Современные подходы к защите персональных данных в медицинских организациях

Сабанов А.Г.,
ЗАО «Аладдин Р.Д.»

Москва, 07.06.2012г.

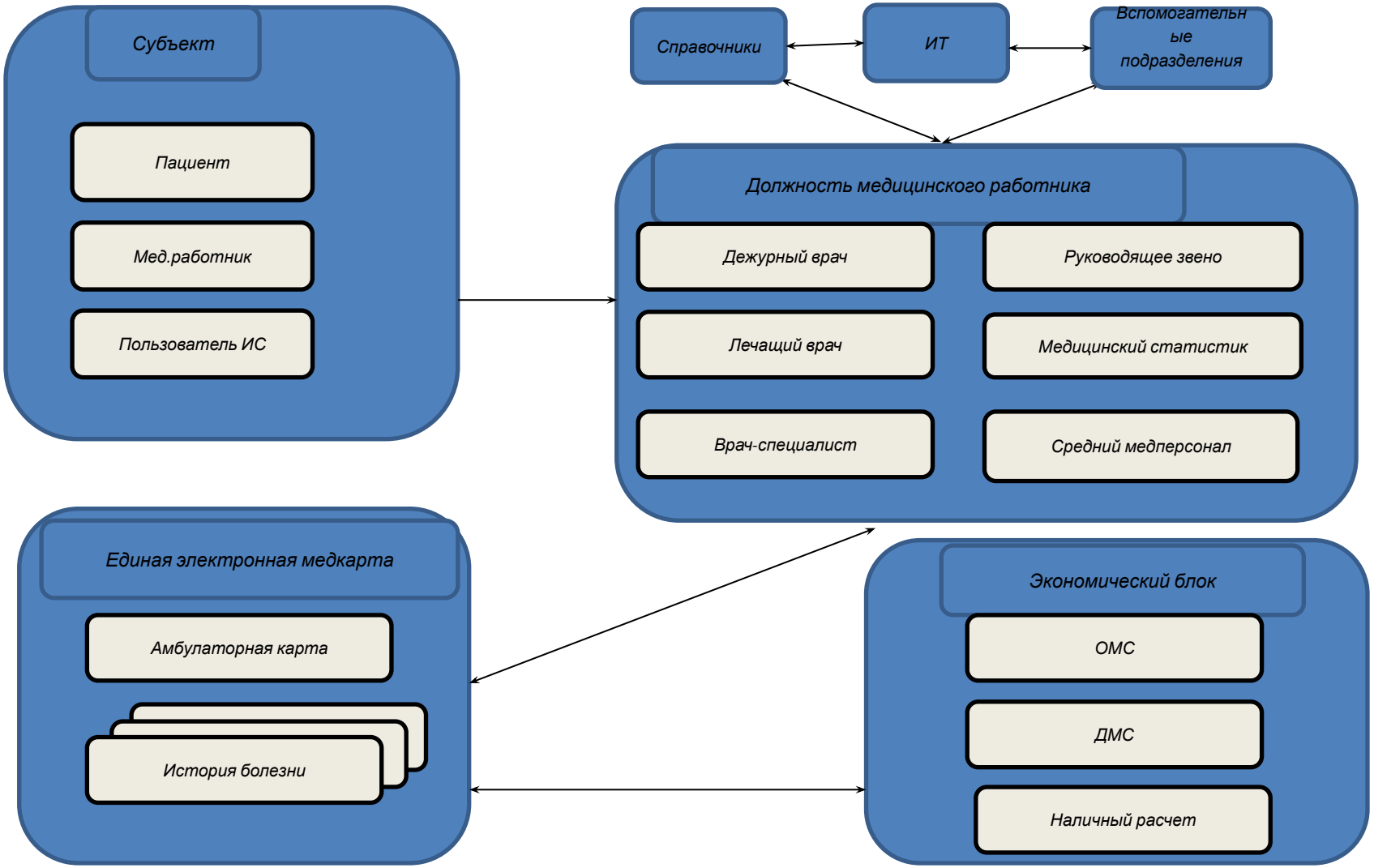
Что такое персональных данные

- **Персональные данные(ПДн)** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); с персональными данными связаны следующие понятия:
- **оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- **автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники;
- **распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Действия с персональными данными

- **блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **уничтожение персональных данных** — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных** (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **трансграничная передача персональных данных** — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

