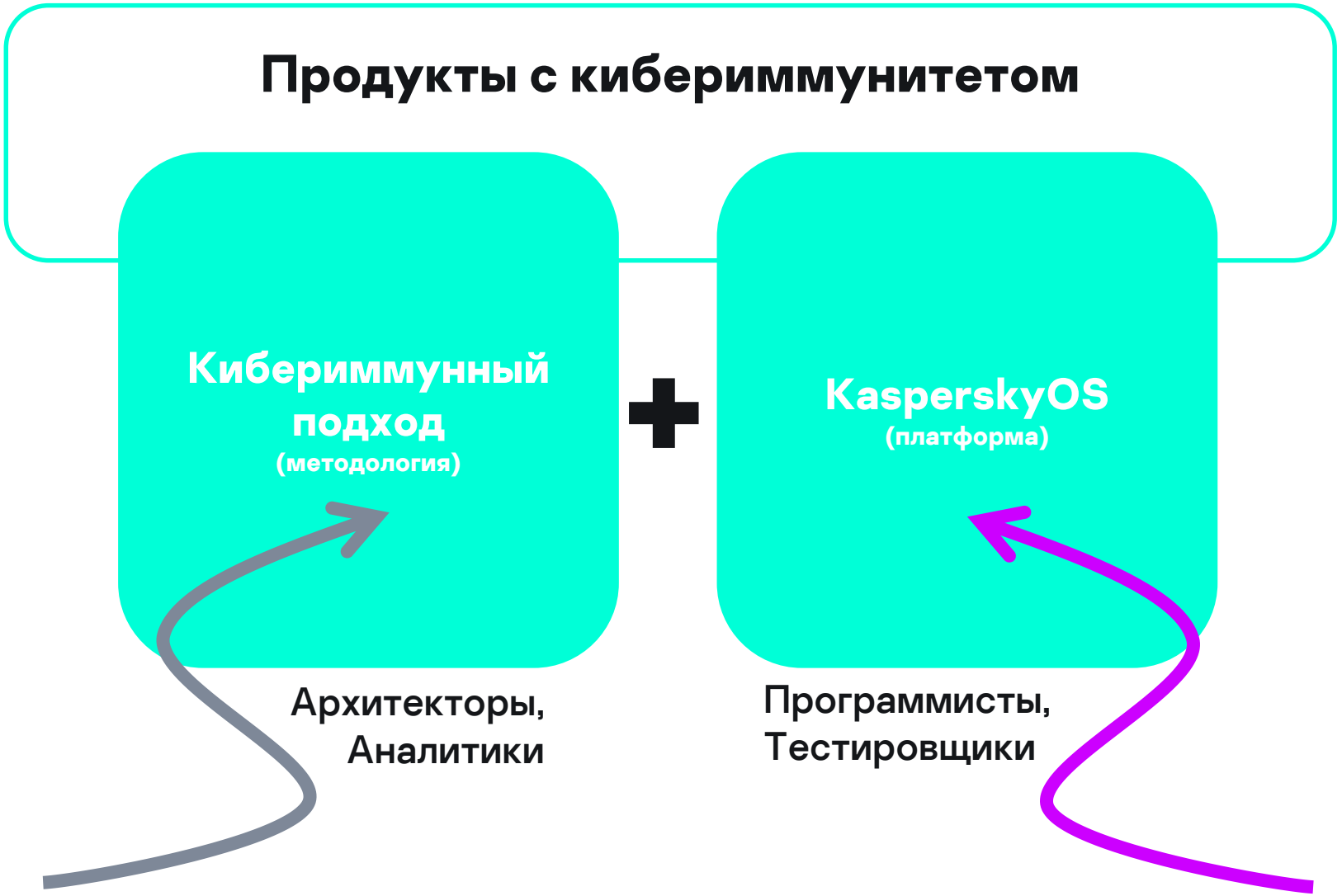
Встреча Ассоциации «Цифровая Энергетика»

Кибериммунный подход к обеспечению безопасности в инфраструктуре для энергетической отрасли

