УЦСБ МОДУЛЬ EPLAT4M «ЦЕНТР ГОССОПКА»

Методические обоснования

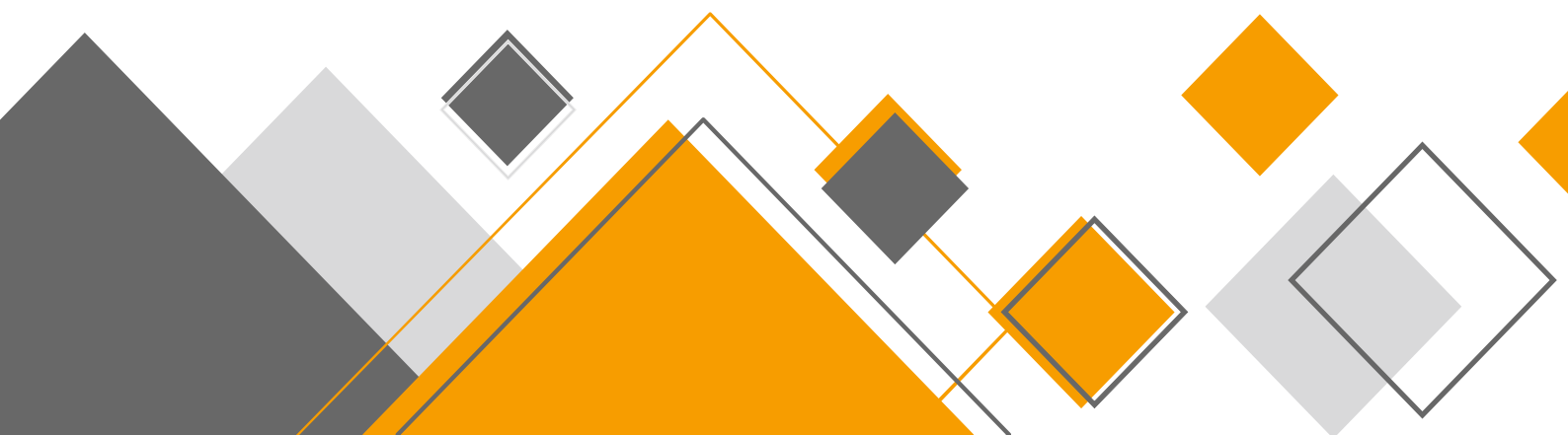
Центр ГосСОПКА – структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА.

Согласно документу ФСБ России «Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА» задачами центра ГосСОПКА являются:

- Обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы (ИР)
- Проведение мероприятий по оценке степени защищенности контролируемых ИР
- Проведение мероприятий по установлению причин компьютерных инцидентов (КИ), вызванных компьютерными атаками на контролируемые ИР
- Сбор и анализ данных о состоянии информационной безопасности в контролируемых ИР
- Осуществление взаимодействия между центрами по вертикали иерархической структуры ГосСОПКА
- Информирование в зоне ответственности субъекта ГосСОПКА заинтересованных лиц по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак
- Формирование и поддержание в актуальном состоянии информации о контролируемых ИР

В рамках своей деятельности центр ГосСОПКА взаимодействует с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) по вопросам обеспечения безопасности ИР и направляет следующую информацию:

- Информация о зоне ответственности центра ГосСОПКА, включая результаты инвентаризации ИР
- Информация о защищенности ИР
- Данные о компьютерных атаках и КИ
- Данные об актуальных угрозах и самостоятельно обнаруженных индикаторах компрометации ИР



МОДУЛЬ EPLAT4M «ЦЕНТР ГОССОПКА»

