ИБ АСУ ТП: от категорирования к реализации защитных мер

Проекты по защите АСУ ТП принимают массовый характер

4 и 5 марта в Москве в Конгресс-центре МТУСИ состоялась восьмая международная конференция «Информационная безопасность АСУ ТП КВО», которая была посвящена вопросам обеспечения информационной безопасности промышленных АСУ ТП критической информационной инфраструктуры. В этом году в ней приняли участие 378 специалистов, представлявших интересы регуляторов, производителей средств защиты и решений АСУ ТП, а также компаний из различных отраслей промышленности, отнесенных к сфере действия Федерального закона № 187 «О безопасности критической инфраструктуры РФ». Конференция была поддержана ФСТЭК России, ФСБ России и Минэнерго РФ, а партнерами стали ООО «Московский завод «Физприбор», «Ростелеком-Солар», ООО «АйТи БАСТИОН», Check Point Software Technologies Ltd., Positive Technologies, InfoWatch, ООО «УЦСБ», АО «ДиалогНаука», AMT GROUP, компания «Информзащита», АО «ЭЛВИС-ПЛЮС», АО «Лаборатория Касперского», R-Vision и Moxa Inc. Организатором конференции выступил Издательский дом «КОННЕКТ», модератором – Виктор Гаврилов, главный научный сотрудник ФИЦ ИУ РАН.

Требования закона

Центральным выступлением пленарной сессии стал доклад Елены Торбенко, заместителя начальника Управления ФСТЭК России, в котором она подвела предварительные итоги категорирования и перечислила основные ошибки, допускаемые промышленными компаниями в процессе исполнения соответствующего постановления Правительства. Она отметила, что количество объектов, которые подлежат процедуре категорирования, составляет 49 тыс. Во ФСТЭК получены сведения о присвоении категории значимости пока только от 5 тыс. субъектов КИИ. Большинство объектов, подлежащих

Президиум

Виктор ГАВРИЛОВ,
главный научный сотрудник, ФИЦ ИУ РАН

Елена ТОРБЕНКО,
заместитель начальника Управления ФСТЭК России

Андрей ДЕНИСЕВИЧ,
ОАЦ при Президенте Республики Беларусь

категорированию, находятся в ведении предприятий топливно-энергетического комплекса, – таких 33%. На втором месте предприятия здравоохранения – 31%, на третьем, с долей всего 9%, – операторы связи.

Доля значимых объектов КИИ довольно велика – 41% всех зарегистрированных в реестре ФСТЭК. Среди них именно АСУ находятся на первом месте – до 85% ЗОКИИ относится к этому типу объектов. К сожалению,категорирование систем управления часто выполняется с ошибками. Среди проблемных показателей при определении категории объекта КИИ Елена Торбенко выделила следующие: причинение ущерба жизни и здоровью граждан (социальный), ущерб субъекту и ущерб бюджету (экономические), воздействие на окружающую среду (экологический) и ущерб от невыполнения ГОЗ (обороноспособность страны). Она заметила, что даже если сейчас компания не участвует в гособоронзаказе, но имеет для этого потенциал, то такой ущерб тоже нужно рассматривать – при получении оборонного заказа перекатегорирование будет затруднено.

В докладе Елена Торбенко затронула вопрос о подписании 25 февраля документа ФСТЭК, который дополняет требования приказа № 239 ФСТЭК правилами самостоятельной оценки

Среди собравшихся половина не завершила процедуру категорирования или сделала это неправильно.
Елена Торбенко

соответствия СЗИ, требованиями по уровням доверия к функциональному ПО для объектов КИИ (для новых объектов вступление этого пункта в силу отложено до 2023 г.) и разрешением удаленного технического обслуживания объектов КИИ. Данный документ включает набор требований по проверке уровней доверия к программному и аппаратному обеспечению объектов КИИ, в том числе внесение их в реестры Правительства РФ по признакам происхождения. Для высоких категорий значимых объектов могут появиться требования по использованию российской программной и аппаратной базы. Подписанный документ находится на утверждении в Минюсте.

Текущим изменениям белорусского законодательства по КВОИ был посвящен доклад начальника сектора Оперативно-аналитического центра (ОАЦ) при Президенте Республики Беларусь Андрея Денисевича (ОАЦ в Беларуси в части КВОИ занимает такое же положение, как ФСТЭК). Предыдущая версия законодательства по КВОИ была принята Президентом Республики Беларусь еще

Наша цель обеспечить безопасность – мы не занимаемся импортозамещением.

