XIII КОНФЕРЕНЦИЯ

«Информационная безопасность АСУ ТП КВО»

ПРОГРАММА

4-5 марта 2025 г.

г. Москва

XIII КОНФЕРЕНЦИЯ

«Информационная безопасность АСУ ТП КВО»

4-5 марта 2025 г., г. Москва

Генеральный партнер

АЙТИБАСТИОН

Стратегический партнер

K2 кибер безопасность

Золотой партнер

КОМПАНИЯ АКТИВ

Серебряный партнер

КИБЕРПРОТЕКТ

Бронзовый партнер

udv|group

Хрустальный партнер

AMT GROUP

Спонсор Ужина ИБ-директоров

Контур staffcop

Партнеры

infotecs

КСБ-СОФТ

информзащита

GIS ГАЗИНФОРМ СЕРВИС

INFOWATCH

ЦИФРОВЫЕ РЕШЕНИЯ

УЦСБ

Партнер второго дня

СВД Встраиваемые Системы

Экспоненты

IST

PVS-Studio

Jet

axxtel

RUSIEM

ДиалогНаука

itprotect

RTT

NGRSOFTLAB

ИНДИД

СИСТЕМОТЕХНИКА-НН

Информационные партнеры

Журнал "ИСУП"

CISOCLUB

ТОЧКА ОПОРЫ

ТЕХСОВЕТ

ПРОМЫШЛЕННЫЙ

ОБОРОННО-ПРОМЫШЛЕННЫЙ ПОТЕНЦИАЛ

Крылья

ICT2GO

ICTONLINE

ЯИТЫ

КОДЕБАЙ АКАДЕМИЯ

Сергей БОЧКАРЕВ:
«Будущее за автоматизацией»

В сфере информационной безопасности немало актуальных задач, требующих первостепенного внимания специалистов. Но в числе наиболее приоритетных эксперты называют выполнение требований безопасности критической информационной инфраструктуры. Какая роль в обеспечении защиты КИИ отводится продуктам для предотвращения несанкционированного привилегированного доступа к объектам, какое влияние на их разработку и внедрение окажет ГОСТ на автоматизированные системы управления, каковы перспективы технологических альянсов в сегменте ИБ? На эти и другие вопросы отвечает Сергей Бочкарев, генеральный директор «АйТи Бастион».

– Какие тенденции в сегменте продуктов для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам вы считаете доминирующими?

– На текущий момент тенденции не изменились. Как и в прошлом году, продукты по контролю привилегированного доступа все сильнее сосредоточиваются вокруг аналитики. Большинство продуктов достигло той зрелости, когда собираемой информации становится достаточно и для поведенческой аналитики, и для более глубокой с использованием математических моделей или моделей машинного обучения. Необходимо выявлять отклонения в таком привилегированном доступе и без участия человека выдавать вердикт, насколько доступ санкционирован и потенциально опасен. Мы этот тренд заметили достаточно давно, около трех лет назад, когда появилась первая версия СКДПУ НТ «Мониторинг и аналитика».

Сегодня мы продолжаем развиваться в этом направлении, чтобы дать конечным пользователям инструменты минимизации ручных операций для анализа, без необходимости выстраивания подобных инструментов на стороне SIEM-систем, чтобы SIEM в качестве центральной точки принимал агрегированные данные и требовал меньше затрат, в том числе по настройке для анализа сырых событий от PAM.

Наряду с развитием ARP- и SUAR-систем появляются точечные варианты развития функциональности PAM: данную закономерность мы тоже заметили еще в прошлом году. Поэтому продолжаем развиваться не только в плане записи действий, но и активного противодействия возникающим угрозам и инцидентам. К примеру, недавно вышли интеграции с InfoWatch Arma в части контроля привилегированного доступа и предотвращения аномалий. Мы считаем, что продолжение этого сотрудничества будет важным пунктом в развитии систем класса PAM и контроля привилегированного доступа.

Таким образом, общий тренд состоит, с одной стороны, в минимизации действий людей при выполнении анализа, а с другой – в дальнейших шагах по превентивному реагированию и блокировке нежелательных действий.

– В России впервые утвержден ГОСТ на автоматизированные системы управления доступом. Как вы оцениваете его влияние на унификацию подходов к разработке, внедрению и настройкам таких систем, сбору необходимых доказательств?

– Вряд ли именно введение ГОСТа кардинально изменит подходы к разработке. ГОСТ в этом случае, скорее, лишь узаконит или опишет общие подходы к тому, как необходимо разрабатывать подобные системы. То есть ГОСТ направлен в первую очередь на четкое описание автоматизированной системы управления доступом, которая в классификации описана как IdM (Identity Management). На мой взгляд, подходы к разработке не изменятся, но появятся понятные узаконенные ориентиры для четкой классификации таких решений и определения их минимально необходимой функциональности.

Однако заказчик по-прежнему, я уверен, будет выбирать продукты, которые подходят под конкретно его бизнес-процессы, не обязательно со всеми обозначенными функциями.

Подобный стандарт – это, по сути, рекомендация по выбору, но для заказчика решение его конкретных задач, причем не только функциональных, но и по обеспечению требований регуляторов, будет приоритетнее рекомендаций.

– Что включает в себя экосистема СКДПУ НТ? В чем ее ключевые преимущества?

– Изначально экосистема строилась по классическому сценарию класса PAM. Позже мы поняли, что задач вокруг привилегированного доступа значительно больше, чем может себе позволить обычный PAM, который на текущий момент неплохо представлен на отечественном рынке. Однако все, что на рынке есть, решает, в основном, задачи классического контроля привилегированного доступа: запись событий и доступ конкретного пользователя к целевой защищаемой системе.

Осознав это, мы начали расширять свою систему и в плане аналитики, и в плане решаемых ею задач. На текущий момент ядро системы СКДПУ НТ – «Шлюз доступа», который является ключевым элементом пазла контроля привилегированного доступа. Вокруг него строится целая плеяда подсистем, и каждая из них решает конкретную задачу. То есть, если «СКДПУ НТ Шлюз доступа» – это средство, которое хранит в себе политики и проводит пользователя к ресурсам, то, например, «СКДПУ НТ Мониторинг и аналитика» служит центром анализа для офицера безопасности.

Второй шаг: «СКДПУ НТ Портал доступа» – подсистема, которая сосредоточена на удобном предоставлении пользователю доступа с разных шлюзов, в том числе в распределенных системах. По сути, это упрощение пользовательского пути: система безопасности не должна быть препятствием для нормального функционирования компании или нормальной деятельности сотрудников. Любая ИБ-система должна быть максимально прозрачной и удобной для пользователя, ведь только в этом случае решения могут приживаться и быть эффективными. Именно с таким подходом мы реализовали «Портал доступа».

В рамках взаимодействия с большими заказчиками мы осознали, что актуальна проблема не только самого контроля, но и конфигурации и делегирования. Так появилась подсистема «СКДПУ НТ Кабинет оператора», которая позволяет в удобной форме делегировать часть полномочий от главного администратора системы СКДПУ НТ к дочерним подразделениям или смежным отделам. Они смогут управлять разрешениями, политиками доступа в рамках своих сегментов. Ключевое преимущество СКДПУ НТ – в подходе.

Кстати, еще одна подсистема появляется буквально на ваших глазах. «СКДПУ НТ Персональные сейфы» позволяет хранить личные секреты, пароли, сертификаты и ключи доступа внутри себя, закрывая большую часть задач. Предоставление доступа – лишь верхушка айсберга. За доступом стоят секреты, поэтому в СКДПУ НТ есть менеджер паролей, который может управлять секретами на конечных машинах. Однако эти секреты не всегда получается передать третьей стороне. Ряд секретов нужны для конкретных задач, их знает только конкретный пользователь. Хранить все это в голове сложно, записывать на бумажках или просто в телефонах – небезопасно. Для решения задач, в том числе по хранению секретов и передаче их между сотрудниками, появились персональные сейфы.

Чаще всего к нам приходят с запросом о необходимости автоматизации. Для этого предназначена подсистема «СКДПУ НТ Агрегатор доступа», позволяющая максимально автоматизировать процесс заведения пользователей и целевых систем под контроль СКДПУ НТ. Будущее за автоматизацией обмена информацией между системами, без этого невозможно развитие продукта в целом.

> Будущее за автоматизацией обмена информацией между системами, без этого невозможно развитие продукта в целом.

Кроме того, пусть и не в рамках прямой экосистемы СКДПУ НТ, но в арсенале «АйТи Бастион» имеется продукт «Синоникс». Он является продолжением общей направленности компании на контроль и автоматизацию процессов в рамках сетей, пользователей и целевых устройств. «Синоникс» обеспечивает безопасный обмен данными и файлами между изначально несвязанными сетями. Таким образом, он закрывает вопросы доступа пользователя и доступа информационной системы из одной сети (или сегмента сети) в другую.

– Какие проекты из реализованных вашей компанией за минувший год вы хотели бы отметить и почему?

– По понятным причинам мы не можем называть большую часть реализованных проектов. Впрочем, последний из публичных и знаковых кейсов касался одной из госкорпораций. Отмечу,

что наша система СКДПУ НТ стабильно востребована в промышленности и нефтегазовом секторе экономики. Продолжаем нарабатывать экспертизу в этих отраслях, оптимизируя наш продукт под решение задач крупных заказчиков из числа субъектов КИИ.

предоставить, по сути, те же альянсы, но под одним брендом.

– Какие изменения произошли в команде «АйТи Бастион» за последний год? Как решаете задачу дефицита кадров?

– Компания активно развивается: за прошедший год коллектив увеличился почти на 40%. А бурный рост требует отладки процессов. «АйТи Бастион» подошел к вопросу серьезно, свои процессы выстраиваем на фоне внедрения системы менеджмента качества (СМК). Иными словами, мы не просто пишем внутренние инструкции, а опираемся на проверенную методику. Налаживаем взаимодействие между подразделениями, вводим необходимые нормативные документы. В 2024 г. большинство руководителей компании прошли обучение по СМК, мы провели несколько внутренних аудитов и один внешний. Надеемся в ближайшее время получить сертификат системы менеджмента качества ISO 9001:2015.

> Компания активно развивается: за прошедший год коллектив увеличился почти на 40%.

– Стремление к формированию технологических альянсов в сегменте ИБ – это закономерное развитие российского рынка? Или ожидания от эффективности подобных структур завышены?

– На мой взгляд, процесс формирования альянсов только стартует. У нас много проектов по построению комплексных систем и станет еще больше. Если изначально мы активно инициировали создание подобных коллабораций, то сейчас с идеями приходят уже к нам.

Однако монополизации таких альянсов ждать не стоит: слишком насыщенный и неоднородный рынок. Победит тот, кто выстроит максимально эффективные взаимосвязи между своими решениями. На примере проектов видим, что заказчики формулируют свои задачи именно как симбиоз нескольких ИБ-решений разных производителей. Это значит, что между ними необходима эффективная связка для исключения «зазоров» между защищаемыми сегментами.

Таким образом, ожидания от эффективности коллабораций не завышены, просто альянсы пока только формируются. Это объясняется тем, что ряд игроков пытается в определенном смысле монополизировать круг ИБ-решений, в том числе за счет поглощений и слияний, чтобы

Что касается дефицита кадров, то стараемся подходить к этому вопросу комплексно. С одной стороны, активно сотрудничаем с вузами, например, с Московским политехом, Финансовым университетом при Правительстве РФ, региональными учебными заведениями. Студенты приходят стажерами и довольно быстро закрепляются в коллективе, мы их зачисляем в штат. С другой стороны, развиваем сотрудников внутри компании. Большинство руководителей «АйТи Бастион» выросли из рядовых менеджеров. Мы обучаем тех, кто стремится развиваться, составляем ИПР, поддерживаем любые образовательные инициативы. В частности, у нас есть корпоративный университет, эффективно работает система наставничества. В общем, у каждого сотрудника есть возможности для роста, было бы желание.

Конечно, стараемся показать себя рынку как ответственного работодателя. Рассказываем об этом соискателям не только на собеседованиях, но и на отраслевых конференциях.

– В каком направлении развиваются продукты «АйТи Бастион»? Каким технологиям компания отдает предпочтение и почему?

– Продукты развиваются прежде всего в части сбора и аналитики данных, более точного контроля и выполнения эксплуатационных сценариев. Ограничиваться сейчас только мерами – странный подход. Можно сколько угодно составлять бумажки, получать сертификаты, но если решение невозможно эксплуатировать в нормальных бизнес-процессах компании, оно не приживется и не будет приносить пользу. Поэтому продукты «АйТи Бастион» развиваются в сторону оптимизации под бизнес-процессы заказчика, его пожелания и запросы. ■

> Продукты «АйТи Бастион» развиваются в сторону оптимизации под бизнес-процессы заказчика, его пожелания и запросы.