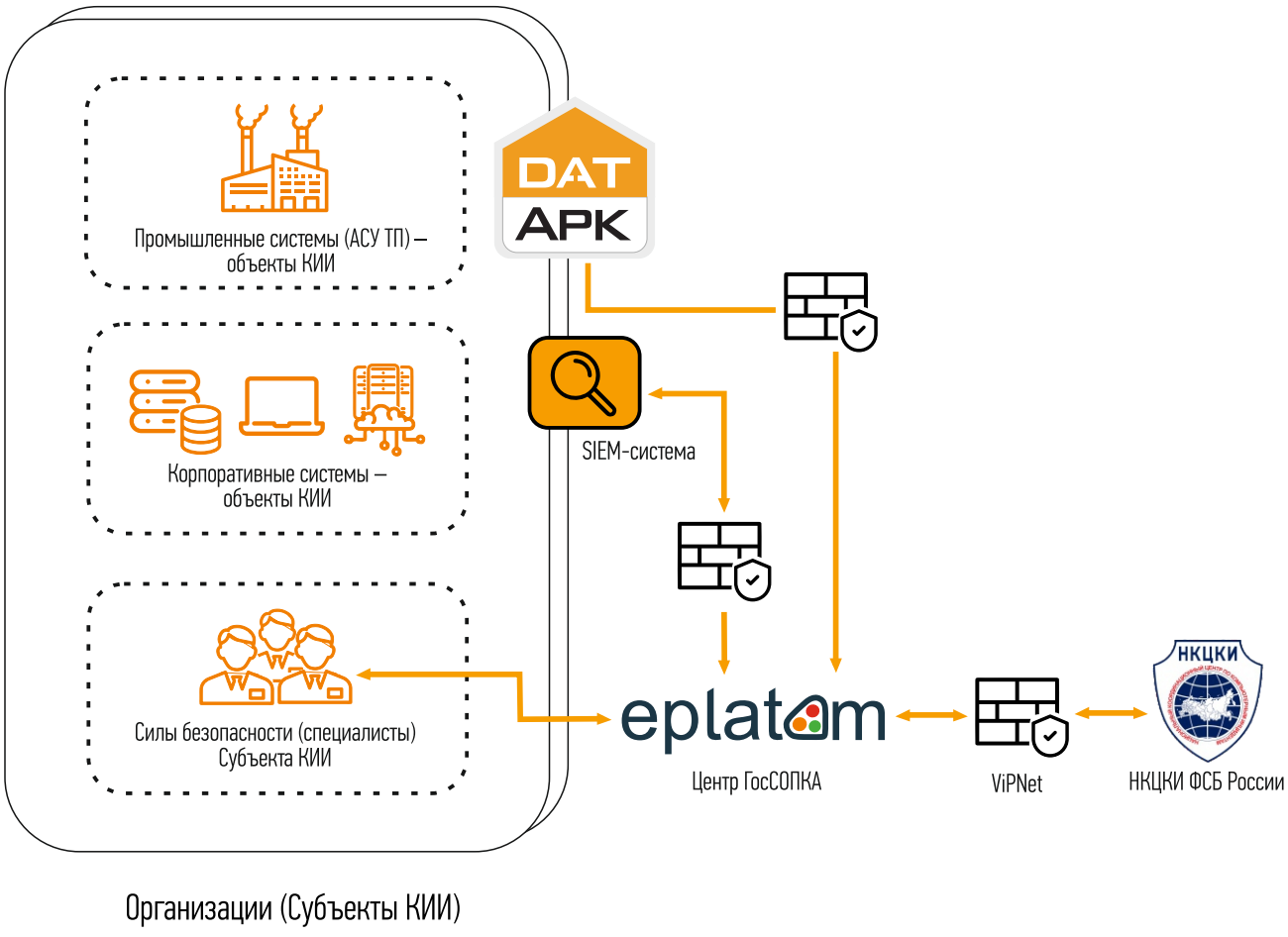
Назначение ПО «модуль ePlat4m «Центр ГосСОПКА»

Программное обеспечение «модуль ePlat4m «Центр ГосСОПКА» представляет собой функциональный модуль для платформы автоматизации ePlat4m Security GRC (http://eplat4m.ru/). Данный модуль предназначен для организации взаимодействия ведомственных, корпоративных и коммерческих центров кибербезопасности с НКЦКИ.

