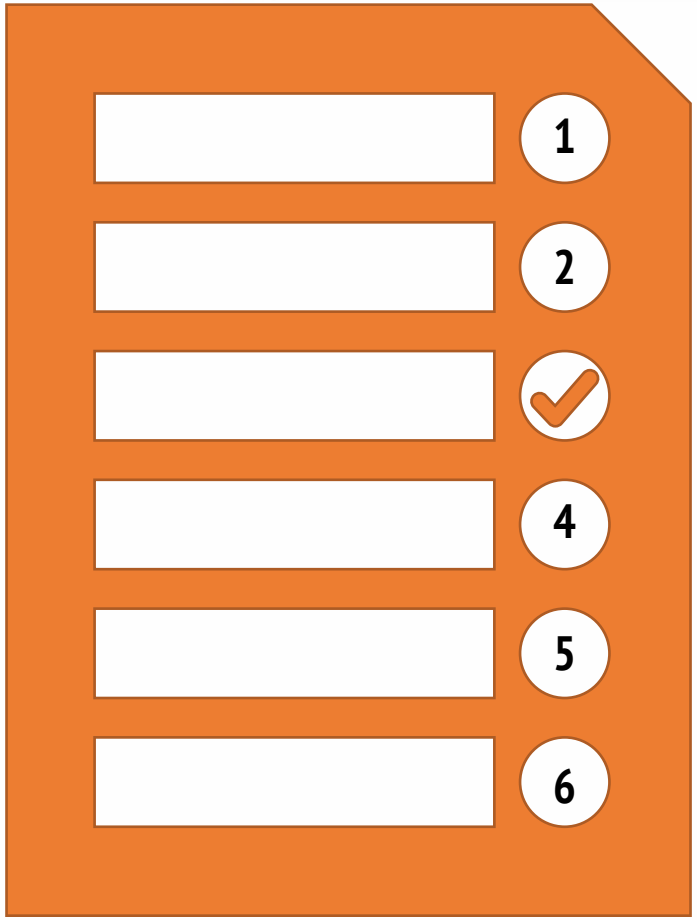
Трудности реализации требований 187-ФЗ для промышленных предприятий

