Yandex Cloud

Персональные данные в «облаке». Безопасность и соответствие требованиям

Андрей Иванов

Руководитель направления развития
сервисов информационной безопасности

Программа

01 Концепция

02 Планирование и реализация

03 Подтверждение соответствия

04 Заключение

01

Концепция

Платформенное решение

SaaS

Магазин партнёрских приложений и сервисов (Yandex.Cloud Marketplace)

PaaS

Управление данными и аналитика

Инструменты управления и разработки

Сервисы машинного обучения

IaaS

Идентификация и безопасность

Виртуальные машины и контейнеры

Объектное и блочное хранилища

Сеть и доставка контента

Соответствие законодательным и индустриальным требованиям

152 ФЗ, УЗ-1. Аттестат соответствия по требованиям 21-го приказа ФСТЭК.

Соответствует для Евросоюза

bsi.

ISO/IEC 27001
Information Security Management

ISO/IEC 27017
Security Controls for Cloud Services

ISO/IEC 27018
Protection of Personally Identifiable Information

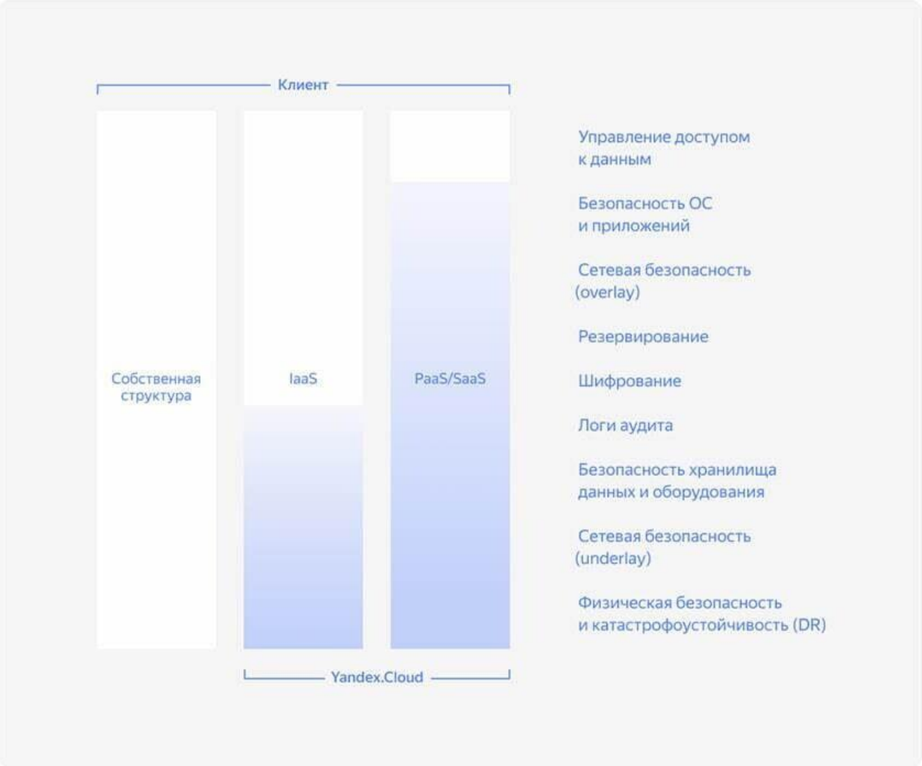
Реестр отечественного ПО

PCI DSS COMPLIANT

Для ЦОД и облачных сервисов

ГОСТ 57580. Безопасность финансовых (банковских) операций

Разграничение ответственности



При переезде в «облако» меняются зоны ответственности

- Инфраструктурную и managed-часть, как правило, берёт на себя провайдер
- Прикладное ПО и любые дополнительные сервисы – за заказчиком

02

Планирование и реализация

Общий план. Часть 1

Категории ПДн		Специальные			Биометрические	Иные			Общедоступные		
Собственные работники		Нет	Нет	Да		Нет	Нет	Да	Нет	Нет	Да
Количество субъектов		Более 100 тыс.	До 100 тыс.			Более 100 тыс.	До 100 тыс.		Более 100 тыс.	До 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Из Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

