Акционерное общество
«Институт точной механики и вычислительной техники
имени С.А. Лебедева
Российской академии наук»

ОТЕЧЕСТВЕННАЯ ИНТЕЛЛЕКТУАЛЬНАЯ СИМ-КАРТА КАК ЯДРО БЕЗОПАСНОСТИ ДОВЕРЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Институт точной механики и вычислительной техники имени С.А. Лебедева Российской академии наук

- ИТМиВТ был основан в 1948 году

- В ИТМиВТ созданы:
  - ✓ электронно-вычислительные машины, ставшие в свое время государственным промышленным стандартом и основой для таких стратегических систем, как Система противоракетной обороны (ПРО), Система предупреждения о ракетном нападении (СПРН), Система контроля космического пространства (СККП)

- Совокупность уникальных компетенций сотрудников Института позволяют выполнять высокотехнологичные работы:
  - ✓ по проектированию, разработке и сертификации распределённых сетей, включающих программные и технические средства защиты:
    - ✓ криптографические алгоритмы;
    - ✓ алгоритмы аутентификации;
    - ✓ системы цифровой подписи;
    - ✓ удостоверяющие центры;
    - ✓ механизмы разграничения доступа и защиты от несанкционированного доступа;
    - ✓ иные программные и аппаратные комплексы

Актуальные задачи информационной безопасности

- Цифровые технологии позволяют повысить эффективность контроля и управления технологическими процессами, в том числе и критически важными, оптимизировать издержки

- Успешная реализация комплексной задачи цифровизации различных отраслей экономики с обеспечением соответствующего уровня информационной безопасности и защиты информации -это:
  - ✓ обеспечение защиты технологических процессов критически важных операций;
  - ✓ реализация систем мониторинга активности в промышленных системах и сетях;
  - ✓ анализ уязвимостей ;
  - ✓ обеспечение безопасности систем связи и коммуникаций в различных комплексных структурах, особенно в условиях массового и глобального внедрения в практику устройств, сервисов и систем глобальной и корпоративной мобильной связи для обмена оперативной производственной информацией, мониторинга производственных процессов, удаленного доступа к корпоративным ресурсам

Практически все используемое в настоящее время программное и аппаратное обеспечение сотовой связи – от СИМ-карты до оборудования операторов - иностранного производства, своеобразные «чёрные ящики» с возможным наличием недекларированных функций

