Последние КИИновации

В Москве состоялась 11-я конференция «Информационная безопасность АСУ ТП критически важных объектов», в которой приняли участие представители ФСТЭК России, ФСБ России, профильных органов власти Республики Беларусь и Республики Казахстан, специалисты компаний из ТЭК, электроэнергетики, ОПК, транспорта и других отраслей. Всего в этом году в конференции приняли участие 628 делегатов. При этом 37% участвующих в опросе участников заявили, что обеспечивают работу систем АСУ ТП и других операционных технологий. Организатор конференции – Издательский дом «КОННЕКТ». Модератором конференции выступил главный научный сотрудник Федерального исследовательского центра «Информатика и управление» РАН Виктор Евдокимович Гаврилов, а помогал ему заместитель генерального директора ИД «КОННЕКТ» Дмитрий Юрьевич Корешков.

АСУ ТП как КИИ

Деловую программу конференции открыл доклад начальника управления ФСТЭК России Елены Борисовны Торбенко под названием «Совершенствование нормативно-правовой базы в области информационной безопасности АСУ ТП и практика реализации контрольно-надзорной функции ФСТЭК России в 2022–2023 гг. Краткий анализ количественного и качественного состава атак на значимые объекты КИИ, природа новых векторов атак, структура атак в отраслевом разрезе». Для него организаторы составили предварительный набор вопросов, на которые Елена Борисовна ответила в конце своего выступления. Вопросы можно было задать и во время выступления в телеграм-канале конференции.

В своем докладе Елена Борисовна озвучила изменения регулирования в области защиты КИИ, а также поделилась первыми результатами проведенного государственного контроля за соблюдением требований Федерального закона № 187-ФЗ «О безопасности КИИ». По ее словам, ни в одной из проведенных проверок не было выявлено полного соблюдения всех требований регуляторов. Елена Борисовна раскрыла наиболее популярные из выявленных нарушений и предупредила об ужесточении наказания как за предоставление недостоверных сведений, так и за нарушение требований в области защиты КИИ. В частности, она отметила, что разбиение объекта КИИ на части, чтобы снизить

Виктор ГАВРИЛОВ,
ФИЦ Информатика и управление Российской академии наук

Елена ТОРБЕНКО,
начальник управления ФСТЭК России

Кирилл АКИМОВ,
представитель НКЦКИ

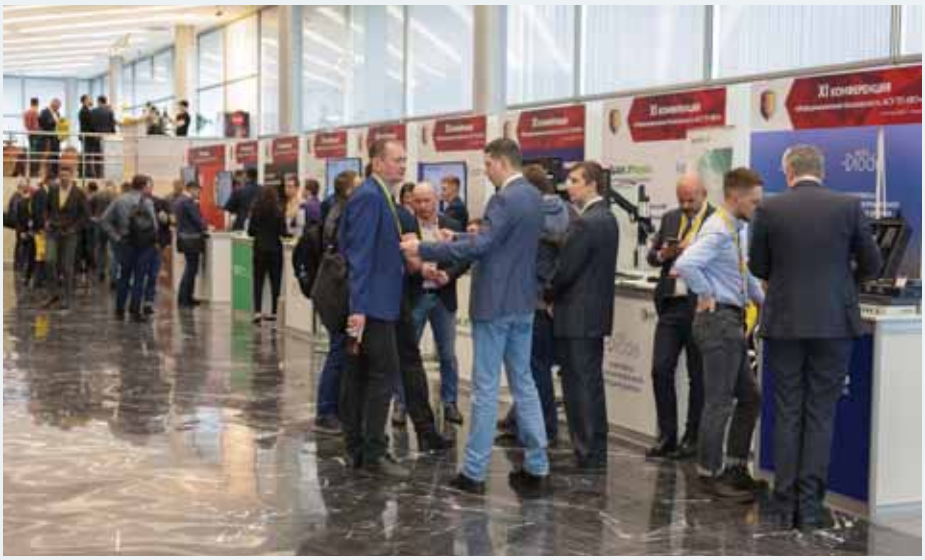
ущерб и тем самым категорию, сейчас не будет работать, поскольку потребуется обеспечить защиту взаимодействия систем между собой. Кроме того, она отметила важность соблюдения компенсирующих мер защиты. «Если вы не можете применить технические меры, применяйте организационные, но добейтесь от сотрудников их соблюдения», – подчеркнула она. Кроме того, отметила, что объекты КИИ проще атаковать через партнеров, что обусловливает необходимость при заключении договоров на обслуживание объектов КИИ включать в них соответствующие требования по безопасности.

Кроме того, Елена Борисовна предупредила о недавних изменениях, внесенных в Постановление Правительства РФ № 127, которое определяет правила категорирования объектов КИИ. Поскольку правила категорирования изменились, субъектам КИИ необходимо в кратчайшие сроки пройти перекатегорирование и сообщить его результаты во ФСТЭК. Также Елена Борисовна сообщила, что ФСТЭК планирует в самое ближайшее время опубликовать для согласования списки типовых элементов отраслевых ОТ с примерными уровнями их значимости. Предполагается, что это упростит процедуру категорирования сложных промышленных решений. Кроме того, планируется внести изменения в приказ № 235. В частности, предполагается разрешить принимать в службу безопасности специалистов, которые закончили средние учебные заведения по специальности «Информационная безопасность».

Доклад представителя НКЦКИ Кирилла Александровича Акимова назывался «Краткий обзор совершенствования и развития системы ГосСОПКА в 2022–2023 гг. Новое в нормативно-правовой базе». Он был посвящен развитию ГосСОПКА и проекту требований к центрам ГосСОПКА, который сейчас обсуждается и в ближайшее время будет опубликован. Он определит задачи и функции центров ГосСОПКА, перечислит требования к персоналу центров, введет классификацию по типам центров и наборам их функций, установит требования к деятельности

Безопасники смотрят не туда, куда надо было бы посмотреть.

Виктор Гаврилов



Не рассматривайте регуляторов как карающий орган, но как инструмент, который позволяет вернуть отступников к православной вере, не ущемляя другие религии.

Александр Соколов

ООО «АйТи Бастион»

и минимально достаточному составу центра ГосСОПКА.