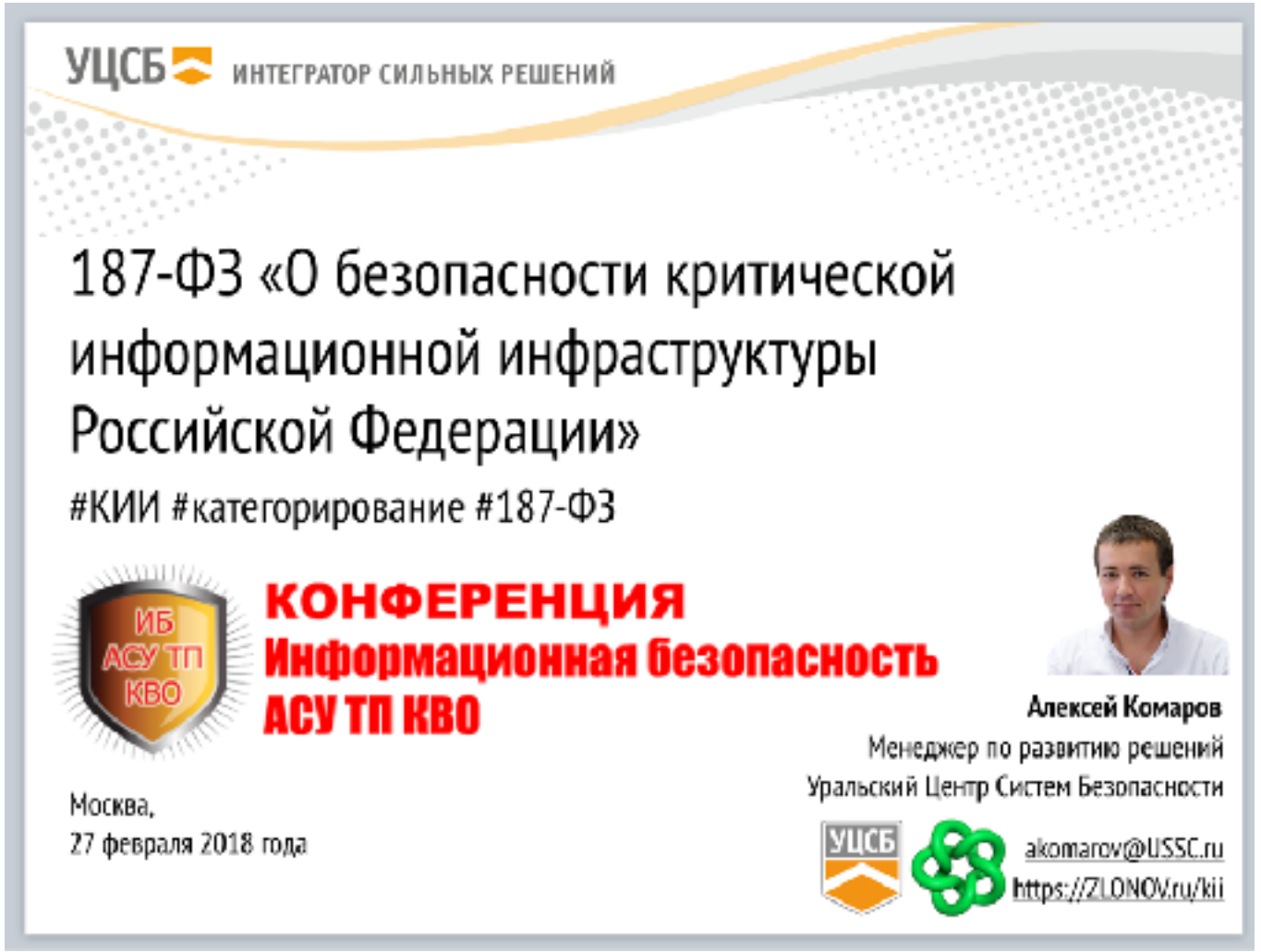
Алексей Комаров

Содержание

- 187-ФЗ год спустя
- Категорирование - автоматизируй это!
- Процессы, в соответствии с ОРД - мы все в Матрице…
- 239 дней до Приказа (…ФСТЭК России)



187-ФЗ вступил в силу больше года назад



Вопросов меньше не стало

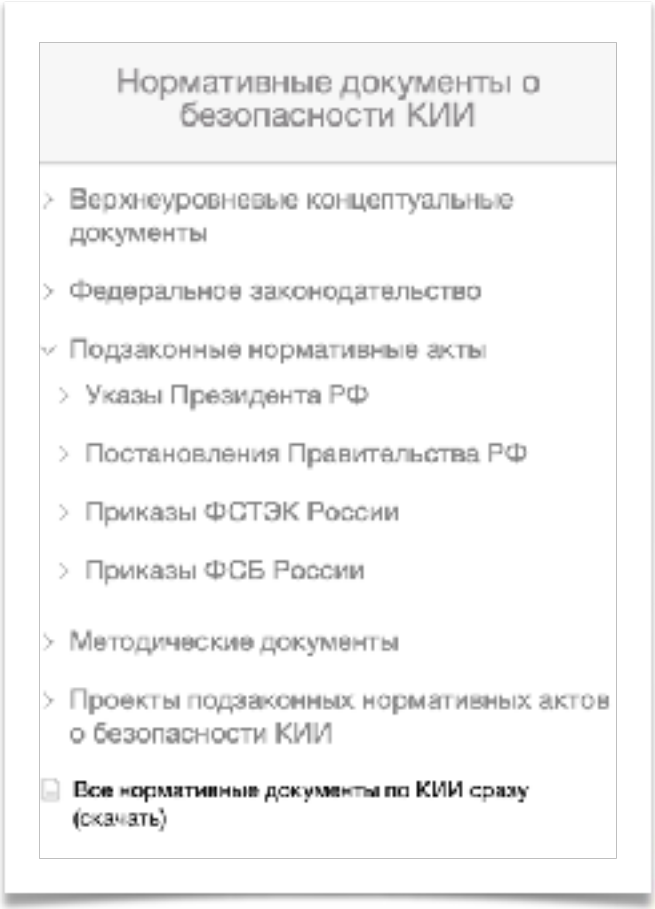
- Безопасность КИИ 187-ФЗ
  - Telegram-чат КИИ 187-ФЗ https://t.me/kii187fz
  - группа Facebook https://facebook.com/groups/kii187fz
  - группа ВКонтакте https://vk.com/kii187fz
  - Twitter https://twitter.com/kii187fz
- Серия вебинаров УЦСБ
  - Безопасность КИИ и требования 187-ФЗ

