

Kaspersky Security CAD



Цифровое моделирование
информационной безопасности
промышленных систем

kaspersky

Ключевая проблема

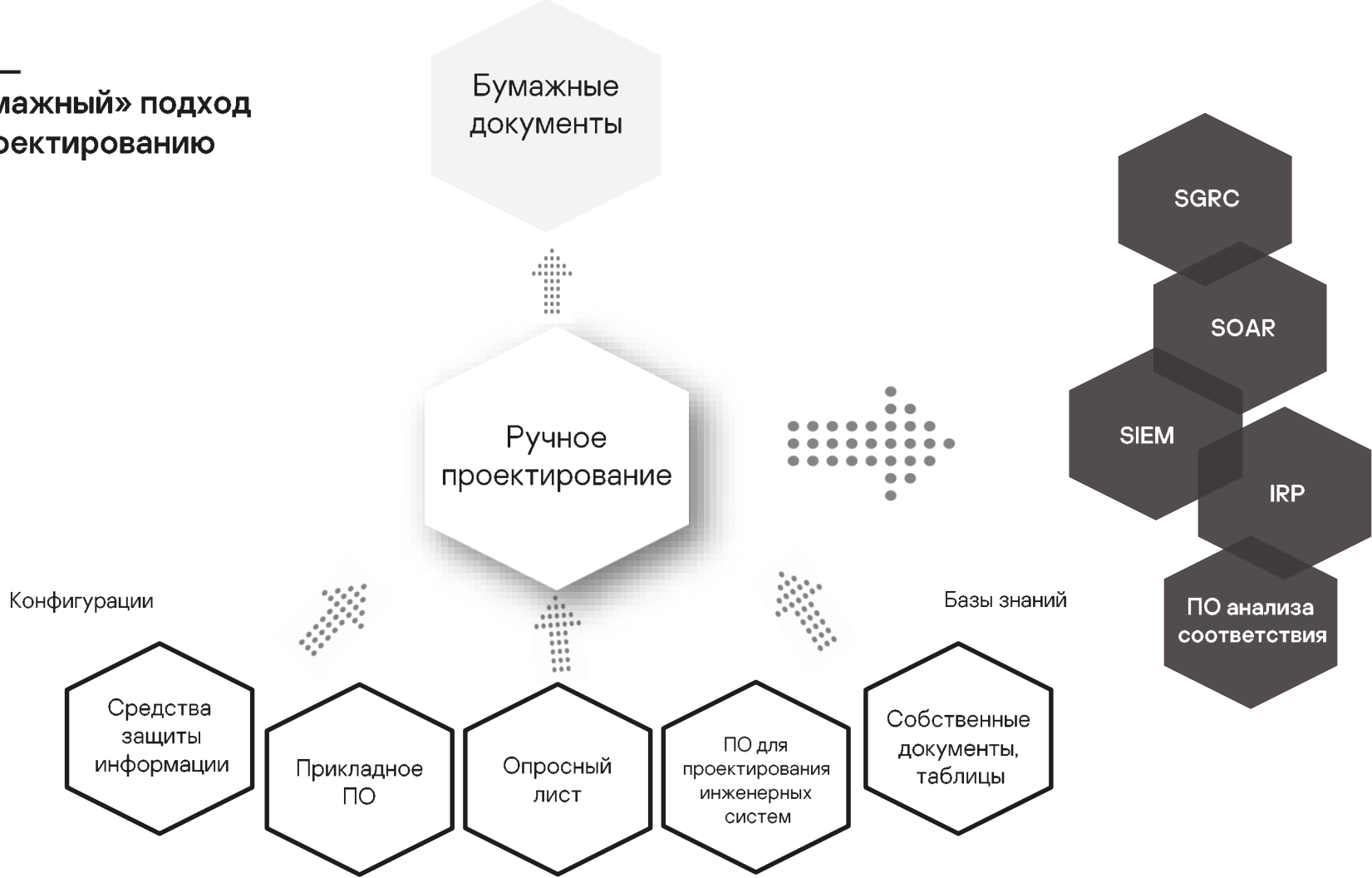
Нет актуальной и консолидированной информации по объектам и системе защиты

Актуальная информация по
СрЗИ и объекту защиты
хранится в разных источниках
и у разных специалистов

Документы по защищаемым
объектам и средствам защиты
(СрЗИ) отличаются от
реального состояния

