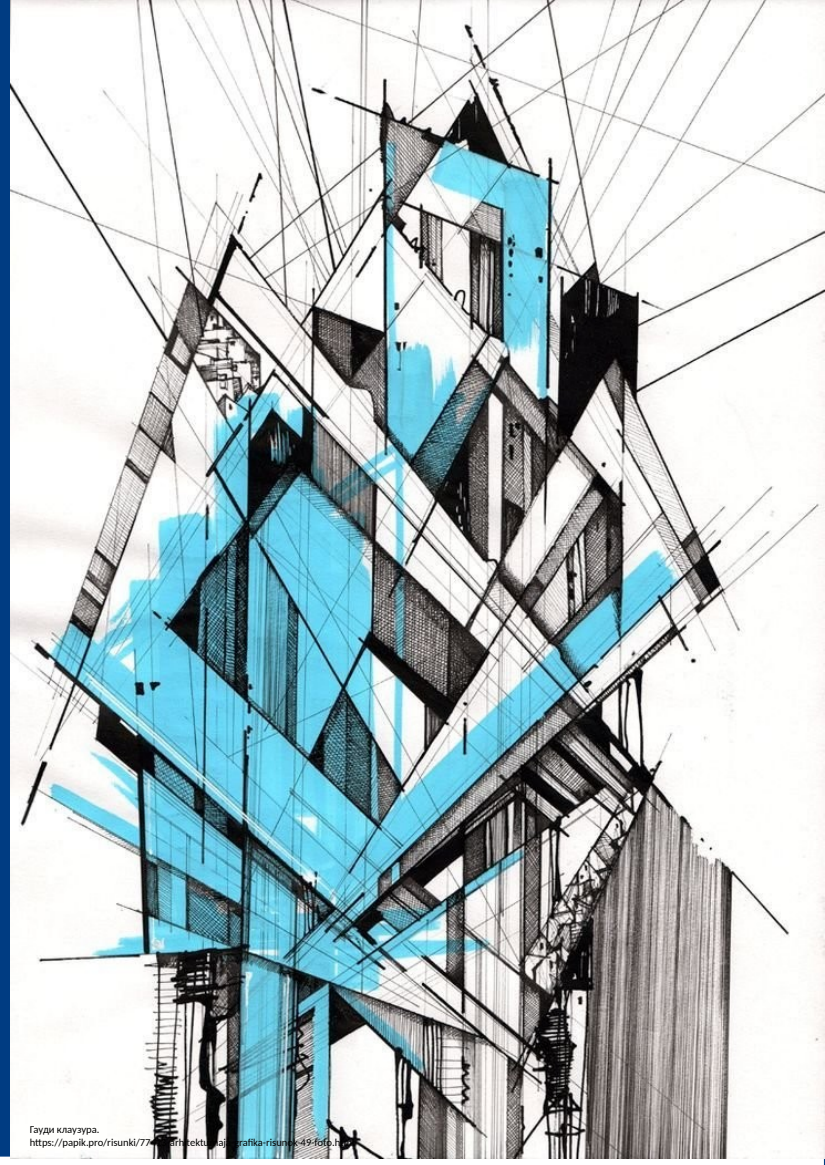
Конструктивная информационная безопасность. Архитектурные средства обеспечения доверия.

А.К. Петренко (petrenko@ispras.ru),

А.В. Хорошилов (khoroshilov@ispras.ru)

Институт системного программирования им. В.П.Иванникова

OSDAY-2025 - Москва, июнь 2025 года



Гауди клаузура.
https://papik.pro/risunki/774-arhitektura-grafika-risunok-49-foto.html

Дорожная карта «СейфНет»

ИСП РАН

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДОРОЖНОЙ КАРТЫ СЕЙФНЕТ

Доверенная ПЛАТФОРМА

1. КОНСТРУКТИВНАЯ БЕЗОПАСНОСТЬ

- Технологические риски и угрозы устойчивого функционирования
- Работа с требованиями
- Безопасная разработка, доверенный инструментарий
- Использование Доверенного ИИ на всех этапах дизайна и разработки
- Валидация и верификация
- Формирование задания на безопасность и профилей защиты

2. АРХИТЕКТУРА ДОВЕРИЯ И БЕЗОПАСНОСТИ

- Создание доверенных систем из элементов с разным уровнем доверия, Микроядерные ОС
- Защита на всех уровнях (от ЭКБ до систем)
- Инфраструктура на основе политик безопасности
- Доверенные Аппаратные Системы
- Защищенные процессорные архитектуры
- ЭКБ доверия и безопасности, Корень Доверия