Вопросов меньше не стало

- Безопасность КИИ 187-ФЗ — 2 078 участников
  - Telegram-чат КИИ 187-ФЗ https://t.me/kii187fz
  - группа Facebook https://facebook.com/groups/kii187fz
  - группа ВКонтакте https://vk.com/kii187fz
  - Twitter https://twitter.com/kii187fz
- Серия вебинаров УЦСБ — 4 482 просмотра
  - Безопасность КИИ и требования 187-ФЗ

Нормативные документы о безопасности КИИ

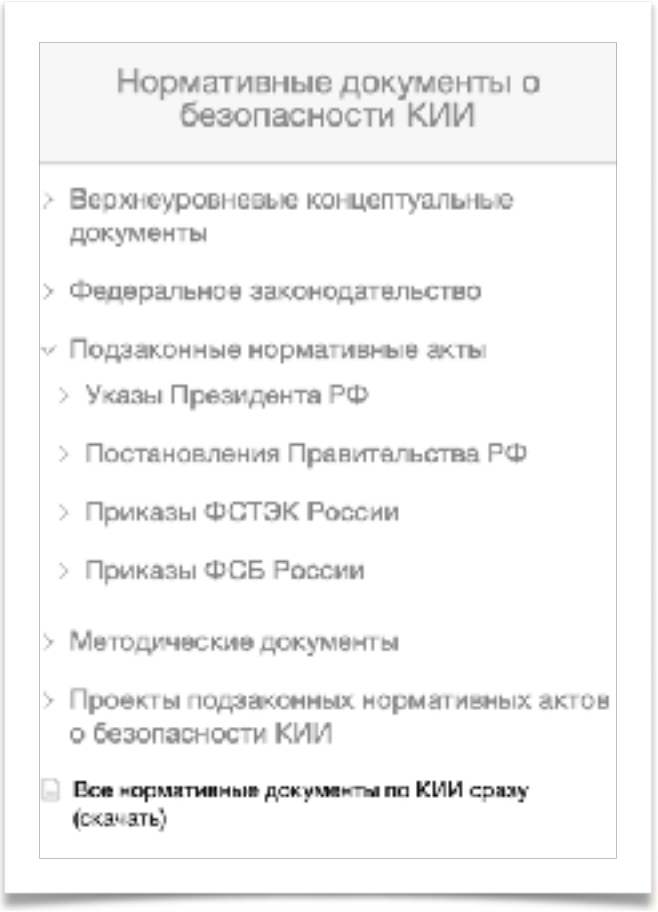
- **3** - Федеральные законы
- **5+3** - Указы Президента РФ
- **3** - Постановления Правительства РФ
- **7** - Приказы ФСТЭК России
- **3** - Приказы ФСБ России
- **?** - Методические документы



