

РИСКИ ОПЕРАТОРОВ ПЕРСОНАЛЬНЫХ ДАнных И ПУТИ ИХ СНИЖЕНИЯ

(технико-правовые и социально-правовые)

Роман Кобцев

2010 год

© Авторские права защищаются
в соответствии с законодательством
Российской Федерации

При использовании ссылка на
первоисточник обязательна



ВНИМАНИЕ!

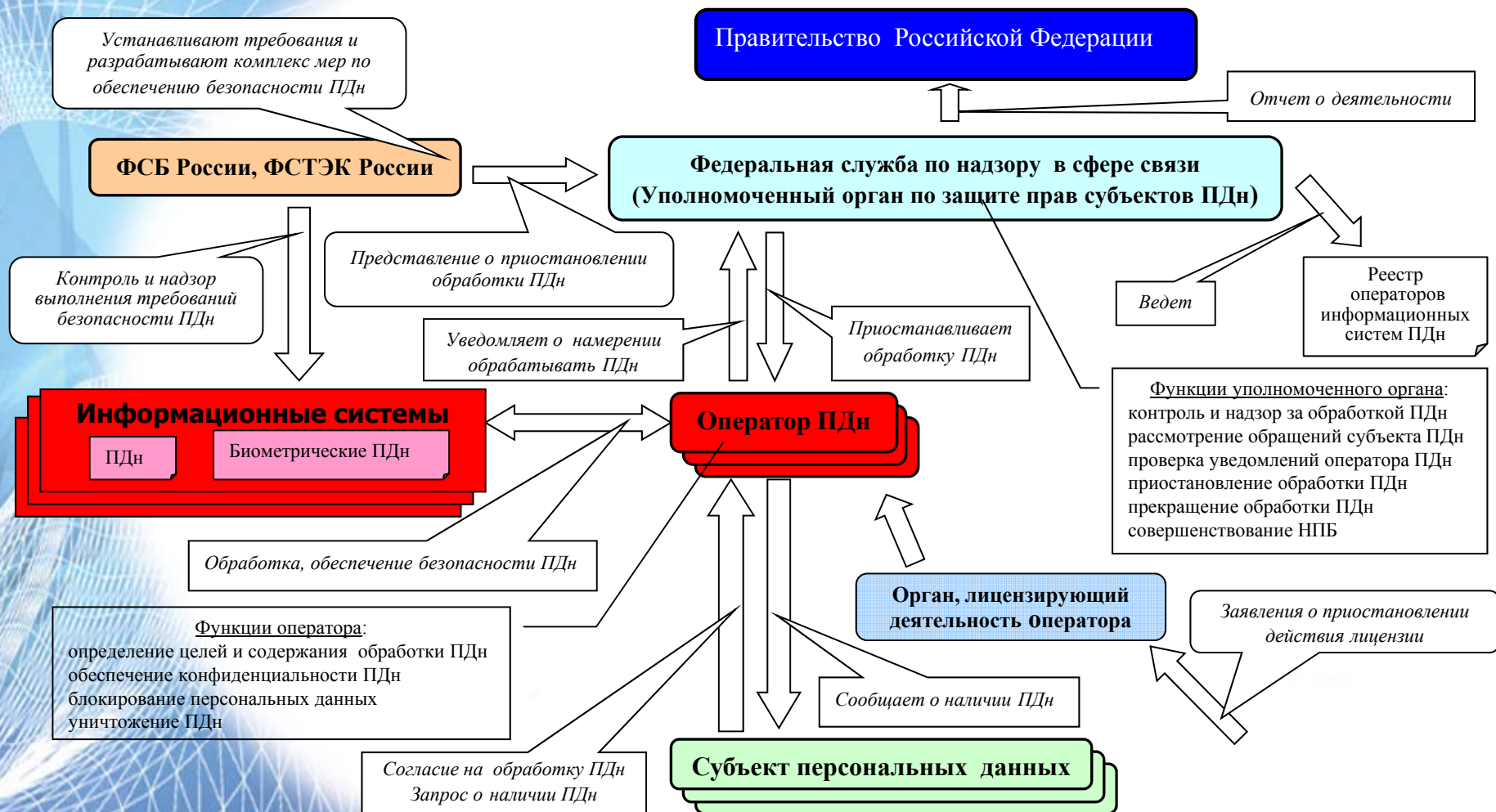
Материалы, изложенные в данной презентации рассматривают только основные технико-правовые и социально-правовые риски, которые могут возникнуть у оператора персональных данных и не претендуют на полноту анализа всего поля угроз