Сотрудник Оперативно-аналитического центра при Президенте Республики Беларусь Александр Николаевич Соколов в своем докладе «Национальная система обеспечения кибербезопасности» рассказал о недавно принятом в их стране указе Президента Беларуси № 40 «О кибербезопасности», в рамках которого создается национальная система обеспечения кибербезопасности (НСОК) – аналог ГосСОПКА. Она будет заниматься постоянным мониторингом уязвимостей в национальном сегменте сети Интернет, анализом информации о кибератаках и инцидентах, минимизацией последствий кибератак на критические объекты инфраструктуры, организацией взаимодействия между госорганами и обслуживающими организациями для предотвращения инцидентов и адекватного реагирования на них, а также оценкой защищенности критических объектов и прогнозированием ситуации в области обеспечения информационной безопасности. Также НСОК будет проводить киберучения для отработки навыков реагирования на кибератаки. Аналогичная работа проводится и в Казахстане, о чем сообщил в своем выступлении на тему «Текущая ситуация (законодательство) в сфере ИБ АСУ ТП КВО Республики Казахстан» специалист ИБ Комитета национальной безопасности Республики Казахстан Талгат Канатович Абдихамитов.

Промышленная безопасность

Следует отметить, что по мере увеличения киберактивности злоумышленников сами АСУ ТП должны несколько видоизменить-ся, чтобы обеспечить надежное сохранение возложенных на них функций по управлению технологическими процессами независимо от проводимых хакерами компьютерных атак. Для решения этой проблемы СТО «Лаборатории технологий автоматизации» Вадим Павлович Подольный предлагает использовать распределенные системы управления. Их концепцию он раскрыл в докладе «Современные распределенные системы управления. Современные задачи и амбициозные вызовы. Технологическая независимость и кибербезопасность». Он предложил разделить системы управления на те, что устойчивы к разрыву связей с другими системами, и те, которые к подобному разрыву неустойчивы и могут выйти из строя. Понятно, что требования по безопасности к этим системам будут разные.

Кроме того, Вадим Павлович ввел понятие «естественная безопасность». Это свойство системы самостоятельно реагировать на изменения условий так, чтобы обеспечить безопасность собственного функционирования.

Александр СОКОЛОВ,
Оперативно-аналитический центр при Президенте Республики Беларусь

Талгат АБДИХАМИТОВ,
Комитет национальной безопасности Республики Казахстан

Такой безопасности можно достигнуть с помощью распределенной системы управления (РСУ), которая позволяет обеспечить резервирование, консистентность, доступность, устойчивость к разделению. Ее функционирование должно быть основано на понимании технологического процесса и возможности его моделирования для прогнозирования развития критических ситуаций и контроля отклонений от модели штатного функционирования. РСУ при правильном подходе к ее построению может обеспечить более надежное функционирование технологических процессов, чем централизованные АСУ ТП.

Экосистему защиты промышленных решений для обеспечения кибербезопасности промышленных предприятий представил в своем докладе директор ООО «Сайбер-Лимфа» Алексей Шанин. Экосистема решений UDV Group позволяет построить на предприятии SOC, который будет защищать как корпоративный сегмент, так и промышленный, причем сможет взаимодействовать с ГосСОПКА и другими сервисами для обеспечения комплексной защиты корпоративной сети клиентов. Ключевым продуктом экосистемы защиты является DATAPK Industrial Kit, который обеспечивает однонаправленное получение данных, прослушивание трафика и его анализ с обработкой выделенных событий и инцидентов. Причем в продукте используются технологии машинного обучения для восстановления структуры закрытых промышленных протоколов и мониторинг отклонений от эталонных моделей с обнаружением несанкционированных изменений в АСУ ТП. Именно этот компонент и выявляет целенаправленные атаки на промышленные системы и помогает обнаружить атаки на промышленные сегменты корпоративной сети.

Место межсетевого экрана в защите технологических процессов определил в своем докладе архитектор решений компании «Инфо-Текс» Андрей Иванов. По его мнению, МСЭ позволяет обеспечить сегментирование корпоративных сетей и выделение промышленного сегмента в отдельную сеть с более высокими требованиями по защите и обеспечению безопасности. Кроме того, межсетевые экраны обеспечивают защищенные каналы связи, что важно для удаленных компонентов АСУ ТП, которые управляют распределенными и протяженными объектами. МСЭ также обеспечивают защиту периметра корпоративных сетей и организацию удаленного доступа, в том числе и для безопасного обслуживания удаленных элементов технологического сегмента. Причем межсетевые экраны промышленного исполнения (тип Д по классификации ФСТЭК) должны понимать и защищать промышленные протоколы.

Для защиты у нас всего хватает – не хватает только желания.

Александр Соколов

Генеральный директор ООО «АйТи Бастион» Сергей Вячеславович Бочкарев и руководитель направления по развитию продуктов Константин Сергеевич Родин прочитали совместный доклад на тему «Большие привилегии – большая ответственность. Безопасный доступ: от классических постулатов к современным требованиям», в котором раскрыли подробности защиты привилегированных пользователей. Такие инструменты позволяют защитить от человеческого фактора, теневых ИТ, несоответствия требованиям, репутационных рисков, а также от поставщика услуг, атаки через цепочки поставок и геополитических рисков. Последние три пункта прибавились совсем недавно и сразу стали наиболее актуальными на рынке инструментов для контроля действий привилегированных пользователей.

Сергей БОЧКАРЕВ,
ООО «АйТи Бастион»

Александр ПОЗНЯКЕВИЧ,
«Лаборатория Касперского»

Вадим ПОДОЛЬНЫЙ,
СТО, Лаборатория Технологий Автоматизации

Штрафы, которые накладываются, могут разорить и нас, и заказчика, и часть бюджета России.

Игорь Рыжов

Тему защиты клиентских устройств в АСУ ТП раскрыл в своем докладе «Переход от антивирусной защиты и системы обнаружения вторжений к технологии XDR в АСУ ТП» руководитель направления по защите промышленных инфраструктур «Лаборатории Касперского» Александр Познякевич. Он отметил, что во второй половине 2022 в России отмечено самое значительное изменение процента атакованных компьютеров в АСУ среди всех стран, обслуживаемых компанией. Этот показатель, по данным «Лаборатории Касперского», увеличился на девять пунктов и составил 39,2%. Поэтому компания разработала единую концепцию промышленной кибербезопасности под названием Kaspersky OT CyberSecurity. Она включает в себя сервисы компании и разработанные ею продукты, которые покрывают до 80% всех мер защиты, требуемых регулирующими органами.

Андрей ИВАНОВ,
архитектор решений, ИнфоТекс

Промышленные инструменты защиты

Далее в пленарном заседании и на секции «Методы, технологии и инструменты защиты АСУ ТП» подробно обсуждались основные проблемы безопасности промышленных информационных систем и средства их защиты.

В частности, руководитель отдела развития InfoWatch ARMA Алексей Петухов в своем выступлении «Что и как защищать в АСУ ТП? Переосмысление концепции ИБ АСУ ТП в 2023 г.» поделился принципами построения встроенных механизмов защиты.

