

Обеспечение информационной безопасности инфраструктуры электронного правительства



И.А.Трифаленков, Директор Центра Информационной Безопасности

Инфраструктура электронного правительства – что это

Электронное
правительство

- Новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий (ИКТ) качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов.

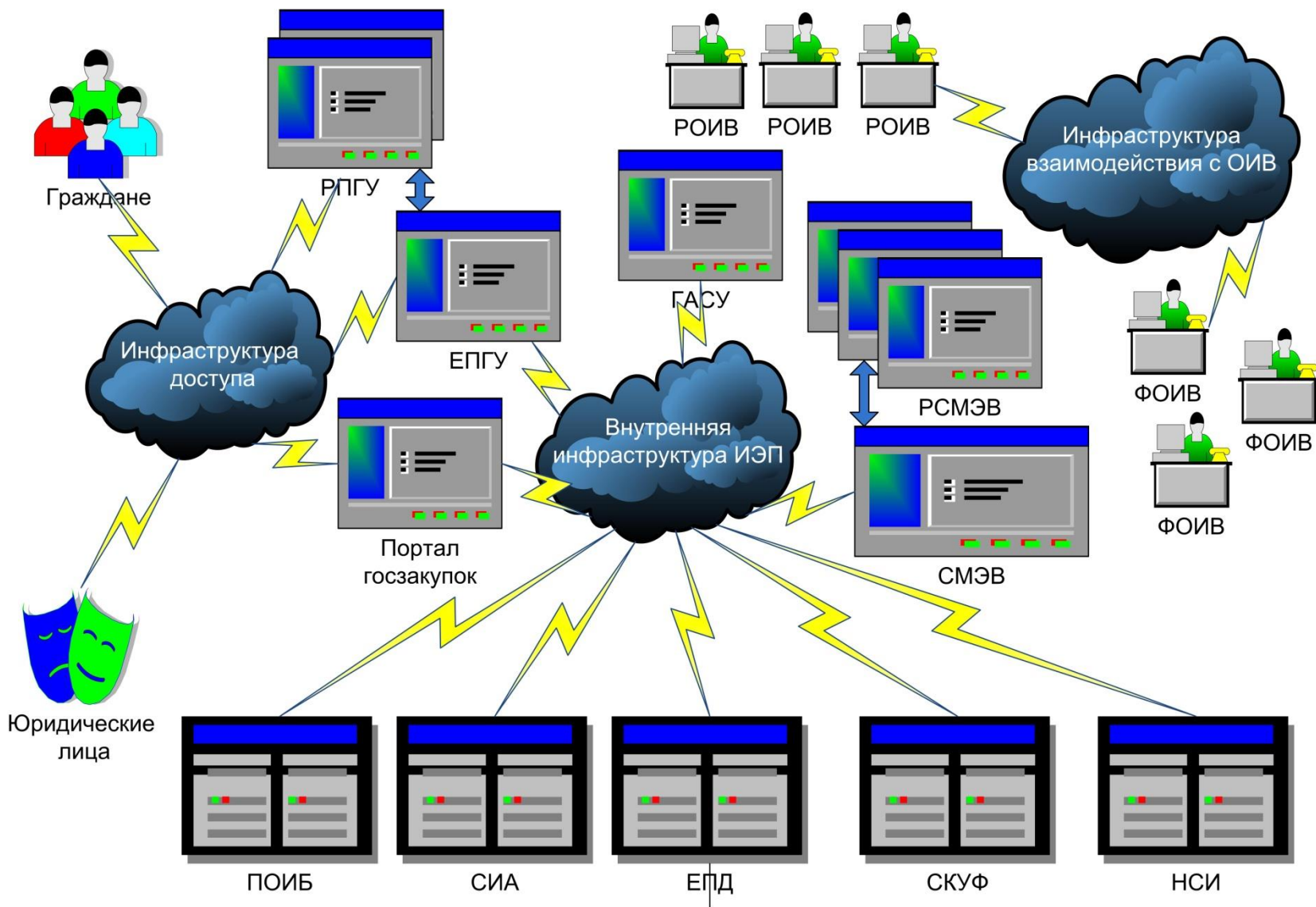
Инфраструктура
электронного
правительства