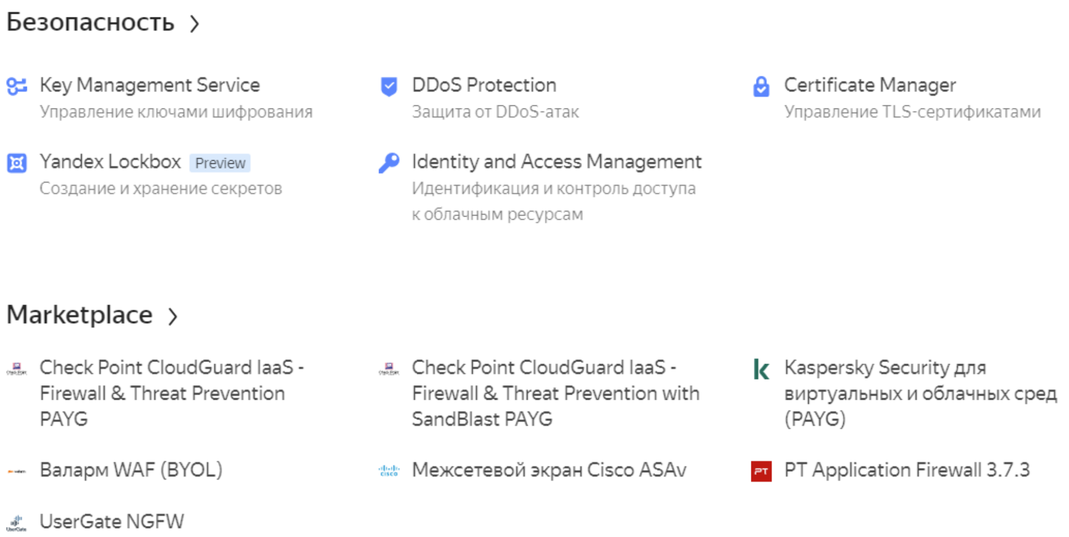
На этапе планирования размещения системы в «облаке» – стандартные процедуры

- Выбор уровня защищённости
- Моделирование угроз

Тут следует учесть, что не стоит использовать модель угроз провайдера. Необходимо разработать свою, учитывая тот факт, что провайдер обеспечил защиту от угроз, актуальных для облачной инфраструктуры.

https://storage.yandexcloud.net/yc-compliance/recomendations/FZ-152-RU.pdf

Общий план. Часть 2



Определиться с СЗИ

- Требования 21 Приказа
- Понимать, какие меры какими средствами будут реализованы
- Понимать, какие сервисы «облака» могут помочь
- Уточнить правильные настройки для ПО
- Уточнить варианты по «привнесению» собственных средств (в Yandex.Cloud, например, доступны решения из Marketplace)

https://storage.yandexcloud.net/yc-compliance/conformance_ru_pdp.pdf

Общий план. Часть 3

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		
ИАФ.5	Защита обратной связи при вводе аутентификационной информации		

Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.1	Учет машинных носителей персональных данных	На уровне физических носителей информации, применяемых в рамках Платформы.	Не применимо
ЗНИ.2	Управление доступом к машинным носителям персональных данных	На уровне физических носителей информации, применяемых в рамках Платформы.	Не применимо

Понять свою зону ответственности

- Требования выполняются как на инфраструктурном уровне платформы, так и на уровне большинства сервисов
- Например, мы в Yandex.Cloud используем таблицу, где указано, что выполняется на стороне провайдера, а что должен делать клиент на своей стороне

Общий план. Часть 4

Соглашение об обработке данных

Настоящий документ (далее — «Соглашение») является неотъемлемой частью Договора на использование сервисов Платформы «Яндекс.Облако» (далее — «Договор»), заключаемого между Яндексом и Клиентом в терминологии Договора и документа, размещенного в сети «Интернет» по адресу: https://yandex.ru/legal/cloud_oferta, и устанавливает порядок обработки Яндексом персональных данных по поручению Клиента.

Все термины и определения, встречающиеся в тексте Соглашения, толкуются в соответствии с Договором, действующим законодательством Российской Федерации и сложившимися в сети Интернет обычными правилами толкования соответствующих терминов.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. Клиент, как оператор персональных данных, несет полную ответственность перед субъектом персональных данных за действия, осуществляемые Яндексом при обработке персональных данных субъекта по поручению Клиента.

