ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ОТЕЧЕСТВЕННЫЙ РЕСУРС ОЦЕНКИ ЗАЩИЩЕННОСТИ АСУ ТП (Ресурс АСУ ТП)

Начальник отдела
«ФАУ ГНИИИ ПТЗИ ФСТЭК России»
Алексей Енютин

Актуальность создания Ресурса АСУ ТП

1.Рост числа компьютерных атак на АСУ ТП, являющиеся объектами КИИ

- За 2022 год (зафиксировано) **самое значительное** увеличение числа выявленных вредоносных программ на компонентах АСУ ТП в России.
- Доля компонентов АСУ ТП, на которых заблокированы вредоносные программы, составляет в России **более 35%**.
- В мире за 2023 год зафиксировано **более 600 атак** на промышленные организации, что на 87 % больше, чем в 2022 году.
- Групп программ-вымогателей, нацеленных на промышленные предприятия, стало **на 35% больше**

2.Широкомасштабный переход на отечественное ПО

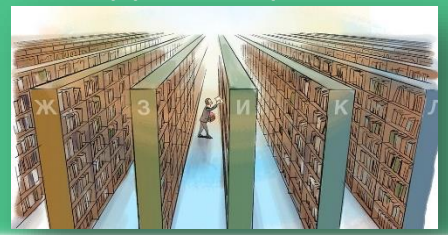
- Необходимость перехода объектов КИИ на отечественное ПО до 2025 года создает острую практическую потребность в расширении объемов производства и номенклатуры отечественных ПЛК, SCADA-систем, ОС. В этих условиях **существенно возрастает потребность в исследованиях по защищенности** этих компонентов.
- Исследования по оценке защищенности производимых компонентов осуществляются вендорами самостоятельно и не всегда в полном объеме **либо не осуществляются совсем**

АКТУАЛЬНОСТЬ СОЗДАНИЯ РЕСУРСА СУ ТП

3. Дефицит специалистов по ИБ

- По результатам государственного контроля установлено, что **недостаточное качество реализации систем защиты** вследствие низкой квалификации специалистов по ИБ имеет широкую распространенность на объектах КИИ.
- Отсутствие у частных исследователей **возможности применения своих навыков** ввиду сложности доступа к дорогостоящим программно-аппаратным компонентам АСУ ТП

4. Отсутствие единого источника исходных данных для защиты АСУ ТП



- Иностранные базы данных угроз и уязвимостей **требуют существенной адаптации** для применения в отечественных АСУ ТП.
- Существующий БДУ содержит сведения об угрозах и уязвимостях для всех информационных систем и **не учитывает специфику АСУ ТП**

5. Внедрение перспективных ИТ в АСУ ТП

- Внедрение таких технологий в АСУ ТП, как IIoT, облачные вычисления, виртуализация, большие данные, приводят к возникновению дополнительных, **не учтенных ранее рисков** реализации угроз безопасности информации.
- Применение неспецифичных до настоящего момента для АСУ ТП технологий **требует детального анализа их защищенности** от угроз безопасности информации

ОТЕЧЕСТВЕННЫЙ РЕСУРС ОЦЕНКИ ЗАЩИЩЕННСТИ АСУ ТП

Цель создания, участники создания

Совершенствование систем защиты информации АСУ ТП и компонентов промышленного Интернета вещей критически важных, потенциально опасных и опасных производственных объектов, повышение качества программного обеспечения, применяемого в указанных системах

Участники создания:

