Одиннадцатая конференция «Информационная безопасность АСУ ТП КВО»

15–16 марта 2023 г., г. Москва

ПРОГРАММА

ДЕНЬ ПЕРВЫЙ

08.30–10.00 **Регистрация. Работа выставки**

10.00–13.00 **Пленарное заседание**

- **Гаврилов Виктор Евдокимович,**
  модератор, главный научный сотрудник, Федеральный исследовательский центр Информатика и управление Российской академии наук
  Вступительное слово
- **Торбенко Елена Борисовна,**
  начальник управления ФСТЭК России
  Совершенствование нормативно-правовой базы в области информационной безопасности АСУ ТП и практика реализации контрольно-надзорной функции ФСТЭК России в 2022–2023 гг. Краткий анализ количественного и качественного состава атак на значимые объекты КИИ, природа новых векторов атак, структура атак в отраслевом разрезе. Дальнейшие планы регулятора. Сессия вопросов и ответов
- **Акимов Кирилл Александрович,**
  представитель НКЦКИ
  Краткий обзор совершенствования и развития системы ГосСОПКА в 2022–2023 гг. Новое в нормативно-правовой базе
- **Соколов Александр Николаевич,**
  сотрудник, Оперативно-аналитический центр при Президенте Республики Беларусь
  Национальная система обеспечения кибербезопасности
- **Абдихамитов Талгат Канатович,**
  специалист ИБ, Комитет национальной безопасности Республики Казахстан
  Текущая ситуация (законодательство) в сфере ИБ АСУ ТП КВО Республики Казахстан
- **Бочкарёв Сергей Вячеславович,**
  генеральный директор, ООО «АйТи Бастион»;

  Родин Константин Сергеевич,
  руководитель направления по развитию продуктов, ООО «АйТи Бастион»
  Большие привилегии – большая ответственность. Безопасный доступ: от классических постулатов к современным требованиям
- **Александр Познякевич,**
  руководитель направления по защите промышленных инфраструктур, «Лаборатория Касперского»
  Переход от антивирусной защиты и системы обнаружения вторжений к технологии XDR в АСУ ТП
- **Подольный Вадим Павлович,**
  СТО, Лаборатория Технологий Автоматизации
  Современные распределенные системы управления. Современные задачи и амбициозные вызовы. Технологическая независимость и кибербезопасность
- **Андрей Иванов,**
  архитектор решений, ИнфоТекс
  Межсетевой экран и криптошлюз для АСУ ТП и не только
- **Алексей Шанин,**
  директор ООО «СайберЛимфа»
  Экосистема решений UDV group для обеспечения кибербезопасности промышленных предприятий

13.00–14.00 Обеденный перерыв. Работа выставки

14.00–17.15 Методы, технологии и инструменты защиты АСУ ТП

- **Алексей Петухов,**
  руководитель отдела развития, InfoWatch ARMA
  Что и как защищать в АСУ ТП? Переосмысление концепции ИБ АСУ ТП в 2023 году
- **Рыжов Игорь Николаевич,**
  заместитель директора Центра промышленной безопасности, АО НИП «Информзащита»
  Защита объектов КИИ и не только. Новые требования рынка и новые реалии построения ИБ систем
- **Евгений Дружинин,**
  ведущий эксперт по информационной безопасности K2 Tex
  Импортозамещение на практике: архитектура, совместимость, гарантии
- **Плотко Сергей Алексеевич,**
  директор по аналитике и интеграции, НПП «Цифровые решения»
  Подключение средств сетевой безопасности к инфраструктуре АСУ ТП
- **Вячеслав Половинко,**
  руководитель направления собственных продуктов, АМТ-ГРУП
  Решения по защите АСУ ТП с использованием решений класса «диод». Вопросы совместимости СЗИ и других решений в периметре КВО
- **Макаров Алексей Александрович,**
  технический директор, Xello
  Игра с нулевой суммой: как выявить злоумышленника в сегменте АСУ ТП с помощью технологии киберобмана (deception)
- **Максимов Александр Юрьевич,**
  ведущий инженер, «Газинформсервис»
  Проблематика контроля АСУ ТП
- **Татьяна Егорова,**
  заместитель руководителя по вопросам промышленной кибербезопасности, КСБ-СОФТ
  Инженерный подход к ИБ в АСУ ТП
- **Андрей Кузнецов,**
  технический директор Национального киберполигона, «Ростелеком-Солар»
  Как правильно провести киберучения для ИБ-специалистов промышленного предприятия
- **Сеньков Андрей Васильевич,**
  технический директор, ООО «СВД Встраиваемые Системы»
  Нейтрино – операционная система реального времени для защищенных АСУ ТП КВО
- **Позднеев Борис Михайлович,**
  председатель правления Ассоциации «Цифровые инновации в машиностроении» (АЦИМ)
  Информационная безопасность в аспекте цифровой трансформации промышленности

