



Все лучшее  
в медицине!



Since 1990



THE SWISS  
LEADING  
HOSPITALS  
Best in class



Система  
менеджмента  
качества  
ISO 9001:2008



# Можно ли быть уверенным в безопасности персональных данных?

## Клиника «Медицина»

Можно ли быть уверенным в  
безопасности персональных данных?

**НЕТ**



Но к этому нужно стремиться





Информация – ценный ресурс

ДА

Информацию нужно защищать

ДА

Безопасности не бывает слишком много

ДА

Давайте потратим деньги на безопасность

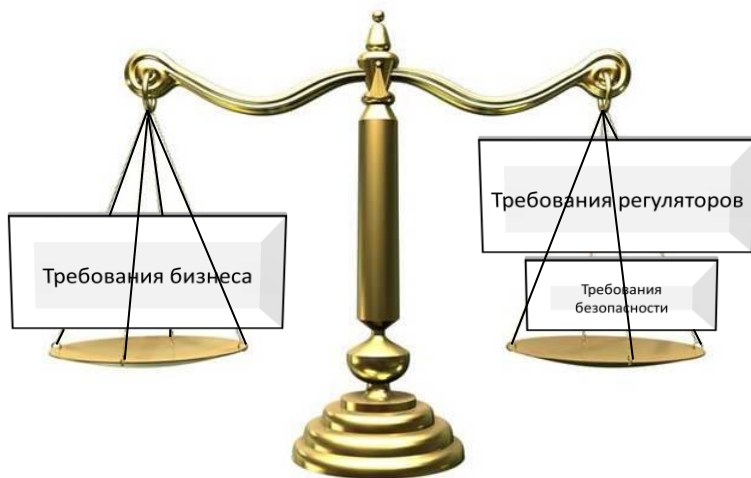
???

А может нас вообще никогда не проверят?

А вдруг проверка ничего плохого не найдет?