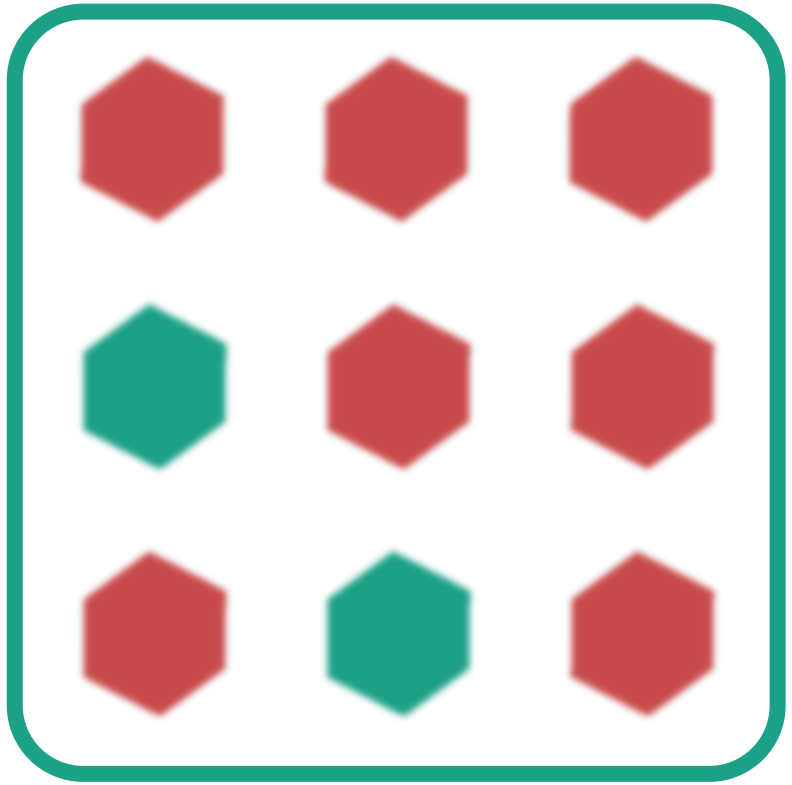
KasperskyOS

Продукты с кибериммунитетом



Кибериммунность

- это методология



Как построить решение,
которому можно доверять,
из компонентов, большинству
из которых доверять нельзя?

kaspersky

Кибериммунность

- Как?

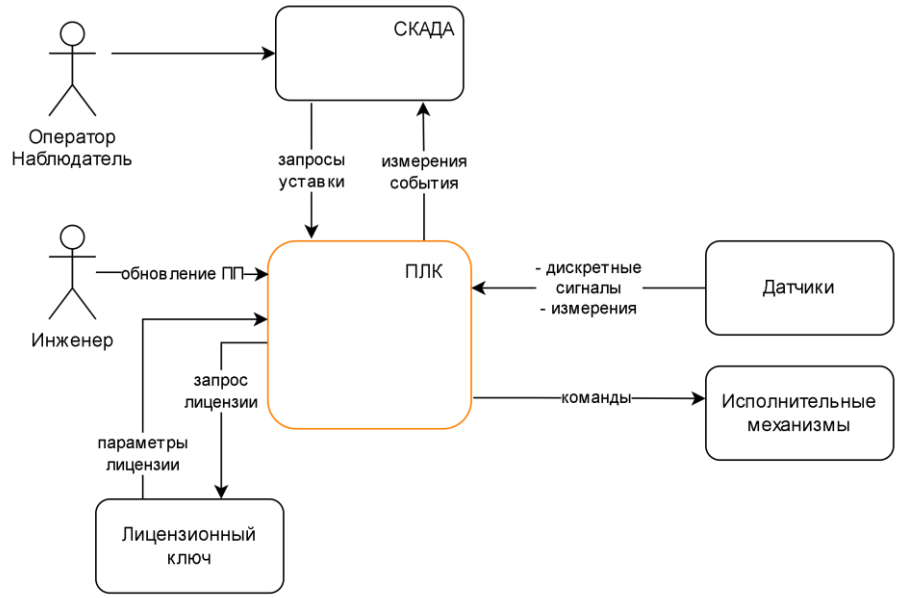
1. Требования к **процессу**
2. Требования к **архитектуре**

kaspersky

Пример реализации ПЛК для АСУ ТП ТЭЦ

Продукт – программируемый логический контроллер, обеспечивающий взаимодействие автоматизированной системы управления технологическим процессом (АСУ ТП) с конечным оборудованием.

	Ценность	Нежелательные события	Комментарий
1	данные, которые получает и передаёт ПЛК	- нарушение целостности (сигнал изменен), - нарушение достоверности сигнала (потерян или искажен источник) - сигнал не обработан (пришел и пропал) - (порча, подделка данных), нарушение доступности данных (потеря)	включает - сырые данные - результат обработки данных на стороне ПЛК
2	команды для оборудования	- команды нет, когда нужно - команда есть, когда не нужно	первое - это доступность
3	прикладная программа (ПП) инженера-разработчика	- использована неаутентичная ПП - неавторизованный доступ к коду ПП	утечка кода ПП в сеть (ущерб интеллектуальной собственности)
4	лицензия на режимы работы ПП	- использование неаутентичной лицензии - неавторизованный доступ к данным лицензии	формат и способ генерации лицензии на выбор команд



Пример реализации ПЛК для АСУ ТП ТЭЦ

Цели безопасности

1. АСУ ТП всегда получает целостные критичные данные от ПЛК
2. ПЛК выполняет только аутентичное ПП
3. Конечное оборудование всегда получает аутентичные команды
4. Только авторизованные пользователи имеют доступ к лицензии ПЛК
5. ПЛК всегда обрабатывает и доставляет сигналы в реальном времени

Предположения безопасности

1. Физическая защита периметра обеспечена
2. Персонал ТЭЦ благонадёжен
3. Аутентичное технологическое оборудование благонадёжно
4. На ТЭЦ установлено только аутентичное технологическое оборудование

