Безопасность ПДн

Можно ли пользоваться иностранными облачными платформами с точки зрения законодательства РФ в области защиты ПДн?

Барышников Александр
Руководитель направления отдела консалтинга
ЗАО НИП «Информзащита»

infosecurity RUSSIA
24-26 СЕНТЯБРЯ 2014
Крокус Экспо, Москва

Информзащита
Системный интегратор

Кто такой Оператор ПДн?

- **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн

Уполномоченное лицо

- Уполномоченное лицо (обработчик по поручению) - лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора

«Облачные» технологии

Тенденции:

- сокращение расходов на собственную ИТ-инфраструктуру

Виды облачных сервисов:

- частное облако
- публичное облако
- общественное облако
- гибридное облако

SaaS

Software-as-a-Service - «программное обеспечение как сервис»

- **доступ к предоставляемому прикладному программному обеспечению**

Microsoft® Office 365

Google™ Drive

EVERNOTE

Dropbox

box

PaaS

Platform-as-a-Service - «платформа как сервис»

- **среда для развертывания базового ПО**

Состав платформ:

- инструментальные средства создания, тестирования и эксплуатации прикладного ПО,
- СУБД,
- среды исполнения языков программирования и др.

Windows Azure

Google app engine

heroku

appfog

IaaS

Infrastructure-as-a-Service - «инфраструктура как сервис».

- **ресурсы вычислительной инфраструктуры**:
  - сетевая инфраструктура,
  - инфраструктура серверного оборудования
  - инфраструктура хранения данных.

Разделение ответственности

Компоненты платформы	Распределение зон ответственности		
	IaaS	PaaS	SaaS
Прикладное ПО (клиентский компонент)	Клиент	Клиент	Клиент
Прикладное ПО (серверный компонент)	Клиент	Клиент	Поставщик
СУБД и платформы (среды) разработки и выполнения ПО	Клиент	Поставщик	Поставщик
Операционные системы	Клиент	Поставщик	Поставщик
Подсистема виртуализации	Поставщик	Поставщик	Поставщик
Аппаратная инфраструктура	Поставщик	Поставщик	Поставщик

Вопрос презентации

Можно ли в России пользоваться «облачными технологиями» при обработке персональных данных?

Договор

Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

- **Цели обработки ПДн**
- **Перечень действий с ПДн**
- **Конфиденциальность ПДн**
- **Требования к защите ПДн**