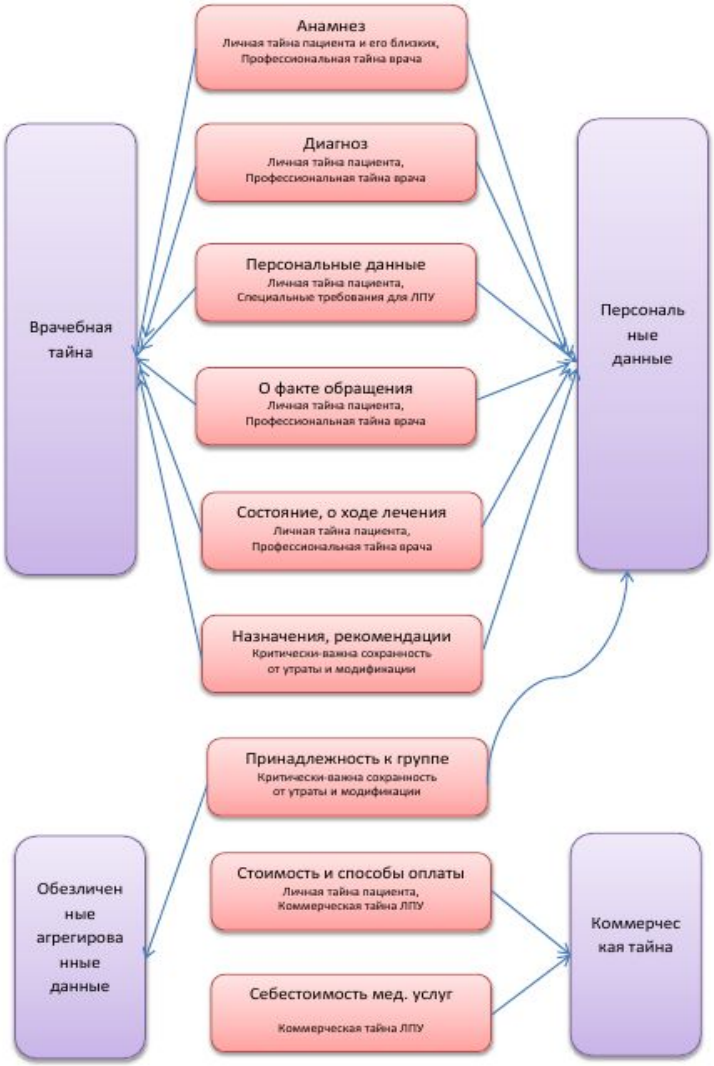
Пример простейшей МИС



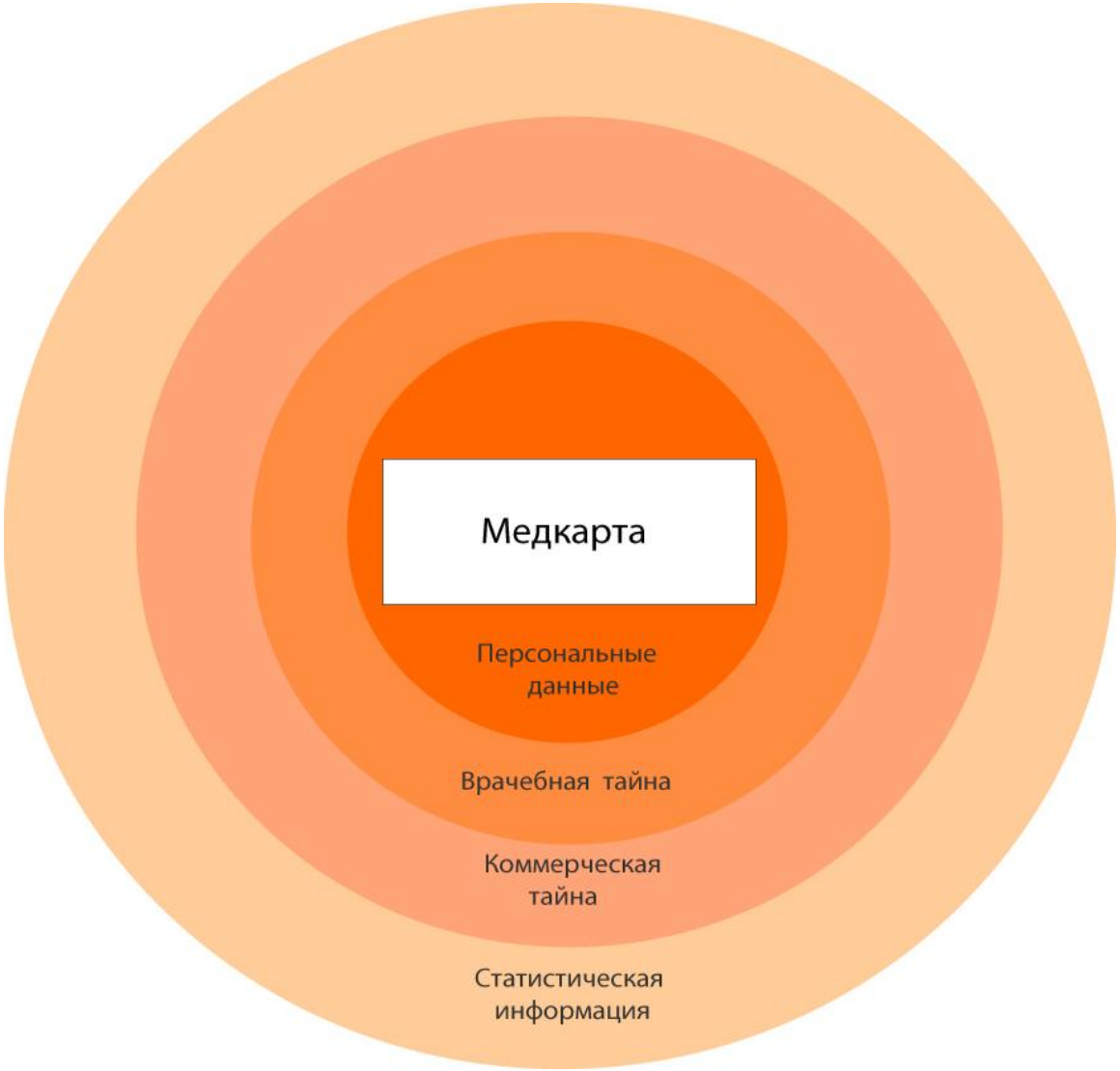
Информация пациента. Виды тайн.