Примечание

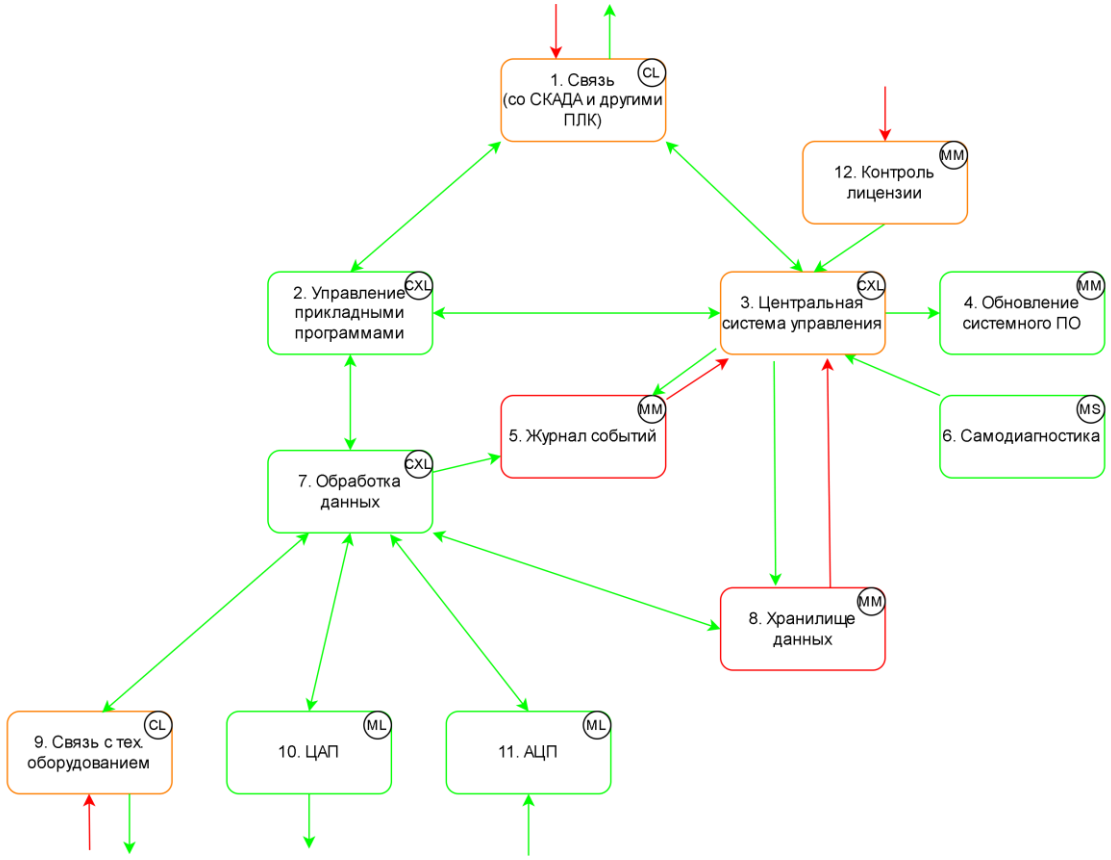
Рассматривается экспериментальная ТЭЦ, где оператор имеет только удалённый доступ к системе управления

Пример реализации ПЛК для АСУ ТП ТЭЦ

Уровни доверия для имеющихся целей безопасности

Цели безопасности

1. АСУ ТП всегда получает целостные критичные данные от ПЛК
2. ПЛК выполняет только аутентичное ПП
3. Конечное оборудование всегда получает аутентичные команды
4. Только авторизованные пользователи имеют доступ к лицензии ПЛК
5. ПЛК всегда обрабатывает и доставляет сигналы в реальном времени



Легенда

- недоверенная сущность
- доверенная сущность
- доверенная сущность, повышающая целостность данных
- высокоцелостные данные
- низкоцелостные данные

Качественные оценки доменов

Сложность - S (simple), M(medium), C (complex) - простой, средней сложности, сложный

Размер (объём) кода - S, M, L, XL - маленький, среднего размера, большой, очень большой

(SS) - простой и маленький

Доверенная кодовая база (не считая OS)

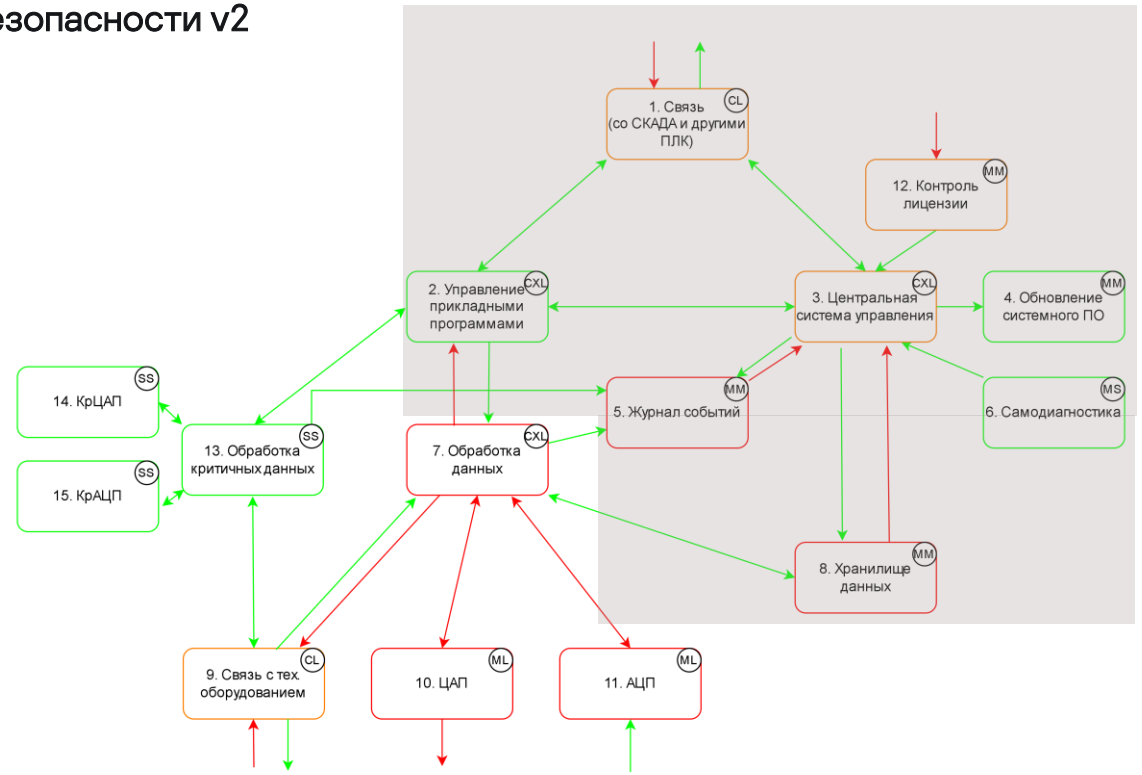
Компоненты. размер+сложность (количество входных интерфейсов):
1.CL(3), 12.MM(1), 2.CXL(3), 3.CXL(6), 4.MM(1), 6.MS(?), 7.CL(5), 9.CL(1), 10.ML(0), 11.ML(0)