3. ГАРАНТИИ ЦЕЛОСТНОСТИ

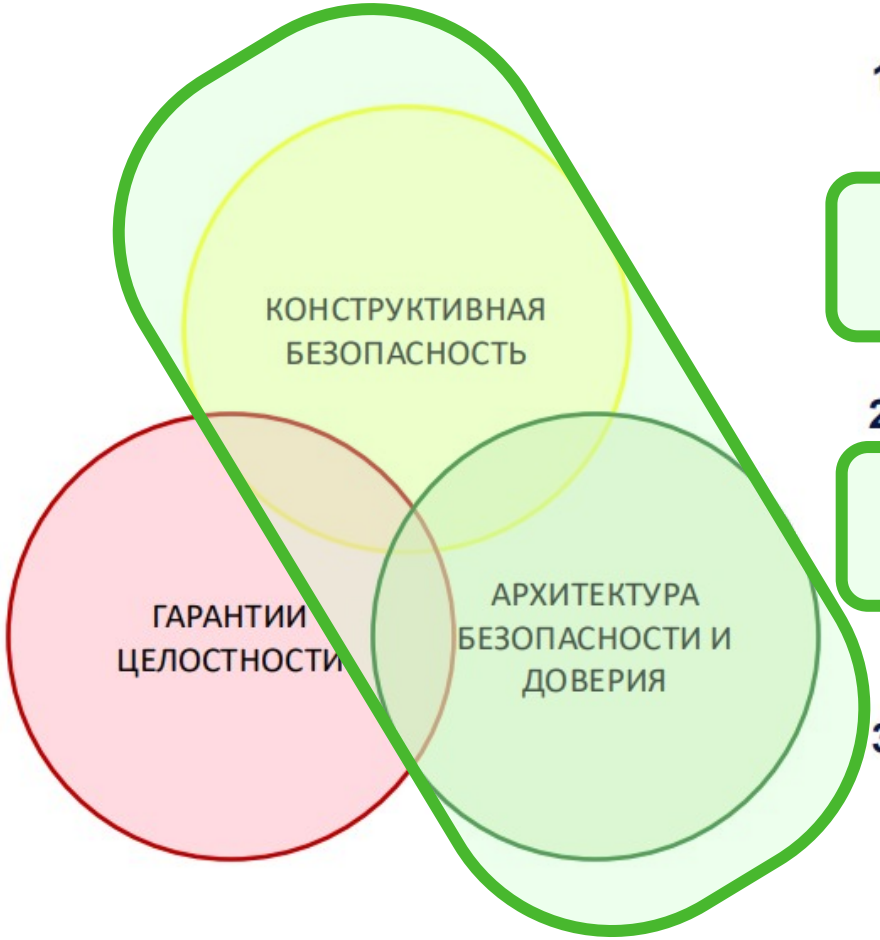
- Отечественная криптография и Удостоверяющие Центры
- Обеспечение целостности жизненного цикла путем использования криптографических методов и механизмов
- Защита информации на всех уровнях (от ЭКБ до систем)
- Цифровая подпись всех объектов

Участие ИСП РАН в Дорожной карте «СейфНет»

ИСП РАН

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДОРОЖНОЙ КАРТЫ СЕЙФНЕТ

Доверенная ПЛАТФОРМА



1. КОНСТРУКТИВНАЯ БЕЗОПАСНОСТЬ

- Технологические риски и угрозы устойчивого функционирования
- Работа с требованиями
- Безопасная разработка, доверенный инструментарий
- Использование Доверенного ИИ на всех этапах дизайна и разработки
- Валидация и верификация
- Формирование задания на безопасность и профилей защиты

2. АРХИТЕКТУРА ДОВЕРИЯ И БЕЗОПАСНОСТИ

- Создание доверенных систем из элементов с разным уровнем доверия, Микроядерные ОС
- Защита на всех уровнях (от ЭКБ до систем)
- Инфраструктура на основе политик безопасности
- Доверенные Аппаратные Системы
- Защищенные процессорные архитектуры
- ЭКБ доверия и безопасности, Корень Доверия

3. ГАРАНТИИ ЦЕЛОСТНОСТИ

- Отечественная криптография и Удостоверяющие Центры
- Обеспечение целостности жизненного цикла путем использования криптографических методов и механизмов
- Защита информации на всех уровнях (от ЭКБ до систем)
- Цифровая подпись всех объектов

Направления работ

1. КОНСТРУКТИВНАЯ БЕЗОПАСНОСТЬ
- Безопасная разработка, доверенный инструментарий (РБПО)
- Использование Доверенного ИИ на всех этапах дизайна и разработки
- Валидация и верификация

