# Защита информации в учреждениях здравоохранения

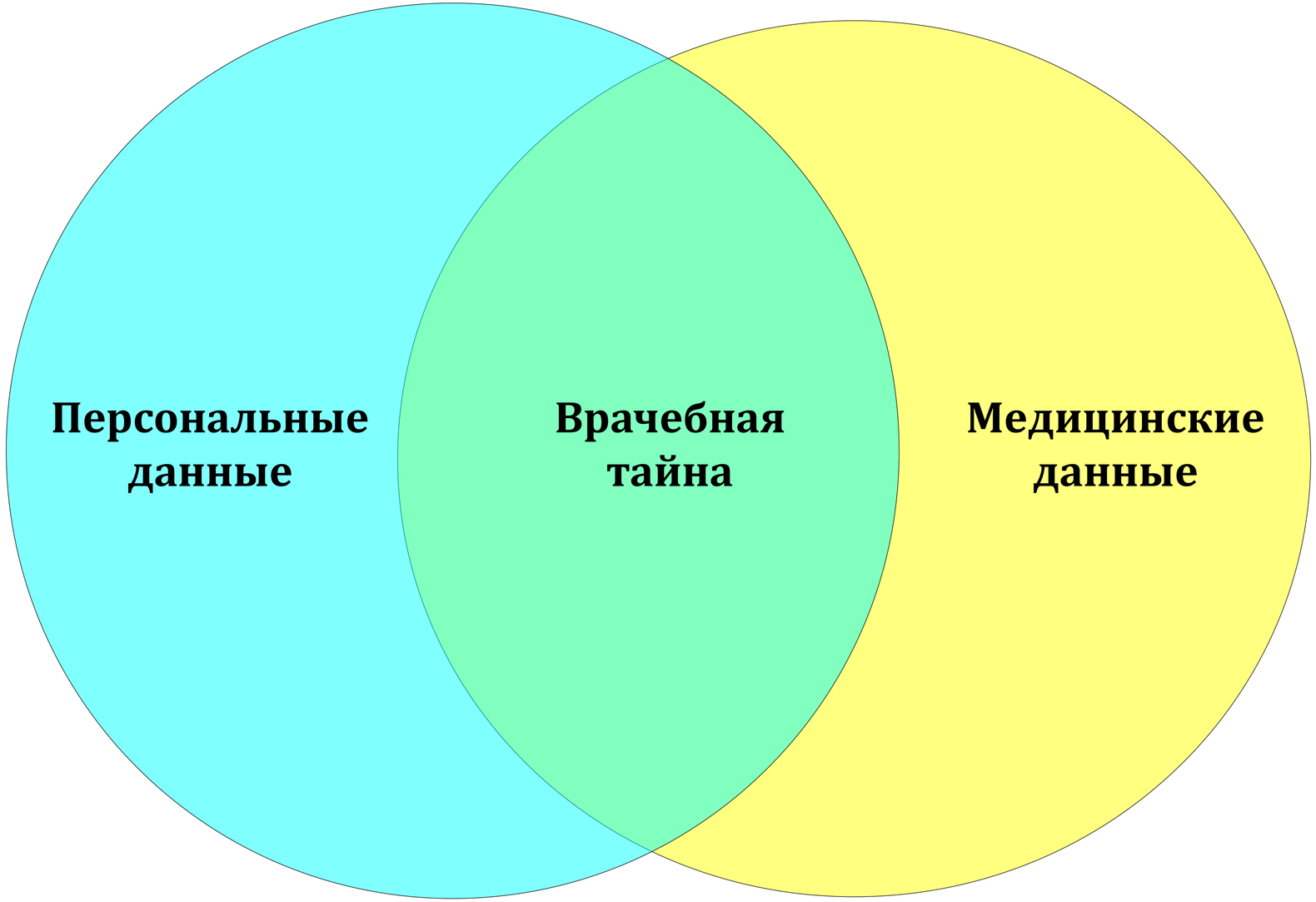
**Демьян Раменский**
руководитель направления
«Информационная безопасность»

