XIV ВСЕРОССИЙСКАЯ научно-практическая конференция
Екатеринбург 18-19 октября

МУНИЦИПАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ
ДОСТИЖЕНИЯ · ПРОБЛЕМЫ · ПЕРСПЕКТИВЫ

Автоматизация процесса категорирования объектов КИИ

Касьянов Роман. Руководитель направления автоматизации процессов ИБ
Уральский Центр Систем Безопасности.

Процессы информационной безопасности

Основания для автоматизации процессов ИБ

- Распределенная структура организации
  - Отсутствие специалистов ИБ в филиалах
  - Требования вышестоящей организации
- Значимые инциденты вызванные несовершенством управления ИБ
  - Проблемы взаимодействия ИБ и ИТ
  - Человеческий фактор в процессах реагирования и контроля
- Отсутствие специалистов по ИБ на предприятии или в филиалах
  - Выполнение требований регуляторов по ИБ
  - Ограниченный бюджет на услуги профильных интеграторов

Платформа автоматизации процессов ИБ

- Гибкая платформа автоматизации. Расширение стандартного функционала
- Модульный принцип. Наращивание функционала по мере необходимости
- Техническая и экспертная поддержка
- Реестр сертифицированных СЗИ. Сертификат № 3796
- Единый реестр российского ПО № 3733

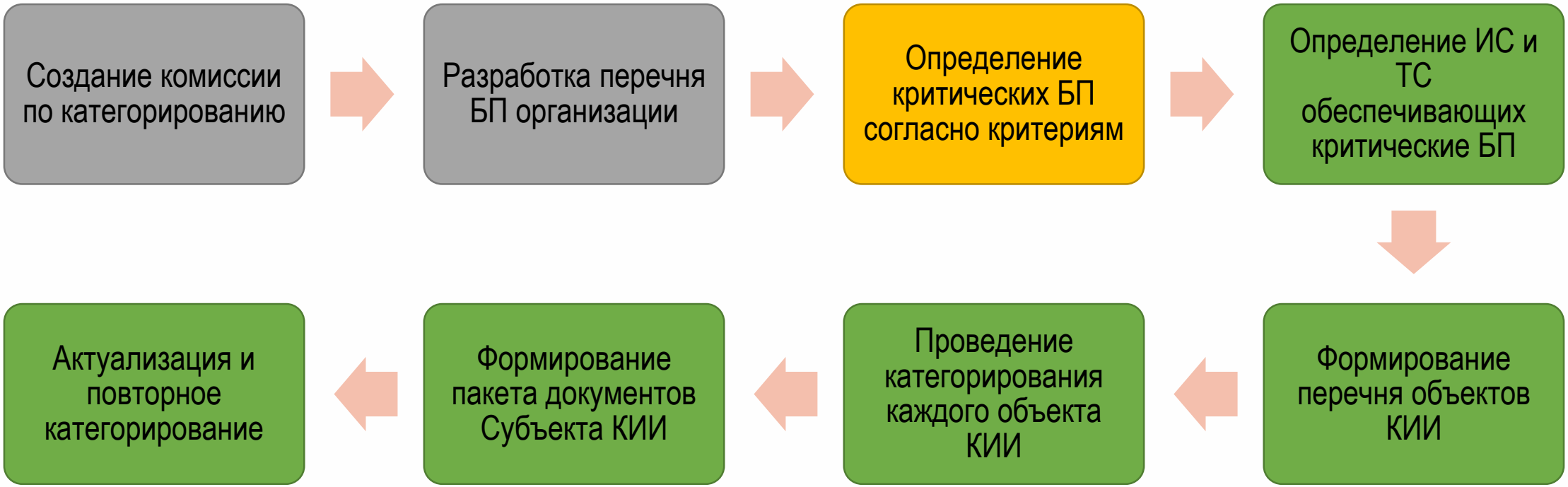
Возможности eplatform

- Готовые модули для распространенных задач ИБ
  - Управление активами, Управление рисками, Управление инцидентами, Классификация и категорирование, Управление ПДН, Управление доступом и другие
  - Все модули открыты для изменения
- Разработка собственных модулей
  - Встроенная среда автоматизации процессов
- Интеграция со смежными системами
  - MaxPatrol SIEM, Infowatch, RSA Archer, MS System Center, MS SQL Server и другие
  - Push & Pull API для интеграции

