XII КОНФЕРЕНЦИЯ

«Информационная безопасность АСУ ТП КВО»

2024 г.

Курс на импортозамещение АСУ ТП как фундамент отраслевой безопасности КВО

13–14 марта 2024 г. в Москве прошла 12-я конференция «Информационная безопасность АСУ ТП КВО», организованная Издательским домом «КОННЕКТ». В мероприятии приняли участие 678 руководителей и специалистов в сфере ИБ и АСУ ТП, отраслевых экспертов, представителей органов исполнительной власти, регуляторов, отраслевой науки и высшей школы, предприятий и организаций из различных секторов промышленности. Основное внимание участники конференции уделили ситуации на рынке защиты АСУ ТП в преддверии вступления в силу законодательных требований по обязательному импортозамещению ПО и ПАК на значимых объектах (ЗО) критической информационной инфраструктуры (КИИ). Темы докладов активно обсуждались в телеграм-канале мероприятия.

Партнерами мероприятия выступили компании «АйТи Бастион», «Лаборатория Касперского», ГК Innostage, «ИнфоТеКС», UDV Group, АМТ-ГРУП, «ДиалогНаука», «КСБ-Софт», «Газинформсервис», УЦСБ, InfoWatch, SoftMall, К2Тех, «Информзащита», СВД ВС, «Актив», «НОРСИ-ТРАНС», «АйЭсТи».

В дни работы конференции была развернута выставочная экспозиция. Свои продукты и решения помимо вышеперечисленных представили компании PVS-Studio, UserGate, «КВ Системы», «Цифровые решения», ГК MONT, «Индид», «Акстел-Безопасность», «Сибирская Академия информационной безопасности», «Инфосистемы Джет», RuSIEM.

Методические подходы

Пленарное заседание открыл главный научный сотрудник Федерального исследовательского центра информатики и управления Российской академии наук **Виктор Гаврилов**, который представил итоги 2023 г. в области кибербезопасности

Преступность нельзя искоренить, нужно ее ввести в рамки.

Виктор Гаврилов

Виктор ГАВРИЛОВ,
ФИЦ информатики и управления РАН

Павел ЗЕНКИН,
ФСТЭК России

Кирилл АКИМОВ,
НИЦ по компьютерным инцидентам

и перспективы на 2024 г. В роли сомодератора выступил заместитель генерального директора ИД «Коннект» **Дмитрий Корешков**.

Виктор Гаврилов рассказал об уязвимости «нулевого дня» и выразил мнение, что для его выявления единственным реальным способом в настоящее время является привлечение проактивных методов на основе искусственного интеллекта с технологией обнаружения аномалий. Отсутствие прецедентов для обучения и использования такой технологии делает процесс еще более сложным. В контексте технологии искусственного интеллекта с выявлением аномалий особенно заметен эффект необъяснимости, поскольку критерии обнаружения аномалий остаются неясными. Это повышает вероятность ложных срабатываний и ошибок в процессе выявления уязвимостей. «Правоохранительные органы говорят, что преступность нельзя искоренить, но можно ввести ее в рамки. Так же и с защитой информации – доступными средствами и в разумные рамки», – подытожил Виктор Гаврилов.

Об особенностях реализации законодательства в области ОБ 30 КИИ, в том числе технических мер по повышению защищенности объектов КИИ, рассказал заместитель начальника управления ФСТЭК России **Павел Зенкин**. ФСТЭК России разработал рекомендации по улучшению уровня защищенности информации. В планах также подготовка изменений в НПА в части установления дополнительных требований по обеспечению информационной безопасности в организациях, выполняющих работы по заказам субъектов КИИ. В частности, рекомендуется обязать подрядчиков реализовывать меры по обеспечению безопасности и контролю за действиями подрядчиков; обеспечить возможность экстренного отключения сессии и отката действий, использования СОВ и анализаторов графика в точках сопряжения в системах подрядчика.

Не надо нам присылать школьные аттестаты ваших сотрудников. Это как-то несерьезно.

Кирилл Акимов

ФСТЭК России разработаны методические документы с целью организации работ по управлению уязвимостями.

Павел Зенкин

Стенд компании «АйТи Бастион»

В настоящее время многие организации, управляющие важными объектами, не обладают эффективными процессами управления уязвимостями. Отсутствуют анализ и необходимые меры по устранению и снижению рисков. Один из ключевых способов борьбы с уязвимостями ПО – регулярное обновление систем. Нехватка квалифицированных разработчиков создает серьезные проблемы в этой области. Однако готовятся рекомендации и методики по устранению уязвимостей, которые доступны на сайте для всех заинтересованных сторон. Особое внимание было уделено работе с отраслевыми перечнями типовых объектов КИИ. Была озвучена позиция регулятора, и даны конкретные рекомендации.

По завершении доклада состоялась «сессия вопросов и ответов регулятору», в рамках которой Павел Зенкин ответил и прокомментировал более полутора десятков вопросов.

Представитель Национального координационного центра по компьютерным инцидентам **Кирилл Акимов** представил краткий обзор функционирования ГосСОПКА и вектора дальнейшего развития системы. Эксперт осветил требования к центрам ГосСОПКА, которые включают проведение широкого спектра мероприятий: от обнаружения и регистрации компьютерных атак до координации подразделений и анализа рекомендаций по повышению защищенности. Процесс проверки в рамках аккредитации включает в себя анализ документов и представленных данных соискателя, проверку знаний и умений сотрудников, а также подтверждение достоверности информации. Центры ГосСОПКА должны соблюдать ряд обязательных требований: организовывать мероприятия по выявлению компьютерных атак и регистрации инцидентов, активно реагировать на инциденты и устранять их последствия, осуществлять оценку уровня защищенности информационных ресурсов от атак. Кроме того, координировать работу подразделений субъектов ГосСОПКА, проводить анализ и разрабатывать рекомендации по обеспечению безопасности информационных ресурсов.

О государственной политике в сфере технологического суверенитета в области АСУ ТП и ИБ рассказал начальник отдела департамента обеспечения кибербезопасности Минцифры РФ **Александр Рукосуев**. «В настоящее время прорабатывается подход к построению безопасных продуктов на платформе «ГосТех». Важно создавать системы, которые были бы защищены от уязвимостей уже на этапе проектирования, а не пытаться исправлять проблемы позже. Сейчас благоприятное время для изменения бизнес-процессов и технологических цепочек

Александр РУКОСУЕВ,
Минцифры России

Илья МЯЧИН,
ОАЦ при Президенте Республики Беларусь

Совместный стенд компаний «Лаборатория Касперского» и «ДиалогНаука»

Не передавать данные – самый безопасный способ.