8 (800) 707-04-12
sale@corpsoft24.ru
corpsoft24.ru

информация ограниченного доступа

**УП 188** конфиденциальная информация

профессиональная тайна




**323-ФЗ**

Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

corpsoft 24

# Обзор законодательства

1

Федеральный закон N 149-ФЗ - Об информационных технологиях и защите информации

Федеральный закон N 98-ФЗ - О коммерческой тайне

Указ Президента N 188 - Перечень сведений конфиденциального характера

2

**Федеральный закон N 152-ФЗ - О персональных данных**

**Постановление Правительства N 1119 - Требования к защите ИСПДн**

**Приказ ФСТЭК N 21 - Состав и содержание орг. и технических мер**

**Приказ ФСБ N 378 - Состава и содержания мер при использовании СКЗИ**

Приказ РКН N 18 - Требования к согласию на распространение ПДн

Постановление Правительства N 687 - Обработка ПДн без автоматизации

Постановление Правительства N 512 - требования к биометрическим ПДн

3

Приказ Минздрава N 911н - Требования к ИС в сфере здравоохранения

Приказ ФСТЭК N 17 - Требований к защите  ГИС

Федеральный закон N 187-ФЗ - О безопасности КИИ

corpsoft 24

# Требования Постановления Правительства № 1119

| Тип ИСПДн | Субъекты ПДн - только сотрудники оператора | Кол-во субъектов ПДн | Тип актуальных угроз | | |
|---|---|---|---|---|---|
| | | | Тип 1 | Тип 2 | Тип 3 |
| ИСПДн-С | Нет | Более 100 000 | УЗ 1 | УЗ 1 | УЗ 2 |
| | | Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | Да | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-Б | Нет | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | | Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | Да | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-И | Нет | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | | Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| | Да | Любое | УЗ 1 | УЗ 3 | УЗ 4 |
| ИСПДн-0 | Нет | Более 100 000 | УЗ 2 | УЗ 2 | УЗ 4 |
| | | Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| | Да | Любое | УЗ 2 | УЗ 3 | УЗ 4 |

corpsoft 24

# Обзор законодательства

Федеральный закон от 21 ноября 2011 г. N **323-ФЗ**
"Об основах охраны здоровья граждан в Российской Федерации"
!Врачебная тайна

Приказ Министерства здравоохранения РФ от 24 декабря 2018 г. **N 911н** “
Требования к ГИС в сфере здравоохранения, МИС медицинских организаций и фармацевтических организаций
+сертифицированные СЗИ

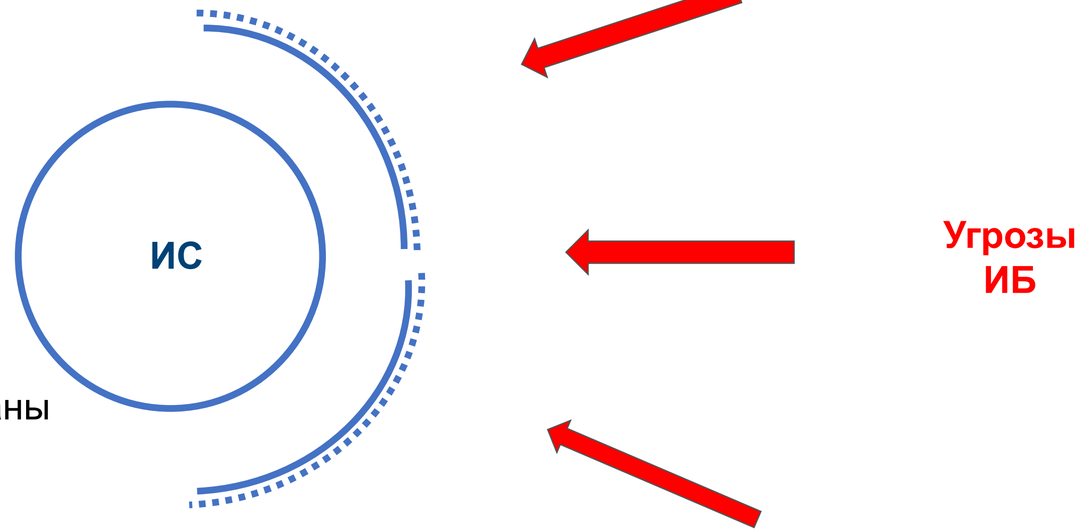
Постановление Правительства РФ от 12 апреля 2018 г. N **447**
Правила взаимодействия иных информационных систем, с информационными системами в сфере здравоохранения (ЕГИСЗ)
+аттестат (пп1119 и 17 приказ ФСТЭК)
+защита канаов связи

# Общие принципы построения систем защиты информации

## Система защиты персональных данных

- Приказы
- Положения
- Регламенты
- Инструкции
- и т.д.