- Совокупность автоматизированных и телекоммуникационных систем, обеспечивающих поддержку процессов информационного взаимодействия всех субъектов электронного правительства с целью обеспечения необходимого уровня предоставления государственных услуг

АС федеральных и
региональных органов
исполнительной
власти

- Множество автоматизированных и телекоммуникационных систем, обеспечивающих поддержку отдельных процессов деятельности при предоставлении государственных услуг

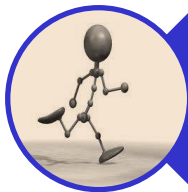
Инфраструктура электронного правительства - состав



Инфраструктура электронного правительства - особенности



Масштаб - проект должен обеспечивать работу сотен систем по всей территории РФ



Динамика – проект реализуется в предельно короткие сроки



Массовость – услуги должны предоставляться всем



Неоднородность – проблемы информационного неравенства и отсутствия стандартизации



Проблемы с нормативным обеспечением

Инфраструктура электронного правительства – технологические вызовы



Недоверенная среда – невозможность
обеспечить ограничения



Множественная идентификация большого
числа субъектов



Сквозные процессы между неоднородными
автоматизированными системами



Виртуализация



Мониторинг защищенности и управление
событиями ИБ

Инфраструктура электронного правительства – принципы создания

Развитие
нормативной базы
как часть проекта

Сочетание
отечественных и
международных
стандартов

Применение
промышленных
решений

Процессно-
ориентированный
подход

Широкая
кооперация
производителей и
исполнителей работ

Инфраструктура электронного правительства – принципы создания

Развитие
нормативной базы
как часть проекта

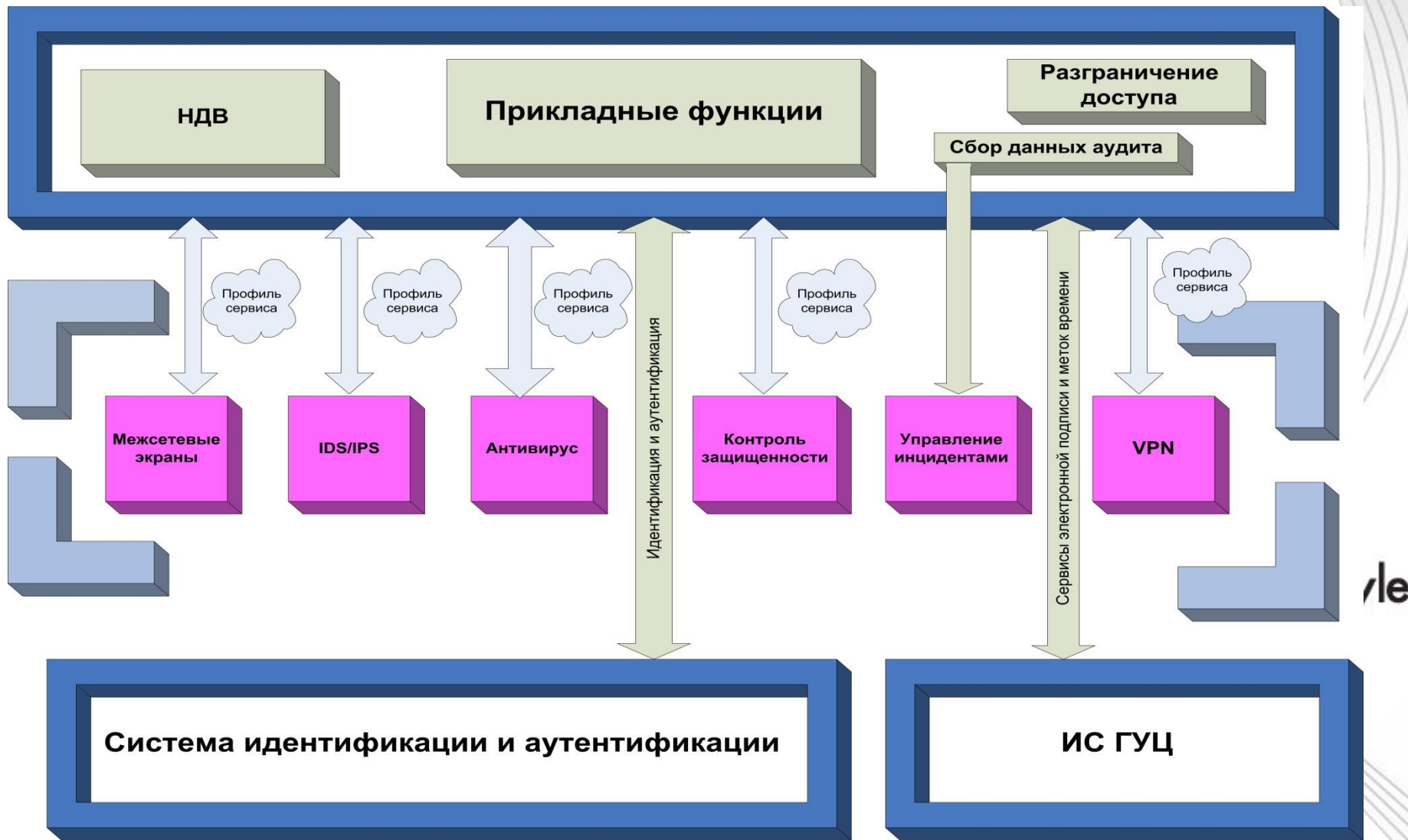
Сочетание
отечественных и
международных
стандартов