Константин Родин

в связи с импортозамещением. Сегодня можно предусмотреть возможные уязвимости и спланировать их устранение с самого начала проектирования. К сожалению, ощущается нехватка дифференцированных методик, и наша методика находится на стадии разработки безопасного конвейера. Отличительная особенность этой методики, которая опубликована на официальном портале Минцифры, – составление списка недопустимых событий. Этот список представляет собой ключевые бизнес-процессы, приостановка или нарушение которых приводит к значительным потерям для предприятия», – пояснил представитель министерства.

Систему правовых средств воздействия на общественные отношения в сфере обеспечения безопасности критически важных объектов информатизации, опыт Республики Беларусь осветил сотрудник Оперативно-аналитического центра при Президенте Республики Беларусь **Илья Мячин**. Согласно концепции национальной безопасности Республики Беларусь, среди основных национальных интересов информационной сферы – надежность и устойчивость функционирования критически важных объектов информатизации. «Главой государства подписан указ о кибербезопасности, который предусматривает создание многоуровневого механизма реагирования, обнаружения и реагирования киберинцидентов. В принципе, у нас все проще с точки зрения территориального устройства», – отметил докладчик.


Сергей БОЧКАРЁВ,
компания «АйТи Бастион»

Все мы знаем великого человека – сотрудника, у которого в руках флешка, переносящая данные из одной сетки в другую.

Сергей Бочкарев

За разумную безопасность

Автоматизации типовых задач объектов АСУ ТП с позиции ИБ посвятили свои выступления генеральный директор компании «АйТи Бастион» **Сергей Бочкарев** и руководитель отдела развития продуктов компании «АйТи Бастион» **Константин Родин**. «Наша компания – за разумную безопасность. Как разработчики мы видим решение в создании универсальных средств защиты, которые позволят выстроить безопасные процессы удобно», – сказал Сергей Бочкарев. На мероприятии представили обновленный продукт «Синоникс» – шлюз безопасного объединения изолированных сетей, который позволяет передавать данные и файлы между ними, сохраняя безопасность каждого из объединяемых сегментов и обеспечивая


Константин РОДИН,
компания «АйТи Бастион»

Про государственную тайну: не будем уголовной ответственностью портить аппетит.

Константин Родин

сокрытие данных об их архитектуре. Устройство, разработанное командой, предназначено в основном для передачи файлов. Однако оно также способно обеспечить передачу данных из изолированного сегмента. Для решения задачи был рассмотрен вариант – передавать данные с использованием межсетевых экранов НГФВ. В этом случае возможно применение диодов, которые специально предназначены для такой цели, что может стать более эффективным и безопасным решением.

Технические характеристики «Синоникса»: производство на базе оборудования отечественного производства, контроль физической блокировки работы устройства двумя «пусковыми» ключами, скорость до 1 Гб/с, оборудование: архитектура x86-64, форм-фактор 1U, ОС AstraLinux 1.7 SE. Ключевые задачи «Синоникса» включают в себя изоляцию сетей на физическом уровне: передачу данных в режиме «точка – точка» как в одну, так и в обе стороны по протоколам TCP и UDP с сохранением «воздушного зазора». Кроме того, валидацию файлов при передаче: встроенный файловый шлюз с проверками маски, размера, ЭЦП объектов и возможностью внешней валидации по ICAP. Разграничение зон ответственности предусматривает разделение интерфейсов управления между ответственными сторонами для подтверждения прохождения данных и игнорирует несогласованные правила с обеих сторон. Физический контроль передачи обеспечивается физической блокировкой передачи «пусковыми» ключами и возможностью запрета удаленного управления, а доступ к конфигурированию осуществляется только через консоль RS-232.

О безопасности распределенной промышленной инфраструктуры, синергии технологий

С 2022 года у нас началась «эра хактивизма».

Андрей Стрелков

Стенд компании Innostage

Андрей СТРЕЛКОВ,
«Лаборатория Касперского»

мониторинга сети и программно-определяемых распределенных сетей рассказал руководитель направления развития продуктов для промышленной безопасности компании «Лаборатория Касперского» **Андрей Стрелков**. По его словам, наступила эпоха хактивизма и целевой киберагрессии. Возросло количество уязвимостей из-за ухода вендоров информационной безопасности, изменения целей киберпреступников и связанных с этим тактик и техник. Началась активная фаза импортонезависимости, когда важность обеспечения безопасности собственной информации становится критической для организаций. «Сложность атак увеличивается. Параллельно расширяется поверхность угроз предприятий в рамках внедрения все большего количества технологий. В ответ на это усиливаются требования предприятий, особенно в отношении объектов критической информационной инфраструктуры», – подчеркнул эксперт.

Построение и эксплуатация киберустойчивых АСУ ТП в современных реалиях – тема выступления заместителя руководителя отдела кибербезопасности АСУ ТП компании Innostage **Айрата Мухаметшина**. Он отметил успешную разработку базовой методики и kill-chain

Айрат МУХАМЕТШИН,
компания Innostage

Марина СОРОКИНА,
компания «ИнфоТеКС»

Алексей ШАНИН,
компания UDV Group

цепочек, а также доработку методик АР в соответствии с аудитом ISO 27005. Активно внедряется процесс автоматизации разработки отчетной документации, планируется предоставление услуги оценки рисков в формате онлайн-сервиса по информационной безопасности. Докладчик выделил развитость управляющих функций АСУ ТП, отметив их ключевую роль в управлении производственными объектами, подчеркнул важность киберзащищенности и необходимость обеспечения устойчивости к кибератакам для сохранения функционала систем. Не менее значимый фактор – совместимость программно-технических комплексов и средств защиты, необходимая для корректного выполнения функций управления технологическими объектами в условиях кибератак.

Руководитель продуктового направления компании «ИнфоТеКС» **Марина Сорокина** посвятила выступление новому национальному стандарту – криптографическому протоколу CRISP, который предназначен для защиты данных в АСУ ТП / АСУ ОКИИ, IIoT-системах, M2M системах, ИСУЭ.

Эксперт описала, какие свойства безопасности обеспечивает протокол. В частности, отметила обеспечение целостности передаваемых данных и конфиденциальности (опционально), аутентификацию с применением общего секретного ключа и защиту от повторного использования сообщений благодаря окну принятых сообщений.