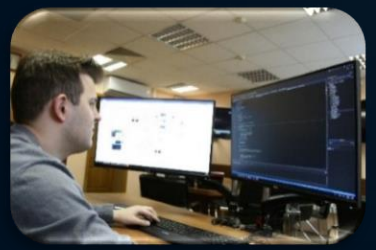
Ростелеком Солар

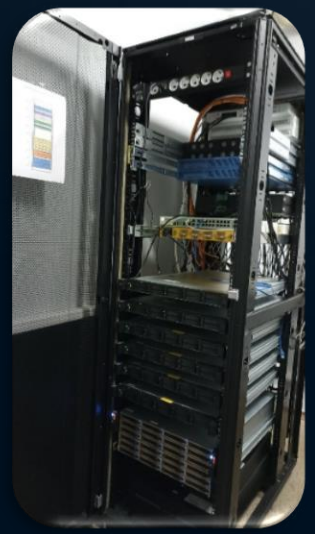
TELECOM INTEGRATION

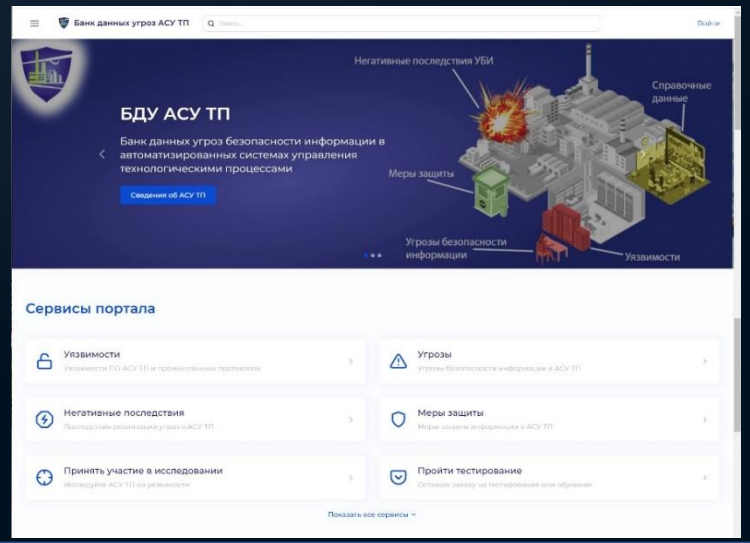
Исследовательский стенд для проведения оценки защищенности перспективных технологий, планируемых к применению в АСУ ТП промышленном интернете вещей

Ресурс АСУ ТП

БДУ АСУ ТП, содержащий сведения об уязвимостях и угрозах в АСУ ТП и потенциальных негативных последствиях реализации угроз