Личная тайна – охраняется основным законом Конституцией (ст.23,24).
Врачебная (в Семейном кодексе – медицинская) тайна – Основы законодательства Российской Федерации об охране здоровья граждан (ст.61, 35).
Персональные данные. С одной стороны, это – специфические требования №152-ФЗ, с другой стороны Закон дает только инструмент защиты прав и свобод человека и гражданина, в правовом отношении это – **личная** тайна, **доверенная** (т.е. переданная) врачу и охраняемая Основным законом РФ (Конституцией).

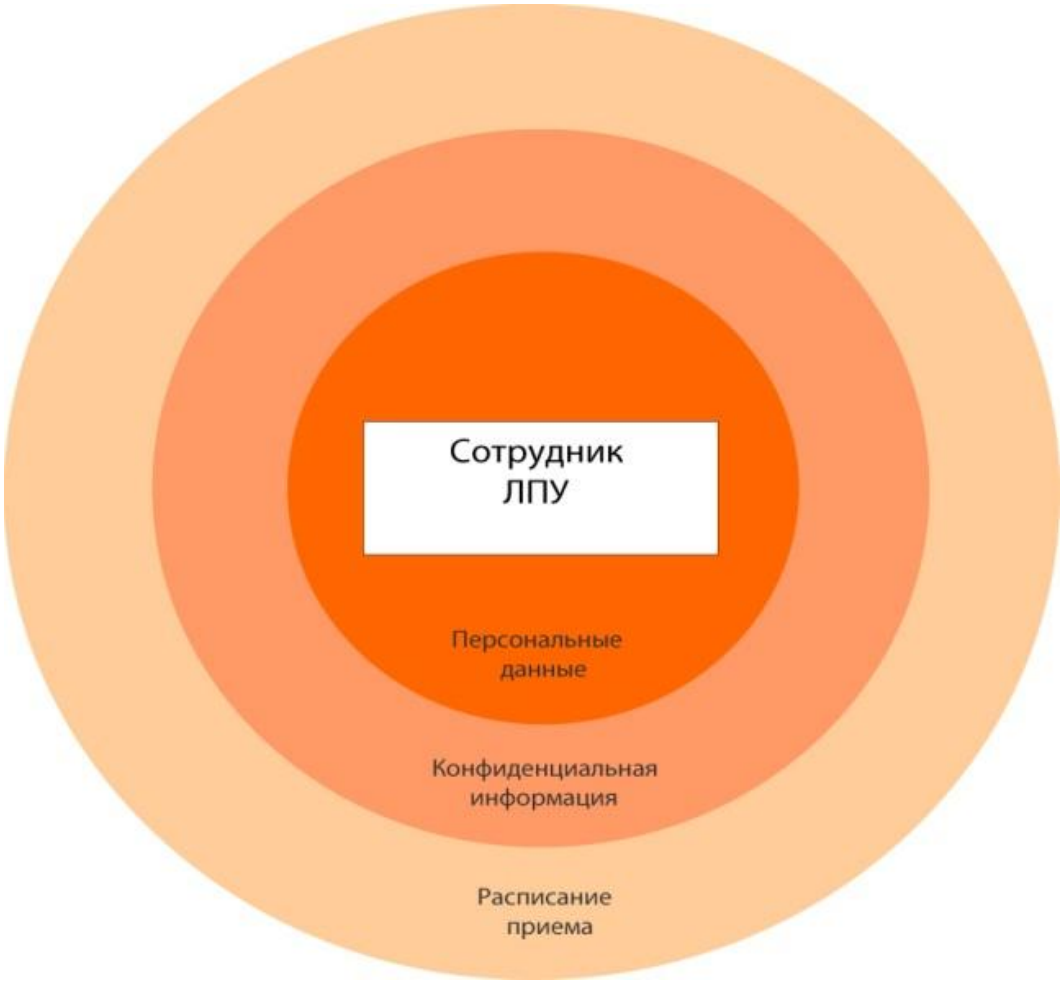
Виды тайн, обрабатываемых в МИС