Алексей ШАНИН,
директор ООО «СайберЛимфа»

По его мнению, встроенными средствами защиты можно управлять централизованно в рамках существующей системы АСУ ТП, а для наложенных это реализуется довольно сложно. Кроме того, использование встроенных средств защиты позволяет создать на отдельном предприятии защищенную программную среду, которая станет функционировать более безопасно и надежно без добавления наложенных инструментов. При этом техническая поддержка комплексного решения со встроенными механизмами безопасности будет работать на уровне самих разработчиков, что позволит превратить межсетевой экран и другие элементы из «черного ящика» в полноценный корпоративный сервис.

Новые требования рынка и его реалии для отечественных промышленных предприятий обсудил в своем докладе заместитель директора Центра промышленной безопасности АО НИП «Информзащита» Игорь Николаевич Рыжов. Он отметил, что сейчас промышленные компании начали реально заниматься защитой АСУ ТП, разбором и защитой промышленных протоколов. Однако для полной замены АСУ ТП потребуются долгие годы. Поэтому компаниям приходится совмещать уже работающие решения и новые, которые построены на

АО «Лаборатория Касперского»

Алексей ПЕТУХОВ,
InfoWatch ARMA

Игорь РЫЖОВ,
АО НИП «Информзащита»

Евгений ДРУЖИНИН,
K2 Тех

решениях новых поставщиков АСУ ТП для отдельных отраслей, – они, по словам Игоря Николаевича, уже начали появляться на нашем рынке. Разделять эти сегменты приходится чуть ли не физически – например, с помощью технологий KVM-терминалов.

Проблемы вызывают и решения с открытым программным кодом. Их разработчики все чаще начинают делить программистов на «правильных» и «неправильных», что в будущем может привести к серьезным проблемам в разработке. Хотя, по его словам, закладки, которые были обнаружены в прошлом году в отдельных проектах, были направлены на получение денег в рамках проектов Bug Bounty и не ставили целью атаки на отечественные промышленные сегменты. Однако безопасность открытого программного кода нужно проверять не менее тщательно, чем остальные решения.

Одной из ключевых тем прошедшего и текущего года является импортозамещение. Его особенности раскрыл ведущий эксперт по информационной безопасности компании K2 Тех Евгений Дружинин в докладе «Импортозамещение на практике: архитектура, совместимость, гарантии». По его мнению, проблема перехода на отечественные продукты должна решаться комплексно, начиная с создания пилотных зон для отработки технологий защиты, и уже по результатам тестирования технологий можно составлять пошаговый план перевода оборудования на отечественные разработки. Важно успеть провести этот процесс до 2025 г., когда использование российского оборудования должно стать обязательным. Поэтому начинать тестирование предлагаемых решений следует уже в текущем году.

Директор по аналитике и интеграции НПП «Цифровые решения» Сергей Алексеевич Плотко в своем докладе «Подключение средств сетевой безопасности к инфраструктуре АСУ ТП» рассказал о такой технологии, как брокер сетевых пакетов, что обеспечивает ответвление сетевого трафика в промышленной сети для его анализа и выявления вредоносной активности. Предлагаемый компанией продукт позволяет не только безопасно для АСУ ТП создать копию всего сетевого трафика, но и сделать его запись на собственном оборудовании. Продукт полностью российский и может стать ключевой частью системы мониторинга АСУ ТП.

Важным компонентом защиты промышленных сетей являются продукты для однонаправленной передачи данных – инфодиоды.

Раньше мы внедряли LDAP в промышленных сетях, а теперь занимаемся его искоренением.

Игорь Рыжов

Об особенностях их использования для защиты АСУ ТП рассказал в своем докладе руководитель направления собственных продуктов АМТ-ГРУП Вячеслав Половинко. Он отметил, что при построении защиты важно определиться с местом, где реально сосредоточено управление АСУ ТП на программном уровне. Иногда оно вообще вынесено во внешний объект. В этом случае кажется, что АСУ ТП изолирована, но на деле оказывается, что она плотно интегрирована с доменными структурами и другими офисными системами. В результате возникает опасность через подобную интеграцию навредить работе основной системы. Сейчас же, когда политические риски стали реальностью и в атаке на АСУ ТП могут участвовать в том числе и производители решений, возникает реальная потребность в полной изоляции промышленных объектов, вплоть до воздушного зазора.

Сергей ПЛОТКО,
НПП «Цифровые решения»

Вячеслав ПОЛОВИНКО,
АМТ-ГРУП

Алексей МАКАРОВ,
Xello

Наложенные СЗИ – это настоящее, а встроенные и встраиваемые – будущее.

Андрей Бондюгин

В своем доклад «Игра с нулевой суммой: как выявить злоумышленника в сегменте АСУ ТП с помощью технологии киберобмана (deception)» технический директор компании Xello Алексей Александрович Макаров рассказал о необходимости построения ловушек для хакеров, что позволит вовремя заметить присутствие посторонних в системе и выявить цели и направления их деятельности. Он отметил, что продвижение злоумышленника в инфраструктуре жертвы описывается теорией игр, что дает возможность использовать математические модели для выявления и локализации посторонних. Алексей Александрович пояснил, что пентестеры в 100% случаев попадают в расставленные ловушки, что и позволяет их быстро выявить и идентифицировать. Использование специально сгенерированных ловушек обеспечивает возможность службе безопасности повысить защищенность всей системы, вовремя обнаруживая врагов.

Ведущий инженер компании «Газинформсервис» Александр Юрьевич Максимов рассказал об использовании такого класса продуктов, как контролер целостности конфигурационных файлов. Он позволяет обнаружить все несанкционированные изменения в конфигурации, провести аудит межсетевого экрана, выявить неисправленные уязвимости и проверить безопасность устройств, в частности оборудования АСУ ТП.

Заместитель руководителя по вопросам промышленной кибербезопасности компании КСБ-СОФТ Татьяна Егорова прочитала доклад на тему «Инженерный подход к ИБ в АСУ ТП», в котором отметила особенности построения защиты промышленных объектов. Она утверждает, что защита АСУ ТП выполняется по тем же процедурам, что и защита офисных ИТ, но имеет нюансы – они начинаются с документации для аудиторов объекта. При этом на безопасность объекта оказывают влияние не только наложенные средства, но и правильное построение сети. Татьяна Егорова отметила,