Обзор рынка защиты АСУ ТП представил директор по продуктам компании UDV Group **Алексей Шанин**. Уровень информационной безопасности предприятий различается. В топ-3 самых используемых классов решений входят защита конечных точек, промышленные СОВ и управление уязвимостями. Особое внимание уделяется документированию процесса реагирования на инциденты в большинстве организаций. Сотрудничество служб информационной безопасности и эксплуатации позволяет эффективно решать задачи по обеспечению ИБ АСУ ТП.

Я та «муза с палкой», которая сказала, что отрасли нужен новый криптографический протокол.

Марина Сорокина

Стенд компании «ИнфоТеКС»

Вячеслав ПОЛОВИНКО,
компания «АМТ-ГРУП»

Алексей ЕНЮТИН,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Алексей ПЕТУХОВ,
компании InfoWatch ARMA

Совершенно биполярная история с АСУ ТП и внешним миром.

Вячеслав Половинко

На комплексных применениях решений InfoDiode остановился руководитель направления собственных продуктов компании «АМТ-ГРУП» **Вячеслав Половинко**. Решения InfoDiode служат интеграционным элементом в ИТ- и ИБ-инфраструктуре промышленного объекта. Применение средств защиты информации на объектах АСУ ТП характеризуется тем, что СЗИ не просто служит обеспечению защиты, а является интеграционным инструментом, объединяющим системы и данные на уровне приложений. Для многих предприятий выполнение требований Указа Президента № 166 критически важно и не ограничивается закупкой средств защиты. Требуются гибкие решения, сроки исполнения которых приближаются. Процессы пуско-наладки и установки СЗИ не должны прерывать работу объекта. При наличии усиленной защиты или изоляции объекта возникают новые вопросы по обновлению ПО и мониторинга, особенно выполняемых централизованно и мультивендорно.

Мониторинг и оптимизация

Продолжением пленарного заседания стала сессия «Методы, технологии и инструменты защиты АСУ ТП. Взгляд ИБ-компаний». Выступающие представили решения по повышению качества работы структурных подразделений в промышленности, в частности, за счет улучшения работы систем по информационный безопасности.

Начальник отдела ФАУ «ГНИИИ ПТЗИ ФСТЭК России» **Алексей Енютин** рассказал об исследовательском стенде, на базе которого ведутся доработки и ставится оценка защищенности АСУ ТП, а также об интернет-портале БДУ АСУ ТП с набором данных для построения систем защиты. Готовое решение способно выполнять множество поставленных задач: предоставлять инфраструктуры для компонентов АСУ ТП, настраивать взаимодействие реальных компонентов АСУ ТП с виртуальными, можно получить ссылку на исследования и т. д. Доступ

Стенд UDV Group

Михаил ЦЕЛИЩЕВ,
компания SoftMall

предоставляется для сторонних исследователей, где данные передаются по защищенным каналам. Вендор может подключить свое оборудование для ликвидации возникших проблем, выявить уязвимости, посмотреть, насколько решения защищены. Существует несколько режимов работы с сайтом. Исследователь регистрируется, получает соответствующий статус, после этого на сайте появляются компоненты, с которыми исследователь работает. Второй вариант – работа с имеющейся на сайте информацией.

Решение предусматривает систему обучения и тестирования, т. е. проверку знаний специалиста. Сотрудник самостоятельно проводит анализ защищенности своих решений и программ. В скором временем программа тестирования будет дополняться другими тестами в сфере категорирования объектов КИИ, создания систем обеспечения безопасности и т. д. Проект создан с целью бесплатного анализа угроз внутри компании.

Исследовательский стенд включает в себя мониторинг действий пользователей, моделирование атак, для исследования предоставляется доступ к реальному ПО и т. д. Сведения о нарушениях работы систем доступны только вендору, который зарегистрировался на сайте, эти данные хранятся в защищенных каналах. На сайте размещены информация о выгрузке сведений из БДУ, инфографика, личный кабинет, рейтинг исследователей, новости, тестирование и т. д. Доступ к исследованиям открывается после прохождения теста. Вендоры пользуются сведениями о возможных уязвимостях, исследователи повышают квалификацию. Проект был разработан при поддержке ФСТЭК, «Ростелекома» и Telecom Integration.

О мерах по совершенствованию ИБ шла речь в выступлении руководителя отдела развития компании InfoWatch ARMA **Алексея Петухова**. По его словам, «КВН уже не тот, мир не тот, все не то». В 2023 г. компания Take Networks провела исследование в четырех странах: Германии, Японии, США и ОАЭ. Выяснилось, что 76% из 400 компаний интегрируют информационные и операционные технологии в единую сеть. 97% опрошенных сообщили, что атаки на ИТ-инфраструктуру затронули ОТ, где 47% атак оказались «вымогателями», которые могли способствовать остановке производства. В качестве примера эксперт рассказал об атаке на металлургическую компанию «Норд-Сидра». Вирус-«вымогатель» привел к большим потерям: прямые потери оценены в 14 млн долл., а прогноз снижения годовой прибыли – 10–15%. Чтобы обеспечить безопасность предприятия, эксперт рекомендует для начала «пользоваться тем, что есть»: российскими разработками. ИБ должна соответствовать требованиям регуляторов (ФСТЭК, ФСБ, Минцифры, Минпрома), а также обеспечивать устойчивость производства к внешним воздействиям в сферах ИТ и АСУ.

Вопросы обеспечения устойчивости систем выходят за рамки ИБ.

Айрат Мухаметшин

Не каждый руководитель дошел до мысли, что вопросы, связанные с ИБ, это очень важно.

Илья Мячин

Стенд компании АМТ-ГРУП

Стенд компнаии «КСБ-СОФТ»

В настоящее время во всех четырнадцати сферах перечни ФСТЭК России согласованы.

Павел Зенкин

Руководитель направления комплексных проектов в сегменте АСУ ТП компании SoftMall **Михаил Целищев** поделился идеями о совершенствовании функционирования системы. Перед началом работы с новым проектом необходимо предварительно запустить пилотную версию.

На секции шла речь об этапах построения рабочей системы: нужно научиться эффективно управлять организационными мерами и процессами, должна быть установлена эшелонированная система предприятия, обеспечена автоматизация управления и реагирования, выполнены требования ФСТЭК. Если все условия будут соблюдены, то процент киберугроз значительно уменьшится внутри предприятия. При этом стоит учитывать и другие факторы, которые оказывают значительное влияние на работу информационной безопасности.

