ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

АКТУАЛЬНЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ

НОВЫЕ РЕАЛЬНОСТИ

- Защита ПД перешла из экзотики в обыденность
- Системы Госуслуг и УЭК – становятся массовыми (более 1 миллиона пользователей)
- Новые элементы складывающегося ЭДО: электронные счета-фактуры с шифрованием и ЭЦП, УЭК как банковская карта
- Число пользователей ЭЦП и SSL превысило 10 миллионов обычных граждан

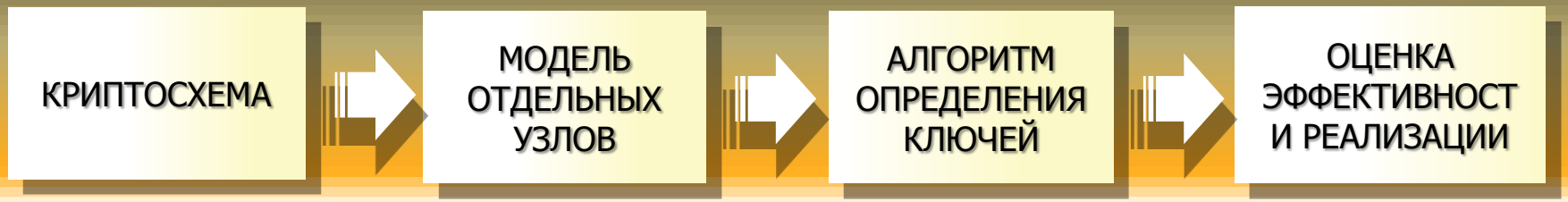
НОВЫЕ ЗАДАЧИ ВЫТЕКАЮЩИЕ ИЗ НОВОЙ РЕАЛЬНОСТИ

ПРОБЛЕМЫ КРИПТОГРАФИИ

- Еще более актуален единый формат (побитно) шифрования IP пакета для гражданского общества
- СКП в ЭЦП требует единого побитного формата. Вариативность – вредна для взаимодействующих АИС
- Изменение криптосхем становиться трудной задачей. Параллельность применения нескольких криптосистем

КУДА МОГУТ РАЗВИВАТЬСЯ КРИПТОИССЛЕДОВАНИЯ

- Схема исследования



- Чем ближе модель к схеме, тем она сложнее рассчитывается
- Резерв в применении и обосновании новых моделей узлов, блоков или криптопримитивов
- Ощущается нехватка квалифицированных математиков-криптографов. Возможно фирменное целевое обучение?

ПО ЗАЩИТЕ ОТ НСД

- Проблема визуализации подписываемой информации
- Сохранение в тайне ключей при массовом шифровании и уже развернутом массовом нападении
- Простые в использовании и массовые в применении средства защиты от НСД к процессам
- Поддержание контролируемой среды вычислений. Удаленный аутсорсинг для граждан

АКТУАЛЬНЫЕ ЗАДАЧИ ВЫЧИСЛИТЕЛЬНЫХ СРЕД

- Преодоление массовой зараженности и невольного участия ПК в бот-сетях. Как антивирус?
- Сертификация режима виртуализации для пользовательского уровня в распространенных ОС типа Windows, Linux
- Сертификация гипервизоров и технологии VDI для развития облачных вычислений. Сейчас только VMware
- Массовые защищенные технологии для основных мобильных устройств доступа к облакам

ЗАКОНОДАТЕЛЬНАЯ БАЗА

- Корректировка закона об ЭП №63. Должен быть полноценный регулятор.

- Корректировка Закона о Лицензировании в части криптографии:
  а) Контроль импорта оставить только для ГО;
  б) Лицензирование услуг шифрсвязи однозначно должно распространяться только на оператора шифрсвязи
  в) Производство средств шифрсвязи должно лицензироваться только для применения ГО

- Законодательно закрепить создание СРО в отрасли защиты ПД, исходя из имеющихся требований ФСБ РФ и ФСТЭК РФ

СПАСИБО ЗА ВНИМАНИЕ