где уже полностью реализованы требования по защите информационной безопасности, – **директор департамента информационных технологий ГУП «Водоканал Санкт-Петербурга» Егор Николаевич Чемоданов**. По понятным причинам водоканал Санкт-Петербурга является КВО – от качества подготовки воды зависит жизнь многомилионного города. Поэтому информационной безопасностью на предприятии занимались с 2011 г., и сейчас все объекты водоканала обеспечены защитой, ключевым элементом которой является межсетевой экран «Континент» производства компании «Код безопасности». Общая система была сертифицирована по требованиям ISO 27001. Система защиты решает три основные задачи: обеспечение устойчивости работы систем водоканала; непрерывность бизнес-процессов; реагирование на инциденты ИБ.

Еще один доклад о результатах реализации стратегии обеспечения безопасности на предприятии сделал **начальник отдела обеспечения безопасности информационных систем ЕВРАЗ Андрей Витальевич Нуйкин**. Цель проекта – отделение промышленной и корпоративной сетей друг от друга, но с обеспечением возможности для администраторов ИТ безопасно управлять оборудованием, подключенным к повышенной сети. Было принято решение организовать для каждого цеха предприятия собственную демилитаризованную зону, в который все действия администратора будут контролироваться, – такое решение было выработано сами администраторами.

Алексей МАРТЫНЦЕВ,
ГМК «Норильский никель»

Александр СЕВОСТЬЯНОВ,
СЭБ ПАО ТМК

Стенд компании Информзащита

Егор ЧЕМОДАНОВ,
ГУП «Водоканал Санкт-Петербурга»

Безопасность от разработчиков АСУ ТП

До сих пор жаркие споры идут между разработчиками средств защиты для АСУ ТП и разработчиками самих АСУ ТП. Понятно, что промышленная система в первую очередь должна выпускать продукцию и только во вторую – сопротивляться сторонним попыткам повлиять на ее работу. Поскольку АСУ ТП строится из тех же компонентов, что и офисные информационные системы, безопасность которых давно и достаточно успешно обеспечивают различные средства защиты, кажется, что для обеспечения информационной безопасности АСУ ТП можно применять те же уже проверенные и отработанные средства защиты. Однако не все так просто. В частности, такому развитию событий сопротивляются сами разработчики АСУ ТП. Проблема в том, что необходимо исключить влияние средств безопасности на технологические процессы. Проверить и гарантировать это может только разработчик АСУ ТП, как следствие, каждый раз приходится сертифицировать средства защиты под конкретных разработчиков АСУ ТП.

Стенд ГК InfoWatch

В своем выступлении **руководитель отдела разработки промышленных систем автоматизации «Иокогава Электрик СНГ» Илья Николаевич Мухин** рассказал о позиции компании Yokogawa в обеспечении защиты ее продукции. В компании реализована многоуровневая концепция средств обеспечения безопасности. Для каждого из уровней – свое средство. Производитель предполагает, что АСУ ТП можно защитить с помощью следующих компонентов: система защиты рабочих станций и серверов, управление обновлениями, контроль целостности, контроль программной среды, резервное копирование и архивирование, антивирусная защита, контроль доступа, межсетевые экраны. Для каких-то уровней у компании есть собственные разработки, для каких-то лицензируются сторонние продукты. Например, для антивирусной защиты рекомендуется использовать антивирусы McAfee, поскольку компания взаимодействует с этим производителем и проверяет на совместимость со своими решениями все выпускаемые компанией обновления. Для сертификации использования стороннего продукта компания проводит его тестирование на совместимость в специально созданной лаборатории в Сингапуре. Пока ни один российский

Андрей НУЙКИН,
ЕВРАЗ

Илья МУХИН,
«Иокогава Электрик СНГ»

Антон ВАСИЛЬЕВ,
ООО «Бомбардье Транспортейшн (Сигнал)»

Роман КРАСНОВ,
Positive Technologies

Василий ТЕКУНОВ,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Руслан ПЕРМЯКОВ,
ООО «СИБ»

разработчик средств защиты не прошел эту процедуру. Тем не менее совместно с «Лабораторией Касперского» компания ведет разработку нового продукта для обеспечения безопасности.

