

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

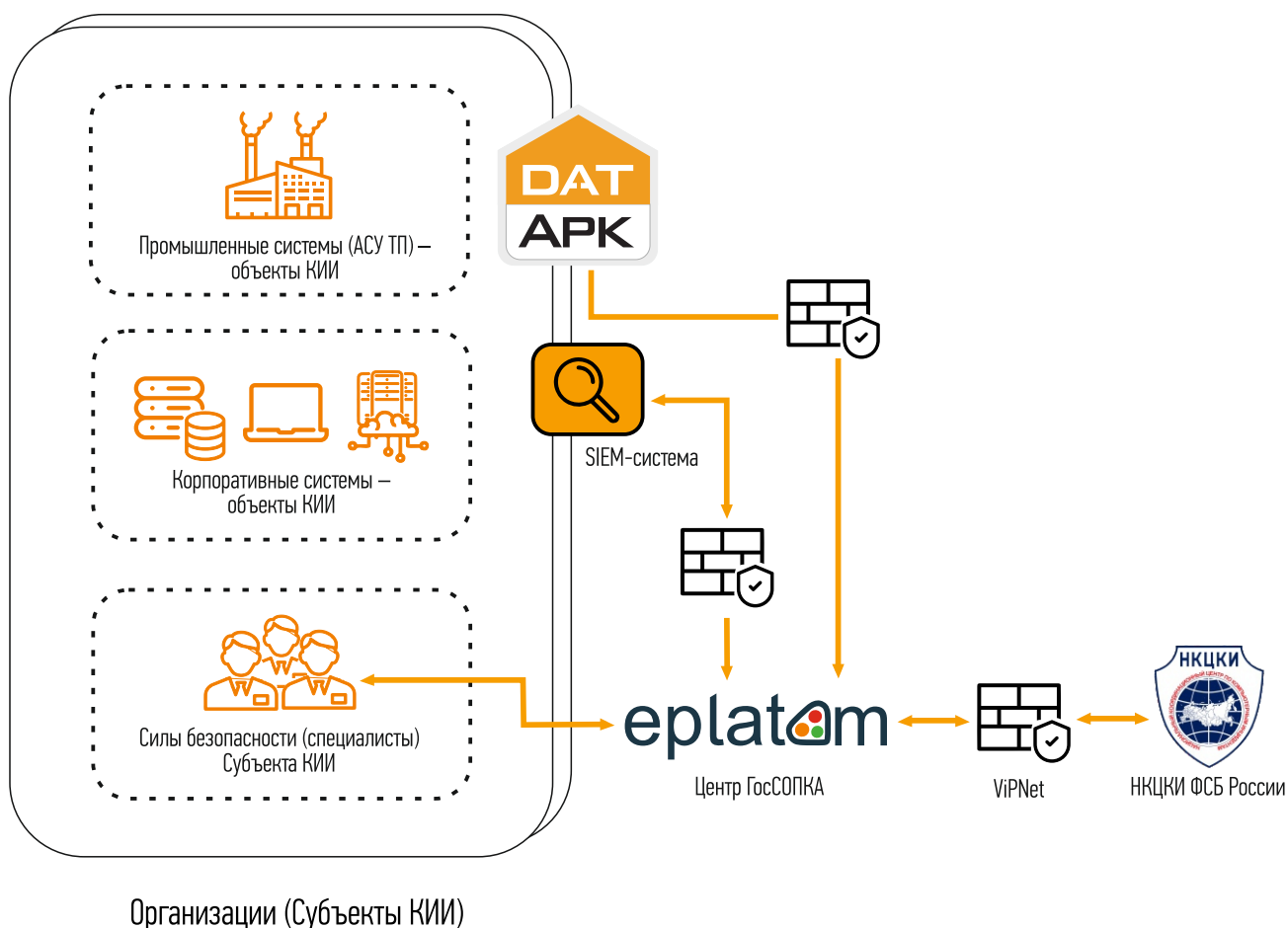
Назначение ПО «модуль ePlat4m «Центр ГосСОПКА»

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





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

Формирование перечня объектов КИИ 0

Ожидает отправки перечня во ФСТЭК 7

Утверждение категорий объектов КИИ 0

Определение категорий объектов КИИ 3

Отправка сведений об объектах КИИ во ФСТЭК 0

Проекты завершены 2

Объекты КИИ 13

- Не выбрано: 4
- I категория: 3
- II категория: 5
- III категория: 1

Объекты без защиты 3

Выявлено несоответствий 232

+ Новый проект 🔍 Искать...

Номер	Наименование	Дата начала	Дата окончания	Статус
№5	Категорирование объектов КИИ	19.07.2018	15.12.2018	Категорирование
№2	Категорирование ИС, АСУ	24.07.2018	01.11.2018	Определение мер
№11	Категорирование SAP и СОД	10.08.2018	24.08.2018	Проект завершен

1 из 1

Пример разработки процесса ePlat4m

Информация о решении | Источники данных | Формы | Отчеты | Иллюстрации | Процессы | Шаблоны

Панель инструментов

Элементы

- Группа действий
- Условие
- Цикл
- Формула
- Математик, функции
- Статистик, функции
- Вызов процесса
- Установить значение переменной

Данные

- Получить запись по ID
- Получить первую запись
- Создать запись
- Сохранить запись
- Выбрать запись
- Обновить запись приложения
- Удалить запись
- Получить значение словаря
- Добавить значение в словарь
- Управление связями

Сообщения

- Пользователи
- Прочие

Диаграмма процесса | Аргументы процесса | Переменные

```

    graph TD
      Start([Начало]) --> Select[Выбрать Показатели критериев значимости]
      Select --> Loop[Для каждого Показателя критериев значимости]
      Loop --> ActionBlock
      subgraph ActionBlock [Действия]
        direction TB
        A1[Если Показатель не применим] --> A1T[Истина]
        A1 --> A1F[Ложь]
        A1T --> A1T1[Получить значение "Без категории"]
        A1T1 --> A1T2[Присвоить категорию]
        A1F --> A1F1[Если Значение установлено]
        A1F1 --> A1F1T[Истина]
        A1F1 --> A1F1F[Ложь]
        A1F1T --> A1F1T1[Получить значение]
        A1F1T1 --> A1F1T2[Получить Категорию по значению]
        A1F1T2 --> A1F1T3[Установить категорию]
        A1F1F --> A1F1F1[Установить значение "Не оценен"]
      end
      A1F1F1 --> Loop
  
```

Контакты:

☎ 000 «УЦСБ»
☎ +7 (343) 379-98-34

✉ info@ussc.ru
🌐 www.ussc.ru