Егор КУЛИКОВ:

«Количество наших проектов по киберзащите КИИ и АСУ ТП увеличилось на 70%»

В условиях импортозамещения построение эффективной киберзащиты объектов критической информационной инфраструктуры требует дополнительных навыков и ресурсов. О характере основных киберугроз, способах и моделях противодействия вирусам шифровальщикам, возможностях SOC (Security Operations Center) и форматах предоставления на их базе услуг рассказал Егор Куликов, руководитель направления безопасности КИИ и АСУ ТП К2 Кибербезопасность.

– Какие киберугрозы сегодня наиболее актуальны для КИИ и АСУ ТП?

– Из года в год мы наблюдаем серьезный рост и усложнение киберугроз во всех российских компаниях. Промышленность входит в тройку наиболее атакуемых отраслей наряду с госсектором и финансами. В прошлом году количество наших проектов по защите КИИ и АСУ ТП увеличилось на 70%.

Основные угрозы – атаки на периметр и через цепочку поставок. Критичны не столько сами атаки, сколько именно лазейки, через которые можно проникнуть. Например, нелегитимные/забытые каналы удаленного доступа, что особенно актуально для промышленных предприятий.

В прошлом году активизировались вирусы-шифровальщики. В наш SOC каждую неделю приходит по несколько заявок от заказчиков. Если шифровальщик попадает из корпоративной среды в производство, то оно просто встает. Для тех, у кого нет ручного управления, это максимально критично.

– Как изменился за последнее время подход к обеспечению проактивной защиты от киберрисков и угроз объектов КИИ и АСУ ТП?

– Несколько лет назад, когда мы приходили к заказчикам и обсуждали вопросы кибербезопасности, видели большое сопротивление со стороны специалистов по эксплуатации промышленных инфраструктур. Сейчас компании начали намного серьезнее подходить к вопросу информационной безопасности. Она встроилась в общую модель управления рисками бизнеса.

Во-первых, большую роль играет ужесточение санкций за неисполнение требований законодательства в области КИИ. Здесь и большие штрафы, и даже уголовная ответственность для гендиректора и ответственных за кибербезопасность, если произошел инцидент, повлекший экономические риски или угрозу здоровья и жизни. Также необходимо учитывать то, что всех обязали проводить регулярный контроль защищенности. Это уже точно не про «бумажную» безопасность. Ну и, конечно, вызовы импортозамещения.

Во-вторых, из-за усложнения атак возросла доля инцидентов, которые направлены на нарушение деятельности организаций. Наиболее частое последствие ИБ-инцидентов в любой промышленности – простои в работе предприятия, что чревато очень большими финансовыми и репутационными рисками.

– Насколько последовательно осуществляется миграция с иностранных ИБ-решений на отечественные, с какими трудностями сталкиваются компании?

– Мы видим, что миграция активно продолжается, но далеко не все успели выполнить требования Указа Президента № 250 и полностью перейти на отечественные средства защиты информации к началу этого года. Согласно нашему прошлогоднему опросу рынка, больше половины (59%) субъектов КИИ еще летом понимали, что у них не хватит времени на полную замену зарубежных продуктов. Основными причинами называли все еще заметную нехватку отечественных аналогов иностранных ИБ-решений, отсутствие бюджета и других ресурсов для осуществления перехода, сжатые сроки и неготовность инфраструктуры.

При этом вопрос импортозамещения постепенно решается. Отечественные производители предлагают все больше решений. Появляются целые экосистемы для безопасности КИИ. Как показывает опыт реализации наших проектов, инфраструктура СОИБ может быть полностью импортозамещена.

Делать долгосрочные прогнозы очень трудно. На мой взгляд, полное импортозамещение потребует несколько лет. Все-таки это вопрос не просто быстрого перехода на отечественные решения, а построения эффективной киберзащиты именно КИИ. Инциденты в них могут повлиять не только непосредственно на организации, но и на очень большое количество людей. К тому же многие ждут более качественных аналогов зарубежных решений, чтобы не перестраиваться в будущем снова.

– Полтора года назад К2 Кибербезопасность вышла на рынок коммерческих SOC. Чем было обусловлено решение? Каков спрос на услуги SOC?

– Нашей целью было предоставить рынку востребованный и эффективный продукт с учетом вызовов: роста и усложнения киберугроз, ужесточения требований законодательства (особенно для КИИ), дефицита на рынке кадров, оптимизации бюджетов и многих других. В таких условиях компаниям трудно самостоятельно быстро трансформировать свои системы киберзащиты и инфраструктуру, оценивать и делать выбор в пользу решений тех или иных вендоров, а затем качественно их внедрять и настраивать, эффективно мониторить и своевременно реагировать на инциденты.

Мы предлагаем комплексное решение – SOC, куда входят и технологический стек, и налаженные процессы, и команда профессионалов с опытом работы в разных отраслях и широкой партнерской сетью.

Регулярно проводимые нами опросы рынка показывают, что мы сделали верный выбор. Согласно нашим данным, 83% корпораций считают SOC ответом на рост киберугроз.

Основными мотиваторами перехода к услугам центров мониторинга кибербезопасности называют оценку ИБ-рисков, опыт прошлых атак, требования регуляторов и оптимизацию ИБ-бюджета. 78% компаний, внедривших SOC, довольны эффективностью его работы, а именно непрерывностью мониторинга, оперативным выявлением инцидентов и реагированием на них.

– По каким моделям предоставляются услуги на базе SOC? Что вы рекомендуете заказчикам?

– Моделей SOC всего три: собственные, гибридные и MSSP. Собственные SOC – это дорогостоящее решение, требующее постоянного внимания и развития. Такой центр нельзя построить, единоразово внедрив технологические решения, например SIEM и IRP. Нужны большие затраты на регулярное обновление оборудования и ПО, а также на персонал высокой квалификации. К тому же внедрение новых средств защиты информации всегда несет риски остановки прикладного оборудования и ПО, что особенно критично для промышленности.

Мы предлагаем более простые по формату альтернативы – SOC по моделям MSSP и гибрид. MSSP-модель выбирают компании, стремящиеся найти готовое решение с предсказуемым бюджетом и получить сервис «под ключ». Этот вариант подходит для крупных организаций и небольших предприятий, не имеющих собственной команды или достаточных ресурсов. Такую модель выбирают из-за прогнозируемых операционных расходов; делегирования провайдеру рисков, связанных с управлением оборудованием; отсутствия необходимости нанимать или обучать команду специалистов; гарантированного уровня обслуживания и т. д.

Для сравнения замечу, что создание и внедрение собственного SOC занимают от одного года, а по MSSP-модели – от одного месяца.

Гибридную модель выбирают в ситуациях, когда внутренних ресурсов компании недостаточно для полноценного функционирования SOC, но есть желание сохранить определенный уровень контроля. Здесь могут быть самые разные варианты распределения ответственности между заказчиком и интегратором. Например, гибрид актуален, когда уже внедренная SIEM-система не справляется с задачами предприятия и необходима внешняя экспертиза для повышения ее эффективности.

– В последнее время возрастают требования к профессиональному уровню специалистов в сфере ИБ, в частности, в АСУ ТП. Как ваша компания наращивает собственную экспертизу, как организовано обучение команды SOC?

– Не секрет, что на рынке дефицит талантливых кадров во всех направлениях кибербезопасности. Многие растят специалистов с нуля чуть ли не со школьной скамьи. Или переквалифицируют ИТ-сотрудников в ИБ-специалистов. Оба варианта требуют времени и других ресурсов на обучение. Из-за этого компании не могут быстро найти нужные кадры и приходят к нам – интеграторам. Мы вырастили у себя специалистов, в том числе в сфере ИБ в АСУ ТП, и продолжаем эту практику.

В целом это непрерывный процесс, поскольку повышение квалификации должно быть регулярным в условиях постоянно появляющихся угроз и технологий. Имеются в виду, в частности, стандартные курсы по кибербезопасности, спецкурсы по управлению СЗИ.

Нам важны не только hard skills, но и soft. Например, наша команда специалистов техподдержки SOC прошла тренинг по коммуникации с заказчиками. Основная цель – научить ребят общаться с клиентами на одном языке, просто и быстро доносить важную информацию без непонятных им узкопрофильных терминов. Во-первых, это крайне важно в случае инцидента, когда каждая минута играет огромную роль, и все должны друг друга четко понимать. Во-вторых, это отлично сработало на повышении лояльности клиентов, которые воспринимают нашу команду как доверительный источник экспертизы в сложных процессах. Например, заказчики могут понять и оценить наши действия, даже если на их стороне нет ИБ-специалиста. ■

Решения для защиты АСУ ТП

не должны быть обременительны финансово и технологически

Руководитель департамента защиты киберфизических систем компании «Актив» Алексей Лазарев и заместитель генерального директора по управлению компании «Актив» Андрей Степин оценили ход импортозамещения в сфере АСУ ТП и рассказали о преимуществах флагманских моделей ключевых носителей Рутокен, сертифицированных ФСБ.

– Какие тенденции в области информационной безопасности АСУ ТП вы могли бы выделить?

– С момента появления данной темы в информационной повестке прошло около десяти лет. Много было сделано, но «много» не означает достаточно. Проблема обеспечения безопасности критических инфраструктур, в том числе АСУ ТП, усугубляется нарастающим отставанием развития средств защиты информации от развития самих инфраструктур (по объемам и темпам). Любая попытка сократить разрыв приводит к значительному увеличению затрат на внедрение новых решений.

С учетом того, что системы обеспечения безопасности не выполняют основные функции целевых систем, а лишь поддерживают исполнение, у пользователей возникает соблазн сэкономить на безопасности. Поэтому перспективные тенденции во многом зависят от регулирования и контроля соблюдения установленных требований. Положительные сдвиги происходят, но работы предстоит много.

– Какие планы у компании «Актив» по развитию продуктов и услуг в контексте защиты ПО и АСУ ТП?

– В ближайших планах вывод на массовый рынок компонентов и решений для защиты ПО и оборудования для АСУ ТП, других систем и направлений ИТ-индустрии. Это будут как собственные разработки компании, так и совместные решения с партнерами. Основная задача – создание эффективных технологических продуктов, которые не обременяют заказчика в финансовом и технологическом плане. Это позволит увеличить количество клиентов и расширить спектр применения.

В дни конференции «ИБ АСУТП КВО – 2025» на нашем стенде эксперты представят линейку активных USB-токенов и смарт-карт Рутокен ЭЦП 3.0. А специалисты еще одного направления компании, AKTIV.CONSULTING, проконсультируют по вопросам обеспечения ИБ на промышленных предприятиях.

– В чем преимущества флагманских моделей ключевых носителей Рутокен ЭЦП 3.0 3120, не так давно сертифицированные ФСБ?

– Расширенный ассортимент устройств Рутокен с интерфейсом USB-C удовлетворил потребность в средствах электронной подписи самых активных и мобильных пользователей, работающих на ноутбуках, планшетах и смартфонах. Сертифицированные токены с сенсорной кнопкой для защиты от удаленного управления обеспечили защиту от более широкого спектра угроз.

Благодаря использованию новой смарт-карточной платформы и внедрению ряда инновационных механизмов именно линейка Рутокен ЭЦП 3.0 3120 максимально адаптирована для использования на относительно неизведанных для нас направлениях. Прежде всего в доверенных, функциональных и высокопроизводительных криптографических модулях для киберфизических систем. ■

Константин ОСТАШОВ:

«Атаки на объекты КИИ стали более изощренными и частыми»

В сфере информационной безопасности объектов КИИ происходят значительные изменения. О факторах, определяющих динамику данного сегмента, возможностях и потенциале востребованных продуктов рассказал Константин Осташов, ведущий тренер по продажам компании «Киберпротект».

– Какие факторы, на ваш взгляд, определяют развитие рынка информационной безопасности объектов КИИ?

– В последние годы на рынке ИБ объектов критической инфраструктуры (КИИ) ужесточаются регуляторные требования, увеличивается количество нормативных актов и стандартов в сфере ИБ, что требует от организаций более строгого соблюдения правил. Например, в 2024 г. были внесены изменения, касающиеся защиты от одной из самых распространенных угроз – DDoS-атак. Речь идет об изменениях требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239 (внесены приказом ФСТЭК России от 28.08.2024 № 159).

Наряду с этим увеличивается число кибератак на объекты КИИ. Злоумышленники все активнее используют искусственный интеллект. Одно из наиболее опасных направлений – развитие интеллектуальных фишинговых атак. Мы как вендор ПО располагаем передовыми решениями, которые помогут заказчикам выстраивать инфраструктуру должным образом.

– С 1 января вступило в силу требование НПБ, ПО для КИИ. Как ситуация будет развиваться применительно к АСУ ТП?