Другой производитель решений для АСУ ТП – компания Bombardier разработала модуль CyberSafemon для безопасного мониторинга журналов микропроцессорных систем управления железнодорожной автоматикой и телемеханикой (МПСУ ЖАТ) для РЖД. С докладом на эту тему выступил **главный специалист отдела качества и безопасности ООО «Бомбардье Транспортейшн (Сигнал)» Антон Юрьевич Васильев совместно с менеджером по продуктовому маркетингу компании Positive Technologies Романом Александровичем Красновым**. Positive Technologies разработала сенсор контроля сетевого трафика в технологической сети для выявления в нем признаков посторонней активности, а Bombardier – безопасное средство отображения полученной сканером диагностической информации. Система мониторинга полностью отделена от технологической сети с помощью диода данных и не может повлиять на работу МПСУ ЖАТ.

Стенд компании «КВМ технологии»

Работы над проектом были инициированы еще в 2013 г., сейчас система сертифицирована по требованиям ФСТЭК и внедряется в эксплуатацию.

Разработчики технологических систем постепенно начинают заниматься средствами обеспечения безопасности, однако далеко не все они осведомлены о требованиях приказа № 31 ФСТЭК. **Генеральный директор ANP Ceges Technology Георгий Цедилкин** провел опрос производителей на предмет знания ими требований ФСТЭК. Предложение было послано 20 производителям АСУ ТП, но откликнулись на него четыре российские и четыре иностранные компании. Выяснилось, что из российских производителей только Fastwell через интегратора «Прософт» знает о наличии требований к информационной безопасности их продукции, а из иностранных – Siemens и WAGO. Правда, опрос проводился по официальным каналам, через контакты, указанные на сайтах компаний. Возможно, во всех опрошенных компаниях есть специалисты по информационной безопасности, однако они находятся «глубоко внутри» и недоступны, что называется, «с первой линии», т. е. для российских клиентов. По результатам опроса можно сделать вывод, что безопасность и соблюдение требований ФСТЭК

являются для производителей АСУ ТП пока не очень актуальной задачей.

Некоторые производители не скрывают, что помогают интеграторам встраивать в свои продукты «логические бомбы», которые предназначены для защиты от недобросовестных клиентов. Такая «бомба» содержит счетчик, который фиксирует количество циклов использования системы и через достаточно большой срок выдает какую-то ошибку, например «невозможно связаться с сервером – обратитесь в службу технической поддержки». Это используется разработчиками для того, чтобы клиенты не прерывали контракты на техническую поддержку продуктов и продолжали платить производителям за обслуживание. Причем далеко не всегда такие закладки являются безобидными, поскольку неизвестно, что именно в них заложили.

К этой же проблеме можно отнести и задачи средств защиты станков с ЧПУ на производственных предприятиях, о которых рассказал в своем докладе **старший научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России» Василий Васильевич Текунов**. Оказалось, что при использовании ЧПУ требования защиты могут существенно измениться. Дело в том, что обычно под безопасностью АСУ ТП подразумевают непрерывность производства и невмешательство посторонних в работу промышленной системы. Здесь на первом месте – доступность данных и их целостность, о конфиденциальности речь идет в последнюю очередь. Для ЧПУ важна именно конфиденциальность, поскольку в программах для станков содержится очень много информации об изделиях, выпускаемых на заводе. Если кому-то удастся похитить набор программ для ЧПУ, то он сможет развернуть аналогичное производство и создать непродуктивную конкуренцию. В том случае, если завод производит изделия для ОПК и других закрытых производств, утечка программ нарушит режим секретности на предприятии. Сейчас большинство предлагаемых станков с ЧПУ – иностранного производства, и они вполне могут содержать неизвестный функционал, позволяющий организовать утечки программ. Защиту программ для станков с ЧПУ можно организовать с помощью сертифицированного средства защиты «Страж ЧПУ», однако опять же требований по сохранению конфиденциальности программ в российском законодательстве нет, и никто из производителей не обращает внимания на эту проблему.