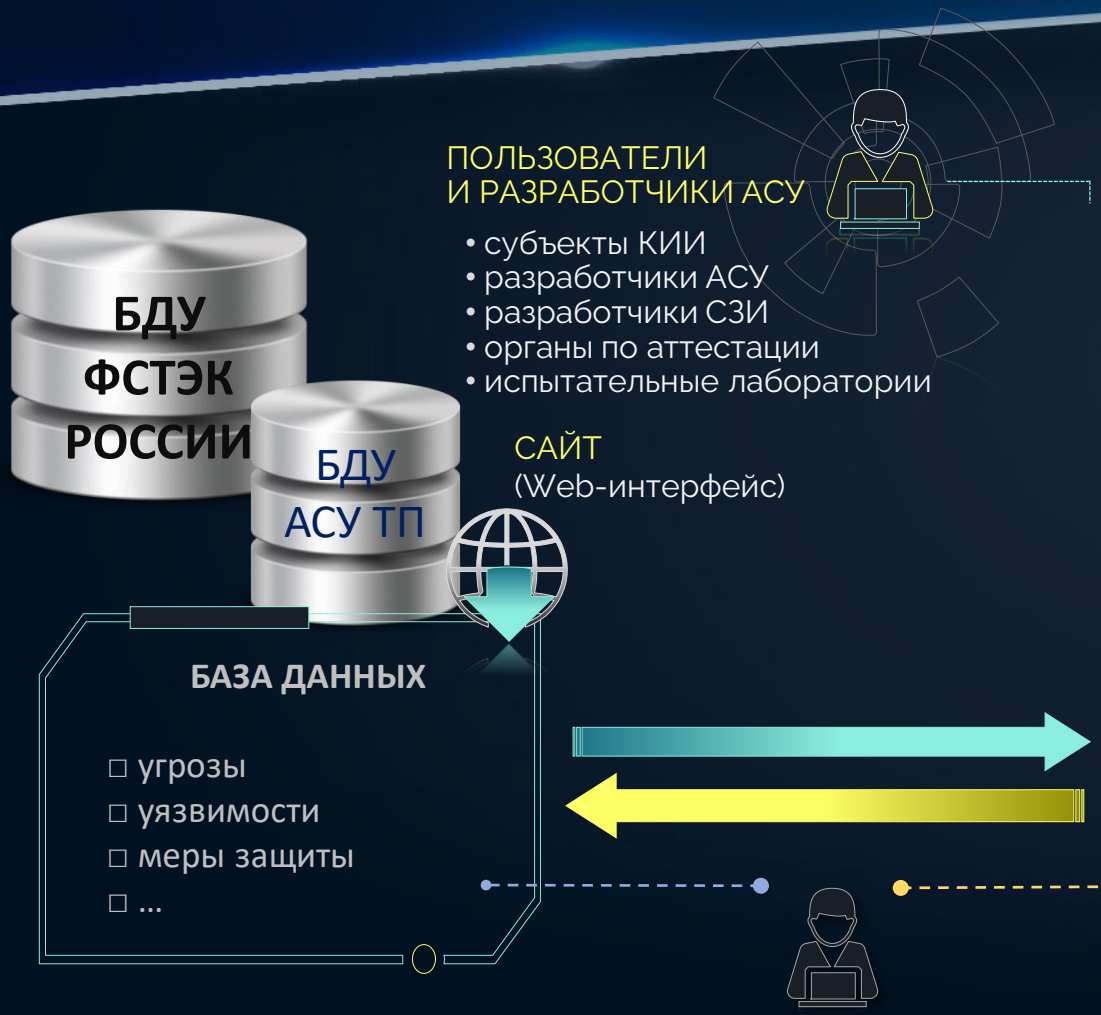






ОТЕЧЕСТВЕННЫЙ РЕСУРС ОЦЕНКИ ЗАЩИЩЕННСТИ АСУ ТП

Назначение



ИССЛЕДОВАТЕЛЬСКИЙ СТЕНД

□ выявление уязвимостей
□ актуализация угроз
□ оценка возможности реализации угроз (сценарии / тактики / техники)
□ оценка защищенности перспективных технологий АСУ (виртуализация / ПИВ / цифровые двойники)
□ анализ, оценка потенциальных негативных последствий
□ выбор мер защиты
□ оповещение операторов АСУ об угрозах / уязвимостях / способах реализации
□ обучение – формирование необходимого уровня компетенций операторов / специалистов / аудиторов

ОТЕЧЕСТВЕННЫЙ РЕСУРС ОЦЕНКИ ЗАЩИЩЕННСТИ АСУ ТП

Решаемые задачи

Предоставление инфраструктуры для компонентов АСУ ТП

Предоставление возможности подключения компонентов АСУ ТП к стенду

Предоставление защищенного удаленного доступа

Оценка защищенности

Задача 1

- Создание виртуальных машин, виртуальных сетей АСУ ТП
- Установка и конфигурирование ПО АСУ ТП

Задача 2

- Подключение реальных компонентов АСУ ТП к виртуальным
- Настройка взаимодействия реальных компонентов АСУ ТП с виртуальными

Задача 3

- Получение ссылки на исследование
- Подключение с использованием защищенного подключения

Задача 4

- Исследования предоставленного фрагмента АСУ ТП
- Формирование отчета и его загрузка в БДУ

Кластеры серверов управления

Коммутационное оборудование

БДУ АСУ ТП

Средства защиты

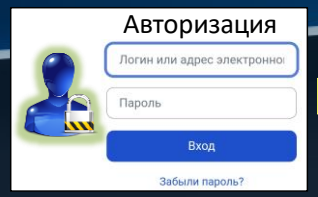
Брокер сетевых пакетов

ОТЕЧЕСТВЕННЫЙ РЕСУРС ОЦЕНКИ ЗАЩИЩЕННСТИ АСУ ТП

Алгоритм работы

Пользователи

- Исследователи
- Разработчики АСУ ТП
- Владельцы АСУ ТП
- Интеграторы систем защиты
- Специалисты испытательных лабораторий
- Обучаемые специалисты



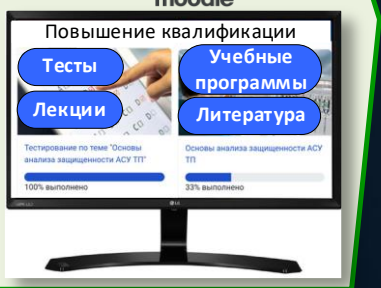
Выбор режима работы

Тестирование, обучение

Получение информации

LMS

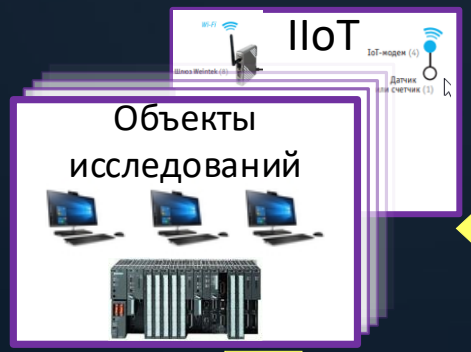
moodle



База данных тестов

Исследования

Выбор объекта исследования



База данных раздела БДУ

Разработка учебно-тренировочных материалов (тестов)