Елена Торбенко

Стенд Московского завода «Физприбор»

в 2011 г., а в декабре прошлого года им был подписан новый Указ № 449 «О совершенствовании государственного регулирования в области защиты информации». В рамках его исполнения ОАЦ уже в феврале текущего года выпустил два приказа: № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь» (аналог постановления Правительства РФ № 127 о категорировании) и № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (аналог «технических» приказов ФСБ и ФСТЭК). В рамках нового законодательства ОАЦ предполагает, что количество КВОИ должно увеличиться. В Беларуси планируется изменить схему назначения КВОИ: если ранее сами владельцы объектов информатизации должны были обращаться в органы управления, а через них в ОАЦ, то теперь процесс присвоения статуса КВОИ будет инициироваться самим ОАЦ. По данным аналитического центра, в Беларуси 39% КВОИ относятся к нефтехимической промышленности, 36% – к телекоммуникациям, 22% – к финансовому сектору и только 3% – к энергетике.

Интерес собравшихся вызвал и доклад Ивана Калачева, начальника отдела департамента информационных технологий ФГБУ «НИЦ «Институт имени Н.Е. Жуковского». Он рассказал об инфраструктуре сбора телеметрических данных и использовании их для слежки за людьми при посредничестве принадлежащих им устройств. В докладе были перечислены сведения, которые собирают и передают своим разработчикам Windows 10, Android, iOS, MS Office, браузеры и их расширения, а также веб-сервисы. Все собранные данные спецслужбы разных стран могут использовать для первоначального сбора информации и поиска методов проникновения в системы российских объектов КИИ.

Теоретическую основу для моделирования угроз и правильного построения защиты предложил в своем докладе заместитель начальника отдела, начальник лаборатории ФАУ «ГНИИИ ПТЗИ ФСТЭК России» Алексей Енютин. Он описал общую модель атаки на АСУ в виде дерева возможных действий злоумышленника, где каждый отдельный элемент зарегистрирован в базе данных угроз и уязвимостей, которую поддерживает ФСТЭК. Использование такого дерева сценариев вероятных атак позволяет моделировать наиболее эффективную систему защиты, которая будет блокировать всевозможные пути злоумышленника. Подобную модель можно анализировать с помощью специализированного программного обеспечения. Докладчик даже привел подготовленную MITRE матрицу действий нарушителей ATT&CK for Industrial Control Systems. ГНИИИ ПТЗИ находится сейчас на раннем этапе формирования такой модели, однако планирует активно использовать уже опубликованный опыт и программное обеспечение.

Иван КАЛАЧЕВ,
ФГБУ «НИЦ «Институт имени Н.Е. Жуковского»

Алексей ЕНЮТИН,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Стенд компании Ростелеком-Solar

> *Сроки сертификации такие, что часто получается «посмертный» сертификат на оборудование.*
> **Георгий Петросюк**

Компоненты защиты

Практические навыки в моделировании угроз можно получить и в процессе киберучений – о них рассказал в своем докладе ведущий аналитик «Ростелеком-Солар» Олег Архангельский. Он проанализировал международный опыт проведения подобных мероприятий и отметил несколько вариантов их реализации: полноценный натурный стенд, имитирующий реальный объект АСУ ТП; полунатурное моделирование, при котором сам технологический процесс моделируется с помощью программного обеспечения, но контролирующее его оборудование вполне реально; математическое моделирование, в котором реальное оборудование АСУ ТП вообще не участвует. Последний вариант самый удобный и универсальный, однако оторван от реальной обстановки. Полноценный стенд максимально точен для отработки навыков, но будет уникален для каждого клиента и завода.

Необходимое системному интегратору сочетание гибкости и точности реализации проще всего достигается на полунатурных стендах. Олег Архангельский выделил два их типа – с включением в контур первичного (PHIL) и вторичного оборудования (HIL). Компания «Ростелеком-Солар» планирует создать подобный полунатурный полигон с использованием оборудования АСУ ТП, которое используется в магистральных и распределительных энергетических компаниях. Со временем к нему может быть добавлено оборудование из транспортной и нефтегазовой отраслей, а также устройства IIoT. Построенный полигон позволит провести сценарный анализ кибератак на модели реальной функционирующей системы и оценить киберфизические последствия деструктивных информационных воздействий на такие системы. Предполагается, что компания будет предоставлять услуги моделирования для заинтересованных в этом субъектов КИИ.