Дмитрий МИХЕЕВ,
«АйТи БАСТИОН»

Сергей ГУЛЯЕВ,
ООО «КВМ технологии»

Стенд компании КРОК

Владимир КАРАНТАЕВ,
ОАО «ИнфоТеКС»

Наложенные средства защиты

В связи с санкциями и разоблачениями Эдварда Сноудена и WikiLeaks возникло определенное недоверие между производителем АСУ ТП и ее пользователями. В своем докладе **заместитель директора по развитию ООО «СИБ» Руслан Анатольевич Пермяко**в отметил, что для укрепления доверия к промышленной сети и подключенному к ней оборудованию необходимо обеспечить следующее: идентифицировать все подключенные к ней объекты и блокировать посторонние; обеспечить безопасный транспорт как команд, так и данных мониторинга; проверить функционал каждого элемента сети на наличие в нем недекларированных возможностей; создать надежное и защищенное хранилище данных диагностической работы систем; контролировать все действия персонала и аутсорсеров, которые получают доступ к промышленному сегменту. Одну часть задач можно решить, другую – нет (например, пока сложно организовать проверку на недекларированные возможности самих программ для АСУ ТП).

В то же время контроль действий критически важных пользователей организовать вполне возможно – об этом рассказывали на конференции **генеральный директор компании «АйТи БАСТИОН» Александр Александрович Новожилов и технический эксперт той же компании Дмитрий Сергеевич Михеев**. Для контроля привилегированных пользователей, как внешних, так и внутренних, компания разработала специальный инструмент, который записывает все действия специалиста технической поддержки. Эти записи можно в дальнейшем проанализировать и выявить действия по обнулению описанных выше счетчиков и настройке других типов «логических бомб».

Еще одно применение продуктов контроля привилегированных пользователей: запись и при необходимости разбор действий ИТ-администраторов при удаленной настройке оборудования технологической сети.

Альтернативным способом организации удаленного доступа к оборудованию в технологической сети является технология KVM, о которой рассказал **директор по развитию ООО «КВМ технологии» Сергей Анатольевич Гуляев**. Она позволяет реализовать удаленное управление компьютерным оборудованием в технологических сетях без непосредственного взаимодействия корпоративной и технологической сетей. Этот способ удаленного доступа продлевает жизнь политике «воздушного зазора» между технологической сетью и остальным миром.

Сергей МАКСИМЕНКО-ЛИТВАК,
ООО «Газинформсервис»

Безопасный транспорт – тема доклада **руководителя направления отдела развития бизнеса ОАО «ИнфоТеКС» Владимира Карантаева**. Его компания разработала многоуровневую защиту каналов связи, начиная от высшего ERP и заканчивая низшими полевыми устройствами. Существующие протоколы взаимодействия полевых устройств, например OPC, позволяют интегрировать в него критические корпоративные механизмы контроля целостности и обеспечения конфиденциальности. Таким образом, можно не только решить проблему защищенного трафика, но и обеспечить аутентификацию устройств сети. При этом стандарт не зависит от алгоритма шифрования и функции хэширования, что позволяет имплементировать в него соответствующие российские алгоритмы. Правда, как отметил в своем заключительном слове **главный специалист по ИБ ФИЦ ИУ РАН Виктор Евдокимович Гаврилов**, использовать существующие ГОСТы для защиты трафика АСУ ТП избыточно – взлом шифра требует нескольких лет работы аналитика, а время жизни команды АСУ ТП – миллисекунды. Поэтому для защиты промышленного трафика лучше применять шифры с не очень большой временной стойкостью.