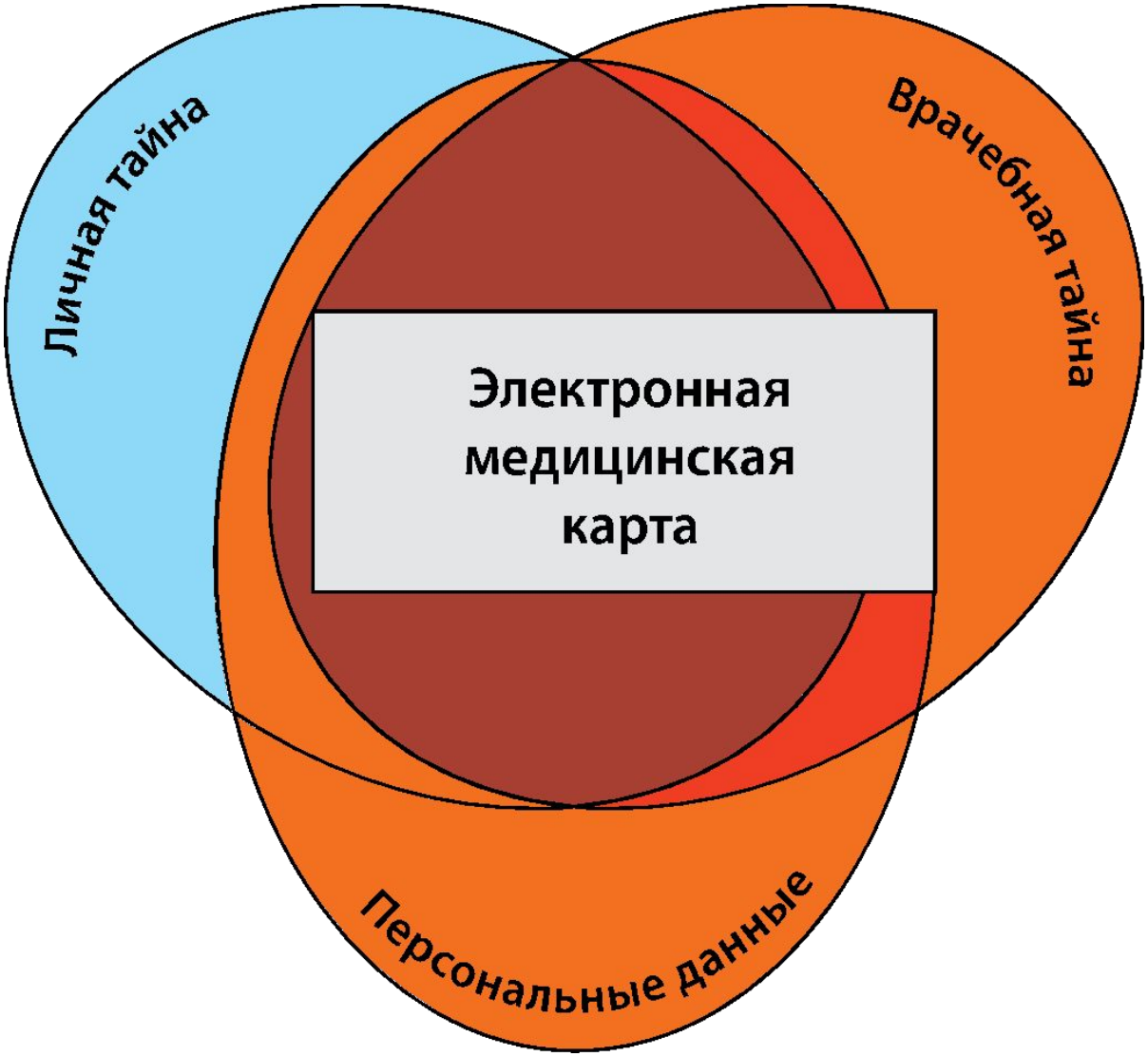
Информация ограниченного доступа. Пациент



Информация о сотруднике ЛПУ



Соотношение требований по защите



Задачи обеспечения безопасности

- Ограничить циркуляцию информации в открытом виде только точками шифрования и расшифрования;
- Использовать надежные решения по управлению ключами, соответствующие национальным стандартам;
- Использовать длины ключей и криптографические алгоритмы, соответствующие национальным стандартам;
- Защитить устройства, выполняющие криптографические операции, от физической и логической компрометации.