Модель угроз

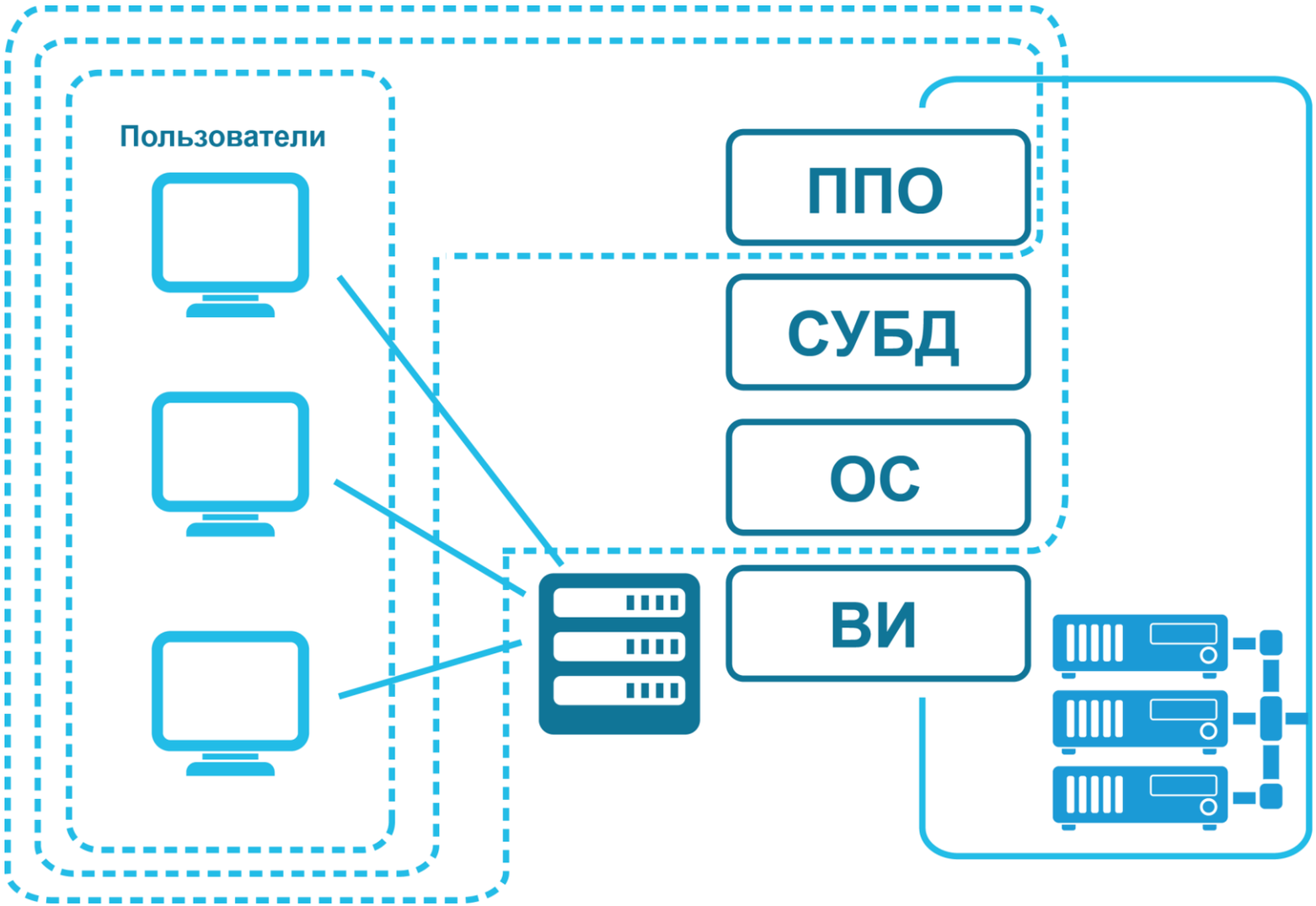
Частные модели угроз

- **распределение ответственности за обеспечение безопасности ПДн** между оператором и поставщиком облачных сервисов.

✓ Частные модели угроз на зоны ответственности Оператора ПДн

✓ Частные модели угроз на зоны ответственности Поставщика услуг (Уполномоченное лицо)