Наиболее эффективным способом защиты от кибератак при построении новых АСУ ТП является использование решений со встроенными механизмами информационной безопасности. На конференции такой продукт представил Московский завод «Физприбор». Заместитель генерального директора по автоматизации Вадим Подольный отметил, что сейчас стоимость АСУ ТП АЭС составляет до 10% стоимости самой атомной электростанции, а стоимость обеспечения безопасности АСУ ТП может достигать половины стоимости внедрения АСУ ТП. «Физприбор» не только производит доверенное оборудование на различных аппаратных платформах вплоть до жесткой логики, но и разрабатывает собственное программное обеспечение для его обслуживания.

Сотрудники компании создали специализированную базу данных реального времени для хранения телеметрии АСУ ТП «Корешок», которая обеспечивает лучшие характеристики по скорости реакции

Олег АРХАНГЕЛЬСКИЙ,
Ростелеком-Solar

Вадим ПОДОЛЬНЫЙ,
Московский завод «Физприбор»

Меняется концепция обеспечения безопасности физических объектов – турбину из резервной копии не восстановишь.

Вячеслав Половинко

по сравнению с традиционными транзакционными СУБД, сохраняя неизменность собираемых данных на уровне блокчейна, хотя цепочку блоков в своей работе не использует. Надежность работы и защита АСУ ТП гарантируется не только неизменностью телеметрических данных в распределенной базе «Корешка», но и использованием нескольких аппаратных платформ для затруднения взлома.

В настоящее время более популярным способом построения защиты уже существующих АСУ ТП являются наложенные решения. Технический директор Check Point по России и СНГ Никита Дуров рассказал, что его компания продает на российском рынке межсетевой экран, сертифицированный ФСТЭК по специальному типу «Д», как МСЭ с возможностью установки в технологические сегменты АСУ ТП. Сертификат по этому классу был получен партнером компании в январе текущего года. Однако межсетевой экран выполняет лишь небольшую часть функций из той самой матрицы ATT & CK for ICS. Для дальнейшего заполнения матрицы требуется

Никита ДУРОВ,
Check Point в России и СНГ

внедрение и других инструментов защиты, таких как СЗИ на рабочих станциях, средства мониторинга технологического сегмента с помощью Thread Intelligence, система реагирования на обнаруженные инциденты. Максимально заполнить матрицу мер защиты, предложенную MITRE, можно только с помощью построения комплексной системы защиты, которая к тому же должна не мешать работе технологического сегмента. Это требование есть и в Федеральном законе № 187, который требует создания системы управления информационной безопасностью (СУИБ) у субъекта КИИ.

Андрей ЮРШЕВ,
ГК InfoWatch

На текущий момент в России только два производителя имеют промышленные межсетевые экраны, которые сертифицированы по типу «Д», – Check Point и InfoWatch. Руководитель отдела развития систем защиты АСУ ТП, ведущий эксперт ГК InfoWatch Андрей Юршев рассказал о преимуществах такого решения. Он привел три критерия выбора средств защиты для технологического сегмента: совместимость с АСУ ТП, выполнение требований регуляторов и проверка соответствия требованиям регуляторов, которая лучше всего выполняется в виде сертификации. Он также напомнил, что нужно учитывать политику импортозамещения для значимых объектов КИИ, которая со временем должна вытеснить из этого сегмента иностранные решения.

Компания «АйТи Бастион» представила свои продукты по контролю действий привилегированных пользователей СКДПУ в защищенном исполнении. Об этом в своем докладе рассказал генеральный директор компании «АйТи БАСТИОН» Александр Новожилов. Так, линейка продуктов «СКДПУ Компакт» предназначена для установки на безлюдных производствах в целях контроля действий привилегированных пользователей. Для отделения

Стенд компании «АйТи БАСТИОН»

Александр НОВОЖИЛОВ,
«АйТи БАСТИОН»

Вячеслав ПОЛОВИНКО,
ДИС АМТ-ГРУП

Получили «письмо счастья» с номером в реестре – приступайте к реализации защитных мер.
Елена Торбенко

технологических сетей от корпоративных клиенты могут внедрить еще один продукт компании под названием «Синоним», который устанавливает правила пропускного режима для информационных пакетов – более строгий аналог межсетевого экрана. Для интеграции всех средств защиты в единую систему «АйТи БАСТИОН» предлагает продукт СКДПУ НТ, обеспечивающий общее управление для всех устройств компании, и интеграционную шину для взаимодействия с другими средствами защиты. Ее можно использовать как основу для построения СУИБ. В скором времени компания планирует выпустить межсетевой экран нового поколения.