Сценарии применения eplatom

- Агрегация и дедупликация событий от систем ИБ (SIEM, DLP, IPS/IDS)
  - Центр мониторинга и реагирования на инциденты
  - Аналитический центр ИБ
- Автоматизация процессов управления событиями, инцидентами и пр.
  - Взаимодействие служб ИБ, ИТ, Корп. безопасности, Подрядчиков.
  - Управление распределенной службой ИБ и аутсорсингом ИБ
- Автоматизация отчетности
  - Классификация ОЗ, **Категорирование объектов КИИ**, Соответствие требованиям

Автоматизация этапов процесса категорирования



Определение ИС, ПО и ТС

Бизнес-процесс	Информационная система	Серверное оборудование	Серверное ПО	Рабочие станции / Прикладное ПО
Основное производство	ИС1	Сервер 1	Windows Server SQL Server	АРМ1: - Windows 7 - MS Office
		Сервер 2	Windows Server 1С Server	АРМ2: - Windows 7 - 1С
		СХД 1	--	--
	ИС2	Сервер 3	Windows Server Web App	АРМ1: - Windows 7 - MS Office

Автоматизация сбора данных о ИС и ТС

3 БП * 5 ИС * 10 Серверов * 15 Системного ПО * 15 Прикладного ПО * 50 АРМ

= Более 1000 записей

- **Интеграция с существующими CMDB и BPM.** Данные автоматически загружаются из существующих систем. Актуально для крупных организаций с развитой автоматизацией
- **Загрузка данных из XLSX, XML, CSV.** Данные загружаются из шаблонных файлов. Актуально для удаленных площадок с низкой автоматизацией
- **Связь БП → ИС → ТС → ПО.** Структурирование данных для дальнейшей обработки. Актуально для объектов КИИ с большой ИТ инфраструктурой

Категорирование объекта КИИ

Объект КИИ	Актуальные угрозы	Модель нарушителя	Возможные последствия	Защитные меры Реализованы / Не реализованы	Мнение эксперта
Объект 1	209 угроз в БДУ ФСТЭК	6 Вариантов	14 Критериев	Порядка 170 требований (Приказ ФСТЭК России №17) (Приказ ФСТЭК России №21) (Приказ ФСТЭК России №31)	Эксперт 1 Эксперт 2 Эксперт 3
Объект 2	-//-	-//-	-//-	-//-	-//-
Объект 3	-//-	-//-	-//-	-//-	-//-

Автоматизация процедуры категорирования

2 объекта КИИ * 209 Угроз * 5 Экспертов * 170 требований ФСТЭК

= 300 – 400 вопросов

- **Фильтрация неприменимых угроз, требований, мер защиты.**
  Исключение из опроса неактуальных угроз и мер защиты на основании общей архитектуры объекта

- **Автоматизация сбора опросных листов и процедуры согласования.**
  Возможность проведения опроса непосредственно в системе или заочно путем заполнения файлов-опросников.

Автоматизированное формирование документов

Перечень объектов КИИ, подлежащих категорированию

Акт категорирования объектов КИИ

Сведения о результатах присвоения объекту КИИ категории значимости

- Соответствие требованиям законодательства
- Единый формат для всех филиалов и объектов
- Реестр документов по категорированию КИИ

