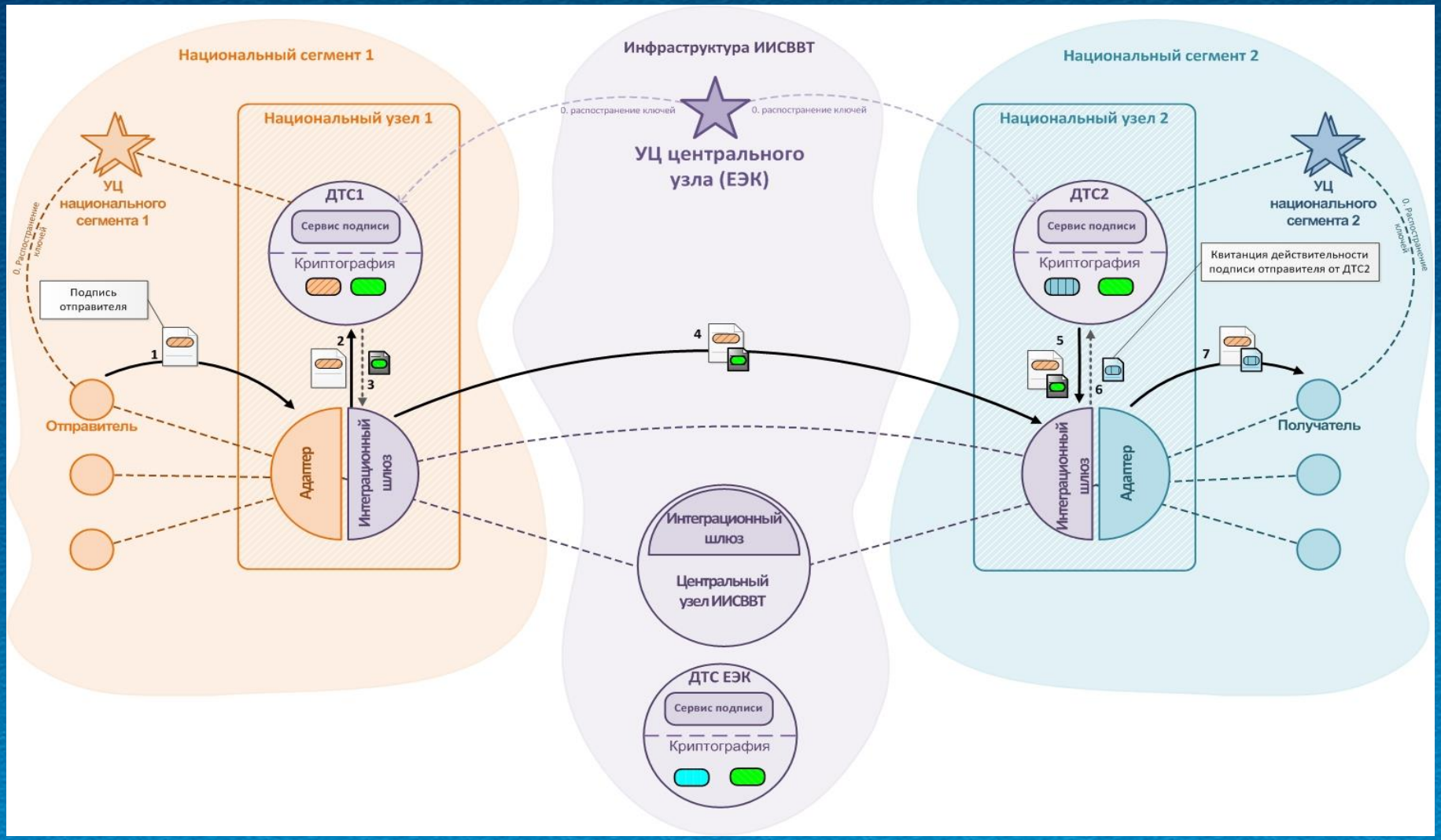
Требования к доверенной третьей стороне в интегрированной информационной системе Евразийского экономического союза