- **Какие риски несет оператор персональных данных (ПДн)?**
- **Реализация каких угроз может привести к возникновению рисков оператора ПДн?**
- **Пути снижения рисков**



ЭЛВИС-ПЛЮС СИСТЕМА ОТНОШЕНИЙ ПРИ ОБРАБОТКЕ ПДн

Особенности регулирования отношений





ЭЛВИС-ПЛЮС ЧТО НАДО УЧИТЫВАТЬ ПРИ ОБРАБОТКЕ ПДн

Особенности обработки

- Основная информация в ИС – личная тайна клиента
- Деликатность взаимоотношений с клиентами
- Жесткий временной регламент работы с информацией
- Наличие одновременно защищаемой и открытой информации
- Фрагментарность обработки и разные права доступа персонала
- Гетерогенность программной и аппаратной платформ ИС
- Мигрируемость информации между прикладными программами

Защита ПДн направлена на исключение несанкционированного доступа, при котором возможно их уничтожение, изменение, блокирование, копирование и распространение



ЭЛВИС-ПЛЮС РИСКИ ОПЕРАТРОВ ПДн ПРИ ОБРАБОТКЕ ПДн

Основные угрозы при нарушении правил обработки и защиты

✓ Возможность материального ущерба

- Угроза судебных исков субъектов ПДн
- Угроза административной ответственности
- Угроза приостановления основной деятельности
- Угроза потери клиентов (перехода к конкуренту)

✓ Возможность репутационного ущерба

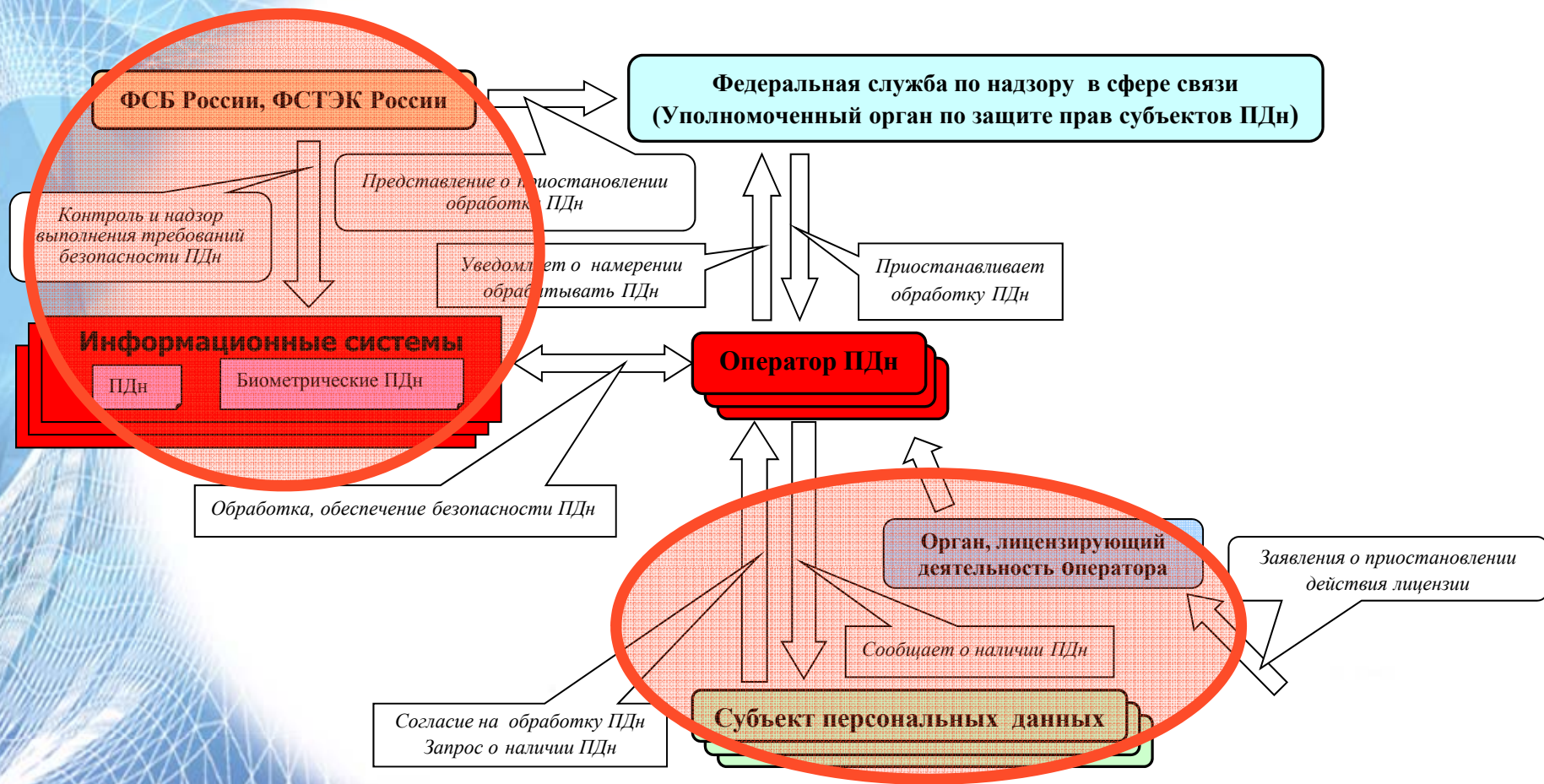
- Угроза публикации нарушений в отчетах регуляторов
- Угроза публикации негативной информации в СМИ
- Угроза распространения неблагоприятных слухов
- Угроза формирования неблагоприятной судебной практики