http://zlonov.ru/kii/

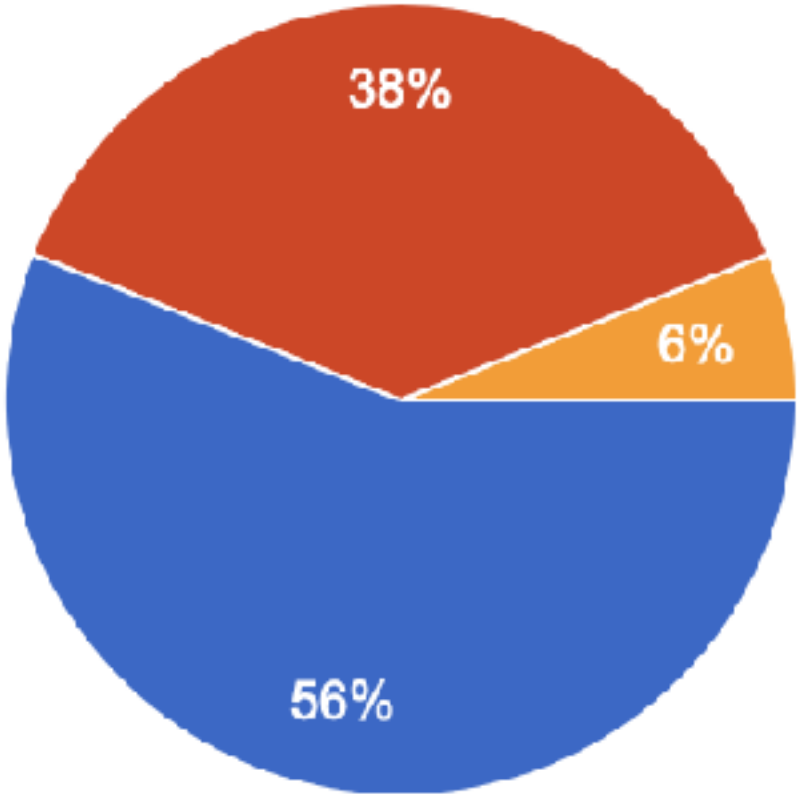
Нормативные документы о безопасности КИИ

- **3** - Федеральные законы
- **5+3** - Указы Президента РФ
- **3** - Постановления Правительства РФ
- **7** - Приказы ФСТЭК России
- **3** - Приказы ФСБ России
- **?** - Методические документы
  - **2+6** - Документы по ГосСОПКА
  - **2** - Информационные сообщения ФСТЭК России



http://zlonov.ru/kii/

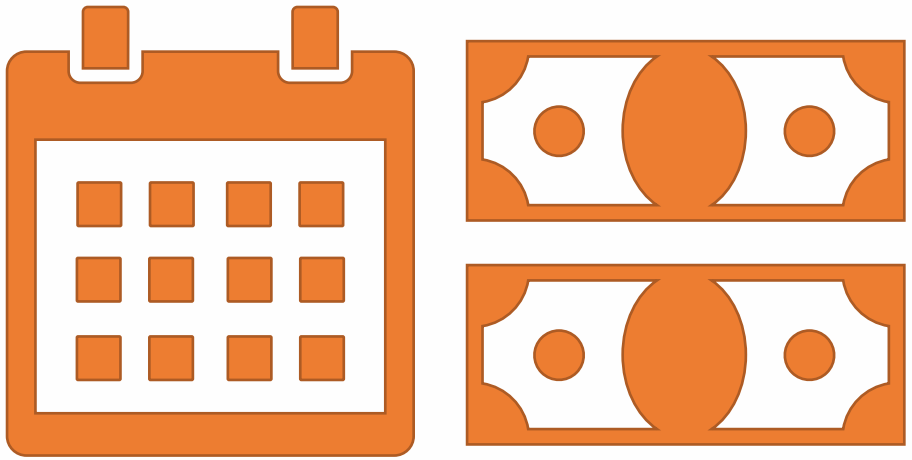
На ваш взгляд - выполнение категорирования организация может:



- Реализовать самостоятельно
- Реализовать в смешанном формате с частичным привлечением интегратора
- Реализовать только с привлечением интегратора в формате «под ключ»