АО «ИнфоТеКС»-

Александр МАКСИМОВ,
ГАЗИНФОРМСЕРВИС

Татьяна ЕГОРОВА,
КСБ-СОФТ

Мы рассматриваем наложенные средства защиты как костыль

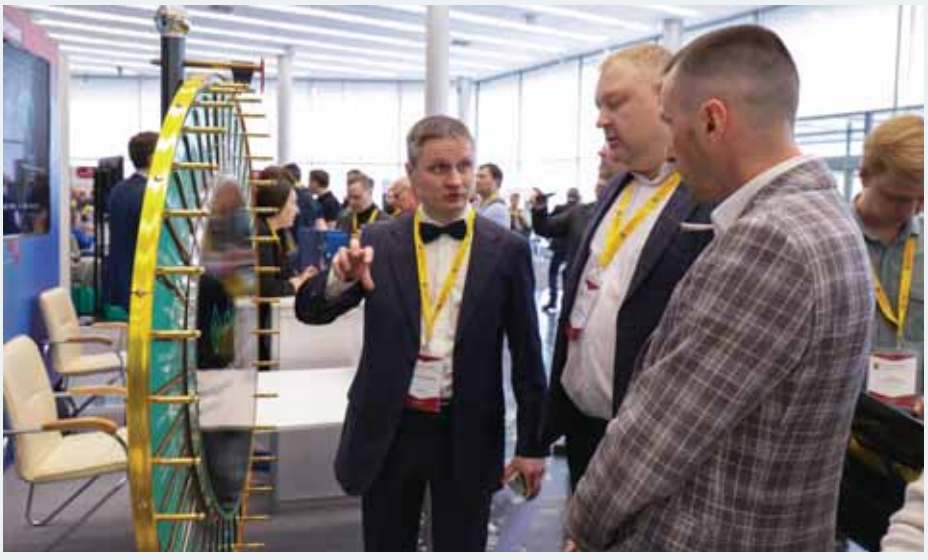
Дмитрий Пономарев

что иногда средства защиты накладываются уже на готовую систему, что обходится значительно дороже варианта, когда средства защиты изначально являются частью проекта внедрения.

Важную тему организации киберучений затронул в своем докладе «Как правильно провести киберучения для ИБ-специалистов промышленного предприятия» технический директор Национального киберполигона компании «Ростелеком-Солар» Андрей Кузнецов. Его компания уже провела более 400 киберучений, в которых использовала для отработки навыков как собственные механики вредоносной активности, так и почерпнутые в открытых источниках. Проведение учений, особенно совместно промышленного и офисного сегментов, помогает специалистам в АСУ ТП лучше понять, как именно их системы могут быть атакованы и к каким последствиям подобные атаки способны привести. Правда, многие специалисты боятся проведения киберучений, которые, по их мнению, могут выдать их некомпетентность. Однако специалист, прошедший тренировку на киберполигоне, обладает более высокими компетенциями, чем тот, который ни разу не сталкивался с изощренными методами кибератак на промышленные и офисные сегменты.

Технический директор ООО «СВД Встраиваемые Системы» Андрей Васильевич Сеньков в своем выступлении рассказал об операционной системе реального времени «Нейтрино», которая может быть использована в составе АСУ ТП. Операционная система является полностью отечественной и имеет необходимый набор инструментов информационной безопасности. На базе этой операционной системы разработана в том числе и SCADA под названием «Фокус», которая может быть использована на производстве. Продукты компании с 2011 г. применяются на предприятиях ОПК и гражданских производствах. Сейчас компания разработала технологию искусственного интеллекта, которая может работать в условиях ограниченных ресурсов. И если раньше производители были сосредоточены на разработке операционной системы для отечественных процессоров, то теперь они планируют расширить выбор процессоров за счет иностранных моделей, в первую очередь китайских.

Важную тему в конце пленарного заседания поднял председатель правления Ассоциации «Цифровые инновации в машиностроении» (АЦИМ) Борис Михайлович Позднеев – «Информационная безопасность в аспекте цифровой трансформации промышленности». Индустрия 4.0 и цифровая трансформация сейчас только наращивают обороты,



UDV group

АМТ ГРУП

Если снести ERP, завод даже не вздрогнет – будем все делать на кальке.

Сергей Седов

однако требования по защите за этим процессом не поспевают. Если первые стандарты для Индустрии 4.0 уже выпущены, то в области информационной безопасности процесса стандартизации не наблюдается.

Пластырь против пилюли

Центральным событием конференции стала дискуссия «Наложенные vs встроенные средства безопасности АСУ ТП», в которой разработчики средств защиты АСУ ТП и их клиенты обсуждали приемлемый компромисс между встроенными в АСУ ТП механизмами защиты и наложенными средствами обеспечения безопасности. На ней, в частности, обсуждались возможности, потенциал и границы применения современных наложенных средств защиты АСУ ТП; технологии, типовые механизмы и задачи, решаемые современными встроенными средствами защиты самих АСУ ТП; кибериммунные продукты, среды и приложения; концепция DevSecOps и ее практическое применение к решению задач в области безопасности АСУ ТП; подходы к поиску баланса и построения гибридных схем создания системы защиты АСУ ТП, включающей встроенные и наложенные средства защиты.

В частности, руководитель группы по сопровождению проектов защиты промышленных инфраструктур «Лаборатории Касперского» Андрей Бондюгин считает, что наложенные СЗИ – это настоящее, а встроенные и встраиваемые – будущее. Он отметил, что существующая нормативная база ориентирована на использование наложенных СЗИ – практически все нормативные акты содержат требования для внешних средств защиты, а встроенные требуют сложного процесса внедрения системы безопасной разработки и сертификации по уровням доверия для всего функционала, а не только для механизмов безопасности.

Впрочем, по словам Андрея Бондюгина, для доверенных платформ АСУ ТП уже есть прототипы, хотя массового их внедрения можно ожидать в течение пяти-десяти лет. Разработчикам АСУ ТП

Андрей КУЗНЕЦОВ,
«Ростелеком-Солар»

Андрей СЕНЬКОВ,
ООО «СВД Встраиваемые Системы»

Борис ПОЗДНЕЕВ,
председатель правления Ассоциации «Цифровые инновации в машиностроении» (АЦИМ)

нужно задумываться о создании элементов доверия. Он определил минимальный набор механизмов безопасности, которые необходимо встроить в АСУ ТП: надежная аутентификация, контроль доступа и формирования событий для передачи в корпоративные системы безопасности и корреляции событий.

По мнению СТО «Лаборатории технологий автоматизации» Вадима Павловича Подольного, встроенные системы – это безопасность в дизайне. Остальное определяется применением. Для готовой системы можно использовать только наложенные СЗИ. Однако если проектируется новая система, то все зависит от того, что выберет клиент. Кроме того, Вадим Павлович ввел принцип естественной безопасности, которая обеспечена естественным путем – без дополнительных мер. Сейчас подобные решения уже начинают разрабатываться, однако, по его мнению, чтобы что-то создать, нужно потратить всего 10 руб., чтобы что-то защитить – 100 руб. Поэтому для разработчиков промышленных систем лучше встраивать необходимые защитные механизмы еще на уровне проектирования – они должны быть уже в техническом задании.