– К сожалению, не все субъекты КИИ в прошлом году выполнили планы по переходу на РПО. Но мы сделали все возможное для того, чтобы самые популярные ОС из реестра Минцифры не остались без защиты от утери или удаления данных. Мы следим за изменениями, которые вносятся вендорами в их ОС, и поддерживаем совместимость с нашим продуктом «Кибер Бэкап».

– Как развивается сотрудничество с лидерами рынка в сфере защиты объектов КИИ?

– Мы сотрудничаем с большим количеством российских разработчиков. Сейчас у нас более 60 технологических партнерств с разработчиками ОС (ГК «Астра», «Альт», «РедОС» и т. д.), решений для виртуализации (zVirt, «Брест», «Базис» и т. д.), СУБД (PostgresPro, ProximaDB и др.), почтовых сервисов.

– Какими компетенциями в области АСУ ТП обладает ваша компания?

– «Киберпротект» – российский разработчик ПО для защиты данных, резервного копирования и восстановления виртуальных, физических и облачных сред. Резервное копирование данных в АСУ ТП обеспечивает защиту информации от потерь, вызванных сбоями оборудования, программными ошибками или внешними угрозами. Наше решение хорошо интегрируется с SIEM-системами. Сертифицированное решение подходит для значимых объектов КИИ I категории, ГИС I класса защищенности, АСУ ТП I класса защищенности, ИСПДн при необходимости обеспечения I уровня защищенности и для ИС общего пользования II класса.

Наша DLP-система для предотвращения утечек конфиденциальной информации и обеспечения соблюдения норм безопасности обеспечивает мониторинг и контроль данных на всех уровнях системы: от пользовательских устройств до серверов и сетевой инфраструктуры. DLP-решение может обнаруживать и блокировать несанкционированный доступ к данным, отслеживать их перемещение внутри и вне системы.

– С какими запросами чаще всего обращаются к вам клиенты в области защиты АСУ ТП?

– Чаще всего клиенты интересуются, работает ли наше ПО для резервного копирования в изолированных контурах, сможем ли мы поддержать ОС, которые давно используются в системах. Конечно, у нас есть вариант применения ПО «Кибер Бэкап» в изолированных средах при помощи загрузочного образа. Также при помощи этого образа мы можем сделать резервное копирование ОС, созданных очень давно. ■

Сергей ОВЧИННИКОВ:

«Атакующая сторона не подчиняется стандартам и правилам»

Спектр угроз, способных блокировать работу АСУ ТП, расширяется. На фоне замещения импортных продуктов повышается сложность интеграционных задач. О подходах к обеспечению ИБ в АСУ ТП и доступных решениях рассказал Сергей Овчинников, директор по маркетингу компании UDV Group.

– Какие проблемы наиболее актуальны в сфере защиты АСУ ТП?

– Атакующая сторона всегда более мобильна, не подчиняется стандартам и правилам. Производители ПО и оборудования ориентируются на релизные циклы, сроки поставки комплектующих и т. п. Увы, вендоры выступают в роли догоняющих тех, кто атакует. Поэтому UDV Group постоянно наращивает компетенции в области инноваций.

Сложность АСУ ТП, обусловленная интеграцией оборудования и ПО, увеличивает поверхность атаки на цепочки поставок. Во многих АСУ ТП применяется устаревшее программное и аппаратное обеспечение. Злоумышленники используют уязвимости для доступа к системам и выполнения вредоносных действий. Непрерывный контроль узлов на наличие уязвимостей, меры по их устранению помогают снизить риски ИБ.

– Каким образом требования Правительства по импортозамещению будут определять развитие ИБ АСУ ТП?

– Раньше в АСУ ТП часто применялся подход «работает – не трогай». Переход на отечественные технологии приводит к изменениям ИТ/ОТ-инфраструктур заказчиков. Есть трудности из-за нехватки специалистов и несовместимости Linux-систем с ПО для зарубежных ПЛК. На объективно сложные проекты импортозамещения в промышленности накладывается специфика российского рынка: защитные решения для Linux даже в корпоративном сегменте создавались с отставанием от аналогов для Windows.

Опыт пилотирования наших решений показывает, что после длительного периода без изменений в технологическом сегменте обнаруживаются узлы, о наличии которых никто не догадывался. Для безопасного перехода необходимо применять ИБ-решения, которые повышают видимость ландшафта и обеспечивают мониторинг ИБ. Такими решениями могут быть системы класса NTA/IDS с поддержкой промышленных протоколов, например, UDV DATAPK Industrial Kit.

– Каковы доминирующие тренды в развитии решений для ИБ АСУ ТП?

– Раньше многие средства защиты информации для обеспечения ИБ АСУ ТП не предусматривали функций реагирования. Заказчикам было достаточно информации об инцидентах и экспертных рекомендаций. Сейчас явный тренд на автоматизацию функций реагирования.

Другой тренд – применение машинного обучения. Работа узлов в технологическом сегменте поддается моделированию в виде конечных автоматов. Отсюда задача построения цифрового двойника техпроцесса для выявления отклонений. Мы эту задачу решили. Основу запатентованного решения UDV EDR for PLC составляют анализ промышленных протоколов (в том числе проприетарных) и работа с управляющими сигналами ПЛК. Без воздействия на защищаемую систему технология позволяет мгновенно определить проблемный узел, источник аномалий и непосредственно сигналы.

– В прошлом году вы анонсировали решение для контроля версий проектов ПЛК в технологических сетях. Что из новинок в ближайших планах?

– Мы выпустили продукт UDV DATAPK Version Control, позволяющий контролировать версии проектов ПЛК. Решение пилотируется, есть внедрения. Мы видим запрос со стороны заказчиков на обеспечение непрерывности технологического процесса. Изменения в техпроцесс вносятся нечасто, и цена некорректных правок может быть высокой. Отмечу, что сегодня UDV DATAPK Version Control – единственное отечественное решение для системного контроля проектов ПЛК.

В мае 2025 г. планируем выпустить масштабное обновление флагманского продукта UDV DATAPK Industrial Kit 3.0 – комплексного решения для мониторинга кибербезопасности и оперативного обнаружения инцидентов в промышленных сетях без негативного влияния на защищаемые системы. ■

Вячеслав ПОЛОВИНКО:

«Контроля исходного кода недостаточно для локализации угроз»

О ключевых вызовах, преимуществах экосистемных решений на рынке информационной безопасности, создании продуктов и выборе мер для локализации актуальных угроз рассказал Вячеслав Половинко, руководитель направления собственных продуктов компании АМТ-ГРУП.

– Каких результатов за последний год достигла ваша компания в выстраивании технологических партнерств?

– За последний год мы серьезно продвинулись в формировании технологических партнерств, заинтересованных в развитии нашего продукта InfoDiode и продуктов от вендоров СЗИ, АСУ ТП, MES и др. Среди основных следует выделить совместные решения с «Гарда», «АльфаПлатформой», «Терралинк», «Индасофт», Kaspersky MLAD и Kaspersky KICS, «Киберпротект», «АлтексСофт» (в части продукта Redcheck), Rvision.

Кроме того, мы сделали акцент на сотрудничестве с компаниями в области энергетики. Прежде всего имею в виду решения от «Релематика», «Монитор-электрик». Работу с вендорами в этой отрасли мы продолжаем, считая ее высокоприоритетной.

– Какие решения будут представлены в выставочной зоне конференции «ИБ АСУТП КВО – 2025»?

– Среди наиболее интересных – решения, предложенные «Лабораторией Касперского» и компанией «Гарда». В частности, стоит отметить интеграции InfoDiode с продуктами семейства KICS (передача SPAN-трафика, данных KICS for Nodes для получения событий на сенсорах KICS for Networks и направления их в SIEM), а также решение аналогичных задач на основе систем от «Гарда».

Есть и разработки в области аналитики и машинного обучения – на базе продукта MLAD от Kaspersky. Технологическое партнерство по этому направлению касается преимущественно передачи данных из АСУ ТП через InfoDiode в систему Kaspersky MLAD. Цели такого обмена через InfoDiode – предоставление данных для прогнозирования аномалий во внешнюю систему в условиях изоляции сегмента-источника. На основе этих данных формируются рекомендации для принятия решений по локализации проблем с оборудованием и технологическими процессами. Все эти решения продемонстрируем на стенде: полностью или частично, в виде готовых референсных схем и архитектур.

– Что АМТ-ГРУП может противопоставить атакам на цепочки поставок?

– Мы ориентируемся на рекомендации недавно принятого ГОСТ Р 56939-2024 по безопасной разработке, учитываем также требования и рекомендательные письма профильного регулятора – ФСТЭК.

Но это не достаточно для локализации обозначенных угроз. Значительную роль играют культура разработки, квалификация сотрудников, степень заимствования компонентов, организация доступа к инфраструктуре разработки исходя из обстоятельств (например, болезни или отпуска сотрудников, текучки кадров), особенности доставки оборудования, правила проведения стейджингов. Все эти вопросы находятся в фокусе нашего внимания.

– В ответ на какие вызовы АМТ-ГРУП намерена расширять линейку и функциональность диодов, повышать производительность и т. д.?

– Мы выделили три основных вызова, актуальных для решений класса «диод». Первый – скорость передачи данных. Представим модель 10G – пока в аппаратном исполнении.

Второй вызов – контроль за передачей данных: так называемые междоменные решения. Такие решения появляются и в нашей линейке.

Третий вызов – возможность получения обратного канала по требованию – в условиях изоляции инфраструктуры посредством InfoDiode. Речь о сценариях, когда двунаправленный канал необходим – но только в регламентное время, относительно редко и/или по требованию. Подобные задачи, на наш взгляд, могут быть решены исключительно с помощью отдельного класса решений, первую версию которых представим на конференции. ■

Тринадцатая конференция «Информационная безопасность АСУ ТП КВО»

4–5 марта 2025 г.
г. Москва

ПРОГРАММА

ДЕНЬ ПЕРВЫЙ

08.30–09.45
Регистрация. Работа выставки

09.45–13.30
Пленарное заседание

- Вступительное слово модератора – *Гаврилов Виктор Евдокимович, главный научный сотрудник, Федеральный исследовательский центр Информатика и управление Российской академии наук*
- Вопросы изменения законодательства в области обеспечения безопасности КИИ – *Зенкин Павел Сергеевич, заместитель начальника управления, ФСТЭК России; Булгаков Андрей Сергеевич, заместитель начальника 3 отдела 9 управления ФСТЭК России*
  Сессия вопросов и ответов
- Особенности проведения мониторинга защищенности информационных ресурсов организаций, деятельность которых связана с обеспечением технологических процессов. Практика проведения НКЦКИ таких мероприятий – *Маркаров Артем Артурович, представитель Национального координационного центра по компьютерным инцидентам*
  Сессия вопросов и ответов
- Национальная система обеспечения кибербезопасности: опыт Республики Беларусь – *Мячин Илья Владимирович, сотрудник Оперативно-аналитического центра при Президенте Республики Беларусь*
- Удобная эксплуатация: как защитить и оптимизировать работу сложных объектов КИИ – *Константин Родин, заместитель директора по развитию бизнеса, АйТи Бастион*
- Единый мониторинг промышленного и корпоративного сегментов: проще, эффективнее, экономнее – *Егор Куликов, руководитель направления безопасности КИИ и АСУ ТП, старший технический менеджер, К2 Кибербезопасность; Бондюгин Андрей Андреевич, руководитель направления предпродажной поддержки решений для бизнеса, «Лаборатория Касперского»*
- А кто это сделал? Вопросы доступа к технологическим системам и их решения – *Ольга Копейкина, ведущий консультант по информационной безопасности, AKTIV.CONSULTING*
- Как противостоять современным угрозам и обеспечивать комплаенс без СРК? – *Константин Осташов, ведущий тренер по продажам, Киберпротект*

- Реализация комплексного подхода для обеспечения ИБ АСУ ТП – *Сергей Овчинников, директор по маркетингу, UDV Group*
- Решения с воздушным зазором InfoDiode в составе комплексных проектов по защите КИИ. Новые функции и решения – *Вячеслав Половинко, руководитель направления собственных продуктов АМТ-ГРУП*

13.30–14.30
Обеденный перерыв. Работа выставки

14.30–17.00
Методы, технологии и инструменты защиты АСУ ТП

- Тенденции развития угроз безопасности информации в АСУ ТП – *Енютин Алексей Юрьевич, начальник отдела, ФАУ «ГНИИИ ПТЗИ ФСТЭК России»*
- Интеграция информационной безопасности и АСУ ТП: вызовы, решения и сценарии взаимодействия в условиях импортозамещения – *Антон Соложенко, директор по развитию бизнеса, ООО «ИнфоВотч АРМА»*
- 7 проблем при создании СОИБ АСУ ТП в 2025 году – *Алексей Комаров, региональный представитель УЦСБ в г. Москв*
- Проектирование комплексных систем ИБ ОКИИ: взгляд со стороны интегратора – *Егорова Татьяна Геннадьевна, заместитель руководителя департамента интеграционных решений по вопросам промышленной кибербезопасности, КСБ-СОФТ*
- Практика защиты объектов КИИ промышленных компаний – *Черкасов Владимир Борисович, начальник управления защиты АСУ ТП и АСУ, «Информзащита»*
- Защита импортозамещенного ландшафта АСУ ТП – *Парфенова Юлия Вячеславовна, помощник менеджера по продукту, ООО «Газинформсервис»*
- Зеркалирование трафика и безопасное подключение средств мониторинга в АСУ ТП – *Лакаев Алексей Анатольевич, начальник отдела развития телекоммуникационного оборудования, НПП «Цифровые решения»*
- Решение ИнфоТеКС для защиты протоколов Industrial IoT на примере LoRaWAN – *Власенко Алексей Юрьевич, ведущий менеджер продуктов, ИнфоТеКС*