Угрозы информационной безопасности

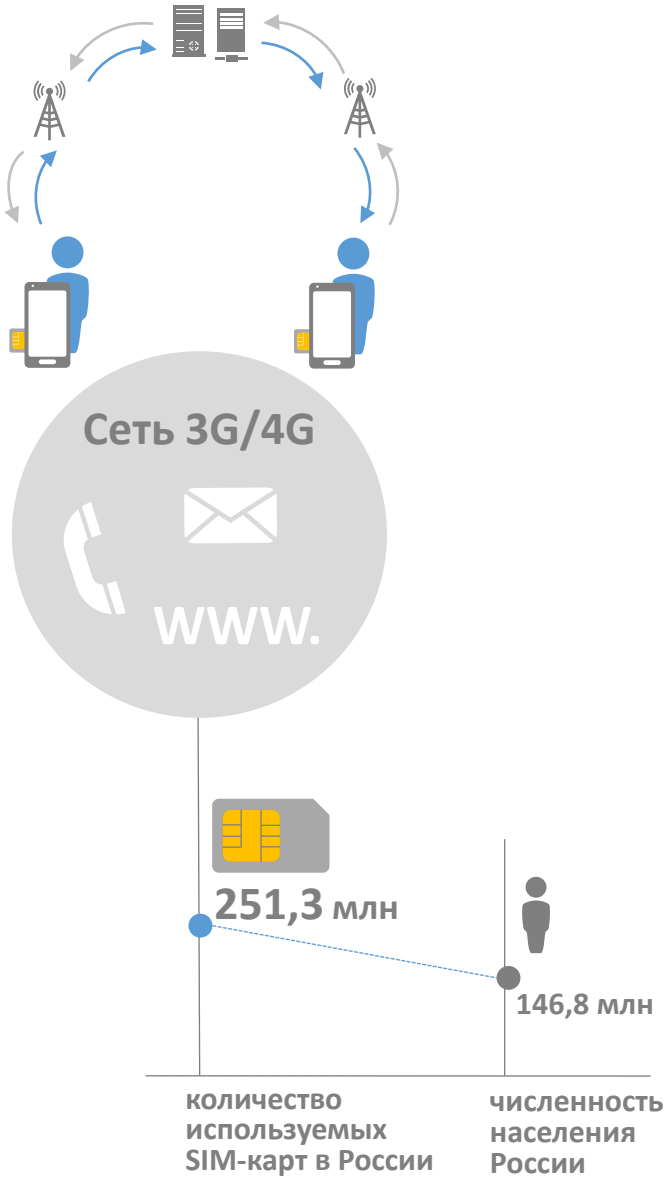
ИТМиВТ

Иностранные алгоритмы генерации ключей

УГРОЗА
доступа третьих лиц к данным абонента

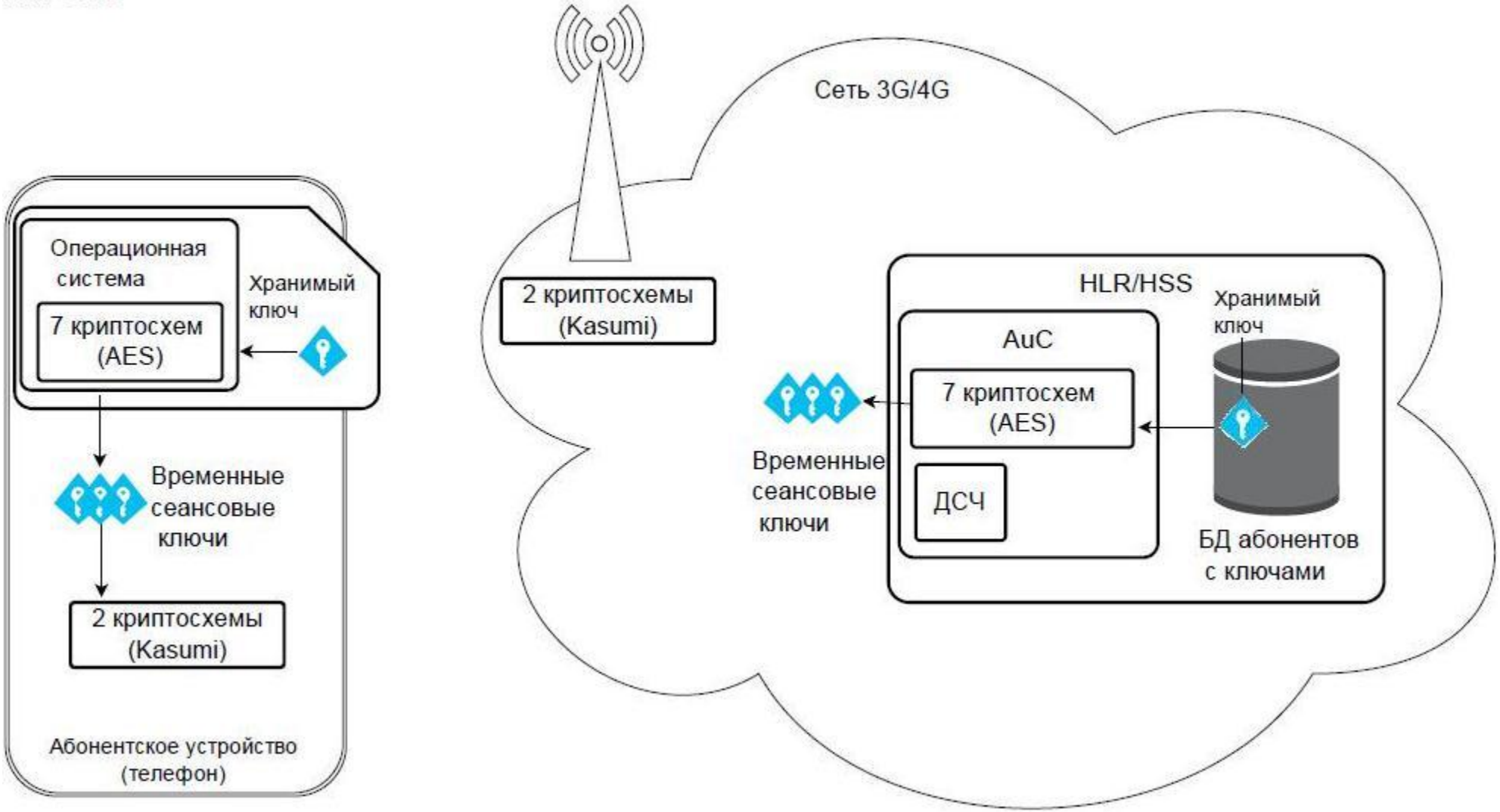
- персональные данные в телефоне
- контроль российского сегмента мобильного интернета
- данные о личных сообщениях и вызовах