Свое мнение на круглом столе высказал и заместитель технического директора по ИБ

Андрей БОНДЮГИН,
«Лаборатория Касперского»

InfoWatch ARMA

ООО «Научно-внедренческая фирма «Сенсоры, Модули, Системы» Дмитрий Анатольевич Пономарев. Он отметил, что рассматривает наложенные средства защиты как костыль. Более правильным подходом является разработка встроенных средств защиты еще при проектировании АСУ ТП. По его данным, с 21 марта действуют новые требования ФСТЭК к наложенным средствам, поэтому заказчикам выгоднее иметь встроенные средства, чтобы меньше платить за безопасность: система проще и точек отказа меньше.

По мнению директора департамента информационной

Дмитрий ПОНОМАРЕВ,
ООО Научно-внедренческая фирма «Сенсоры, Модули, Системы»

Самая большая угроза – это то, что документы для АСУ ТП пишут айтишники.

Сергей Седов

и компьютерной безопасности АСУ ТП АО «РАСУ» Константина Валерьевича Сахарова, в разных отраслях должны быть разные наложенные средства, поскольку в них все зависит от специфики. Тем не менее будущее за встроенными средствами защиты.

В то же время руководитель продуктового направления АО «ИнфоТеКС» Марина Викторовна Сорокина напомнила, что регулятор не мыслит отдельными устройствами, а системами, и это надо менять. Необходимо разрабатывать требования к отдельным механизмам, а не к системам в целом. Именно потому сейчас встроенные средства не достигли достаточного уровня – им нужно развиваться в течение двух-трех лет, чтобы достичь требуемого уровня.

Было признано, что в АСУ ТП должны быть, как минимум, базовые механизмы защиты, которые перечислил Андрей Бондюгин: аутентификация,

Марина СОРОКИНА,
АО «ИнфоТеКС»

Константин САХАРОВ,
АО «РАСУ»

Сергей СЕДОВ,
ПАО «Газпром нефть»

Мы каждый год живем в новой реальности.

Сергей Бочкарев

контроль доступа и журнал событий, а все остальное можно отдать на откуп наложенным, более гибким и интеллектуальным системам обеспечения информационной безопасности. Выступающими также было отмечено, что в условиях увеличения количества и повышения изощренности атак на информационную инфраструктуру всех отраслей именно импортозамещение средств защиты и самих АСУ ТП является основой для построения надежных и устойчивых к внешним воздействиям промышленных систем.

В рамках конференции также состоялись отраслевые круглые столы: «Опыт защиты АСУ ТП в топливно-энергетическом комплексе и нефтехимической промышленности», «Опыт защиты АСУ ТП в металлургии и трубной промышленности», «Опыт защиты АСУ ТП в оборонно-промышленном комплексе и космической промышленности» и «Опыт защиты АСУ ТП на транспорте». На каждом из них была организована дискуссия между разработчиками средств защиты и их потребителями по четырем главным вопросам: «Что защищаем?», «От чего защищаем?», «Как защищаем?» и «Чем защищаем?», где подробно обсуждались нюансы каждой из перечисленных отраслей в сфере защиты промышленных высокоинтеллектуальных объектов.

НПП «Цифровые решения»-

Энергия защиты

В рамках круглого стола по ТЭК и энергетике руководитель Центра промышленной автоматизации и метрологии ПАО «Газпром нефть» Сергей Юрьевич Седов рассказал о современных платформенных решениях по промышленной автоматизации и подходах к обеспечению их защиты. Он отметил, что большинство АСУ ТП основаны на коммерческих технологиях иностранных разработчиков, что и приводит к проблемам перехода от одного производителя к другому. В то же время в мире уже есть открытые платформы для построения АСУ ТП, например O-PAS. Для этого открытого стандарта выпускается оборудование,

Александр НИКОЛАЕВ,
«Лаборатория Касперского»

Дмитрий ПРАВИКОВ,
РГУ нефти и газа (НИУ) имени И.М. Губкина

Повторение – мать заикания.

Константин Родин

ориентация на него позволяет компаниям выбрать производителей из списка совместимого оборудования и не привязываться к конкретному производителю решений. Такой стандарт удобен как для постепенного импортозамещения, так и для организации конкуренции уже на уровне отдельных устройств и компонентов АСУ ТП. Однако пока у нас переведен только самый минимум международных стандартов – два из 11, что затрудняет реализацию стратегии импортозамещения, основанной на стандартах.

Заведующий кафедрой КБ КВО, РГУ нефти и газа (НИУ) имени И.М. Губкина Дмитрий Игоревич Правиков обсудил с собравшимися за круглым столом проблемы кибербезопасности при реализации «Промышленной революции 4.0» в нефтегазовом секторе. Он отметил, что внедрение технологий, относящихся к Индустрии 4.0, позволяет компании увеличить производительность труда на предприятии в среднем на 15%. Он также пожаловался, что «Ростехнадзор» при анализе производственных аварий до сих пор не рассматривает кибератаку как возможную причину возникновения ЧП, хотя понятно, что сейчас это всегда может рассматриваться в качестве первой версии случившегося – вмешательство со стороны злоумышленников и провоцирование аварии.

Практику безопасного разрешения вопросов обеспечения ИБ для случаев удаленного мониторинга и удаленного доступа со стороны разработчиков промышленного оборудования и АСУ ТП разобрал в своем докладе ведущий инженер поддержки продаж ООО «АйТи Бастион» Алексей Юрьевич Ширикалов. Он отметил, что администрирование АСУ ТП удаленно из общественного места по Wi-Fi является одной из серьезных угроз, поскольку такое соединение можно перехватить и организовать атаку типа «человек посередине». В принципе, сейчас уже появляются решения, которые позволяют выявить потенциально опасное поведение подобных удаленных подключений, причем не требуя существенной перестройки инфраструктуры. Такое решение обеспечивает возможность контролировать взаимодействие привилегированных пользователей при удаленном подключении и передавать в системы мониторинга безопасности предупреждения о подозрительном поведении администраторов.

Менеджер по безопасности критической информационной инфраструктуры ООО «Распадская угольная компания» Константин Викторович Куртуков отметил, что для них значимыми объектами являются системы жизнеобеспечения, поэтому ключевой АСУ ТП становится ИС аэрогазового контроля. Если злоумышленникам удастся на нее повлиять, то может произойти необратимая авария. Примерами значимых объектов являются также системы позиционирования людей в шахте и управления вентиляторами.

ООО «СВД ВС»

Я не говорю про гиперинтеллектуальные системы типа ChatGPT, я говорю про статистику.