17.15–17.45 Перерыв

17.45–19.15 Дискуссия: «Наложенные vs встроенные средства безопасности АСУ ТП»

Вопросы

- **Возможности, потенциал и границы применения современных наложенных (внешних) средств защиты АСУ ТП**
- **Технологии, типовые механизмы и задачи, решаемые современными встроенными (внутренними) средствами защиты самих АСУ ТП**
- **Кибериммунные продукты, среды и приложения. Идеология, заявленные возможности, преимущества и практическая реализация**
- **Концепция DevSecOps и ее практическое применение к решению задач в области безопасности АСУ ТП. Проверка безопасности открытых библиотек, используемых при разработке АСУ ТП. Теория и практика реализации**
- **Подходы к поиску баланса и построения гибридных схем создания системы защиты АСУ ТП, включающей встроенные и наложенные средства защиты**

Участники

- **Андрей Бондюгин,** руководитель группы по сопровождению проектов защиты промышленных инфраструктур, «Лаборатория Касперского»
- **Алексей Петухов,** руководитель отдела развития, InfoWatch ARMA
- **Подольный Вадим Павлович,** СТО, Лаборатория Технологий Автоматизации
- **Вячеслав Половинко,** руководитель направления собственных продуктов, АМТ-ГРУП
- **Пономарев Дмитрий Анатольевич,** заместитель технического директора по ИБ, ООО Научно-внедренческая фирма «Сенсоры, Модули, Системы»
- **Рыжов Игорь Николаевич,** заместитель директора Центра промышленной безопасности, АО НИП «Информзащита»
- **Сахаров Константин Валерьевич,** директор департамента информационной и компьютерной безопасности АСУ ТП, АО «РАСУ»
- **Сергеев Константин Анатольевич,** директор по развитию, ООО «ИНБРЭС»
- **Сорокина Марина Викторовна,** руководитель продуктового направления, АО «ИнфоТеКС»

19.15–21.00 Фуршет

ДЕНЬ ВТОРОЙ

08.00–09.00 Регистрация участников. Работа выставки

09.00–12.30 Круглый стол: «Опыт защиты АСУ ТП в топливно-энергетическом комплексе и нефтехимической промышленности»