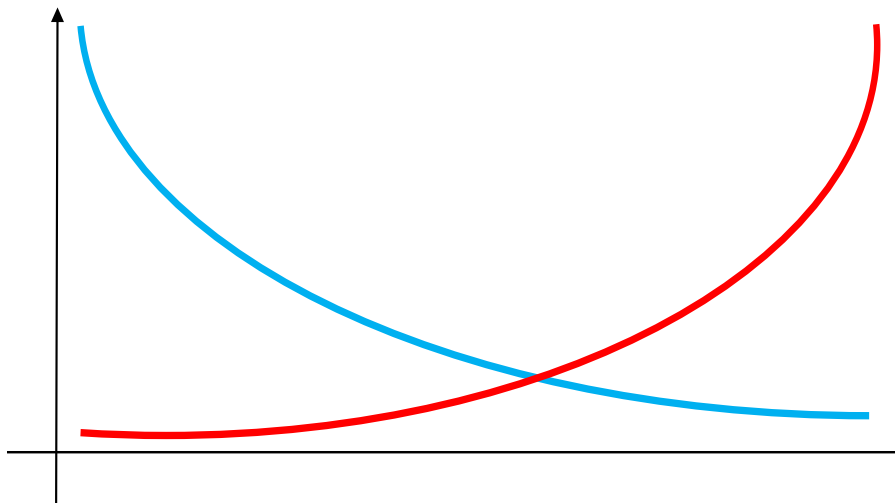
А мы с комиссией договоримся

Штраф и прочие последствия обойдутся гораздо  
дешевле внедрения системы ИБ



## Баланс требований безопасности и бизнеса

## Вопросы стоимости



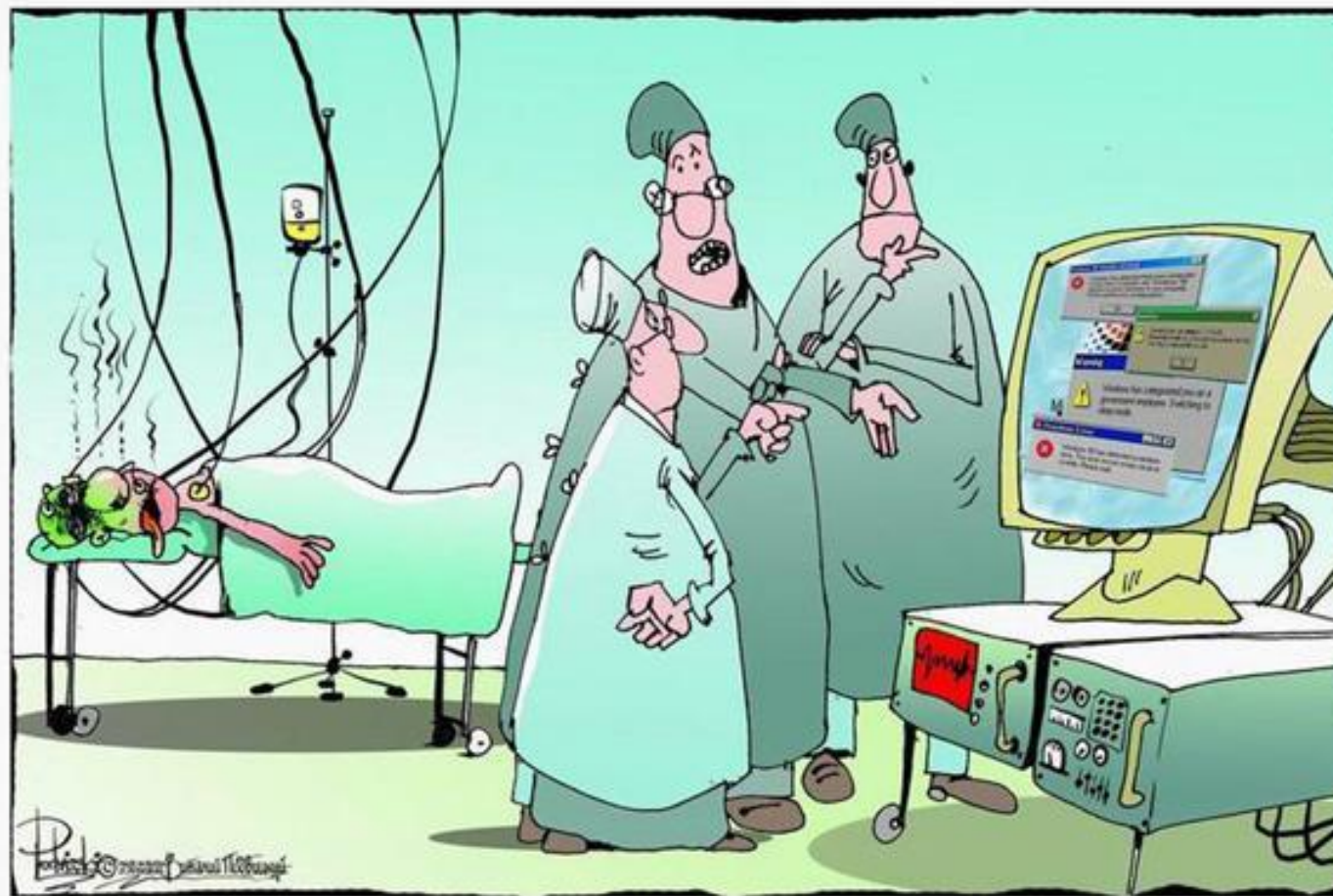
## Требования при внедрении СУИБ

1. Минимизация изменений, вносимых в технологические процессы обработки информации;
2. Максимально возможное использование:
  - существующих в ИС основных технических средств вычислительной техники, системного и прикладного программного обеспечения;
  - структуры информационных систем и особенностей их построения;
  - средств защиты информации;
  - персонала, ответственного за техническое сопровождение, системное администрирование и обеспечение информационной безопасности, с учетом его состава и квалификации;
  - топологии технологических процессов обработки информации;
  - распорядительной документации Клиники в части касающейся безопасности обработки конфиденциальной информации.





### 3. Внедряемые средства защиты не должны снижать показатели надежности подключенного к ИС медицинского оборудования



PODVITSKI.RU

CARICATURA.RU



Ежегодно нам доверяют самое ценное –  
собственное здоровье **более 60 тысяч пациентов**  
Каждый пациент – **субъект персональных данных**

В год врачами клиники «Медицина» было  
оказывается более **2 000 000 услуг** –

это более **2 000 000 записей**, содержащих  
**сведения конфиденциального характера**

**2** дата-центра. **80** серверов, с теоретической суммарной  
вычислительной мощностью **30 терафлопс**;  
хранится **200 терабайт** информации  
**17** кроссовых



Сведения конфиденциального характера  
ОАО «Медицина»

Все лучшее  
в медицине!



