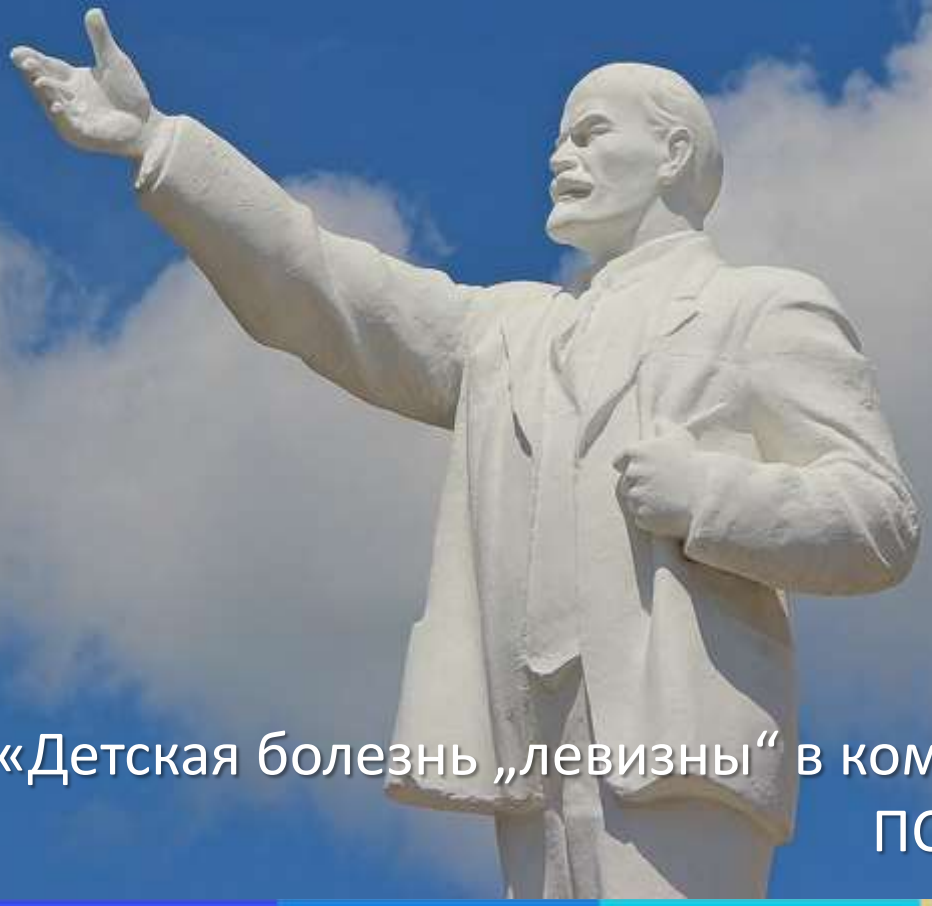
«Верхи не могут, Низы не хотят…», или

сказ о том, как правильно SecaaS делать

*«Лишь тогда, когда **„низы“ не хотят** старого и когда **„верхи“ не могут** по-старому, лишь тогда революция может победить»*

В. И. Ленин



«Детская болезнь „левизны“ в коммунизме». 1920 г.
ПСС - т.41. - стр.69-70

Революционная ситуация в облаках

Как рынок облачных вычислений оказался в позиции «Ждём-с…»

Заказчик облачных услуг

Заказчик:

- Очень хочет в «облака»
- Обрабатывать информацию / реализовывать бизнес-процесс
- Имеет собственные требованиях по ИБ

У заказчика 2 пути:

- Обеспечивать ИБ самому …. ☹
- «Свалить» на поставщика услуг … ☺

Информзащита
Системный интегратор
20 лет

Поставщик облачных услуг

Поставщик (ЦОД и/или «Облако»):

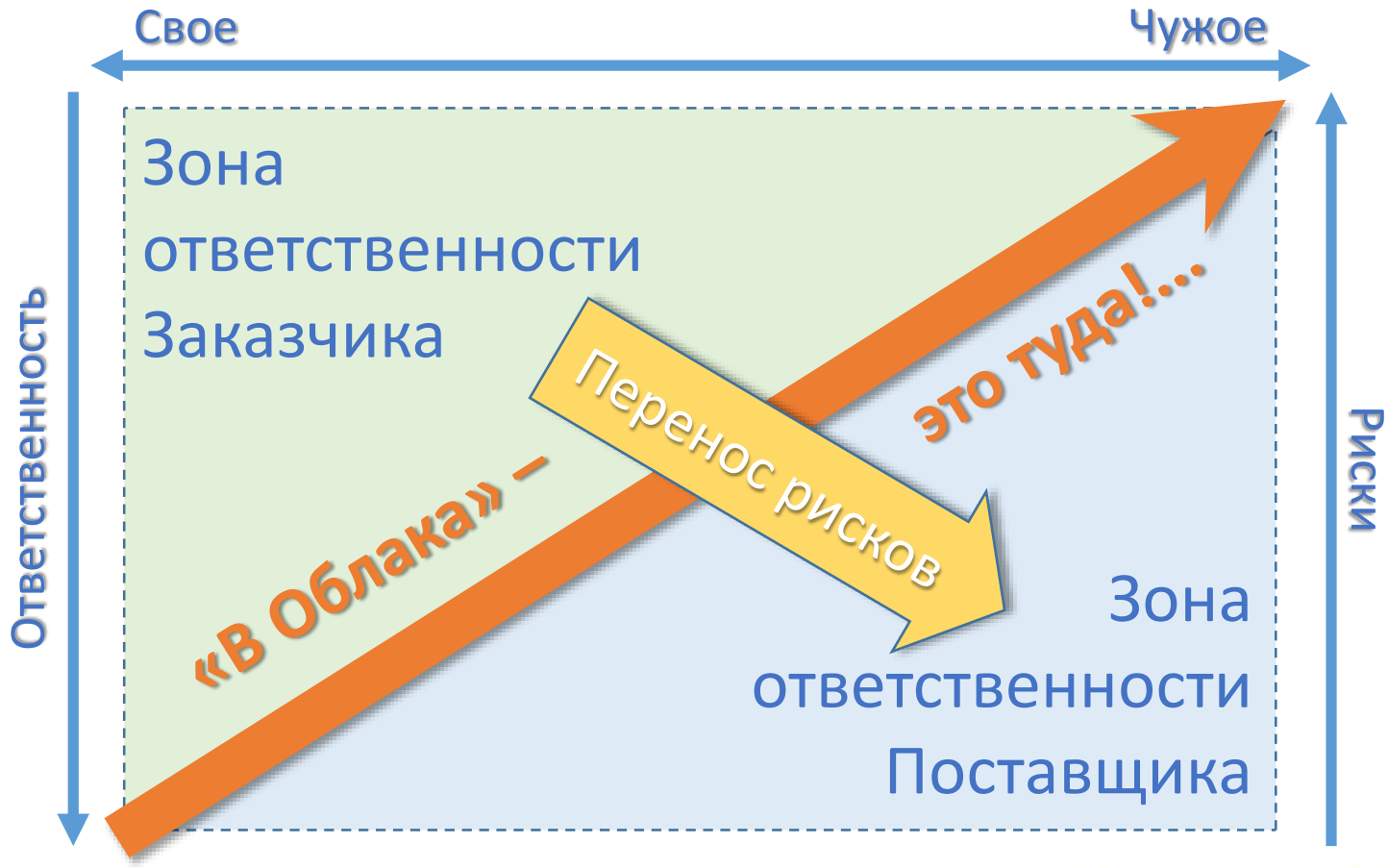
- Заинтересован в привлечении клиентов
- Снижает расходы на стоимость услуги
- Не всегда компетентен в вопросах ИБ