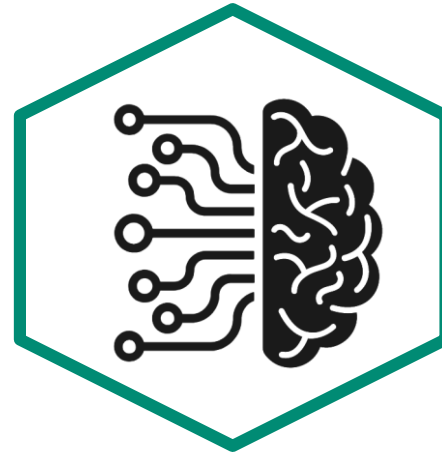
Проектирование/актуализация
проекта требует много
ресурсов и быстро устаревает

«Бумажный» подход к проектированию



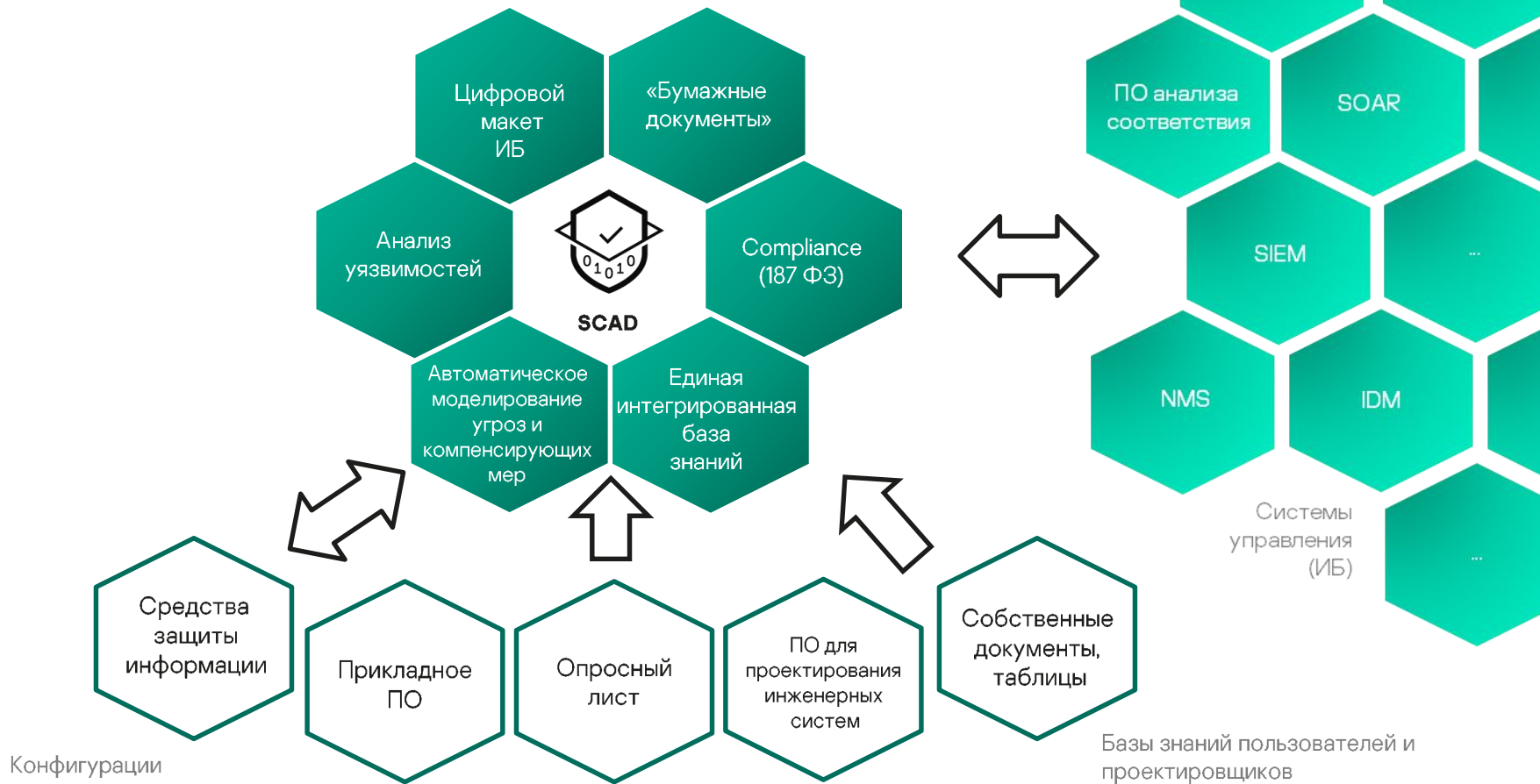


**Создание цифрового макета ИБ,
вместе с классическим
проектированием**



**Автоматическое формирование
угроз, мер защиты и документов
при вводе и корректировке данных**

Цифровая модель

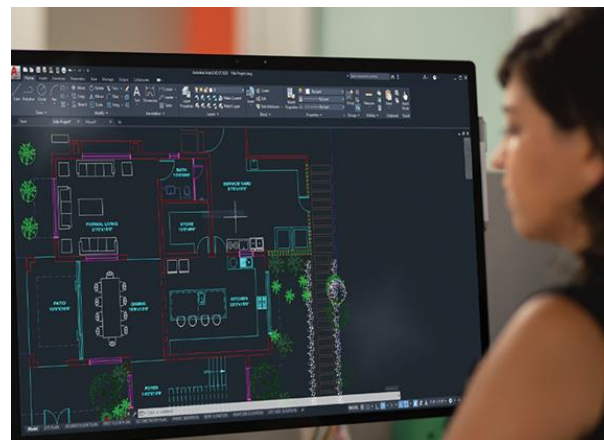


Проектирование

Ручной труд

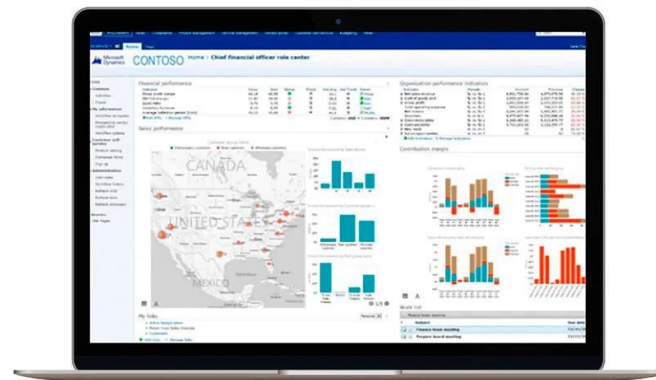


Автоматизированный



6

Бухгалтерия

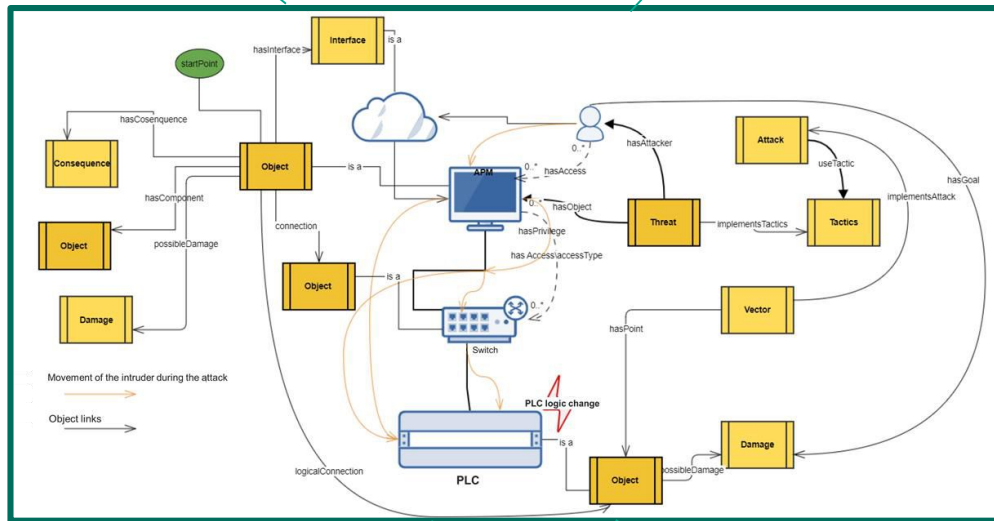




МУиН ФСТЭК
05.02.2021

Приказы ФСТЭК 235, 239
МЭК 62443, NIST SP 800-XX

Входные
данные



Модель угроз

Меры защиты

Проектные
документы

Модель АСУ ТП

Роли пользователей

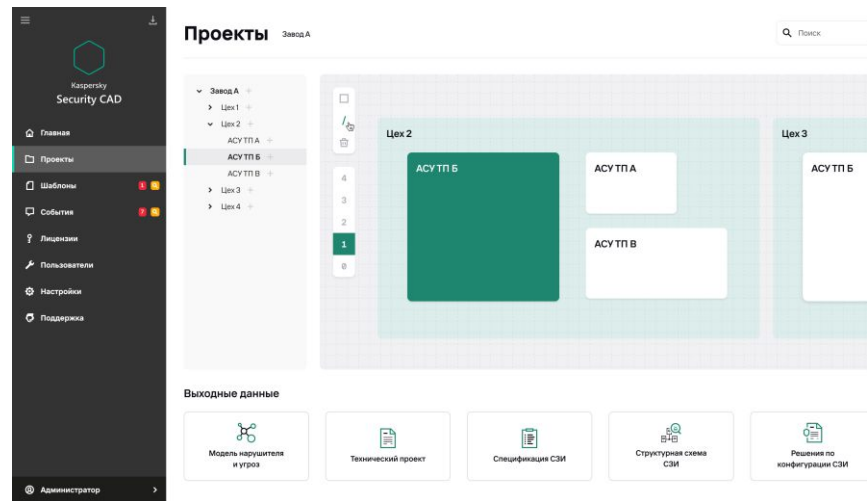
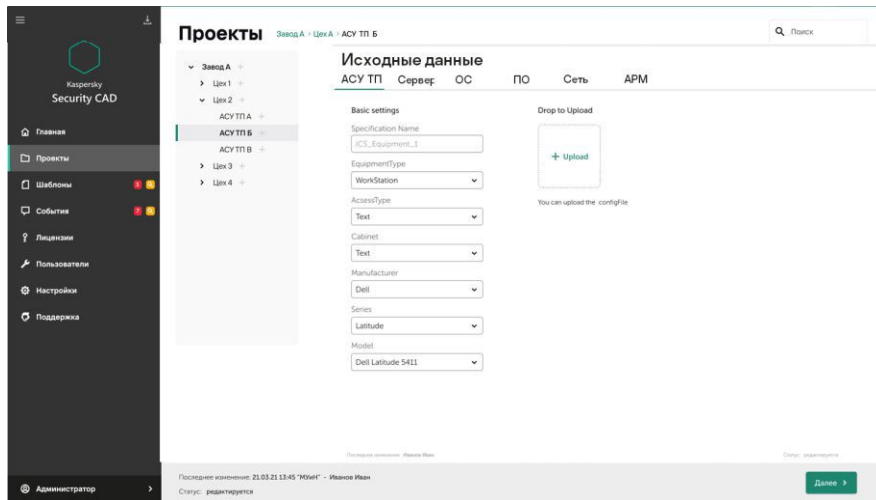
Входные данные

