



XIV КОНФЕРЕНЦИЯ

«Информационная безопасность
АСУ ТП КВО»

ПРОГРАММА

3-4 марта 2026 г.
г. Москва



XIV КОНФЕРЕНЦИЯ

«Информационная безопасность АСУ ТП КВО»

3-4 марта 2026 г., г. Москва

Генеральный партнер



Стратегический партнер



Бронзовый партнер



Корпорация ЭЛАР

Хрустальный партнер



Партнеры



Партнеры второго дня



Экспоненты



Информационные партнеры

При информационной поддержке



Защита АСУ ТП без риска для управления процессами

Как современные ИБ-решения выявляют угрозы и контролируют инфраструктуру, не влияя на работу систем



Безопасность АСУ ТП всегда требует баланса между защитой и стабильной работой систем. Любое неверное вмешательство может дорого обойтись, поэтому внедрение средств ИБ на действующих объектах требует точного, аккуратного подхода. О том, как строить защиту без влияния на критические контуры, почему прицельные атаки вытесняют массовые и какую роль в этом играют РАМ-системы, интеграция с SIEM и AI, мы поговорили с экспертом **Константином РОДИНЫМ**, заместителем директора по развитию бизнеса компании «АйТи Бастион».

– **Какие основные технические и организационные вызовы возникают при внедрении ваших решений на действующих объектах? Как вы минимизируете риски воздействия на непрерывность технологического процесса?**

– Внедрение РАМ-системы и защищенного информационного обмена в действующих АСУ ТП на примере наших решений всегда осложняется требованиями к непрерывности технологического процесса, гетерогенностью и зачастую возрастом промышленной среды, а также очень высокой ценой любой ошибки.

Если говорить о ключевых технических вызовах, то это, как правило, большое разнообразие

промышленных протоколов и жесткие ограничения на любые активные воздействия на технологические узлы. Именно поэтому наша РАМ-платформа СКДПУ НТ чаще всего применяется в безагентской модели с настроенными паттернами оповещения об опасных действиях и не вмешивается в работу АСУ ТП, а программный комплекс «Синоникс» встраивается в существующие каналы обмена без изменения логики системы, обеспечивая контролируемый, в том числе односторонний, обмен данными или файлами без установки ПО на критические компоненты.

РАМ-система используется для административных и сервисных сессий подключений, а также для контроля и анализа активности сотрудников на предмет неправомерных действий. Средство информационного обмена между изолированными сетями применяется для передачи данных, точечной автоматизации процессов обмена телеметрией, служебной информацией и файлами, с четким разделением зон

ответственности между ИБ, ИТ и АСУ ТП и, как следствие, снижением рисков, связанных с человеческим фактором.

С организационной точки зрения основное зачастую – это конфликт приоритетов между службами. Он снимается за счет прозрачных регламентов доступа, конфигурации аварийного доступа, понятного распределения ответственности и такого контроля, который не блокирует работу, а сохраняет привычный режим, помогая при этом принимать решения. Отдельной задачей часто остается отсутствие формализованного управления привилегированным доступом, и здесь мы идем эволюционным путем – без ломки существующей архитектуры и привычных процессов. Поэтому оба наших решения внедряются поэтапно: сначала аудит и наблюдение без какого-либо влияния на технологический процесс, и только потом – аккуратное, ограниченное внедрение элементов принудительного контроля, разумеется, где это допустимо.

– Насколько глубоко ваше решение СКДПУ НТ может интегрироваться с другими ключевыми системами на промышленном объекте, например с SIEM-системами, системами мониторинга технологических процессов или системами управления инцидентами?

– В СКДПУ НТ реализовано свыше десятка интеграций с наиболее востребованными системами безопасности на промышленных объектах. События обрабатываются SIEM «из коробки», мы обмениваемся данными с промышленными IDS для предотвращения несанкционированного доступа, и на этой основе автоматически поднимаем инциденты удаленных подключений в обход установленных правил. На практике это показывает отличный результат в сборе и анализе аномальных подключений и повышает прозрачность работы с точки зрения безопасности.

Также у нас реализована интеграция с системами управления инцидентами и реагирования. В результате выстраивается единый контур безопасности, который мы последовательно развиваем уже несколько лет. Мы активно взаимодействуем с другими игроками рынка, понимая, что один класс решений не покрывает все задачи, и фокусируемся на том, чтобы наши продукты легко и нативно встраивались в общую комплексную систему защиты заказчика.

– Как вы видите эволюцию угроз для АСУ ТП в России? Поменялся ли профиль типичного нарушителя за последние 5 лет?

– За последние пять лет атаки на АСУ ТП существенно эволюционировали в сторону большего профессионализма атакующих. Если раньше преобладали массовые атаки: рассылки, сканирования, веерное применение простых эксплойтов, то сегодня злоумышленники действуют прицельно, с четким выбором целей и очень тщательным подходом к реализации атак.

АСУ ТП перестали быть побочной целью массового киберкриминала с мотивацией быстрого заработка или случайного интереса. На первый план вышли целенаправленные атаки на конкретные предприятия – выведение объектов из строя, профессиональный шпионаж и глубокое внедрение в инфраструктуру. Для этого используются APT-атаки, многоступенчатые сценарии, человеческий фактор и цепочки поставок. Параллельно вырос и уровень защищенности промышленных объектов, поэтому стандартные средства взлома перестали работать. Проникновение в АСУ ТП теперь требует времени, подготовки и глубины знаний, атаки же все чаще нацелены именно на узлы управления и поддержки технологического процесса, а не только на ИТ-сегменты.

приближен к уровню защищаемых объектов, с которыми они взаимодействуют. Иначе общий контур безопасности теряет эффективность.

– В чем вы видите конкурентное преимущество вашей компании в сравнении с другими российскими вендорами на рынке?

– Конкурентное преимущество нашей компании заключается в профессионализме команды и способности решать нестандартные сложные задачи. Именно такие задачи сегодня возникают на рынке в условиях высокой неопределенности. Мы можем решать то, к чему конкуренты зачастую не готовы, и видим развитие рынка чуть дальше. Решения «АйТи Бастион» позволяют точно контролировать процессы в рамках

Конкурентное преимущество нашей компании заключается в профессионализме команды и способности решать нестандартные сложные задачи.

Соответственно, изменился и профиль типичного нарушителя. Сегодня это организованные группы с высоким уровнем профессионализма, использующие сложные, не скриптовые техники, максимально приближенные к легитимным действиям персонала, вплоть до ручной эксплуатации уязвимостей и перемещения. Их цель – как можно дольше оставаться незаметными и последовательно, шаг за шагом, углубляться в инфраструктуру.

В этих условиях изолированных средств защиты уже недостаточно. Продукты информационной безопасности должны работать во взаимодействии друг с другом и охватывать не только сам объект, но и цепочки поставок. Уровень защищенности таких цепочек должен быть максимально

единой комплексной ИБ-системы. Именно поэтому мы еще много лет назад одни из первых начали выстраивать технологическое взаимодействие с лидерами российского рынка ИБ, когда это еще не было мейнстримом.

Кроме того, большинство наших продуктов развивается не по моде иностранных рынков, а под реальные потребности заказчиков и инфраструктур, в первую очередь – российских. Мы учитываем конкретные задачи клиентов и стараемся максимально эффективно решать их в рамках разрабатываемых продуктов.

– «Синоникс» и СКДПУ НТ применяются в совершенно разных отраслях – от медицины до тяжелой промышленности. Как технически реализуется

адаптация одного продукта под столь разные технологические среды и профили угроз?

– Адаптация продуктов достигается за счет широких технических возможностей и высокого профессионализма нашей команды. Многолетний опыт позволяет гибко подходить к требованиям разных отраслей и типов угроз. Мы понимаем, как защищать объекты АСУ ТП, ИТ-объекты и обеспечивать точечный информационный обмен между сетями, которые ранее были изолированы, но связь между которыми требуется для бизнеса. Технические возможности продуктов «АйТи Бастион» позволяют реализовать сложные проекты: ограничивать прямой доступ к системам, контролировать передачу файлов и буфер обмена, жестко регулировать удаленные привилегированные подключения, сохраняя при этом функциональность и удобство эксплуатации. Ядро наших решений построено так, чтобы выстраивать сложные инфраструктуры и модели доступа в разных отраслях и при этом сохранять максимальный контроль и безопасность.

– В контексте растущей актуальности ИИ как вы оцениваете их роль в эволюции систем безопасности АСУ ТП в таких задачах, как обнаружение аномалий и анализ поведения? Какое практическое применение этих технологий уже существуют или возможны в ближайшие годы?

– Я оцениваю роль ИИ в безопасности АСУ ТП крайне положительно. Нельзя сегодня игнорировать инструменты, которые атакующие уже используют для построения сложных атак. При этом ИИ пока не готов полностью заменить человека в принятии точных решений, но как средство обнаружения аномалий, анализа поведения и ускорения детектирования сложных атак он уже эффективно применяется на практике. Думаю, что в ближайшие годы можно ожидать активного использования агентов и интеграции с разными

системами, что позволит автоматизировать и ускорить реагирование на инциденты.

Именно в этой логике развиваются и наши продукты. Уже сейчас в них реализованы расширенные системы мониторинга и анализа, позволяющие строить поведенческие модели пользователей. Дальнейшее развитие мы видим в применении ИИ для более широкого круга задач анализа и объединения данных, перехода от аналитических моделей к превентивным моделям реагирования. Все это напрямую повышает качество и скорость реакции на инциденты.

– В своем прошлом интервью для нашего журнала вы упоминали работу с вузами. Достойных специалистов по ИБ для АСУ ТП по-прежнему не хватает. Развиваете ли вы совместные программы или курсы вместе с университетами сегодня?

– Достойных специалистов по ИБ действительно катастрофически не хватает, и за последнее время здесь ничего принципиально не изменилось. Мы продолжаем активно взаимодействовать с вузами, ведем переговоры о совместных программах и обучении специалистов, в том числе по работе с нашими продуктами. Важно делиться практическим опытом «с передовой», что называется, чтобы выпускники выходили из университетов уже подготовленными и могли как можно быстрее включаться в защиту инфраструктур: как АСУ ТП, так и ИТ в целом.

Среди вузов, с которыми у нас уже сложились продуктивные отношения, – Московский политех МГТУ им. Баумана, Финансовый университет. Мы по-прежнему открыты к предложениям со стороны образовательных учреждений и готовы сотрудничать с ними по самому широкому спектру задач. В частности, использовать наши продукты в учебном процессе, привлекать наших специалистов к обучению, работать со студентами старших курсов и стажерами. Для нас принципиально важно,

чтобы такое взаимодействие продолжалось и чтобы на рынок выходило больше действительно компетентных специалистов.

– Можете ли вспомнить пример из вашей практики, когда внедрение РАМ предотвратило реальный инцидент в АСУ ТП? Что это был за сценарий?

– Да, подобный пример, правда, без названия компании, я могу рассказать. Кстати, пример достаточно типовой, и его смогут «примерить на себя» многие. Речь идет об объекте с сегментированной инфраструктурой АСУ ТП и корпоративного ИТ. При этом в рамках рабочих процессов сохранялись удаленные подключения для инженерного и вендорского обслуживания: обновления оборудования, проверки конфигураций. Формально это был полностью легитимный доступ с легитимными учетными записями.