17.00–17.30
Перерыв. Работа выставки

17.30–19.00
«Практикум»

Разработка унифицированной (целевой) защищенной архитектуры АСУ ТП для предприятий металлургической отрасли

Постановщик
Дзьобан Павел Игоревич, заместитель руководителя Сервисной линии эксплуатации систем безопасности производственных и технологических систем, ООО «Норникель Спутник»

Свои решения представляют:
- Никулин Василий Геннадьевич, менеджер по сопровождению ключевых корпоративных проектов (Solution Architect), Лаборатория Касперского
- Вячеслав Половинко, руководитель направления собственных продуктов АМТ-ГРУП
- Алексей Шанин, директор департамента технической поддержки продаж, УЦСБ

17.30–19.00
Мастер-класс по диодам данных

- Знакомство с диодом одного из отечественных разработчиков
- Настройка UDP-туннелирования
- Использование VLC для трансляции и приема экрана на Astra Linux

19.00–20.30
Фуршет

20.00–01.00
Ужин ИБ-директоров (по приглашению)

ДЕНЬ ВТОРОЙ

08.30–09.15
Регистрация участников. Работа выставки

09.15–11.00
Панель (доклады + дискуссия)
Практический опыт создания системы ИБ АСУ ТП
В фокусе – нефтегазовая отрасль

- Особенности защиты информации в АСУ ТП транспортировке углеводородов – *Пономарев Дмитрий Анатольевич, заместитель технического директора по ИБ, ООО НВФ «СМС»*
- Методы конструктивной безопасности при разработке УРУ АСУ ТП ОА – *Карантаев Владимир Геннадьевич, MBA руководитель направления «Кибербезопасность», Центр НТИ МЭИ ФГБОУ ВО «НИУ МЭИ», к. т. н.*
- Резервное копирование на производственных объектах – *Владимир Орлов, специалист по поддержке продаж продуктов, Киберпротект*

➢Решение задач информационного обмена с помощью ПК «Синоникс» на понятных примерах – *Александра Гончарова, инженер поддержки продаж/пресейл, АйТи Бастион*

Вопросы дискуссии

- Специфика защиты АСУ ТП в нефтегазовом секторе. Динамика изменения угроз количественная и качественная. Распределенные системы управления (РСУ, DCS системы управления технологическими процессами, с построением высокорезервированных, распределенных систем ввода-вывода и децентрализованной обработкой данных) как один из наиболее критических классов АСУ ТП и специфика их защиты
- Проблематика импортозамещения АСУ ТП в отрасли. Неготовность части предприятий отрасли к импортозамещению и ее причины. Реальность и перспективы создания отраслевых АСУ ТП, в том числе на базе открытой архитектуры. Концепция обеспечения технологической независимости и ИБ открытых АСУ ТП (подготовленная Минпромторгом) и ее практические перспективы
- Опыт работы с отраслевым реестром. Механизмы пополнения и применения реестра в части АСУ ТП. Открытые вопросы

Участники

- *Васильев Сергей Викторович, руководитель практики автоматизации ПАО «Газпром Нефть»*
- *Александра Гончарова, инженер поддержки продаж/пресейл, АйТи Бастион*
- *Бибик Андрей Валерьевич, директор департамента защиты информации, ООО «АВТОМАТИКА-СЕРВИС» (Газпром нефть)*
- *Карантаев Владимир Геннадьевич, MBA руководитель направления «Кибербезопасность», Центр НТИ МЭИ ФГБОУ ВО «НИУ МЭИ», к. т. н.*
- *Владимир Орлов, специалист по поддержке продаж продуктов, Киберпротект*
- *Пономарев Дмитрий Анатольевич, заместитель технического директора по ИБ, ООО НВФ «СМС»*

11.00–12.45
Панель (доклады + дискуссия)
Практический опыт создания системы ИБ АСУ ТП
В фокусе – электроэнергетика

➢ИБ АСУ ТП проблематика внедрения и разумная достаточность – *Шеметов Андрей Сергеевич, нчальник управления развития РЗА и метрологии, Департамент РЗ метрологии АСУ ТП, ПАО «Федеральная сетевая компания Россети», Департамент релейной защиты, метрологии и автоматизированных систем управления технологическими процессами, «Россети»/«Россети ФСК ЕЭС»*

- Актуальные вопросы обеспечения информационной безопасности в электроэнергетике – *Капустин Александр Владимирович, заместитель начальника службы информационной безопасности, АО «СО ЕЭС»; Правиков Дмитрий Игоревич, заведующий кафедрой КБ КВО, РГУ нефти и газа (НИУ) имени И.М. Губкина*
- Организация процесса РБПО для КВО под управлением ЗОСРВ «Нейтрино» – *Дужак Евгений, руководитель группы разработки СЗИ и сетевых технологий, ООО «СВД ВС»*
- Защита на максимум: как выстроить безопасность АСУ ТП эффективно – *Егор Куликов, руководитель направления безопасности КИИ и АСУ ТП, старший технический менеджер, К2 Кибербезопасность*

Вопросы дискуссии

- Уровень защищенности АСУ ТП на предприятиях отрасли. Основные факторы, сдерживающие выполнение всех требований регулятора по построению системы защиты информации АСУ ТП. Опыт расчетов показателя защищенности согласно действующим методикам и с учетом специфики отрасли и «подводные камни»
- Специфика угроз АСУ ТП в различных отраслях энергетики. Новые и «перспективные» векторы и рекомендации по их нейтрализации
- Уровень и глубина импортозамещения решений АСУ ТП отрасли. Основные классы и наличие отечественных аналогов. Опыт разработки отраслевых АСУ ТП силами самих энергокомпаний и оценка его эффективности. Учет требований регулятора в области защиты АСУ ТП и аспекты безопасной разработки. Потенциал встроенных средств ИБ

Участники

- *Капустин Александр Владимирович, заместитель начальника службы информационной безопасности, АО «СО ЕЭС»*
- *Дужак Евгений, руководитель группы разработки СЗИ и сетевых технологий, ООО «СВД ВС»*
- *Шеметов Андрей Сергеевич, начальник управления развития РЗА и метрологии, Департамент РЗ метрологии АСУ ТП, ПАО «Федеральная сетевая компания Россети»*

12.45–13.45
Обеденный перерыв. Работа выставки

13.45–15.45
Панель (доклады + дискуссия)
Практический опыт создания системы ИБ АСУ ТП
В фокусе – транспорт

- Особенности обеспечения безопасности информации в системах железнодорожной автоматики и телемеханики. Различие подходов и практический опыт – *Безродный Борис Фёдорович, заместитель руководителя центра кибербезопасности, АО «НИИАС»*

- Особенности защиты информации в АСУ ТП аэропортовой инфраструктуры – *Савченко Сергей Юрьевич, начальник службы по обеспечению информационной безопасности, ООО «Воздушные Ворота Северной Столицы»*
- Аппаратный корень доверия для обеспечения защиты данных: варианты реализации – *Панасенко Сергей Петрович, директор по научной работе, Компания «Актив»*
- Обеспечение информационной безопасности интеллектуальных транспортных систем – *Иконников Сергей Евгеньевич, доцент, Российский университет Транспорта (МИИТ), к. т. н.*

Вопросы дискуссии

- Взаимодействие с регулятором и формирование отраслевой нормативной базы. Отраслевой реестр типовых объектов КИИ транспортного комплекса
- Особенности обеспечения непрерывности технологических процессов на транспорте, в контексте информационной безопасности АСУ ТП
- Положение дел с импортозамещением АСУ ТП на транспорте. Ситуация на различных видах транспорта. Готовность разработчиков инвестировать в узкоспециализированные АСУ ТП

Участники

- *Безродный Борис Фёдорович, заместитель руководителя центра кибербезопасности АО «НИИАС»*
- *Иконников Сергей Евгеньевич, доцент, Российский университет Транспорта (МИИТ), к. т. н.*
- *Клочко Герман Александрович, начальник отдела, ФГУП «Росморпорт» СЗб филиал*
- *Половников Сергей Викторович, руководитель Центра компетенций по импортозамещению программного обеспечения транспортной отрасли, ФГУП «ЗащитаИнфоТранс»*
- *Савченко Сергей Юрьевич, начальник службы по обеспечению информационной безопасности, ООО «Воздушные Ворота Северной Столицы»*
- *Хмелевская Наталья Владимировна, начальник отдела обеспечения безопасности значимых объектов КИИ, ОАО «РЖД»*

15.45–17.30
Панель (доклады + дискуссия)
Практический опыт создания системы ИБ АСУ ТП
В фокусе – металлургия

- Практический опыт обеспечения информационной безопасности АСУ ТП Норникеля – *Дзьобан Павел Игоревич, заместитель руководителя Сервисной линии эксплуатации систем безопасности производственных и технологических систем, ООО «Норникель Спутник»*

- Применение решений InfoDiode при построении систем, в которых субъект управления расположен в менее доверенных сегментах – *Вячеслав Половинко, руководитель направления собственных продуктов АМТ-ГРУП*
- Особенности защиты информации в АСУ ТП на металлургическом производстве. Практический опыт: Основные вектора кибератак на субъекта КИИ в 2024 году – *Севостьянов Александр Владимирович, директор ДЭБ, АО «ДИАЙПИ» (Группа ТМК)*
- Актуальные вопросы контроля версий проектов ПЛК – *Владислав Ганжа, руководитель производственного направления, UDV Group*

Вопросы дискуссии

- Зрелость отечественных АСУ ТП для металлургии. Подходы металлургов к выбору поставщиков для поддержания, обновления или замены АСУ ТП в текущих условиях: российские решения, китайские аналоги, параллельный импорт. Претензии промышленности к отечественным разработчикам: отсутствие «клиентоориентированного» подхода и сервиса, низкий уровень зрелости, отсутствие требуемого функционала и т. д.
- Проблематика импортозамещения ПАК, задействованных в АСУ ТП. Готовность ИТ-индустрии разработать и представить отечественные аналоги и мнение промышленности. Особенности металлургической отрасли
- Высокие темпы распространения решений на базе ИИ в промышленности, в том числе использующих данные АСУ ТП, как источник дополнительных рисков. Оценка реальности угрозы и возможные меры безопасности

Участники

- *Владислав Ганжа, руководитель производственного направления, UDV Group*
- *Гордеев Станислав Александрович, начальник отдела промышленных ИТ, ООО «Объединённая сервисная компания»*
- *Дзьобан Павел Игоревич, заместитель руководителя Сервисной линии эксплуатации систем безопасности производственных и технологических систем, ООО «Норникель Спутник»*
- *Нуйкин Андрей Витальевич, начальник управления, ООО «ЕВРАЗ»*
- *Вячеслав Половинко, руководитель направления собственных продуктов АМТ-ГРУП*
- *Севостьянов Александр Владимирович, директор ДЭБ, АО «ДИАЙПИ» (Группа ТМК)*

17.30–19.00

«Практикум»

Реализация функции по фильтрации трафика промышленного протокола для целей защиты АСУ ТП от атак

Постановщик:
Устич Наталия Владимировна, архитектор по ИБ АСУ ТП, ПАО «Интер РАО»

Свои решения представляют:
- Антон Соложенко, директор по развитию бизнеса, ООО «ИнфоВотч АРМА»
- Андрей Иванов, архитектор решений, ИнфоТеКС
- Иван Николаев, технический директор, Русьтелетех

19.00–19.15
Открытый микрофон. Подведение итогов

19.15-20.30
Фуршет

Построение платформ ИБ при обеспечении инфообмена с компанией «АйТи Бастион»

4 марта с 14.30 до 16:00 в рамках конференции «Информационная безопасность АСУ ТП КВО» состоится круглый стол компании «АйТи Бастион» и компаний заказчиков на тему: **«Мультивендорный подход к построению платформ безопасности при обеспечении информационного обмена на объектах КИИ»**.

Мы часто слышим, что реальная информационная безопасность – это неудобно или вовсе мешает работать. Поэтому зачастую защита выстраивается только по «чек-листу»: такая безопасность не мешает, но и не защищает. Но очевидно, что обеспечение безопасности не должно противоречить задачам эксплуатации сложных систем, особенно объектов КИИ.