Доклады

- **Седов Сергей Юрьевич,**
  руководитель Центра промышленной автоматизации и метрологии, ПАО «Газпром нефть»
  Современные платформенные решения по промышленной автоматизации и подходы к обеспечению их защиты
- **Александр Николаев,**
  старший аналитик по информационной безопасности, «Лаборатория Касперского»
  Использование кибериммунного шлюза для безопасной реализации цифровых двойников в нефтегазовой отрасли
- **Правиков Дмитрий Игоревич,**
  заведующий кафедрой КБ КВО, РГУ нефти и газа (НИУ) имени И.М. Губкина
  Проблемы кибербезопасности при реализации промышленной революции 4.0 в нефтегазовом секторе
- **Ширикалов Алексей Юрьевич,**
  ведущий инженер поддержки продаж, ООО «АйТи Бастион»
  Практика безопасного разрешения вопросов обеспечения ИБ для случаев удаленного мониторинга и удаленного доступа со стороны вендоров промышленного оборудования и АСУ ТП
- **Подольный Вадим Павлович,**
  СТО, Лаборатория Технологий Автоматизации
  Современные распределенные системы управления. Встроенная модель защиты
- **Алексей Шанин,**
  директор ООО «СайберЛимфа»
  Адекватная защита промышленных сетей объектов ТЭК
- **Алексей Власенко,**
  ведущий менеджер продуктов, ИнфоТеКС
  Решение ИнфоТеКС для защиты данных интеллектуальной системы учета
- **Куликов Сергей Николаевич,**
  заместитель начальника отдела ССПБ, ООО «Распадская угольная компания»
  Борьба с внутренним нарушителем. Ограничение доступа невзрывозащищённых устройств к подземной сети Wi-Fi на угольных шахтах

Вопросы дискуссии

- **Что защищаем. Какие АСУ ТП входят в наиболее распространенные значимые объекты КИИ в электроэнергетике, нефтяной и газовой промышленности. Как и какие объекты категорируются. Примеры конфигурации типовых систем**

- **От чего защищаем. Каковы основные риски и векторы атак. Последствия с точки зрения функциональной безопасности. Специфика и примеры атак в электроэнергетике, нефтяной и газовой промышленности**
- **Как защищаем. Типовые варианты организации системы безопасности. Специфика отраслей и ее учет на методическом, организационном и техническом уровнях. Как и чем помогает Минэнерго. Роль и место отраслевых центров ГосСОПКА в организации защиты предприятий ТЭК. Примеры защиты наиболее распространенных АСУ ТП в отраслях ТЭК**
- **Чем защищаем. Какие продукты отечественных разработчиков наиболее распространены в отраслях ТЭК. Какие дополнительные требования выдвигают предприятия к продуктам и интеграторам. Какие иностранные средства еще остаются у заказчиков и почему. Как оцениваются перспективы импортозамещения и безопасного перехода на отечественные решения**

Участники

- **Алексей Власенко,** ведущий менеджер продуктов, ИнфоТеКС
- **Куртуков Константин Викторович,** менеджер по безопасности критической информационной инфраструктуры, ООО «Распадская угольная компания»
- **Москаленко Андрей Михайлович,** ведущий специалист группы по обеспечению безопасности объектов критической информационной инфраструктуры, ООО «ЛУКОЙЛ-Нижневолжскнефть»
- **Александр Николаев,** старший аналитик по информационной безопасности, «Лаборатория Касперского»
- **Подольный Вадим Павлович,** СТО, Лаборатория Технологий Автоматизации
- **Правиков Дмитрий Игоревич,** заведующий кафедрой КБ КВО, РГУ нефти и газа (НИУ) имени И.М. Губкина
- **Седов Сергей Юрьевич,** руководитель Центра промышленной автоматизации и метрологии, ПАО «Газпром нефть»
- **Устич Наталия Владимировна,** архитектор по ИБ АСУТП, ПАО «Интер РАО»
- **Алексей Шанин,** директор ООО «СайберЛимфа»
- **Ширикалов Алексей Юрьевич,** ведущий инженер поддержки продаж, ООО «АйТи Бастион»

12.30–13.30 Обеденный перерыв. Работа выставки

13.30–15.30 Круглый стол: «Опыт защиты АСУ ТП в металлургии и трубной промышленности»

Доклады

- **Нуйкин Андрей Витальевич,**
  начальник отдела обеспечения безопасности информационных систем, ООО «ЕВРАЗ»
  Защита информации в АСУ ТП. Безопасность технологического сегмента
- **Севостьянов Александр Владимирович,**
  начальник управления информационной безопасности СЭБ, ПАО «ТМК»
  Актуальные вопросы комплексной защиты металлургического предприятия в рамках взаимодействия подразделений информационной и экономической безопасности
- **Авраменко Дмитрий Николаевич,**
  руководитель отдела кибербезопасности АСУ ТП, компания Innostage
  Анализ рисков информационной безопасности в системах промышленной автоматизации: что, где, когда и для чего
- **Сергей Панасенко,**
  директор по научной работе, компания «Актив»
  Комплексная система контроля и мониторинга носителей данных