РАМ внедрялся поэтапно и на первом этапе работал в режиме проксирования, без жестких блокировок и отключений. В ходе эксплуатации была зафиксирована нестандартная сессия в нерегламентное время – ночное подключение с рабочих станций ИТ-сегмента по легитимному каналу. В связке с SIEM-системой были выявлены действия, выходящие за рамки нормального времени работы, когда с этими системами работать никто не должен.

Инцидент оперативно остановили и проверили, до развития атаки дело не дошло, к счастью. По сути, это классический сценарий, когда сначала компрометируются учетные записи в ИТ-инфраструктуре, а затем предпринимается попытка расширить атаку на объект АСУ ТП. В данном случае РАМ позволил выявить нестандартное время и поведение пользователя при подключении к критически важной системе и купировать развитие инцидента. Подобный пример, разумеется, не единственный, просто говорить о них публично не принято. А ведь обмен опытом – особенно с детальными данными расследований – очень полезная вещь для всей отрасли, на мой взгляд. ■

«Лаборатория Касперского» о новых угрозах для КИИ и защите промышленных систем



Ни для кого не секрет, что вопрос защиты КИИ стоит остро последние несколько лет. Тем не менее, мы отчетливо видим, что злоумышленники окончательно сменили фокус с кражи данных на физическое уничтожение инфраструктуры. В преддверии новых вызовов мы побеседовали с **Дмитрием АСТАПОВЫМ**, старшим менеджером по продукту «Лаборатории Касперского».

но и отработанные сценарии поиска слабых мест в инфраструктуре, реагирования на инциденты, а также подготовленный персонал и четкое распределение ролей между службой безопасности, технологами и руководством.

По последним проектам мы видим, что большинство наших клиентов уже начали решать задачу комплексно и стремятся заранее интегрировать кибербезопасность в жизненный цикл технологических систем – от проектирования и ключевых архитектурных решений до эксплуатации и организационных мер.

– В каких новых, нетривиальных отраслях или на каких типах объектов вы в последнее время видите наиболее активный спрос на ваши решения для АСУ ТП?

– В последнее время мы наблюдаем расширение области применения наших решений за пределы промышленных предприятий. Если раньше спрос формировался в основном в отраслях топливно-энергетического комплекса, то сейчас активный интерес проявляют секторы, где физические процессы также тесно переплетены с цифровыми системами, но вопросы безопасности ранее стояли не так остро. Прежде всего, это инфраструктуры с высокими требованиями к качеству продукции и, как следствие, развитой

цифровизацией производства: предприятия пищевой промышленности, производства высокотехнологичных товаров в области электроники, машиностроения и других товаров общего потребления. Также транспортная отрасль была одной из самых атакуемых в 2025 г.

Спрос также появляется в сегменте умных зданий – от систем управления лифтами и вентиляцией до парковок и систем видеонаблюдения. Эти объекты традиционно рассматривались как ИТ-инфраструктура, но с увеличением их роли в обеспечении безопасности возрастает и потребность в продвинутых средствах защиты. Согласно отчетам центра исследования угроз Kaspersky ICS CERT, отрасль автоматизации зданий оставалась в лидерах по числу атак в течение 2025 г., поэтому запрос на повышение кибербезопасности в этой отрасли закономерен.

– «Лаборатория Касперского» является лидером рынка и имеет уникальный опыт реализации сотен комплексных проектов. Какой самый важный урок или инсайт, полученный от ваших заказчиков в последние годы, повлиял на развитие ваших решений и подходов?

– Сегодня наши решения работают в самых разных отраслях, и мы находимся в постоянном и близком контакте со службами

– Что, по вашему мнению, должно стать следующим стратегическим шагом для перехода к построению реальной киберустойчивости критически важных объектов?

– Реальная киберустойчивость определяется не тем, насколько хорошо система защищена на бумаге, а тем, насколько быстро и управляемо организация способна обнаружить атаку, локализовать ее и восстановить бизнес-процессы.

После этапов категоризации объектов, проектирования и внедрения СОИБ следующий стратегический шаг – переход к управлению реальными киберрисками, то есть к пониманию того, какие цифровые активы наиболее критичны и уязвимы, какие последствия могут вызвать атаки на них и как можно минимизировать такие сценарии. Для этого требуются не только технические средства мониторинга,

ИБ, инженерами АСУ ТП, операторами центров мониторинга и другими специалистами. Возможность прямого диалога с экспертами на стороне заказчика в части развития и улучшения решения является для нас одним из ключевых драйверов.

За последний год мы провели обширное исследование пользовательского опыта и несколько опросов удовлетворенности нашими решениями. Для нас было неожиданностью, насколько много пользователей откликнулось и было готово поделиться как своими болями, так и новыми идеями.

доступны в рамках тренинг-курса по продукту.

Также в ближайшее время мы хотим сформировать сообщество экспертов для обмена опытом, анонсами и демонстрациями новых возможностей платформы: хотим делиться новостями с сообществом как можно раньше.

– Какие новые векторы атак вы наблюдали в 2024–2025 гг., на которые должны в первую очередь обратить внимание операторы критической инфраструктуры, уже защитившие свои объекты базовыми средствами?

для проникновения в периметр КИИ и дальнейшую разведку, и закрепление в инфраструктуре. При этом наблюдается массовое применение техник, при которых вредоносная активность маскируется под легитимные действия системных утилит, что позволяет обходить сигнатурные методы обнаружения.

В этих условиях приоритетной задачей для служб безопасности становится смещение фокуса с исключительно превентивных мер на обеспечение отказоустойчивости и восстановления, включая внедрение систем резервирования и регулярную валидацию планов по реагированию на инциденты.

– Искусственный интеллект и машинное обучение – это модные слова, многие компании стремятся интегрировать ИИ в свои продукты ради того, чтобы говорить, что работают с ИИ. Как ИИ реализован в ваших решениях практически? Помогают ли ваши алгоритмы на основе ИИ обнаруживать аномалии в работе технологического процесса или ранее неизвестные угрозы, которые пропускают сигнатурные методы?

– В наших решениях ИИ – это не дань моде, а специализированный инструмент для решения задач, с которыми сигнатурные методы и правила не всегда успешно справляются.

Сигнатурное обнаружение работает только для известных угроз и только в том случае, если их признаки легко наблюдаемы и однозначно распознаваемы. Но в промышленных средах необходимо обнаруживать как атаки, так и аномалии – например нетипичное поведение оборудования в сети или нестабильные параметры технологического процесса. В общем смысле аномалия – это любое отклонение от нормального поведения, такие отклонения могут указывать на ошибки конфигурации, вызванные сбоями или умышленными изменениями настроек устройства.

В наших решениях ИИ – это не дань моде, а специализированный инструмент для решения задач, с которыми сигнатурные методы и правила не всегда успешно справляются.

В традиционных условиях закрытости критических сегментов сетей и невозможности автоматически получать оттуда продуктивную аналитику, нам удалось получить много полезной обратной связи от большого числа реальных пользователей, операторов ИБ АСУ ТП, ежедневно решающих большой спектр задач. К сожалению, мы также отмечаем, что из-за низких темпов обновления инсталляций на производственных площадках и разного профессионального бэкграунда не всем специалистам удается своевременно опробовать новую функциональность.

Это один из вопросов, над которым мы активно работаем. Например, в прошлом году мы разработали новые форматы обучения – проведения расследования инцидента на базе KICS и соревнование для экспертов по продукту в формате Capture the Flag (CTF). Сейчас эти форматы

– В 2024–2025 гг. киберугрозы претерпели качественную трансформацию: от массовых атак злоумышленники перешли к сложным многоступенчатым и распределенным по времени операциям.

Значительная часть инцидентов в КИИ была связана с использованием программ-шифровальщиков и вайперов, нацеленных не столько на получение выкупа, сколько на полное уничтожение инфраструктуры, данных и, как следствие, остановку бизнес-процессов.

Также значимым вектором являются атаки через доверенных цифровых посредников. Речь идет о компрометации подрядчиков и партнеров в цепочке поставок, которые обладают легитимным доступом к критическим сегментам инфраструктуры, включая промышленные среды. Злоумышленники используют менее защищенную инфраструктуру подрядных организаций как точку входа

В наших продуктах мы используем принцип постоянного обучения на реальных данных в сетевом трафике, чтобы сформировать «нормальный профиль» работы конкретного устройства – будь то рабочая станция или промышленный контроллер.

Важной частью этого подхода является классификация устройств по их сетевому поведению. Алгоритмы анализируют, какие протоколы использует устройство, с кем и как часто оно обменивается данными, какие команды и типы трафика генерирует. На этой основе система автоматически делает предположение о категории устройства – ПЛК, сервер, инженерная станция и т. д. – даже если оно не описано в инвентарных базах. Это особенно важно для промышленных сетей, где часто присутствуют неучтенные или неизвестные устройства.

После того как для каждого устройства сформирован его поведенческий профиль, ИИ отслеживает аномалии в сетевой активности: неожиданные соединения, нетипичные команды, изменение частоты или объема обмена данными. Такие отклонения могут указывать как на технические проблемы (ошибки конфигурации, деградацию оборудования), так и на киберугрозы, например компрометацию инженерной станции или попытку скрытно управлять контроллером.

В отличие от чисто сигнатурных методов, которые находят только известные шаблоны атак, наши модели способны выявлять ранее неизвестные и «тихие» угрозы, проявляющиеся именно через изменение поведения. При этом мы комбинируем ИИ с правилами и технологическим контекстом, чтобы минимизировать ложные срабатывания.

– Помимо ИИ, какие еще ключевые нововведения или значимые обновления в вашей платформе Kaspersky Industrial CyberSecurity вы бы выделили как наиболее востребованные рынком сегодня?

– На сегодня на рынке ИБ АСУ ТП востребованы решения, позволяющие решать максимальное количество задач – мультифункциональные платформы для управления активами, выявления уязвимостей и рисков, обнаружения угроз и расследования инцидентов.

Применение множества различных решений, попытки адаптации решений для корпоративного сегмента, как правило, существенно повышают сложность внедрения и обслуживания, а также несут риски негативного воздействия на инфраструктуру. Зачастую на объекте может даже не хватать места для установки требуемого комплекта оборудования. Помимо этого, платформа должна легко встраиваться в существующие информационные системы, обеспечивать обмен данными с центрами мониторинга информационной безопасности (SOC), системами управления активами, в том числе с АСУ ТП.

Мы развиваем платформу KICS с соблюдением этих принципов как универсальную систему для решения любых задач ИБ АСУ ТП – от базовой инвентаризации активов до расследования инцидентов и реагирования. Такой подход позволяет использовать KICS как полноценное решение класса XDR, так и интегрировать платформу в корпоративный SOC.

Основные нововведения в платформе связаны с развитием интеграции между решением для защиты промышленных узлов KICS for Nodes и решением для мониторинга технологической сети KICS for Networks – централизованный сбор и агрегация данных с уровня узлов и из сети позволяет обеспечить полную наблюдаемость инфраструктуры и своевременное обнаружение угроз.