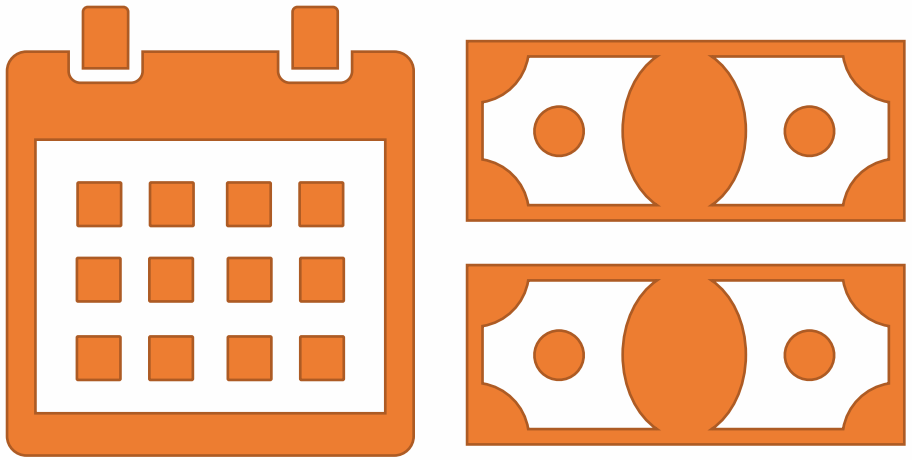
https://blog.zlonov.ru/187-fz-answers/

Сколько стоит категорирование?



- Проект 1.
  - 4 площадки + центральный офис
  - Этапы:
    - Обследование объектов
    - Выявление КП и формирование перечня объектов КИИ
    - Формирование моделей угроз и модели нарушителя для объектов КИИ
    - Категорирование объектов КИИ
    - Подготовка Плана-графика мероприятий по выполнению требований 187-ФЗ
  - Плановые затраты: **345 человеко-дней** + командировочные расходы

Сколько стоит категорирование?



- Проект 2.
  - 5 площадок + центральный офис
  - Этапы:
    - Обследование объектов КИИ
    - Актуализация Перечней объектов КИИ
    - Категорирование объектов КИИ
    - Оформление сведений о результатах категорирования объектов КИИ
  - Плановые затраты: **376 человеко-дней** + командировочные расходы