Применение
промышленных
решений

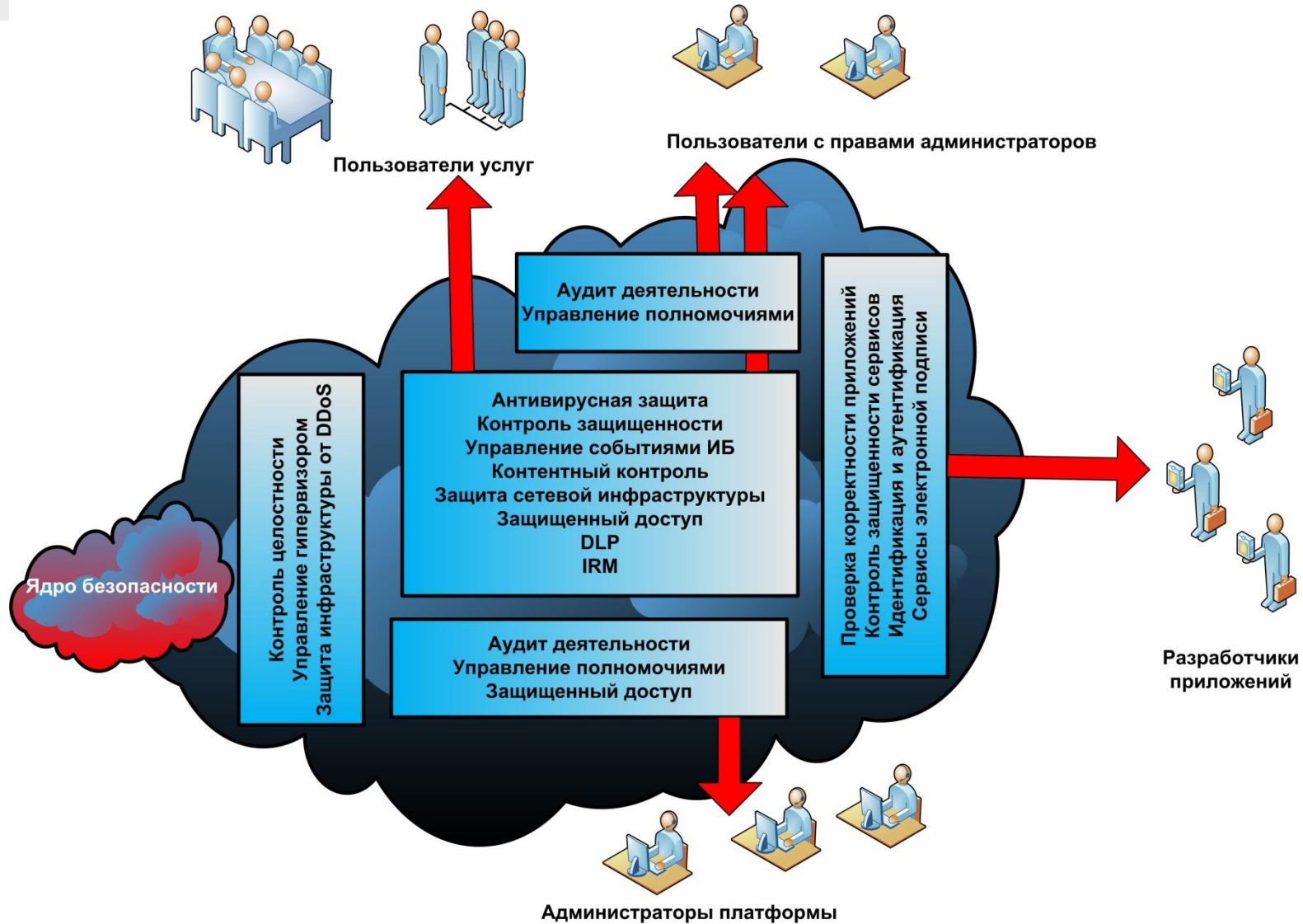
Процессно-
ориентированный
подход

Широкая
кооперация
производителей и
исполнителей работ

Инфраструктура электронного правительства – система информационной безопасности



Адресаты услуг инфраструктуры ИБ



Что нужно от приложений с точки зрения ИБ

Интеграция с внешним сервисом идентификации и аутентификации

Интеграция с внешними криптографическими сервисами

Проверка соответствия на отсутствие НДВ

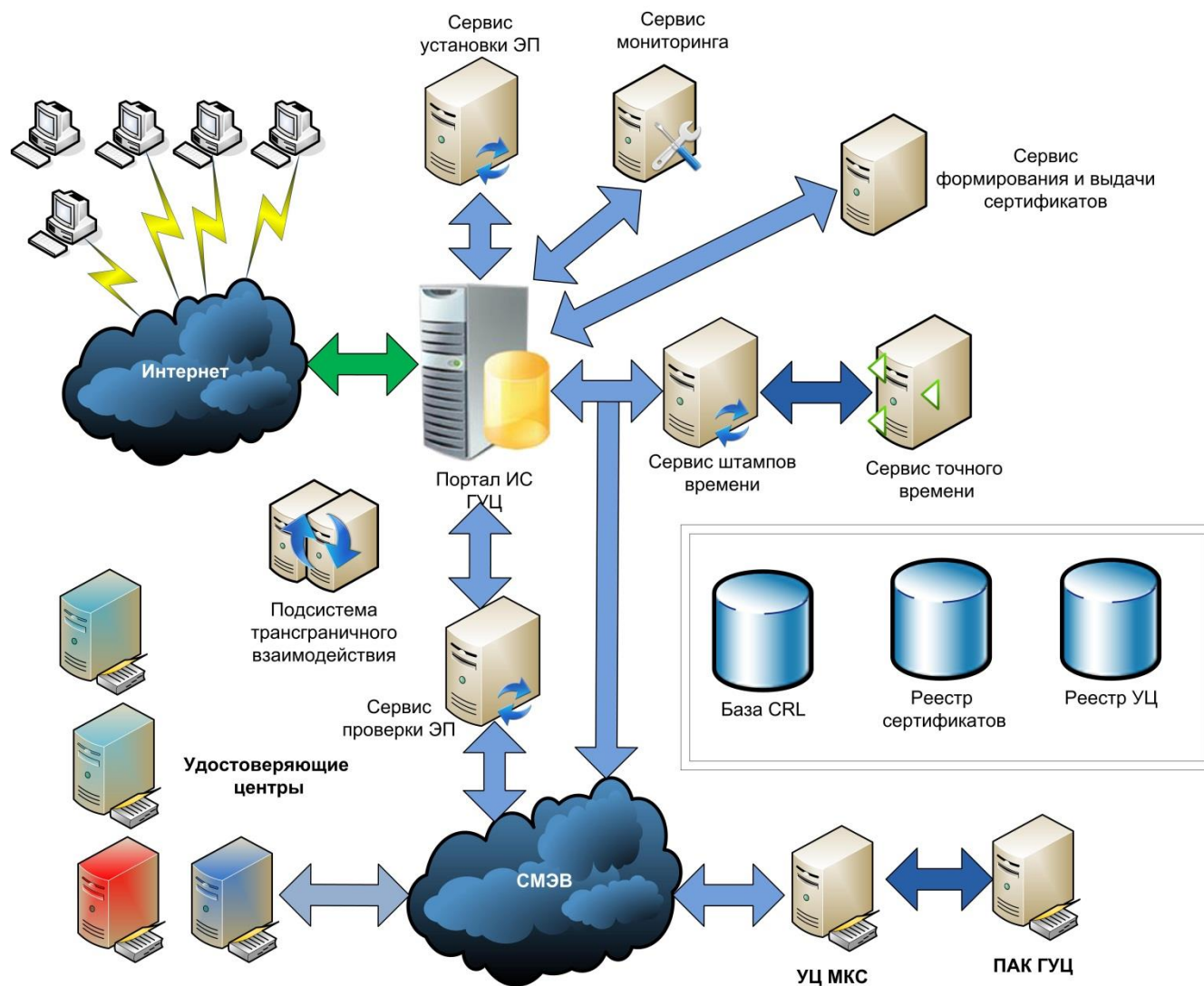
Профиль сервисов ИБ

Проверка на отсутствие потенциально опасных структур кода

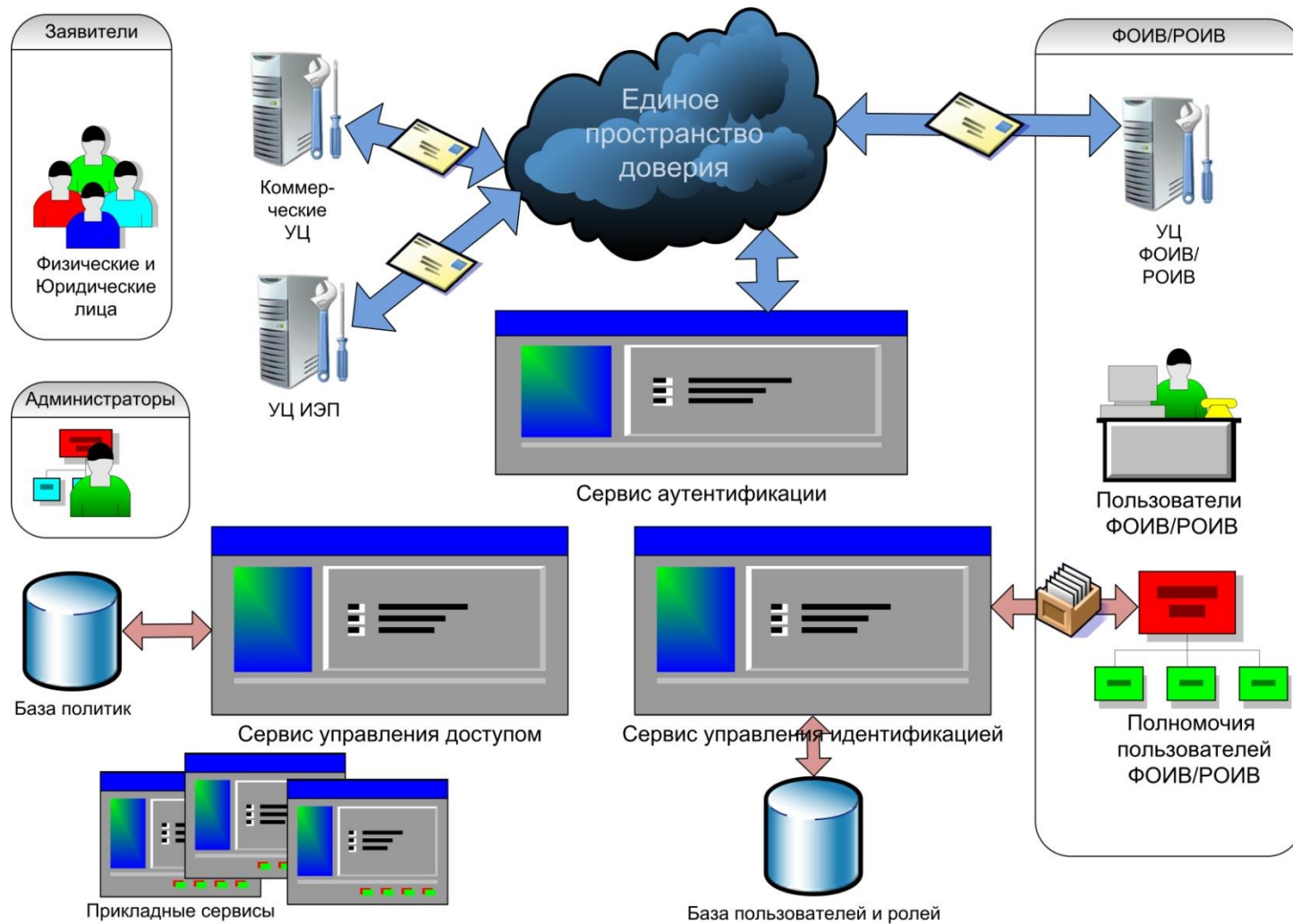