Зоны ответственности



Поправка в законодательстве

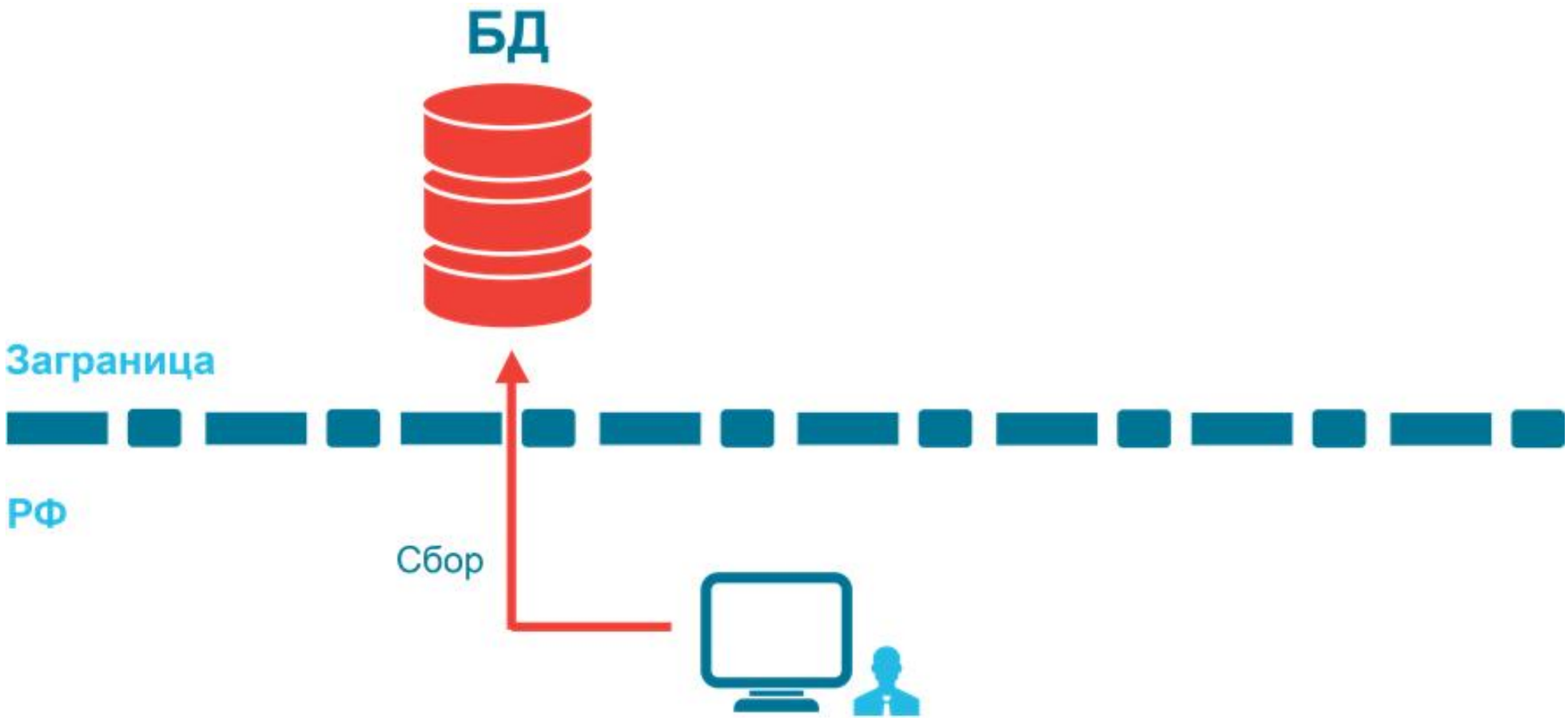
242-ФЗ от 21.07.2014

При **сборе персональных данных**, в том числе посредством информационно-телекоммуникационной сети "Интернет", **Оператор обязан** обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