Мы как эксперты в области ИБ считаем, что мультивендорный подход к построению систем безопасности на объектах КИИ – это не только «хайповая», но и по-настоящему важная тема. По сути – это необходимость. Выстроить комплексную безопасность, как и комплексную АСУ ТП, силами и решениями только одного вендора невозможно. Поговорим об этом!

В рамках круглого стола будут рассмотрены темы:

- Актуальность информационного обмена на объектах КИИ
- Мультивендорный подход: выгоды и риски
- Непрерывный обмен данными или безопасность
- Информационный обмен на объектах КИИ: отраслевые сценарии

Встреча направлена на обмен опытом и ответы на вопросы о построении платформ безопасности на объектах КИИ. В дискуссии примут участие представители компаний-заказчиков.

Бонусом круглого стола будут закуски и напитки

Место проведения:

Москва, Hotel Soluxe, ул. Вильгельма Пика, д.16, 2 этаж, зал Чжуцян

Мастер-класс по работе с диодами данных

Время проведения: с 17.30 до 19.00, в рамках конференции «ИБ АСУ ТП КВО- 2025».
Место проведения: 3 этаж, Soluxe Hotel Moscow 5*, Москва, ул. Вильгельма Пика, 16

Ведущий: Лев Николаев, АНО ДПО «Техническая академия Росатома»
Цель мероприятия: научиться базовым операциям по односторонней передаче данных с использованием диода данных
Формат мероприятия: мастер-класс (участники выполняют задание вместе с ведущим)

В программе мастер-класса:
- Знакомство с диодом одного из отечественных разработчиков
- Настройка UDP-туннелирования
- Использование VLC для трансляции и приема экрана на Astra Linux

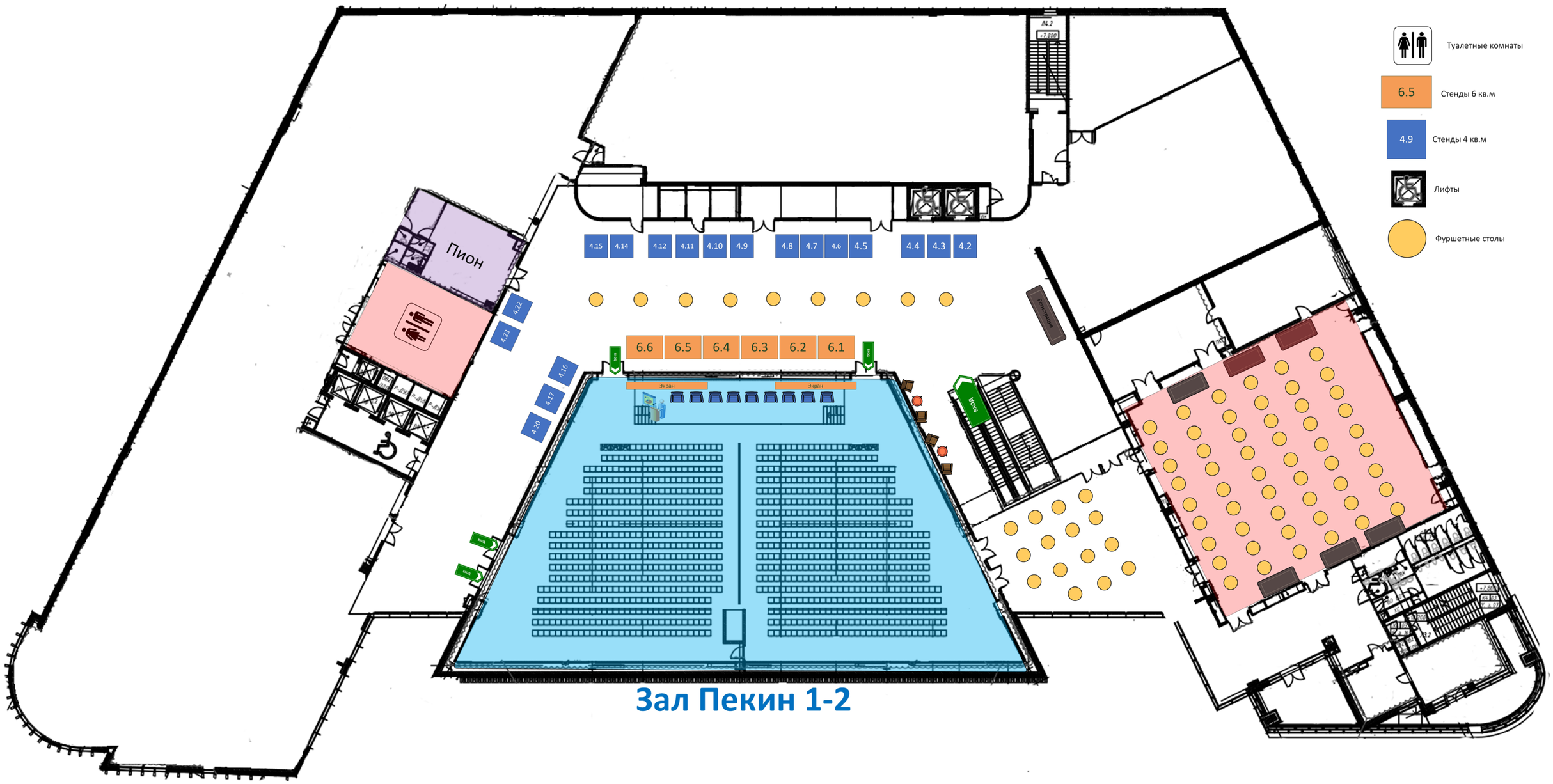
Что получат участники:
Практические навыки конфигурирования диода данных для передачи изображения из промышленной сети в открытую

Для кого предназначено:
- Сетевые и системные администраторы
- Администраторы ИБ

Требования к участникам:
С собой необходимо иметь ноутбук с Wi-Fi-адаптером и браузером и любой операционной системой

Количество мест ограничено (20 участников)

СХЕМА ВЫСТАВКИ



РАСПИСАНИЕ ПРЕЗЕНТАЦИЙ НА СТЕНДАХ — 4 марта

Время	Стенд 1	Компания 1	Презентация
14.00-14.15	6.6	АМТ-ГРУП	Междоменные решения (МДР) – следующее поколение решений по сегментации сетей
14.15-14.30	4.8	ИнфоВотч	Разбор промышленных протоколов до уровня команд: как межсетевой экран предотвращает атаки и сохраняет непрерывность техпроцессов
14.30-14.45	4.23	Системотехника-НН	Научно-производственное предприятие нового поколения «Системотехника-НН»
17.00-17.15	4.6	Цифровые решения	Подключение систем сетевой безопасности в АСУ ТП с использованием агрегирующего однонаправленного шлюза ФЕНИКС-ДИОД. Ключевые отличия и преимущества данного решения
17.15-17.30	4.10	АйЭсТи	Кибербезопасность АСУ ТП: Стратегии защиты критической инфраструктуры

Время	Стенд 2	Компания 2	Презентация
14.00-14.15	4.5	КСБ-Софт	Автоматизация оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ
14.15-14.30	4.14	RuSIEM	RuSIEM как ядро инфраструктуры информационной безопасности для АСУ ТП
14.30-14.45			
17.00-17.15	4.2	Русьтелетех RTT	Межсетевой экран RTT-M300F: защита промышленных сетей АСУ ТП
17.15-17.30	4.15	Акстел-Безопасность	HoneyCorn в АСУ ТП: ложные цели и реальные угрозы

РАСПИСАНИЕ ПРЕЗЕНТАЦИЙ НА СТЕНДАХ — 5 марта

Время	Стенд 1	Компания 1	Презентация
13.30-13.45	4.17	Индид	Комплексная защита identity
13.45-14.00	6.6	АМТ-ГРУП	Применение InfoDiode без потери управления сегментом: решения, практика, сценарии

Время	Стенд 2	Компания 2	Презентация
13.30-13.45	4.22	NGRSoftlab	Выход и регистрация нового ИБ-продукта, не имеющего аналогов в России
13.45-14.00	4.3	Itprotect	Создаем среду безопасности для АСУ ТП: как интегрировать промышленные системы со средствами защиты

Каталог продуктов и услуг участников экспозиции конференции «ИБ АСУ ТП КВО-2025»

Номер стенда 6.1

Название организации	Официальный сайт
ООО «АйТи БАСТИОН»	https://it-bastion.com/

Компетенции в области ИБ АСУ ТП

«АйТи Бастион» разрабатывает решения в области кибербезопасности с 2014 года. Специалисты компании глубоко погружены в сферу производства и постоянно улучшаю продукты и сервисы, ориентируясь на актуальные запросы операторов АСУ ТП. Флагманский продукт – платформа класса PAM (Privileged Access Management) СКДПУ НТ – успешно применяется в инфраструктурах крупных технологических предприятий, простой в работе которых может обернуться крупными бизнес-потерями.

Решение СКДПУ НТ помогает снизить проблемы человеческого фактора, сведя всю работу администраторов к принципу «нулевого доверия» (zero trust). PAM-платформа позволяет не только проводить расследования и мониторить несанкционированные действия привилегированных пользователей, но и предвосхищать инциденты ИБ.

Ещё одно решение от «АйТи Бастион» – средство информационного обмена «Синоникс». Данный программный комплекс предназначен для автоматизации передачи данных и файлов между системами из несвязанных сетей. Разработка актуальна в области ИБ АСУ ТП, поскольку позволяет обновлять оборудование в изолированных сегментах сети в автоматическом режиме, передавать данные мониторинга и управления без раскрытия структуры стыкуемых объектов сетевой инфраструктуры, а также противодействовать потенциально неизвестным уязвимостям на конечных системах путем сокрытия данных о сетях и информационных системах в их окружении.

Продукты и/или услуги

Название: СКДПУ НТ
Назначение: Защита доступа к информационным системам объектов КИИ и АСУ ТП для сохранения целостности ИТ-инфраструктуры, непрерывности технологических процессов, а также обеспечения выполнения мер защиты, изложенных регуляторами.
С помощью СКДПУ НТ осуществляется контроль и мониторинг действий внутренних администраторов и сотрудников подрядных организаций. PAM-платформа легко масштабируется на филиальную сеть предприятия, является отказоустойчивым продуктом.

Название: «Синоникс»
Назначение: Автоматизация процессов передачи файловой и потоковой информации между сетевыми приложениями. Организация автоматизированной однонаправленной или двунаправленной передачи данных и файлов между узлами двух сетей с сокрытием информацию об их окружении.
Ключевые возможности продукта:
Изоляция на физическом уровне
Архитектура и технологии «Синоникса» обеспечивают автоматизированную контролируемую передачу данных в режиме «точка-точка» как в одну, так и в обе стороны по протоколам TCP и UDP без прямой связанности узлов.
Физический контроль передачи
Физическая блокировка передачи «пусковыми» ключами и возможность с их помощью блокировать удаленное управление с доступом к конфигурированию только через консоль RS-232.
Разграничение зон ответственности
Встречный контроль, реализованный через управление двумя ответственными лицами для подтверждения прохождения данных. Несогласованные с обеих сторон правила игнорируются.
Проверка файлов перед передачей
Проверка размера и маски, а также целостности передаваемых объектов. Имеет встроенные механизмы дополнительной верификации по ICAP-протоколу.

Опыт работы в отраслях

- ☑ Нефтегаз
- ☑ Металлургия
- ☑ Химическая промышленность
- ☑ ОПК
- ☑ Энергетика
- ☑ Транспорт
- ☑ Ракетно-космическая промышленность
- ☑ Финансовый сектор и ретейл

Заказчики в сфере ИБ АСУ ТП

Номер стенда 6.3

Название организации	Официальный сайт
Компания «Актив»	https://www.aktiv-company.ru/

Компетенции в области ИБ АСУ ТП

Рутокен – направление Компании «Актив», одной из специализаций которой является разработка встраиваемых в оборудование заказчика программно-аппаратных криптографических средств аутентификации элементов системы и защиты каналов связи (линейка Рутокен Модуль).

Важной особенностью таких средств является использование аппаратно-реализованной криптографии с неизвлекаемой ключевой информацией. Это обеспечивает высокий уровень защиты от несанкционированного доступа и повышает надёжность системы в целом".

AKTIV.CONSULTING – направление Компании «Актив», консультанты которого реализуют проекты, требующие комплексной, системной экспертизы в сфере ИБ в интересах субъектов КИИ, кредитно-финансовых организаций, промышленных предприятий, представителей ТЭК, отечественных разработчиков ПО и организаций из других отраслей.

Продукты и/или услуги

Название: Рутокен Модуль

Назначение: линейка встраиваемых средств криптографической защиты информации, состоящее из набора интегрируемых программно-аппаратных средств обеспечения безопасности межмашинного взаимодействия (M2M), защиты автоматизированных систем управления технологическими процессами (АСУ ТП) и интернета вещей (IoT).