Сбор информации:

- Опросник + *Очное обследование представителем интегратора
- **Конфигурации СЗИ, результаты активного/пассивного сканирования

*При необходимости

**При возможности



Модель угроз

Используемые документы и БД:

- БДУ ФСТЭК
- МУиН (от 05.02.21)
- MITRE ATT & CK
- MITRE CVE
- Возможность подключения собственных источников

Таблица 18 – Возможные актуальные угрозы безопасности информации

№ п/п	Идентификатор угрозы	Наименование угрозы
1	УБИ012	Угроза деструкции окружения прог
2	УБИ013	Угроза декларированно
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

7.2. Описание возможных безопаснсти информации

Для каждой возможной угрозы без в таблице 18, приведены сценарии каждой

СОДЕРЖАНИЕ

- Общие положения 4
 - Назначение и область действия документа 4
 - Термины и сокращения 4
 - Нормативно-методическая база 6
 - Наименование обладателя информации / заказчика / оператора объекта защиты 6
 - Подразделения/должностные лица/ответственные за обеспечение защиты информации (безопасности) объекта защиты 7
 - Наименование организации - разработчика модели УБИ 7
- Описание объекта защиты 8
 - Наименование объекта защиты 8
 - Категория значимости объектов защиты 8
 - Основные процессы (бизнес-процессы) обладателя информации 8
 - Состав и архитектура объекта защиты 8
 - Описание групп внешних и внутренних пользователей объекта защиты 12
 - Описание интерфейсов 13
- Определение негативных последствия 16
- Возможные объекты воздействия угроз безопасности информации 17
- Источники угроз безопасности информации 19
 - Характеристика и категории актуальных нарушителей 19
 - Описание возможностей нарушителей 25
- Способы реализации (возникновения) угроз безопасности информации 31