Пример реализации ПЛК для АСУ ТП ТЭЦ

Уровни доверия для имеющихся целей безопасности v2

Цели безопасности

1. АСУ ТП всегда получает целостные **критичные** данные от ПЛК
2. ПЛК выполняет только аутентичное ПП
3. Конечное оборудование всегда получает аутентичные команды
4. Только авторизованные пользователи имеют доступ к лицензии ПЛК
5. ПЛК всегда обрабатывает и доставляет сигналы в реальном времени



Легенда

- недоверенная сущность
- доверенная сущность
- доверенная сущность, повышающая целостность данных
- высокоцелостные данные
- низкоцелостные данные

Качественные оценки доменов

Сложность - S (simple), M(medium), C (complex) - простой, средней сложности, сложный

Размер (объём) кода - S, M, L, XL - маленький, среднего размера, большой, очень большой

(SS) - простой и маленький

Доверенная кодовая база – дкб (не считая OS)

Компоненты. размер+сложность (количество входных интерфейсов):

1.CL(3), 12.MM(1), 2.CXL(3), 3.CXL(6), 4.MM(1), 6.MS(?), 9.CL(1), **13.SS(4), 14.SS(0), 15.SS(0)**

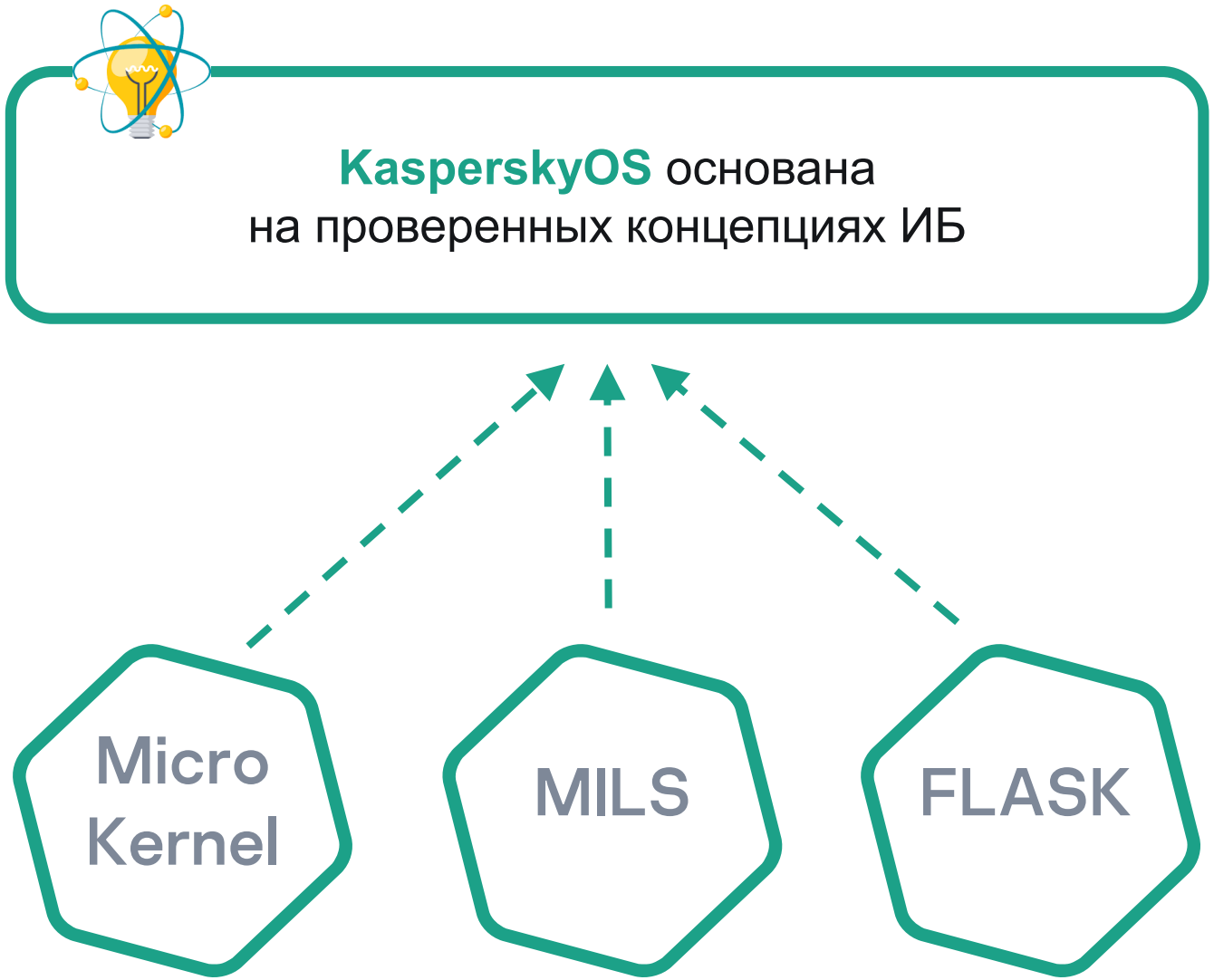
Вывели из дкб 7.CXL(5), 10.ML, 11.ML за счёт трёх простых и маленьких компонентов