4.2. Яндекс несет ответственность перед Клиентом, в пределах, установленных Договором, за действия в отношении обработки персональных данных субъектов по поручению Клиента, в том числе за действия (бездействие) своих работников, получивших доступ к обрабатываемым по поручению Клиента персональным данным, повлекшие разглашение таких персональных данных.

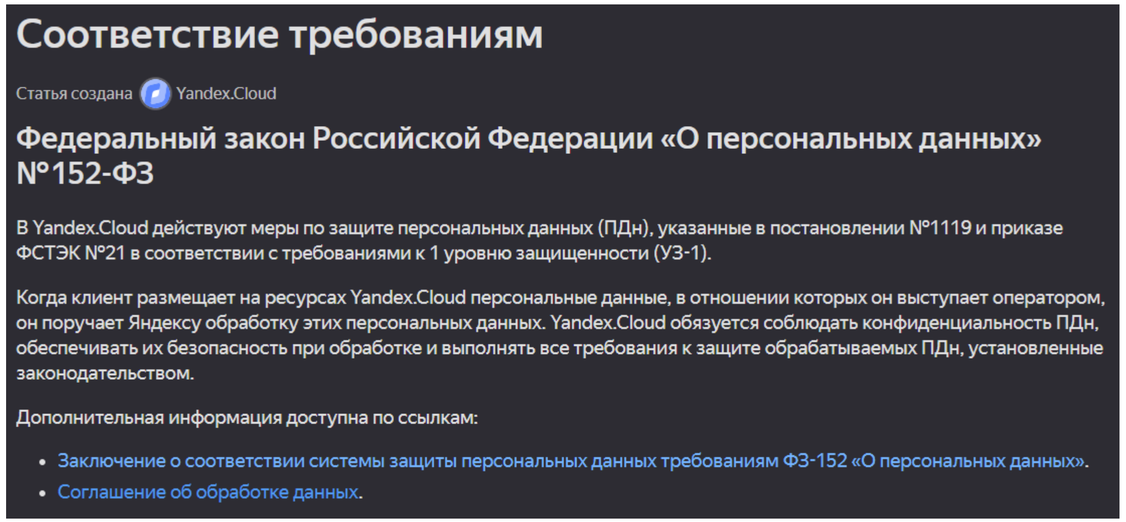
Позаботиться о документальной «обвязке» процессов

- Прописать документально зоны ответственности
- Например, мы в Yandex.Cloud ссылаемся на таблицу разграничения ответственности

03

Подтверждение соответствия

Вопросы соответствия и аттестации



Соответствие требованиям

Статья создана Yandex.Cloud

Федеральный закон Российской Федерации «О персональных данных» №152-ФЗ

В Yandex.Cloud действуют меры по защите персональных данных (ПДн), указанные в постановлении №1119 и приказе ФСТЭК №21 в соответствии с требованиями к 1 уровню защищенности (УЗ-1).

Когда клиент размещает на ресурсах Yandex.Cloud персональные данные, в отношении которых он выступает оператором, он поручает Яндексу обработку этих персональных данных. Yandex.Cloud обязуется соблюдать конфиденциальность ПДн, обеспечивать их безопасность при обработке и выполнять все требования к защите обрабатываемых ПДн, установленные законодательством.

Дополнительная информация доступна по ссылкам:

- Заключение о соответствии системы защиты персональных данных требованиям ФЗ-152 «О персональных данных».
- Соглашение об обработке данных.

Подготовиться к процедуре оценки соответствия

- Убедиться, что в рамках своей зоны ответственности всё настроено и работает корректно
- Иметь доступ к заключению о соответствии ИС провайдера требованиям ФЗ (в форме, предусмотренной законодательством РФ)

На этом этапе необходимо понимать, что всё, что касается зоны ответственности провайдера, уже прошло проверку (следствием которой является аттестат или заключение о соответствии в другой форме). Следовательно, нужно сфокусировать усилия на своей части.

04

Заключение

Напоследок…

В новом «облачном» подходе нет ничего такого, что не объяснялось бы здравым смыслом. Нужно просто помнить об изменениях и держать в голове следующее:

- Разделение ответственности
- Моделирование угроз
- Выполнение части требований 21-го приказа на стороне провайдера
- Использования «облачных» СЗИ, где возможно
- Юридические вопросы

Yandex Cloud

Спасибо! Q&A

Андрей Иванов

Руководитель направления развития
сервисов информационной безопасности

andriva@yandex-team.ru