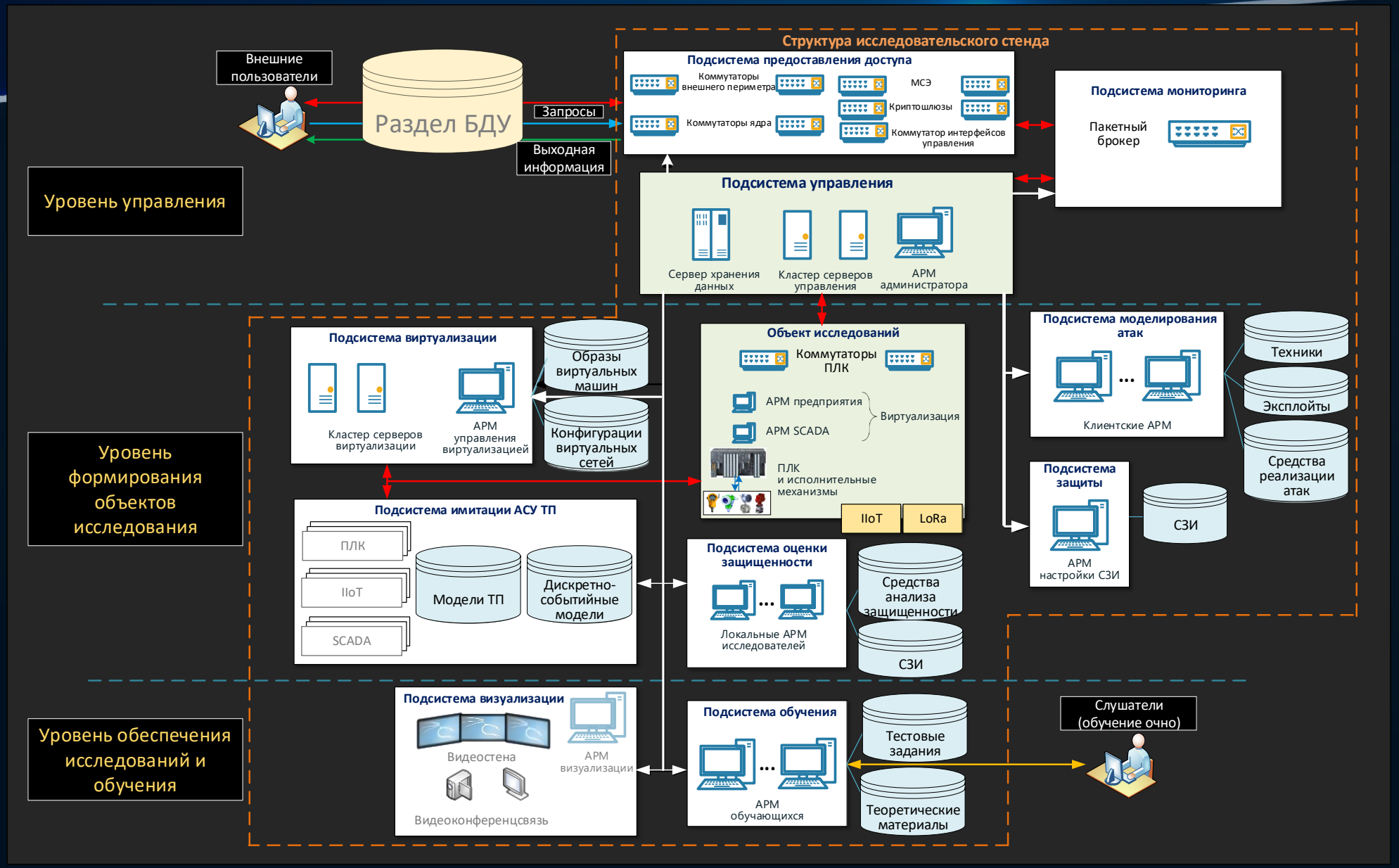
Проведение исследований

Получение новых знаний об уязвимостях

Формирование отчета об исследовании

ИССЛЕДОВАТЕЛЬСКИЙ СТЕНД АСУ ТП

Структура



БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ АСУ ТП

Сервисы БДУ АСУ ТП

Публикация новостей

Выгрузка сведений из БДУ

Инфографика

Тестирование и обучение (внешний сервис)