Организационные меры




- Межсетевые экраны
- Криптосредства
- Детекторы атак
- Сканеры уязвимостей
- и т.д

Технические меры

corpsoft 24

# Построение систем защиты ПДн с использованием облачных услуг

corpsoft 24

# Построение систем защиты с использованием облачных услуг

## Комплексная услуга «Хостинг ИСПДн»

| Модуль №1 | Модуль №2 | Модуль №3 |
|---|---|---|
| **Аттестованная облачная инфраструктура** | **Сертифицированные СЗИ, СКЗИ** | **Документация, проектирование, аттестация** |
| • Центр обработки данных<br>• Сеть передачи данных<br>• Серверное оборудование<br>• Система хранения данных<br>• Среда виртуализации | • Средства межсетевого экранирования<br>• СКЗИ для защиты каналов связи<br>• Сертифицированные операционные системы<br>• Средства защиты от НСД<br>• СКЗИ для защиты баз данных, дисков и файлов<br>• Средства антивирусной защиты<br>• Средства анализа защищенности и поиска уязвимостей<br>• Средства обнаружения вторжений<br>• Средства резервного копирования | • Аудит процессов обработки ПДн<br>• Аудит ИСПДн<br>• Разработка модели угроз и модели нарушителя<br>• Определение требуемого уровня защищенности<br>• Проектирование системы защиты персональных данных<br>• Разработка ЛНА и ОРД<br>• Разработка технического паспорта ИСПДн<br>• Оценка эффективности принимаемых мер безопасности<br>• Аттестация ИСПДн |

# Разработка ЛНА и ОРД

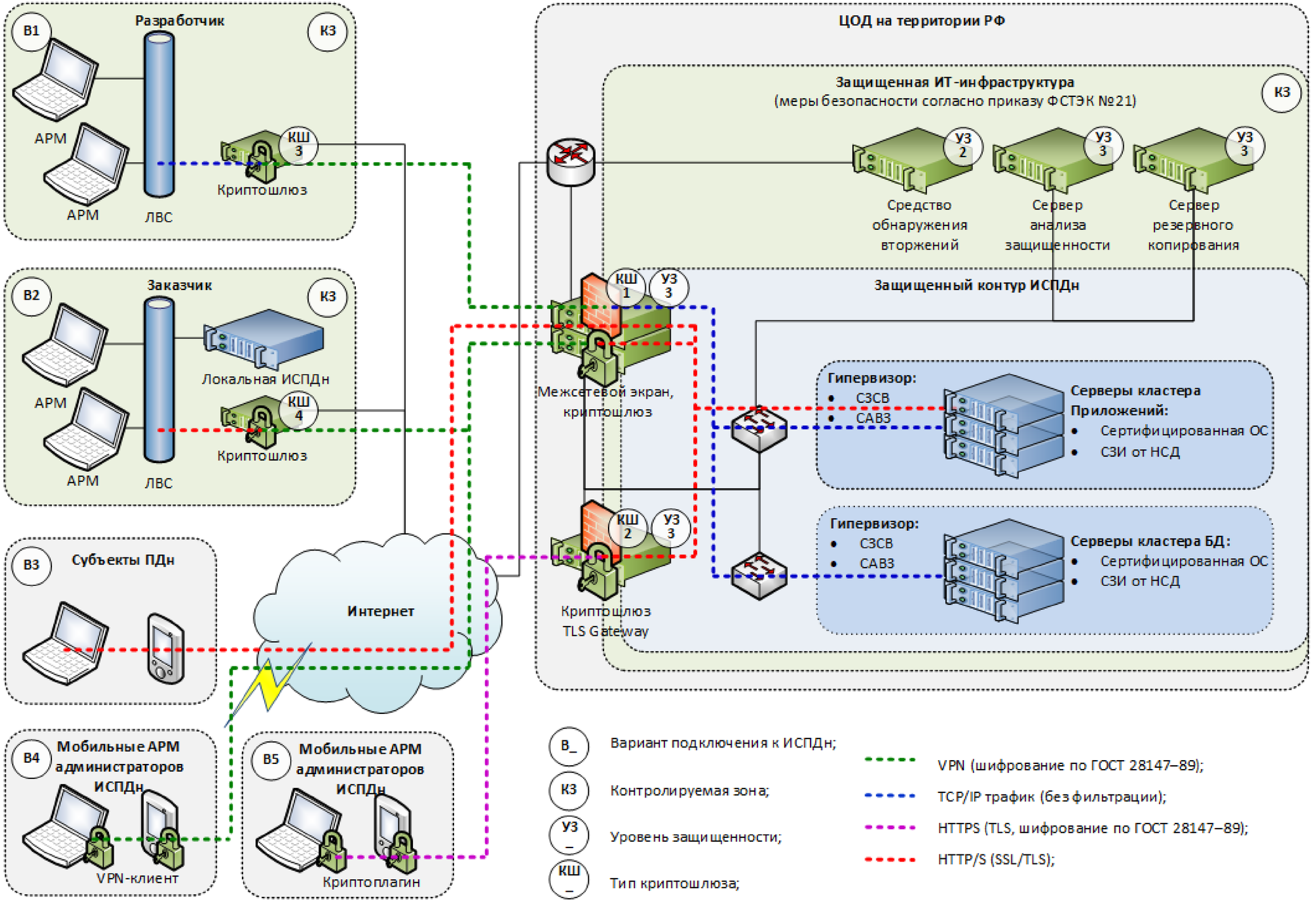
**Иерархия организационно-распорядительной документации**