Персональные данные  
(в т.ч. специальные и  
биометрические)

Врачебная тайна

Коммерческая тайна

ОАО  
«Медицина»

# Основные поддерживаемые информационные системы



- Active Directory
- Exchange
- Файловый сервер
- E-Staff
- Marketing Analytic
- IntraService
- Аптека
- Контингент
- BioTime
- Казначейство
- Внутренний портал «Медицина»
- Система видеонаблюдения Endura
- Система видеонаблюдения Trassir
- 1С. Материальный учет
- 1С. Зарплата и управление персоналом

Все лучшее  
в медицине!



Since 1990



Все лучшее  
в медицине!



Since 1990



# Центр обработки данных.

## Общие показатели и основные характеристики

Все лучшее  
в медицине!



**Два ввода**

Надежное  
электропитание

**ДГУ 800 кВт**



**APC Symmetra  
350 кВт**



Эффективное охлаждение

**InRow кондиционеры APC**



**APC**  
Legendary Reliability™  
InRow Cooling

Постоянная связь с Интернет

**2 независимых провайдера 100 Мбит/с**

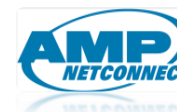
Защищенный периметр и VPN  
доступ

**Кластеризованный межсетевой экран и  
VPN-шлюз Stonesoft FW 1030**

# Система резервного копирования и архивирования данных

Передовые сетевые решения

СКС 7 категории от



Надежное серверное оборудование

Дублирование оборудования ядра сети

Лучшее от



2 СХД IBM  по 40 Тб

Виртуализация, разнообразие ОС и приложений



Надежная защита данных



Ленточная библиотека IBM TS 3310

Квалифицированный персонал

Более 10 лет опыта



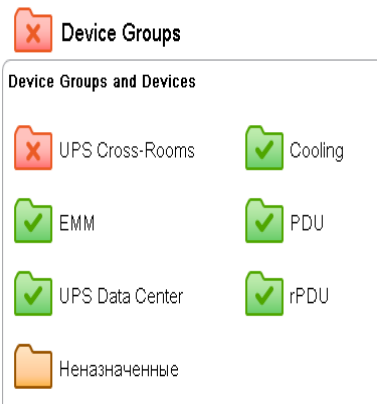
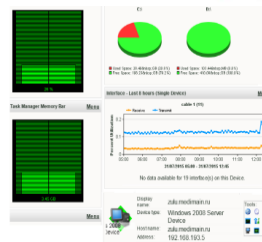
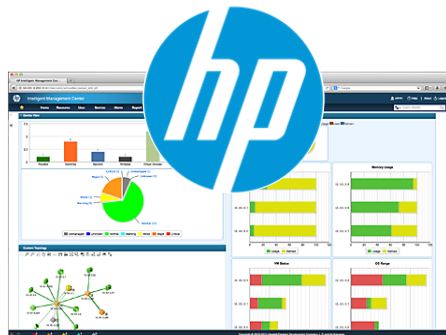
Все лучшее  
в медицине!



Since 1990



# Система мониторинга

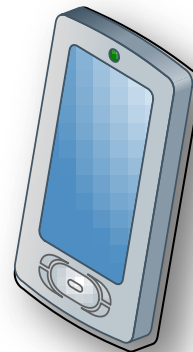


Мониторинг инфраструктуры обеспечивают три системы:

**WhatsUpGold** – для наблюдения за серверами,

**Hewlett Packard IMC** – для наблюдения за сетевым оборудованием,

**Schneider Electric Data Center Expert** – для наблюдения за оборудованием электропитания и охлаждения. Аварийные уведомления приходят на мобильное устройство дежурного специалиста.



Все лучшее в медицине!