О применении такого специализированного инструмента для защиты АСУ ТП, как однонаправленные шлюзы или информационные диоды, рассказал руководитель направления бизнес-аналитики и собственных продуктов ДИС АМТ-ГРУП Вячеслав Половинко. Он отметил, что сейчас возникла необходимость внедрения инструментов защиты, которые полностью, на физическом уровне, блокируют передачу обратного сигнала. Инфодиоды используются для сбора с датчиков и сенсоров телеметрической информации, обеспечивая защиту от проникновения в сеть посторонних сенсоров. Для исполнительных устройств управляющие сигналы также можно передавать через информационные диоды, что затрудняет взлом подобных устройств. В любом случае устанавливать инфодиоды нужно на границах сетей с различными уровнями критичности. Таким образом, они являются инструментами для более жесткой и строгой сегментации компьютерных сетей наряду с классическими межсетевыми экранами.

В настоящее время наиболее популярными элементом СУИБ технологических сетей являются системы мониторинга, которые иногда называют системами обнаружения вторжений (СОВ) или системами обнаружения атак (СОА). Рынок промышленных СОВ/СОА проанализировал руководитель направления Kaspersky Industrial CyberSecurity «Лаборатории Касперского» Алексей Петухов. По его мнению, указанные продукты могут реализовать значительную часть мер из матрицы ATT&CK for ICS, не оказывая существенного влияния на сам технологический процесс, поскольку они могут быть отделены от промышленного сегмента информационным диодом. Такие системы должны обеспечить, как минимум, глубокий анализ промышленного трафика, анализ сетевых протоколов, инвентаризацию активов, сбор и корреляцию событий и в результате выявление признаков проникновения. Дополнительными инструментами для систем обнаружения должны быть механизмы реагирования на обнаруженные инциденты и решения для проведения аудита функциональных элементов технологической сети.

Компания Positive Technologies представила на конференции свое видение построения комплексной системы защиты – его раскрыл в докладе руководитель группы

Стенд компании Check Point

Алексей ПЕТУХОВ,
Kaspersky Industrial CyberSecurity «Лаборатории Касперского»

Дмитрий ДАРЕНСКИЙ,
Positive Technologies

Владимир АКИМЕНКО,
АО «ЭЛВИС-ПЛЮС»

Соблюдение требований Закона № 187-ФЗ – это больше вопрос правильного оформления, чем внедрения дополнительных средств защиты.

Валерий Комаров

систем защиты промышленных сетей компании Дмитрий Даренский. Он отметил, что непрерывность технологических процессов не зависит от корпоративного сегмента ИТ. В то же время для бизнеса в разы важнее обеспечение работоспособности именно технологической сети, однако на ее информационную безопасность выделяется существенно меньше средств. В результате в технологических сетях проблем с защитой информационных систем и АСУ значительно больше, чем в корпоративных. Поэтому Positive Technologies будет переносить технологии, которые уже отработаны для корпоративных сетей, в промышленные сегменты. Для корпоративных сетей существует концепция по переходу от реактивного реагирования на инциденты (COB/COA) к проактивным процедурам минимизации поверхности атаки. Для этого нужно не просто заниматься мониторингом ситуации в технологических сегментах, но и управлять рисками, выявлять критические системы, управлять их кибербезопасностью и максимально точно разрабатывать политики безопасности. Такая стратегия требуется и для соблюдения Закона № 187-ФЗ, но только Positive Technologies планирует разработать набор инструментов для автоматизации процессов управления рисками, реагирования на инциденты, расследования происшествий и принятия ответных мер по результатам расследования.

Помощь партнеров

В секции «Методы, технологии и техника защиты» представители системных интеграторов обменялись опытом проведения процедуры категорирования и построения по ее результатам комплексных систем защиты. В частности, руководитель Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС» Владимир Акименко попытался проанализировать требования различных регуляторов по информационной безопасности и свести их к единой терминологической основе. Оказалось, что сделать это сложно: докладчик описал ситуацию как «терминологический треш», в котором достаточно легко запутаться. В юридическом поле законодательных актов, связанных с КИИ, есть целый набор очень похожих терминов, таких как «событие ИБ»,

Стенд компании Positive Technologies

Николай ДОМУХОВСКИЙ,
УЦСБ

«инцидент ИБ», «компьютерный инцидент», «компьютерная атака», «возникновение угроз ИБ», «реализация угроз ИБ» и многое другое. Свести их в единую схему затруднительно, а без этого сложно понять, что же именно требуют регуляторы. Тем не менее в докладе некоторая схема соотношения различных терминов законодательства была представлена, и «ЭЛВИС-ПЛЮС» активно использует ее в своих проектах по защите объектов КИИ.