KasperskyOS

Базирование на лучших проверенных концепциях

Изоляция и доверие

https://www.youtube.com/watch?v=77Eb88HB6hY



kaspersky

Выводы

- Конструктивная защита начинается с целей безопасности и проявляется в архитектуре
- Доверенный код – код, критичный для целей безопасности, включает в себя уровень системного ПО (операционку), его тоже необходимо минимизировать
- Меньше доверенного кода – дешевле разработка и сопровождение, успешнее продукт
- Для полноценной реализации устойчивого к атакам решения необходимо изолировать домены безопасности и контролировать их взаимодействие
- Изоляция и контроль должны быть частью ядра, чтобы это нельзя было обойти

Платформы на основе KasperskyOS и их возможности

Эволюция кибериммуных платформ

Этап I: Статические Кибериммунные системы

Этап II: Статические Кибериммунные системы с GUI

Этап III: Полу-динамические Кибериммунные системы с GUI

Этап IV: Открытые Динамические Кибериммунные системы с GUI

Продукт

IoT шлюз

PLC

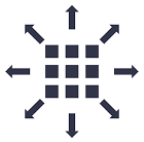
Продукт

Тонкий клиент

Прототип

IoT шлюз

Прототип



Каталог приложений

Прототип

KASG

Прототип

KPMP

IoT Шлюз

Подробности:

- Статическая система, которая не поддерживает сторонние приложения

Тонкий Клиент

Подробности:

- Статическая система с графическим интерфейсом, которая не поддерживает сторонние приложения;
- Централизованное управление

Шлюзы с Edge Computing

Подробности:

- Динамическая система с графическим интерфейсом, которая поддерживает сторонние приложения с ограниченным функционалом;

Мобильные устройства

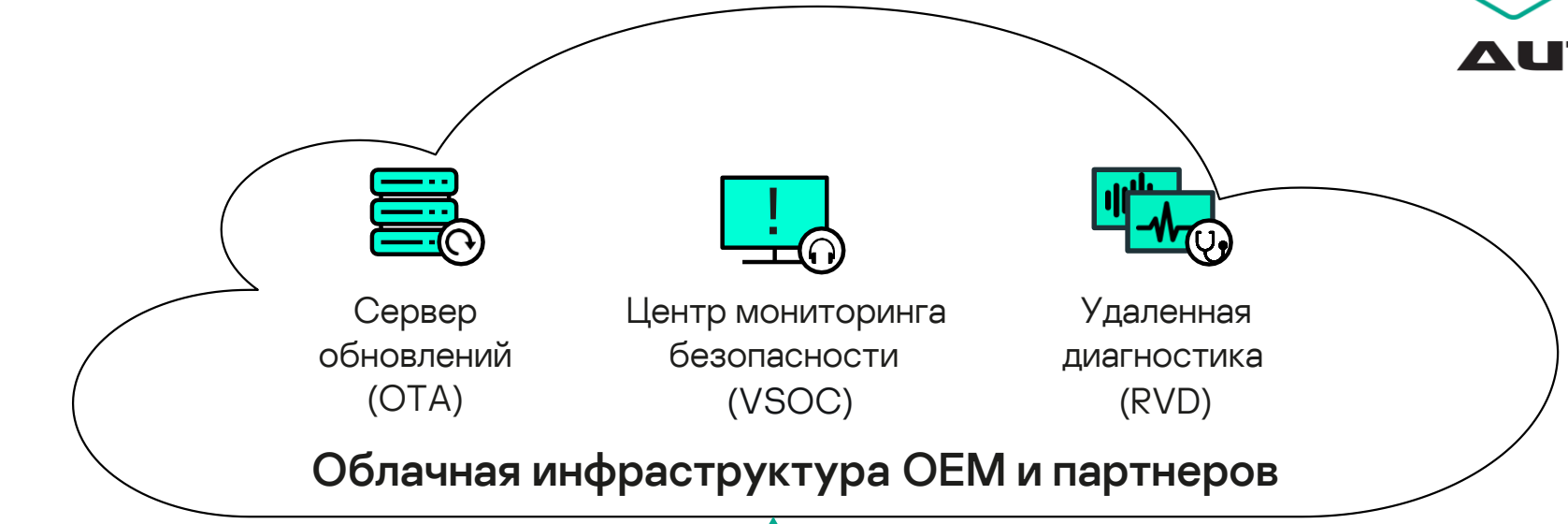
Подробности:

- Динамическая система, которая поддерживает любые сторонние приложения

Автомобильный шлюз безопасности Kaspersky Automotive Secure Gateway

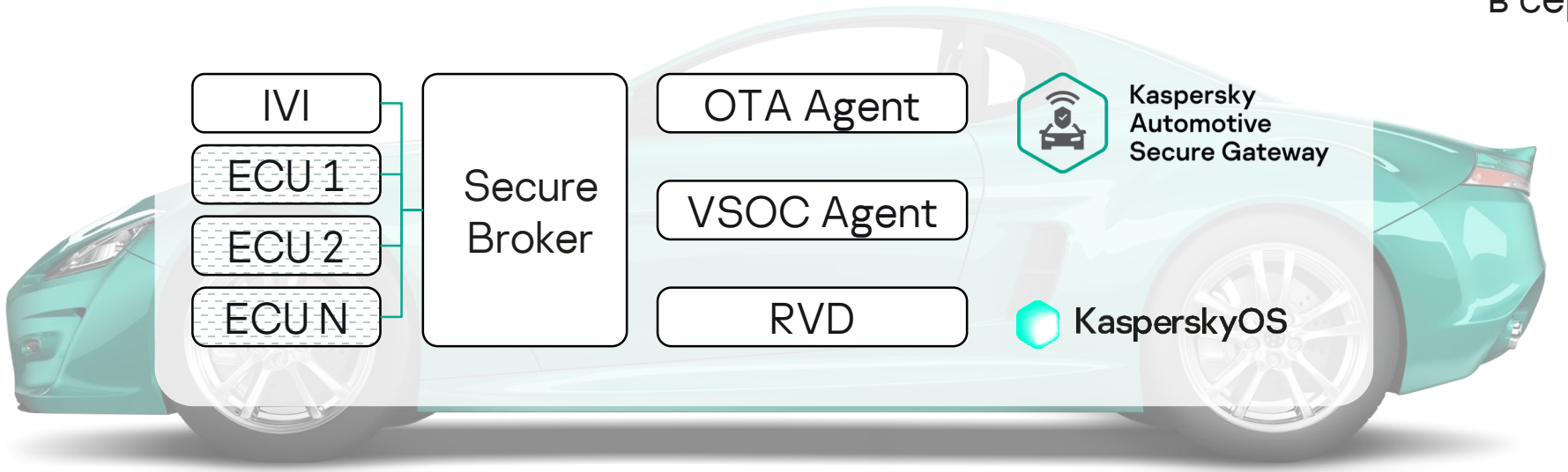
Kaspersky Automotive Secure Gateway

AUTOSAR

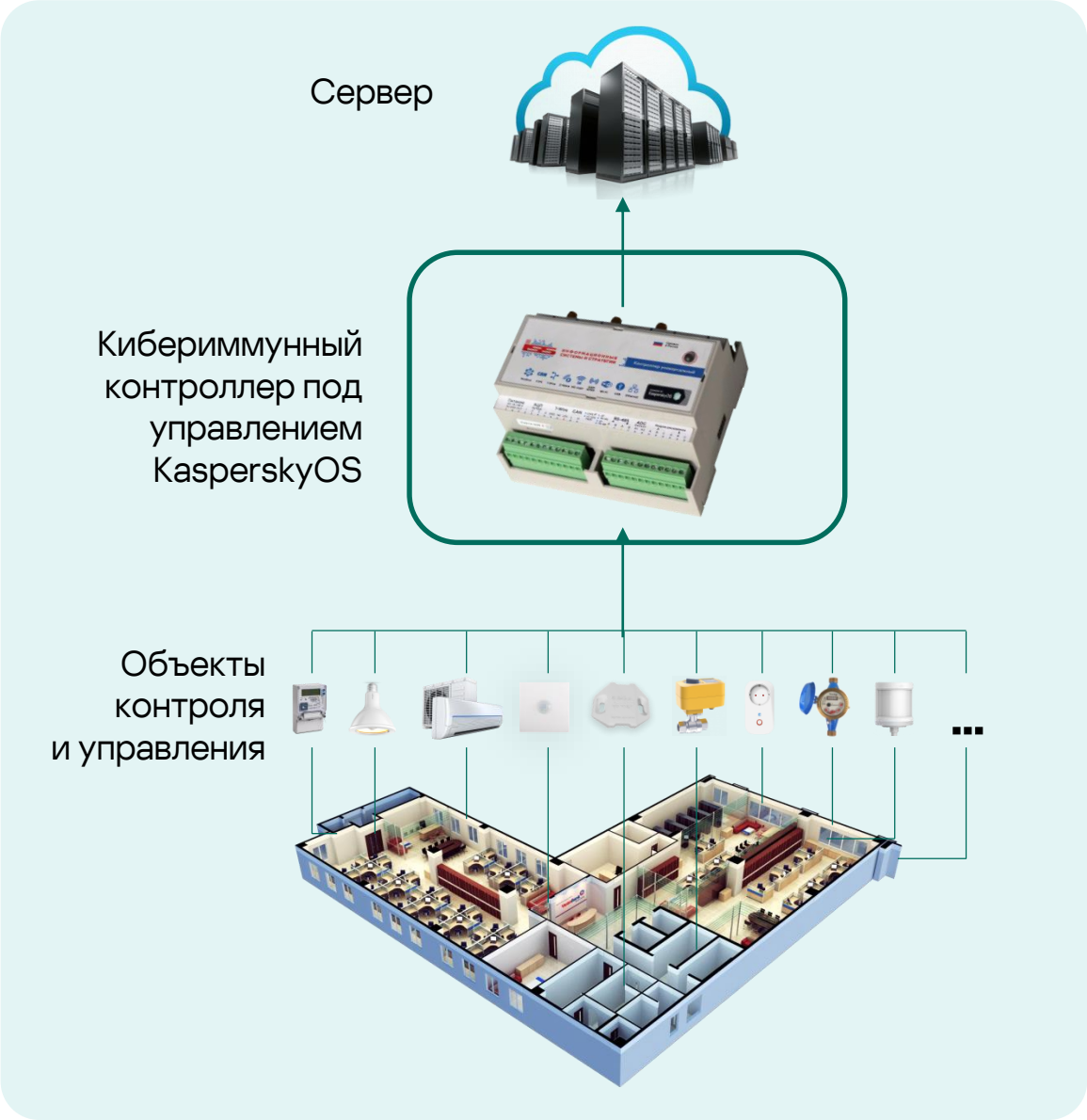


Смартфоны водителя и пассажиров

Устройства диагностики в сервис-центрах