- Клонирование СИМ карт
- Перехват трафика у критических объектов
- Прослушивание телефонной связи



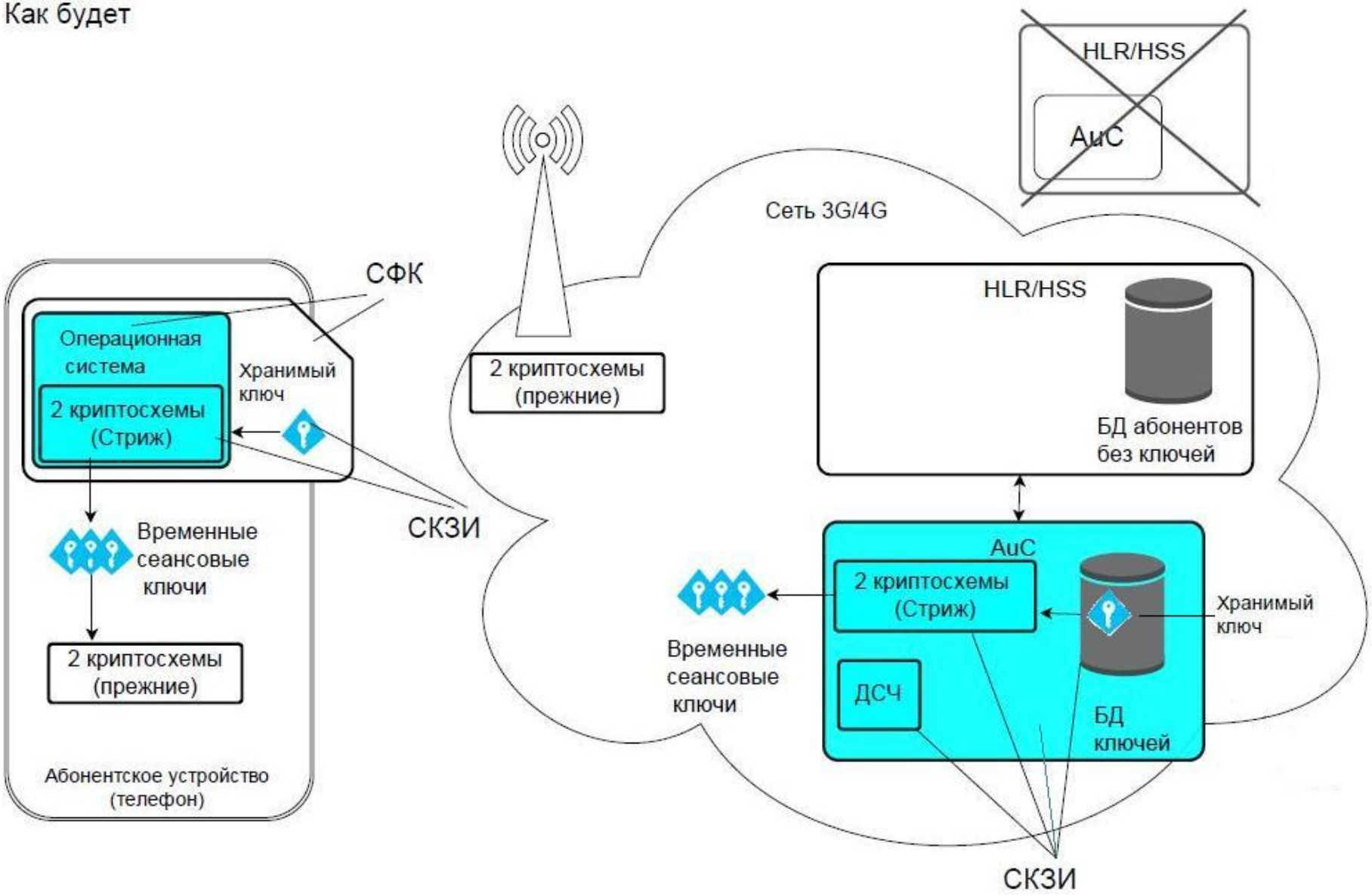
Решение для повышения информационной безопасности