У поставщика 2 пути:

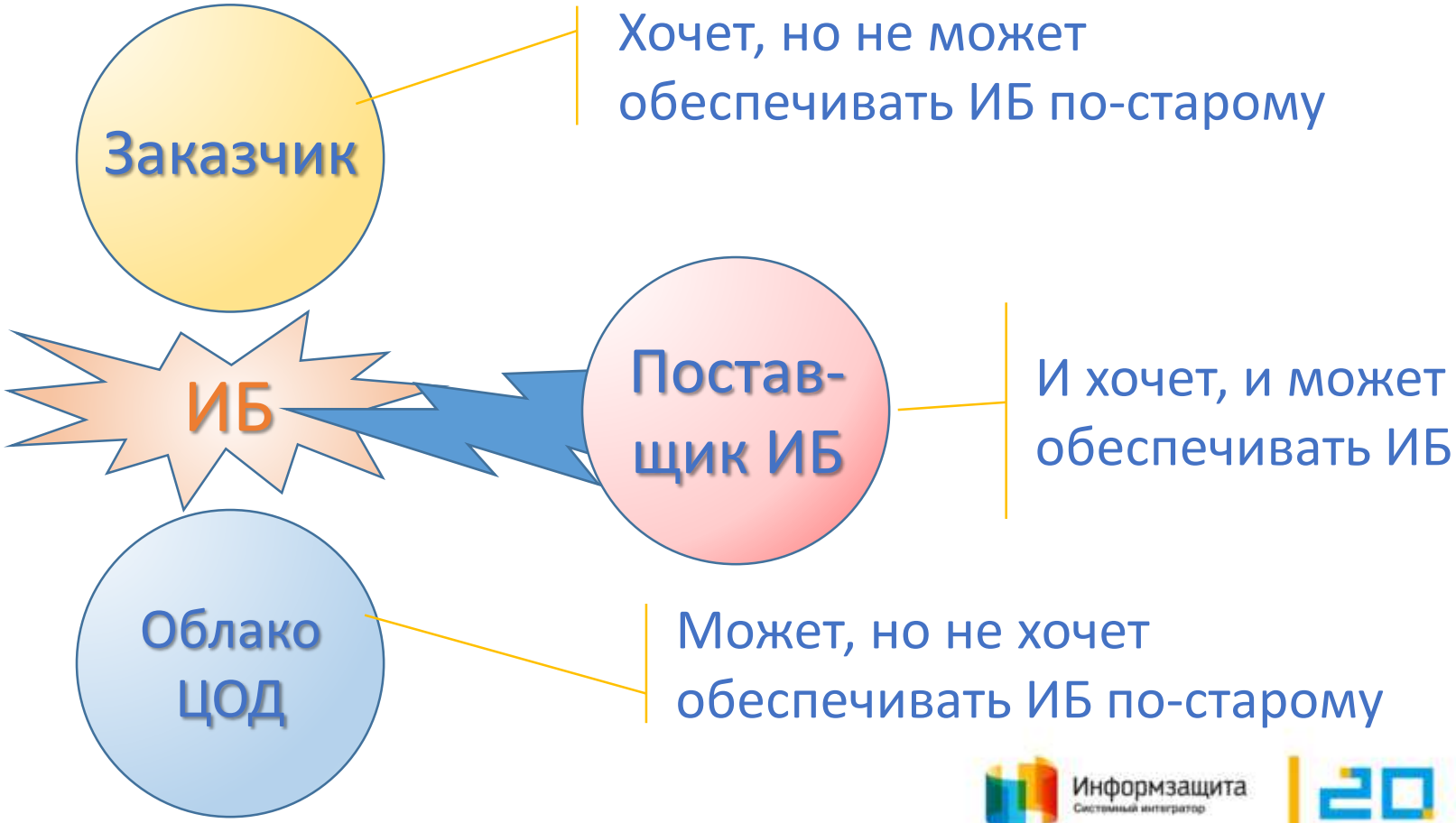
- Обеспечивать требования ИБ самому … 😐
- Позвать поставщика услуг ИБ … ☺ ?

Информзащита
Системный интегратор
20 лет

Перенос ответственности



Кто чего хочет?



Информзащита
Системный интегратор
20 лет

Поставщик услуг ИБ

Поставщик услуг ИБ

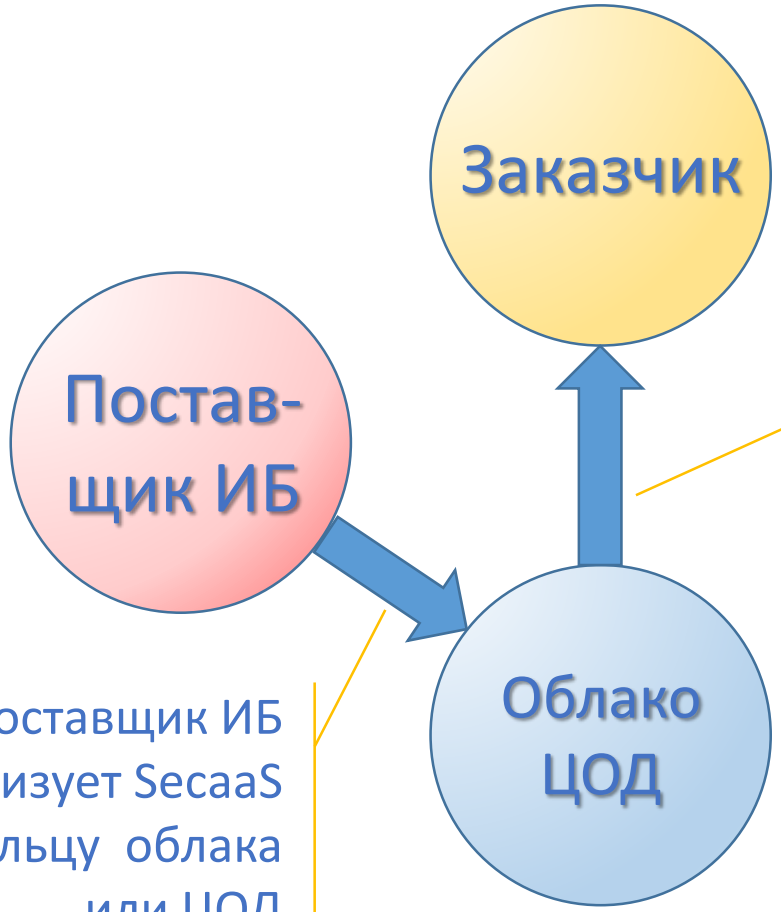
- Компетентен в области ИБ:
  знания, навыки, опыт, практика, лицензии…

Может:

- Создать сервис для поставщика «облака»
- Внедрить систему защиты Заказчику
- Продавать собственные услуги Заказчику или Поставщику

Информзащита
Системный интегратор
20 лет

Кто кому делает SecaaS ? (1)