Информация □□ Данные

Администратор безопасности

Администратор СУБД

Управление Ключами и шифрованием

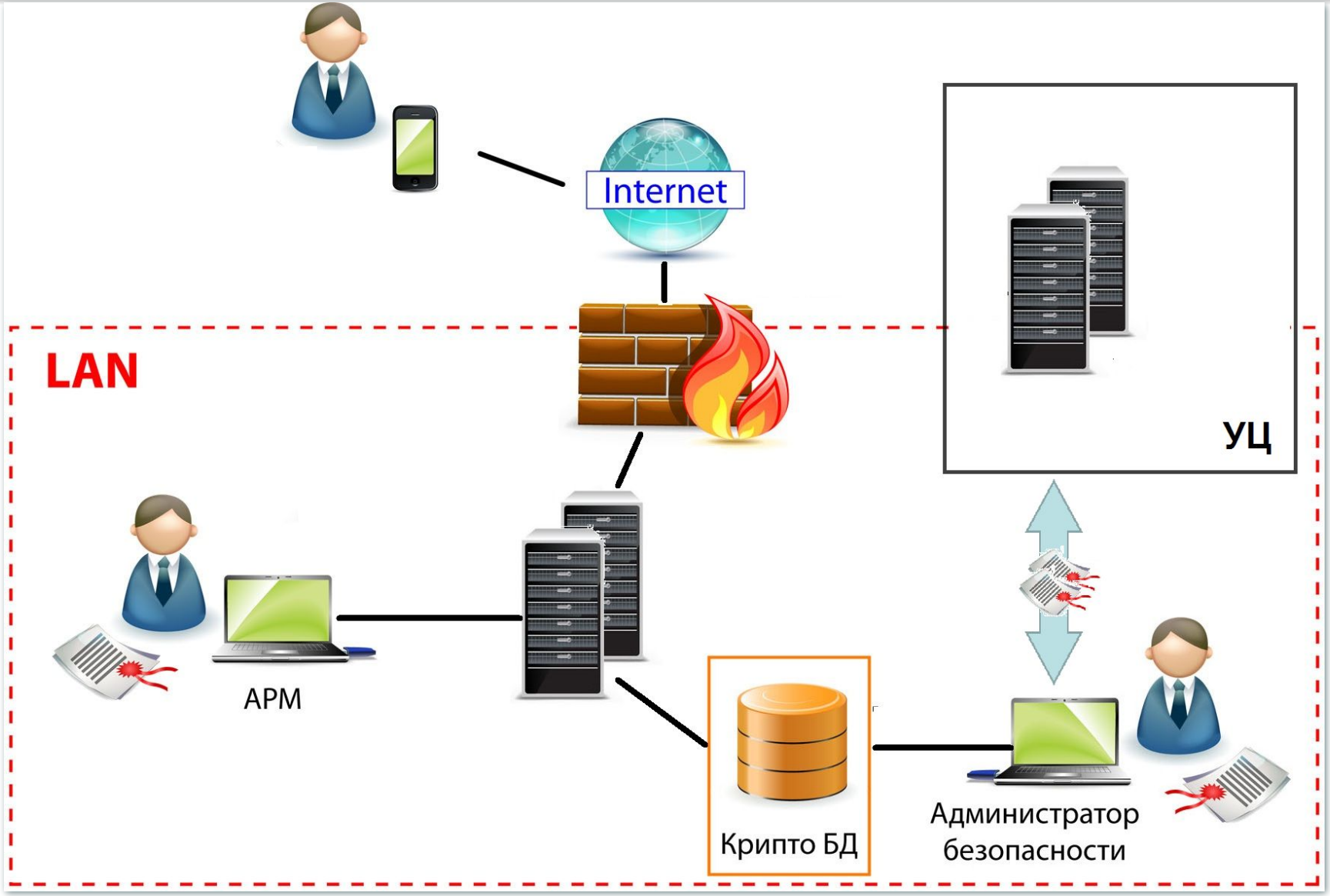
Управление данными

Потребитель информации

Шифрование/электронная подпись

Хранилище данных

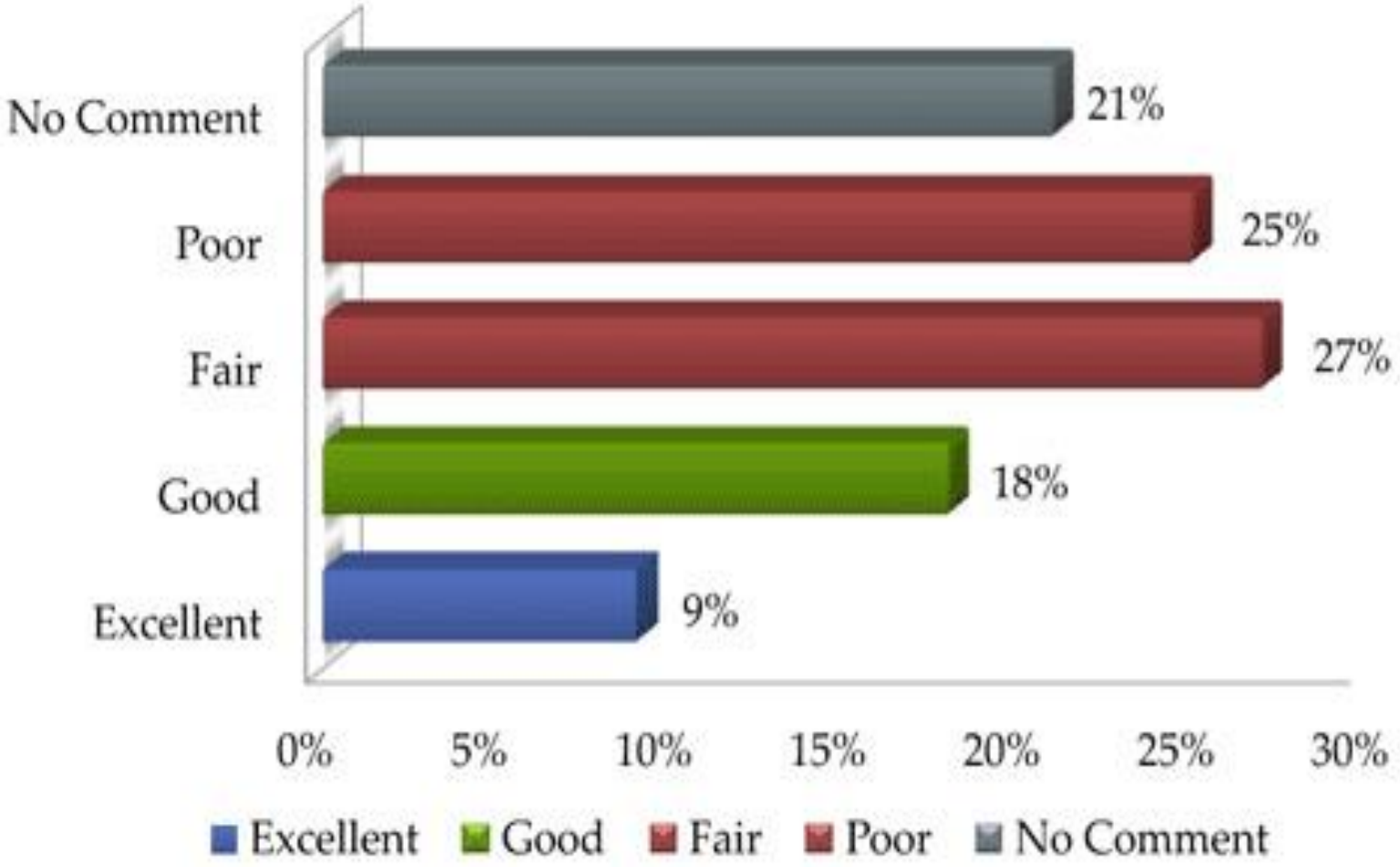
Защита ПДн в МИС



Облака: возможности и проблемы