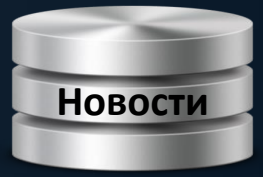
Личные кабинеты

Целевое информирование (рассылки)

Рейтинг исследователей

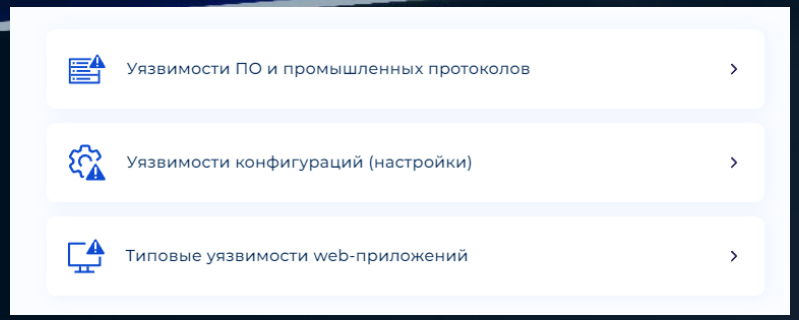
Предоставление доступа к стенду

Контент БДУ АСУ ТП



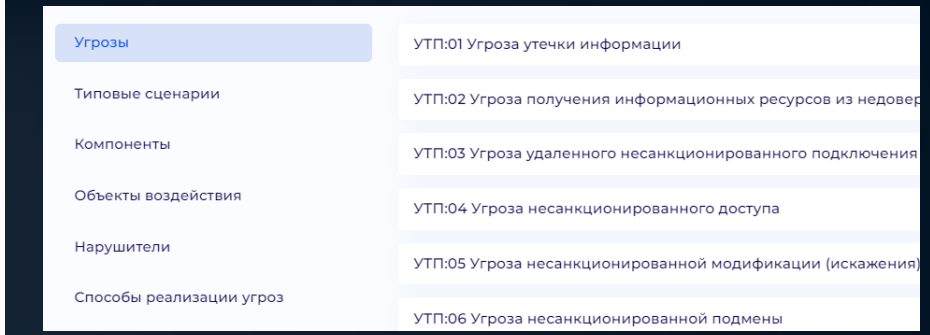
https://bduasutp.fstec.ru

ОСНОВНЫЕ МОДУЛИ БДУ АСУ ТП

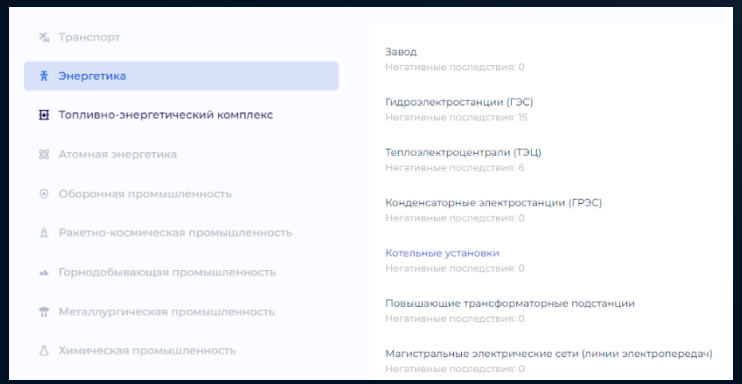


Модуль уязвимостей

Модуль справочных данных

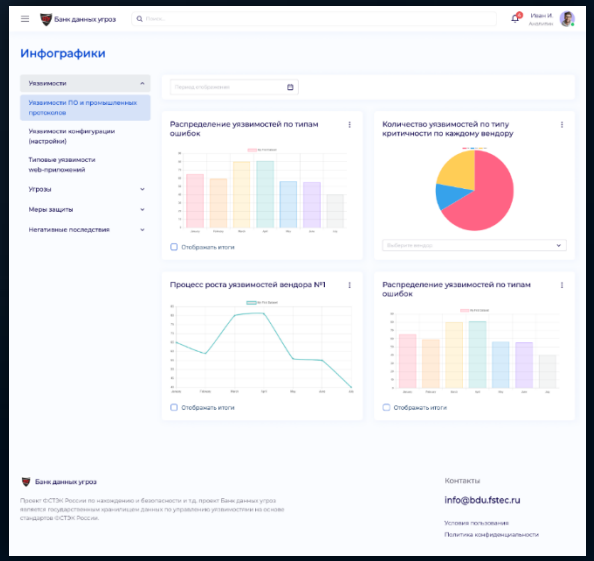