Руководитель практики промышленной кибербезопасности компании Positive Technologies **Дмитрий Даренский** рассказал об основных трудностях, связанных с ИТ-инфраструктурой предприятий. Особое внимание уделил проблемам прикладного характера: неавтоматизированные каналы связи, незащищенные точки доступа, отсутствие сегментации сети, «паразитный» трафик и т. д. Эксперт привел примеры, описывающие, как нарушения информационной безопасности системы прикладного характера привели к масштабным проблемам. В частности, на нефтебазе, где произошел слив хранилища и вывоз десятка автовозов с нефтепродуктами (сокрытие следов в SCADA), в центре переработки ТБО (незаконный ввоз и разгрузка ТБО на территории центра). В данном случае не было возможности отследить доступ к системе СКУД, который был у водителей (разгрузка в обход системы контроля).

В рамках промышленной экспертизы компания Positive Technologies составляет базу знаний об устройстве системы промышленной автоматизации различных платформ и вендоров, разрабатывает скрипты сканирования, проводит аудиты, создает среды для обнаружения вредоносного ПО и попыток эксплуатации «нулевого дня». Кроме того, Positive Technologies разрабатывает кросспродуктовые пакеты экспертизы для поддержки отдельных вендорских платформ автоматизации.

Заместитель генерального директора КСБ-СОФТ **Михаил Шипицын** выделил ключевые принципы информационной работы в АСУ ТП: должна быть экспертиза, стоит попробовать пилотную версию решения, которое планируется внедрять, должно исключаться управляющее воздействие и т. д. Решение Socrat, созданное для мониторинга информационной безопасности предприятия, обеспечивает выявление событий и инцидентов, предотвращает инциденты, осуществляет взаимодействие с «ГосСопка», повышает уровень защищенности инфраструктуры и т. д.

Руководитель группы внедрения и поддержки специального ПО УЦСБ **Александр Мерзляков** заострил внимание на типичных проблемах в обеспечении ИБ АСУ ТП, предпосылках внедрения СОИБ (системы обеспечения информационной безопасности), отметил ее преимущества и особенности внедрения. Центр кибербезопасности является российским дистрибьютором передовых практик и технологий


Дмитрий ДАРЕНСКИЙ,
компания Positive Technologies

Стенд компании «Газинформсервис»

Вопрос разметки местности – что происходит и куда все это катится – становится вопросом выживания.

Алексей Шанин

для защиты критически важных систем от цифровых атак. Наиболее частые проблемы, с которыми сталкиваются предприятия в сфере информационной безопасности: устаревшее ПО, слабое аппаратное обеспечение, отсутствие технических условий. Эти проблемы могут стать предпосылками для внедрения системы СОИБ. Предложение СОИБ включает в себя антивирусную защиту, систему обнаружения вторжений, обнаружения и анализ уязвимостей, контроль целостности и т. д.

О том, как обеспечить стабильную и безотказную работу систем, рассказал руководитель направления безопасности КИИ и АСУ ТП компании К2Тех **Егор Куликов**. В проектах при работе с АСУ ТП чаще всего используются такие механизмы, как встроенные механизмы безопасности, межсетевые экраны, СКЗИ, антивирусная защита и т. п. Нередко у заказчиков слабые АРМ и серверы, и при подключении новых средств защиты происходит перегрузка системы, отмечается снижение производительности. Компании удалось справиться с этим вызовом. Эксперт дал несколько рекомендаций по устранению проблем совместимости устройств: предварительное тестирование для систем, с которыми отсутствует подтверждение совместимости с СЗИ, замена или апгрейд устаревшего оборудования, гибкая настройка средств защиты (необходимо оставить только базовые защитные функции).

Первый день работы конференции завершился панельной дискуссией на тему «Практические аспекты защиты АСУ ТП: разбираем реальные ситуации и даем практические рекомендации», которую провел заместитель технического директора по ИБ ООО НВФ «Сенсоры, Модули, Системы» **Дмитрий Пономарев**. На вопросы отвечали семь спикеров. В ходе бурной дискуссии каждый из выступающих поделился личным опытом, представил свою точку зрения и дал рекомендации. Ведущему удалось задать оптимальный вектор общения: аудитория


Михаил ШИПИЦЫН,
компания «КСБ-СОФТ»


Александр МЕРЗЛЯКОВ,
компания «УЦСБ»


Егор КУЛИКОВ,
компания К2Тех

Не все происходящее на производстве можно описывать языками программирования.

Сергей Васильев

получила ответы на актуальные вопросы, прозвучало много дельных рекомендаций и советов по ведению ИБ на предприятиях.

В рамках конференции компания «АйТи Бастион» вместе с предприятиями-заказчиками провела круглый стол на тему «Технологии объединения изолированных сетей: от «воздушного зазора» к цифровизации предприятий». В ходе обсуждения эксперты отметили актуальность обеспечения безопасности ИТ-инфраструктур и процессов, чтобы избежать утечки данных.

От проектирования до эксплуатации

Во второй день работы конференции «Информационная безопасность АСУ ТП КВО» состоялась сессия «Методы, технологии и инструменты создания безопасных АСУ ТП. Практический опыт формирования системы ИБ АСУ ТП». Представленные на заседании доклады носили преимущественно практический характер и охватывали различные направления проектирования и обеспечения информационной безопасности АСУ ТП КВО: компонентную базу, ПО, вопросы организации защиты систем, средства тестирования и методические подходы к обеспечению безопасности. Несколько выступлений были посвящены взаимосвязи элементов функциональной и информационной безопасности.

Главный менеджер отдела информационной безопасности АСУ ТП управления информационной безопасности, ООО ИК «СИБИНТЕК» («Роснефть») **Михаил Богатырёв** поделился опытом внедрения организационных мер обеспечения безопасности объектов КИИ и АСУ ТП. По его словам, все технические меры имеют организационную составляющую: администрирование и мониторинг неисправностей, контроль работы, устранение возникающих проблем. Правила или регламент должны предусматривать распределение ролей, перечень процедур и порядок выполнения, контроля и устранения проблем. Например, за исполнение отвечает инженер АСУ ТП, контролирует работник отдела ИБ, принимает решения и устраняет проблемы руководитель ИБ.

Александра ГОНЧАРОВА,
компании «АйТи Бастион»

Сергей ВАСИЛЬЕВ,
ПАО «Газпром нефть»

Использованию комплекса СКДПУ НТ в ИБ-инфраструктуре сегмента АСУ ТП посвятила свое выступление инженер поддержки продаж/пресейл компании «АйТи Бастион» **Александра Гончарова**. Одна из тенденций в поведении киберпреступников состоит в том, что злоумышленник может находиться в инфраструктуре долгое время, изучая уязвимые точки и планируя атаку с наибольшим ущербом. Комплекс СКДПУ НТ относится к классу решений, позволяющих ограничивать, отслеживать,

Стенд компании УЦСБ

Сергей ЗЫЛЬ,
«СВД ВС»

Сергей ЛУПАНОВ,
компания «Информзащита»

обнаруживать, предотвращать и расследовать несанкционированный привилегированный доступ к критически важным ресурсам. В частности, при помощи комплекса можно идентифицировать время изменения скорости оборудования и соотнести с сессиями в этот период.