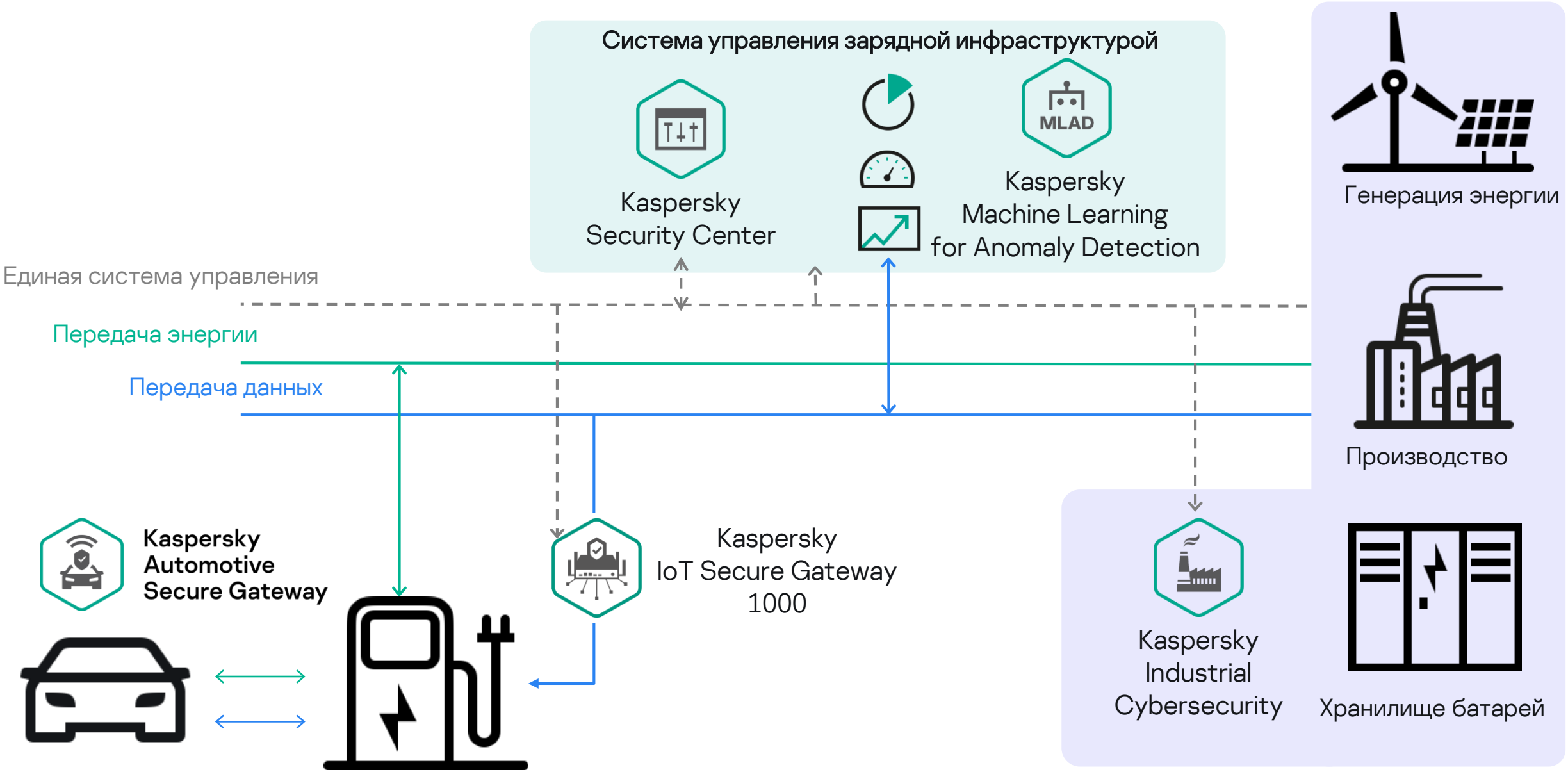
Система энергомониторинга Inspark.IoT Platform



Параметры мониторинга:

- электроснабжение;
- водоснабжение;
- теплоснабжение;
- комфортность среды (в подъездах);
- работоспособность лифтов, открытие дверей в шахтах;
- работоспособность домофонов;
- срабатывание пожарной сигнализации;
- срабатывание систем контроля доступа;
- и другие.