Повторное категорирование и актуализация

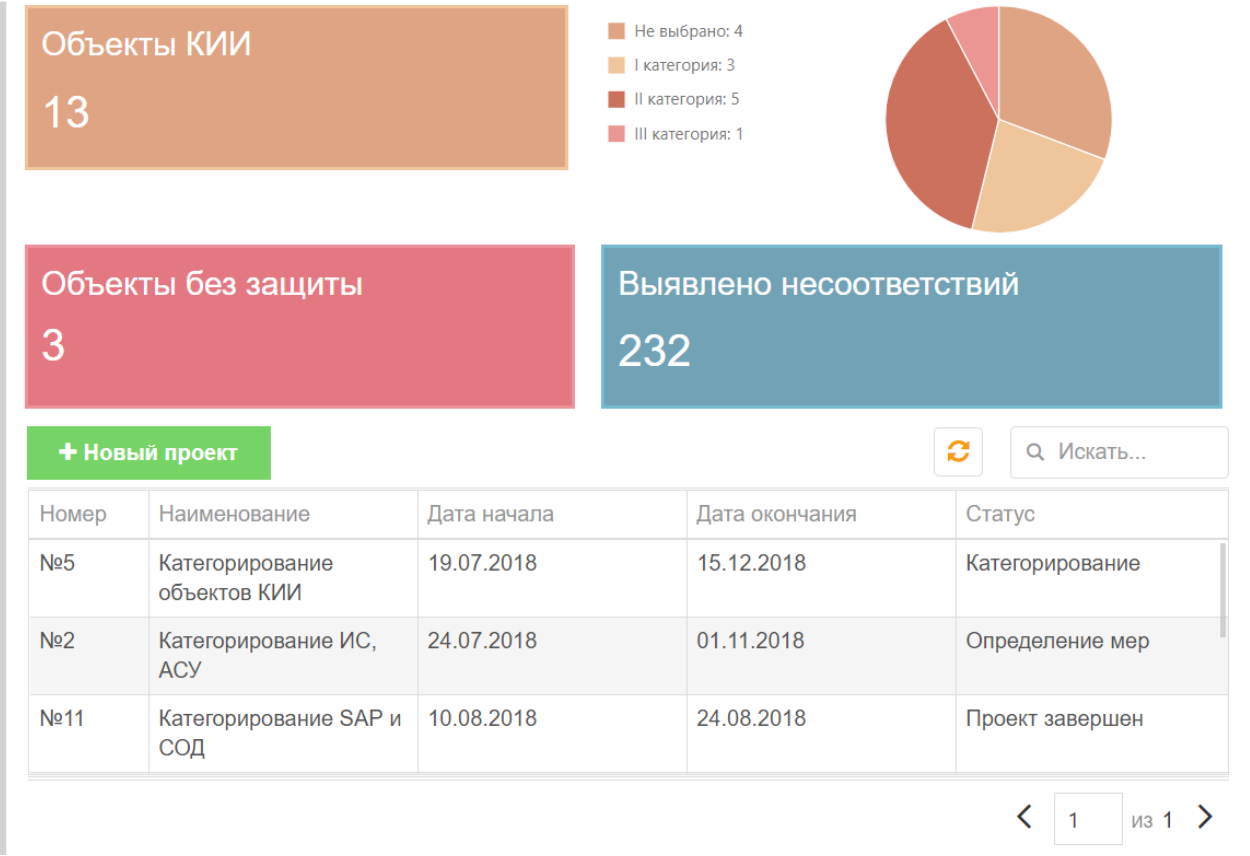
Пересмотр категории при изменении объекта КИИ