Модуль угроз



Модуль негативных последствий

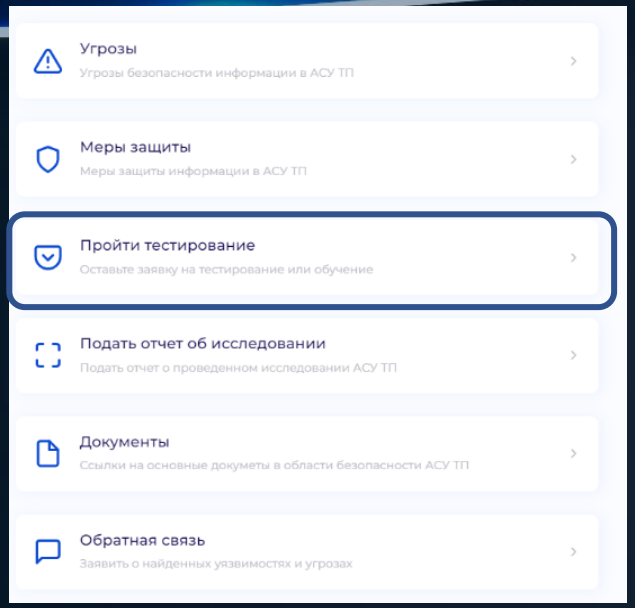
Модуль мер защиты



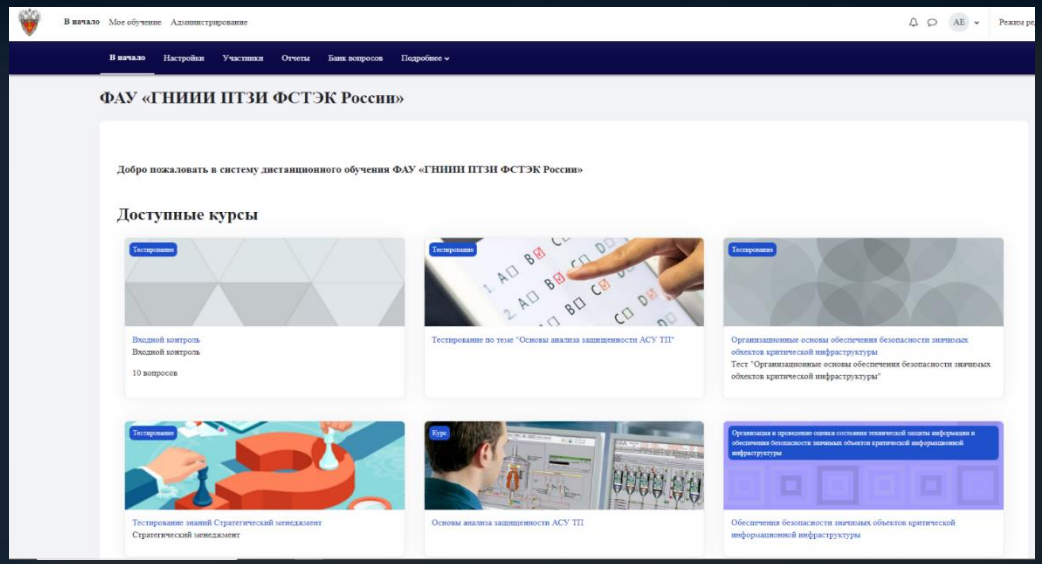
Модуль инфографики

СИСТЕМА ОБУЧЕНИЯ И ТЕСТИРОВАНИЯ СПЕЦИАЛИСТОВ

БДУ АСУ ТП



Интерактивная площадка в сети Интернет



Элементы курса

Задание

Учебный элемент «Задание» позволяет администратору добавлять коммуникативные задания, собирать студенческие работы, оценивать их и предоставлять отзывы