Из последних нововведений – новый модуль для управления изменениями конфигураций как для Windows, Linux узлов, так и сетевого оборудования и промышленных логических контроллеров (ПЛК). Это один из примеров, демонстрирующий

ценность специализированных решений – мониторинг изменения конфигураций доступен в том числе для ПЛК.

Наравне с этим мы развиваем и детектирующие технологии платформы: в уникальные модули по контролю целостности проекта ПЛК и обнаружению аномалий в работе промышленного ПО была добавлена поддержка новых промышленных систем. Напомню, в рамках расследования инцидентов, выявленных с помощью KICS, доступны понятный граф развития атаки и опциональная возможность выполнить реагирование для завершения атаки или предотвращения повторного инцидента. В зависимости от компетенций и должностных инструкций оператор системы может оперативно установить первопричину инцидента и даже ее устранить.

Также уже несколько лет подряд мы расширяем перечень поддерживаемых операционных систем в Kaspersky Industrial CyberSecurity for Nodes, добавляя как устаревшие операционные системы, так и самые новые, в том числе специализированные, используемые в промышленном сегменте.

Узлы, использующие устаревшие ОС – не редкость, и их число вряд ли будет сокращаться, они до сих пор остаются в строю по причине того, что системы, функционирующие на них, невозможно модернизировать. В свою очередь появляются и новые современные ОС, адаптированные под задачи производства. Мы развиваем решение как максимально универсальное и обеспечиваем поддержку широкого диапазона ОС.

Наша особая гордость – поративное решение для аудита и защиты изолированных систем, позволяющее выполнять не только базовое антивирусное сканирование незащищенных узлов, но и полноценную инвентаризацию, включая поиск уязвимостей и комплаенс-проверки настроек безопасности для последующей централизованной обработки данных. ■

От периметра к процессам: практические шаги для перехода к управлению рисками в промышленной ИБ



Цифровое ядро современного производства – это сплав АСУ ТП, корпоративных информационных систем и данных. Его защищенность напрямую определяет бесперебойность и устойчивость бизнеса, попутно обеспечивая соответствие растущим регуляторным требованиям. Как перевести эту системную работу по обеспечению требуемого уровня защищенности из сферы ручного контроля в плоскость управляемых и измеримых процедур? Об этом рассказывает директор департамента технической поддержки продаж ИТ-компании УЦСБ **Алексей ШАНИН**.

– Как службе ИБ промышленного предприятия перестать быть «пожарной командой» и начать предвидеть факт реализации угрозы для АСУ ТП, перейдя к управлению ИБ?

– Чтобы высокочрезвычайно и малоэффективное в стратегической перспективе «тушение пожаров» осталось в прошлом, надо переходить от точечных, реактивных мер к построению непрерывного процесса управления безопасностью. Сегодня недостаточно раз в год провести аудит и составить толстый отчет. Угрозы и сама технологическая среда – АСУ ТП, сети, ПО – меняются постоянно. Но дело не только в динамике изменений. Главная системная проблема заключается в том, что мероприятия по информационной безопасности значимых объектов КИИ часто изначально не встроены в производственный процесс. На многих предприятиях организационно-распорядительные

документы по безопасности объектов КИИ существуют сами по себе и не соответствуют реальным условиям эксплуатации и реальной архитектуре защищаемых систем. Контракты с подрядчиками, которые проектируют или модернизируют промышленные объекты, заключаются без учета требований законодательства в области ИБ. Как следствие, создаваемые системы не защищаются ни внутри, ни снаружи. Пока безопасность не станет присутствовать на всех этапах жизненного цикла, служба ИБ так и останется «пожарной командой», фиксирующей последствия.

– Получается, требования есть, но в реальной производственной среде они не всегда работают. Как же встроить безопасность в процессы?

– Тут важно настроить автоматизацию процесса оценки и мониторинга защищенности, но так, чтобы этот процесс действительно работал на безопасность, а не просто штамповал отчеты.

Именно поэтому мы в УЦСБ создали CheckU – автоматизированную платформу для аудита ИБ и оценки состояния защищенности информационных систем. Платформа базируется на поддерживаемой в актуальном состоянии

модели требований (КИИ, ПДн, отраслевые стандарты) и глубокой адаптации к применению в промышленных системах автоматизации. CheckU – это отчетность в динамике, позволяющая службе ИБ видеть, как изменился уровень рисков после обновления, ввода нового участка, изменения конфигурации защищаемой системы и ее компонентов. Платформа автоматически выявляет отклонение настроек от безопасных, несанкционированные изменения, несоответствия требованиям, таким образом, дает команде ИБ инструмент для проактивного управления защищенностью: вы видите потенциальную уязвимость до ее эксплуатации, потому что отклонение контролируемых параметров можно отследить в панели мониторинга комплекса. Так обеспечивается основа для принятия управленческих решений.

– Почему автоматизация аудита ИБ становится вопросом операционной эффективности не только для крупных, но и средних производств? Какие бизнес-риски она помогает предотвратить?

– Автоматизация аудита ИБ действительно перестала быть прерогативой крупных

корпораций и стала насущной необходимостью для средних компаний. И основная причина – в фундаментальном изменении экономики безопасности. Классический ручной аудит, дорогостоящий и ресурсоемкий, вынуждал средний бизнес прибегать к формальному решению вопроса и создавал скрытые, но критичные риски. Именно поэтому внедрение таких решений, как платформа CheckU от УЦСБ, перестраивает логику обеспечения безопасности: вместо разовой затратной процедуры компания получает постоянно действующий инструмент для непрерывного контроля, что позволяет напрямую предотвращать ключевые бизнес-угрозы, такие как дорогостоящий простой производства из-за кибератаки, многомиллионные регуляторные санкции за несоответствие требованиям по защите КИИ и ПДн, а также утечки критичных данных.

с самой критичной ИБ-потребности. Например, для быстрого старта и оценки текущего состояния защищенности, мы предлагаем экспресс-аудит, который за две недели дает четкую картину ситуации с точки зрения ИБ, и дорожную карту для ее корректировки и устранения уязвимостей. Следу-

предприятием, где мы начали с экспресс-оценки защищенности, оперативно подключили SOC, а затем перешли к плановому сопровождению систем, позволяет Заказчику наращивать защиту поэтапно, без крупных первоначальных затрат и с немедленным практическим результатом.

CheckU – это отчетность в динамике, позволяющая службе ИБ видеть, как изменился уровень рисков после обновления, ввода нового участка, изменения конфигурации защищаемой системы и ее компонентов.

ющим логичным шагом становится подключение непрерывного мониторинга через наш УЦСБ SOC,

– **Обеспечение киберустойчивости часто означает смену самой парадигмы – от защиты периметра к управлению рисками для бизнеса. Какие шаги и процессы сопровождают такой переход?**

– Эта смена парадигмы реализуется через последовательную перестройку процессов. Первый шаг – оценка активов через призму их влияния на ключевые производственные процессы, такие как бесперебойность технологического процесса. Следом необходим переход к непрерывному мониторингу безопасности, который отражает динамику угроз в реальном времени. Ключевым становится умение транслировать технические уязвимости в понятные бизнесу последствия, такие как риск простоя, и его финансовую оценку. Это формирует основу для аргументированного диалога с руководством. Финальный этап – интеграция выводов в операционную деятельность: фокус для SOC, план работ для служб эксплуатации и требования для подрядчиков и разработчиков. Таким образом, безопасность становится неотъемлемой частью производственного контура, а не отдельной его функцией. ■

К УЦСБ SOC легко подключаются и другие услуги – будь то безопасная разработка, классический аудит АСУ ТП или сопровождение средств защиты информации.

– **Как на практике меняется запрос Заказчиков из промышленности? Вы видите спрос на отдельные услуги, например, разовый аудит, или же на комплексные решения?**

– Промышленные компании все реже приходят за разовой «справкой» – им уже недостаточно однократного пентеста или аудита для галочки. Ключевым трендом становится запрос на киберустойчивость как сервис – измеримый и оперативный в получении результата. В сервис-ориентированной модели Заказчик может гибко формировать пакет необходимых ему услуг, начиная

который предоставляется по подписке и разворачивается за считанные дни, обеспечивая круглосуточную защиту без необходимости создавать собственную 24/7-команду. Именно этот сервис сегодня является ядром комплексного запроса, так как закрывает критическую потребность в оперативном обнаружении инцидентов ИБ и реагировании на них. При необходимости к УЦСБ SOC легко подключаются и другие услуги – будь то безопасная разработка, классический аудит АСУ ТП или сопровождение средств защиты информации. Такой подход, как в нашем недавнем проекте с химическим

Бэкап последней надежды:

как оптические диски защищают данные КИИ от шифрования и уничтожения



В связи с кратным ростом кибератак, нацеленных на компрометацию и уничтожение важных данных объектов критической информационной инфраструктуры (КИИ) и промышленных предприятий, традиционные средства хранения и резервного копирования уже не справляются с задачей сохранения критически важной информации. В таких условиях безопасность данных определяется не количеством копий, а недоступностью носителя и его защитными свойствами, которые гарантируют неизменность данных при любом сценарии атаки. **Олег КОРОТОВСКИЙ**, руководитель направления по защите информации компании ЭЛАР, рассказал, почему аппаратно-защищенные бэкапы на базе оптических дисков однократной записи становятся обязательным элементом страховых фондов данных КИИ и как изменяются требования к системам хранения на стратегических предприятиях.

– На рынке много решений для резервного копирования. Чем принципиально отличается подход «ЭЛАРобот НСМ» с использованием оптических дисков? Как продукт позволяет закрывать самые уязвимые точки в системе хранения, а именно возможность изменения, удаления, заражения или кражи данных?

– ЭЛАР не стремится заменять традиционные решения в области ИБ, как, например: SIEM-решения, межсетевые экраны, SOAR и другие. Наш подход – защита данных на аппаратном уровне без привязки к программной составляющей, а конкретно – обеспечение сохранности данных на физическом уровне носителя информации.

С начала 2000-х гг. ЭЛАР производит специальные системы хранения данных в формате роботизированных программно-аппаратных комплексов (ПАК).

Это архивные оптические накопители серии «ЭЛАРобот НСМ», которые представляют собой ПАК для холодного хранения на базе оптических дисков однократной записи.

Благодаря использованию непerezаписываемых дисков формата Blu-ray XL Archival Grade это оборудование на уровне носителя информации обеспечивает сохранность записанных данных на протяжении десятилетий. Физические свойства дисков позволяют обеспечить 100% гарантию неизменности данных при любых кибератаках, нацеленных на злонамеренное шифрование, компрометацию или уничтожение важных данных.

На базе архивных оптических накопителей можно организовать отдельный аппаратно-защищенный сегмент хранения важнейшей информации. Даже

при уничтожении всей остальной инфраструктуры хранения у вас всегда будет так называемый «бэкап последней надежды», с которого начнется восстановление в случае катастрофы.

– Вы исторически известны решениями для архивирования и оцифровки. Насколько для вас стало естественным развивать направление в сторону создания специализированных, изолированных решений для режимных объектов и субъектов КИИ? Как эта специализация вписывается в общую стратегию компании?

– ЭЛАР давно сотрудничает с государственными структурами и субъектами КИИ. Мы занимается оцифровкой и электронными архивами более 30 лет. Широкой общественности прекрасно известны такие

проекты по Великой Отечественной Войне, как «Подвиг народа» и «Память народа», созданные в тесном сотрудничестве с Минобороны России.