Технический проект

1. Ведомость технического проекта
2. Пояснительная записка
3. Структурная схема ИБ
4. Схема функциональной структуры ИБ
5. Ведомость покупных изделий

Используемые документы:

- 239 приказ ФСТЭК
- 235 приказ ФСТЭК
- 187 ФЗ
- МЭК 62443
- NIST SP 800
- ГОСТ 34.201-89
- ГОСТ 34.601-90
- ГОСТ 34.003-90
- ГОСТ Р 51583-2014
- ГОСТ Р 51624-2000
- ГОСТ Р ИСО/МЭК 27001-2006 ГОСТ Р 50739-95
- ГОСТ Р 52447-2005
- СП 77.13330.2016

Рабочая документация

1. Пояснительная записка к рабочей документации
2. Ведомость рабочей документации
3. Таблица IP адресации
4. Ведомость объёмов работ
5. Таблица соединений
6. Спецификация
7. Используемые документы НТД и БД

Используемые документы:

- ГОСТ 34.201-89
- ГОСТ 34.601-90
- ГОСТ 34.003-90
- ГОСТ Р 51583-2014
- ГОСТ Р 51624-2000
- ГОСТ Р ИСО/МЭК 27001-2006 ГОСТ Р 50739-95
- ГОСТ Р 52447-2005
- СП 77.13330.2016

Цифровая модель

Визуальный интерфейс:

- Интерактивная работа с информацией:
- Возможность автоматической корректировки всех документов
- Ведение реестра изменений проекта и возможность возврата к предыдущей версии
- Обобщённая информация по запроектированным системам

Интеграция с другими системами

Возможность выгружать документы:

- DOCX для документов
- SVG для схем
- PDF для всех файлов
- XLSX для вывода данных
- Передача во внешние через JSON/XML

Возможность загружать документы:

- Ввод описательной части
- Схемы
- Конфигурации СЗИ, сетевого оборудования и ПО
- Фотографии

Моделирование и оценка необходимых мер при планируемых или фактических изменениях.

Помощь в расследование инцидентов

Консолидированная и визуально понятная информация об объекте защиты, его характеристиках, настройках основных компонентов и СрЗИ

Периодический анализ актуальности системы защиты на появление новых уязвимостей и соответствию требований регулятора

Консолидированные данные по имеющимся объектам защиты, используемым СрЗИ, орг. мерам и документам, а также требуемым мерам и СрЗИ для отчётности, обоснования и планирования развития.

Принцип работы

Сбор данных

Формирование документов

Создание цифрового макета

Сдача проекта

Эксплуатация

Специалист интегратора заполняет данные в SCAD

SCAD формирует, а специалист интегратора проверяет и утверждает:

Цифровую модель
Модель угроз
Соответствие требованиям 187 ФЗ
Технический проект
Рабочую документацию

Заказчик получает цифровую модель объекта защиты с комплектом проектной документации

Документы актуальны
Цифровая модель
Compliance (187 ФЗ)
Анализ уязвимостей

2 дня

2 дня

1 день

1 день

* Указаны оценочные затраты времени на выполнение работ по каждому этапу без учёта времени на командировки, согласование встреч и т. д. В зависимости от размеров объекта и процедур предприятия сроки могут корректироваться.