Автоматизация этапов процесса категорирования

Высокий потенциал

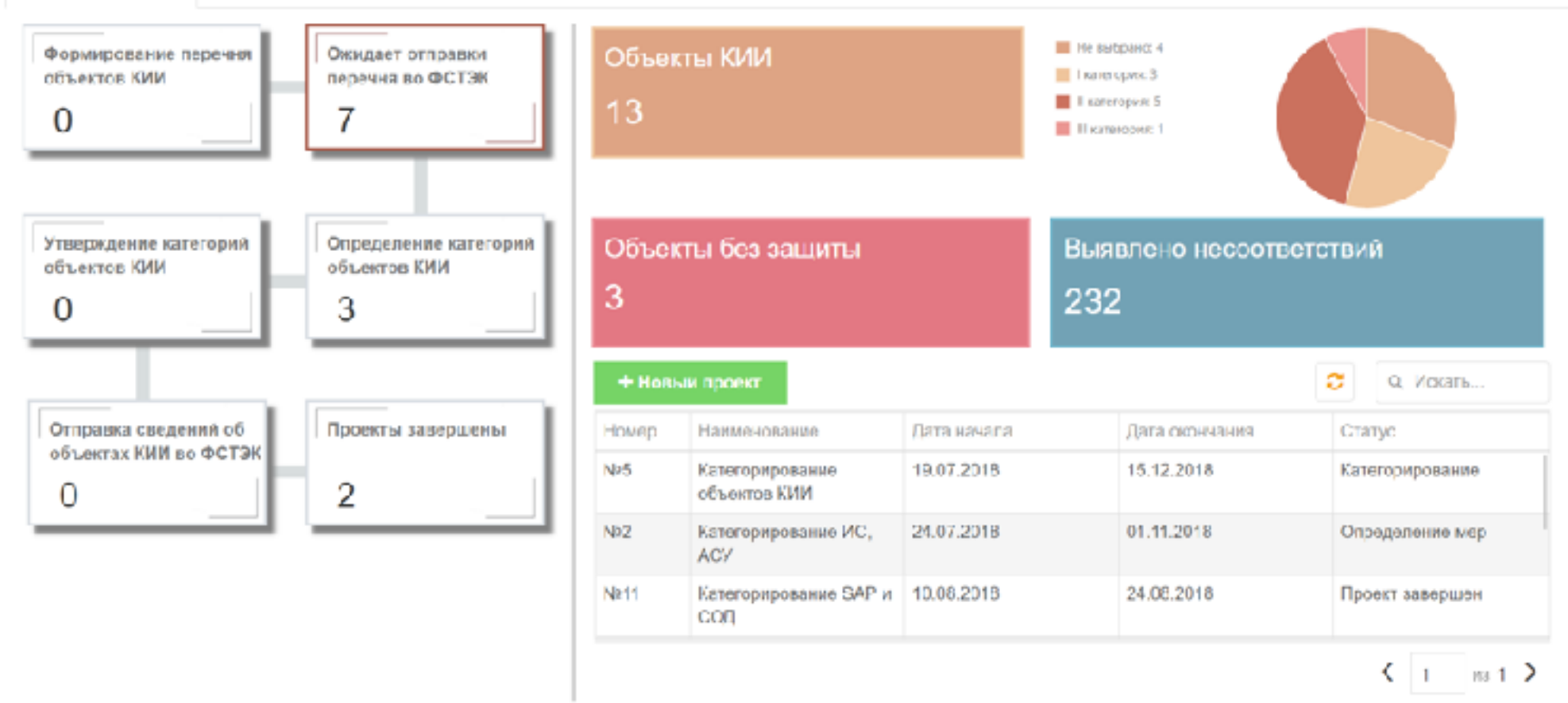
Средний потенциал

Низкий потенциал

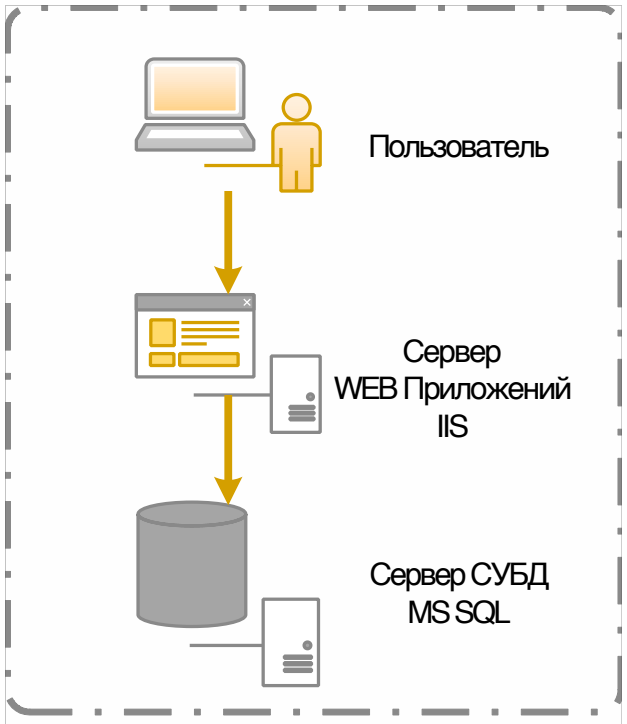
Модуль категорирования КИИ на базе eplat4m

- Программный комплекс, обеспечивающий автоматизацию процессов, предусмотренных 187-ФЗ «О безопасности КИИ РФ» реализует рабочие процессы:
- «Жизненный цикл объекта КИИ» - выявление, категорирование, присвоение категории, пересмотр категории
- «Процесс категорирования» - содержит стадии категорирования объектов КИИ
- Осуществляется выполнение следующих функций:
    - Ведение реестра субъектов и объектов КИИ
    - Ведение справочников
    - Проведение оценки соответствия выявленных объектов требованиям 187-ФЗ