Для решения проблем с выполнением требований руководящих документов уже разрабатываются специализированные инструменты. Так, заместитель генерального директора УЦСБ Николай Домуховский отметил: «Чтобы не быть погребенными под тоннами бумаги при реализации организационных мер, при защите объектов КИИ необходимо внедрять средства автоматизации: системы анализа и мониторинга событий, а также управления СЗИ». Действительно, формальное соблюдение регламентов закона может привести к излишней жесткости процедур по работе с АСУ ТП, которые обусловлены использованием организационных мер вместо построения реальной защиты промышленных сетей и объектов. Более эффективным способом реализации требований Закона № 187-ФЗ является построение полноценной СУИБ или хотя бы аутсорсинг услуг защиты у коммерческого центра реагирования SOC. В своем докладе Николай Домуховский рассказал о процессе постепенного построения коммерческого SOC в компании УЦСБ и о возможностях, которые получают, в частности, промышленные клиенты, подключившись к нему на аутсорсинг. В этом случае большую часть рутинной работы по реальной защите информационных ресурсов можно передать профессиональной команде аутсорсера.

Системные интеграторы также предлагают услуги не только по аутсорсингу, но и по созданию СУИБ на территории заказчика. Руководитель направления «Защита АСУ ТП» Центра промышленной безопасности НИП «Информзащита» Игорь Рыжов рассказал о наборе сервисов для владельцев объектов КИИ по построению собственной СУИБ. В ассортименте «Информзащиты» четыре типа таких сервисов: категорирование, проектирование систем защиты, построение СУИБ и последующее развитие и модернизация ее в соответствии с требованиями регуляторов. Сейчас промышленные компании все чаще заказывают услуги по внедрению промышленных антивирусных продуктов, решений для сегментирования сетей, систем мониторинга промышленных сегментов и обнаружения

Перед этапом исследования объекта АСУ ТП нужно сначала пройти этап знакомства с его руководством.
Игорь Рыжов

вторжений, решений для контроля привилегированных пользователей, настройки двухфакторной аутентификации и построения центров реагирования на инциденты. Это означает, что промышленные компании переходят от этапа инвентаризации промышленных активов к их защите и построению полноценной СУИБ.

Будни безопасности

Секция «Отраслевой опыт. Опыт эксплуатации, разработки и проектирования АСУ ТП» была посвящена внедрению и обслуживанию средств защиты АСУ ТП субъектов КИИ. Важной темой, обсуждаемой в этой сессии, стали требования по функциональной безопасности объектов КИИ, которые только частично связаны с информационной безопасностью. Выступающие неоднократно говорили о необходимости предъявления дополнительных требований по безопасности для киберфизических систем, а не только для ИС, АСУ и ИТС. Однако Елена Торбенко пояснила, что установить дополнительные требования функциональной безопасности должны именно

Стенд ГК InfoWatch

Стенд УЦСБ

Мой тезка Касперский сказал: «Те предприятия, которые не цифровизируются, умрут, а те, кто цифровизируются, тоже умрут, поскольку получат «цифровую торпеду» и будут уничтожены».

Евгений Акимов

отраслевые регуляторы. Она лишь отметила, что категорирование необходимо включать в моделирование угроз функциональные системы субъекта КИИ.

Опытом категорирования поделился начальник отдела обеспечения осведомленности Управления информационной безопасности ДИТ Москвы Валерий Комаров. Российская столица имеет довольно обширное хозяйство, в котором около четверти объектов информатизации из перечня КИИ можно отнести к категории АСУ. В Москве для категорирования всех ресурсов была создана комиссия из девяти рабочих групп. В них вошли 53 высокопоставленных сотрудника ДИТ Москвы и подведомственных организаций, которые провели 12 заседаний, затратив на это как минимум 393 человеко-часа. В результате проведенной работы выяснилось, что ДИТ Москвы не имеет ни одного значимого объекта КИИ – департамент является только их оператором, а к субъектам относятся органы исполнительной власти столицы.

Неприятная ситуация с законодательным регулированием ИБ в государственных ведомствах. По Законам № 152 «О персональных данных» и № 149 («трехглавому») ДИТ Москвы должен был реализовать требования приказов ФСТЭК № 17 (ГИС), 21 (ИСПДн) и 31 (КВО), в то время как органы исполнительной власти обязаны исполнять требования Закона № 187 и реализовать меры, указанные в приказах ФСТЭК № 235 и 239. При этом защитные меры перечисленных приказов практически полностью пересекаются. В результате теперь они могут быть обвинены в нецелевом расходовании средств и двойном финансировании ИБ, хотя им приходилось исполнять требования различных нормативных актов.