Сравнение для 10 АСУ ТП

		Проектирование	Актуализация / модернизация	Эксплуатация
Проектирование				
	Продолжительность	6 месяцев + конкурсные процедуры	3 месяца + конкурсные процедуры	1 месяц + конкурсные процедуры
	Стоимость	8 000 000	8 000 000	3 000 000 Compliance (187 ФЗ и пр.), 1 000 000 анализ уязвимостей
	Результат	Документы (с состоянием АСУ ТП 1-2 месячной давности) Compliance (187 ФЗ и пр.)	Актуальные документы Compliance (187 ФЗ и пр.)	СЗИ и документы не коррелируют Анализ уязвимостей Compliance (187 ФЗ и пр.)
Цифровая модель				
	Продолжительность	3 недели + конкурсные процедуры	1 день	1 день
	Стоимость	12 000 000	(8 000 000, если прошло более года)	-
	Результат	Актуальные документы Цифровой макет Compliance (187 ФЗ и пр.) + Анализ уязвимостей	Актуальные документы Цифровой макет Compliance (187 ФЗ и пр.) Анализ уязвимостей	Настроенные СЗИ и Актуальные документы Цифровой макет Compliance (187 ФЗ и пр.) Анализ уязвимостей



Kaspersky
Security CAD

Главная

Проекты

Шаблоны



События



Лицензии

Пользователи

Настройки

Поддержка

Администратор



Проекты

Завод А > Цех А > АСУ ТП Б

Поиск

Входные данные



Схема АСУ ТП



Сведения
о нарушителе



Опросный лист



Акт категорирования

Выходные данные



Модель нарушителя
и угроз



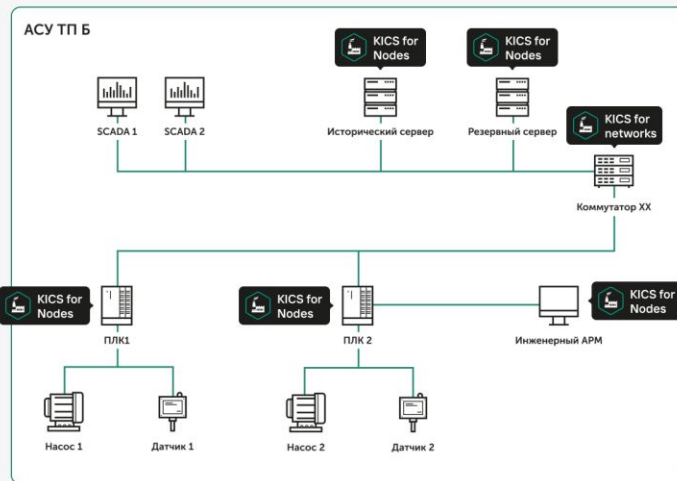
Технический проект



Спецификация СЗИ



Рабочая
документация



Информация об объекте



Адрес:
Россия, Область, город,
улица, доп. данные

Ответственный за ИБ:
Фамилия И. О.