За все эти годы через нашу фабрику оцифровки прошли гигантские массивы документов, в том числе масса документов ограниченного доступа. Производство и поставка аппаратно-защищенных систем хранения – пример естественного развития наших компетенций и реакция на изменившиеся потребности рынка.

ЭЛАР комплексно подходит к своей работе, покрывая весь жизненный цикл критически важных документов: от оцифровки, распознавания, создания электронных архивов для режимных учреждений, и вплоть до аппаратно-защищенного хранения.

– Можете ли вы рассказать о реализованном проекте с «ЭЛАРобот НСМ» для предприятия из сферы КИИ или АСУ ТП? С какой основной проблемой или запросом к вам обратился заказчик, и как ваше решение помогло ее закрыть?

– В последние годы наблюдается кратный рост кибератак, нацеленных на компрометацию и унич-

систем хранения данных «ЭЛАРобот НСМ».

За последний год у нас появилось множество клиентов из отрасли промышленности и ВПК. Архивные оптические накопители позволяют сохранить в неизменном виде важнейшую проектную и конструкторскую документацию, ценные

– Постепенно вырабатываются новые стандарты и ИБ-инструменты, которые находят применение как в государственных учреждениях, так и в частном бизнесе. Мы наблюдаем тенденцию по унификации требований, поскольку каждый новый инцидент, получивший известность в публичном поле, неумолимо

ЭЛАР давно сотрудничает с государственными структурами и субъектами КИИ. Мы занимается оцифровкой и электронными архивами более 30 лет.

данные испытаний различных изделий, показания телеметрии и другие данные частных и государственных производителей, в том числе исполнителей ГОЗ. Десятки предприятий по всей стране уже сейчас формируют страховые фонды и «бэкапы последней надежды» критически важных данных, страхуя себя от возможных инцидентов и катастроф ИТ-инфраструктуры.

сближает требования корпоративного и государственного сектора. Например, если раньше бизнес при выборе решений не учитывал факт нахождения ПО или оборудования в реестрах Минпромторга и Минцифры РФ, то сейчас этот фактор играет значимую роль.

Если говорить о стратегическом развитии, какие ключевые цели и планы вы ставите перед собой на этот год? На развитии каких технологий или компетенций вы планируете сделать особый акцент?

В рамках трендов на изолированность и повышение надежности ИТ-инфраструктуры мы планируем дальше развивать линейку архивных оптических накопителей «ЭЛАРобот НСМ».

В 2026 г. ЭЛАР ожидает появление на рынке комплексных самодостаточных решений в формате ПАК, включающих: горячее хранилище на СХД, холодное хранилище на оптических носителях и набор программных надстроек. Подобные устройства позволят закрывать широкий спектр задач резервного копирования критически важных данных. ■

В рамках трендов на изолированность и повышение надежности ИТ-инфраструктуры мы планируем дальше развивать линейку архивных оптических накопителей «ЭЛАРобот НСМ».

тожение ценных данных. Страна сталкивается с новыми экзистенциальными вызовами. Все это служит драйвером развития наших продуктов, и интереса ним. Растет количество заявок на приобретение аппаратно-защищенных

– Чем, на ваш взгляд, принципиально отличаются задачи и требования к защите данных на стратегических предприятиях от задач защиты данных в обычном корпоративном секторе?

Четырнадцатая конференция «Информационная безопасность АСУ ТП КВО»

**3–4 марта 2026 г.
г. Москва**

ПРОГРАММА

ДЕНЬ ПЕРВЫЙ

08.30–09.45

Регистрация. Работа выставки

09.45–13.00

Пленарное заседание

- Гаврилов Виктор Евдокимович, главный научный сотрудник, Федеральный исследовательский центр «Информатика и управление Российской академии наук»
Вступительное слово
- Рогоза Максим Викторович, советник отдела управления ФСТЭК России
Краткий обзор нововведений в области законодательства и развития нормативно-правовой базы в сфере безопасности КИИ за 2025–2026 гг.

Сессия вопросов и ответов регулятору

- Пыхтин Иван Геннадьевич, сотрудник, Национальный координационный центр по компьютерным инцидентам
Основные изменения в нормативно-правовой базе ФСБ России в системе ГосСОПКА

Сессия вопросов и ответов регулятору

- Мячин Илья Владимирович, сотрудник, Национальный центр кибербезопасности (Республика Беларусь)
Об административной ответственности владельцев объектов информационной инфраструктуры за нарушение требований по кибербезопасности в Республике Беларусь
- Родин Константин Сергеевич, заместитель директора по развитию бизнеса, «АйТи Бастион»
Расширение понятия «безопасная автоматизация процесса» на базе решения «Синоникс»: синергия безопасности и автоматизации
- Стрелков Андрей Владимирович, руководитель направления развития продуктов для промышленной безопасности, «Лаборатория Касперского»
Современные подходы к защите промышленных инфраструктур для обнаружения и реагирования на целевые атаки

- Олег Коротовский, руководитель направления по защите информации, ЭЛАР
Защита информации объектов КИИ с помощью отечественных ПАК на базе оптических носителей однократной записи
- Шанин Алексей Андреевич, директор департамента технической поддержки продаж, УЦСБ
Верните мой 2016-й: эволюция кибербезопасности АСУ ТП за 10 лет и взгляд в 2026 год

13.00–14.00

Обеденный перерыв. Работа выставки

14.00–15.30

Воркшоп «Подходы к организации комплексной защиты в работе в технологическом сегменте (ТСПД) – опыт «АйТи Бастион» и «Лаборатории Касперского»»

14.00–16.45

Методы, технологии и инструменты защиты АСУ ТП

- Енютин Алексей Юрьевич, заместитель начальника управления, ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
Применение технологий искусственного интеллекта в исследованиях по обеспечению безопасности АСУ ТП
- Назаренко Денис Максимович, руководитель отдела технической поддержки продаж UDV Group
Групповой портрет АСУ ТП в киберландшафте
- Роман Писарев, руководитель департамента консалтинга и аудита, iTPROTECT
От «бумажной» безопасности к «железной» защите. Как выполнение требований законодательства может стать основой противодействия реальным угрозам
- Вячеслав Половинко, руководитель направления собственных продуктов, АМТ-ГРУП
Междоменная передача данных через InfoDiode: архитектурные решения, применение киосков данных
- Николаев Иван Александрович, технический директор, ООО «Русьтелетех»
Модуль проксирования трафика для анализа и инспекции промышленных протоколов
- Андрей Лаптев, директор департамента продуктового развития, «Индид»
Защита ключевой инфраструктуры объекта АСУ ТП – управление привилегированным доступом
- Андрейчиков Игорь Владимирович, руководитель проекта, ООО «ИНКОНТРОЛ»
Эффективные подходы к внедрению СОИБ АСУ ТП на объектах электроэнергетики
- Вадим Подольный, руководитель комитета промышленной автоматизации, АРПП «Отечественный софт»
Актуальные технологические вызовы в задачах промышленной кибербезопасности

16.45–17.00

Перерыв. Работа выставки

17.00–19.30

«Практикум»

Задача № 1

Создание информационной защиты видеопотока с камеры видеонаблюдения, а также передачи событий при взаимодействии с внешними системами по REST full API, Onvif profile (M/T), RTSP, HTTP, информационном обмене с АСУ ТП на объекте ЗО КИИ

Постановщик задачи: Куксилов Евгений Александрович, руководитель департамента эксплуатации автоматизированных систем технологического управления и связи, АО «ОЭК»

Задача № 2

Реализация метода защиты программируемых логических контроллеров от внутреннего нарушителя

Постановщик задачи: Сахаров Константин Валерьевич, директор технического департамента по направлению «Информационная безопасность» «Росатом автоматизированные системы управления»

19.30–21.00

Развлекательная программа. Фуршет

ДЕНЬ ВТОРОЙ

09.00–09.45

Регистрация участников. Работа выставки

09.30–11.30

Практический опыт создания системы ИБ АСУ ТП
В фокусе – нефтегазовая и химическая отрасли

- Сорокина Марина Викторовна, руководитель продуктового направления, АО «ИнфоТеКС»
Практические кейсы обеспечения кибербезопасности АСУ ТП в нефтегазовой отрасли: от кустовых площадок до магистральных трубопроводов

- ▶ **Бондюгин Андрей Андреевич**, директор направления по сопровождению проектов промышленной безопасности, «Лаборатория Касперского»
Искусственный интеллект как универсальный инструмент на стыке информационной и промышленной безопасности для обеспечения непрерывности производства
- ▶ **Тяплашкин Александр Иванович**, директор по разработке и технологическому развитию, АО НИЦ «ИНКОМСИСТЕМ»
Интеграция ПЛК в контур кибербезопасности АСУ ТП: от пассивного звена к активному барьеру
- ▶ **Гончарова Александра Игоревна**, инженер поддержки продаж/пресейл, ООО «АйТи БАСТИОН»
Интегрируемая платформа для контроля информационного обмена: как «Синоникс» стал частью операционных процессов

Вопросы панельной дискуссии

- *Какие типовые отраслевые АСУ ТП являются наиболее перспективными объектами для атак злоумышленников. Какие из них вошли в реестры типовых объектов КИИ. Есть ли понимание необходимости и достаточности реестров. Что можно сказать об импортозамещении самих АСУ ТП. Есть ли в наличии весь необходимый инструментарий для их защиты*
- *Есть ли изменения векторов атак на отраслевые АСУ ТП за последнее время. В чем проявляется специфика нефтегазовой и химической отраслей. Появляются ли новые угрозы и откуда они исходят. Что можно им противопоставить*
- *Что происходит с импортозамещением ПЛК для нефтегаза. Что можно сказать о защищенности самих ПЛК. Какие риски стоит учитывать и какие инструменты применять*

Участники дискуссии

- **Бибик Андрей Валерьевич**, директор департамента защиты информации, ООО «Автоматика-сервис» («Газпром нефть»)
- **Бондюгин Андрей Андреевич**, директор направления по сопровождению проектов промышленной безопасности, «Лаборатория Касперского»
- **Гончарова Александра Игоревна**, инженер поддержки продаж/пресейл, ООО «АйТи БАСТИОН»
- **Сорокина Марина Викторовна**, руководитель продуктового направления, АО «ИнфоТеКС»
- **Тяплашкин Александр Иванович**, директор по разработке и технологическому развитию, АО НИЦ «ИНКОМСИСТЕМ»
- **Голубовский Евгений Викторович**, заместитель начальника управления по производству в Управлении по реализации стратегических проектов ПАО «Газпром автоматизация»

11.30–13.30**Воркшоп «Охота на аномалии с помощью Kaspersky MLAD»****11.30–13.30****Практический опыт создания системы ИБ АСУ ТП
В фокусе – электроэнергетика**

- Ямин Артем Дмитриевич, руководитель группы специализированных проектов, УЦСБ
Сквозная безопасность АСУ ТП: от обследования до сервисного обслуживания
- Дорошенко Борис Алексеевич, старший менеджер предпродажной поддержки решений для бизнеса, «Лаборатория Касперского»
Комплексная защита объектов энергетики: от протоколов до архитектуры
- Никандров Максим Валерьевич, директор ООО «Интеллектуальные Сети», к.т.н.
Тестирование ПАК для объектов КИИ в Испытательной лаборатории системы добровольной сертификации КИИ-СЕРТ «iGrids»
- Верещака Александр Игоревич, старший научный сотрудник, НИЦ «Курчатовский институт»
Особенности обеспечения ИБ АСУ ТП АЭС