Евгений Акимов, директор по кибербезопасности АО «Концерн «Калашников», рассказал о принципах проведения процедуры категорирования на предприятиях с большим влиянием гособоронзаказа. Он отметил, что основная цель категорирования с точки зрения бизнеса – максимально оптимизировать выполнение всех государственных требований и снизить уровень значимости принадлежащих ему объектов в целях сохранения конкурентоспособности. «Нам не удалось решить последнюю задачу на 100%», – посетовал докладчик, хотя оптимизации за счет объединения проектов по соблюдению требований Законов № 152 и 187 добиться удалось. Причем доля АСУ ТП среди значимых объектов у концерна оказалась меньше половины. Однако компания приняла решение подключать к системе ГосСОПКА все объекты КИИ, в том числе незначимые, что законодательство позволяет. К сожалению, при категорировании компаниям приходится оценивать чужие риски – для государства, обороноспособности, экологии и граждан, но открытой статистики по инцидентам на объектах КИИ нет, что затрудняет возможности точной оценки рисков. Поэтому было бы неплохо, чтобы НКЦКИ как оператор ГосСОПКА опубликовал обезличенный реестр инцидентов для оценки вероятности наступления того или иного события либо хотя бы более точную статистику по уже состоявшимся инцидентам.

Рассказ об исполнении требований закона на предприятиях ОПК продолжил руководитель группы информационной безопасности АО «НПП «Исток» им. Шокина» Дмитрий Гаращенко. Он отметил, что цифровизация в ОПК неизбежно приводит к увеличению количества объектов КИИ на предприятиях. А к производственным компаниям, относящимся к ОПК, предъявляются дополнительные требования, перечисленные в приказе ФСТЭК № 31,

Игорь РЫЖОВ,
НИП «ИНФОРМЗАЩИТА»

в котором фактически сказано о том, что к системам управления производством SCADA должны предъявляться требования, приведенные в приказе ФСТЭК № 17 для ГИС. Кроме того, важным элементом СУИБ для предприятий ОПК должны стать механизмы защиты станков с ЧПУ.

ФГУП «ЦЭНКИ», который входит в структуру «Роскосмоса» и занимается техническим сопровождением космических полетов, также отчитался о проведении категорирования. Начальник отдела обеспечения безопасности объектов КИИ управления экономической безопасности предприятия Юрий Амелёхин рассказал, что в процессе категорирования было обследовано 83 наземных объекта, из которых 41 отнесен значимым: 11 из них располагаются в космическом центре «Восточный», 29 – в космическом центре «Южный» и еще один – в центре ликвидации межконтинентальных баллистических ракет. Предприятие подключено к корпоративному центру ГосСОПКА «Роскосмоса».

Своим опытом проведения процедуры категорирования для объектов ТЭК поделился менеджер ООО ИК «СИБИНТЕК» Михаил Богатырев. Его компания одной из первых подала перечень объектов КИИ еще в августе 2018 г., а к августу 2019 г. уже отправила во ФСТЭК результаты

Стенд компании «ДиалогНаука»

завершившейся процедуры. Всего было обследовано 30 предприятий ТЭК. Среди обнаруженных на них объектов КИИ около 99% являются АСУ ТП. Был соблазн использовать для категорирования декларацию безопасности опасного промышленного объекта (ОПО), которую компания уже подготовила при реализации Закона № 116 «О безопасности ОПО». Тогда процедуру можно было бы завершить быстро, но выяснилось, что это приводит к сильному завышению категории значимости. Более точная работа со специалистами-технологами позволила существенно снизить категории значимости для пяти из девяти промышленных установок компании. Сейчас компания находится на этапе создания собственной СУИБ (в «СИБИНТЕК» она называется ГРИИБ) и подключения ее к ГосСОПКА.

Тему киберзащищенности промышленных АСУ ТП поднял в своем докладе заместитель руководителя Центра кибербезопасности АО «НИИАС» д. т. н., профессор Борис Безродный. Он предложил подход к обеспечению безопасности киберфизических систем, состоящий из трех элементов: информационной, функциональной и физической

Валерий КОМАРОВ,
Управление информационной безопасности ДИТ Москвы

Евгений АКИМОВ,
АО «Концерн «Калашников»

Дмитрий ГАРАЩЕНКО,
АО «НПП «Исток» им. Шокина»

Юрий АМЕЛЁХИН,
ФГУП «ЦЭНКИ»

Михаил БОГАТЫРЕВ,
ООО ИК «СИБИНТЕК»

Борис БЕЗРОДНЫЙ,
АО «НИИАС»

Могу подготовить за три дня группу студентов, и железная дорога «ляжет» на месяц. Нам должны платить, чтобы наши студенты не применяли свои знания на практике.