2. АРХИТЕКТУРА ДОВЕРИЯ И БЕЗОПАСНОСТИ
- Создание доверенных систем из элементов с разным уровнем доверия. Микроядерные ОС
- Инфраструктура на основе политик безопасности

Имеющийся задел

ИСП РАН

1. КОНСТРУКТИВНАЯ БЕЗОПАСНОСТЬ

- Безопасная разработка, доверенный инструментарий

  РБПО:

  - статические и динамические анализаторы кода, построение поверхности атак по коду, отладчики, симуляторы, генераторы тестов по коду, фаззеры, безопасный компилятор, технологии глубокой верификации программ
- Использование Доверенного ИИ на всех этапах дизайна и разработки
  - локализация причин ошибок, выявленных статическими и динамическими анализаторами
- Валидация и верификация
  - дедуктивная верификация, software model checking, анализ архитектурных моделей авионики

2. АРХИТЕКТУРА ДОВЕРИЯ И БЕЗОПАСНОСТИ

- Создание доверенных систем из элементов с разным уровнем доверия. Микроядерные ОС
  - архитектуры защищенных ОС на основе capabilities
- Инфраструктура на основе политик безопасности
  - дедуктивная верификация моделей управления доступом, динамическая верификация СЗИ на основе формальных моделей

Конструктивный подход к информационной безопасности (1)

ИСП РАН

Конструктивный подход к обеспечению информационной безопасности *)
(конструктивный подход): Подход, при использовании которого системе в процессе её создания **с момента замысла** придаются характеристики (свойства), которые должны обеспечивать соответствие целям безопасности, включая проверку такого соответствия.

Примечание – Примерами таких характеристик являются модульность, иерархичность, распределенность, устойчивость к сбоям и угрозам за счет резервирования элементов системы и т.п., которые могут выполняться не только для систем с конструктивной информационной безопасностью.

Примечание – Конструктивный подход применяется на протяжении жизненного цикла соответствующей системы, начиная с замысла, формирования концепции и проектирования…

*) – Проект **ГОСТ Р Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки**

Конструктивный подход к информационной безопасности (2)

ИСП РАН

Подход применим не только к новым разработкам. **Возврат к замыслу полезен**, а иногда и необходим не только при появлении новых требований и новых условий развертывания и эксплуатации программных систем, но и при развитии систем с учетом полученного опыта и багажа знаний о вскрытых проблемах и найденных дефектах программ.

Конструктивная безопасность – комплексный подход к разработке ПО и ПАК ответственного назначения, в котором особое внимание уделяется методам и средствам для поддержки **forward-инженеринга** с целью не только выявить устранить возможные дефекты и уязвимости систем, но и предупредить их появление на возможно более ранних фазах жизненного цикла.

Совместный проект ИСП РАН и Лаборатории Касперского

ИСП РАН

Дорожная карта
«Архитектурные средства обеспечения доверия программных систем» - АрКИБ

- Hardering
- Безопасные языки программирования
- Инструменты разработки архитектурных моделей и их исследования
- Интеграция инструментов и разнообразных артефактов и представления программ на разных фазах жизненного цикла
- Архитектурные паттерны, архитектурные модели, виды анализа
  - Репозитории архитектурных ошибок и уязвимостей

Уровни готовности технологий

ИСП РАН

- Hardering
- Безопасные языки программирования
- Инструменты разработки архитектурных моделей и их исследования
- Интеграция инструментов и разнообразных артефактов и представления программ на разных фазах жизненного цикла
- Архитектурные паттерны, архитектурные модели, виды анализа
- Репозитории архитектурных ошибок и уязвимостей

Архитектурные модели. Интеграция процессов моделирования и верификации в жизненный цикл

ИСП РАН

Один из подходов - включение в ЖЦ работ по созданию и верификации архитектурных моделей с целью выявления потенциальных уязвимостей. Использование этого подхода требует:

- наличие развитых инструментов и технологий создания и анализа архитектурных моделей,
- интеграции инструментов архитектурного моделирования с другими процессами и технологиями,
- ведение сбора и систематизации
  - паттернов и анти-паттернов проектирования надежных и защищенных систем,
  - лучших практик, сценариев использования инструментов и методов проектирования и анализа архитектурных решений, верификации моделей и интеграции этих техник в жизненный цикл разработки.