В модуле ePlat4m «Центр ГосСОПКА» реализованы следующие функции:

- Личный кабинет субъекта КИИ (клиента Центра ГосСОПКА)
- Рабочие области специалистов Центра ГосСОПКА в соответствии с ролевой моделью
- Ведение карточек с информацией о субъектах и объектах критической информационной инфраструктуры (КИИ)
- Регистрация КИ и ведение карточек КИ для каждого зарегистрированного субъекта КИИ
- Двустороннее взаимодействие Центра ГосСОПКА и субъекта КИИ
- Двустороннее взаимодействие с НКЦКИ

Архитектура решения на базе модуля ГосСОПКА



ПЛАТФОРМА АВТОМАТИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (СУИБ)

Назначение ePlat4m:

- Автоматизация деятельности организации в области ИБ в соответствии с законодательными и бизнес-требованиями, а также с концепцией GRC
- Организация совместной работы различных категорий пользователей: высшего руководства, подразделения ИТ, подразделения ИБ, работников организации
- Централизованное хранение информации по вопросам ИБ
- Автоматизированный сбор и систематизация данных из внешних информационных систем и средств защиты информации
- Представление информации в графическом, табличном и ином удобном виде

Модули ePlat4m:

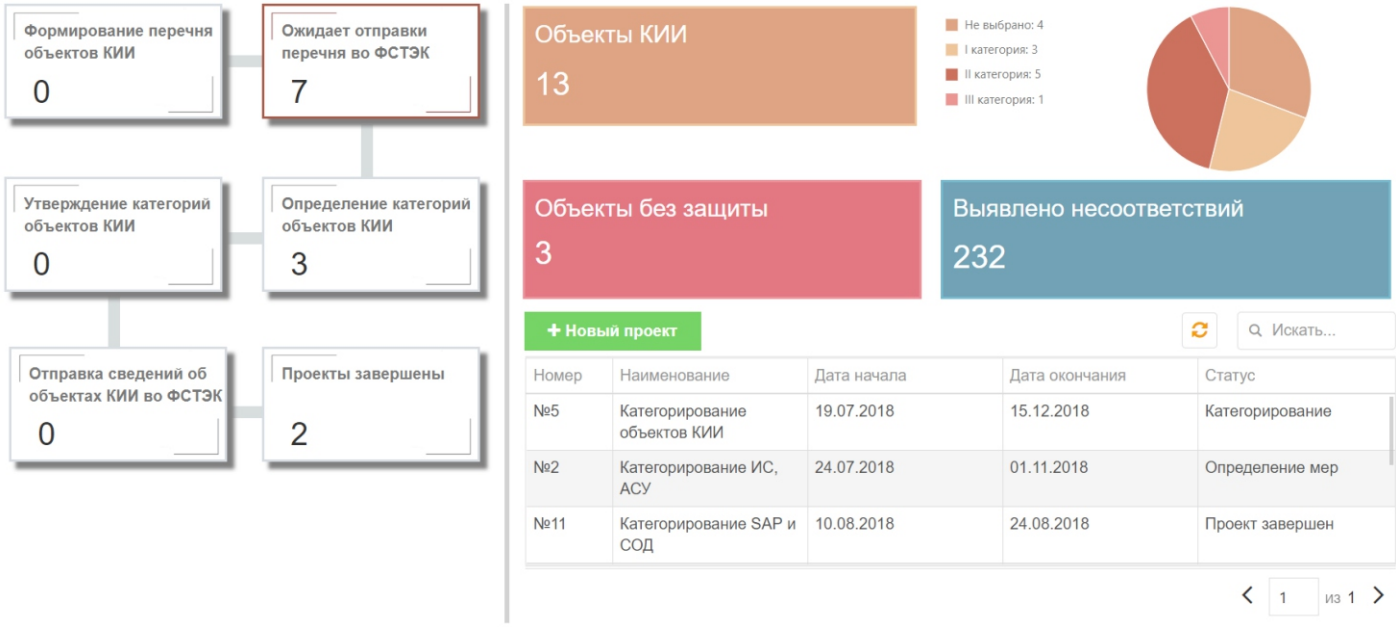
Модульный принцип системы позволяет использовать экспертизу компаний интеграторов, подключая готовые модули, и разрабатывать собственные решения