Since 1990

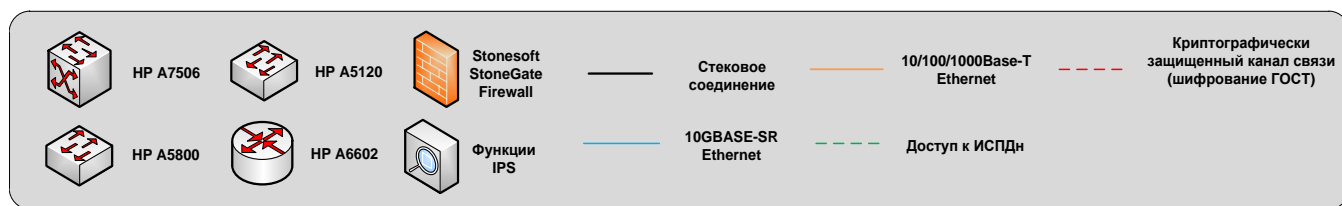
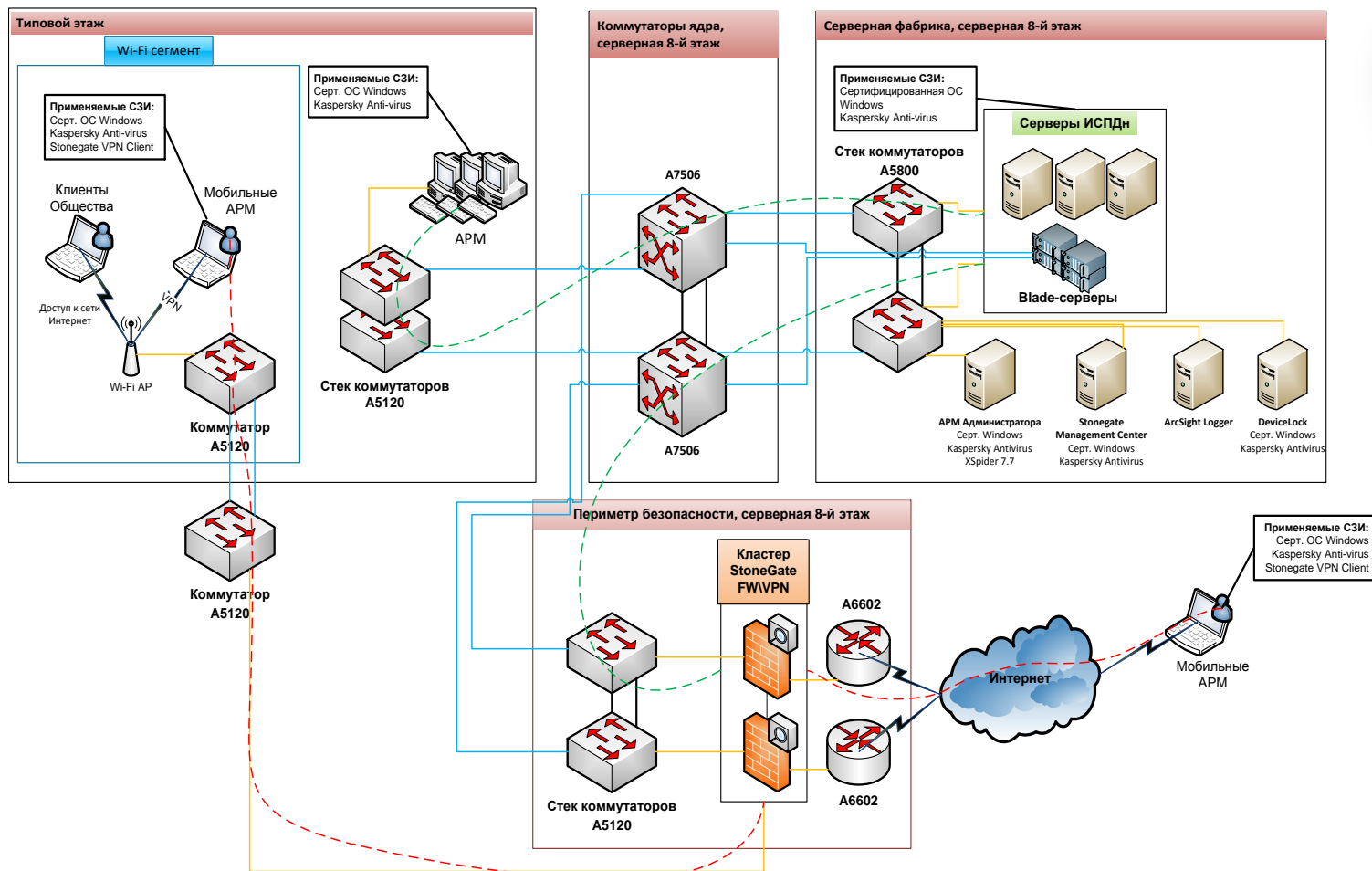