**Положения** – документы, определяющие общие подходы и требования по обработке и защите ПДн оператором.

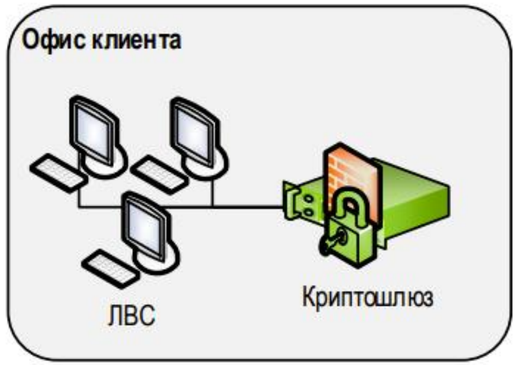
**Регламенты** – документы, устанавливающие порядок проведения мероприятий по обработке и защите ПДн.

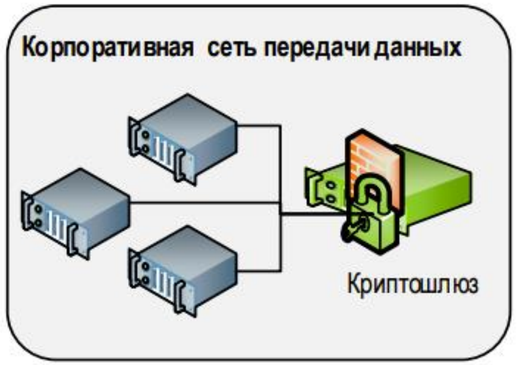
**Инструкции** – документы, содержащие детализированные правила и указания по осуществлению определенных операций по обработке и защите ПДн.