***Нарушение установленных правил обработки защиты ПДн
влечет не только потерю репутации, но прямые
материальные потери***



ЭЛВИС-ПЛЮС СИСТЕМА ОТНОШЕНИЙ ПРИ ОБРАБОТКЕ ПДн

Особенности регулирования отношений



Основные уязвимости, приводящие к реализации угроз

✓ Социально-правовые уязвимости

- Неправомерное распространение ПДн (иск в суд о возмещении ущерба)
- Нарушение порядка обработки ПДн (жалоба в надзорный орган)
- Конфликт, не связанный с обработкой ПДн (жалоба в надзорный орган)
- Отказ клиента в обработке своих ПДн (блокирование работы ИСПДн)
- Запрос сведений, касающихся обработки ПДн (ст.14,ФЗ-152 проблемы)

✓ Техничко-правовые уязвимости

- Нарушение порядка обработки ПДн (проверка регуляторов)
- Отсутствие средств защиты ПДн (проверка регуляторов)
- Отсутствие документации по защите ПДн (проверка регуляторов)

Социальный аспект играет важную роль в устранении рисков страховых компаний при обработке ПДн, но не исключает необходимости решения технических проблем



Основной угрозой оператора персональных данных (с точки зрения ведения бизнеса) после вступления в силу ст. 25 Федерального Закона «О персональных данных» является

Угроза приостановления или прекращения обработки персональных данных оператором.

- ✓ **Принять меры к снижению социального накала**
 - Построить позитивные отношения с клиентом
 - Декларировать гарантии по защите ПДн
 - Ясно разъяснять цели сбора и обработки ПДн
 - Предупреждать клиента обо всех операциях с ПДн
- ✓ **Принять меры по снижению класса защищенности ИСПДн**
 - Правильно оценить угрозы (модель) и исключить не актуальные
 - По возможности сократить количество субъектов ПДн
 - По возможности снизить категорию ПДн
- ✓ **Разделить риски с другими**
 - Операторы связи (провайдеры)
 - Зарубежные партнеры

✓ Организационные методы

- Уточнить необходимость для бизнеса имеющегося объема ПДн
- Применять кодирование диагнозов
- Применять при обработке обезличенные ПДн
- Перейти при обработке на табельные или абонентские номера
- Исключить часть ПДн из автоматизированной обработки

✓ Технические методы

- Разделить ИС на сегменты по функциональному признаку
- Выделить БД в отдельный сегмент системы – ЦОД
- Создать сегмент для ПДн, идентифицирующих субъекта
- Использовать технологии терминального доступа
- Перенастроить пользовательские интерфейсы
- Разместить наиболее критичные ПДн на съемных носителях

Если стоимость реализации организационных и технических методов снижения категории ПДн ниже, чем стоимость системы защиты, то есть повод для раздумий

- максимальное использование возможностей уже имеющихся в ИС средств защиты информации, возможностей ОС и прикладного ПО
- принятие дополнительных мер, позволяющих снизить требования к части ИСПДн или сегментам сети, где такие ИСПДн расположены
- сокращение количества АРМ, обрабатывающих ПДн, разделение функций пользователей, минимизирование одновременной обработки ПДн из разных систем
- разделение ИС межсетевыми экранами на отдельные сегменты (ИСПДн), классификация каждого сегмента и снижения требований к ним

Даже если ИСПДн имеет высокий класс, всегда остаются пути снижения затрат на защиту ПДн

Вариант с использованием терминальный доступ

✓ **Особенности терминального доступа**

- обмен с сервером только кодами клавиш и «снимками» экранов
- данные не обрабатываются и не хранятся
- изоляция терминальных сессии по данным