Вопросы дискуссии

- **Что защищаем. Какие АСУ ТП входят в наиболее распространенные значимые объекты КИИ металлургии. Как и какие объекты категорируются. Примеры конфигурации типовых систем**
- **От чего защищаем. Каковы основные риски и векторы атак. Последствия с точки зрения функциональной безопасности. Специфика и примеры атак в металлургии и металлообработке**
- **Как защищаем. Типовые варианты организации системы безопасности. Специфика отрасли и ее учет на методическом, организационном и техническом уровнях. Примеры защиты наиболее распространенных АСУ ТП в металлургии**

- **Чем защищаем. Какие продукты отечественных разработчиков наиболее распространены в металлургии и металлообработке. Какие дополнительные требования выдвигают предприятия к продуктам и компетенциям интеграторов. Какие иностранные средства еще остаются у заказчиков и почему. Как оцениваются перспективы импортозамещения и безопасного перехода на отечественные решения**

Участники

- **Авраменко Дмитрий Николаевич,** руководитель отдела кибербезопасности АСУ ТП, компания Innostage
- **Нуйкин Андрей Витальевич,** начальник отдела обеспечения безопасности информационных систем, ООО «ЕВРАЗ»
- **Сергей Панасенко,** директор по научной работе, компания «Актив»
- **Севостьянов Александр Владимирович,** начальник управления информационной безопасности СЭБ, ПАО «ТМК»
- **Растунин Алексей Васильевич,** заместитель генерального директора по информационной безопасности, ООО «Завод вакуумной металлургии»

15.30–17.15 Круглый стол: «Опыт защиты АСУ ТП в оборонно-промышленном комплексе и космической промышленности»

Доклады

- **Сычев Артем Константинович,**
  начальник центра мониторинга и реагирования на компьютерные инциденты,
  АО «ИБ Реформ»
  Подходы к оценке уровня зрелости кибербезопасности промышленных предприятий
- **Митюшкин Евгений Александрович,**
  ведущий менеджер по работе с корпоративными клиентами, UserGate
  Построение устойчивого к киберрискам технологического процесса
- **Дополнительный доклад**
  Тема доклада уточняется

Вопросы дискуссии

- **Что защищаем. Какие АСУ ТП характерны и наиболее распространены в отраслях ОПК. Проблематика обеспечения конфиденциальности данных. Специфика ОПК как преимущественно машиностроительного комплекса. Как и какие объекты категорируются. Примеры конфигурации типовых систем**
- **От чего защищаем. Каковы основные риски и векторы атак. Специфика модели угроз. Последствия с точки зрения конфиденциальности и функциональной безопасности. Специфика и примеры возможных атак в ОПК**
- **Как защищаем. Особенности регулирования вопроса в ОПК. Типовые варианты организации системы безопасности. Специфика ОПК на методическом, организационном и техническом уровнях. Варианты защиты наиболее распространенных АСУ ТП в отраслях ОПК**
- **Чем защищаем. Какие продукты отечественных разработчиков наиболее распространены в отраслях ОПК. Какие дополнительные требования выдвигает законодательство к продуктам и интеграторам. Как оцениваются перспективы импортозамещения и безопасного перехода на отечественные решения**

Участники

- **Артамонова Мария Анатольевна,** руководитель направления по цифровизации процессов Департамента по цифровой трансформации, ГК «Ростех»
- **Ахмеев Алексей Владимирович,** начальник Управления информационной безопасности, АО «Концерн «Калашников»
- **Митюшкин Евгений Александрович,** ведущий менеджер по работе с корпоративными клиентами, UserGate
- **Надеин Павел Андреевич,** начальник отдела технической защиты информации и НИОКР, АО «Концерн «НПО «Аврора»