Вопросы панельной дискуссии

- Какие типовые отраслевые АСУ ТП являются наиболее сложными для защиты и почему. Какие из них вошли в реестры типовых объектов КИИ в электроэнергетике. Есть ли уже практический опыт их защиты и какие инструменты можно рекомендовать
- Как меняется портрет злоумышленника в последнее время. Какие технологии и инструменты появляются в его арсенале. Какие новые технологии и вызовы, приходящие из ИТ-сферы, уже стоит учитывать при оценке рисков для АСУ ТП
- Насколько широко сегодня применяются стандарты безопасной разработки и проектирования АСУ ТП в электроэнергетике. В какой мере это позволяет снять риски ИБ для АСУ ТП. Видите ли вы угрозу в применении ИИ в процессе создания/ программирования самих АСУ ТП и средств ИБ АСУ ТП

Участники дискуссии

- Верещака Александр Игоревич, старший научный сотрудник, НИЦ «Курчатовский институт»
- Дорошенко Борис Алексеевич, старший менеджер предпродажной поддержки решений для бизнеса, «Лаборатория Касперского»
- Никандров Максим Валерьевич, директор, ООО «Интеллектуальные Сети», к.т.н.
- Ямин Артем Дмитриевич, руководитель группы специализированных проектов, УЦСБ

13.30–14.30

Обеденный перерыв. Работа выставки

14.30–15.30

Практический опыт создания системы ИБ АСУ ТП
В фокусе – машиностроение

- ▶ Лекомцев Александр Николаевич, заместитель директора по безопасности и режиму, АО «Мотовилихинские заводы»
Повышение производительности как драйвер для создания системы защиты станков с ЧПУ
- ▶ Олег Коротовский, руководитель направления по защите информации, ЭЛАР
Что такое страховые фонды предприятий? Специфика защиты, резервного копирования и долговременного хранения информации

15.30–17.00

Практический опыт создания системы ИБ АСУ ТП
В фокусе – транспорт

- ▶ Безродный Борис Федорович, Руководитель отдела обеспечения безопасности информации систем АСУ ТП, доктор наук, профессор, ООО «Группа компаний 1520»
Практика задания и реализации требований функциональной и информационной безопасности в АСУ ТП ЖТ. Противоречия и разночтения
- ▶ Михайличенко Александр Сергеевич, Консультант по информационной безопасности, АКТИВ.CONSULTING (Компания «Актив»)
Коллизия реальностей: почему стандарты Safety (функциональной безопасности) становятся вектором атаки на транспорт. И роль iDMZ в разрешении конфликта

Вопросы панельной дискуссии

- *Какие типовые отраслевые АСУ ТП являются, на ваш взгляд, первоочередными для различных видов транспорта и почему. Какие из них вошли в реестры типовых объектов КИИ на транспорте. Что можно сказать об импортозамещении транспортных АСУ. Есть ли уже практический опыт их защиты*
- *Функциональная или транспортная безопасность и ее соотношение с информационной безопасностью АСУ на транспорте: есть ли противоречия в подходах и в чем их суть. Как они решаются на практике, на различных видах транспорта*

- Особенности защиты АСУ ТП на разных видах транспорта и транспортной инфраструктуры. Основные векторы атак и их изменения за последние год–два для основных видов транспорта
- Новые вызовы в области защиты АСУ ТП беспилотного транспорта и его инфраструктуры. Примеры АСУ ТП и возможных угроз. Готовность разработчиков предложить средства защиты

Участники дискуссии

- Безродный Борис Федорович, Руководитель отдела обеспечения безопасности информации систем АСУ ТП, доктор наук, профессор, ООО «Группа компаний 1520»
- Ключко Герман Александрович, начальник отдела по ЗИ, СЗФ ФГУП «Росморпорт»
- Ольга Копейкина, руководитель отдела консалтинга по ИБ, АКТИV.CONSULTING
- Хмелевская Наталья Владимировна, начальник отдела обеспечения безопасности значимых объектов КИИ, ОАО «РЖД»
- Новиков Дмитрий Владимирович, начальник Подразделения информационной безопасности Службы безопасности ГУП «Московский метрополитен»

17.00–18.30

Практический опыт создания системы ИБ АСУ ТП В фокусе – металлургия

- Нуйкин Андрей Витальевич, начальник управления, ЕВРАЗ
Мониторинг и контроль ИТ-подрядчиков
- Севостьянов Александр Владимирович, советник заместителя генерального директора по безопасности – начальника СЭБ, ПАО «ТМК»
Проблемные вопросы обеспечения безопасности КИИ металлургического предприятия в условиях экономической нестабильности

Вопросы панельной дискуссии

- Какие типовые отраслевые АСУ ТП являются наиболее сложными для защиты и почему. Какие из них вошли в реестры типовых объектов КИИ в металлургии. С какими сложностями приходится сталкиваться на практике
- Текущее состояние работ по созданию открытой архитектуры универсальной АСУ ТП. Когда ждать систему «в железе». Насколько востребованной она станет для различных типов АСУ ТП, и где баланс универсальности и учета специфики. Что известно про систему обеспечения ИБ
- Настоящее и будущее применения ИИ на металлургическом производстве. Внедрение ИИ-ассистентов как серьезный фактор риска, в том числе для безопасности АСУ ТП. ИИ как инструмент в руках злоумышленников. ИИ как инструмент в руках безопасников



Участники дискуссии

- Малышенко Владислав Викторович, руководитель службы по информационной безопасности, ПАО «Кокс»
- Нуйкин Андрей Витальевич, начальник управления, ЕВРАЗ
- Севостьянов Александр Владимирович, советник заместителя генерального директора по безопасности – начальника СЭБ, ПАО «ТМК»

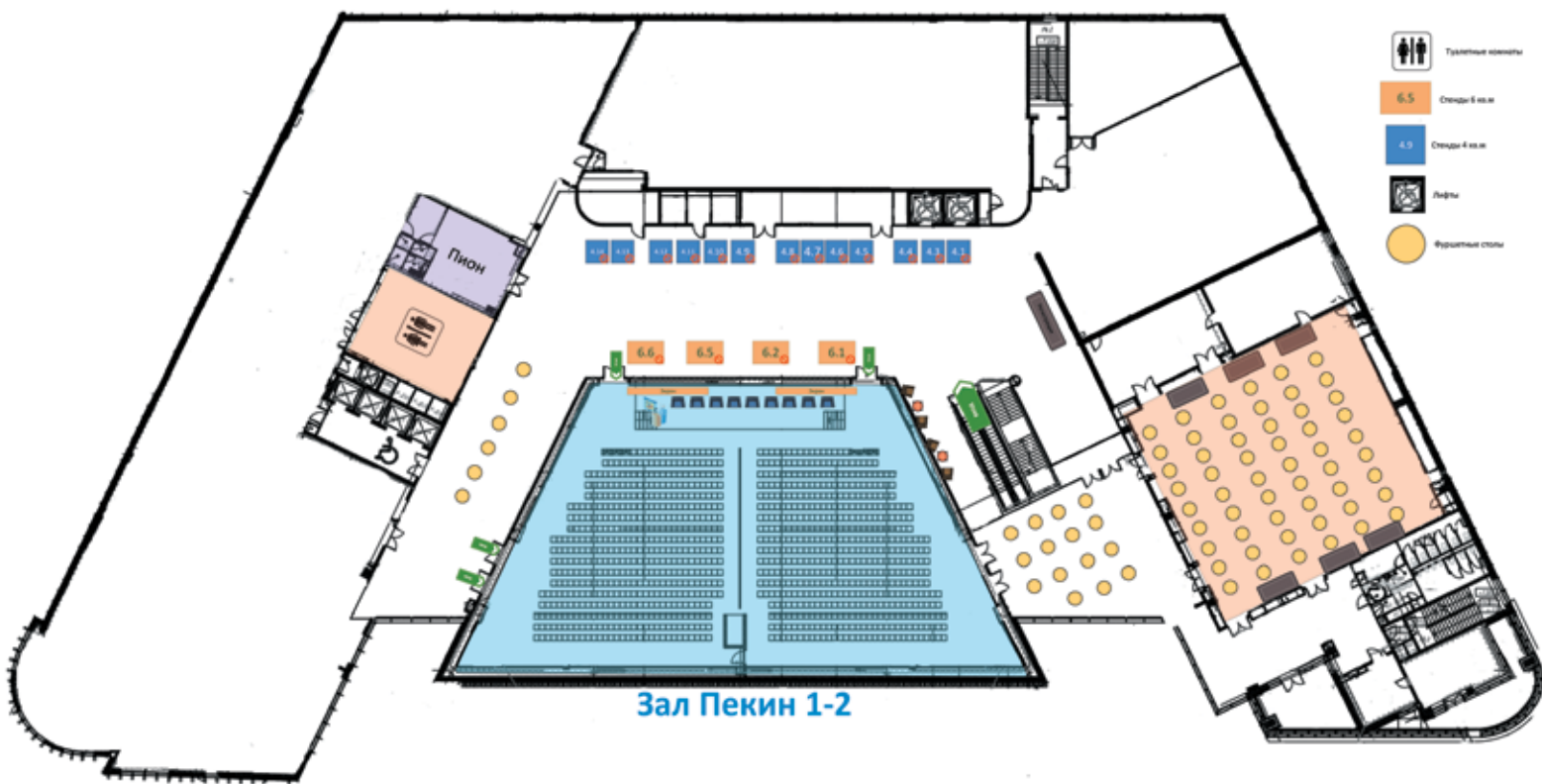
18.30–18.45

Открытый микрофон. Подведение итогов

18.45–19.30

Фуршет

СХЕМА ВЫСТАВКИ



СТЕНДЫ 6 метров

- 6.1 - АйТи Бастион
- 6.2 - Лаборатория Ксаперского
- 6.5 - ЭЛАР
- 6.6 - УЦСБ

СТЕНДЫ 4 метра

- 4.1 - АКТИV.CONSUlTING
- 4.3 - Интеллектуальные сети
- 4.4 - НИЦ ИНКОМСИСТЕМС
- 4.5 - КСБ-СОФТ
- 4.6 - АНСЕР ПРО
- 4.7 - ИнфоТеКС
- 4.8 - АЛТЭКС-СОФТ
- 4.9 - RTT
- 4.10 - iTPROTECT
- 4.11 - ИНКОНТОРОЛ
- 4.12 - Индид
- 4.13 - UDV Group
- 4.14 - АМТ-ГРУП



Подходы к организации комплексной защиты в работе в технологическом сегменте (ТСПД) – опыт «АйТи Бастион» и «Лаборатории Касперского»

3 марта, в 14.00, в рамках конференции «Информационная безопасность АСУ ТП КВО» состоится совместный воркшоп компаний «АйТи Бастион» и «Лаборатория Касперского» на тему: «Подходы к организации комплексной защиты в работе в технологическом сегменте (ТСПД)».