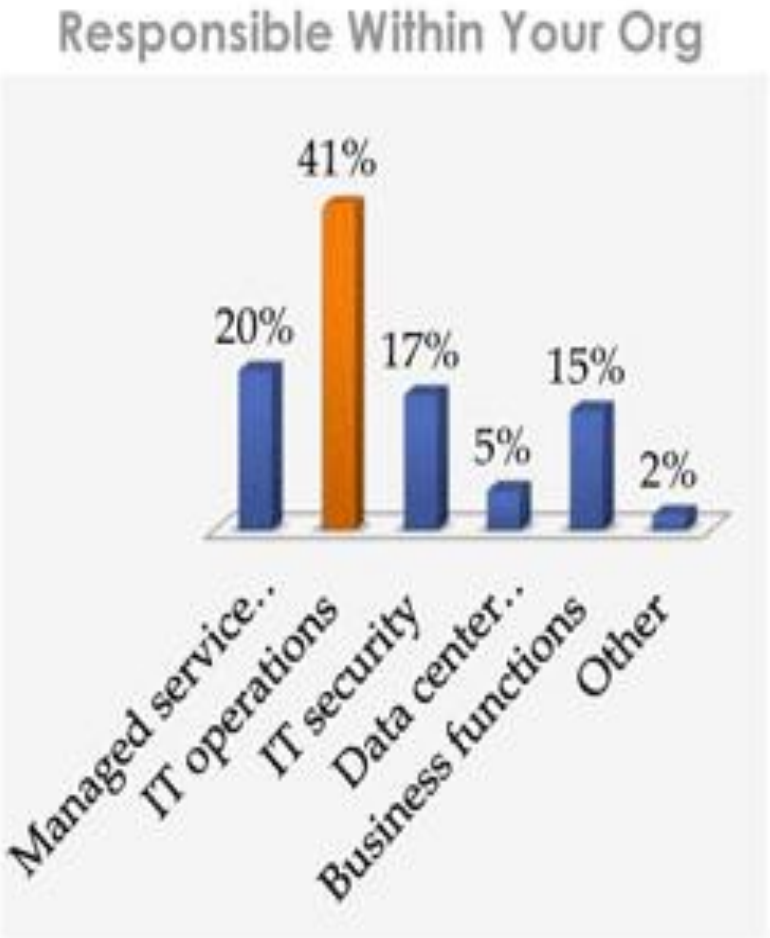
- Всю информацию контролирует и хранит провайдер
  - Сняты ограничения по размещению информации
  - Экономия за счет масштаба
  - Привлекательность для преступников и конкурентов
- Изменения в ИТ процессах
  - Физическая безопасность обеспечивается провайдером
  - Провайдер юридически независим