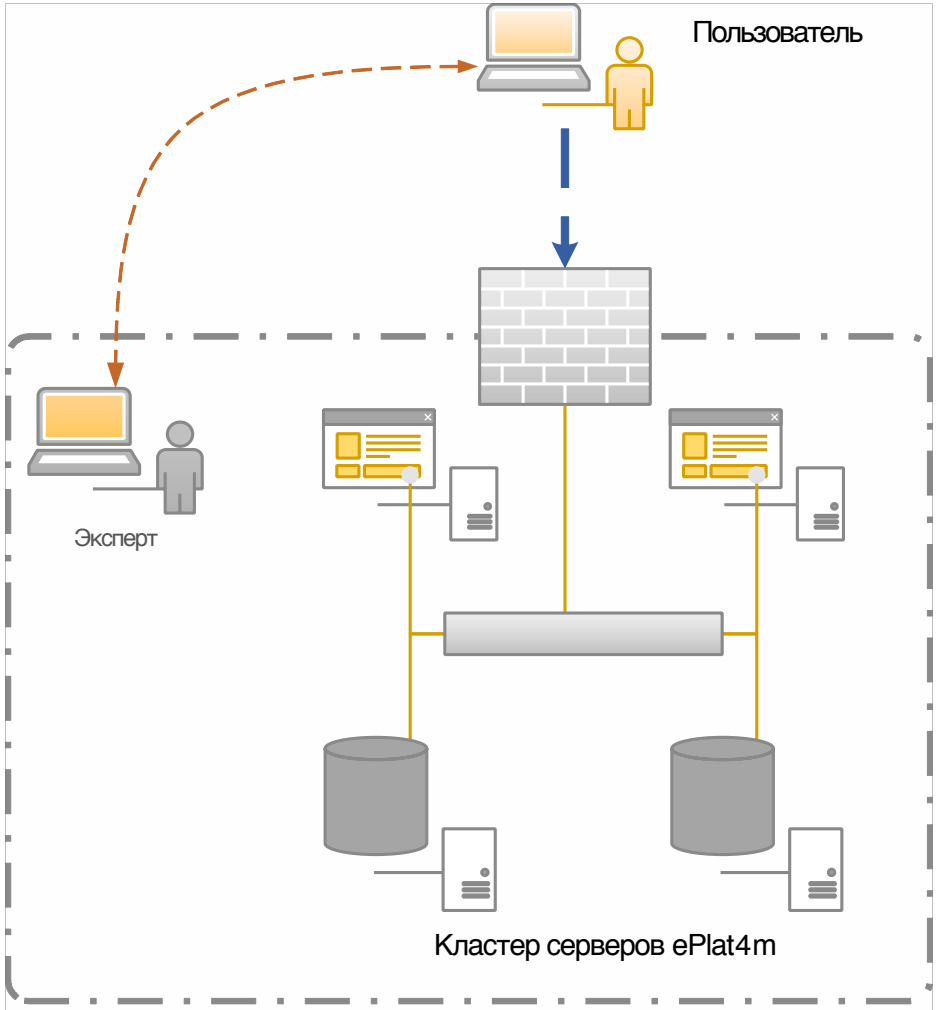
Интерфейс пользователя



Архитектура



Размещение в сети заказчика



Размещение в ЦОД УЦСБ

ОРД по безопасности ЗО КИИ 1/3

- Организационно-распорядительные документы по безопасности значимых объектов должны определять:
  - цели и задачи обеспечения безопасности,
  - основные угрозы безопасности информации и категории нарушителей,
  - основные организационные и технические мероприятия по обеспечению безопасности ЗО КИИ,
  - состав и структуру системы безопасности и функции ее участников, порядок применения, формы оценки соответствия ЗО КИИ и средств защиты информации требованиям по безопасности;

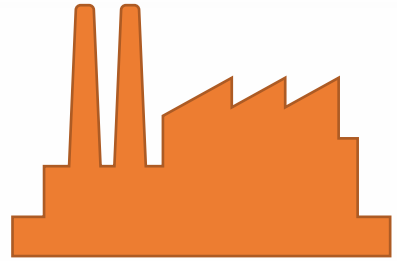
ОРД по безопасности ЗО КИИ 2/3

- Организационно-распорядительные документы по безопасности значимых объектов должны определять:
  - планы мероприятий по обеспечению безопасности ЗО КИИ,
  - модели угроз безопасности информации в отношении ЗО КИИ,
  - порядок реализации отдельных мер по обеспечению безопасности ЗО КИИ,
  - порядок проведения испытаний или приемки средств защиты информации,
  - порядок реагирования на компьютерные инциденты,
  - порядок информирования и обучения работников,

ОРД по безопасности ЗО КИИ 3/3

- Организационно-распорядительные документы по безопасности значимых объектов должны определять:
  - порядок взаимодействия подразделений/работников субъекта КИИ при решении задач обеспечения безопасности ЗО КИИ,
  - порядок взаимодействия субъекта КИИ с ГосСОПКА;
  - правила безопасной работы работников субъекта КИИ на ЗО КИИ,
  - действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.