Руководитель практики автоматизации ПАО «Газпром нефть» **Сергей Васильев** представил решения с открытой архитектурой для построения систем промышленной автоматизации нового поколения. Актуальность открытой АСУ ТП рассматривается в контексте перехода от автоматизации производства к построению киберфизических систем: этого требуют вызовы «Индустрии 4.0». Смена технологической парадигмы необратима. Архитектура перспективных АСУ ТП должна поддерживать работу в гетерогенных сетях. Создание полностью вендоронезависимой кросс-отраслевой российской платформы автоматизации, обеспечивающей переход к открытой архитектуре для перспективных промышленных систем управления, эксперты оценивают как стратегическую возможность. Рабочая группа «Открытая АСУ ТП» (в рамках приказа Минпромторга РФ № 2939 от 14.08.2023) ведет деятельность по нескольким направлениям (стандарты, универсальная среда разработки, промышленный протокол передачи данных и т. д.). При этом реализуется композитный архитектурный подход к построению систем на основе совместимости. Планируется, что открытые стандартные протоколы будут доступны на рынке для вендоров, проектировщиков, заказчиков, контролирующих органов. Это один из принципов построения доверенной среды. Создана также подгруппа по развитию компетенций и образования в области АСУТП. По словам докладчика, для стабилизации и удешевления создаваемых технологий, формирования их облика необходимо, чтобы в проект были вовлечены все заинтересованные участники рынка.

Мы как представители самого низкого уровня промышленных систем, горшки обжигаем, поэтому и проблемы приземленные.

Сергей Зыль

Стенд компании InfoWatch

О важности развития в организациях культуры безопасности говорил на секции заместитель генерального директора по научной работе ООО «СВД ВС» **Сергей Зыль**. В своем докладе он проанализировал подходы и инструменты поддержки безопасной разработки ПО реального времени для критически важных объектов. В частности, шла речь об инструментах двух типов: для статического анализа – без выполнения программы и динамического, когда требуется выполнение кода. Статические анализаторы способны обнаружить ошибки программирования на ранних этапах разработки ПО, например, переполнение буфера, выход за границы, ошибки

ИБ-специалист нужен не для эксплуатации средств защиты, а чаще всего – для контроля.

Михаил Богатырев

доступа к памяти, недостижимый код, утечку информации через сообщения об ошибках. Динамический анализ требует применения нескольких инструментов, таких как трассировка потоков данных, модульные, нагрузочные, тесты СЗИ, пентесты. Для систем реального времени готовых универсальных российских инструментов нет. Ситуация с инструментарием для статического анализа в нашей стране улучшилась.

Защита от угроз, обеспечение безопасности – это не фиксация факта ущерба, а работа на опережение и автоматизация реагирования, отметил начальник отдела проектирования Центра промышленной безопасности компании «Информзащита» **Сергей Лупанов** в докладе «Автоматизированное реагирование при защите критических объектов».

К актуальным киберугрозам для предприятий относятся компрометация учетных записей, проникновение, остановка производственных процессов, деструктивная деятельность с непредсказуемыми последствиями. Для остановки производственных процессов иногда достаточно нарушения работоспособности одной АСУ ТП из технологической цепочки. После ухода зарубежных вендоров предприятия выбирают новых производителей технологических линий, SCADA-систем (российских, китайских). По аналогии с предыдущими решениями западных вендоров возникает необходимость тестирования на совместимость со средствами защиты информации, разбора методик, получения знаний о возможностях администрирования устройств и систем. Особенно много вопросов возникает в связи со строительством новых объектов капитального строительства, закупки оборудования. Расширение взаимосвязей систем, СЗИ и обработка больших массивов данных сетей АСУ ТП заставили системных интеграторов и вендоров больше внимания уделять производительности. Работа с комплексом сложных систем по безопасности не подразумевает ручного управления с учетом ограничений по количеству

Александр КАПУСТИН,
АО «СО ЕЭС»

Дмитрий ПРАВИКОВ,
«Энерго ЦИБ»

Александр МАЗУРКЕВИЧ,
РУП «Гродноэнерго»

персонала. Автоматизированное реагирование – это уже не рекомендации, а требование сегодняшнего дня.

Теме консолидации усилий компаний электроэнергетики для совместного противодействия компьютерным атакам посвятил свой доклад заместитель начальника службы информационной безопасности АО «СО ЕЭС» **Александр Капустин**. Актуальность создания отраслевых центров кибербезопасности продиктована тем, что информационная безопасность в настоящее время имеет ярко выраженную отраслевую специфику. Экспертиза по отраслевой специфике обеспечения информационной безопасности сосредоточена в отраслевых центрах. Требует проработки нормативная процедура формирования таких центров. Содокладчик **Дмитрий Правиков** рассказал о направлениях деятельности «Энерго ЦИБ» – центра экспертизы (обмена и анализа информации) по вопросам информационной безопасности в электроэнергетике. К ним относятся выстраивание партнерской сети и подготовка платформы для реализации задач, обеспечение «профилирования» компаний электроэнергетики по результатам обмена информацией по соглашениям, формирование каталога услуг «Энерго ЦИБ».

Денис БАБАЕВ,
Kaspersky ICS CERT

В частности, в текущем году планируется реализовать проект «Паспортизация процессов разработки и обеспечения качества программного обеспечения».

Варианты применения решений InfoDiode в ТЭК и энергетике представил на сессии руководитель направления собственных продуктов компании АМТ-ГРУП **Вячеслав Половинко**. Компания предлагает полную линейку решений класса «диод» для защиты КИИ, ОПО, АСУ ТП, а также ИТ-инфраструктуры. Эксперт рассказал, как подбирать устройства однонаправленной передачи данных InfoDiode, как проводить их пусконаладку. Отмечалось, что остановка объекта при этом не требуется. Объект либо не сопрягается с менее доверенным сегментом, либо выполняется параллельный запуск с последующей заменой имеющихся средств изоляции сети на InfoDiode. Внедрение InfoDiode и коннекторов не затрагивает исходную АСУ ТП-систему. Подключение происходит параллельно текущему функционированию. Для масштабирования или разделения системы нужно установить дополнительное устройство. Ограничения, как правило, срабатывают не на InfoDiode, а на коннекторах. У InfoDiode большой запас производительности. Устройство включено в реестры, завершена его сертификация.

