Мероприятия по переходу на использование российских криптографических алгоритмов между государством и обществом

Докладчик: **Пьянченко А.А.**

Дата: 17 сентября 2019 г.

МЫ ВЫНУЖДЕНЫ

- покупать сертификаты за границей
- пользоваться западной криптографией при информационном взаимодействии
- использовать западную реализацию алгоритмов и протоколов

МЫ НЕ МОЖЕМ

- гарантировать доверие к веб-ресурсу
- обеспечить защиту данных гражданина
- управлять инфраструктурой PKI

Как следствие

4 июня 2018 года

*«К сожалению, наложенные Соединенными Штатами Америки санкции требуют, чтобы мы отозвали ваш сертификат для *.oprf.ru из-за того, что ваша организация аффилирована с Донецкой Народной Республикой, находящейся под санкциями Управления по контролю над иностранными активами».*

Основание

Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования (Пр-1380).

При разработке указанного комплекса мероприятий предусмотрите в числе прочих:

1) предоставление безвозмездного доступа гражданам Российской Федерации к использованию российских средств шифрования для электронного взаимодействия с органами государственной власти и органами местного самоуправления;

2) законодательные меры с целью исключить применение оборудования, позволяющего третьим лицам вмешиваться в работу криптографических протоколов при передаче данных с использованием сети связи общего пользования, кроме случаев реализации органами, осуществляющими оперативно-разыскную деятельность, мероприятий по снятию информации с технических каналов связи в соответствии с требованиями законодательства Российской Федерации.

Основание

План мероприятий перехода в 2018 - 2020 годах федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления на использование российских криптографических алгоритмов и средств шифрования при электронном взаимодействии между собой, с гражданами и организациями № 6660п-П10 (дорожная карта М.А. Акимова).

Федеральный проект «**Информационная безопасность**» Нацпрограммы «**Цифровая экономика** России 2024»