- Проблемы хранения персональных данных и иной важной информации
- Проблемы проведения расследования киберпреступлений

Безопасность «облачных вычислений»



Источник: http://www.cnews.ru/reviews/free/security2011/articles/articles3.shtml

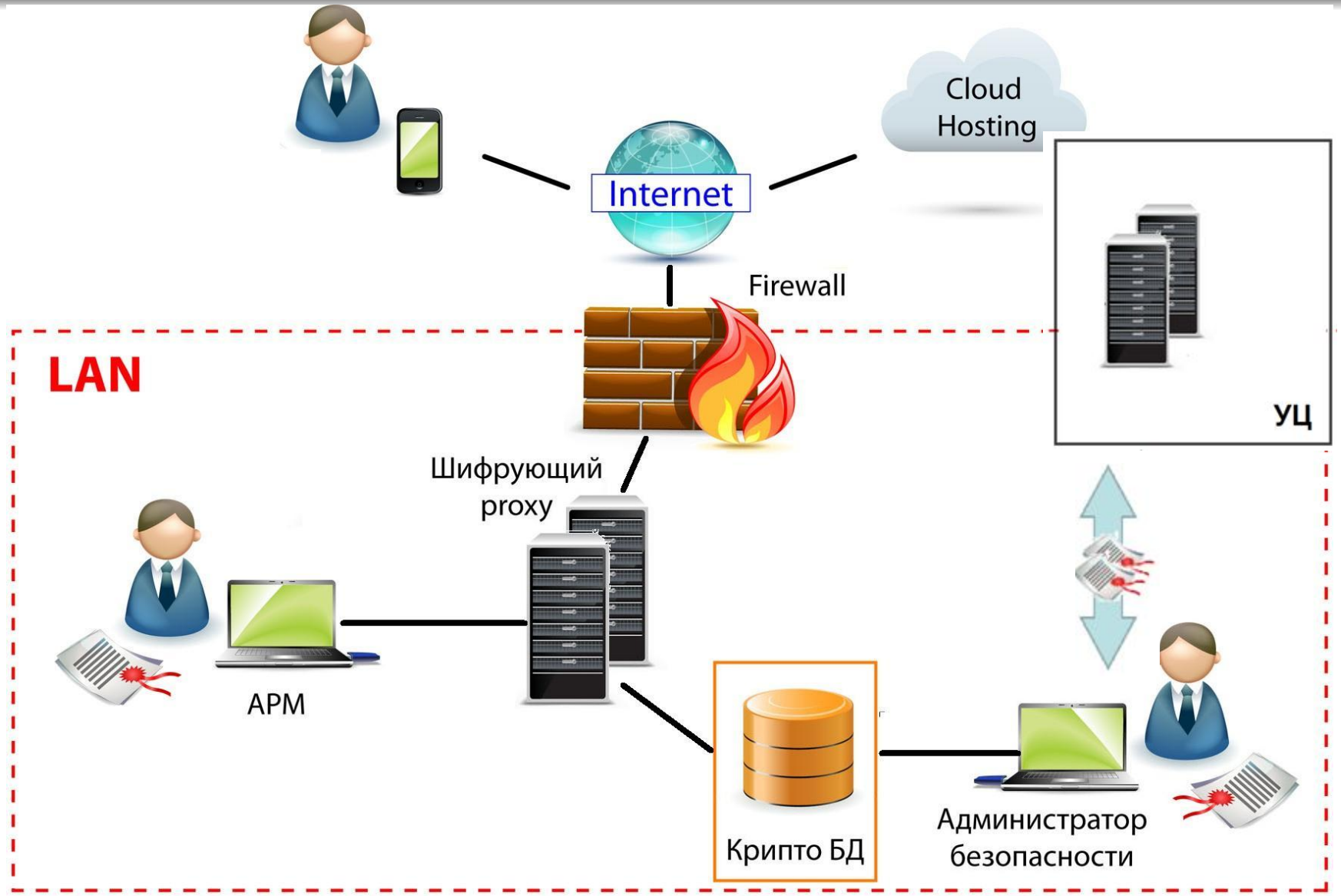
Кто отвечает за безопасность «облака»



