Secure-by-Design /кибериммунитет/

или
как разрабатывать доверенные программы

Андрей Духвалов
Вице-Президент
Департамент Перспективных Технологий

kaspersky

Состояние индустрии информационной безопасности



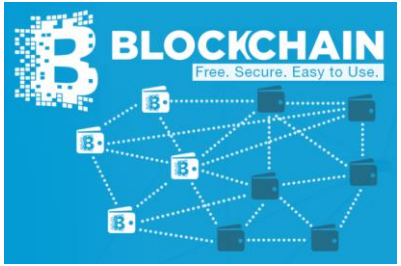
современные подходы и проблемы

Сложность современных IT-систем

Современные информационные системы — суперсложные

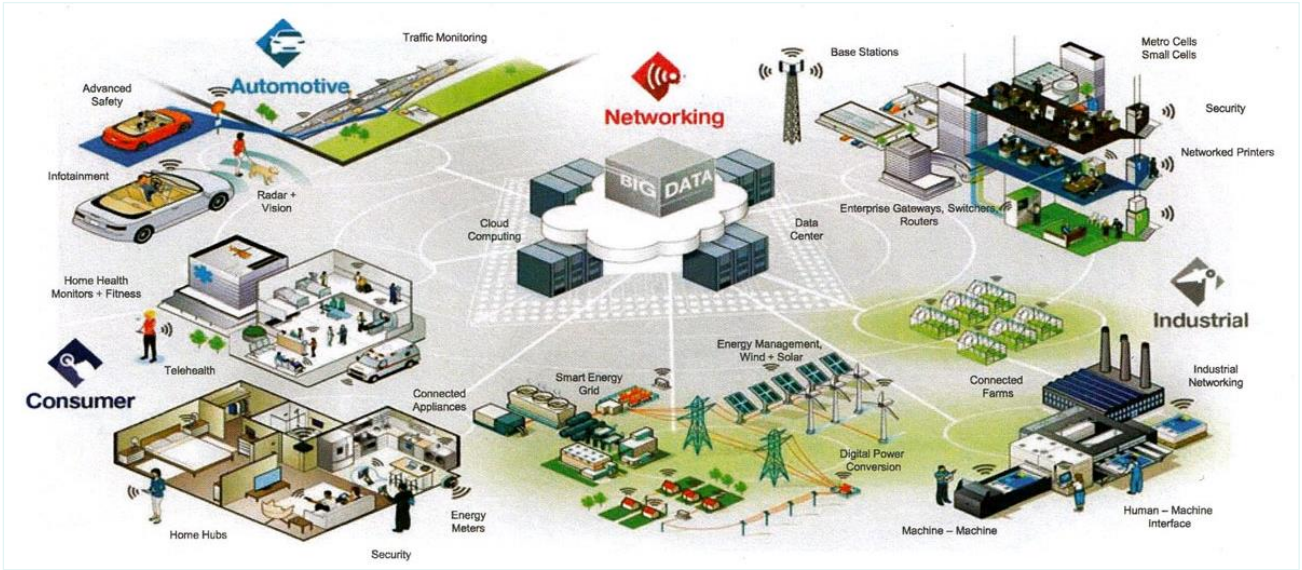
Сращиваются с физическим миром посредством различных умных устройств

Взаимодействуют между собой, образуя системы систем









Вызовы для CyberSecurity



Количество защитных технологий постоянно растет

- AntiVirus
  - / signatures
  - / SRC-checker
  - / ...
- application behavior blocker
- system behavior blocker
- whitelisting
- ...

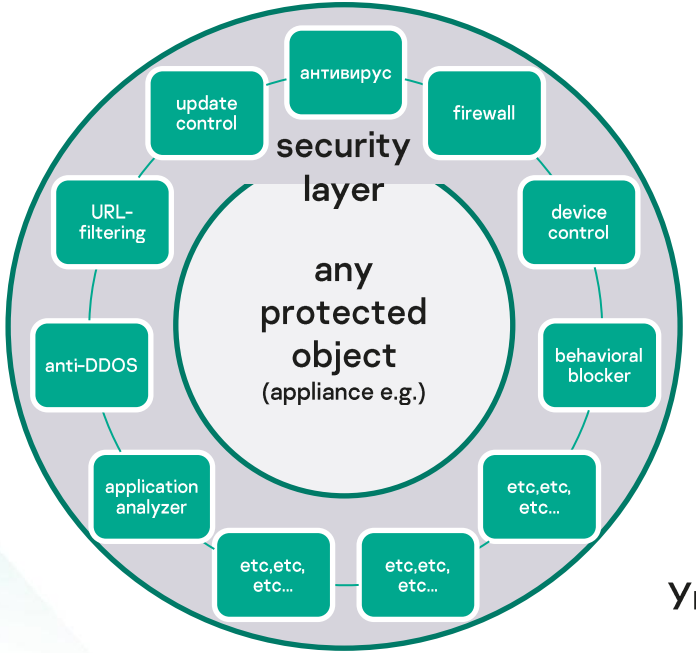
- anonymizer
- device control
- network analyzer
- process analyzer
- script-checker
- URL-filtering
- statistic analyzer
- secure payment
- web-antivirus
- ...