Задачи дорожной карты «АрКИБ». Предшественники

ИСП РАН

- Гильберт (1900) - 23 проблемы (к 2025 г. решено 16)
- Сэр Тони Хоар (2003) - Grand Challenges for Computing Research. Требования к Grand Challenge задаче:

- **Фундаментальная**
- **С проверяемым результатом**
- **Революционная**
- **Вдохновляющая**
- **Понятная**
- **Сложная**
- **Полезная**
- **С историей**
- **Решаемая**
- **Декомпозируемая**
- **Стимулирует кооперацию**
- **Допускает конкуренцию**

Сэр Тони Хоар - Grand Challenges for Computing Research*)

ИСП РАН

- Prove that P is not equal to NP (open)
- The Turing test (outstanding)
- The verifying compiler (abandoned in 1970s)
- A championship chess program (completed)
- A GO program at professional standard (too difficult)
- Automatic translation from Russian to English (failed in 1960s)
- A mathematical model of the evolution of the web (new)
- A wearable computer serving as a guide dog for the blind (new)

*) Journal of the ACM (JACM), Volume 50, Issue 1, 2003.

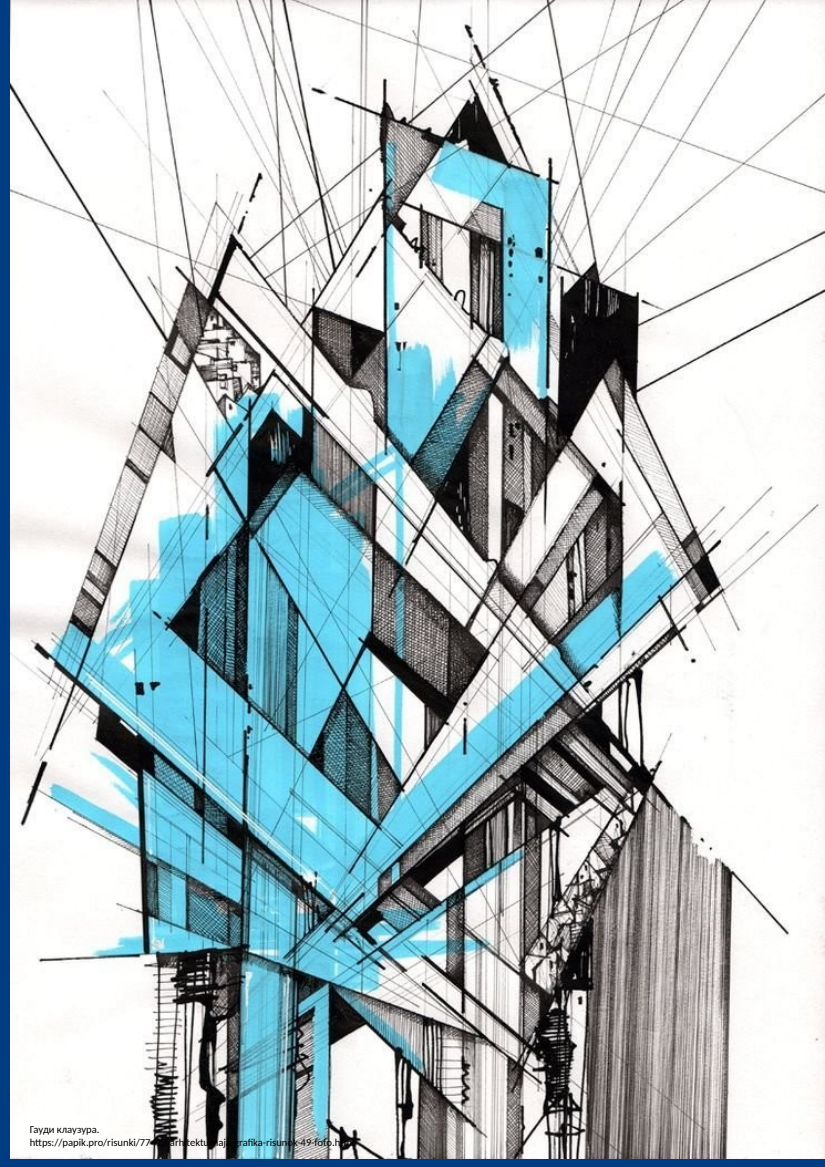
Задачи дорожной карты «АрКИБ»

ИСП РАН

Оценка задач дорожной карты «АрКИБ»

- Фундаментальная
- С проверяемым результатом
- Революционная
- Вдохновляющая
- Понятная
- Сложная
- Полезная
- С историей
- Решаемая
- Декомпозируемая
- Стимулирует кооперацию
- Допускает конкуренцию

Спасибо!



Гауди клаузура.
https://papik.pro/risunki/77...