В ходе встречи разберем практические сценарии, которые обеспечивают безопасный и контролируемый обмен данными между изолированными друг от друга сегментами. При этом у сотрудников ИБ сохраняются расширенные интеграционные возможности по мониторингу, контролю и анализу пользовательской активности, в т. ч. привилегированных пользователей.

Сценарии разработаны с применением продуктов СКДПУ ИТ, ПК «Синоникс» от «АйТи Бастион» и Kaspersky Scan Engine, KICS, KUMA SIEM и другие от «Лаборатории Касперского».

Что дают такие сценарии:

- Устойчивость к кибератакам. Комплекс решений обеспечивает эшелонированную защиту АСУ ТП.
- Операционная эффективность. Автоматизация процессов обеспечивает не только удобство работы в АСУ ТП, но и более высокий уровень защиты производства, а значит, – снижение трудозатрат ИТ- и ИБ-специалистов.
- Прозрачность и скорость реагирования.

Чем для вас будет полезно участие в воркшопе:

- Знакомством с новыми подходами к работе в технологическом сегменте.
- Возможностью задать вопросы техническим экспертам «АйТи Бастион» и «Лаборатории Касперского».
- Возможностью поделиться собственным опытом работы с продуктами вендоров. А также высказать замечания, предложения, претензии!

Дата и время:

3 марта 2026 года

Место проведения:

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

ДО ВСТРЕЧИ!

kaspersky

Охота на аномалии с помощью Kaspersky MLAD

Воркшоп посвящен возможностям систем машинного обучения и предиктивной аналитике. На примере сбоя системы измерения покажем, как Kaspersky MLAD выявляет аномалии, детектирует скрытые отказы оборудования и предотвращает выпуск бракованной продукции, обеспечивая непрерывность и качество производственных процессов.

Анонс:

«Лаборатория Касперского» приглашает на круглый стол «Охота на аномалии с помощью Kaspersky MLAD»

На примере сбоя системы измерения покажем, как Kaspersky MLAD выявляет аномалии в технологических процессах, обнаруживает скрытые отказы оборудования и помогает предотвращать выпуск бракованной продукции.

Разберем, как машинное обучение и предиктивная аналитика помогают обеспечивать непрерывность и качество производства.

Присоединяйтесь!

Дата и время:

4 марта 2026 с 11.30 до 13.30

Место проведения:

Москва, Hotel Soluxe, 2-й этаж, зал Чжуцян

РАСПИСАНИЕ ПРЕЗЕНТАЦИЙ НА СТЕНДАХ
3 марта

Время	Стенд	Компания	Презентация
13.45-14.00	6.2	Лаборатория Касперского	Kaspersky MLAD – решения для выявления аномалий в технологических процессах
13.45-14.00	6.6	УЦСБ	Облачные сервисы непрерывного анализа защищенности приложений: решение проблемы дефицита узкоквалифицированных кадров
14.00-14.15	4.1	АКТИВ.CONSULTING	Оптимальный бюджет по ИБ. Как?
14.15-14.30	4.12	ИндиД	Indeed PAM – контроль привилегированного доступа к корпоративным ресурсам
14.30-14.45	4.5	КСБ-СОФТ	Вендоры, регуляторы, подрядчики: как выстроить «треугольник доверия» при защите объектов КИИ
15.00-15.15	4.8	АЛТЭК-СОФТ	Техника сканирования компонентов АСУ ТП с помощью RedCheck
15.30-15.45	4.6	AnswerPro	Решения AnswerPro для криптографической защиты объектов АСУ ТП
16.00-16.15	4.11	ИНКОНТРОЛ	Гарантированная безопасность, гарантированная доступность: технологии однонаправленной передачи технологической информации для критической инфраструктуры
16.15-16.30	4.3	Интеллектуальные сети	Образцы RCE-атак на коммутаторы CISCO
16.30-16.45	6.5	ЭЛАР Корпорация ЭЛАР	Роботизированные оптические накопители ЭЛАРобот НСМ для защиты критичной информации предприятий
16.45-17.00	4.10	Инфозащита	Эффект экосистемы: практическое обнаружение и нейтрализация угроз в промышленном сегменте на примере продуктов Kaspersky
16.45-17.00	4.9	РТТ	Модуль проксирования трафика для анализа и инспекции промышленных протоколов

РАСПИСАНИЕ ПРЕЗЕНТАЦИЙ НА СТЕНДАХ
4 марта

Время	Стенд	Компания	Презентация
14.15-14.30	6.2	Лаборатория Касперского	Решение Kaspersky Industrial Cybersecurity для защиты промышленных инфраструктур
14.15-14.30	6.6	УЦСБ	CheckU – комплексное решение для контроля соответствия требованиям ИБ в промышленной сфере

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 г. Специалисты компании постоянно улучшают продукты и сервисы, ориентируясь на актуальные запросы операторов АСУ ТП.

ПК «Синоникс» – средство информационного обмена, предназначенное для автоматизации при одно- и двунаправленной передачи данных и файлов между системами из несвязанных сетей, минимизируя риски человеческого фактора. Разработка актуальна в области ИБ АСУ ТП, так как позволяет обновлять оборудование в изолированных сегментах сети, передавать данные мониторинга и управления, в том числе и с помощью промышленных протоколов MQTT и MODBUS TCP. Также «Синоникс» помогает противодействовать потенциально неизвестным уязвимостям на конечных системах путем сокрытия данных о сетях и информационных системах в их окружении. Безопасность при передаче достигается и благодаря разграничению зон ответственности при передаче.

Еще один продукт – РАМ-платформа (Privileged Access Management) СКДПУ НТ – успешно применяется в инфраструктурах крупных технологических предприятий. Она помогает снизить риски человеческого фактора, сведя всю работу администраторов к принципу «нулевого доверия» (zero trust). РАМ-платформа позволяет не только проводить расследования и мониторить несанкционированные действия привилегированных пользователей, но и выявлять аномалии, предвосхищать инциденты ИБ и реагировать на них.

Оба решения компании помогают эффективно автоматизировать процессы и обеспечить высокий уровень безопасности.

Продукты и/или услуги

СКДПУ НТ предназначен для защиты 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, в частности, ФСТЭК РФ.

РАМ-платформа СКДПУ НТ позволяет решать не только базовые задачи по контролю доступа и фиксации событий. С ее помощью реализуется расширенный комплексный подход к проблеме контроля привилегированного доступа и созданию безопасной ИТ-инфраструктуры: непрерывный мониторинг, централизованное хранение аудита, управление секретами, обработка событий и выявление аномалий в рамках их анализа, а также поиск инцидентов и реагирование на них. В рамках работы СКДПУ НТ можно использовать не только стороннюю MFA, но и собственную двухфакторную аутентификацию (2FA) на основе алгоритма TOTP.

На базе РАМ-платформы создается мультивендорная экосистема надежных ИБ-решений. Совместная работа ИТ- и ИБ-систем, которые предоставляют друг другу профильные данные, обеспечивает более комфортную и эффективную защиту инфраструктуры заказчика. У компании – более 30 технологических партнеров, которые разрабатывают ИБ-решения различных классов.

Название: «Синоникс»

Назначение: Решение для **безопасной** однонаправленной или двунаправленной передачи данных и файлов между узлами, в том числе из несвязанных сетей. Обеспечивает **автоматизированный** обмен информацией без раскрытия окружения взаимодействующих систем.

Изоляция на физическом уровне. Автоматизированная контролируемая передача данных в режиме «точка-точка» как в одну, так и в обе стороны по протоколам TCP и UDP без прямой связности узлов.

Сокрытие окружения объединяемых объектов. Принципы передачи не позволяют приложениям и пользователям узнать реальный адрес конечной информационной системы и адреса окружения «Синоникса».

Разграничение зон ответственности. Встречный контроль, реализованный через управление двумя ответственными для подтверждения прохождения данных.

Проверка файлов перед передачей. Проверка размера, маски, типа, расширения, целостности передаваемых объектов, а также проверка во внешних системах по ICAP-протоколу.

Автоматизация передачи файлов. Возможность забирать файлы из файлового хранилища по расписанию и после проведения необходимых проверок передавать их на другой Узел, а оттуда – в хранилище на другой стороне.

Физический контроль передачи. Физическая блокировка передачи «пусковыми» ключами.

Опыт работы в отраслях

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

Заказчики в сфере ИБ АСУ ТП

**Название организации****Официальный сайт****АО «Лаборатория Касперского»**<https://www.kaspersky.ru/>**kaspersky**

Компетенции в области ИБ АСУ ТП

Компетенции «Лаборатории Касперского» в области информационной безопасности АСУ ТП охватывают полный цикл защиты промышленных систем – от разработки до реагирования на инциденты. Компания обладает глубокой экспертизой в защите критической инфраструктуры, включая энергетику, нефтегазовый сектор, транспорт и производство.

Ключевые компетенции включают: анализ угроз и моделирование рисков для АСУ ТП; разработку архитектуры безопасности промышленной сети; разработку и внедрение специализированных решений для защиты сетевой инфраструктуры, серверов, рабочих станций операторов, ПЛК и SCADA-систем; мониторинг и обнаружение атак в реальном времени; реагирование на инциденты и цифровую криминалистику.

Эксперты компании участвуют в международных исследованиях угроз промышленной автоматизации и формируют практики безопасности для объектов КИИ

Продукты и/или услуги

Название: Kaspersky Industrial CyberSecurity for Networks, Kaspersky Industrial CyberSecurity for Nodes, Kaspersky MLAD, Kaspersky Unified Monitoring and Analysis Platform

Назначение: Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) – платформа для централизованной защиты промышленной сети. Обеспечивает инвентаризацию активов, анализ уязвимостей, обнаружение аномалий и кибератак в технологическом сегменте, а также глубокий анализ промышленных протоколов. Предназначена для мониторинга безопасности без вмешательства в технологические процессы.

Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes) – комплексное решение для защиты конечных узлов АСУ ТП (SCADA-серверов, АРМ, инженерных станций). Обеспечивает антивирусную защиту, контроль приложений, контроль устройств, защиту от сетевых атак и централизованное управление политиками безопасности.

Kaspersky MLAD (Machine Learning for Anomaly Detection) – специализированный модуль для выявления отклонений в технологических процессах на основе машинного обучения.

Анализирует телеметрию промышленного оборудования и выявляет аномалии, указывающие на кибератаки или технологические сбои.

Kaspersky Unified Monitoring and Analysis Platform – один из ключевых компонентов на пути к реализации единой платформы кибербезопасности. Решение обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, объединяет решения «Лаборатории Касперского» и продукты сторонних поставщиков в единую экосистему, в том числе, является центральным элементом XDR-платформы Kaspersky Symphony XDR.

Опыт работы в отраслях

- | | | | |
|--|---|---|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> Финансовый сектор и ретейл |

Заказчики в сфере ИБ АСУ ТП

**Название организации****Официальный сайт****Корпорация ЭЛАР**www.elar.ru

Компетенции в области ИБ АСУ ТП

Компания ЭЛАР является одним из лидеров в области цифровой трансформации и защиты данных промышленности и оборонного комплекса. Мы являемся разработчиками программной платформы для создания защищенных электронных архивов, которые могут работать с информацией ограниченного доступа. Имеем глубокие компетенции в разработке заказных решений и технологий искусственного интеллекта для обработки и анализа данных. Компания занимается производством отечественной радиоэлектронной продукции – специализированных систем хранения данных на базе оптических дисков для резервного копирования, защиты и долговременного хранения критически-значимой информации. У компании есть лицензии ФСТЭК и ФСБ для создания средств защиты информации и работы с гостайной.