# Структурная схема комплекса технических средств системы защиты информации

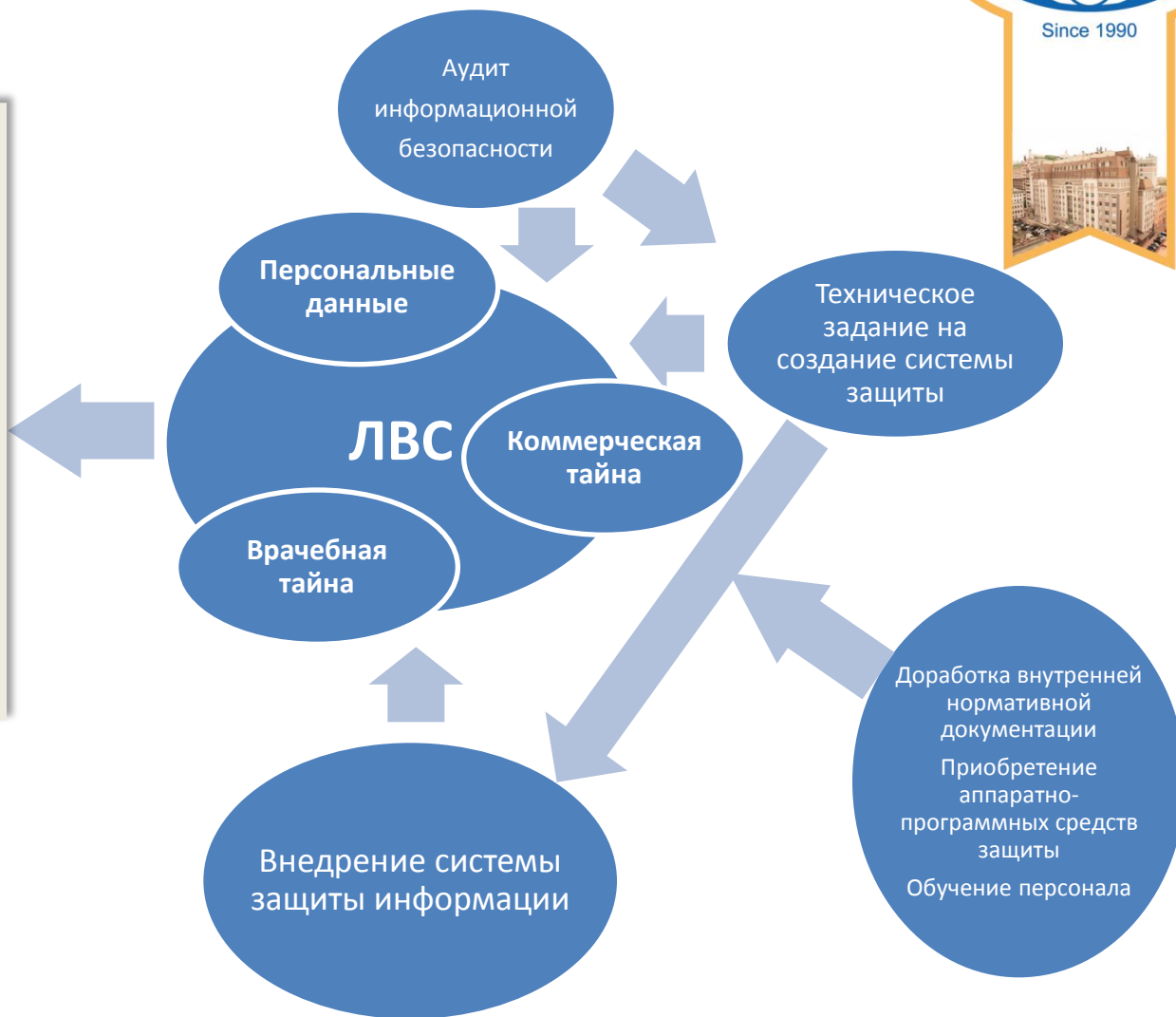
Все лучшее  
в медицине!