Источник: http://www.cnews.ru/reviews/free/security2011/articles/articles3.shtml

Какие облака могут быть построены?

Метод защиты ПДн в «Облаках»



Выполнение требований регуляторов…

- Обезличивание всей необходимой информации
- Применение сертифицированных СЗИ
- Управление информационной безопасностью в контролируемой зоне

… и реальные результаты защиты

- Обезличенная информация неинтересна для киберпреступников и конкурентов на стороне хостера
- Расследование инцидентов НСД – полностью под контролем Обладателя ПДн
- Обработка персональных данных и иной важной информации – только под контролем Обладателя ПДн

Крипто БД: сертифицированное СКЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-1569*** от "***06***" ***ноября*** 201***0*** г.

Действителен до "***06***" ***ноября*** 201***3*** г.

Выдан закрытому акционерному обществу «АЛАДДИН Р.Д.».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Крипто БД Версия 1.0»** (исполнения 1 и 2) в составе согласно формуляру 643.46538383.50 1430 005-01 30 01

соответствует требованиям ГОСТ 28147-89 и требованиям ФСБ России к СКЗИ класса КС1 (для исполнения 1) и КС2 (для исполнения 2) и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование и вычисление имитовставки пользовательских данных) информации, не содержащей сведений, составляющих государственную тайну, хранящейся в таблицах баз данных под управлением СУБД Oracle.

Проблемы защиты персональных данных в организациях здравоохранения

1. Нормативная база изменяется

- За последние 2 года изменилось/появилось 6 законов
  - 149-ФЗ «Об информации, информационных технологиях и защите информации» - ред. 06.04.2011,
  - 210-ФЗ «Об организации предоставления гос.услуг» - 27.07.2010,
  - 99-ФЗ «О лицензировании…» - ред.04.05.2010,
  - 152-ФЗ «О персональных данных» - ред.25.07.2011,
  - 326-ФЗ «Об обязательном медицинском страховании»- 29.11.2010,
  - 323-ФЗ «Об основах охраны здоровья…» - 21.11.2011г.
- Опубликовано несколько Постановлений Правительства (№ 313 от 16.04.2012г. Об утверждении Положения о лицензировании…, №79 от 03.02.12 О лицензировании…, №171 от 03.03.12 по разработке и пр-ву СЗ конф.инф)
- Изменились многие понятия (ст.18, 19, 84, 92,… 323-ФЗ «Об основах охраны здоровья…»

Проблемы

2. Методические материалы и некоторые вспомогательные материалы, подготовленные Минздравсоцразвития РФ за период 2009-2011гг, устаревают и требуют постоянного обновления. Ощущаются явные проблемы с организацией процесса защиты персональных данных в центре и в регионах.

3. Проблемы финансирования. Бюджеты в регионы выделяются, защищаются в Минздраве, а насколько эффективно они реально используются – очень большой вопрос.

4. Пока остаются неясными перспективы развития информатизации отрасли и построения систем защиты информации.

Проблемы (продолжение)

5. Продолжается кадровый голод и неясности по использованию специалистов по защите информации в организациях здравоохранения.

6. Проблемы реальной, а не «бумажной», защищенности Пдн. Насколько реально защищаются ПДн пациентов и медицинского персонала?

7. Проблемы интеграции МИС и систем защиты. Интероперабельность, стандартизация

8. Один из нерешенных вопросов для пациентов. Как будет организован доступ к электронной медицинской карте?

9. Один из нерешенных вопросов для всех граждан. Самые развитые виды МИС - медицинские системы, разработанные для отчетности и управления. Пока на рынке нет МИС для удобства процесса лечения пациентов.

Спасибо за внимание!

a.sabanov@aladdin-rd.ru