Надежда на то, что созданию систем ИБ будет предшествовать анализ, а не аварийный опыт эксплуатации.

Денис Бабаев

Организационно-техническим мероприятиям по обеспечению кибербезопасности в РУП «Гродноэнерго» посвятил свой доклад директор филиала ПСДТУ РУП «Гродноэнерго» **Александр Мазуркевич**. Параллельно с созданием СЗИ корпоративного сегмента обеспечивается защита информации в АСУ ТП. Реализация стратегии эшелонированной защиты АСУ ТП предполагает выполнение следующих шагов: подготовка специалистов АСУ ТП на соответствующих курсах – первый этап по обеспечению ИБ в АСУ ТП; инвентаризация активов в технологической сети – определяется перечень всех объектов АСУ ТП, составляется схема сетевых взаимодействий, проверяется конфигурация оборудования,

Запретили в шахту проносить смартфоны, даже увольнением наказываем, но люди не успокаиваются.

Сергей Куликов

оцениваются потенциальные уязвимости. В рамках мониторинга технологической сети выявляются признаки компьютерных атак и сетевых аномалий, что не мешает технологическому процессу. Комплексная защита конечных узлов АСУ ТП предусматривает, что средства защиты не должны оказывать влияние на функции по управлению технологическим процессом и вызывать задержки в работе АСУ ТП. Сбор и анализ событий информационной безопасности в автоматизированном режиме позволяют сократить время реагирования.

Старший аналитик группы аналитики безопасности Kaspersky ICS CERT **Денис Бабаев** выступил с докладом «Предварительная оценка стоимости системы обеспечения ИБ-инфраструктуры АСУ ТП сложного технического комплекса на примере АЭС». Эксперт отметил структурную сложность объекта: более 30 подсистем АСУ ТП, свыше 15 тыс. датчиков, 4 тыс. исполнительных механизмов, 230 регуляторов, 150 тыс. сигналов. Впечатлил аудиторию и прайслист ущерба. В 1,2 млн долл. оценивается один день простоя энергоблока АЭС-2006. Архитектура безопасности включает в себя эшелонированную защиту, сегментирование и управление потоками. Экономия ресурсов достигается за счет формирования зон ИБ – распределения ограниченных сил и средств для защиты объекта. Проектный путь – проблема для многих сложных систем. Эксперты рекомендуют, в частности, создавать систему на унифицированных решениях, а не проектно-сметную документацию. Система управления ИБ должна быть интегрирована в систему менеджмента качества. Что касается стоимости системы, то за безопасность надо платить, поскольку за ее отсутствие приходится расплачиваться.

О борьбе с внутренним нарушителем, поиске невзрывозащищенных устройств на угольных предприятиях в сегменте АСУ ТП шла речь в докладе заместителя начальника отдела ССПБ ООО «Распадская угольная компания» **Сергея Куликова**. В семи шахтах компании оборудована обширная сеть Wi-Fi на глубине 300, 800 м. Процессы

Сергей КУЛИКОВ,
«Распадская угольная компания»

выстроены так, что сотрудники (рабочие, ИТР) имеют взрывозащищенные смартфоны для выполнения своих обязанностей (например, фиксируют факт неисправности и передают на-гора). В прошлом году был внедрен RADIUS (Remote Authentication Dial In User Service) на границе наземной и подземной корпоративных сетей, чтобы устройства в невзрывозащищенном исполнении не могли получить доступ к интернету. Сервер RADIUS обеспечивает централизованное управление аутентификацией и авторизацией устройств, которые пытаются подключиться к сети и воспользоваться услугами. В ходе проведения выборочных проверок были выявлены случаи подключения к подземным точкам Wi-Fi мобильных устройств невзрывозащищенного исполнения. Для ограничения доступа подземных устройств был изменен процесс контроля их доступа к корпоративной сети. На телефоны установили соответствующий режим, позволяющий выполнять ограниченный набор функций. Web-интерфейс приложения дает возможность обнаружить нелегитимные устройства в режиме онлайн, устанавливать необходимые фильтры для более точного поиска, оперативно реагировать на появление устройств в шахте.

Стенд компании K2Tex

Юрий ОСЕТРОВ,
АО «Пигмент»

Дмитрий АВРАМЕНКО,
компания Innostage

Роман ЯКУШЕВ,
ФГУП «ЗащитаИнфоТранс»

Есть возможность просмотра и анализа истории подключений, поиска закономерностей для идентификации конечного пользователя. Внедрение proxy-сервера позволило ограничить доступ к нецелевому, развлекательному контенту. Комплекс мероприятий по минимизации рисков ИБ и промышленной безопасности в корпоративном сегменте подземной сети с некритичными устройствами АСУ ТП показывает положительную динамику и значительно сокращает возможность деструктивного воздействия внутреннего нарушителя.

Начальник отдела АСУ ТП АО «Пигмент» **Юрий Осетров** рассказал о переходе АСУ ТП на оборудование, входящее в состав реестра российской промышленной продукции. «Пигмент» – российский производитель химической продукции, известной на рынке под торговым знаком «Крата». Программное обеспечение для ПЛК и мнемосхем разрабатывается на языках программирования стандарта МЭК 61131-3, используются и классические языки программирования. По словам докладчика, стандарты МЭК – отличное решение, но на практике не универсальное. Специалисты компании столкнулись с тем, что библиотеки есть не под все протоколы связи, не хватает скорости обработки данных. В ходе поиска решения под корпоративные задачи компания перевела разработку на язык C++. Разрабатываемое ПО продуктивно используется. В настоящее время для предприятия актуальны задачи замены контроллеров (для некоторых из них аналогов в реестре пока не найдено), а также ОС Windows на Linux.

Модернизацию объекта КИИ завершили, а потом вспомнили, что где-то должна быть безопасность.

Дмитрий Авраменко

Стенд компании SoftMall

Приоритеты и заблуждения

Опытом обеспечения безопасности АСУ ТП в современных условиях поделился руководитель отдела кибербезопасности АСУ ТП компании Innostage **Дмитрий Авраменко**. Вопросы оптимизации затрат на ИБ эксперт раскрыл в формате

Стенд компании «СВД ВС»

Нельзя защитить процесс, не зная его физики.

Борис Безродный

Если проводить аналогию с организмом человека, то АСУ ТП – это нервная система.