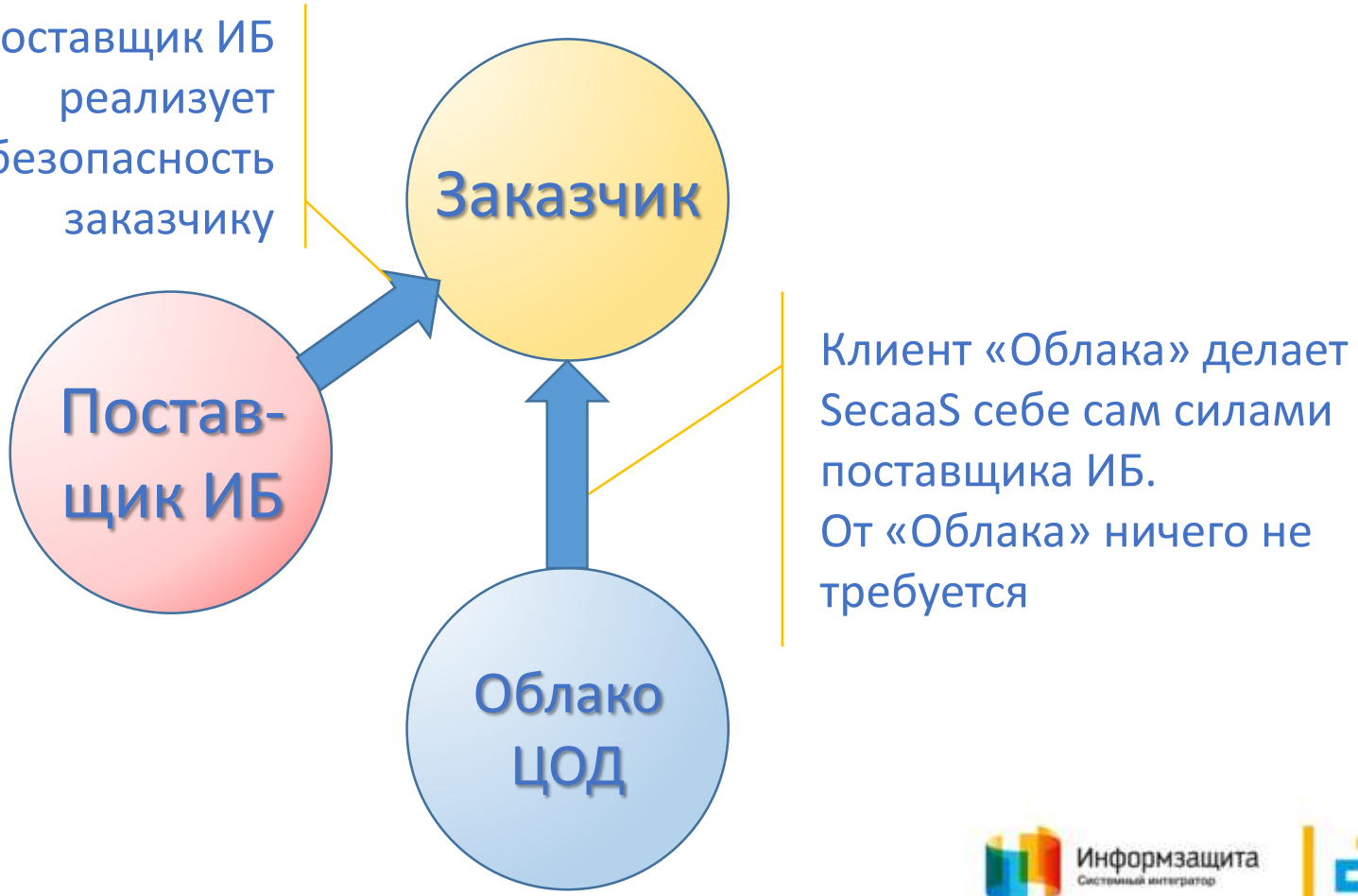
Поставщик «Облака» делает SecaaS своим клиентам

Поставщик ИБ реализует SecaaS владельцу облака или ЦОД

Информзащита
Системный интегратор

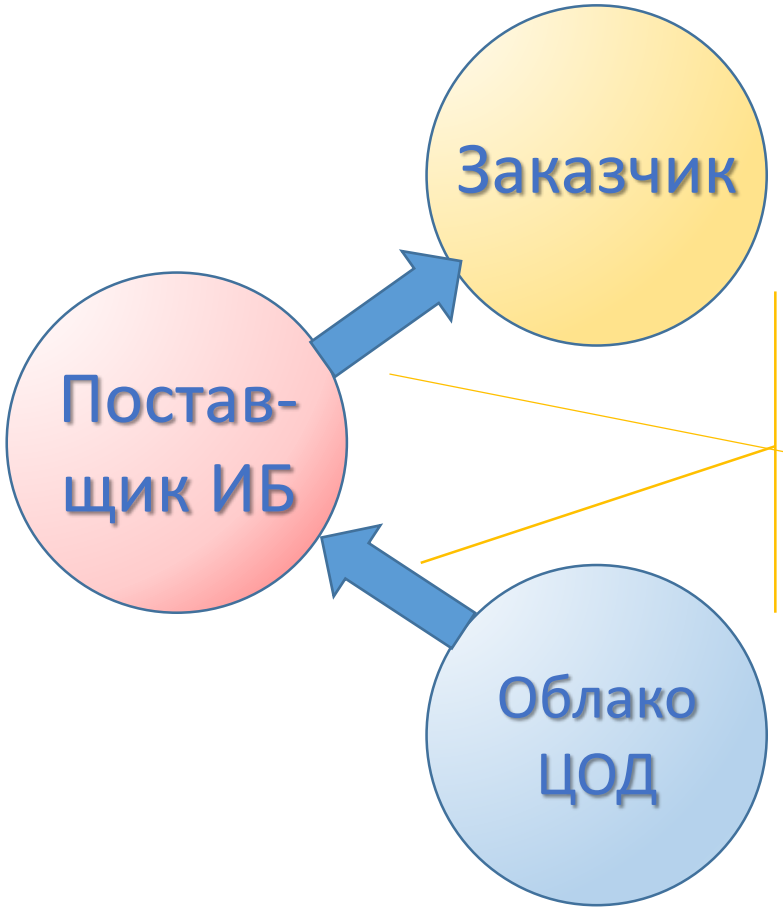
20 лет

Кто кому делает SecaaS ? (2)



Информзащита
Системный интегратор
20 лет

Кто кому делает SecaaS ? (3)