Как есть



Решение для повышения информационной безопасности

Как будет



Доверенная СИМ-карта в цифровой среде

- Доверенная СИМ-карта позволяет:
  - ✓ реализовать контроль и блокировку попыток несанкционированного обращения к защищаемым алгоритмам и данным;
  - ✓ построить доверенную программно-аппаратную среду, выполняющую следующие функции:
    - ✓ хранение персональных данных и другой значимой служебной информации;
    - ✓ замкнутой доверенной среды, реализующей основные криптографические примитивы (выработка псевдослучайных чисел, выработка цифровой подписи с использованием личного ключа, проверка цифровой подписи, выработка сеансового ключа, зашифрование (расшифрование) сообщений)
- Перечисленные технические возможности позволяют обеспечить безопасную аутентификацию пользователя СИМ-карты и защищенный канал связи для передачи идентификационных данных и служебной информации

Защищенный канал связи позволит обеспечить безопасность передаваемых служебных (персональных) данных и дополнит функционал информационной системы, закрыв риски, связанные с использованием недоверенной программно-аппаратной среды на стороне пользователя

Перспективы использования доверенной СИМ-карты

- Доверенная СИМ-карта как элемент структуры цифрового доверия позволит обеспечить:

  - ✓ внедрение мобильной квалифицированной электронной подписи (КЭП);
  - ✓ реализацию услуг удаленного доступа к различным документам;
  - ✓ электронную регистрацию документов, с подтверждением подлинности действий;
  - ✓ реализацию на базе закрытой области памяти защищенного хранилища паролей для доступа к критически важным системам;
  - ✓ предоставление абонентам возможности доверенного и защищенного хранения персональных данных (цифрового профиля абонента) и безопасного доступа к ним;
  - ✓ возможность загрузки доверенных приложений и операционной среды (например, ОС Sailfish Rus) из магазинов ПО с проверкой подписи и сертификатов и блокирование записи на мобильное устройство потенциально вредоносного программного обеспечения;
  - ✓ защищенный безопасный обмен информацией специализированными устройствами – «интернет вещей», M2M, «умный город»;
  - ✓ реализацию новых перспективных безопасных функций, в частности, защищенного голосового канала для конфиденциального общения

ИТМиВТ

Спасибо за внимание !