Анатолий Хорев

безопасности. В РАО РЖД разработан отраслевой стандарт информационной безопасности СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия». Именно на его основе и строятся системы обеспечения безопасности движения на железнодорожных предприятиях России. Центром кибербезопасности АО «НИИАС» еще в 2015–2016 гг. был разработан ряд методических документов по обеспечению безопасности информационных систем, используемых в РАО РЖД. Компания активно проводит исследование различных киберфизических систем на уязвимости по методическим документам. На текущий момент ее специалистами было обнаружено 233 уязвимости, большая часть которых устранена разработчиками.

Стенд компании АМТ-ГРУП

Генеральный директор АО «ДиалогНаука» Виктор Сердюк рассказал о проекте создания СУИБ, который уже несколько лет реализуется в электросетевой компании АО «ОЭК». Ранее в компании уже были внедрены МСЭ, которые позволили сегментировать технологическую сеть компании. Далее с помощью KICS для хостов и сетей были взяты под контроль рабочие станции промышленных сегментов. Причем разработчикам технологического оборудования пришлось по заказу клиента внедрить в свои продукты дополнительные механизмы защиты с помощью перепрошивки ПЛК. В 2020 г. компания завершила проект внедрения подсистем защиты более высоких уровней, таких как системы управления уязвимости, СКДПУ, мониторинга событий информационной безопасности и двухфакторной аутентификации для защиты от несанкционированного доступа. В результате реализации проекта на предприятии построена система обеспечения кибербезопасности АСТУ ЦУС и 12 подстанций высокого напряжения. Планируется расширить решение на все подстанции, подконтрольные компании, подключить систему мониторинга к ГосСОПКА и создать круглосуточный центр мониторинга информационной безопасности.

Виктор СЕРДЮК,
АО «ДиалогНаука»

Стенд компании «Информзащита»

Своим опытом эксплуатации распределенной СУИБ поделился куратор по направлению сопровождения и эксплуатации систем ИБ АСУ ТП ПАО «ГМК «Норильский никель» Иван Деркачев. На его предприятии уже внедрен отдельный технологический процесс обеспечения информационной безопасности АСУ ТП, который отделен от службы информационной безопасности всего предприятия. Суть процесса – вовлечение в процедуры обеспечения ИБ технологическогоперсонала АСУ ТП. На предприятии создан единый межрегиональный центр управления, который работает по модели «Следуй за Солнцем». Фактически ГМК «Норильский никель» продвинулся дальше других в части исполнения требований Федерального закона № 187.

Центральным выступлением секции «Отраслевой опыт. Опыт эксплуатации АСУ ТП. Подготовка кадров» стал доклад Анатолия Хорева, заведующего кафедрой ИБ НИУ МИЭТ, который рассказал о планах подготовки специалистов в области информационной безопасности в вузах России. Он предложил предприятиям, которые подпадают под действие Федерального закона № 187, сформировать запрос на обучение кадров по специальностям в области защиты информации, поскольку регуляторы требуют наличия у субъекта КИИ квалифицированного персонала для защиты критической инфраструктуры.

В рамках конференции была проведена панельная дискуссия «Цифровизация производств как основной вызов безопасности КИИ», модератором которой выступил Георгий Петросюк, директор департамента информационных технологий ФГБУ «НИЦ «Институт имени Н.Е. Жуковского». В дискуссии были затронуты вопросы влияния информационной безопасности на процессы цифровизации российских промышленных предприятий и возникновения новых информационных рисков при реализации на предприятиях концепции «Индустрия 4.0».

У РЖД в отстойниках есть паровозы, которые можно будет использовать в случае чего. А при цифровизации у всех есть такие паровозы?
Георгий Петросюк

В частности, собравшимися были высказаны сомнения в необходимости использования при цифровизации промышленных предприятий облачных технологий и опасения по поводу увеличения площади атаки при внедрении цифровых сервисов. При проведении цифровизации ключевым вопросом является обеспечение защиты новых сервисов и уже работающих технологических процессов. При этом

Стенд компании ЭЛВИС-ПЛЮС

Иван ДЕРКАЧЕВ,
ПАО «ГМК «Норильский Никель»

Анатолий ХОРЕВ,
ИБ НИУ МИЭТ

Георгий ПЕТРОСЮК,
ФГБУ «НИЦ «Институт имени Н.Е. Жуковского»

Я могу прекратить вашу конференцию с помощью включения двух устройств.