Обеспечение кибербезопасности зарядной инфраструктуры



Возможности разработки под KasperskyOS

Возможности KasperskyOS

- Инструменты для удобной разработки на KasperksyOS в том числе различные средства отладки (GDB, профилировщики и т.д.)
- Прослойка совместимости со сторонними ОС
- POSIX-совместима
- SMP и IOMMU
- Поддержка широко используемых библиотек
- Звуковая, Графическая и Сетевая подсистема
- Поддержка различной периферии (USB, сенсоры и т.д.)
- Разработка драйверов в пространстве пользователя
- Менеджер пакетов и приложений
- Поддержка широко используемых файловых систем включая виртуальные (VFS)
- Соответствие требованиям регулятора

Что доступно для возможности разработки

- инструменты разработки (SDK)
- доступ к документации и другим материалам по разработке ПО для KasperskyOS
- доступ к средствам технической поддержки
- канал для оперативного решения вопросов
- инструмент для дистрибуции приложений
- инструмент для подписи приложений

Пример взаимодействия с технологическим партнёром

kaspersky
cyber
immunity

Спасибо!

KasperskyOS

«Киберугрозы для АСУ и промышленных предприятий в 2023 году», отчёт Kaspersky ICS Cert

Существенное увеличение поверхности атаки

Цифровизация в погоне за повышением эффективности IIoT и SmartXXX

Увеличение количества атак на компьютеризированные системы

Уязвимые отрасли экономики:

- сельское хозяйство, производство удобрений, сельхозтехники и продуктов питания
- логистика и транспорт (включая транспорт энергоресурсов)
- энергетика, добыча и обработка полезных ископаемых, цветная и чёрная металлургия, химическая промышленность, судостроение, приборо- и станкостроение
- хайтек-компании, фармацевтика и производство медицинского оборудования
- + «традиционные» цели: госсектор, предприятия ВПК

https://ics-cert.kaspersky.ru/publications/reports/2022/11/22/ics-cyberthreats-in-2023-what-to-expect/

Кибериммунность

❶ Процесс

❶ Концепция безопасности продукта

❷ Цели и предположения безопасности

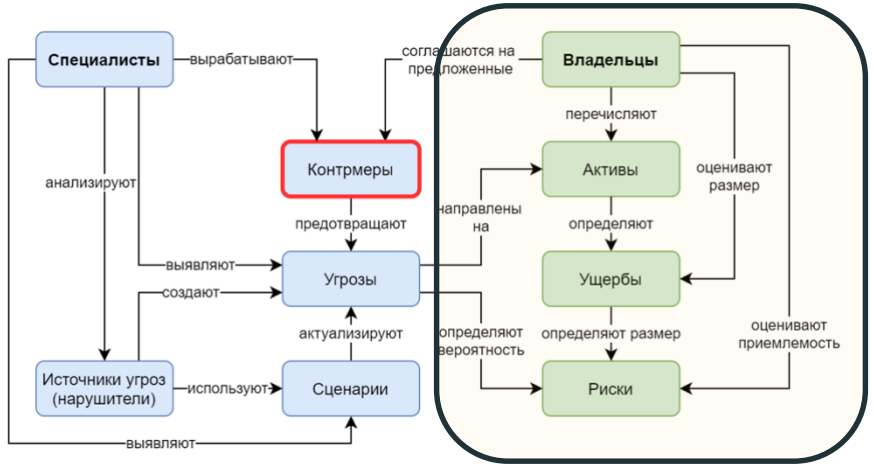
❸ Архитектура

❹ Разработка и тестирование

❺ Моделирование угроз

❻ Верификация

Заказчик или владелец ДОЛЖЕН описать ценности и какие риски в отношении них для него неприемлемы.



kaspersky

Кибериммунность

❶ Процесс

❶ Концепция безопасности продукта

❷ Цели и предположения безопасности

❸ Архитектура

❹ Разработка и тестирование

❺ Моделирование угроз

❻ Верификация

Не бывает безопасности «вообще», от всего и навсегда. Цели безопасности отражают неприемлемые риски, определенные заказчиком.

Без целей безопасности НЕТ кибериммунности.

kaspersky

Кибериммунность

❷ Архитектура

❶ Концепция продукта

❷ Цели безопасности

❸ Архитектура

❹ Разработка и тестирование

❺ Моделирование угроз

❻ Верификация

Архитектура строится под достижение целей безопасности. Основной инструмент – политика архитектуры. Декомпозируем и максимально используем шаблоны безопасности.

Один из итогов - выделение и минимизация доверенной кодовой базы.

Состав SDK

- Документация с примерами
- Toolchain
- Отладчик
- Эмулятор
- Плагин для VSCode
- Образ ядра
- Драйверы
- 3-rd party библиотеки
- Заголовочные файлы системных компонентов и драйверов

Holistic educational program (trainings)