Денис Бабаев

«вредных советов». Об уровне защиты российских предприятий можно судить по тому, что половина из них признают, что кибератака с большой вероятностью будет успешной, столько же подтверждают, что риск несет с собой критические последствия. Лишь 10% респондентов уверены, что смогут противостоять целевой атаке. Источниками угроз являются террористы, криминал, конкуренты, кибервойска, а также подрядчики и персонал, имеющие полный доступ к АСУ ТП, в том числе удаленный, и мотивированные к мошенничеству и саботажу. Что касается экономии на ИБ, то многие организации предпочитают делать все сами, не погружаться в детали, снижать категорию. Для этого они проводят «деление» на подсистемы, не рассматривают «маловероятные» сценарии, рассчитывают, что все «легко» может перейти на ручное управление. Но на практике дает о себе знать «размытость» границ объектов КИИ, а ОКИИ разделяется только «на бумаге». Эксперт привел примеры реальных объектов, где перестарались с их дроблением. Разумный совет применительно к экономии на ИБ состоит в том, что обеспечение безопасности должно выполняться на всех этапах жизненного цикла. Объект КИИ должен запускаться в эксплуатацию совместно с системой защиты. Грамотное обеспечение ИБ предприятия требует реализации единого подхода к решению этой задачи.

Представитель ФГУП «ЗащитаИнфоТранс» **Роман Якушев** посвятил свой доклад отраслевому центру компетенций по информационной безопасности транспортной отрасли как совокупности ресурсов (организационных, технических, технологических, кадровых), механизмов,

Андрей ИВАНОВ,
компания «ИнфоТеКС»

Сергей САВЧЕНКО,
«Воздушные Ворота Северной Столицы»

Артём МИНАКОВ,
ЗАО «НОРСИ-ТРАНС»

методов, направленных на координацию и обеспечение ИБ с учетом отраслевой специфики, на базе соответствующей оргструктуры. Эксперт отметил ряд преимуществ реализации такого подхода: понимание особенностей информационной инфраструктуры отрасли и повышение эффективности при оказании помощи при обнаружении и реагировании на атаки, взаимодействие с НКЦКИ, учет специфики отрасли при формировании нормативных актов, рекомендаций и методических материалов. Такой центр выступает в качестве доверенной площадки для обмена компетенциями, экспертизой в рамках отрасли.

О вариантах и устройствах защиты каналов, периметра, сегментов шла речь в выступлении архитектора решений компании «ИнфоТеКС» **Андрея Иванова**. Основное внимание было уделено одному из решений вендора – линейке ViPNet Coordinator IG, которая разрабатывалась специально для применения в системах АСУ ТП. С помощью этого программно-аппаратного комплекса можно обеспечить защиту канала передачи данных, периметра систем и сегмента. В докладе были представлены различные сценарии реализации такого решения.

На трудностях импортозамещения в сетях АСУ ТП заострил внимание аудитории начальник отдела информационной безопасности ООО «Воздушные Ворота Северной Столицы» **Сергей Савченко**. К основным системам АСУ ТП транспортной отрасли относятся система сортировки и обработки багажа, системы светосигнального оборудования, досмотра багажа. Среди актуальных проблем эксперт назвал уход ключевых иностранных игроков с российского рынка ИБ, появление аналогов российского производства на импортной элементной базе, недостаточную зрелость продуктов российского производства, риски наличия «закладок» в имеющихся импортных решениях, значительное увеличение стоимости продуктов иностранного производства, поставляемых по модели «параллельного» импорта. Снижение конкуренции приводит к увеличению стоимости и падению качества разрабатываемых систем ИБ и их поддержки. Санкции повлияли на рынок СЗИ в значительной мере вследствие неготовности российских производителей одномоментно заменить ушедшие с рынка решения. Остро ощущается нехватка квалифицированных специалистов, имеющих опыт и компетенции в управлении системами, вышедшими на российский рынок ИБ. С учетом перечисленных обстоятельств в обозримом будущем направление информационной безопасности является достаточно перспективным и имеет большой запас для развития.

Защита от угроз, обеспечение безопасности – это не фиксация факта ущерба, а работа на опережение.

Сергей Лупанов

В поисках баланса

Современные подходы к автоматизации поиска в открытых источниках представил начальник отдела информационной безопасности ЗАО «НОРСИ-ТРАНС» **Артём Минаков**. На конкретных примерах он показал, насколько уязвимы организации и их сотрудники благодаря технологии разведки в открытых сетях OSINT (Open Source Intelligence) – сбору данных по открытым источникам. Ранее OSINT использовали только разведывательные службы, а теперь и киберпреступники. Эксперт рассказал о продуктах компании.

Фёдор МАСЛОВ,
компания UDV

Масса продуктов на российском рынке нам импонирует – это не гвоздями прибитые решения.

Роман Якушев

Артём КРАСАВИН,
компания «АйЭсТи»

Наталья ХМЕЛЕВСКАЯ,
ОАО «РЖД»

«Виток-OSINT» – это стек технологий для формирования запросов в открытые источники и приложение для поиска и анализа данных. «Виток-Портрет» – веб-приложение для поиска информации в открытых источниках. Поиск выполняется на стеке технологий «Виток-OSINT». «Виток-М» – информационно-аналитический веб-сервис мониторинга СМИ и блогосферы. Поиск также осуществляется на стеке технологий «Виток-OSINT». Взаимодействие с источниками осуществляется таким образом, что пользователю не приходится задумываться над решением инфраструктурных вопросов, связанных с аккаунтами, прокси-серверами, API-токенами, очередью задач. Разведка в открытых сетях ведется по сути «из коробки». Единое досье формируется согласно общей онтологии данных и информации, полученной из разных источников Досье разбивается на структурированные блоки, которые содержат разную информацию – контакты, интернет-активность, сфера профессионального и личного интереса и пр. Докладчик привел пример работы поисковой методики с использованием ИИ.

«Контроль версий проектов программируемых логических контроллеров (ПЛК) в период импортозамещения» – тема выступления менеджера продукта компании UDV **Фёдора Маслова**. На базе экосистемы решений UDV Group обеспечиваются защита АСУ ТП и объектов КИИ, мониторинг информационной безопасности и реагирование на инциденты, автоматизация бизнес-процессов. В рамках развития платформы кибербезопасности для промышленного контура компания расширяет возможности решения DATAPK Industrial Kit. Заказчикам доступен глубокий анализ сетевых пакетов (DPI) с элементами машинного обучения, а также контроль версий проектов ПЛК. Среди особенностей проектов по импортозамещению эксперт отметил трудности с техническими характеристиками ПЛК, высокую цену ошибки при проектировании и внедрении, эксплуатацию ПЛК от разных производителей. Изменения в проектах контроллеров неизбежны, при этом отсутствует возможность централизованного управления версиями проектов ПЛК. Новое решение UDV – DATAPK Version Control – обеспечит совместную работу над исходным кодом, контроль и отслеживание изменений, резервное копирование и восстановление исходного кода, отчеты и уведомления, аудит изменений.