Обработка ПДн

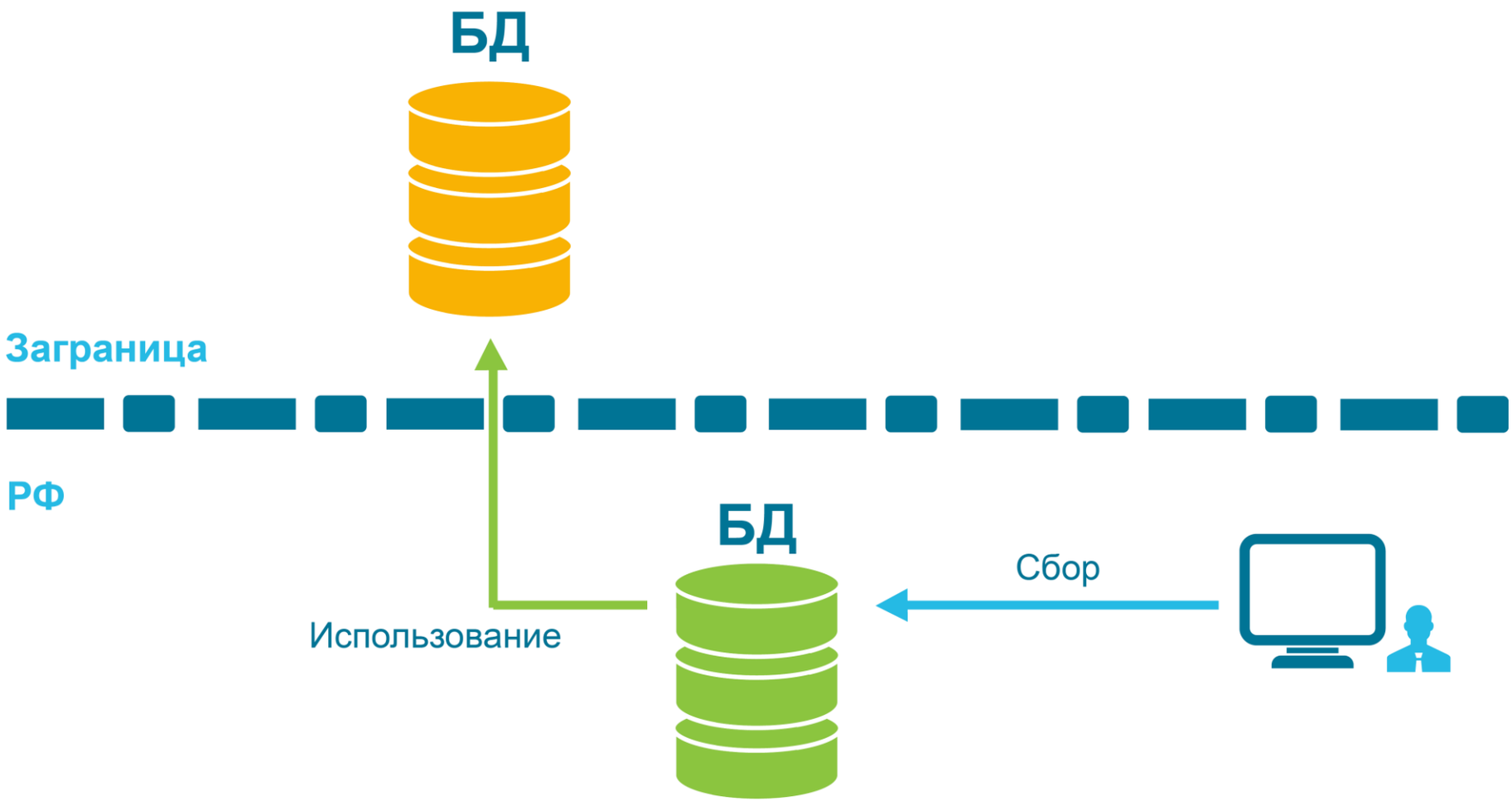
152-ФЗ	242-ФЗ
сбор	**сбор**
запись	запись
систематизацию	систематизацию
накопление	накопление
хранение	хранение
уточнение (обновление, изменение)	уточнение (обновление, изменение)
извлечение	извлечение
использование	
передачу (распространение, предоставление, доступ)	
обезличивание	
блокирование	
удаление	
уничтожение	

Незаконная обработка ПДн



НЕ верно

Обработка «по закону»



ВЕРНО

Легитимные схемы обработки

Как можно обрабатывать ПДн в «облаках»?

- создание БД на компьютере и после синхронизация с облаком – **ДА**
- создание БД сразу в облаке – **НЕТ**

Нереализуемо? Опыт Apple

«Корпорация Apple признала, что часть данных о ее китайских пользователях хранится на серверах в Китае — этого требуют условия контракта с China Telecom. Американская компания утверждает, что хранение данных в Китае не ставит под угрозу безопасность ее пользователей, поскольку информация зашифрована.»

Ведомости

«Apple хранит пользовательские данные в Китае»

Нереализуемо? Опыт SAP

DataLine: SAP по модели SaaS

3 августа группа компаний Inline Technologies Group в лице DataLine и Triangle Consulting анонсировала новую услугу «SAP как сервис».

DataLine и Triangle Consulting прошли сертификацию компанией SAP и обладают правом предоставлять ПО SAP на условиях аренды по модели SaaS. В качестве хостинг-площадки арендуемого ПО DataLine предлагает как физическое размещение в дата-центрах, соответствующих уровню Tier3, так и размещение с использованием облачных технологий на базе среды CloudLine.

Ведомости

«DataLine: SAP по модели SaaS»

Доверяй, но проверяй!

Аудит

- выполнение требований законодательства
- контроля и обеспечения адекватного уровня защиты вашей информации

Обработка допустима!

Обрабатывать ПДн в «облаках» можно!

Требуется:

- ✓Договор
- ✓Определение зон ответственности
- ✓Модели угроз в соответствии с зонами ответственностями
- ✓БД на территории РФ
- ✓Контроль принимаемых мер

Барышников Александр

Руководитель направления
Отдела консалтинга

+7(495) 980-2345 (640)

a.baryshnikov@infosec.ru

Информзащита
Системный интегратор