✓ **Снижение требований к рабочему месту**

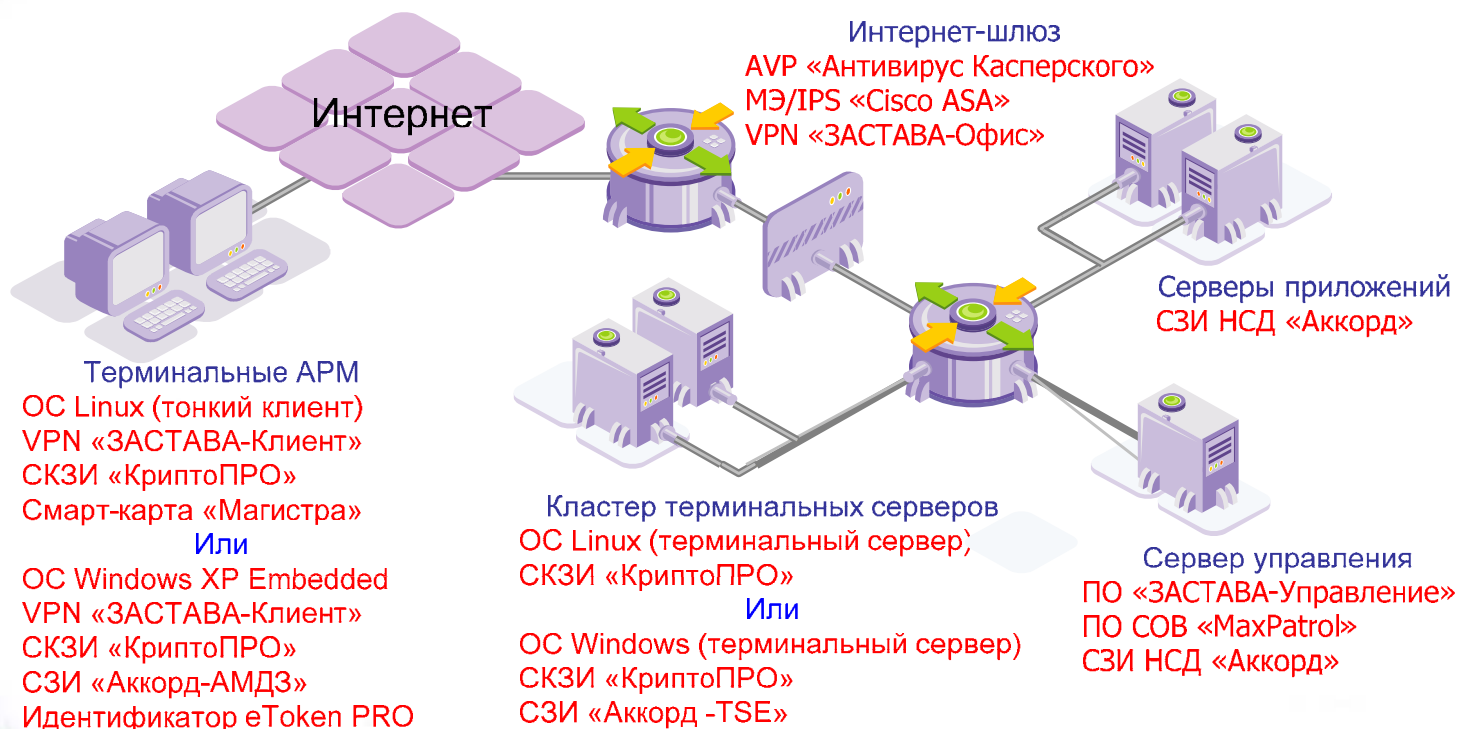
- простая модель угроз ПДн
- ПДн не обрабатываются и не хранятся
- невозможность передать на сервер (в ЦОД) вредоносный код
- параллельная работа с открытыми и конфиденциальными данными
- из функции ИБ – защита канала и защита от клавиатурных шпионов

✓ **Экономия на защите ИСПДн**

- снижение стоимости аудита
- только защита канала и целостности (защита от снифинга клавиатуры)
- экономия на СЗИ, AVP, IPS
- снижение стоимости аттестации
- Возможно использование тонкого клиента на свободном ПО

ИСПДн с архитектурой терминального доступа – реально снижает затраты на защиту ПДн

Пример: применение терминального доступа для SMB-сегмента



Внутри тонкого клиента обработка персональных данных не ведется!

ВОПРОСЫ?

e-mail: vsv@elvis.ru



ЭЛВИС-ПЛЮС

Спасибо за внимание !

e-mail: krj@elvis.ru