Since 1990



# Этапы подготовки системы к аттестации



# Аттестация СЗИ



## Выгоды от внедрения СУИБ:

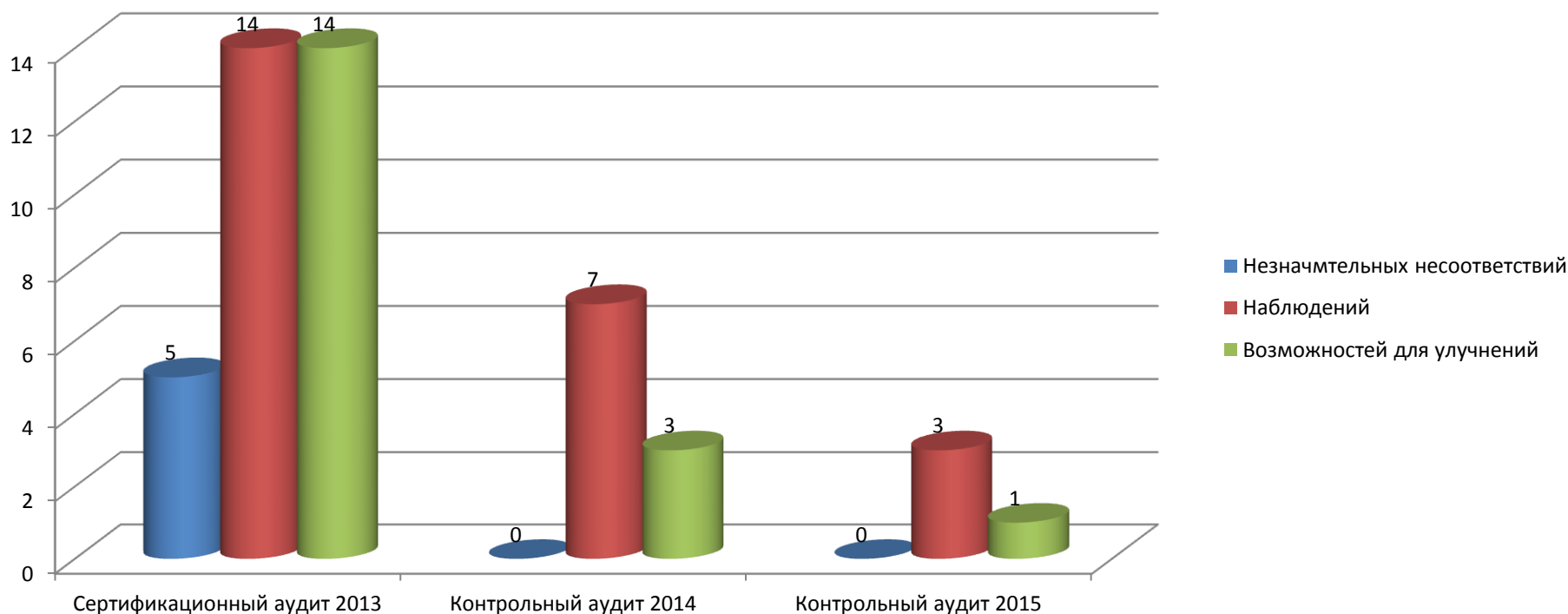
- Оптимизация обоснование расходов на информационную безопасность.
- Снижение рисков, связанных с возможными ущербами для активов компании.
- Снижение операционных затрат, за счет формализации процессов ИБ.
- Обеспечение соответствия уровня ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса.

## Преимущества сертификации на соответствие требованиям международного стандарта ISO27001:2013

- Повышение международных рейтингов компании, необходимых для привлечения
- зарубежных инвестиций, выхода на международные рынки.
- Повышение доверия со стороны заказчиков и партнеров.
- Защита инвестиций.
- Увеличение капитализации компании.
- Повышение стоимости акций компании.
- Повышение доверия к компании со стороны заинтересованных сторон.



Стандарты серии ISO обеспечивают постоянное совершенствование в своей области применения. В качестве примера можно привести динамику сокращения недостатков системы управления информационной безопасности Клиники за один сертификационный цикл.