К вопросам кибербезопасности АСУ ТП через призму разумного баланса между организационными и техническими мерами защиты рекомендует подходить ведущий пресейл-инженер решений информационной безопасности

Стенд ккомпании «АйЭсТи»

Мы немножко предельные ребята.

Вячеслав Половинко

компании «АйЭсТи» **Артём Красавин**. По его словам, кибербезопасность АСУ ТП отличается от классической информационной безопасности, и вопрос ее обеспечения сегодня весьма актуален. Для предприятий важно с помощью экспертов определить критические бизнес-процессы, а также возможные события, наступление которых приведет к разрушительным или фатальным для организации последствиям. Специалисты компании выявят информационные системы и элементы телекоммуникационной инфраструктуры, которые связаны с данными бизнес-процессами или событиями, определят уязвимости, спроектируют и внедрят систему кибербезопасности, нацеленную на исключение возможности наступления недопустимых событий. Докладчик заострил внимание на нескольких заблуждениях, которые продолжают культивироваться в профессиональной среде. В частности, АСУ ТП полностью изолированы от внешнего мира, «нас никто не пытается взломать», АСУ ТП надежно защищены разработчиком. В докладе были проанализированы типовые недостатки АСУ ТП, названы векторы проникновения в нынешних условиях.

Влияние компьютерных атак на безопасность систем управления движением поездов (СУДП) проанализировали в докладе начальник отдела обеспечения безопасности значимых объектов КИИ ОАО «РЖД» **Наталья Хмелевская** и заместитель начальника Центра – начальник отдела АО «НИИАС» **Борис Бездродный**. Эксперты представили диаграмму различных состояний систем управления движением

Борис БЕЗРОДНЫЙ,
АО «НИИАС»

Сергей ПАНАСЕНКО,
компания «Актив»

поездов – от исправного до опасного отказа системы. Согласно ГОСТ Р 53431-2009 безопасность СУДП – это свойство непрерывно сохранять работоспособное или защищенное состояние в течение установленного времени либо наработки на отказ. Применительно к обеспечению функциональной безопасности докладчики обрисовали опасные и защитные отказы технических средств. Характеризуя отличие кибератаки от информационной атаки, они отметили их причины, средства и цели, которые в конечном итоге приводят к инцидентам. На примере модели АСУ ТП эксперты обрисовали характер потерь и ущербов от них. Докладчики рассказали, как удалось наладить взаимодействие специалистов, отвечающих за ИБ и за функционирование АСУ ТП.

Директор по научной работе компании «Актив» **Сергей Панасенко** рассказал о применении протоколов строгой аутентификации на основе неизвлекаемых ключей для разграничения доступа к ресурсам информационных систем. Разграничение доступа пользователей к ресурсам ИС – одна из основных мер защиты от различного рода деструктивных воздействий информации, обрабатываемой в ИС, и системы в целом. Пользователи авторизуются на доступ к ресурсам

Самое главное, что специалист по ИБ в РЖД – это уже не слон в посудной лавке, а подкованный наблюдатель.

Борис Безродный

ИС в соответствии с правилами разграничения доступа, по результатам прохождения идентификации и аутентификации. Актуальным вопросом остается аутентификация на основе уязвимых средств и методов. Кража и подделка аутентификационных данных приводят к получению несанкционированного доступа к ресурсам защищаемой системы. Защитить процесс и результаты аутентификации даже от нарушителя очень высокого уровня позволяет строгая аутентификация на основе стандартизованных и доказуемо стойких криптографических протоколов, с помощью сертифицированных аппаратных средств (смарт-карт, криптографических токенов). Один из возможных вариантов – взаимная аутентификация, когда можно получить общий ключ, который впоследствии может быть использован для защиты канала связи. Ключи

Некоторые перестарались с дроблением объектов КИИ.

Дмитрий Авраменко

не покидают носитель в процессе аутентификации (неизвлекаемые ключи). Эксперт представил «Рутокен KeyBox» – средство администрирования и управления жизненным циклом ключевых (аутентифицирующих) носителей (от постановки на учет и ввода в эксплуатацию до вывода из эксплуатации и списания). В компании считают, что разработчики ИС и СЗИ должны применять строгую аутентификацию в своих решениях, а заказчики – требовать наличия средств строгой аутентификации и внедрять их в составе используемых систем.

Компании-разработчики рассказали на сессии о своих достижениях, возможностях и преимуществах предлагаемых продуктов и решений. Ряд экспертов поделились прогнозами относительно угроз информационной безопасности с учетом развития технологий, проанализировали уровень готовности к новым вызовам в данной сфере.

Продолжение следует

По просьбе организаторов конференции участники сессии предложили темы, которые стоит включить в программу мероприятия в следующем году. В частности, представляют интерес выступления компаний-вендоров и интеграторов, занятых разработкой программно-аппаратных комплексов и реализацией проектов в сфере АСУ ТП. Среди вопросов, заслуживающих более широкого обсуждения, – виртуализация в АСУ ТП и инструменты защиты, информационная безопасность АСУ ТП в оборонно-промышленном комплексе, других отраслях промышленности, порядок получения заключений об отсутствии аналогов зарубежных ПАК, опыт безопасной разработки ПО и внедрения соответствующих процессов, реализации наложенных мер ИБ, применения встроенных средств защиты информации.

Аудиторию интересует также тематика надежности импортозамещенных систем. В период использования зарубежных решений производственные предприятия привыкли к высоким стандартам защиты АСУ ТП. Сегодня важно уметь отсеивать проблемное (несовершенное) оборудование, ПО и другую продукцию компаний-«однодневок».

Один из выводов конференции «АСУ ТП КВО – 2024» состоит в том, что обеспечение информационной безопасности значимых объектов КИИ требует не только материальных, финансовых, но и интеллектуальных затрат и усилий. Коллективное обсуждение задач, проблем в этой области в текущих экономических условиях на фоне меняющихся требований законодательства способствует поиску нестандартных решений, обмену опытом и наработками, доказавшими эффективность на практике. ■