Константин Родин

Алексей ШИРИКАЛОВ,
ООО «АйТи Бастион»

Алексей ВЛАСЕНКО,
ИнфоТеКС

Заместитель начальника отдела ССПБ ООО «Распадская угольная компания» Сергей Николаевич Куликов рассказал о борьбе с внутренними нарушителями при ограничении доступа невзрывозащищенных устройств к подземной сети Wi-Fi на угольных шахтах. Такие устройства создают серьезные угрозы взрыва в условиях шахты, однако сотрудники все равно берут их с собой, чтобы иметь возможность поиграть на них во время смены. Для предотвращения подобных злоупотреблений в шахте решили использовать Radius-сервер со списком легитимных для доступа пользователей в Интернет.

По мнению ведущего специалиста группы по обеспечению безопасности объектов критической информационной инфраструктуры ООО «ЛУКОЙЛ-Нижневолжскнефть» Андрея Михайловича Москаленко, главная задача закона – спасение человеческих жизней. Правда, основным риском зачастую является «внутренний нарушитель». В то же время чаще всего категорируются АСУ ТП, коммерческие системы и системы учета. При этом другие системы практически не учитываются, что как раз и не позволяет правильно оценить их защищенность и работоспособность.

СТО «Лаборатории технологий автоматизации» Вадим Павлович Подольный отмечает, что если АСУ ТП работает и технологический процесс идет в штатном режиме, то лучше его не трогать, а для защиты от внешних воздействий использовать только организационные меры и наложенные средства. Иногда лучшая защита – ничего не делать, поскольку не всегда понятно, как установка средств защиты повлияет на технологический процесс.

По мнению заведующего кафедрой КБ КВО, РГУ нефти и газа (НИУ) имени И.М. Губкина Дмитрия Игоревича Правикова, разделение регулятором АСУ на значимые и незначимые объекты носит чисто тактический характер. Защищать в любом случае придется все. Он также отметил, что самый большой риск создает «внутренний нарушитель», который может вызвать аварию и длительный простой предприятия. Минэнерго сейчас идет по пути построения отраслевых центров мониторинга – в них будет сконцентрирована помощь по предотвращению инцидентов и расследованию последствий. В ТЭК внимательно относятся к функциональной безопасности и не допускают на объектах вольностей. «Не навреди – это правильный подход при защите предприятия», – считает Дмитрий Игоревич.

Архитектор по ИБ АСУТП ПАО «Интер РАО» Наталия Владимировна Устич полагает, что лучшая форма защиты – полностью отрезать все системы без использования инфодиода. Однако никто не готов отказаться от «сырых» данных, поэтому приходится идти на компромиссы.

«Газинформсервис»

Константин КУРТУКОВ,
ООО «Распадская угольная компания»

Андрей МОСКАЛЕНКО,
ООО «ЛУКОЙЛ-Нижневолжскнефть»

Наталия УСТИЧ,
«Интер РАО»

При этом каждую систему нужно защищать по своим правилам. Невозможно сделать цифровой двойник для всех – на каждом объекте есть нюансы. В результате получается очень дорого. Основной метод защиты – контроль целостности, что позволяет держать под контролем в том числе и «внутреннего нарушителя». Наталия Владимировна отмечает важность типового перечня объектов, подлежащих категорированию, поскольку для некоторых систем очень тяжело понять принципы их категорирования. При этом она отметила, что в части оборудования защиты по-прежнему останется дисбаланс в пользу иностранного оборудования. Наиболее массово нашими производителями представлены диоды данных, SIEM и антивирусы, однако не хватает промышленных межсетевых экранов нового поколения (NGFW).

Информационная броня

В рамках круглого стола «Опыт защиты АСУ ТП в металлургии и трубной промышленности» руководитель отдела кибербезопасности АСУ ТП компании Innostage Дмитрий Николаевич Авраменко провел «Анализ рисков информационной безопасности в системах промышленной автоматизации: что, где, когда и для чего».

Он отметил: даже если у вас все сделано по правилам, это не будет гарантией защиты от кибератак. В начале 2022 г. у большинства атакованных компаний было все сделано правильно, но тем не менее у некоторых что-то пошло не так. По его мнению, службы ИБ должны взаимодействовать с другими типами безопасности и реализовать меры, которые обеспечат максимальный эффект.

Директор по научной работе компании «Актив» Сергей Панасенко посвятил свое вступительное слово на круглом столе вопросам построения комплексной системы контроля и мониторинга носителей данных. С помощью подобных инструментов можно контролировать различные мобильные носители данных, которыми приходится пользоваться в случае полного разрыва сетей вплоть до воздушного зазора.

Нормативная база бежит впереди и всех подгоняет.

Вячеслав Половинко

K2Tex

Нефтегазовой компании тащить на себе облака накладно – придется доверить это дело кому-то еще.

Дмитрий Правиков

ООО «АТБ Электроника»

На круглом столе начальник отдела обеспечения безопасности информационных систем ООО «ЕВРАЗ» Андрей Витальевич Нуйкин рассказал о событиях прошедшего года. Он отметил, что все начиналось с массовых DDoS-атак, за которыми последовали вредоносы, которые пытались воздействовать на системы предприятия со всех сторон. Однако к 1 сентября, видимо, когда новоиспеченные хакеры пошли в школу, количество атак уменьшилось. Сейчас ситуация стабильна. В результате подобной вредоносной активности в компании было принято решение не допускать никакого управления извне. Параллельно происходит процесс импортозамещения некоторых средств защиты. К сожалению, сейчас в России нет адекватного NGFW, поэтому приходится снижать планку требований. В частности, в компании тестируют Usergate на строящихся сетях, поскольку пока это не очень критично. Usergate ближе всего подошел к функционалу NGFW. Кроме того, не хватает дешевых сканеров уязвимости, поскольку разработчики существующего сканера стараются продать сразу всю экосистему своих продуктов.

Аналогичные киберинциденты отметил и начальник управления информационной безопасности СЭБ ПАО «ТМК» Александр Владимирович Севостьянов. У компании также все начиналось с DDoS, но сейчас процесс обеспечения безопасности сместился на контроль «внутреннего нарушителя» и подрядчиков. Компания вынуждена проверять все их действия, чтобы подрядчики под видом услуг не осуществили диверсию. Когда в компании 60 тыс. человек, контролировать всех достаточно сложно. Приходится применять специализированные средства автоматизации подобного контроля. Параллельно стартовал процесс импортозамещения: антивируса, PAM и других механизмов защиты. К сожалению, российские разработки не всегда удовлетворяют требованиям таких взыскательных клиентов.

Андрей НУЙКИН,
ООО «ЕВРАЗ»

Александр СЕВОСТЬЯНОВ,
ПАО «ТМК»

Дмитрий АВРАМЕНКО,
компания Innostage

ГК Innostage

Инфо-ОПК

На круглом столе «Опыт защиты АСУ ТП в оборонно-промышленном комплексе и космической промышленности» собравшиеся обсудили особенности защиты наиболее критических на данный момент отраслей отечественной промышленности. В этих отраслях публичный обмен опытом особенно затруднителен в связи с особенностями законодательства, поэтому ценно каждое выступление, которое помогает другим участникам указанных отраслей построить свою защиту в соответствии с лучшими практиками отрасли и сделать ее более надежной.