- Использование ранее внесенных данных

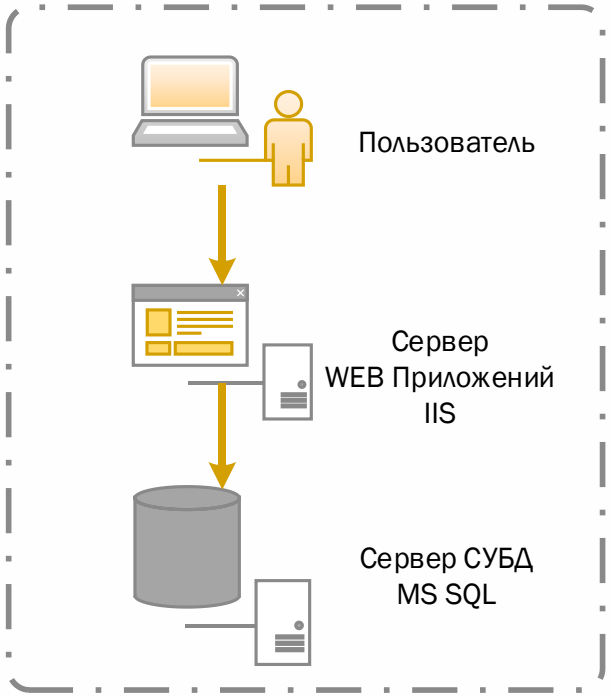
Повторное категорирование через 5 лет

- Применение новых шаблонов документов в случае их изменения

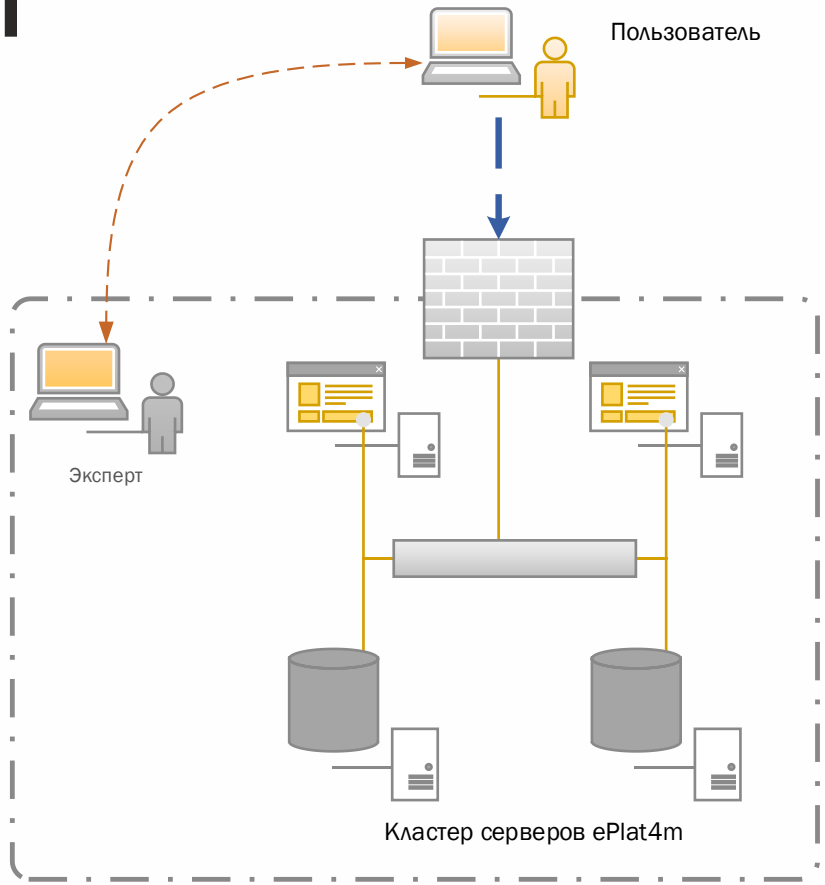
Интерфейс пользователя eplatom



Архитектура eplatom



Размещение в сети заказчика



Размещение в ЦОД УЦСБ

Решение от компании УЦСБ

ePlat4m как Проект:

- Размещение в сети заказчика
- Полный цикл реализации:
  - Предпроектный анализ
  - Индивидуальные сценарии автоматизации
  - Интеграция с системами заказчика
  - Опытная эксплуатация и обучение

ePlat4m.КИИ как Сервис:

- Размещение в ЦОД УЦСБ
- Быстрый старт
  - Не требует капитальных затрат
  - Консультации эксперта включены в стоимость
  - Стандартные сценарии автоматизации
  - Готовые коннекторы интеграции

Дополнительная информация

- http://eplat4m.ru/ - Видеопрезентации, документация
- Стенд ePlat4m. КИИ на МИС 2018
- Вводный вебинар и Демо доступ по запросу

Контакты:

Роман Касьянов
Руководитель направления, Аналитический центр
Уральский центр систем безопасности

620100, Екатеринбург, ул. Ткачей, 23, 11й этаж.
Тел.: +7 (343) 379-98-34 (вн. 1440)
Моб.: +79226124243
Факс: +7 (343) 382-05-63
E-mail: rkasyanov@ussc.ru