- **Сычев Артем Константинович,** начальник центра мониторинга и реагирования на компьютерные инциденты, АО «ИБ Реформ»
- **Хабибуллин Дамир Мунирович,** начальник управления информационной безопасности, АО «Технодинамика»
- **Дополнительный участник**

17.15–19.00 Круглый стол: «Опыт защиты АСУ ТП на транспорте»

Доклады

- **Безродный Борис Федорович,**
  заместитель начальника Центра – начальник отдела, АО «НИИАС»
  Обеспечение безопасности систем железнодорожной автоматики и механики как объектов КИИ

Вопросы дискуссии

- **Что защищаем. Какие АСУ ТП входят в наиболее распространенные значимые объекты КИИ на транспорте (ж/д, автомобильном, воздушном и морском). Как и какие объекты категорируются, по видам транспорта и инфраструктуры. Примеры конфигурации типовых систем**
- **От чего защищаем. Каковы основные риски и векторы атак. Последствия с точки зрения функциональной безопасности. Специфика и примеры атак на ж/д, автомобильной, воздушной и морской транспортной инфраструктуре**
- **Как защищаем. Типовые варианты организации системы безопасности. Специфика отраслей и ее учет на методическом, организационном и техническом уровнях. Как и чем помогает Минтранс. Примеры защиты наиболее распространенных АСУ ТП по видам транспорта**
- **Чем защищаем. Какие продукты отечественных разработчиков наиболее распространены на транспортных предприятиях. Какие дополнительные требования выдвигают транспортники к продуктам и интеграторам. Как развиваются встраиваемые средства защиты. Как оцениваются перспективы импортозамещения и безопасного перехода на отечественные решения**

Участники

- **Безродный Борис Федорович,** заместитель начальника Центра – начальник отдела, АО «НИИАС»
- **Генералова Полина Юрьевна,** эксперт отдела обеспечения безопасности значимых объектов КИИ ЦИБ, ОАО «РЖД»
- **Рязанов Вячеслав Юрьевич,** руководитель отдела качества и безопасности, ООО «ЛокоТех-Сигнал»

19.00–19.30 Подведение итогов.
Прогноз развития ИБ АСУ ТП. Основные вызовы и тренды на 2023 год

19.30–20.30 Фуршет

Круглый стол
Практика применения контролируемого доступа с компанией «АйТи Бастион»

15 марта с 14.00 до 15:30 в рамках конференции «Информационная безопасность АСУ ТП КВО» состоится круглый стол компании «АйТи Бастион» и компаний заказчиков на тему **«Реальные истории применения системы контроля привилегированного доступа от первого лица»**.
Многие годы идут разговоры о необходимости применения PAM-систем не только в корпоративном, но и промышленном сегменте для обеспечения безопасного контролируемого доступа привилегированных пользователей, подрядных организаций и самих сотрудников к критическому оборудованию. При этом вопросы реального применения были слабо освещены и системы данного класса были мало представлены в сегментах АСУ ТП.

В рамках круглого стола будут рассмотрены следующие вопросы:
- Базовые сценарии применения комплекса СКДПУ НТ на опыте компании «АйТи Бастион»;
- Опыт эксплуатации и применения комплекса СКДПУ НТ на опыте реальных инфраструктур заказчиков;
- Опыт проектирования, эксплуатации и применения комплекса СКДПУ НТ на опыте компании интегратора систем безопасности АСУ ТП.

Встреча направлена на обмен опытом и ответы на вопросы применения систем мониторинга и контроля привилегированных пользователей, автоматизации доступа к информационным системам и построению доверенной среды удаленного доступа.

Компании-спикеры:
1. «АйТи Бастион»
2. «Данные – центр обработки и автоматизации» (ДЦОА)
3. АО «Россети Цифра»
4. iGrids – «Интеллектуальнее сети»