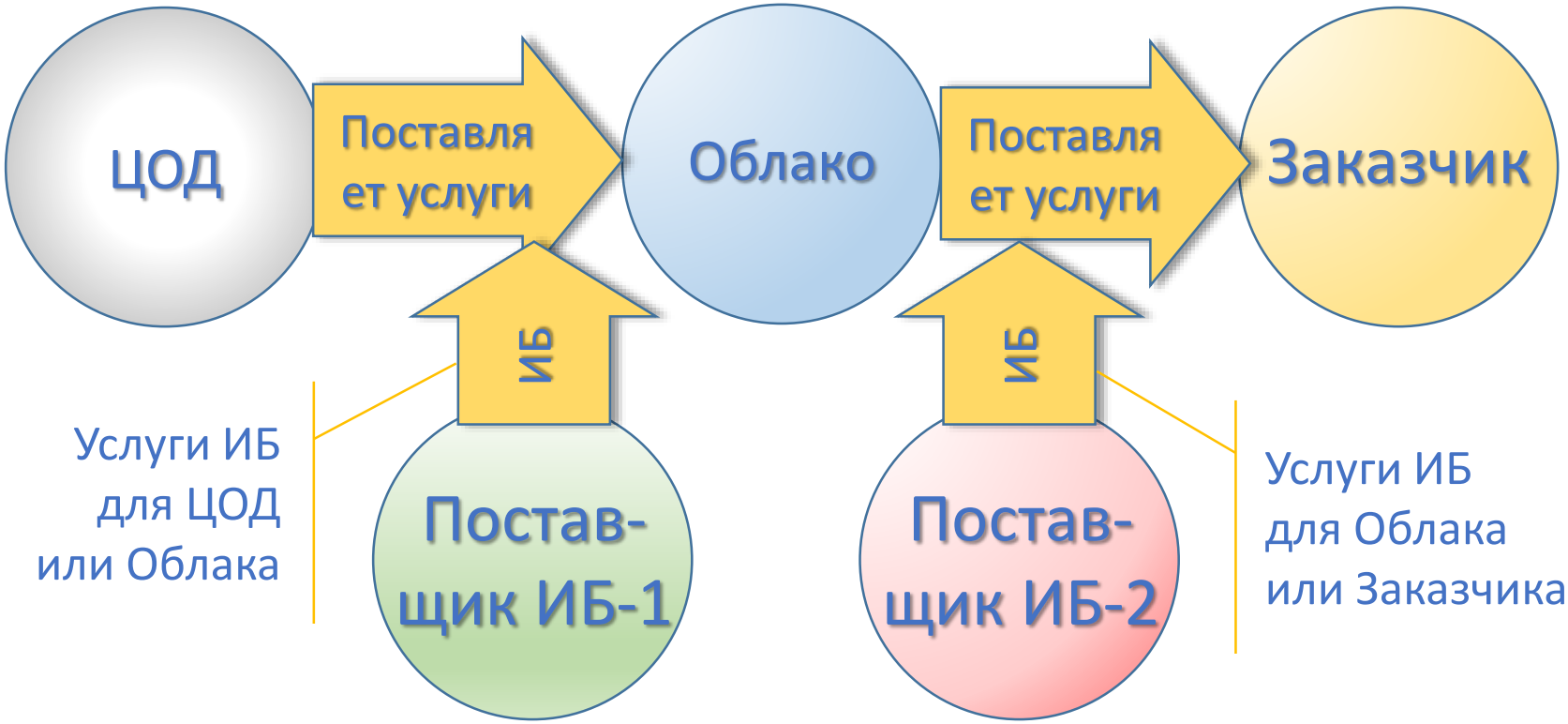


Поставщик ИБ договаривается с поставщиком «Облака» о продаже собственных услуг клиентам по модели SecaaS

Информзащита
Системный интегратор
20 лет

«Матрешка» ответственности

- Так чьи же в «облаке» шишки?
- Кто будет за всё отвечать?



SecaaS, как он есть

Услуги облачной безопасности

Услуги безопасности

- Решают какую-то **конкретную** задачу
- Решают её **лучше, чем Заказчик**

- Идеальная безопасность – её **не видно**

- Задача: дать Заказчику **то, что он хочет**, а не то, что поставщик **умеет делать** лучше всего или **хочет продать**

Информзащита
Системный интегратор
20 лет

Канонический SecaaS

cloud security alliance®

SecaaS™
Security as a Service
Working Group

CSA Working Group в 2011-2016:

- Определили **12 категорий**
- Выпустили **11** подробных **руководств по внедрению**

Информзащита
Системный интегратор

20 лет

Виды SecaaS в теории и практике

Business Continuity and Disaster Recovery	Intrusion Management
Continuous Monitoring	**Network Security**
Data Loss Prevention	Security Assessments
Email Security	**Security Information and Event Management**
Encryption	**Vulnerability Scanning**
Identity and Access Management (IAM)	**Web Security**

Вот где-то здесь...

Информзащита
Системный интегратор

20 лет

Почему-же не взлетает?

Менталитет

- Всё сводится к безопасности частных облаков → безопасность виртуализации
- Причины: регуляторика, «страхи» Заказчиков

Несовершенство СЗИ

- Не поддерживаются «тенанты»
- Отсутствуют ср-ва интеграции с облаками, ср-вами управления

Информзащита
Системный интегратор
20 лет

Архитектура построения классического SecaaS

Информзащита
Системный интегратор

20 лет

Что еще должно быть у Поставщика услуг?

- Соответствие требованиям. Лицензии
- Договорная работа. Обязательства и ответственность
- SLA по каждому виду услуг
- Контракты поддержки вендоров
- Готовность инф-ры к проверкам. Обеспечение требований НПА
- Страхование рисков ??? В стадии амнезии

Информзащита
Системный интегратор

20 лет

Что должно быть у Заказчика услуг?

- Понимание требований ИБ
- Орг.еденица для контроля кач-ва услуг
- Оргмеры на уровне Заказчика
- СЗИ на уровне АРМ/EndPoint

Информзащита
Системный интегратор
20 лет

Чем можно привлекать клиентов?

- Пробные периоды
- Постоянный мониторинг атак и/или угроз
- Быстрая поддержка в «трудную минуту» с последующей оплатой – ИБ по факту
- Повременная оплата пользования лицензиями*

Информзащита
Системный интегратор
20 лет

SecaaS в публичных облаках

Пример реализации сервисов ИБ
в проекте Национального облака

СОИБ НОП и Сервисы ИБ

- Ростелеком. 2013 г.
- Модели угроз и нарушителя
  - для платформы
  - для сервисов ИБ
- Оркестрация сервисов ИБ, предоставляемых платформой
- Портал самообслуживания

Информзащита
Системный интегратор

20 лет

SecaaS для последней мили

Пример реализации сервисов ИБ
в проекте телеком-оператора

SecaaS на кончике провода

Цель:

- Повышение прибыли за счет продажи дополнительных сервисов ИБ

Средства:

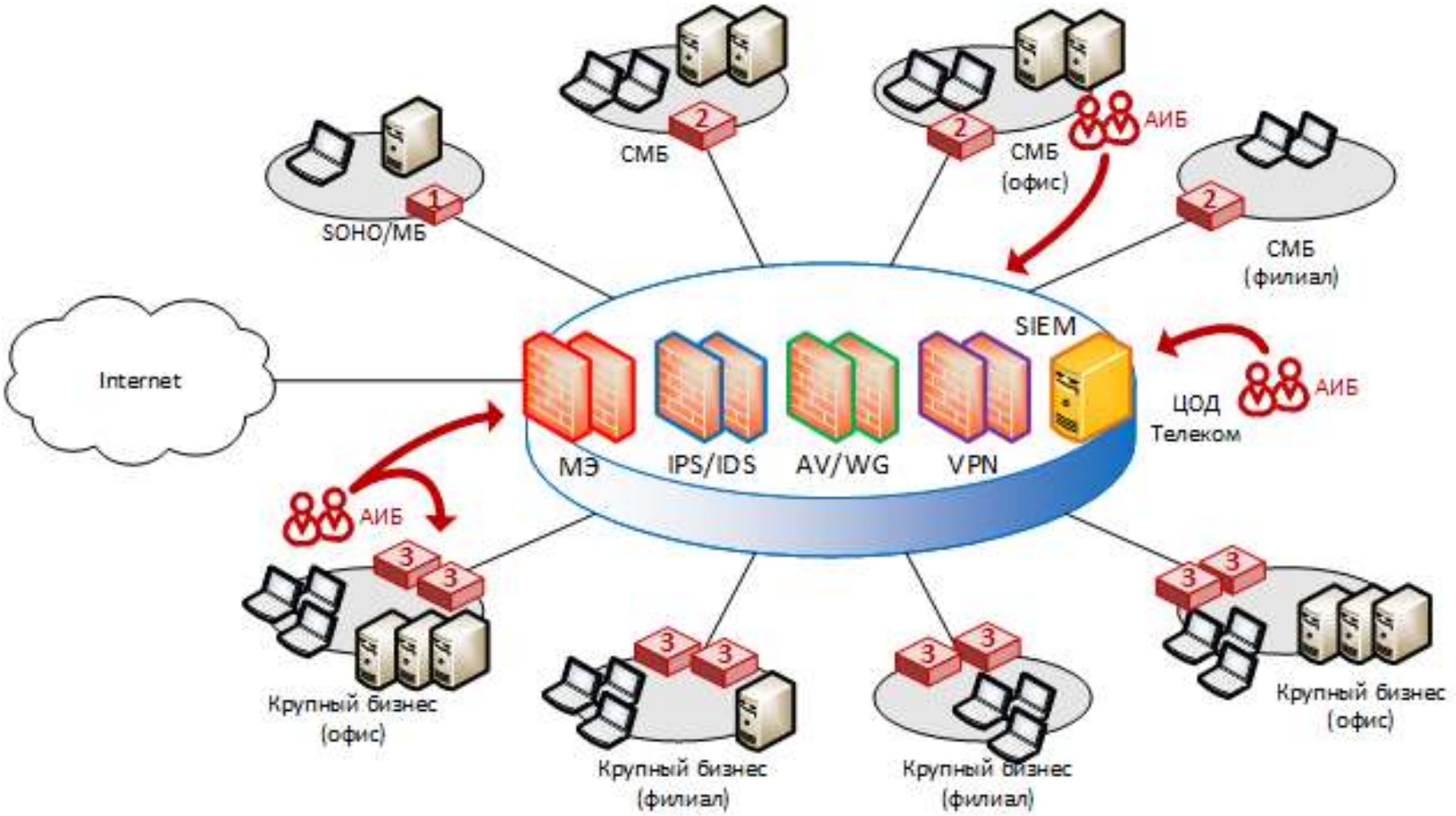
- Простые интуитивно понятные сервисы ИБ для SOHO и управляемые сервисы ИБ для SME