На открытии круглого стола начальник центра мониторинга и реагирования на компьютерные инциденты АО «ИБ Реформ» Артем Константинович Сычев прочитал доклад на тему «Подходы к оценке уровня зрелости кибербезопасности промышленных предприятий», в котором подчеркнул, что Указ Президента РФ № 250, принятый 1 мая прошлого года, потребовал отчитаться об уровнях зрелости, поэтому компаниям пришлось заняться работой в области информационной безопасности. Проблемой стало

Сергей ПАНАСЕНКО,
компания «Актив»

Артем СЫЧЕВ,
АО «ИБ Реформ»

Модель продаж простая – договариваемся.

Вадим Подольный

то, что компании не всегда понимали, какие недопустимые события и негативные последствия у них могут быть. Пришлось провести инвентаризацию ИТ-активов и разработать методику проверок доступности отдельных вычислительных ресурсов и серверов. Параллельного приходилось заниматься совершенствованием практических навыков персонала. Однако лучше подобную работу доверить профессионалам – именно для этого и предназначены такие организации, как киберполигон. При этом кадровым резервом для ИБ службы часто выступает ИТ-департамент.

Своим опытом отражения кибератак поделился и начальник Управления информационной безопасности АО «Концерн «Калашников» Алексей Владимирович Ахмеев. Он отметил, что его компании пришлось полностью отключить АСУ ТП и ЧПУ от сети. Станки находятся в защищенной зоне – в компании заранее подготовились к возможной конфликтной ситуации. Однако основной проблемой является человеческий фактор. Отрасль ОПК всегда была наполнена специфическими требованиями от регуляторов, поскольку везде существует ГОЗ. Периодически возникают проблемы по взаимодействию с производителем – сложно прогнозировать, как поведут себя поставщики.

Алексей Владимирович отмечает, что сейчас вектор атак сместился в сторону профессиональных хакерских группировок. Причем вектор отклонился от шпионажа в направлении кибератак и кибертерроризма. А в предыдущие два года был бум вымогателей. Для импортозамещения именно NGFW – основная

Евгений МИТЮШКИН,
UserGate

Алексей АХМЕЕВ,
АО «Концерн «Калашников»

Борис БЕЗРОДНЫЙ,
АО «НИИАС»

Иногда самая лучшая ваша защита – ничего не делать.

Вадим Подольный

проблема, но дальше есть потребности в качественных PAM и IDM. Причем в отрасли большое количество станков с ЧПУ иностранного производства, и если они будут признаны объектами КИИ, то их придется полностью замещать.

Безопасность на транспорте

Заместитель начальника Центра – начальник отдела АО «НИИАС» Борис Федорович Безродный посвятил свое вступительное слово на круглом столе вопросам обеспечения безопасности систем железнодорожной автоматики и механики по требованиям к объектам КИИ. По его словам, если система функционирует штатно, то и ущерба быть не может. Он возникает, если система выходит из штатного функционирования. Существуют три аварийные ситуации: опасный, защитный и случайный отказы. Причем случайный отказ может быть «рукотворный», в том числе в результате кибератак.

Для отказов строится сеть Маркова, в которой используются вероятности перехода из одного состояния в другое. Для кибератаки сеть не меняется – меняются только вероятности переходов. У защитных и случайных отказов ущерб может быть, но он ограничен. Однако при введении защитных отказов надежность системы снижается, хотя вероятность перехода в опасный отказ уменьшается. Это означает, что без внешнего воздействия инцидента быть не может. Его нужно полностью исключить. Остается «внутренний нарушитель», за которыми нужно следить. На станционных АРМ есть только экран и мышь. Клавиатуры нет – захочешь, ничего не наберешь. Все USB-порты, которые используются для технического обслуживания, опломбированы. Защита отказа, отсутствие НДВ, проверка логики работы системы – этого достаточно для штатного функционирования транспортных АСУ.

По данным эксперта отдела обеспечения безопасности значимых объектов КИИ ЦИБ ОАО «РЖД» Полины Юрьевны Генераловой, в компании есть значимые объекты, в том числе АСУ ТП, системы управления

ООО «УЦСБ»

Полина ГЕНЕРАЛОВА,
ОАО «РЖД»

Вячеслав РЯЗАНОВ,
ООО «ЛокоТех-Сигнал»

Чтобы что-то создать, нужно потратить 10 руб., чтобы что-то защитить – 100 руб.

Вадим Подольный

движением поездов и системы управления диспетчерской. Высокую категорию получают те системы, которые находятся на высоконагруженных участках. Там существуют требования к функциональной безопасности. После оценки рисков и моделирования угроз, возможно, потребуются дополнительные меры. Причем обычно в системах РЖД циркулирует техническая информация, разглашение которой не приведет к опасным последствиям. Если информация будет неполной или недостоверной, то система просто уйдет в защитный отказ.

Вся информация обрабатывается исключительно во внутренней сети, поэтому актуален только «внутренний нарушитель». Совершить вредоносные действия может лишь узконаправленный специалист самой компании. Если команда некорректна, то система также уходит в защитный отказ. Взаимосвязанные системы проверяют корректность получаемых команд. Если подкупленный диспетчер пытается перевести поезд на занятый путь, то опять же происходит защитный отказ – корректность действий персонала проверяет специальная логическая система.