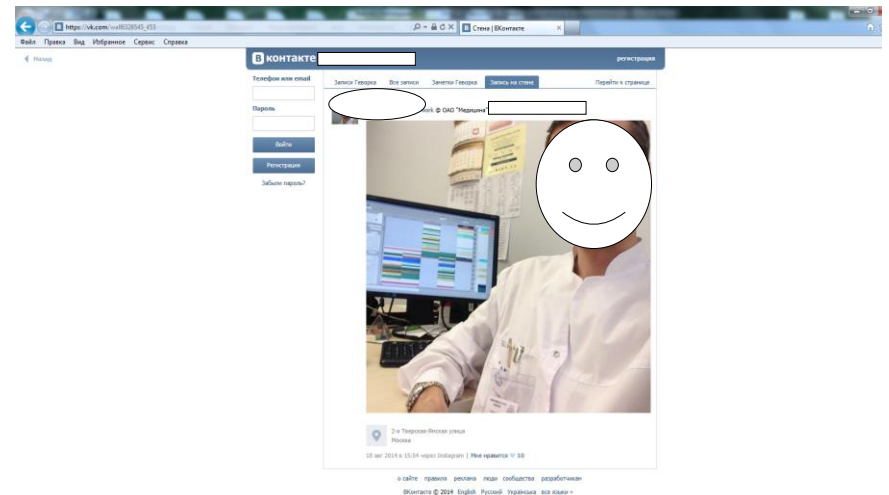
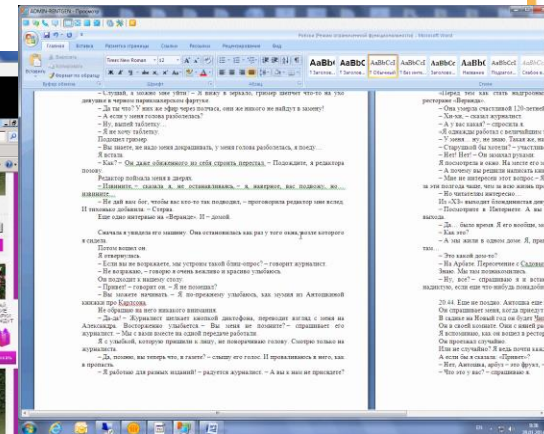
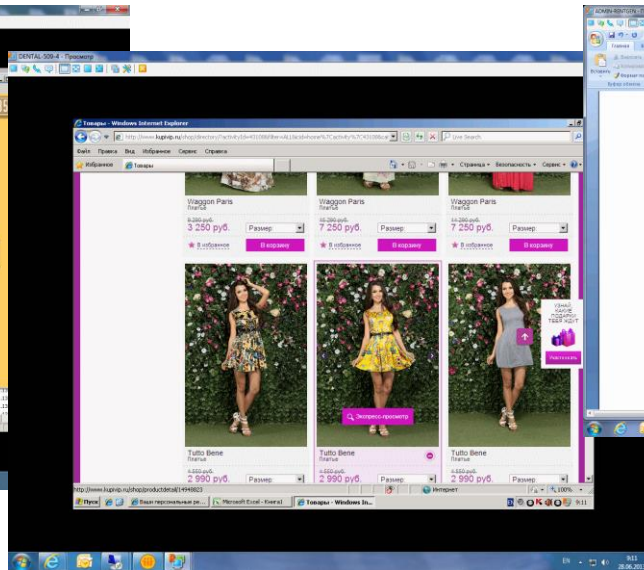


# Постоянный мониторинг

Все лучшее  
в медицине!



Since 1990



Клиника «Медицина»