НУЦ

Веб-ресурс

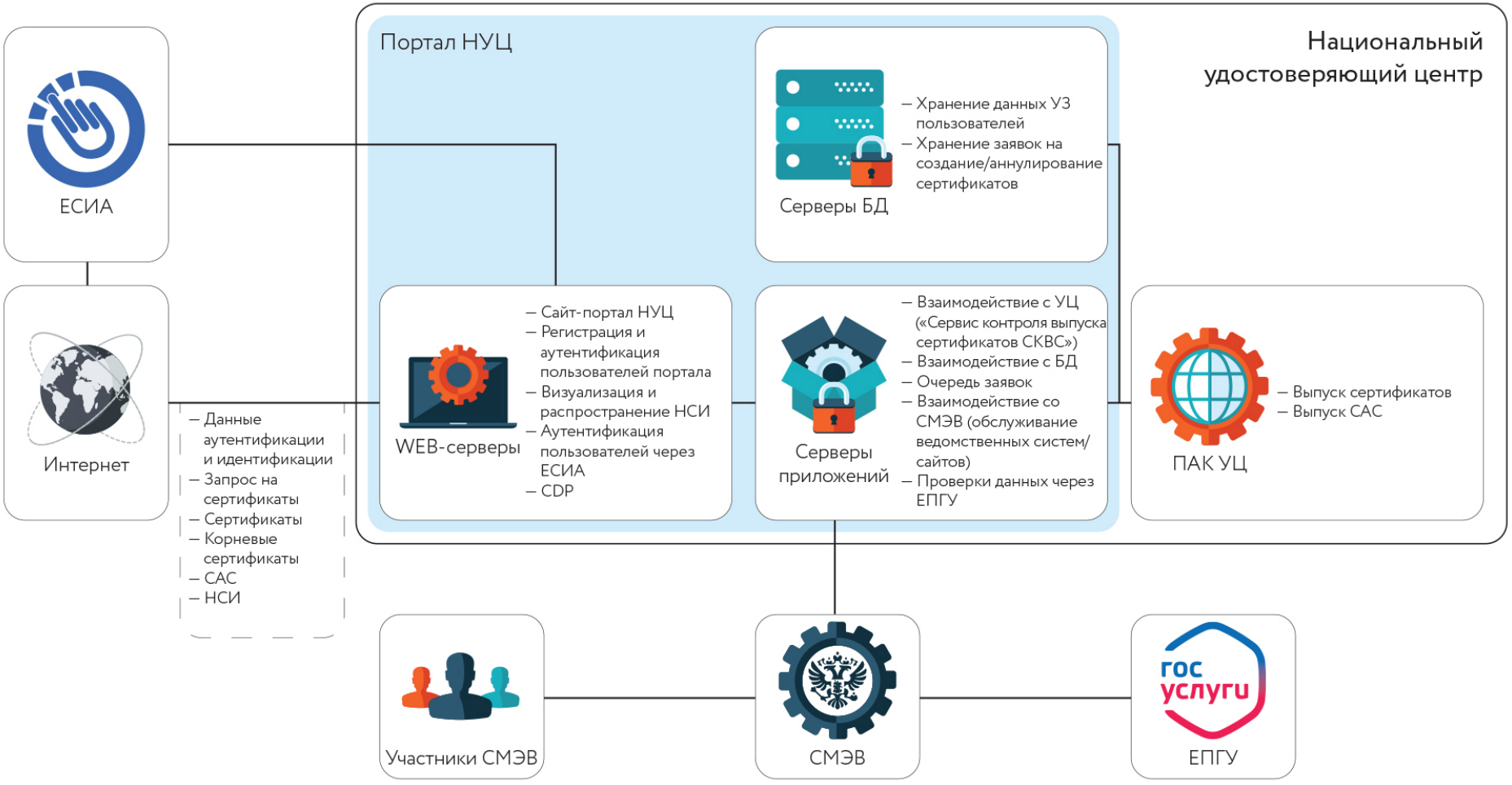
Гражданин

Национальный удостоверяющий центр

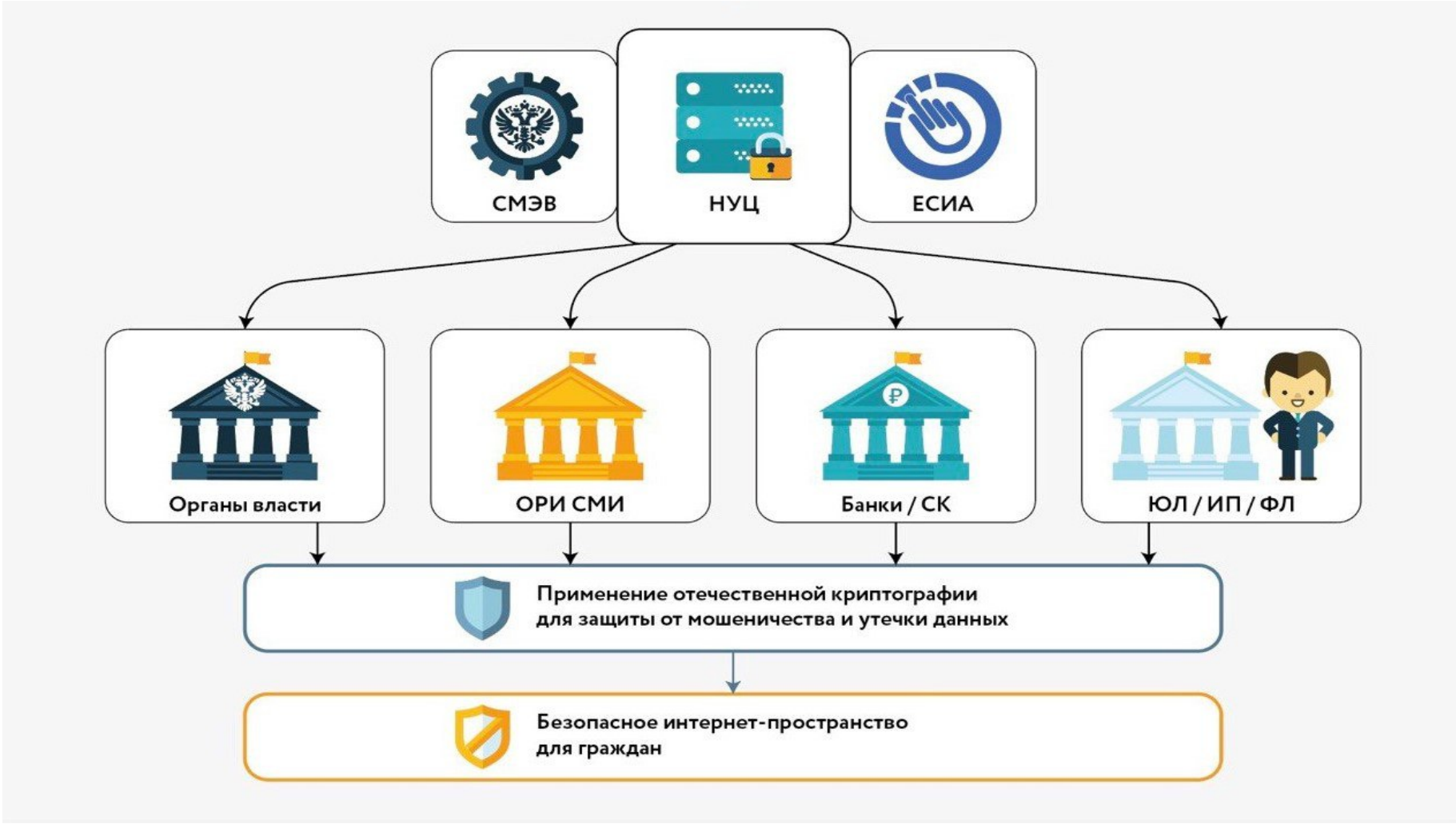
Национальный удостоверяющий центр
Предназначение