- anti-DDOS
- antispam
- antiphishing
- parental control
- update control
- firewall
- sandboxing
- ...

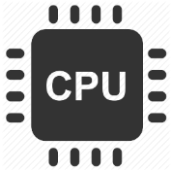
Количество угроз постоянно растет -> индустрии приходится отвечать реактивно

Современный подход – сложность технологий безопасности

современный подход:
“наложенная” безопасность



Такой подход требует:



Дополнительных вычислительных ресурсов



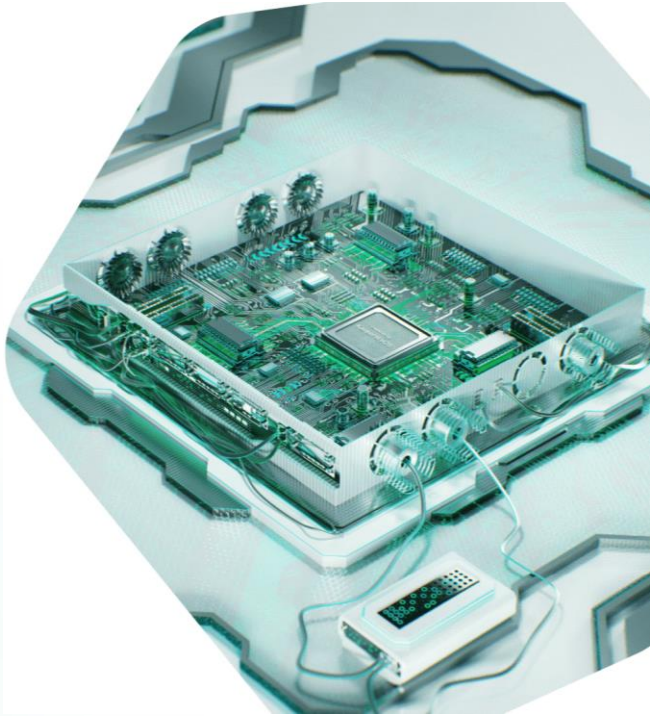
Расходы на электроэнергию



Дополнительный вес и размеры

Увеличивается сложность систем – уменьшается надежность

Кибериммунитет



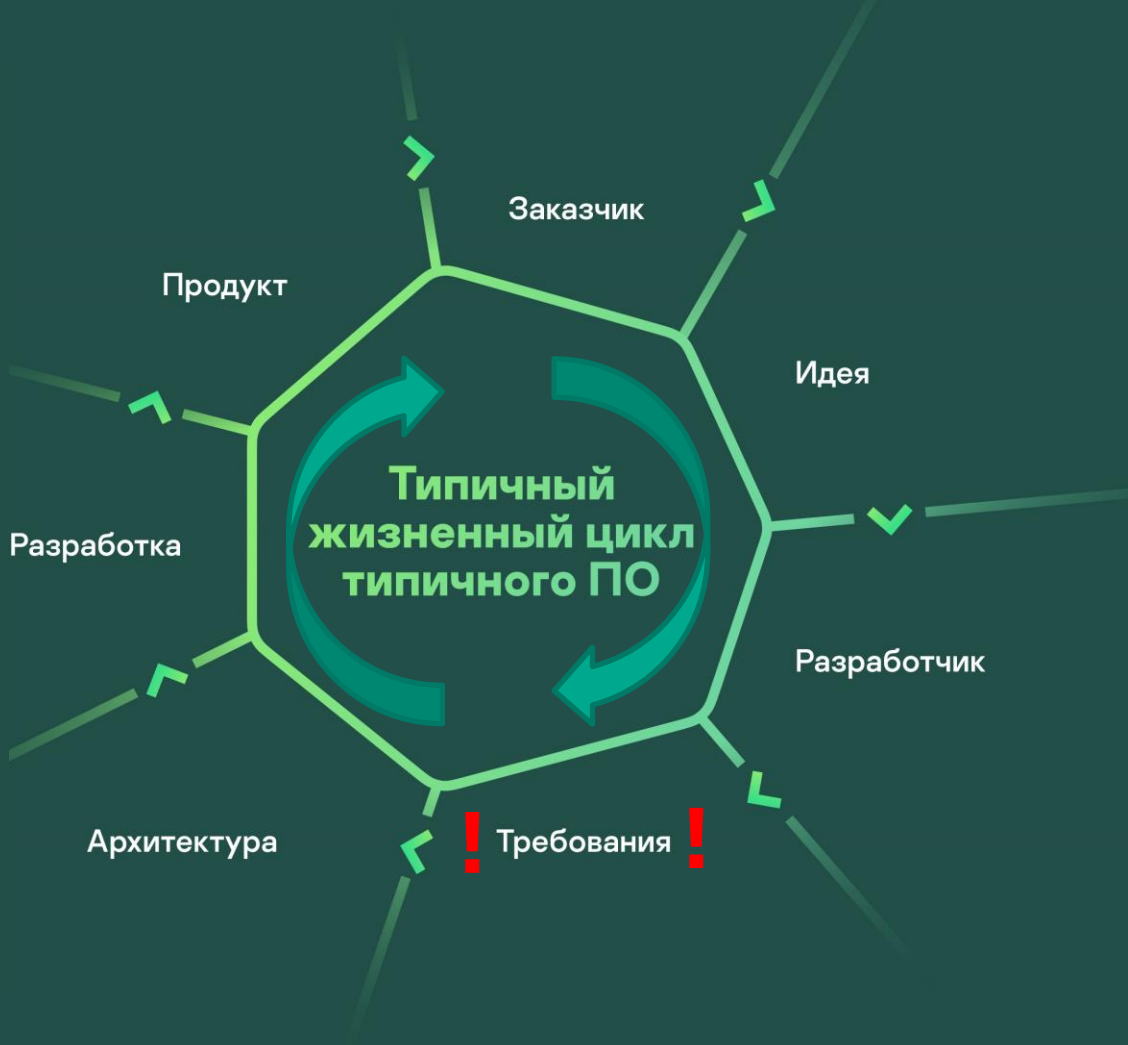
современный подход к разработке безопасных IT-решений

Кибериммунитет

Конструктивная безопасность
Secure-by-design

- Требования по безопасности учитываются наравне с другими бизнес-требованиями с самого начала разработки

- Методология разработки, позволяющая разрабатывать ПО способное устойчиво работать в неблагоприятной информационной среде



СТАНДАРТЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ВСЕХ УРОВНЯХ

Наследование или цепочка доверия



*Корень Доверия: в информационной системе (ИС) - вычислительный модуль, электронный компонент, код, и/или данные высшей степени доверия, предоставляющий базовые услуги безопасности остальной части ИС. В разных исполнениях, может быть частью ИС или внешним, по отношению к ней, модулем.

SECURE-BY-DESIGN

- Обязательное требование по анализу рисков и угроз на этапе проектирования
- Формальное доказательство требований доверия
- Множественные уровни безопасности