Доктор физико-математических наук
Кузьмин Алексей Сергеевич

Функциональная схема ИИС ЕАЭС



Функциональные требования к ДТС

осуществление легализации (подтверждение подлинности) электронных документов и электронных подписей субъектов информационного взаимодействия в фиксированный момент времени

обеспечение гарантий доверия в международном (трансграничном) обмене электронными документами

обеспечение правомерности применения электронных подписей в исходящих и (или) входящих электронных документах в соответствии с законодательством государств-членов и актами ЕАЭС

Базовые сервисы

- служба доверенного времени
- служба проверки подлинности ЭП
- службы реализации политик безопасности
- службы каталогов сертификатов
- служба OCSP
- центры атрибутирования
- служба архивирования электронных документов

Общие Требования к информационной безопасности ДТС

Сервис доверия должен обеспечивать безопасную обработку персональных данных

При функционировании сервиса доверия должны гарантироваться конфиденциальность и целостность данных пользователей

При функционировании сервиса доверия должны реализовываться надлежащие технические и организационные меры для управления угрозами безопасности

В случае возникновения при функционировании сервиса доверия нарушений безопасности необходимо уведомить компетентный орган в области информационной безопасности не позднее, чем через 24 часа после того, как о нарушениях стало известно

Сервис доверия должен нести ответственность за любые прямые убытки, вызванные ненадлежащим выполнением обязанностей

В части безопасности информации национальные требования, применимые к квалифицированным сервисам доверия, должны быть согласованы с требованиями, учрежденными в государственном объединении

Основные разделы Требований к информационной безопасности ДТС

I. Требования к программному обеспечению ДТС

Программное обеспечение ДТС:

- не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы;
- должно использовать только документированные функции операционной системы, не должно содержать известных уязвимостей;
- должно обеспечивать разграничение доступа системного администратора, оператора и пользователей, к информации, обрабатываемой в ДТС, на основании правил разграничения доступа, заданных системным администратором;
- исходные тексты должны пройти проверку на отсутствие недекларированных возможностей;
- должен применяться механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа;
- должен применяться механизм, обеспечивающий устойчивость к компьютерным атакам из внешних сетей.

II. Требования к аппаратным средствам ДТС:
Проводится проверка (совместно с анализом программного кода BIOS) реализации целевых функций ДТС на основе системы тестов для аппаратных средств ДТС, с целью исключения негативных функциональных возможностей. Проводится оценка параметров надежности функционирования аппаратных средств.

III. Требования к целостности:
Средства ДТС должны содержать механизм контроля случайного или преднамеренного искажения информации, программных средств и аппаратных средств до загрузки операционной системы.

IV. Требования к управлению доступом:
В ДТС должен обеспечиваться дискреционный принцип контроля доступа и должно быть обеспечено создание замкнутой рабочей среды.

V. Требования к защите данных:

ДТС должна обеспечивать передачу данных, содержащих информацию ограниченного доступа, способом, защищенным от НСД, должен быть реализован механизм защиты данных при передаче их между физически разделенными компонентами на основе криптографических средств.

VI. Требования к регистрации событий

Базовая операционная система средств ДТС должна поддерживать ведение защищенного журнала аудита системных событий и событий, связанных с выполнением ДТС своих функций.

VII. Требования к резервному копированию:

Средства ДТС должны реализовывать функции резервного копирования и восстановления, должны быть приняты меры обнаружения несанкционированных изменений сохраненных данных; должны быть определены требования ко времени восстановления.

VIII. Требования к формату сертификатов

ДТС должна использовать квалифицированные сертификаты.

IX. Требования к средствам ЭП

ДТС должна использовать средства ЭП класса – КВ2, реализуемые на основе доверенного вычислительного устройства, имеющего средства отображения результатов создания/проверки ЭП.

X. Требования к криптографическим стандартам

ДТС должна использовать криптографические средства в которых реализуются отечественные стандарты - ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», для криптографических средств обеспечения режима конфиденциальности информации ограниченного доступа - ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Класс защиты ДТС национального сегмента Российской Федерации

КВ2

СПАСИБО ЗА ВНИМАНИЕ