- Использование международных протоколов взаимодействия участников сети Интернет на базе отечественной криптографии (TLS-ГОСТ)
- Адаптация общепринятых видов сертификатов для российского сегмента сети Интернет
- Применение надежных способов валидации запросов, в том числе с использованием государственных электронных сервисов
- Адаптация международной практики выдачи TLS-сертификатов для российского сегмента сети Интернет, с учетом состава участников, применяемых средств доступа в сеть и распространения средств отечественной криптографии

Национальный удостоверяющий центр
Архитектура



Национальный удостоверяющий центр
Участники взаимодействия



Национальный удостоверяющий центр
Этапы создания

I этап	II этап	III этап
• Концепция НУЦ • Требования к НУЦ • ТЗ на разработку и внедрение НУЦ • ЧТЗ по безопасности НУЦ • Эскизный проект НУЦ	• Техническое проектирование НУЦ • Разработка СПО НУЦ • Проведение необходимых исследований СПО НУЦ	• Пуско-наладочные работы • Испытания НУЦ • Аттестация НУЦ • Ввод НУЦ в промышленную эксплуатацию

- Разработка и/или доработка нормативных и правовых актов для закрепления роли НУЦ в российском цифровом пространстве

Инфраструктура защищенного электронного взаимодействия граждан и организаций с органами государственной власти и органами местного самоуправления с использованием российских криптографических алгоритмов

Инфраструктура защищенного электронного взаимодействия. Варианты реализации

Разработка типовых технических решений для применения в информационных системах органов государственной власти и органов местного самоуправления