Проверка на отсутствие уязвимостей и нарушений требований ИБ

Профиль сервиса иммитации работы приложения

ИС ГУЦ – управление электронной подписью



ЕСИА – управление идентификацией и аутентификацией



Организация доступа пользователей



Компьютер

- Обеспечение взаимной идентификации и аутентификации пользователей с ПГУ
- Обеспечение ЭП запросов к ПГУ
- Обеспечение конфиденциальности передаваемых ПД
- Обеспечение контроля пользовательской среды
- Определение политик доступа в соответствии с типом услуги и способом доступа к ПГУ
- Аудит действий пользователей ПГУ



Мобильное устройство

- Аутентификация пользователя – по одноразовому паролю, сервера – средствами GSM/3G
- ЭП на стороне оператора (HSM)
- Конфиденциальность данных обеспечивается средствами GSM/3G и VPN между мобильным оператором и ГПУ
- Контроль пользовательской среды невозможен
- Контроль прав доступа осуществляется средствами мобильного оператора и средствами ИЭП (СИА и ПОИБ)



Инфомат

- Аутентификация пользователя по паролю, сервера – по VPN-ключу
- ЭП на внешнем устройстве (токене, карте)
- Конфиденциальность данных обеспечивается VPN туннелем
- Контроль пользовательской среды оператором инфоматов
- Контроль прав доступа и аудит осуществляется средствами ИЭП (СИА и ПОИБ)

Организация работ по созданию ИБ

Создание кооперации исполнителей и производителей в соответствии с их специализацией

Выделение проекта обеспечения базовых сервисов ИБ

Использование систем проверки соответствия (сертификации и аттестации) с учетом требований международных стандартов

Использование механизмов аутсорсинга при эксплуатации систем включая ПОИБ

Разработка способов компенсации остаточных рисков (страхование)

**Благодарим за внимание
и приглашаем к сотрудничеству!**

R-Style

123022 г. Москва, ул. Рочдельская д. 15 к. 16а

Т. +7 (495) 514-14-10

www.R-Style.com



 **R-Style**