Сделано:

- Разработка архитектуры сервисов
- Выбор поставщика СЗИ

Информзащита
Системный интегратор
20 лет

Каждому клиенту свой кусочек безопасности



ИТОГО…

1. Ломать привычную схему и стереотипы надо.
2. Как это делать и какая из этого выгода, мы вам расскажем. НИП Информзащита

Приглашаем к сотрудничеству!

Информзащита
Системный интегратор
20 лет

Спасибо за внимание

Константин Феоктистов

ГА ДКР ЗАО НИП «ИНФОРМЗАЩИТА»

Тел: +7 (495) 980-2345

k.feoktistov@infosec.ru

Приведение ЦОДов в соответствие требованиям ИБ

как средство повышение привлекательности ЦОДов

Что происходит ?

Рынок ЦОД в настоящее время

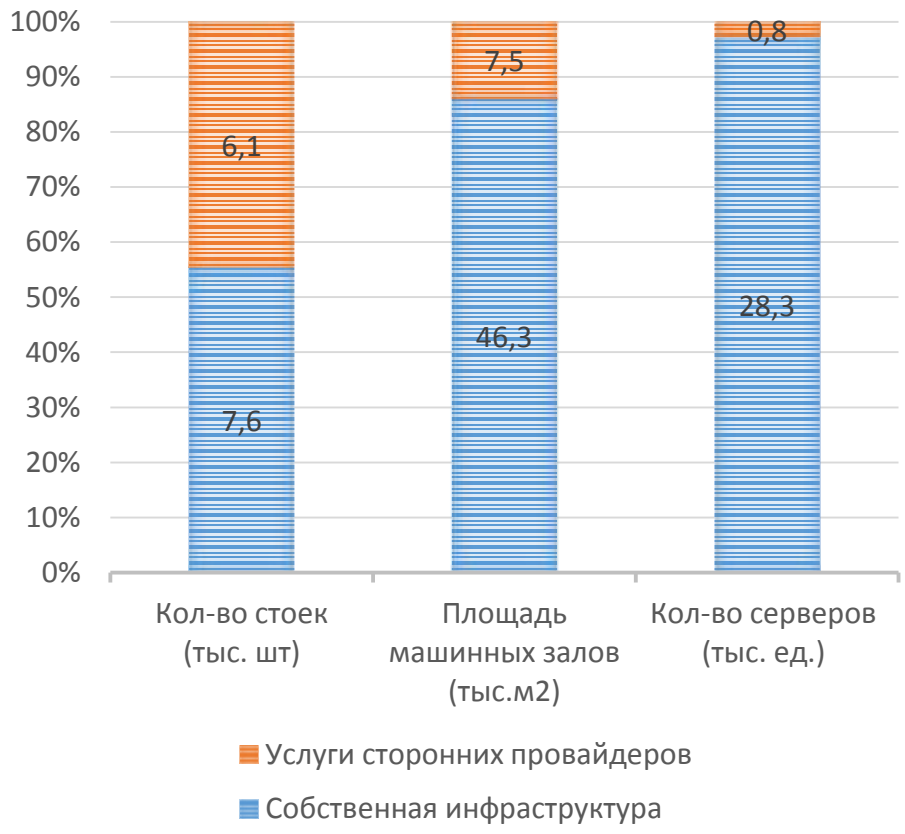
Рынок коммерческих ЦОД в России

Характеристики рынка на 2015 год:

- **180+** площадок - крупные и средние коммерческих ЦОД - **102,4** тыс. м^2
- В 2014 г + **12** новых технологических площадок - **17,4** тыс. м^2
- Среднегодовой доход ~ **0,5 млн. ₽** на стойку (42U)
- Средняя нагрузка **7-10 кВт** на стойку

Минкомсвязь России

Потребление услуг ЦОД гос. организаций



- **1,3** стойки в среднем на одну серверную комнату
- **3,7** сервера на стойку (4-14U на стойку 42U)
- 67 % стоек с потреблением менее **3 кВт**
- До **18 млрд. ₽ в год** – затраты федерального бюджета на содержание инфраструктуры

Информзащита
Системный интегратор
20 лет

Конкуренция на рынке услуг ЦОДов

- ЦОДов много, потребителей мало.
  Средняя загрузка ЦОД в РФ ~ 30%
  – высокая конкуренция
- Программа строительства ЦОД для нужд государственных и муниципальных органов к 2018г. (МКС, Правительство РФ)
  – конкуренция со стороны государства
- Обеспечить стабильный рост
  – «повернуться лицом» к ожиданиям клиентов

Информзащита
Системный интегратор

20 лет

Предпосылки

Изменение законодательства
и его последствия

Заграница не поможет

- 242-ФЗ внес изменения в 152-ФЗ в части обработки ПДн на территории РФ с 01.09.2015
- Реакция рынка – появление спроса на услуги ЦОД
- Ожидание Постановления Правительства РФ в части организации проверок порядка обработки ПДн – вопрос о полномочиях РКН

Информзащита
Системный интегратор
20 лет

Интерес заказчика

Что заказчик ожидает
от предоставляемых услуг

Интерес № 0: Реальная безопасность

Цель:

- Защита от реальных угроз на ИС клиента, размещаемые в ЦОД

Как обеспечить:

- Наличие средств защиты инфраструктуры
- Предоставление дополнительных сервисов безопасности (SecaaS) по требованию

Чем клиенту грозит неготовность:

- Финансовые и репутационные риски организации
- Потери бизнеса, клиентов, партнеров

Информзащита
Системный интегратор
20 лет

Интерес 1: Соответствие по ПДН

Чему соответствовать:

- Защита ПДн. Требования приказа №21 ФСТЭК в части 152-ФЗ

Как обеспечить:

- Привести инфраструктуру в соответствие требованиям
- Подтвердить наличием аттестата

Чем клиенту грозит несоответствие:

- Финансовые и репутационные риски организации
- Приостановка деятельности, штрафные санкции

Информзащита
Системный интегратор
20 лет

Интерес 2: Соответствие по PCI DSS

Чему соответствовать:

- Защита платежных данных. Требования PCI DSS

Как обеспечить:

- Привести инфраструктуру в соответствие требованиям
- Провести сертификацию ЦОД

Чем клиенту грозит несоответствие:

- Финансовые и репутационные риски организации
- Невозможность запуска новых сервисов

Информзащита
Системный интегратор
20 лет

Интерес 3: Соответствие по ISO 27001

Чему соответствовать:

- Процессы управления ИБ. Требований стандарта ISO 27001

Как обеспечить:

- Привести процессы управления ИБ в соответствие требованиям
- Провести сертификацию системы управления

Чем клиенту грозит несоответствие:

- Состояний защищенности не гарантировано и не подтверждено
- Несоответствие корпоративным стандартам (для западных компаний)

Информзащита
Системный интегратор
20 лет

Интерес 4: Соответствие требованиям CSA

Чему соответствовать:

- Требования безопасности для поставщиков облачных услуг. Cloud Security Alliance

Как обеспечить:

- Провести самооценку
- Реализовать требования и внедрить процессы
- Провести сертификацию

Чем клиенту грозит несоответствие:

- Состояний защищенности не гарантировано и не подтверждено
- Несоответствие корпоративным стандартам

Информзащита
Системный интегратор
20 лет

Интерес 5: Соответствие требованиям Положения 382-П

Чему соответствовать:

- Защита информации о переводах денежных средств. Требования Положения 382-П ЦБ РФ

Как обеспечить:

- Определить роль участника НПС
- Проводить оценку соответствия требованиям
- Разработать план по устранению соответствий

Чем клиенту грозит несоответствие:

- Финансовые и репутационные риски организации
- Ограничение (приостановление) оказания услуг, связанных с переводом денежных средств

Информзащита
Системный интегратор
20 лет

Наши предложения для ЦОДов

Что мы можем предложить

ЦОД, как заказчик услуг ИБ

- Разработка стандартов безопасности для ЦОД
- Сертификация для ЦОД: 27001, PCI DSS, CSA STAR
- Аттестация на соответствие требований по ПДн
- Консалтинг ЦОД на соответствие стандартам
- SOC для ЦОД
- Сервис сканирования уязвимостей
- Аудит соответствия требованиям
- Сопровождения ИБ при проверках регуляторов

Информзащита
Системный интегратор
20 лет

ЦОД, как поставщик услуг ИБ

- Реализация методологии размещения ИС заказчиков в защищенном ЦОД в соответствии с требованиями
- Разработка для ЦОД услуг по безопасности, предоставляемых клиентам ЦОД по модели сервисов (SecaaS)

Информзащита
Системный интегратор
20 лет

Организация, как заказчик услуг защищенного ЦОД

- Консалтинг клиента для размещения в ЦОД
- Разработка стандартов безопасности для размещений ИС клиентов в ЦОД
- Аудит защищенности инфраструктуры ЦОД
- Аудит соответствия требованиям ФЗ-161 (НПС) и СТО БР ИББС
- Аудит соответствия требованиям PCI DSS
- Сертификация по PCI DSS
- Обеспечение безопасности ПДн и приведение порядка обработки ПДн к соответствию требованиям
- Аудит безопасности ИС
- Сопровождения ИБ при проверках регуляторов

Информзащита
Системный интегратор
20 лет

Комплексный подход

Опыт компании Информзащита

Комплексный подход

Плюсы для ЦОД

- Формируется безопасная среда, привлекательная для клиентов
- Соответствие – это не только «бумаги и сертификаты» – это и реальная безопасность на приемлемом уровне
- Оптимизация затрат ЦОД при планомерной реализации проектов в части ИБ

Плюсы для заказчиков

- ЦОД обеспечивает базовые услуги ИБ
- Партнер ЦОД обеспечивает дополнительные услуги безопасности
- Возможность выбирать услуги ИБ в рамках своих потребностей не меняя поставщика услуг ЦОД

Информзащита
Системный интегратор
20 лет

Опыт компании Информзащита

- Проект создания **защищенной облачной среды О7** (Ростелеком)
  - Внедрение защищённой инфраструктуры Облачной платформы
  - Разработка сервисов безопасности как услуги для клиентов О7
- Партнерство с **Cloud DC** - поставщиком услуг ЦОД (Зеленоград)
  - Программа развития системы защиты ЦОД
  - Предоставления услуг безопасности клиентам ЦОД
- **DataLine** – поставщик услуг ЦОД
  - Сертификация по PCI DSS, Подготовка к сертификации ISO 27001

Информзащита
Системный интегратор
20 лет

ВЫВОДЫ

1. Рынок активно готовится к переходу клиентов в ЦОД
2. Клиенты заинтересованы в обеспечении безопасности
3. Оптимальный путь для предоставления - обеспечение соответствия
4. 20-ти летний опыт реализации процессов обеспечения ИБ
5. Мы решаем задачи комплексно, учитывая лучшие практики

Приглашаем к сотрудничеству!

Информзащита
Системный интегратор
20 лет

Обеспечение соответствия требованиям по безопасности информации ИТ-инфраструктуры

для размещения типовых информационных систем организации

Постановка вопроса

Причины возникновения вопроса?

В чем суть проблемы?

Безопасность инфраструктуры. Зачем?

- Бизнес функции организации ←
  ← Информационная система (ИС) ←
  ← Окружение / среда / условия ←
  ←Обеспечение безопасности
- Инфраструктура – основа ИС
- Безопасность инфраструктуры – база для безопасной эксплуатации и развития ИС организации
- Инфраструктура – поставщик услуг безопасности, обеспечивающих базовые требования

Информзащита
Системный интегратор
20 лет

Как решается: «Как лучше» или «Как обычно»?

Имеются угрозы безопасности ИС

~~«Нас это не касается!»~~

Касается всех

Проведите анализ защищенности /пен-тест

~~«Должно быть. Так у всех сделано»~~

Реализуем только то, что нужно

Оцените риски, смоделируйте угрозы

Информзащита
Системный интегратор

20 лет

Суть проблемы

- Создается новая ИС,
- Развиваются существующие ИС,
- Слияние/поглощение организаций с их ИС

Под каждую ИС реализуется

- собственная система защиты
- под собственные требования

Результат:

- избыточность компонентов,
- слабая управляемость,
- несогласованность,
- затраты на интеграцию

Информзащита
Системный интегратор
20 лет

Альтернативный подход:

- Создается инфраструктура
  - удовлетворяющая базовым требованиям безопасности
  - с собственной подсистемой безопасности
- Подход позволяет:
  - сократить общие затраты на ИБ
  - обеспечить унификацию подхода и платформ
  - систематизировать процессы управления ИБ
- Реализуется:
  - собственными силами организации
  - силами поставщика услуг ИБ

Информзащита
Системный интегратор
20 лет

Формирование базовых требований ИБ

Источники и консолидация

Какая безопасность вам нужна?

- Реальная безопасность…
  - … или соответствие требованиям

Информзащита
Системный интегратор

20 лет

Реальная безопасность…

- Угрозы бизнесу / деятельности организации
- Выявить проблемные мест в ИС
- Затраты на подсистему защиты.
  А оно вам «надо»?
- Чем доказать необходимость и эффективность применяемой защиты
- Когда начинать работы по реализации?