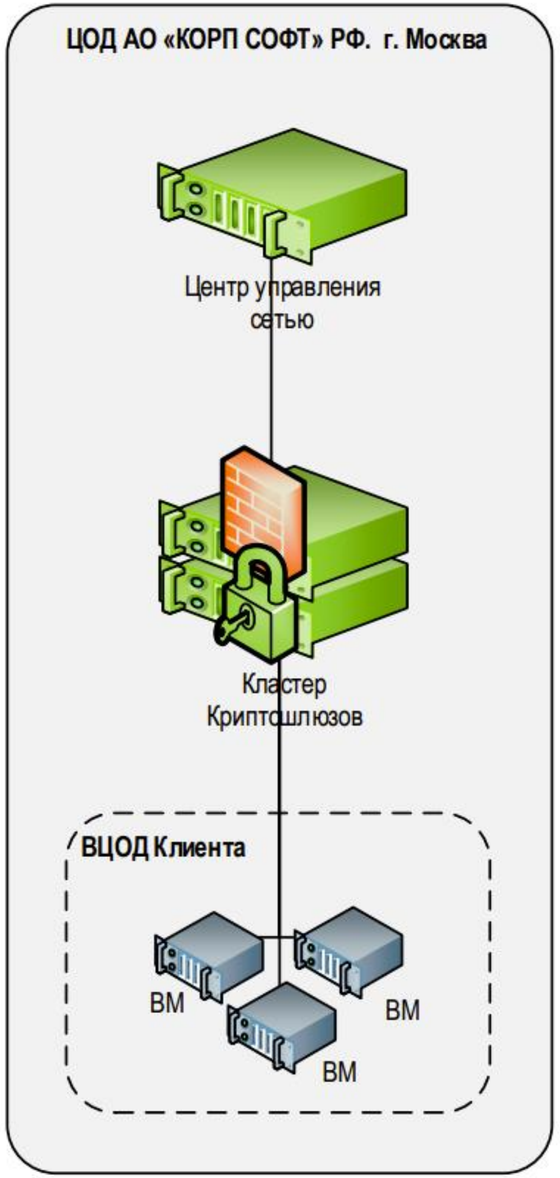
**Планово-учетные документы** – документы, содержащие записи о мероприятиях и результатах деятельности по обработке и защите ПДн.

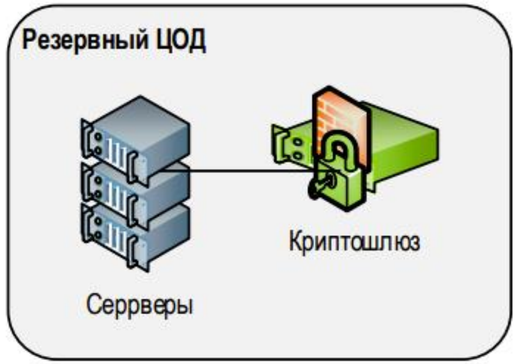

В1
Разработчик
КЗ
АРМ
АРМ
ЛВС
КШ 3
Криптошлюз
В2
Заказчик
КЗ
АРМ
АРМ
ЛВС
Локальная ИСПДн
КШ 4
Криптошлюз
В3
Субъекты ПДн
Интернет
В4
Мобильные АРМ администраторов ИСПДн
VPN-клиент
В5
Мобильные АРМ администраторов ИСПДн
Криптоплагин
ЦОД на территории РФ
Защищенная ИТ-инфраструктура
(меры безопасности согласно приказу ФСТЭК №21)
КЗ
УЗ 2
Средство обнаружения вторжений
УЗ 3
Сервер анализа защищенности
УЗ 3
Сервер резервного копирования
Защищенный контур ИСПДн
КШ 1
УЗ 3
Межсетевой экран, криптошлюз
КШ 2
УЗ 3
Криптошлюз TLS Gateway
Гипервизор:
СЗСВ
САВЗ
Серверы кластера Приложений:
Сертифицированная ОС
СЗИ от НСД
Гипервизор:
СЗСВ
САВЗ
Серверы кластера БД:
Сертифицированная ОС
СЗИ от НСД
В_ Вариант подключения к ИСПДн;
КЗ Контролируемая зона;
УЗ _ Уровень защищенности;
КШ _ Тип криптошлюза;
VPN (шифрование по ГОСТ 28147–89);
TCP/IP трафик (без фильтрации);
HTTPS (TLS, шифрование по ГОСТ 28147–89);
HTTP/S (SSL/TLS);

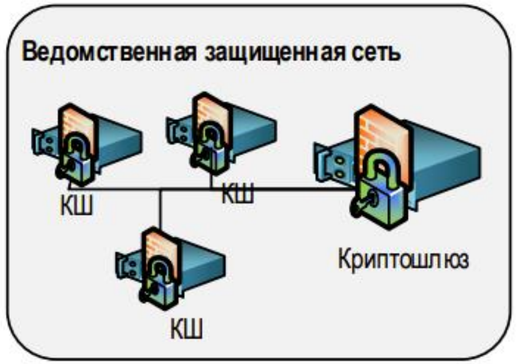
# СКЗИ для защиты каналов связи – ГОСТ VPN