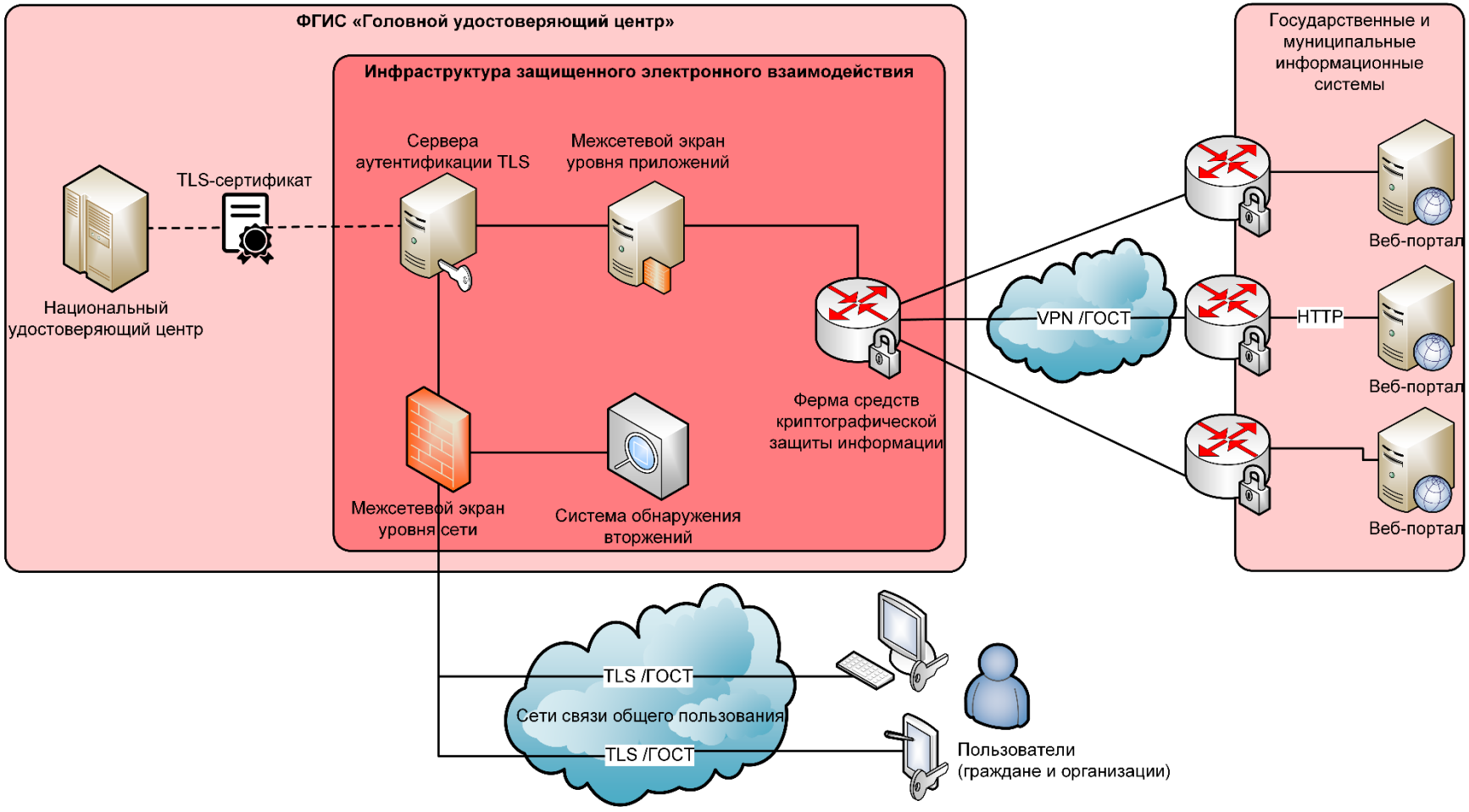
Закупка, внедрение и сопровождение технических решений осуществляется для каждой государственной и муниципальной информационной системы в отдельности.

Централизованная инфраструктура не предусматривается.

Создание инфраструктуры защищенного электронного взаимодействия граждан и организаций с органами государственной власти и органами местного самоуправления

Создается централизованная инфраструктура, доработка отдельных государственных и муниципальных информационных систем не требуется, снижаются затраты на внедрение, сопровождение и проведение мероприятий по информационной безопасности

Архитектурная схема централизованных решений и взаимосвязи с внешними информационными системами



Последняя миля

Гражданин

Последняя миля
Подходы

- использование существующих на рынке решений
- разработка бесплатного государственного решения для граждан
- разработка публичных требований к решениям для граждан

План по переходу