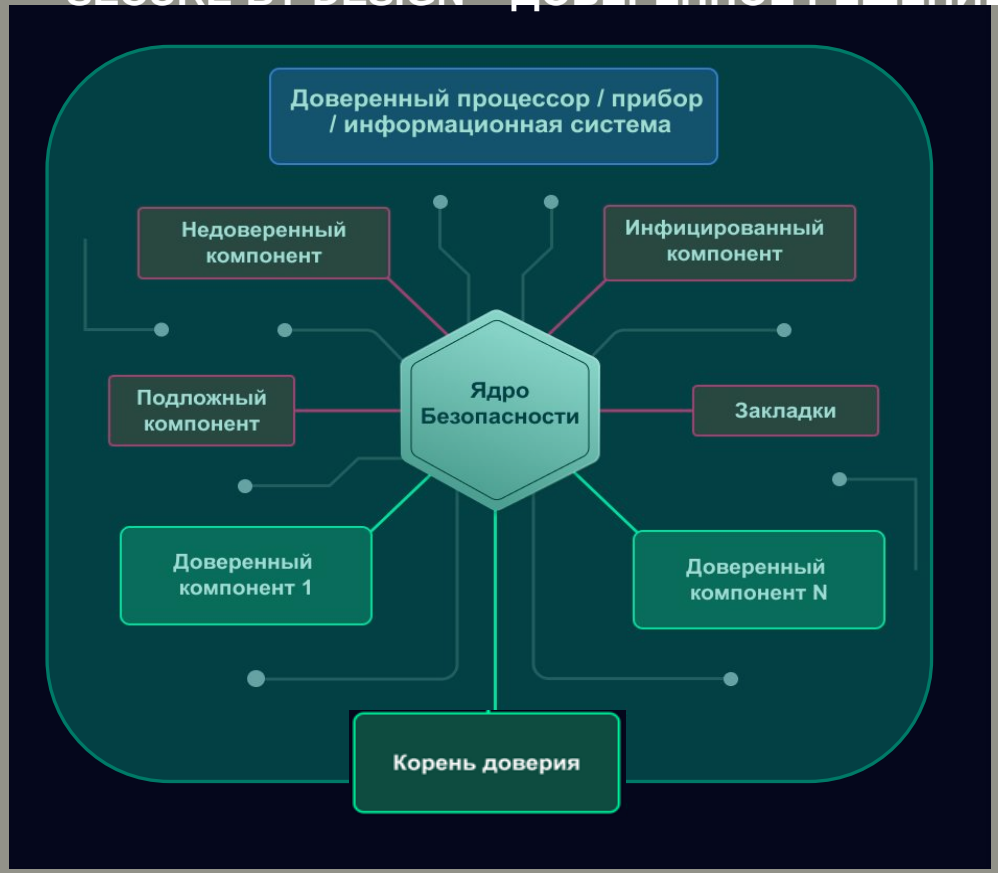
ДОВЕРЕННЫЙ ЖИЗНЕННЫЙ ЦИКЛ

- Корень доверия
- Доверенные маршруты проектирования
- Доверенные инструменты разработки
- Выполнение требований регулятора
- Верификация и контроль

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

- Корень доверия в каждом процессоре
- Идентификация на основе корня доверия
- Защита хранения и передачи данных обеспечивается шифрованием, привязанным к корню доверия

SECURE-BY-DESIGN = ДОВЕРЕННОЕ РЕШЕНИЕ ИЗ НЕ ДОВЕРЕННЫХ КОМПОНЕНТОВ



Изоляция и методы контроля исключают влияние на цели безопасности

Не доверенных компонентов

Их можно использовать без влияния на доверие к прибору

Изоляция и методы контроля позволяют создать «тепличные» условия для

Доверенных компонентов

Их можно использовать без опаски атаки на них

Доверенный Жизненный Цикл + архитектура Secure-by-Design позволяют создавать доверенные системы, используя недоверенные компоненты

Secure-by-Design = изоляция + ограничение прав. Запрещено все, что явно не разрешено

Secure-by-Design = меньше затрат на обеспечение безопасности, надежнее система

Secure-by-Design = выполнение целей безопасности обеспечивается ТОЛЬКО доверенными компонентами

Лаборатория Касперского — участие в разработке современных стандартов

Организация	Стандарт
IIC	✓ Industrial Internet Security Framework
	✓ Key Safety Challenges for the IIoT
	✓ IoT Security Maturity Model
ISO/IEC	ISO/IEC 30149 «Trustworthiness Principles»
	ISO/IEC 30141 «IoT Reference Architecture»
ITU/МСЭ	✓ X.iotsec: «Security capabilities supporting safety of the Internet of Things»
GP	Trusted Execution Environment (TEE)
	Technology Security Evaluation Standard for IoT Platforms (SESIP)
IEEE	✓ P2413. IoT Architectural Framework Standard
	P2413.1 IoT Architectural Framework for SmartCities
	P2418 & P2418.1 Standard for the framework of blockchain use in IoT

✓ Принято и опубликовано

Стандарты разработки информационных систем ТК362/РГ-8

Лаборатория Касперского –
Участие в создании современных стандартов (ГОСТов) разработки информационных систем, устойчивых к деструктивным воздействиям

Методология разработки доверенных приложений secure-by-design
Система оценки зрелости безопасности
Принцип многочисленных независимых уровней безопасности (MILS)
Доверенные операционные системы. Термины, определения, классификация
IoT. Системы с разделением доменов

Активируй будущее

Андрей Духвалов
Вице-Президент
Департамент Перспективных Технологий

kaspersky