Продукты и/или услуги

Название: ЭЛАРобот НСМ

Назначение: Специализированные российские программно-аппаратные комплексы для резервного копирования, обеспечения долговременного хранения и защиты информации. Комплексы являются роботизированными системами хранения на базе оптических носителей информации (Blu-ray Archival Grade), гарантирующих хранение данных сроком свыше 50 лет. Диски не нужно менять, они не портятся и не стареют. Информацию, записанную на диски, невозможно изменить или удалить, таким образом обеспечивается безусловная защита данных от любых киберугроз и злонамеренных действий. Комплексы поддерживают режим офлайн-хранения, когда критически важные данные перемещаются на хранение в полностью изолированный контур, в том числе в географически удаленном формате.

Опыт работы в отраслях

- | | | | |
|--|---|--|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

ОМК, СУЭК, «ФосАгро», «Комос Групп», «Алмаз-Антей», Газпром

**Название организации****Официальный сайт****Российский системный интегратор УЦСБ**<https://www.ussc.ru/>

Компетенции в области ИБ АСУ ТП

УЦСБ предлагает полный спектр услуг по обеспечению безопасности промышленных систем автоматизации и управления, включая собственные сервисы.

- Аудит АСУ ТП: идентификация и классификация активов, тесты на проникновение, анализ истории инцидентов, оценка рисков, разработка стратегии развития системы безопасности.
- Создание комплексного решения по обеспечению безопасности АСУ ТП: обследование, построение модели угроз и оценка рисков, формирование требований с учетом международных стандартов и лучших практик, разработка проектной и рабочей документации, ввод в действие комплексной системы безопасности.
- Сервисная поддержка: комплекс услуг по техническому сопровождению систем безопасности.

Продукты и/или услуги

Название: CheckU**Назначение:** Решение для самостоятельного контроля соответствия требованиям ИБ.**Название:** Apsafe**Назначение:** Облачная платформа непрерывного анализа защищенности приложений.**Название:** УЦСБ SOC**Назначение:** Сервис для мониторинга и реагирования на инциденты ИБ.**Название:** Экспресс-повышение уровня защищенности**Назначение:** Комплекс мероприятий для оперативного выявления наиболее критичных недостатков ИБ и повышения уровня защищенности ИТ-инфраструктуры за счет применения рекомендованных безопасных конфигураций.**Название:** Сопровождение и техническая поддержка АСУ ТП**Назначение:** Обеспечение непрерывной работы программно-аппаратных комплексов и систем, поддержание максимального уровня защиты информационных ресурсов.

Опыт работы в отраслях

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

Заказчики в сфере ИБ АСУ ТП

«Норникель», «Юнипро», «Лукойл» и другие компании (под NDA).

**Номер
стенда
4.1****Название организации****AKTIV.CONSULTING
(Компания «Актив»)****Официальный сайт**<https://aktiv.consulting/>

Компетенции в области ИБ АСУ ТП

Бизнес-направление AKTIV.CONSULTING специализируется на оказании услуг по консалтингу и аудиту в области ИБ. Специалисты AKTIV.CONSULTING обладают широкими техническими компетенциями и собственными методиками для реализации проектов, требующих комплексной, системной экспертизы в сфере ИБ промышленных организаций, а также представителей других отраслей. Направление использует в работе уникальный подход, который предполагает восприятие организации как целостного организма, где направление ИБ является полноценной бизнес-функцией, гармонично взаимодействующей с остальными подразделениями.

Продукты и/или услуги

Экспертов AKTIV.CONSULTING привлекают для обеспечения:

- создания службы ИБ, внедрения процесса управления рисками ИБ и оценки уровня зрелости ИБ;
- защиты ИС и инфраструктуры, внедрения процессов по защите АСУ ТП и построения СОИБ;
- проведения пентестов, анализа защищенности и RED TEAM;
- моделирования угроз по методологии ФСТЭК РФ, категорирования и внедрения требований по защите объектов КИИ;
- внедрения процесса DevSecOps, SAST, DAST, fuzzing.

Опыт работы в отраслях

- | | | | |
|--|---|--|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> Финансовый сектор и ретейл |

Заказчики в сфере ИБ АСУ ТП

**Номер
стенда
4.3****Название организации****ООО «Интеллектуальные
Сети»****Официальный сайт**<https://igrids.ru/>

Компетенции в области ИБ АСУ ТП

Компания «iGrids» (ООО «Интеллектуальные Сети») – ваш надежный интегратор в области информационной безопасности. Мы предлагаем полный спектр услуг в области проектирования, разработки и внедрения решений по обеспечению информационной безопасности. Имеем собственную лабораторию, позволяющую физически оценить работоспособность, безопасность, а также совместимость выбранного оборудования. Главным приоритетом для нас является сохранение целостности и непрерывности технологического процесса. У нас есть полный набор технических компетенций, современных средств и необходимых лицензий для обеспечения вашей безопасности.

Продукты и/или услуги

Разработка, внедрение и сопровождение комплексных систем обеспечения ИБ:

- Проведение аудита информационной безопасности
- Разработка организационно-распорядительной документации
- Проектирование комплексной системы обеспечения информационной безопасности
- Внедрение программных и технических средств защиты информации
- Обучение персонала
- Техническое сопровождение систем обеспечения информационной безопасности

Собственная лаборатория, позволяющая физически оценить работоспособность, безопасность, а также совместимость выбранного оборудования.

Консультационные услуги по внедрению принципов безопасной разработки ПО.

Опыт работы в отраслях

- | | | | |
|--|--------------------------------------|---|---------------------------------|
| <input checked="" type="checkbox"/> Нефтегаз | <input type="checkbox"/> Металлургия | <input type="checkbox"/> Химическая промышленность | <input type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

ПАО «Россети», АО «Сетевая компания», ПАО «РусГидро», ПАО «СИБУР Холдинг», АО «Восточный Порт», АО «Крымэнерго», АО «Апатит»

Номер
стенда
4.4

Название организации

Официальный сайт

**ИНКОМСИСТЕМ
(АО НИЦ
«ИНКОМСИСТЕМ»)**

<https://incomsystem.ru>

35 лет **ИНКОМСИСТЕМ**
научно-инженерный центр

Компетенции в области ИБ АСУ ТП

Аудит информационной безопасности АСУ ТП; проектирование комплексной системы защиты информации (СОИБ); внедрение технических средств защиты АСУ ТП; экспертное сопровождение решений по защите АСУ ТП; Полный цикл разработки, производства и технической поддержки программируемого логического контроллера «АБАК ПЛК».

Продукты и/или услуги

Название: 1. Безопасность КИИ, АСУ ТП.

2. Программируемый логический контроллер «АБАК ПЛК».

Назначение: 1. Обеспечение комплексной защиты критической информационной инфраструктуры, систем управления технологическими процессами и соответствия требованиям 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) РФ», Приказам ФСТЭК России.
2. «АБАК ПЛК» – программируемый логический контроллер, предназначенный для построения распределенных систем управления (РСУ), противоаварийной защиты (ПАЗ), автоматического контроля загазованности (АСКЗ) и пожарной сигнализации (АСПС).

Опыт работы в отраслях

Нефтегаз

Металлургия

Химическая промышленность

ОПК

Энергетика

Транспорт

Ракетно-космическая промышленность

прочее

Заказчики в сфере ИБ АСУ ТП

ПАО «НОВАТЭК», ПАО «Лукойл», ПАО «Роснефть», ПАО «Сибур», ПАО «ФосАгро», ПАО «Газпром нефть», ПАО «ГМК «Норильский Никель»

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, занимающимся 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

Название: 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

ООО «АНСЕР ПРО»

<https://answerpro.ru/>



Компетенции в области ИБ АСУ ТП

Опыт внедрения и администрирования криптошлюзов в составе АСУ ТП. Организация защищенных каналов связи между технологическими сегментами, настройка VPN и межсетевое экранирование. Управление сертификатами и ключевой информацией, обеспечение корректной работы СКЗИ. Контроль криптографической защиты трафика, изоляция сегментов и защита удаленного доступа к объектам технологической инфраструктуры.

Продукты и/или услуги

VanGuard – криптошлюз с поддержкой алгоритмов ГОСТ шифрования. Предназначен для внедрения в существующую инфраструктуру для обеспечения взаимной аутентификации узлов и защиты передаваемого трафика между устройствами.

VanGuard поддерживает классы защиты KC1, KC2, KC3 в зависимости от варианта исполнения.

Опыт работы в отраслях

- | | | | |
|-------------------------------------|---|---|---|
| <input type="checkbox"/> Нефтегаз | <input type="checkbox"/> Металлургия | <input type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

ФГБОУ ВО «КАМЧАТГТУ», АО «ИНФОРМТЕХТРАНС», Департамент дорожного хозяйства, благоустройства и транспорта администрации города Твери, Администрация местного самоуправления г. Владикавказ, Дирекция по развитию дорожно-транспортной инфраструктуры г. Севастополя, Министерство транспорта и дорожного хозяйства Липецкой области, ГБУ СЕВАСТОПОЛЬСКИЙ АВТОДОР, АО АСТИАГ; ООО ОКБ «Бурстройпроект».

Номер
стенда
4.7

Название организации

Официальный сайт

АО «ИнфоТеКС»

Infotecs.ru



Компетенции в области ИБ АСУ ТП

Комплексное обеспечение безопасности АСУ ТП, ИСУЭ, М2М и IoT-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 автоматике ViPNet SIES Core.
- Миниатюрный крипточип для защиты конечных устройств АСУ, IoT и приборов учета ViPNet SIES Core Nano.
- Программное СКЗИ для устройств верхнего уровня АСУ ТП, IoT и ИСУЭ ViPNet SIES Unit.

Опыт работы в отраслях

- | | | | |
|--|---|--|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП


Название организации
Официальный сайт
АЛТЭК-СОФТ
redcheck.ru


Компетенции в области ИБ АСУ ТП

АЛТЭК-СОФТ – российский разработчик решений в области аудита безопасности и управления уязвимостями под брендом RedCheck.

SCADA-модуль в составе ПО RedCheck, выполняет сканирование компонентов АСУ ТП и сопутствующего ПО в сканируемой сети, определение версий и предоставление информации об известных уязвимостях компонентов, способах их устранения.

Сканирование осуществляется без привилегий или использования учетных записей, что позволяет быстро и эффективно провести аудит защищенности промышленных систем АСУ ТП (SCADA), построить отчет с рекомендациями по устранению и привести технологический сегмент сети в соответствие с требованиями Регулятора.

Продукты и/или услуги

Название: Средство анализа защищенности RedCheck

Назначение: RedCheck – система анализа защищенности и соответствия стандартам ИБ для мониторинга защищенности ИТ-инфраструктуры предприятия. Обеспечивает поиск и анализ уязвимостей из-за неверных настроек параметров безопасности, слабости парольной защиты, несанкционированной установки программного и аппаратного обеспечения, несвоевременной установки критичных обновлений и нарушений принятых политик безопасности.