Управление доступом: Матрица доступа



- Предоставленные субъектам доступа права доступа к компонентам АСУ ТП должны быть **зафиксированы в матрице доступа**
- Работники подразделения ИБ АСУ ТП должны проводить периодический **контроль не реже 1 раза в месяц** прав доступа субъектов согласно матрице доступа
- Матрица доступа должна содержать сведения о **составе субъектов** и **объектов** доступа, а также разрешенных (запрещенных) **действиях** (операциях) с ними
- **Изменения** должны вноситься **на основе заявок** на предоставление (изменение) доступа в АСУ ТП, а также при прекращении (аннулировании) прав доступа

Функции DATAPK®

- Инвентаризация компонентов АСУ ТП
- Контроль конфигураций компонентов АСУ ТП
- Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
- Контроль защищённости компонентов АСУ ТП
- Обнаружение компьютерных атак
- Контроль соответствия требованиям по обеспечению ИБ (включая 187-ФЗ)
- **NEW!** Автоматизация процессов по обеспечению безопасности ЗО КИИ (АСУ)

DATAPK® - российская разработка

- Сертификат ФСТЭК России №3731
- Включен в Единый реестр российских программ для электронных вычислительных машин и баз данных
- Использует уникальные модули платформы CyberLympha (резидент Сколково)

Участник

CyberLympha®

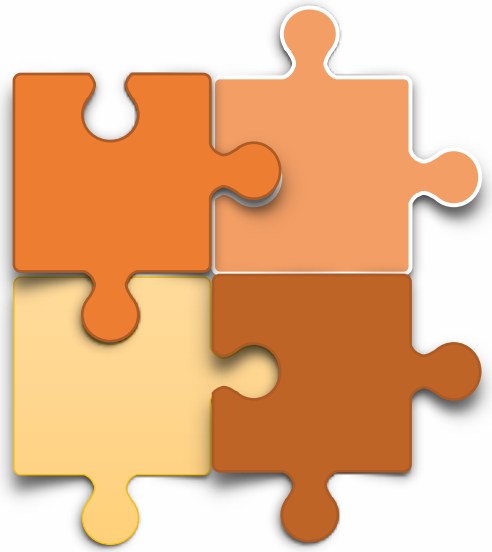
DATAPK® - Реализация мер Приказа ФСТЭК России №239

- В том или ином виде реализуется более 40 различных мер:

Обозн. и № меры	Мера обеспечения безопасности значимого объекта	К3	К2	К1	DATAPK
XIII. Управление конфигурацией (УКФ)					
УКФ.1	Идентификация объектов управления конфигурацией				+, в соответствии с объектом защиты
УКФ.2	Управление изменениями	+	+	+	+, контроль изменения конфигурации
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+	+, в части контроля списка установленного ПО

Полная версия таблицы - по запросу в УЦСБ

Вместо заключения - предложения УЦСБ



- Комплексная услуга по **категорированию** объектов КИИ
- **Платформа** для **управления** жизненным циклом объектов КИИ
- Разработка **комплекта ОРД** документов по безопасности ЗО КИИ
- **Создание систем безопасности** ЗО КИИ и обеспечение их функционирования (**сервисная поддержка**)
- **Реализация требований** по обеспечению безопасности ЗО КИИ
- **DATAPK® - специализированное** решение для обеспечения безопасности ЗО КИИ, являющихся **АСУ (ТП)**

info@ussc.ru
https://USSC.ru

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Алексей Комаров

akomarov@USSC.ru

https://ZLONOV.ru

USSC.RU

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