www.medicina.ru



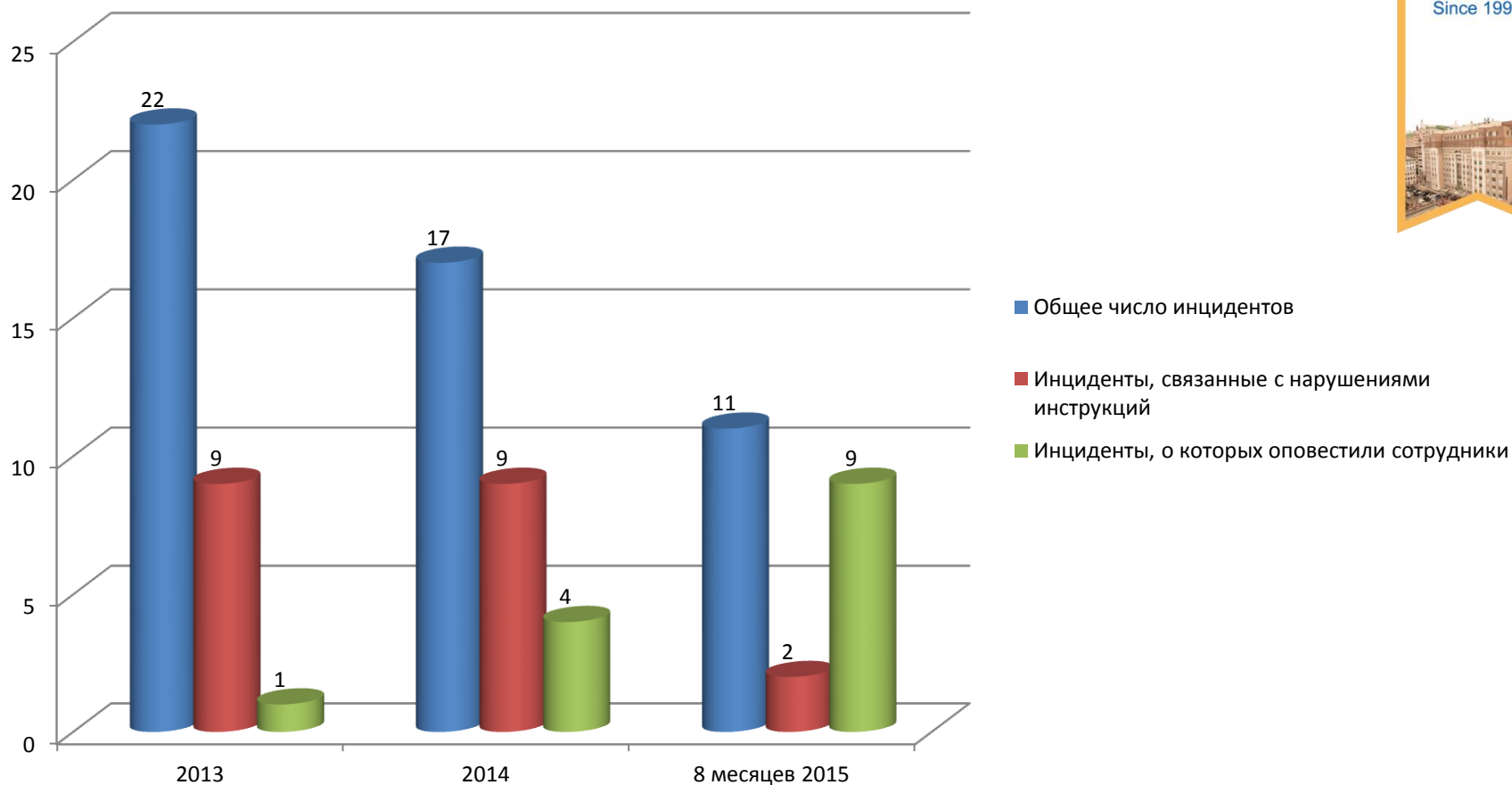
Все лучшее  
в медицине!



Since 1990



## Инциденты информационной безопасности



# Проблемы обеспечения ИБ

Все лучшее  
в медицине!



- 1. Сложность определения всех категорий субъектов персональных данных, процессов обработки ПДн, систем и т.п.**
- 2. Противоречия между производственными задачами и задачами обеспечения безопасности.**
- 3. Неоднозначность трактовок нормативно-распорядительной документации.**
- 4. Реализация некоторых требований крайне затруднена как технически, так и организационно.**
- 5. «Внезапные» изменения в нормативно-распорядительной документации.**
- 6. Проблемы репутационного характера**



## Возможные решения

- 1. Аттестация и сертификация информационных систем.**
- 2. Регулярные независимые аудиты.**
- 3. Постоянное совершенствование СЗИ.**
- 4. Не только техническая, но и юридическая поддержка.**
- 5. Постоянный мониторинг изменений в законодательстве.**
- 6. Использование международных стандартов и лучших практик.**

Все лучшее  
в медицине!



Since 1990



# Спасибо за внимание