Экспертов AKTIV.CONSULTING привлекают для обеспечения:

- защиты информационных систем и инфраструктуры, включая анализ защищенности и пентесты, разработку ИБ-требований к ИС и внедрение требований по защите АСУ ТП;
- комплаенса для объектов КИИ (187-ФЗ\250УП\235 Приказ ФСТЭК РФ\239 Приказ ФСТЭК РФ\127 ПП РФ\152-ФЗ\63-ФЗ);
- управления функцией ИБ, включая формирование ИБ-службы, разработку стратегии по ИБ и оценку уровня зрелости ИБ;
- внедрения процесса безопасной разработки, включая анализ уязвимости ПО и разработку требований безопасности ПО;
- защиты конфиденциальной информации, интеллектуальной собственности и персональных данных.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☐ ОПК
☑ Энергетика	☐ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Названия заказчиков пока не готовы называть.

Номер стенда 6.4

Название организации	Официальный сайт
ООО «Киберпротект»	https://cyberprotect.ru/

Компетенции в области ИБ АСУ ТП

Киберпротект — российский разработчик ПО для защиты данных, резервного копирования и восстановления виртуальных, физических и облачных сред.

Резервное копирование данных в АСУ ТП обеспечивает защиту информации от потерь, вызванных сбоями оборудования, программными ошибками или внешними угрозами, такими как кибератаки. Наше решение хорошо интегрируется с SIEM-системами. Решение сертифицировано и подходит для значимых объектов КИИ 1 категории, ГИС 1 класса защищенности, АСУ ТП 1 класса защищенности, ИСПДн при необходимости обеспечения 1 уровня защищенности, и для ИС общего пользования II класса.

Наша DLP-система предназначена для предотвращения утечек конфиденциальной информации и обеспечения соблюдения норм безопасности. Она мониторит и контролирует данные на всех уровнях системы: от пользовательских устройств до серверов и сетевой инфраструктуры. DLP-решение может обнаруживать и блокировать несанкционированный доступ к данным, а также отслеживать их перемещение внутри и вне системы.

У нас большой опыт обеспечения доступности и целостности данных на предприятиях с АСУ ТП подтвержденный публичными кейсами.

Продукты и/или услуги

Название: Кибер Бэкап, Кибер Инфраструктура, Кибер Протего, Кибер Файлы

Назначение: **Кибер Бэкап** – это универсальное решение для резервного копирования и восстановления данных с защитой от вирусов-шифровальщиков.

Кибер Инфраструктура – позволяет сформировать универсальную, масштабируемую и защищенную гиперконвергентную ИТ-систему на основе стандартного серверного оборудования архитектуры x86-64, объединенного в группу, и обеспечивает централизованное управление всеми компонентами системы.

Кибер Протего – Российская DLP-система обеспечивает комплексную защиту от утечки данных с корпоративных компьютеров, серверов и из виртуальных сред

Кибер Файлы – универсальное решение для организации совместной работы и обмена файлами, позволяющее обеспечить структурированность, доступность и защищенность корпоративной информации в соответствии с нормативными требованиями и стандартами безопасности организации.

Опыт работы в отраслях

- ☑ Нефтегаз
- ☑ Металлургия
- ☑ Химическая промышленность
- ☑ ОПК
- ☑ Энергетика
- ☑ Транспорт
- ☑ Ракетно-космическая промышленность
- ☑ прочее

Заказчики в сфере ИБ АСУ ТП

Предоставить информацию нет возможности, NDA

Номер стенда 6.5

Название организации	Официальный сайт
UDV Group	https://udv.group/

Компетенции в области ИБ АСУ ТП

UDV Group — российский разработчик решений для эффективного и безопасного использования современных технологий. Группа объединяет продукты компаний «СайберЛимфа», «КИТ Разработка» и «КИТ» в экосистему кибербезопасности UDV. Продукты компаний «ФТ-СОФТ» и «ТриниДата» входят в направление цифровой трансформации.

Компетенции и возможности для обеспечения ИБ АСУ ТП:

- Глубокий анализ сетевого трафика с поддержкой разбора промышленных протоколов.
- Инвентаризация узлов промышленной сети.
- Выявление инцидентов информационной безопасности.
- Сбор и корреляция событий безопасности, поступающих в том числе из внешних источников.
- Анализ узлов промышленной сети на наличие уязвимостей.
- Контроль конфигураций узлов промышленной сети.
- Выявление аномального поведения ПЛК с помощью технологий машинного обучения.
- Контроль версий проектов ПЛК, их резервное копирование и восстановление.
- Межсетевое экранирование с поддержкой промышленных протоколов.
- Ответвление сетевого трафика (TAP).
- Мониторинг функционирования автоматизированных и информационных систем, в том числе, АСУ ТП.

В собственной лаборатории R&D – центре современных технологий обработки данных и кибербезопасности – сотрудники исследуют возможности использования искусственного интеллекта для предиктивной аналитики, применение которой позволяет не допускать инцидентов и простоев производства.

Продукты и/или услуги

Решения UDV Group созданы специально для защиты АСУ ТП и объектов КИИ, и учитывают особенности промышленных сетей. Их применение позволяет комплексно подходить к вопросам обеспечения кибербезопасности промышленных предприятий, применяя передовые технологические разработки и соблюдая требования регуляторов:

1. UDV DATAPK Industrial Kit – комплексное решение для мониторинга кибербезопасности и оперативного обнаружения инцидентов в промышленных сетях без негативного влияния на защищаемые системы.
2. UDV ITM – система зонтичного мониторинга, предназначенная для мониторинга функционирования распределенных автоматизированных и информационных систем различного назначения, в том числе АСУ ТП.
3. UDV DATAPK Version Control помогает специалистам АСУ ТП решить задачу централизованного хранения проектов ПЛК и отслеживания изменений в них, при необходимости — быстро отследить цепочку изменений и восстановить требуемую версию проекта ПЛК.
4. EDR for PLC – безагентный EDR для поведенческого анализа и контроля ПЛК в технологических сетях на основе машинного обучения.
5. UDV TAP Diode – диод данных и ответвитель трафика (TAP) с аппаратным байпасом. Предназначен для передачи сетевого трафика в системы мониторинга ИБ, а также для гарантированной односторонней передачи сетевого трафика между сегментами сети.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☑ прочее

Заказчики в сфере ИБ АСУ ТП

Информация предоставляется по запросу.

Номер стенда 6.6

Название организации	Официальный сайт
АМТ-ГРУП	www.amt.ru

Компетенции в области ИБ АСУ ТП

Проектирование и внедрение систем защиты информации технологических процессов, систем промышленной автоматизации и технологических сетей с учетом специфики отдельных сфер деятельности: транспорт, связь, энергетика, ТЭК, атомная энергия, оборонная, горнодобывающая, металлургическая и химическая промышленность.

Разработка и производство средств защиты информации, включая решения для обеспечения ИБ АСУ ТП.

Разработка и реализация стратегии импортозамещения ИБ-инфраструктуры систем промышленной автоматизации и технологических сетей с учетом требований по обеспечению технологической независимости.

Обеспечение ИБ при внедрении/модернизации/техническом перевооружении АСУ ТП, в ходе импортозамещения оборудования и ПО АСУ ТП, включая проработку и настройку штатных СЗИ ПО и оборудования АСУ ТП, защиту периметра технологических систем и сетей, реализацию эшелонированного подхода к обеспечению безопасности, изоляции и защите отдельных сегментов (систем/ устройств SCADA, DCS, PLC, SIS, RTU и др.).

Моделирование угроз и оценка рисков ИБ АСУ ТП.

Выявление и анализ технических уязвимостей, проведение анализа защищенности/ тестирования на проникновение систем промышленной автоматизации и технологических сетей.

Макетирование и тестирование СЗИ, в том числе совместно с заказчиками и производителями решений АСУ ТП, включая проверку работоспособности и совместимости СЗИ с отдельными компонентами защищаемых систем, проверку выполнения СЗИ заданных требований по защите информации.

Продукты и/или услуги

Название: InfoDiode

Назначение: Продукты

InfoDiode — линейка решений аппаратной и аппаратно-программной защиты, которые обеспечивают реализацию однонаправленной передачи данных, гарантируя защиту объекта на физическом уровне. Комплексы InfoDiode предназначены для организации обмена данными с критичными сегментами (например, АСУ ТП, КИИ, сегменты ГИС). InfoDiode может применяться для обеспечения безопасности АСУ ТП, АСДТУ в промышленности, энергетике, ТЭК, на транспорте, в государственных организациях, силовых структурах, в коммерческих предприятиях любых отраслей, использующих закрытые сегменты и сети.

Услуги

Проектирование и внедрение систем защиты информации технологических процессов, АСУ ТП, в том числе с применением специализированных решений: средства анализа трафика промышленных сетей для выявления отклонений и обнаружения сетевых атак, решения для защиты конечных точек промышленных систем от информационных угроз, системы однонаправленной передачи данных, средства контроля целостности конфигураций и др.

Опыт работы в отраслях

☐ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☐ ОПК
☐ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Концерн Росэнергоатом, РусГидро, РЖД, Евросибэнерго, АО «ТГК-16», Афипский НПЗ, Славянский НПЗ, Транснефть, Евросибэнерго, ERG (Евразийская Группа), «Альянс Алтын»

Название организации	Официальный сайт
АО НИП «ИНФОРМЗАЩИТА»	infosec.ru

Компетенции в области ИБ АСУ ТП

В компании «Информзащита» функционирует специализированный Центр промышленной безопасности, который сосредоточен на реализации комплексных проектов по защите автоматизированных систем управления технологическими процессами, систем управления производством и систем управления жизненным циклом сложных изделий. Специалисты интегратора обладают глубокой экспертизой, охватывающей не только информационную безопасность, но и особенности различных отраслей промышленности. Компетенции экспертов подтверждены признанными отраслевыми сертификатами. Компания обладает высокими партнерскими статусами среди ключевых российских вендоров и имеет своем портфеле порядка 200 партнеров.

С 2018 года мы являемся сертифицированным центром ГосСОПКА класса А в области обнаружения, предупреждения и ликвидации компьютерных атак.

Продукты и/или услуги

Название:

- Оценка текущего уровня защищенности промышленных объектов.
- Работы по категорированию объектов критической информационной инфраструктуры (КИИ).
- Взаимодействие со ФСТЭК по 187-ФЗ.
- Проектирование, внедрение и сопровождение системы защиты.
- Проработка решений с ведущими вендорами в области информационной безопасности.
- Проработка интегрированных решений с ведущими производителями оборудования АСУ ТП.
- Консультирование по сертификации программных и аппаратных компонентов.
- Исследование встроенных механизмов защиты промышленных систем.
- Консультирование проектных организаций по вопросам информационной безопасности проектируемых систем.
- Анализ защищенности сетей и систем, тесты на совместимость ПО и СЗИ.
- Проведение тестов на проникновение в промышленных сетях и организация киберучений.
- Обучение специалистов Заказчика новым технологиям и средствам защиты.
- Подключение к ГосСОПКА.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

ПАО «НЛМК», ПАО «Фосагро», ПАО «Селигдар», АО «Уральская сталь», ПАО «РКК Энергия», АО «Иркутсккабель», ПАО «Авиационный комплекс им. С.В.Ильюшина», АО «Концерн ВКО “Алмаз-Антей”», АО «ВМЗ».

Название организации	Официальный сайт
ООО «АТОМ БЕЗОПАСНОСТЬ»	https://www.staffcop.ru

Компетенции в области ИБ АСУ ТП

Система для расследования инцидентов внутренней информационной безопасности Staffcop Enterprise состоит из двух частей: сервера и службы-агента.

Функционал включает в себя следующие возможности:

- **Контроль переписки в почте и мессенджерах**
  Связка «кейлоггер-приложение/сайт-скриншот» позволяет отслеживать переписки в любых системах обмена сообщениями, онлайн-чатах, соцсетях и прочих коммуникациях через интернет.
- **Контроль подключения внешних устройств**
  Регулирует предоставление каждому конкретному пользователю доступа к USB-входам. Анализ статистики использования принтеров, МФУ на предприятии и информации, отправленной на печать.
- **Ограничения доступа к приложениям**
  Блокировка ПО на компьютере осуществляется как на отдельных устройствах, так и для конкретных групп пользователей. Доступно ограничение действий на сайтах, не относящихся к работе.
- **Отчеты по инвентаризации установленного оборудования**
  Отчеты по инвентаризации установленного оборудования, WiFi-подключений и ПО. Реакция на изменения конфигурации и контроль установки нерегламентированных приложений.
- **Уведомление при обнаружении угроз**
  Уведомления специалистов по почте или в Telegram об обнаруженных инцидентах безопасности, гибкие настройки доступа администраторов системы.
- **Текстовый поиск**
  Все заголовки окон, названия документов, буфер обмена, содержимое перехваченных файлов и др. попадает в текстовую базу Staffcop Enterprise. После индексации событий в базе данных возможен полнотекстовый поиск этой информации.