Юрий МУХОРТОВ,
«ЭЛВИС-ПЛЮС»

Правда, в России такие разработки не ведутся.

О комплексных системах мониторинга, которые и должны обеспечить надежное хранилище диагностической информации, рассказал в своем докладе **руководитель группы поддержки продаж ООО «Газинформсервис» Сергей Борисович Максименко-Литвак**. Его компания создала собственную комплексную систему мониторинга АСУ ТП, которая позволяет собирать диагностические данные с промышленного оборудования различных производителей, ИТ-систем и средств мониторинга событий безопасности, что позволяет обслуживающему персоналу получить наиболее полную картину состояния всех элементов технологического процесса. Когда систему обслуживают три подразделения – АСУ ТП, ИТ и ИБ – каждое со своей системой управления и мониторинга, то общую картину получить не удается и важные данные могут потеряться на «стыках». Если же создать единую комплексную систему мониторинга, то ее могут эффективно использовать все три подразделения для решения своих задач.

Михаил СМИРНОВ,
АО «ИнфоВотч»

Владимир ЧЕРКАСОВ,
ЗАО НИП «Информзащита»

Александр БУРЦЕВ,
ЗАО «НТЦ «Станкоинформзащита»

Александр ГРУШО,
АО «РНТ»

Отдельная проблема – интеграция сетей промышленных объектов с корпоративной системой управления. Особенности подобных решений обсудил с собравшимися **директор департамента специальных проектов «ЭЛВИС-ПЛЮС» Юрий Валерьевич Мухортов**, рассказавший об опыте реализации проектов по интеграции АСУ ТП и других источников данных с MES в топливно-энергетическом комплексе. Он отметил, что не всегда даже наличие датчиков позволяет правильно оценить состояние установки. Некоторые производственники умудряются сделать врезки в трубопроводы, которые не контролируются датчиками. Отслеживать такие процессы на уровне АСУ ТП невозможно, они выявляются только визуальной проверкой и, возможно, анализом данных на уровне MES по подозрительно низкой продуктивности установки.

Не менее важной задачей системы защиты является организация полного жизненного цикла работы с программным обеспечением. О создании такого процесса рассказал **руководитель бизнес-направления «Защита АСУТП» АО «ИнфоВотч» Михаил Смирнов**, а о самих программных инструментах для организации обновления и развития программных компонентов – **и. о. начальника отдела промышленных систем Центра промышленной безопасности ЗАО НИП «Информзащита» Владимир Черкасов**. Исправление уязвимостей в компонентах АСУ ТП и базовых ИТ-продуктах затрудняет злоумышленникам реализацию атак и проникновение внутрь промышленной сети. Еще об одном элементе защиты сообщил на конференции **директор департамента АСУ ТП ЗАО «НТЦ «Станкоинформзащита» Александр Геннадьевич Бурцев**. Его доклад был посвящен возможностям системы обнаружения вторжений для промышленного сегмента. Таким образом, бóльшая часть инструментов для восстановления доверия к АСУ ТП у клиентов есть – их только нужно правильно внедрить и обслуживать.

Заключение

Одним из заключительных докладчиков был **главный системный аналитик АО «РНТ» Александр Александрович Грушо**, который сравнил системы защиты облачных вычислений и АСУ ТП, отметив их схожесть. Причем обнаружилось, что, с одной стороны, можно управлять облачными системами как промышленными процессами, с другой – защищать современные сервисы промышленного Интернета вещей при помощи облачных инструментов, т. е. эти отрасли развиваются совместно, совершенствуя друг друга.

Во время конференции было проведено анкетирование участников по ряду острых практических вопросов, связанных с защитой информации АСУ ТП. В опросе приняли участие 245 человек. По его результатам подготовлен подробный отчет, включающий анализ ключевых аспектов внедрения ИБ в АСУ ТП отечественных предприятий, – он опубликован на нашем сайте. ■