Информзащита
Системный интегратор
20 лет

… или соответствие требованиям

- Угрозы никуда не исчезли
- Соответствие требованиям регуляторов
- Существуют ли требования?
- Помогают ли они, нужны ли они

Информзащита
Системный интегратор
20 лет

Откуда берутся угрозы / требования ?

- Угрозы в реальной безопасности
- Требования в области соответствия
  - Регуляторы, нормативные документы
  - Типы ИС, обрабатываемая информация и источники требований
- Пересечение состава требований - базовый уровень обеспечения безопасности

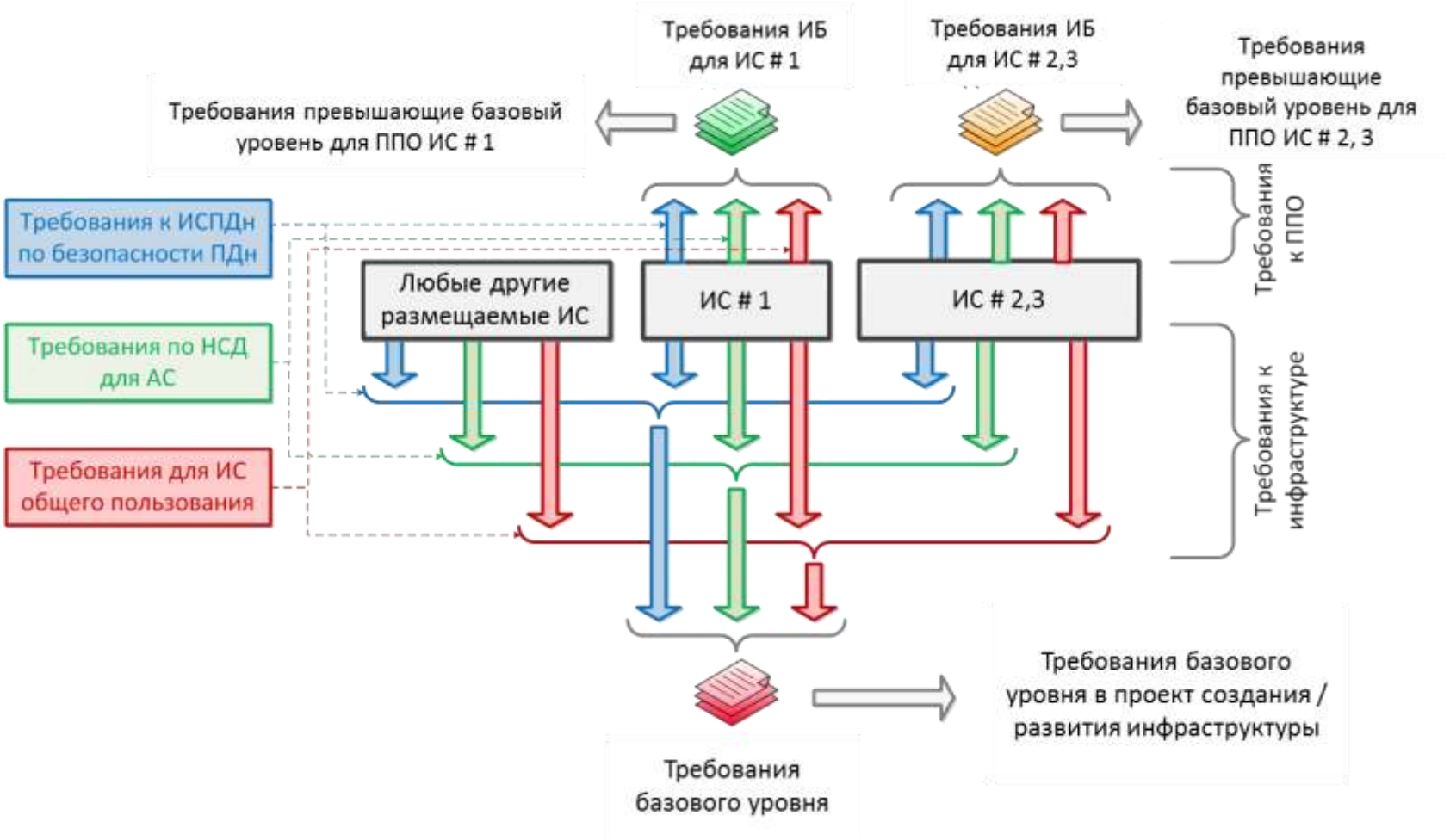
Информзащита
Системный интегратор

20 лет

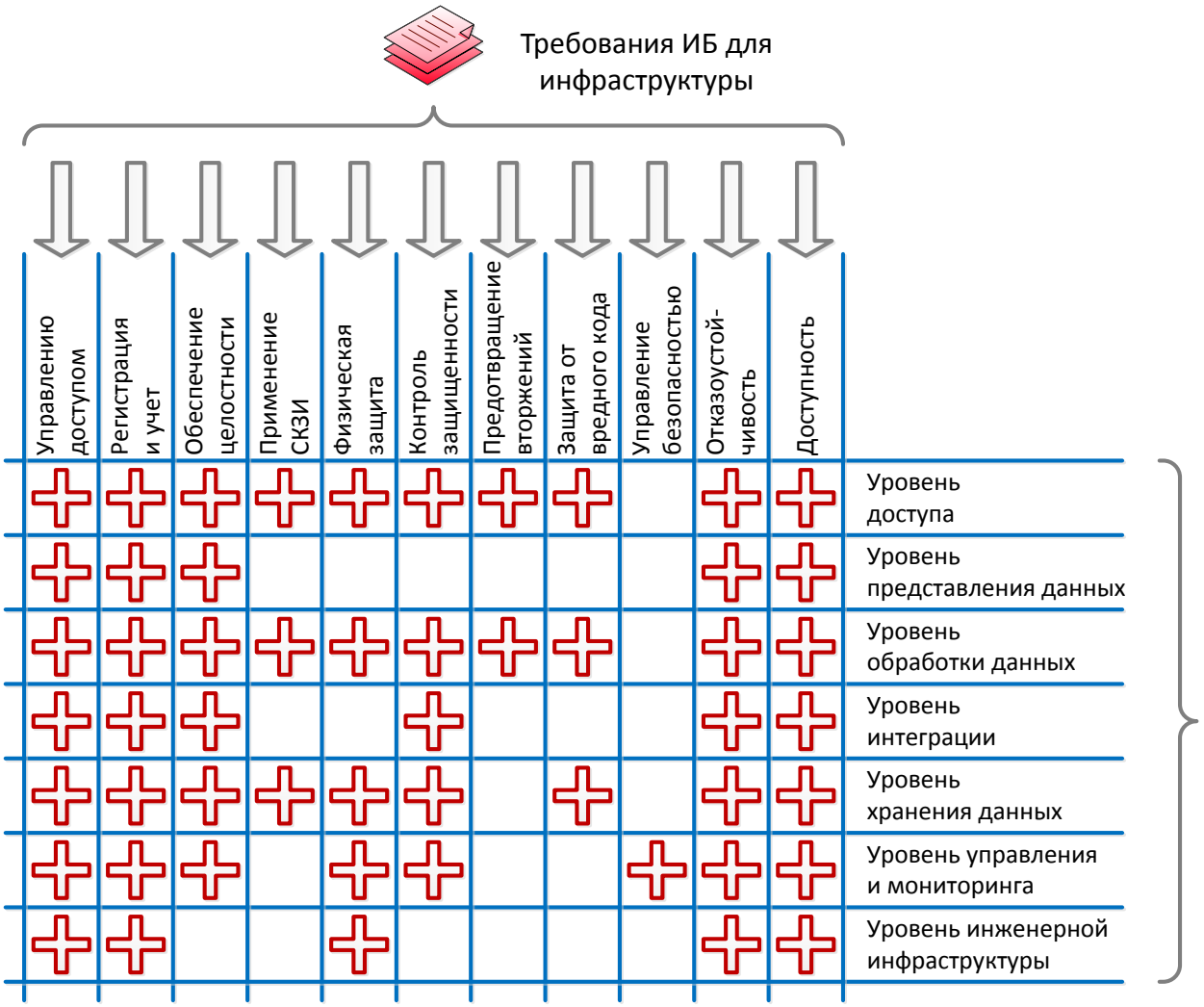
Консолидация требований ИБ к ИС

	РД по НСД АС (1Г)	Защита ИСПДн (УЗХ)	СТР-К	ISO 27001|27002	BSI 25999|ISO 25777	TIA/EIA-942 (Tire III)	Пр. 416/489 (Класс 1)	Результирующие требования
Требования по управлению доступом	+	+	+	+		+		+
Требования по регистрации и учету	+	+	+	+				+
Требования по обеспечению целостности	+	+		+				+
Требования по защите от вредоносного кода		+		+				+
Требования по защите межсетевого взаимодействия		+		+				+
Требования по использованию СКЗИ	+		+	+				+
Требования к техническим средствам		+	+					+
Требования к использованию СЗИ		+	+					+
Требования по организации обеспечения ИБ			+	+	+			+
Требования к надежности и доступности				+		+		+
Требования к ИС общего пользования							+	+
Требования непрерывности бизнеса и восстановлению после сбоев				+	+	+		+

Выделение базовых требований ИБ



Распределение базовых требований по уровням архитектуры



Распределение базовых требований по уровням инфраструктуры

Реализация базовых требований ИБ

Защитим!
Методы достижения

Защитный меры

- Организационные
  - персонал
  - оргструктура
  - процессы безопасности
  - функции
- Технические
  - архитектура
  - автоматизация процессов
  - средства защиты

Средства защиты

Телеком. инфраструктура		Подключение провайдеров	МЭ IPS VPN DDoS AV КЗ SIEM IDM SC
		Подключение ведомств	МЭ IPS VPN КЗ SIEM
Сетевая инфраструктура		ЛВС ЦОД ФНС	МЭ IPS AV КЗ SIEM ФБ
		ЛВС ИИСЭБ	МЭ IDS AV КЗ SIEM IDM SC DLP ФБ
Вычислительная инфраструктура	Виртуальная среда	Уровень ОС	HIDS AV НСД ЭЗ КЗ SIEM IDM SC DLP
		Уровень гипервизора	МЭ IPS AV НСД КЗ SIEM
		Уровень серверного оборудования	HIDS AV НСД ЭЗ КЗ SIEM ФБ
Инфраструктура хранения данных		Сеть хранения	НСД КЗ SIEM ФБ
		Хранилища данных	НСД КЗ SIEM ФБ
		Архивы и резервные копии	Орг.Меры SIEM IRM ФБ
Инфраструктура контроля и управления		Система монторинга	МЭ AV КЗ SIEM
		Система управления	МЭ HIDS VPN AV НСД КЗ SIEM IDM SC DLP ФБ
Инфраструктура репликации ЦОДов		На уровне ЛВС	VPN SIEM
		На уровне СХД	SIEM
Инженерная инфраструктура		Комплексные сист. безопасности	SIEM IDM ФБ
		Гарантированное обеспечени	ФБ

МЭ	Мэжсетевое экранирование
IPS	Предотвращение вторжений
IDS	Обнаружение вторжений
HIDS	Обнаружение вторжений на уровне хоста
VPN	Создание VPN