Книга

Модуль «Книга» позволяет преподавателю создать многостраничный ресурс, подобный книге, с главами и подглавами

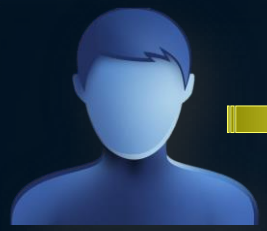
Тест

Элемент курса «Тест» позволяет преподавателю создавать тесты, состоящие из вопросов разных типов

Файл

Модуль «Файл» позволяет преподавателю представить файл как ресурс курса

ИСПОЛЬЗОВАНИЕ РЕСУРСА АСУ ТП НА ПРАКТИКЕ



Исследователь

Проведение исследований

ИССЛЕДОВАТЕЛЬСКИЙ СТЕНД

Оборудование АСУ ТП

Отчет об исследованиях

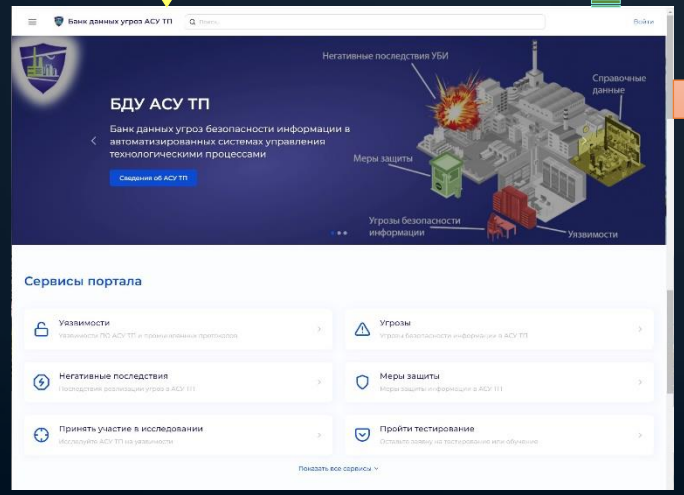
Выявленные:

Угрозы

Уязвимости

Сценарии атак

БДУ АСУ ТП



Сведения об:

Угрозах

Уязвимостях

Сценариях атак

Мерах защиты

Негативных последствиях

Вендор

Устранение уязвимостей

Администратор ИБ АСУ ТП

Актуализация

Частная модель угроз

План мероприятий по защите

Система защиты

АСУ ТП

СОЦИАЛЬНО-ЗНАЧИМЫЕ ЭФФЕКТЫ СОЗДАНИЯ РЕСУРСА АСУ ТП

Повышение защищенности

Повышение защищенности критической инфраструктуры Российской Федерации и эффективности систем обеспечения безопасности КИИ за счет централизованного проведения комплекса исследований угроз и уязвимостей АСУ ТП в кооперации исследователей безопасности, разработчиков, владельцев и операторов АСУ, а также оперативного информирования пользователей о выявляемых угрозах, уязвимостях и необходимых мерах защиты

Информирование об угрозах

Накопление в отечественном ресурсе знаний о способах реализации и лучших практиках выявления и предотвращения угроз безопасности информации в интересах своевременного принятия мер защиты при проектировании и эксплуатации АСУ ТП в различных сферах деятельности

Импортозамещение

Создание условий для безопасного перехода субъектов КИИ на отечественные средства промышленной автоматизации путем реализации технологии обеспечения конструктивной безопасности с учетом результатов исследований защищенности разрабатываемых элементов АСУ ТП

Повышение квалификации персонала

Повышение уровня квалификации персонала, ответственного за реализацию мероприятий по обеспечению безопасности КИИ, за счет созданной системы тестирования специалистов в области защиты информации и проведения практической отработки навыков применения средств защиты информации и проведения практической отработки навыков применения средств защиты информации на реальных компонентах АСУ ТП

Обеспечение полноты исследований защищенности

Вовлечение в процесс защиты КИИ широкого круга исследовательских организаций и независимых экспертов для отработки практических действий по тестированию на проникновение различных, в том числе вновь создаваемых, АСУ ТП и их компонентов

СПАСИБО ЗА ВНИМАНИЕ!

https://bduasutp.fstec.ru

Начальник управления
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
Александр Суховерхов