Продукты и/или услуги

Название: Staffcop Enterprise

Назначение: **Staffcop Enterprise – система расследования инцидентов внутренней информационной безопасности (событий, связанных с действиями пользователей на их рабочих станциях). Staffcop обеспечивает комплексный контроль и анализ активности сотрудников для проактивного расследования и предотвращения инцидентов информационной безопасности. Система адаптирована для выявления и расследования утечек данных, мошенничества и других инцидентов, произошедших из-за действий сотрудников.**
Под защитой Staffcop Enterprise больше 250 000 компьютеров в 20 отраслях бизнеса, промышленности, крупных госструктурах в 40 странах мира.
Staffcop Enterprise – единственный из продуктов РФ рынка ИБ, который попал в рейтинг Forbes Advisor «Лучшее программное решение контроля действий сотрудников» в 2023 и 2024 годах по лучшему соотношению цены и качества для крупных компаний.
Staffcop Enterprise внесен в Единый реестр Российского ПО под № 8828.
Сертифицирован ФСТЭК России, сертификат № 4234. Соответствует требованиям документов: требования к СКН, профиль защиты СКН (контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ. СКН. П4. П3), 3Б.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☑ прочее

Заказчики в сфере ИБ АСУ ТП

Название организации	Официальный сайт
ООО «НПП «Системотехника-НН»	Systec-nn.ru

Компетенции в области ИБ АСУ ТП

На сегодняшний день специалисты предприятия обеспечивают выполнение технических требований, необходимых для получения лицензии ФСТЭК в области информационной безопасности: сотрудники проходят специализированное обучение и повышение квалификации, на предприятии оборудуется помещение с требуемыми характеристиками для выполнения соответствующих работ, приобретаются необходимые аппаратно-программные средства. После получения лицензии предприятие сможет осуществлять проектирование разделов информационной безопасности, проводить аудит уже существующих систем, выполнять пусконаладочные работы программно-аппаратных средств информационной безопасности.

Продукты и/или услуги

Название: Производство ПЛК и радиоэлектронных изделий, разработка и проектирование АСУ ТП (включая раздел информационной безопасности), разработка программного обеспечения, монтажные и пусконаладочные работы АСУ ТП (включая программно-аппаратные средства информационной безопасности). А также аудит существующих систем информационной безопасности

Назначение: Полный комплекс работ по автоматизации технологических процессов в различных областях промышленности: проектирование, включая средства информационной безопасности, разработка и изготовление оборудования, разработка необходимого программного обеспечения, монтаж и пусконаладочные работы АСУ ТП на объектах Заказчиков.

Опыт работы в отраслях

☐ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☐ ОПК
☐ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда 4.2

Название организации	Официальный сайт
RTT	https://ртт.рф

Компетенции в области ИБ АСУ ТП

RTT – разработчик и производитель надежных и безопасных сетевых решений. Наше оборудование позволяет создавать функциональные и защищенные сети, обеспечивая защиту периметра ИТ-инфраструктуры АСУ ТП, объектов КИИ и промышленных сетей от атак и угрозы различного класса и вектора.

Продукты и/или услуги

Название: Универсальный промышленный шлюз безопасности RTT-M300F

Назначение: RTT-M300F предназначен для защиты периметра ИТ-инфраструктуры АСУ ТП, объектов КИИ и промышленных сетей от несанкционированного доступа, попыток атак, вторжений, вредоносного трафика и других киберугроз. Промышленное исполнение и архитектура устройства предусматривает повышенную отказоустойчивость и соответствует стандартам информационной безопасности, что делает их оптимальным решением для надежной защиты сегментов промышленной сети.

Опыт работы в отраслях

☐ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☑ ОПК
☑ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда **4.3**

Название организации	Официальный сайт
iTPROTECT	www.itprotect.ru

Компетенции в области ИБ АСУ ТП

Компания оказывает комплекс услуг для обеспечения безопасности промышленных предприятий: от аудита, категорирования и аттестации объектов критической информационной инфраструктуры (КИИ) до внедрения решений «под ключ» для защиты различных сегментов сети и систем, включая АСУ ТП.

За 16 лет работы эксперты iTPROTECT реализовали 100+ проектов в ключевых отраслях промышленности: от нефтегазовой и химической до машиностроения и энергетики.

Решения и услуги iTPROTECT для промышленного сектора защищают предприятия от кибератак на оборудование, сеть, SCADA-системы и прочие элементы промышленной инфраструктуры.

Продукты и/или услуги

1. Тестирование на проникновение (Pentest)
В рамках тестирования происходит оценка уровня защищенности и обнаружение уязвимостей промышленной инфраструктуры. По итогам специалисты iTPROTECT предоставляют отчет обо всех обнаруженных проблемах и формируют рекомендации по их устранению.

2. Консалтинг в области защиты КИИ
Эксперты iTPROTECT помогают наладить учет и обеспечить безопасность объектов КИИ в полном соответствии с требованиями законодательства (187-ФЗ и подзаконные акты) и актуального ландшафта угроз. В портфеле полный комплекс услуг: от обследования процессов и категорирования объектов КИИ до моделирования угроз и проектирования системы безопасности.

3. Защита узлов в промышленной сети (Industrial Endpoint Protection)
Решение для защиты конечных узлов (серверов, рабочих станций, операторских панелей) направлено на предотвращение атак, блокировку вредоносного ПО, контроль целостности файлов и предотвращение несанкционированных изменений. Специализированные инструменты адаптированы под промышленные системы и не влияют на стабильность технологических процессов.
Продукты: Kaspersky Industrial CyberSecurity for Nodes («Лаборатория Касперского»).

4. Мониторинг технологического трафика (INAD)
Решение помогает оперативно выявить факты вмешательства в промышленную сеть. Системы этого класса анализируют протоколы промышленной сети и предупреждают о киберугрозах, сбоях или подозрительных конфигурациях команд управления. Это позволяет минимизировать риски, повысить отказоустойчивость инфраструктуры и обеспечить контроль над безопасностью технологических процессов.
Продукты: PT Industrial Security Incident Manager (Positive Technologies),
Kaspersky Industrial CyberSecurity for Networks («Лаборатория Касперского»).

5. Промышленные межсетевые экраны (Industrial firewall)
Промышленные межсетевые экраны обеспечивают фильтрацию трафика, контроль доступа и защиту от угроз. Решение определяет специализированные промышленные протоколы и предотвращает несанкционированное вмешательство в работу SCADA, PLC и других критичных узлов. Это снижает риски атак и повышает киберустойчивость производства.
Продукты: ПАК ViPNet Coordinator IG (ИнфоТеКС), Next-Generation Firewall (UserGate)

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда 4.4

Название организации	Официальный сайт
АО «Инфосистемы Джет»	https://jet.su

Компетенции в области ИБ АСУ ТП

«Инфосистемы Джет» обеспечивает комплексную защиту всех сегментов технологической и корпоративной сети, оказывает полный цикл услуг по обеспечению объектов КИИ системами информационной безопасности.

Эксперты проводят комплекс мероприятий для оценки текущего состояния активов субъекта КИИ, в том числе: обследование объектов, оценка уровня зрелости процессов и мер по защите информации, разработка стратегии развития защиты АСУ ТП, категорирование и перекатегорирование объектов КИИ, проводят оценку соответствия требованиям нормативной документации, а также применяют централизованный подход к проектированию и построению систем безопасности, используя комплексную методологию, охватывающую не только внедрение наложенных средств защиты информации, но и модернизацию вычислительной, сетевой и инженерной инфраструктуры.

Продукты и/или услуги

Название:
Назначение:

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☐ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☑ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда 4.5

Название организации	Официальный сайт
КСБ-СОФТ	https://ksb-soft.ru

Компетенции в области ИБ АСУ ТП

Компания обладает широким набором различных компетенций в части информационной безопасности АСУ ТП. В штате подразделения, занимающегося защитой объектов КИИ и АСУ ТП, работают высококвалифицированные специалисты с богатым опытом работы по проектированию и наладке АСУ ТП, а также специалисты по информационной безопасности с профильным образованием. Основные компетенции: понимание специфики АСУ ТП; знание стандартов и нормативных требований; анализ угроз и сценариев атак; проектирование, внедрение и испытания комплексных систем ИБ АСУ ТП, мониторинг событий ИБ, безопасная разработка ПО.

Продукты и/или услуги

1) Безопасность АСУ ТП и объектов КИИ.
2) Услуги центра мониторинга SOCRAT (SOC).
3) Внедрение процессов безопасной разработки (SDL)

Назначение: 1) Комплексное решение по обеспечению ИБ КИИ Российской Федерации.
2) Центр мониторинга SOCRAT является корпоративным центром ГосСОПКА и предлагает полный комплекс услуг по мониторингу и реагированию на инциденты ИБ.
3) Комплексная технология создания и развития программных продуктов, снижающая риски от вредоносного воздействия в течение всего жизненного цикла.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

ПАО «Россети», ПАО «СИБУР Холдинг», ПАО «Интер РАО», ПАО «ФосАгро», ПАО «Роснефть», АО «Сахаэнерго», ПАО «НОВАТЭК», ФГБУ «Канал имени Москвы».

Номер стенда 4.6

Название организации	Официальный сайт
АО «НПП «Цифровые решения»	https://dsol.ru

Компетенции в области ИБ АСУ ТП

Российский разработчик и производитель сетевого оборудования для подключения средств информационной безопасности. Оборудование включено в реестр Минпромторга России, имеет сертификацию ФСТЭК России по 4 уровню доверия, а также соответствует критериям доверенных ПАК. Решения компании успешно применяются в инфраструктурах энергетических компаний, нефтегазовой и горнодобывающей промышленности.

Продукты и/или услуги

Название: Ответвители сетевого трафика DS Optic-TAP и DS Copper-TAP
Однонаправленный шлюз Феникс-ДИОД
Брокеры сетевых пакетов DS Integrity
Сетевые байпасы DS Copper-Bypass

Назначение: Продукты
Сетевое оборудование от компании «Цифровые решения» используется для зеркалирования трафика, его агрегации и однонаправленной передачи во внешний контур для дальнейшей обработки. Оборудование позволяет на аппаратном уровне изолировать сеть АСУ ТП от воздействия со стороны средств мониторинга. Для оптимизации данных, собранных с большого количества сегментов, используются пакетные брокеры.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☐ Химическая промышленность	☐ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Не можем разглашать

Номер стенда 4.7

Название организации	Официальный сайт
Газинформсервис	www.gaz-is.ru

Компетенции в области ИБ АСУ ТП

- Экспертиза требований законодательства России в сфере АСУ ТП.
- Консалтинг по ИБ АСУ ТП.
- Аудит ИБ АСУ ТП, включая тестирование на проникновение.
- Создание системы безопасности АСУ ТП.
- Аутсорсинг корпоративного центра ГосСОПКА для АСУ ТП.
- Разработка организационно-распорядительных документов по безопасности АСУ ТП.
- Сопровождение, техническое обслуживание, техническая поддержка системы безопасности АСУ ТП.
- Проведение совместных работ с производителями АСУ ТП по безопасному и эффективному взаимодействию средствам защиты информации с АСУ ТП.

Продукты и/или услуги

Название:
Назначение:

Опыт работы в отраслях

☐ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☐ ОПК
☐ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда 4.8

Название организации	Официальный сайт
InfoWatch	https://www.infowatch.ru

Компетенции в области ИБ АСУ ТП

ГК InfoWatch – ведущий российский разработчик решений в области информационной безопасности и защиты данных. ГК InfoWatch была основана в 2003 году Натальей Касперской и сегодня является одним из лидеров рынка защиты данных.

Два ключевых направления – это линейка продуктов по защите данных и средства защиты критической информационной инфраструктуры предприятий.

Решения ГК InfoWatch прошли сертификацию на соответствие требованиям ФСБ, ФСТЭК РФ и отраслевым стандартам, включены в Реестр отечественного ПО.

Продукты и/или услуги

Название: InfoWatch Центр расследований**Назначение: Продукты**
InfoWatch Центр расследований – единая система защиты данных вместо разрозненных СЗИ: защита от утечек, контроль хранения и прав доступа, мониторинг действий сотрудников, контроль использования внешних устройств, визуальная аналитика и граф связей, поведенческая аналитика и группы риска.

Название: InfoWatch ARMA
InfoWatch ARMA – отечественная система для обеспечения кибербезопасности АСУ ТП и защиты сетевой инфраструктуры бизнеса в соответствии с приказом ФСТЭК РФ № 239.

Опыт работы в отраслях

☑ Нефтегаз	☐ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Публичные упоминания названий компаний ограничены по соображениям конфиденциальности.