Управление активами	Автоматизирует процессы учета и классификации информационных и физических активов
Управление рисками ИБ	Автоматизирует процессы идентификации, анализа, оценки и обработки рисков ИБ
Управление инцидентами ИБ	Автоматизирует процессы регистрации, обработки инцидентов ИБ
Работа с персоналом по вопросам ИБ	Автоматизирует процессы доведения организационно-распорядительной документации и контроля знаний сотрудников по требованиям ИБ
Контроль соответствия требованиям ИБ	Автоматизирует процессы внутреннего аудита и оценки соответствия СУИБ организации требованиям по ИБ

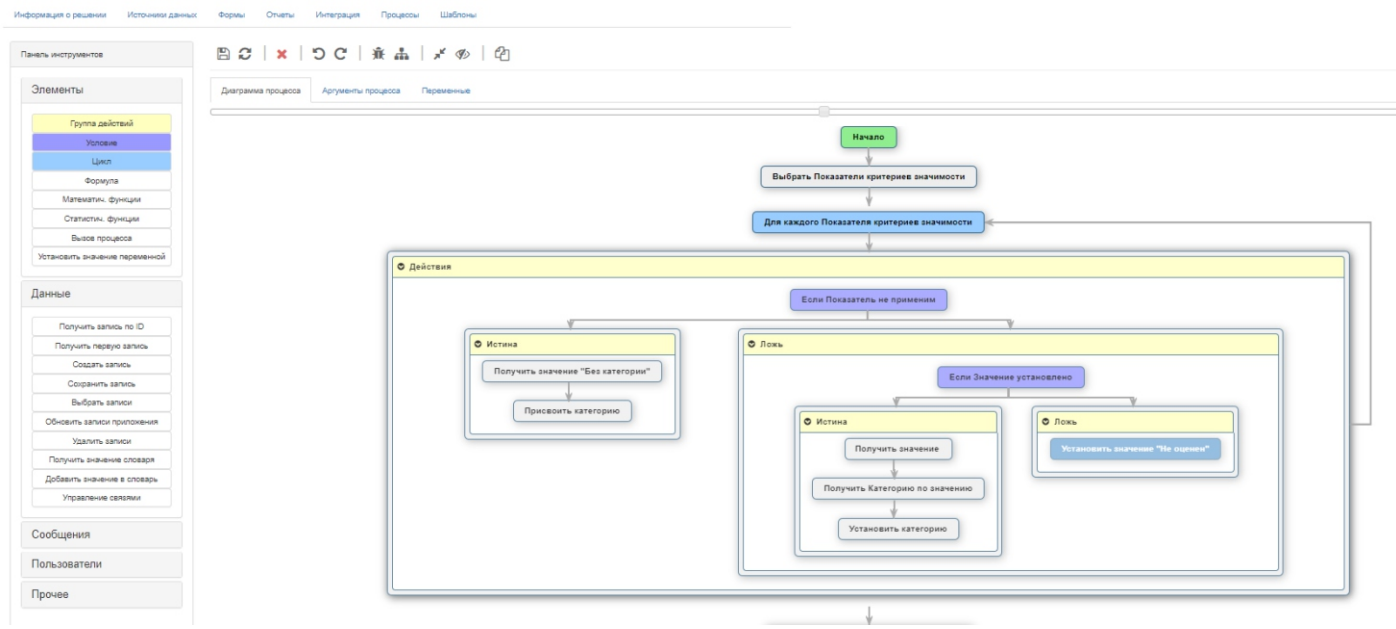
ИНТЕРФЕЙС

ePlat4m имеет эргономичный современный web-интерфейс. Представление и степень детализации данных зависит от роли пользователя. Все функциональные модули связаны между собой, и данные одного модуля могут быть представлены в контексте рабочей области другого.

Рабочая область эксперта по КИИ



Пример разработки процесса ePlat4m



Контакты:

ООО «УЦСБ»
+7 (343) 379-98-34
info@ussc.ru
www.ussc.ru