RedCheck сертифицирован ФСТЭК России, внесен в реестр российского ПО. Его функции реализуют меры защиты информации в ИС и АСУ в соответствии с приказами ФСТЭК России.

Опыт работы в отраслях

- | | | | |
|--|---|--|---------------------------------|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП


Название организации
Официальный сайт
РТТ
<https://ртт.пф/>


Компетенции в области ИБ АСУ ТП

РТТ – 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: RTT-UNAF

Назначение: Универсальная аппаратная платформа для промышленных ПК, АРМ, межсетевых экранов, маршрутизаторов, шлюзов безопасности и другого оборудования.

Название: RTT-M300F

Назначение: Промышленный шлюз безопасности для защиты периметра ИТ-инфраструктуры АСУ ТП и объектов КИИ от НСД, атак, вторжений, вредоносного трафика и киберугроз.

Название: RTT-M200

Назначение: Промышленный МЭ для защиты внутренней ИТ-инфраструктуры АСУ ТП, объектов КИИ и промышленных сетей; обеспечивает инспекцию, анализ и защиту трафика технологического сегмента.

Опыт работы в отраслях

- | | | | |
|--|--------------------------------------|---|---|
| <input type="checkbox"/> Нефтегаз | <input type="checkbox"/> Металлургия | <input type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

Номер
стенда
4.10

Название организации

Официальный сайт

iTPROTECT

www.itprotect.ru

Компетенции в области ИБ АСУ ТП

Компания iTPROTECT 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 17 лет работы эксперты iTPROTECT реализовали сотни 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

iTPROTECT обеспечивает комплексную информационную безопасность (ИБ) промышленной инфраструктуры. В числе услуг – аудит, тестирование на проникновение (pentest), консалтинговые услуги по защите объектов КИИ с учетом 187-ФЗ (от обследования процессов и категорирования объектов КИИ до моделирования угроз и проектирования системы безопасности), аттестация объектов информатизации, а также внедрение и техподдержка ИБ-решений на базе продуктов от лидирующих игроков рынка.

В продуктовом портфеле компании, в частности, такие продукты, как Kaspersky Industrial CyberSecurity for Nodes («Лаборатория Касперского») для защиты узлов в промышленной сети, PT Industrial Security Incident Manager (Positive Technologies) и Kaspersky Industrial CyberSecurity for Networks – для мониторинга технологического трафика, промышленные межсетевые экраны ViPNet Coordinator IG (ИнфоТеКс) и UserGate NGFW.

Опыт работы в отраслях

- | | | | |
|--|---|--|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

Номер
стенда
4.11

Название организации

Официальный сайт

ООО «ИНКОНТОРОЛ»

Inctrl.ru

Компетенции в области ИБ АСУ ТП

Группа компаний «Инконтрол» обладает подтверждённой экспертизой в области информационной безопасности АСУ ТП для объектов КИИ. Более 11 лет опыта в ИБ, 42 проекта по внедрению ИБ в АСУ ТП под ключ и свыше 100 модернизированных систем под требования безопасности. Реализовано 15 полноценных СОИБ уровня предприятия. Компания выполняет категорирование КИИ, проектирование и внедрение СОИБ, настройку АСУ ТП под требования ИБ и сопровождение жизненного цикла систем. В основе решений – собственные доверенные ПАК и промышленное производство.

Продукты и/или услуги

- Название:** ИК.ДИОД – однонаправленная передача данных, 100% защита периметра.
 ИК.ДС – мониторинг техсостояния и событий ИБ АСУ ТП.
 ИК.ОПДУ – защищённое дистанционное управление.
 ИК.УД – безопасный удалённый доступ с контролем действий.
 ИК.ШОФ – безопасный внос/вынос файлов (чистая/грязная зоны).
 ИК.ДМ – однонаправленная передача UDP-трафика во внешние системы.

Назначение: категорирование КИИ; СОИБ «под ключ»; настройка АСУ ТП под ИБ; тестирование совместимости; поддержание жизненного цикла; мониторинг и реагирование; консультации и техподдержка

Опыт работы в отраслях

- | | | | |
|--|---|---|---------------------------------|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input type="checkbox"/> Химическая промышленность | <input type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

ИНТЕР РАО ЕЭС, РУСГИДРО, РОСНЕФТЬ, РОСАТОМ, ЮНИ ПРО, ГАЗПРОМ

Номер
стенда
4.12

Название организации

Официальный сайт

Индид<https://indeed-id.ru/>

Компетенции в области ИБ АСУ ТП

«Индид» – российский разработчик комплекса решений в области защиты айдентити. Продукты «Индид» уже более 15 лет внедряют крупнейшие компании из России и СНГ, работающие во всех отраслях экономики. Программное обеспечение включено в реестр Минцифры (реестр российского ПО), подходит для выполнения требований программы импортозамещения, принятой в РФ, и помогает соблюдать положения различных нормативно-правовых актов в сфере информационной безопасности (государственных стандартов, постановлений ФСТЭК и других подобных документов). «Индид» самостоятельно разрабатывает все свои продукты на территории Российской Федерации. Сайт компании: indeed-id.ru. Штаб-квартира: г. Москва, Россия.

Продукты и/или услуги

Название: **Indeed Privileged Access Manager (PAM)** – контроль доступа привилегированных пользователей

Назначение: • защитить привилегированные учетные записи от несанкционированного доступа; • организовать аудит работы администраторов систем; • контролировать доступ подрядчиков; • записывать действия привилегированных пользователей и расследовать киберинциденты.

Название: **Indeed Access Manager (AM)** – управление доступом к цифровым активам компании с возможностью многофакторной аутентификации (MFA)

Назначение: • построить систему централизованного управления доступом; • заменить простые пароли на многофакторную аутентификацию (SMS, одноразовые пароли, PUSH-уведомления, аппаратные смарт-карты и токены); • защитить удаленный доступ сотрудников к ИТ-ресурсам; • объединить логический доступ к ИТ-системам и физический доступ в помещения.

Название: **Indeed Certificate Manager (CM)** – централизованное управление жизненным циклом ключевых носителей и сертификатов

Назначение: • автоматизировать управление PKI и сократить затраты на ее сопровождение; • внедрить аутентификацию по цифровым сертификатам на смарт-картах и токенах или без них; • организовать внутренний электронный документооборот; • вести учет СКЗИ согласно требованиям регуляторов.

Название: **Indeed Identity Threat Detection and Response (ITDR)** – комплексная защита инфраструктуры айдентити

Назначение: • управлять айдентити и минимизировать риск компрометации данных; • выявлять современные атаки на инфраструктуру айдентити за счет непрерывного мониторинга событий запроса доступа в реальном времени; • мгновенно реагировать в случае обнаружения угрозы; • воплотить принцип «одного окна» для реализации MFA и других мер защиты доменов и система аутентификации; • реализовать MFA нового поколения без установки агентов.

Название: **Octopus Identity Management (IdM)** – централизованное управление привилегиями и доступом к цифровым активам компании

Назначение: • контролировать жизненный цикл доступа всех пользователей ко всем системам компании на всех этапах работы; • централизованно управлять привилегиями пользователей; • ускорить выдачу прав доступа сотрудникам; • предотвращать несанкционированное изменение настроек доступа.

Название: **BearPass** – безопасное хранение и администрирование корпоративных паролей и других секретов

Назначение: • хранить корпоративные пароли и другие секреты безопасным способом; • централизованно управлять доступом к корпоративным секретам; • автоматически генерировать сложные уникальные пароли для каждой ИТ-системы; • подключить двухфакторную аутентификацию для приложений с поддержкой TOTP, биометрии (Face ID, Touch ID) и аппаратных токенов.

Название: **Сервис Indeed MFA** – усиленная защита корпоративных данных с использованием облачных технологий многофакторной аутентификации

Назначение: • значительно повысить безопасность корпоративных ресурсов с помощью многофакторной аутентификации; • избежать сложных процедур развертывания в собственной инфраструктуре; • подключить конечных пользователей (сотрудников) в течение 1 часа; • снизить капитальные затраты на обеспечение ИБ за счет их перевода в разрез OPEX.

Опыт работы в отраслях

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

Заказчики в сфере ИБ АСУ ТП

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

**Номер
стенда
4.13****Название организации****Официальный сайт****UDV Group**<https://udv.group/>**Компетенции в области ИБ АСУ ТП**

- Киберзащита АСУ ТП и объектов КИИ. Комплексный подход к выявлению атак и угроз с гибкостью и инновационными технологиями, сертифицированными ФСТЭК России. Данный подход позволяет обеспечить результативную киберзащиту производства и выполнить требования законодательства в условиях ограниченного бюджета.
- Мониторинг инфраструктуры АСУ ТП и ИТ. Решение для промышленного сегмента реализует мониторинг доступности и производительности инженерной и ИТ-инфраструктуры, аппаратного обеспечения, приложений, серверов и каналов связи.
- Безопасная разработка ПО для ПЛК
- Центр мониторинга информационной безопасности (SOC)
- Выполнение требований законодательства

Продукты и/или услуги**Название:** UDV DATAPK Industrial Kit**Назначение:** Комплексное решение для кибербезопасности любых АСУ ТП, предоставляющее полную видимость ландшафта АСУ ТП, выявляющее атаки и скрытые угрозы до момента их реализации и позволяющее выполнить требования законодательства.**Название:** UDV DATAPK Version Contro**Назначение:** Помогает специалистам АСУ ТП и экспертам по кибербезопасности решить задачу централизованного хранения проектов ПЛК и отслеживания изменений в них.**Название:** UDV ITM**Назначение:** Система зонтичного мониторинга автоматизированных и информационных систем различного назначения, в том числе АСУ ТП.**Опыт работы в отраслях**

- | | | | |
|--|---|---|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input type="checkbox"/> Транспорт | <input type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

Не для разглашения.

**Номер
стенда
4.14****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 отрасли. Разработка и производство средств защиты информации, включая решения для обеспечения ИБ АСУ ТП. Макетирование и тестирование СЗИ. Обеспечение ИБ при внедрении/модернизации/техническом перевооружении АСУ ТП. 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.

Продукты и/или услуги**Название:** InfoDiode**Назначение:** Решения по аппаратной защите, обеспечивают однонаправленную передачу данных, гарантируя защиту объекта на физическом уровне. InfoDiode предназначен для организации обмена данными с критичными сегментами (например АСУ ТП, КИИ, сегменты ГИС). InfoDiode может применяться для обеспечения безопасности АСУ ТП, АСДТУ в организациях и на предприятиях любых отраслей, использующих закрытые сегменты и сети.**Опыт работы в отраслях**

- | | | | |
|--|---|--|---|
| <input checked="" type="checkbox"/> Нефтегаз | <input checked="" type="checkbox"/> Металлургия | <input checked="" type="checkbox"/> Химическая промышленность | <input checked="" type="checkbox"/> ОПК |
| <input checked="" type="checkbox"/> Энергетика | <input checked="" type="checkbox"/> Транспорт | <input checked="" type="checkbox"/> Ракетно-космическая промышленность | <input type="checkbox"/> прочее |

Заказчики в сфере ИБ АСУ ТП

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