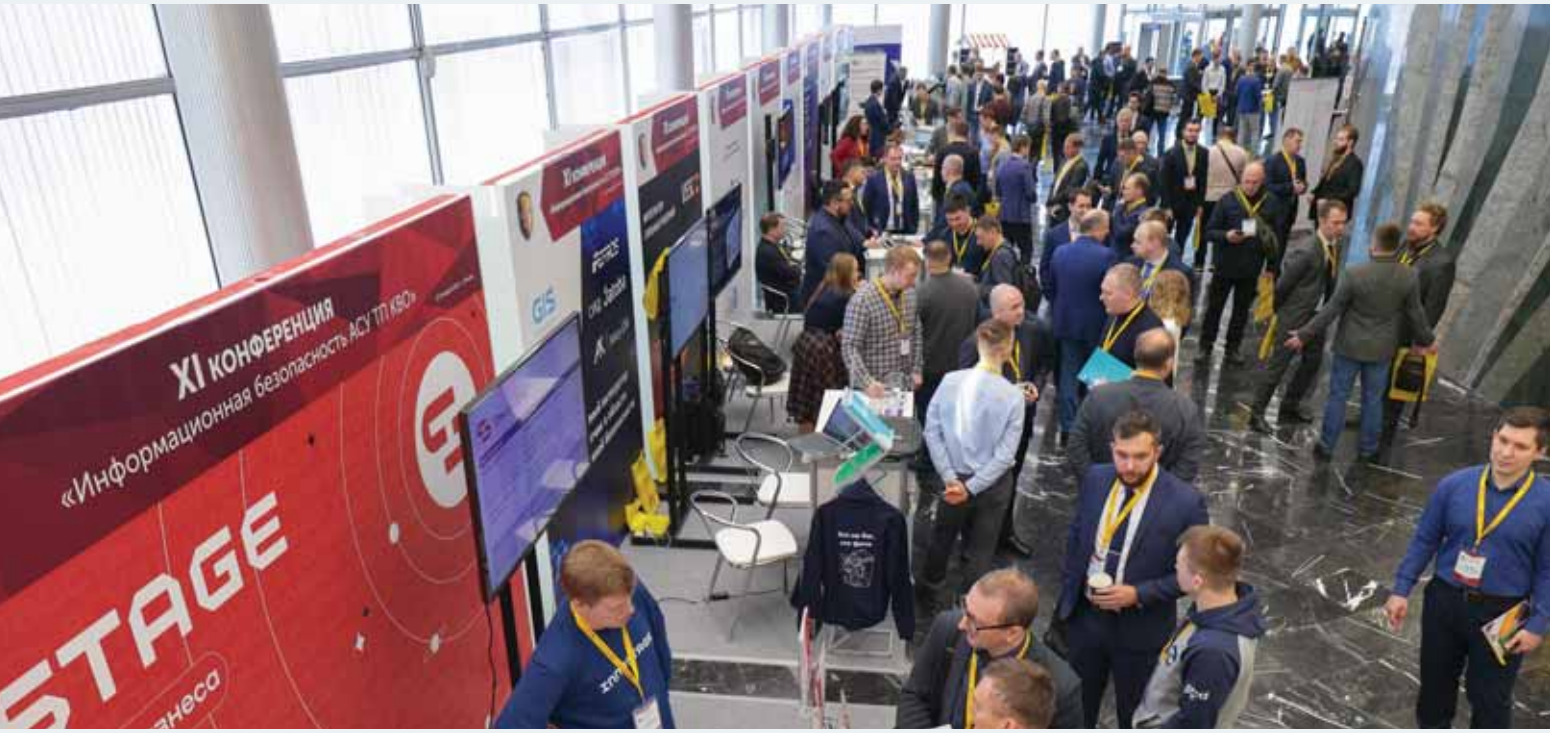
В своем выступлении на круглом столе руководитель отдела качества и безопасности ООО «ЛокоТех-Сигнал» Вячеслав Юрьевич Рязанов отметил, что стоит обратить пристальное внимание на беспилотный транспорт, причем сделать это нужно уже сегодня. Эти технологии также должны быть включены в перечень систем, которые необходимо защищать. Однако в части требований информационной безопасности сейчас много недопонимания по поводу необходимых инструментов для защиты транспортных информационных систем, что ограничивает темпы категоризации объектов по требованиям Закона № 187-ФЗ.

В телеграм-канале конференции был проведен опрос участников конференции, а также организовано обсуждение каждого доклада – все выступающие получили огромное количество вопросов, на которые они смогли ответить как во время своего выступления, так и в самом телеграм-канале.

Обмен опытом контроля

В рамках конференции «Информационная безопасность АСУ ТП КВО» также состоялся круглый стол компании «АйТи Бастион» для заказчиков на тему «Реальные истории применения системы контроля привилегированного доступа от первого лица». В его рамках разбирались базовые сценарии применения комплекса СКДПУ НТ на опыте компании «АйТи Бастион», опыт эксплуатации и применения этого комплекса на реальных инфраструктурах заказчиков, а также принципы проектирования, эксплуатации и применения комплекса

PLC Technology



Реальность отличается от того, что можно нарисовать в вакууме.

Алексей Шанин

СКДПУ НТ на опыте компании интегратора систем безопасности АСУ ТП. В круглом столе принимали участие представители таких заказчиков, как «Данные – центр обработки и автоматизации» (ДЦОА), АО «Россети Цифра» и iGrids – «Интеллектуальнее сети». Встреча была посвящена обмену опытом и ответам на вопросы о применении систем мониторинга и контроля привилегированных пользователей, автоматизации доступа к информационным системам и построению доверенной среды удаленного доступа.

В фойе конференции была организована выставка, где партнеры смогли продемонстрировать свои достижения в области защиты промышленных технологий и обменяться опытом использования представленных продуктов. В этом году партнерами конференции стали ООО «АйТи Бастион», АО «Лаборатория Касперского», ООО «Лаборатория технологий автоматизации», АО «ИнфоТеКС», UDV group, ГК «Кейсистемс», AMT GROUP, InfoWatch ARMA, АО «ДиалогНаука», ООО «СВД ВС», НПП «Цифровые решения», K2Tex, «Газинформсервис», НИП «Информзащита», ООО «СОЛАР СЕКЬЮРИТИ», ООО «Юзергейт», компания «Актив», ГК Innostage, ООО «УЦСБ», ООО «АТБ Электроника», ГК MONT, ООО «ЦИБИТ», PLC Technology и ООО «Код Безопасности».

Судя по выступлениям на конференции, российская система защиты критической информационной инфраструктуры выдержала самое сложное испытание, не допустив серьезных провалов и консолидировав опыт промышленных предприятий в рамках системы ГосСОПКА. Однако дальнейшее развитие системы защиты должно выполняться уже в рамках отдельных индустрий, которые перечислены в Законе № 187-ФЗ «О безопасности КИИ», чтобы наиболее точно учесть требования различных индустрий: ТЭК, энергетики, металлургии, ОПК, космической отрасли, транспорта и др. Сравнение подходов защиты, которое было проведено в рамках соответствующих круглых столов, показало, что у каждой из индустрий накопился опыт обеспечения безопасности функционирования собственного оборудования, поэтому кибербезопасность промышленных решений нужно вписать в существующие системы функциональной, противоаварийной и других видов защиты.

Именно потому ФСТЭК и НКЦКИ создают отраслевые правила защиты критической информационной инфраструктуры и центры ГосСОПКА, разрабатывая для этого и нормативные требования, и организационную инфраструктуру. Сейчас пока не очень понятно, в какие формы такие отраслевые правила и организации выльются, однако, судя по выступлениям международных спикеров, наши ближайшие соседи идут по тому же пути, вырабатывая аналогичные собственные решения. Возможно, со временем реализованные в российском киберпространстве решения по защите, в том числе промышленных систем, будут тиражироваться и в международном масштабе. ■