Номер стенда 4.9

Название организации	Официальный сайт
АО «ИнфоТеКС»	Infotecs.ru

Компетенции в области ИБ АСУ ТП

Комплексное обеспечение безопасности АСУ ТП, ИСУЭ, M2M и IIoT-систем.
– Сертифицированные сетевые средства защиты для обеспечения безопасности передаваемых в информационно-телекоммуникационных системах данных на всех уровнях АСУ ТП.
– Сертифицированные встраиваемые законченные средства криптографической защиты информации для интеграции с защищаемыми устройствами АСУ ТП.

Обучение и поддержка:
– Консультации и техническая поддержка.
– Обучение специалистов в области ИБ в Учебном центре «ИнфоТеКС».
– Подготовка кадров: специализированные лаборатории и курсы повышения квалификации в вузах России.

Продукты и/или услуги

– Шлюзы безопасности для защиты промышленных сетей ViPNet Coordinator IG.
– Шлюзы безопасности – межсетевые экраны следующего поколения ViPNet Coordinator HW 5.
– Индустриальный криптомодуль для защиты интеллектуальных устройств автоматики ViPNet SIES Core.
– Миниатюрный крипточип для защиты конечных устройств АСУ, IIoT и приборов учета ViPNet SIES Core Nano.
– Программное СКЗИ для устройств верхнего уровня АСУ ТП, IIoT и ИСУЭ ViPNet SIES Unit.

Опыт работы в отраслях

☐ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☐ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☑ прочее

Заказчики в сфере ИБ АСУ ТП

Номер стенда **4.10**

Название организации	Официальный сайт
ООО «АйЭсТи»	https://zaschita-it.ru/company/

Компетенции в области ИБ АСУ ТП

13 лет опыта в сфере промышленной безопасности. Команда сертифицированных экспертов в сферах систем мониторинга, инфраструктурных решений, документального обеспечения.

Продукты и/или услуги

Выстраивание системы результативной кибербезопасности для АСУ ТП

Назначение: Мы выстраиваем результативный кибербез с помощью актуализации категории КИИ через сегментацию ИС. Это эффективный метод построения ИБ, т. к. серьезно усложняет процесс возможной атаки и уменьшает затраты на СЗИ. Наш комплексный подход с предварительным тестированием и макетированием инфраструктуры заказчика, детальной подготовкой к внедрению и бэкапами гарантирует построение надежной защиты и бесперебойное производство.

Опыт работы в отраслях

☑ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☑ ОПК
☑ Энергетика	☐ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

ООО «СВГК», ГБУЗ «СОДКБ им. Н.Н. Ивановой», СОКБ им. В.Д. Середавина

Номер стенда **4.11**

Название организации	Официальный сайт
ООО «ПВС»	pvs-studio.ru

Компетенции в области ИБ АСУ ТП

1. Поиск критических ошибок, опечаток и потенциальных уязвимостей в исходном коде программ.
2. Проверка соответствия исходного кода индустриальным стандартам MISRA C, MISRA C++ и AUTOSAR Coding Guidelines.
3. Выдача предупреждений анализатора с привязкой к CWE (Common Weakness Enumeration) и SEI CERT, что упрощает интерпретацию информации о потенциальных уязвимостях.
4. Технологическое сотрудничество с разработчиками российских ОС реального времени.

Продукты и/или услуги

Название: PVS-Studio

Назначение: PVS-Studio – это инструмент для выявления ошибок и потенциальных уязвимостей в исходном коде программ, написанных на языках C, C++, C# и Java.

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☐ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

ООО «СВД ВС», АО «Нефтеавтоматика», АО «ЭЛАРА», ООО «ПРЕДПРИЯТИЕ “ЭЛТЕКС”», ООО «НПП «Итэлма», ООО «НПО “ВЫМПЕЛ”»

Номер стенда 4.12

Название организации

ООО «СВД ВС»

Официальный сайт

www.kpda.ru

СВД Встраиваемые Системы

Компетенции в области ИБ АСУ ТП

- Разработка встроенных средств защиты информации от несанкционированного доступа по требованиям НПА ФСТЭК России по требованиям ИТ.ОС.А2.ПЗ и ИТ.ОС.В2.ПЗ к ОС.
- Разработка средств межсетевого экранирования.

Продукты и/или услуги

Название: Операционная система реального времени «Нейтрино»

Назначение: «Нейтрино» – POSIX-совместимая встраиваемая ОС жесткого реального времени.

Преимущества ОСРВ «Нейтрино»:

- **Микроядерная отказоустойчивая архитектура реального времени.**
- **Поддержка многих отечественных и мировых процессорных платформ и архитектур.**
- **Развитые инструментальные средства.**
- **Высокая отработанность.**
- **Соответствие требованиям функциональной безопасности.**

Опыт работы в отраслях

☑ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Концерн Росэнергоатом, РусГидро, РЖД, Евросибэнерго, АО «ТГК-16», Афипский НПЗ, Славянский НПЗ, Транснефть, Евросибэнерго, ERG (Евразийская Группа), «Альянс Алтын»

Номер стенда 4.14

Название организации

RuSIEM

Официальный сайт

www.rusiem.com

RUSIEM

Компетенции в области ИБ АСУ ТП

Продукты и/или услуги

- RuSIEM – коммерческая версия системы класса SIEM, включающая корреляцию в режиме реального времени, визуализацию данных и поиск по ним, долгосрочное хранение сырых и нормализованных событий, инцидент-менеджмент и отчеты
- RuSIEM Analytics – модуль для коммерческой версии RuSIEM, дополняемый возможностями ML (Machine learning), DL (data learning), по визуализации данных
- RuSIEM Monitoring – система мониторинга ИТ-инфраструктуры с возможностью удаленного администрирования и встроенной системой HelpDesk
- RuSIEM IoC – модуль выявления угроз для корпоративных устройств на основе индикаторов компрометации

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

Концерн Росэнергоатом, РусГидро, РЖД, Евросибэнерго, АО «ТГК-16», Афипский НПЗ, Славянский НПЗ, Транснефть, Евросибэнерго, ERG (Евразийская Группа), «Альянс Алтын»

Номер стенда 4.15

Название организации	Официальный сайт
ООО «Акстел-Безопасность»	https://axxtel.ru

Компетенции в области ИБ АСУ ТП

Акстел-Безопасность – экспертная компания с опытом более 10 лет в сфере информационной безопасности.

Компания сотрудничает с лидерами рынка, включая финансовые организации, и имеет партнерские статусы с ведущими производителями средств защиты информации.

Высокий уровень компетенций сотрудников подтвержден международными сертификатами и опытом реализации сложных проектов.

На стенде будет представлена группа компаний Axxtel:

- **Акстел-Безопасность** расскажет о подходах к выбору стратегии защиты ИТ-инфраструктуры и внедрению комплексных решений по безопасности.
- **Сибирская академия информационной безопасности** покажет платформу для рассылок социальной инженерии и обучения сотрудников.
- **HoneyCorn** продемонстрирует свою систему по созданию ловушек для злоумышленников.

Продукты и/или услуги

Название:
Назначение:

Опыт работы в отраслях

☑ Нефтегаз	☑ Металлургия	☑ Химическая промышленность	☐ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП

НПП «Радиосвязь», «Сибирский Цемент», ЦФТ, «Распадская угольная компания», «Новая Горная УК», «НефтеХимСервис», «Стройсервис», «ТопПром», АТС, «Евраз» и др.

Номер стенда 4.16

Название организации	Официальный сайт
ДиалогНаука	https://dialognauka.ru

Компетенции в области ИБ АСУ ТП

- Выявление и категорирование объектов критической информационной инфраструктуры.
- Разработка моделей угроз безопасности объектов КИИ.
- Проектирование и внедрение системы обеспечения безопасности значимых объектов КИИ.
- Защита АСУ ТП.
- Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов КИИ.
- Техническое сопровождение и поддержка СЗИ.

Продукты и/или услуги

Название:
Назначение:

Опыт работы в отраслях

☑ Нефтегаз	☐ Металлургия	☑ Химическая промышленность	☑ ОПК
☑ Энергетика	☑ Транспорт	☑ Ракетно-космическая промышленность	☑ прочее

Заказчики в сфере ИБ АСУ ТП

За 2023–2024 годы компания реализовала несколько десятков проектов по защите АСУ ТП для компаний из различных отраслей.

Номер стенда 4.17

Название организации	Официальный сайт
Индид	https://indeed-company.ru

Компетенции в области ИБ АСУ ТП

Компания Индид – российский вендор программного обеспечения. Наши программные комплексы предназначены для решения задач по управлению цифровыми сертификатами и их носителями, доступом пользователей к информационным ресурсам компаний и организаций.

Продукты и/или услуги

Название: **Indeed Access Manager** – Продукт обеспечивает многофакторную аутентификацию сотрудников и создает единую точку доступа к ИТ-системам компании
Ideed Privileged access Manager – Управляет доступом привилегированных пользователей к ИТ-системам компании
Indeed Certificate Manager – Управляет жизненным циклом ключевых носителей и цифровых сертификатов, ведёт журнал СКЗИ, автоматизирует рутинные задачи
Identity threat detection and response – Адаптивная защита учетных данных в корпоративной сети

Опыт работы в отраслях

- [x] Нефтегаз
- [x] Металлургия
- [x] Химическая промышленность
- [x] ОПК
- [x] Энергетика
- [x] Транспорт
- [x] Ракетно-космическая промышленность
- [ ] прочее

Заказчики в сфере ИБ АСУ ТП

«Вертолеты России», «Черкизово», ЕВРАЗ, «Металлоинвест», «РусГидро – Ленгидропроект», Кока Кола Coca-Cola – Мултон Партнерс, СЗРЦ «Алмаз-Антей» (АО «ГОЗ Обуховский завод»)

Номер стенда 4.20

Название организации	Официальный сайт
УЦСБ (Уральский центр систем безопасности)	https://www.ussc.ru

Компетенции в области ИБ АСУ ТП

Компания УЦСБ предлагает полный спектр услуг по обеспечению безопасности промышленных систем автоматизации и управления:

- аудит АСУ ТП, включающий в себя идентификацию и классификацию активов, проведение тестов на проникновение, проведение анализа истории инцидентов, оценку рисков, разработку стратегии развития системы безопасности;
- создание комплексного решения по обеспечению безопасности АСУ ТП, включая работы по обследованию, построению модели угроз и оценки рисков, формированию требований с учетом международных стандартов и лучших практик, разработку проектной и рабочей документации, ввод в действие комплексной системы безопасности;
- сервисная поддержка, включающая в себя комплекс услуг по техническому сопровождению систем безопасности.

Продукты и/или услуги

Название: USSC-SOC
Назначение: Мониторинг и реагирование на инциденты ИБ в АСУ ТП

Название: DevSecOps
Назначение: Безопасная разработка

Название: Решения системной интеграции
Назначение: Контроль конфигураций и управление изменениями

Название: Сервисная поддержка
Назначение: Обеспечение непрерывной работы программно-аппаратных комплексов и систем, поддержание максимального уровня защиты информационных ресурсов компании

Опыт работы в отраслях

- [x] Нефтегаз
- [x] Металлургия
- [x] Химическая промышленность
- [x] ОПК
- [x] Энергетика
- [x] Транспорт
- [x] Ракетно-космическая промышленность
- [ ] прочее

Заказчики в сфере ИБ АСУ ТП

ЕВРАЗ, «Норникель», «Сибинтек», СИБУР, «Юнипро», «Лукойл», «Газпром», «Салым Петролеум Девелопмент», АГРОЭКО, «Уралвагонзавод»

Номер стенда 4.22

Название организации	Официальный сайт
NGR Softlab	https://www.ngrsoftlab.ru

NGRSOFTLAB

Компетенции в области ИБ АСУ ТП

Мониторинг и реагирование на инциденты информационной безопасности, разработка защищенного программного и аппаратного обеспечения, мониторинг действий, обнаружение аномалий и предотвращение угроз.

Продукты и/или услуги

Название:
1. SIEM-система Alertix
2. PAM-система Infrascope
3. Аналитическая платформа Dataplan
4. Система управления безопасностью файлов

Назначение:
1. Мониторинг и учет инцидентов ИБ, управление журналами ИТ-систем, контроль ресурсно-сервисных моделей, поддержка управления изменениями данных.
2. Контроль привилегированных учетных записей, управление привилегированным доступом, мониторинг и протоколирование действий.
3. Работа с данными, поведенческая аналитика, ролевое моделирование, выявление аномалий.
4. Оркестрация проверки файлов в СЗИ, очистка файлов методом реконструкции

Опыт работы в отраслях

☑ Нефтегаз	☐ Металлургия	☐ Химическая промышленность	☐ ОПК
☑ Энергетика	☑ Транспорт	☐ Ракетно-космическая промышленность	☐ прочее

Заказчики в сфере ИБ АСУ ТП