DDoS	Предотвращение атак типа «отказ в обслуживании»
AV	Защита от вредоносного кода (антивирусные средства)
НСД	Защита от несанкционированного доступа
ЭЗ	Доверенная загрузка и обеспечение целостности ПО
КЗ	Контроль защищенности
SIEM	Управление событиями ИБ (SIEM)
IDM	Управление учетными данными пользователей
IRM	Управление правами доступа к данным
SC	Усиленная аутентификация (Smart Card|USB Token)
DLP	Предотвращение утечки данных
ФБ	Физическая безопасность элементов

Извечный русский вопрос…

- «Кто виноват?»
- «Что делать?»
- … 21 век: «И чо?»

Информзащита
Системный интегратор

20 лет

Что делать?

- Реализация базового уровня:
  - Организационных мер
  - Технических мер
  - СЗИ и КСЗИ
    - сертифицированные
    - несертифицированные
- Где взять знания/компетенции:
  - Своими силами – собственные службы ИБ
  - Чужими руками – поставщик услуг ИБ

Информзащита
Системный интегратор
20 лет

ВЫВОДЫ

1. Инфраструктура, отвечающая базовым требованиям ИБ снижает общее расходы на создание и развитие ИС
2. Организация может самостоятельно реализовать Базовые требования ИБ или с привлечением поставщиков услуг ИБ

Приглашаем к сотрудничеству!

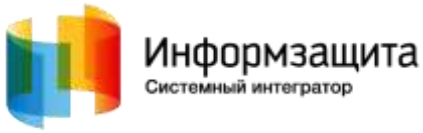
Информзащита
Системный интегратор
20 лет

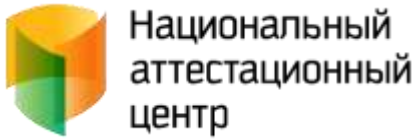
«Информзащита»

свобода в решениях,
безопасность в бизнесе

ГК «Информзащита»

Группа компаний «Информзащита» специализируется в области обеспечения безопасности информационных систем и уже 20 лет является лидером российского рынка ИБ.





«Информзащита» сегодня

Наши заказчики

Федеральная таможенная служба

Федеральное казначейство РФ

Министерство финансов РФ

Банк России

РОСГОССТРАХ

СБЕРБАНК

Ростелеком

Билайн

Российские железные дороги

Альфа-Банк

ВТБ

UniCredit Bank

АЛЬФА СТРАХОВАНИЕ

Allianz

X5 RETAIL GROUP

Coca-Cola

СОГАЗ СТРАХОВАЯ ГРУППА

JTI

Ашан

НОРИЛЬСКИЙ НИКЕЛЬ

IKEA

TOYOTA

КИТФинанс

Ключевые партнеры

Код Безопасности
ГК «Информзащита»

IMPERVA

infotecs

INFOWATCH
BECAUSE YOUR DATA IS YOUR BUSINESS

KASPERSKY lab

IBM

intel Security

POSITIVE TECHNOLOGIES

websense
ESSENTIAL INFORMATION PROTECTION™

observe it
people audit

Аладдин рд

Symantec.

Check Point
SOFTWARE TECHNOLOGIES LTD.

КРИПТО ПРО

paloalto
NETWORKS
the network security company™

BalaBit
IT Security

BLUE COAT

CISCO

TREND MICRO

ORACLE

VARONIS

CYBERARK

Лицензии и сертификаты

Высокое качество предоставляемых услуг подтверждается наличием лицензий и аккредитаций на полный спектр услуг по защите информации начиная от разработки средств защиты и заканчивая аттестацией готовых систем.

Компания активно принимает участие в работе экспертных групп, направленных на формирование нормативной базы в области защиты информации.

Спасибо за внимание

Константин Феоктистов

Главный архитектор
Департамент комплексных решений
ЗАО НИП «ИНФОРМЗАЩИТА»

Тел: +7 (495) 980-2345

k.feoktistov@infosec.ru