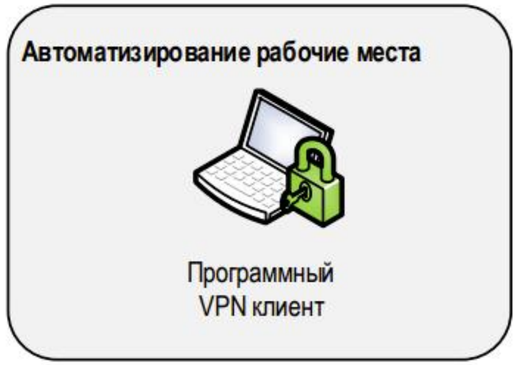


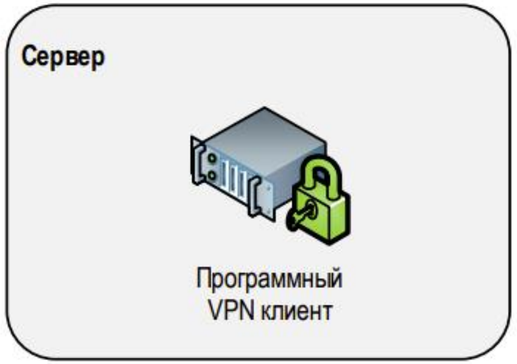




infotecs

ViPNet Client

ViPNet Coordinator

КОД безопасности

АПКШ Континент

Континент АР

corpsoft 24

# Сравнительный анализ подходов к реализации СЗПДн

| **Критерии** | Сами | Интегратор | Облако |
|---|---|---|---|
| **Время** | **3** | **2** | **1** |
| **Деньги** | **2** | **3** | **1** |
| **Качество** | **2** | **1** | **1** |

# Требования к поставщикам услуг

## Лицензии и сертификаты


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

ЛИЦЕНЗИЯ

№ 143462 от "22" сентября 2016 г.

На оказание

*телематических услуг связи*

Настоящая лицензия предоставлена

*Акционерному обществу*

*"Корп Софт"*

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН, ОГРНИП)

*1117746256110*

Идентификационный номер налогоплательщика (ИНН)

*7743813810*

Лицензия Роскомнадзора

России на оказание телематических

услуг связи


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

ЛИЦЕНЗИЯ

№ 119385 от "10" апреля 2014 г.

На оказание

*услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации*

Настоящая лицензия предоставлена

*Закрытому акционерному обществу*

*"Корп Софт"*

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН, ОГРНИП)

*1117746256110*

Идентификационный номер налогоплательщика (ИНН)

*7743813810*

Лицензия Роскомнадзора

России на оказание услуг по

передаче данных


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

ЛИЦЕНЗИЯ

№ 119384 от "10" апреля 2014 г.

На оказание

*услуг связи по предоставлению каналов связи*

Настоящая лицензия предоставлена

*Закрытому акционерному обществу*

*"Корп Софт"*

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН, ОГРНИП)

*1117746256110*

Идентификационный номер налогоплательщика (ИНН)

*7743813810*

Лицензия Роскомнадзора

на услуги связи по предоставлению

каналов связи


ФЕДЕРАЛЬНАЯ СЛУЖБА по техническому и экспортному контролю

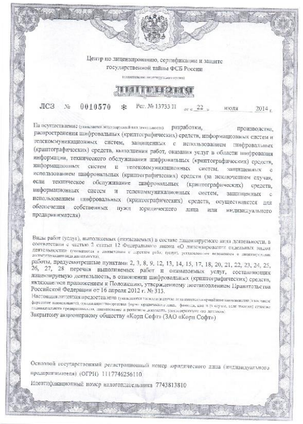
ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Лицензия ФСТЭК России

на деятельность по технической защите конфиденциальной

информации


ЛИЦЕНЗИЯ

Лицензия ФСБ России

на разработку, производство и распространение шифровальных

средств


СИСТЕМА СЕРТИФИКАЦИИ ГОСТ Р

РЕГИСТР СИСТЕМ КАЧЕСТВА

СЕРТИФИКАТ СООТВЕТСТВИЯ

Сертификат соответствия

системы менеджмента качества

требованиям ГОСТ

ISO 9001-2011

# Ответы на вопросы

corpsoft 24

## Спасибо за внимание!

??????

t.me/corpsoft24

vk.com/corpsoft_24