Анатолий Хорев

всегда приходится сочетать наложенные средства защиты со встроенными. «Для корпоративных решений не удалось сделать защиту только встроенной, не удастся это сделать и для АСУ ТП», – пояснил Евгений Акимов.

Слушатели могли проголосовать за понравившийся доклад. В этом году больше всего симпатий участников конференции вызвали выступления Елены Торбенко, Ивана Калачева и Евгения Акимова. В фойе конференции была организована выставка, на которой все партнеры представили свои предложения в области защиты критически важных объектов.

Выводы

Любое внедрение начинается с выработки технического задания, которое определит контуры будущих информационных систем. С учетом законодательства по КИИ проектом по выработке технического задания на построение будущей системы защиты объектов критической инфраструктуры является категорирование. В процессе выполнения этой процедуры компаниям пришлось моделировать атаки на собственные цифровые активы и определять последствия от действий злоумышленников. На текущий момент большинство промышленных компаний справились с этой задачей, как минимум, с помощью системных интеграторов или юридических консультантов. Теперь наступает время реализации проектов по мониторингу состояния своих ресурсов, выявлению атак на них и выстраивания политики реагирования на инциденты.

Все эти функции выполняются центрами реагирования на инциденты или СУИБ. Некоторые компании уже приступили к созданию подобных центров, другие подключились к коммерческим SOC, специалисты которых в соответствии с договорами осуществляют мониторинг работы промышленных АСУ ТП и реагируют на инциденты вместо сотрудников самой компании. Причем эти центры реагирования, как корпоративные, так и аутсорсинговые, должны быть подключены к ГосСОПКА – для передачи событий информационной безопасности и для реагирования на предупреждения, которые приходят от НКЦКИ. Когда большинство промышленных предприятий построит подобные системы реагирования и подключатся к ГосСОПКА,тогда построение системы защиты критической инфраструктуры будет завершено.

Параллельно идет процесс цифровизации промышленности, которая требует, в частности, решения вопросов информационной безопасности. Связано это с тем, что предусмотренное в них использование технологий больших данных, предиктивной аналитики и Интернета вещей предполагает получение данных из промышленных и других автоматизированных систем управления. Адепты цифровой трансформации обещают сокращение расходов и повышение маржинальности производства – за счет увеличения производительности труда, интенсивности и эффективности использования и обслуживания оборудования и т. д. Однако внедрение цифровых сервисов требует повышения уровня безопасности АСУ ТП, причем специалисты по ИБ сейчас могут предложить только запретительные и ограничительные меры. В результате специалисты ИБ воспринимаются как тормоз на пути к светлому цифровому будущему. На самом же деле безопасность технологических процессов должна обеспечить их непрерывность, предсказуемость и эффективность. Но достижение этих целей требует пересмотра отношения к информационной безопасности и ее развития совместно с цифровыми сервисами.

Прошедшая конференция показывает, что сейчас российские промышленные предприятия

Стенд компании R-Vision

в основной своей массе находятся на этапе завершения процедуры категорирования, моделирования угроз и формирования требований по защите информационных систем. Теперь им предстоит построить системы защиты в соответствии с требованиями ФСТЭК, создать СУИБ и подключиться к ГосСОПКА. Для решения этих задач производители средств защиты и разработчики АСУ ТП сейчас уже предлагают необходимый набор специализированных решений для создания полноценной промышленной СУИБ. Системные интеграторы подготовили услуги или собственную инфраструктуру, которые помогут построить такие системы защиты или подключиться к коммерческим SOC.

Компания Моха

Важным элементом является наличие персонала и компетентных сотрудников, которые могли бы адекватно реагировать на инциденты. Поэтому подготовка кадров в области защиты информации является важным элементом в построении комплексной защиты критической инфраструктуры Российской Федерации, хотя пока субъекты КИИ уделяют этому вопросу не очень много внимания. Впрочем, компетенцию персонала можно поднять и за счет проведения киберучений, в которых отрабатываются навыки реагирования на события ИБ: действия каждого сотрудника должны быть отработаны заранее, поскольку от скорости реакции сейчас зависит качество обеспечения защиты критической инфраструктуры. Индустрия проведения подобных киберучений должна в ближайшее время сложиться и в России, как это уже произошло на Западе.

В целом можно отметить, что реализация требований Закона № 187-ФЗ проходит в хорошем темпе и без серьезных сбоев. Важно только, чтобы этот процесс не остановился на этапе категорирования и был продолжен до полного создания реальной защиты объектов критической информационной инфраструктуры России. ■