Телефон:
+7 123 456 789

E-mail:
FIO@domen.ru

Объект:
КИИ 3 категории

Дата проекта:
21.03.2021

Предыдущая версия проекта:
Отсутствует

Исполнитель проекта:
Интегратор X



Kaspersky

Security CAD

Главная

Проекты

Шаблоны



События



Лицензии

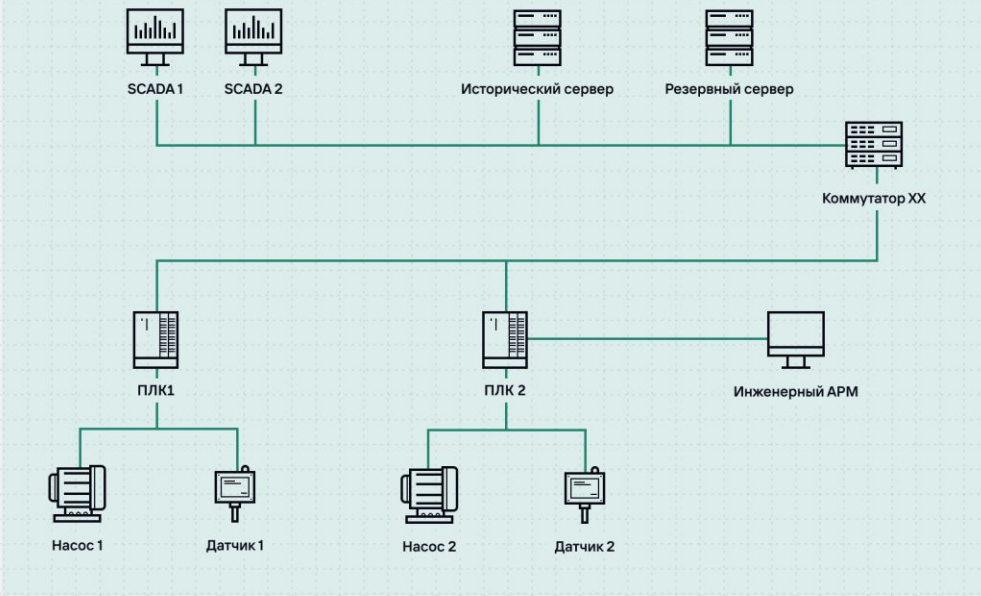
Пользователи

Настройки

Поддержка

Администратор

АСУ ТП Б



Библиотека ^

Устройства

АРМ

Сервер

Контроллер

Коммутатор

Маршрутизатор

Насос

Задвижка

Датчик

ПЛК



Насос 1



Датчик 1





Kaspersky
Security CAD

- Главная
- Проекты
- Шаблоны 1 Q
- События 7 Q
- Лицензии
- Пользователи
- Настройки
- Поддержка

Администратор >

Главная

Смотреть отчеты

Поиск

Общая статистика



21

Запроектировано



3

Внедряется



1

Проектируется



9

Объектов КИИ



3

Ответственных



32

АСУ ТП



180

Дней до проверки



50

Орг. документов



122

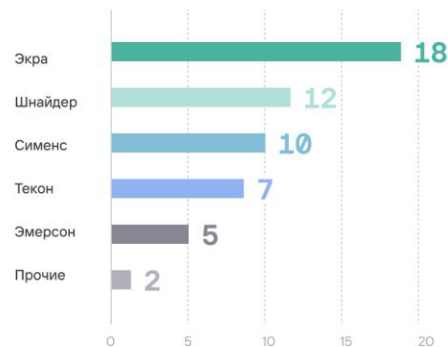
СрЗИ



300

Угроз
нейтрализовано

Устройства



Объекты



- 1 Объект первой категории
- 2 Объекта второй категории
- 5 Объектов третьей категории

Соответствие требованиям 187 ФЗ



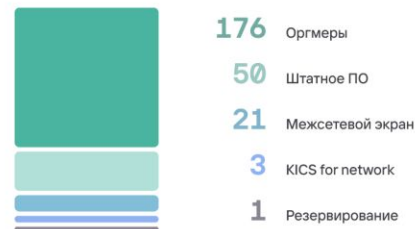
80%

Соответствует требованиям

20%

Не соответствует требованиям

Системы



21.12.2021

Первая версия SCAD
Только АСУ ТП

Анализ уязвимостей (БДУ ФСТЭК)
Compliance (187 ФЗ)
Моделирование угроз (МуИИ ФСТЭК, частично MITRE (ICS, CVE))
Автоматический подбор СрЗИ и орг. мер.
Автоматическая генерация эскизов документов

22.04.2022

Полнофункциональная MITRE ATT&CK for ICS

30.10.2022

Вторая версия SCAD
Полное предприятие

Генерация конфигов СрЗИ
Контроль актуальности данных
Интеграция с СрЗИ (типа SIEM, МЭ, SGRC и т.п.)

21.04.2023

Автоматизированный Compliance

30.10.2023

Третья версия SCAD
Любая компания

Подгрузка любых БДУ и Фидов 3D цифровой макет
Двусторонняя интеграция с внешними системами (CAD, SIEM, SRGC, BIM и т.п.)

Лицензия требуется для работы аналитических модулей и интерактивной работы цифрового макета

Стоимость лицензий определяется исходя из:

- количества объектов
- продолжительности действия лицензий (1-3 года)
- формы работы с ними (покупка или обновление)

Лицензия не требуется для того что бы:

- Внести данные по объекту
- Загрузить внутренние документы
- Настроить шаблоны
- Сформировать группы пользователей и их права
- Загрузить и посмотреть проекты

Сокращение времени на проектирование в разы

Актуальность данных

Актуализация данных требует минимум времени и сил.

Оптимизация затрат

Созданный цифровой макет можно потом использовать для актуализации данных, анализа уязвимостей, соответствия 187 ФЗ и разбора инцидентов.

Преимственность знаний

Данные в цифровом макете содержат все данные по объекту, визуализированы и понятны новому пользователю

Помощь в разборе инцидентов

Сформированный цифровой макет полезен для анализа и реагирования на инциденты, а также планирования мер информационной безопасности

Спасибо!



Петухов Алексей

Руководитель проекта

SCAD@kaspersky.com

kaspersky