

Технические средства ОРМ для провайдеров
хостинга

Как компаниям жить с новым
введенным регулированием



ВИМАНА
Научно-технический центр

Действующее нормативно-правовое регулирование для провайдеров хостинга

 Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.11.2023 № 935

«Об утверждении требований к вычислительной мощности, используемой провайдером хостинга, для проведения уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач»

ФЗ от 27.07.2006 №149-ФЗ:

- 1) ст. 2. п.18 – определение провайдера хостинга
- 2) Ст. 10.2-1 – требование к реализации TC OPM

 Постановление Правительства Российской Федерации от 22.11.2023 г. № 1952

«Об утверждении Правил взаимодействия провайдеров хостинга с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации»

 Постановление Правительства Российской Федерации от 29.11.2023 № 2011

«Об утверждении Правил прохождения идентификации и (или) аутентификации лицами, обратившимися к провайдеру хостинга в целях получения вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети "Интернет»

Текущая эволюция НПА с начала 2025г и общий тренд

У провайдеров хостинга

- ✦ В процессе принятия Приказ о типовом плане мероприятий внедрения ТС ОРМ
- ✦ Изменение кодекса об административных правонарушениях с введением штрафов с 1 ноября 2025г для провайдеров хостинга не входящих в реестр

У операторов связи и ОРИ

- ✦ Изменение срока хранения информации для организаторов распространения информации на 3 года (01.04.2025 N 41-ФЗ), изменения об IP-портах в ПП РФ 1526 от 09.10.2024
- ✦ Начало действия с 1 декабря 2024г ПП РФ от 22.11.2024 №1604 о выдаче заключения о соблюдении операторами требований к реализации СОРМ

Требования Приказа №935: требования к накоплению и сборка цепочек

Статистическая информация о фактах взаимодействия пользователей - 1 год

- о фактах взаимодействия пользователей сети Интернет с информационными ресурсами, созданными в ИС провайдера хостинга пользователями провайдера хостинга
- о фактах взаимодействия пользователей услуг провайдера хостинга с пользователями сети Интернет в течение одного года со дня осуществления действий.

Информация об оказанных услугах – 1 год

- о фактах авторизации и выхода из ИС провайдера хостинга, прекращения регистрации
- информация, фиксируемая в ИС провайдера хостинга об оказанных пользователям услугах

Справочная информация

3 года

Регистрационные данные пользователей

Сборка цепочек о фактах взаимодействия:

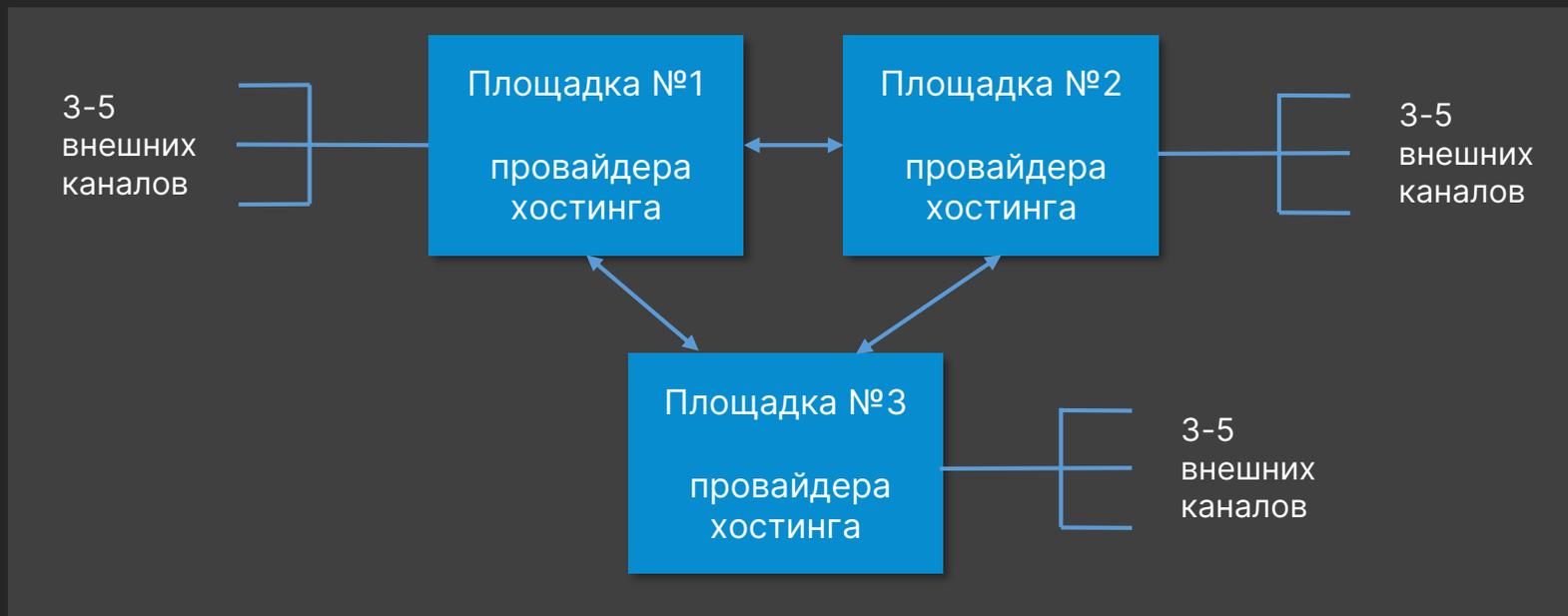


L7-балансировка, криптошлюзы и проблематика арендных DDoS + WAF



Площадки, каналы: как построить ТС ОРМ и иметь прозрачный OPEX при эксплуатации

Пример типовой инфраструктуры
(средний провайдер хостинга с 3 площадками и 3-5 каналов на площадке)



Разбираемся в объеме трафика на площадку



Разбираемся о назначении межплощадочного трафика

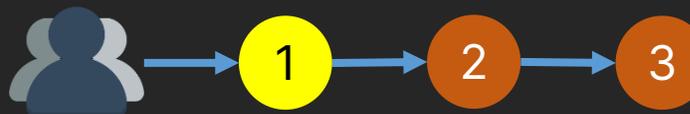


Определяем где размещать оборудование – выпадающие из работы U и электропитание



Проверяем доступную полосу для передачи информации на другую площадку

Сборка цепочек о фактах взаимодействия:



ТС ОРМ без съемника: как жить когда его некуда ставить



ВИМАНА
Научно-технический центр

Сбор данных ТС ОРМ осуществляется с каждого продукта в составе программных стеков по услугам



Реализация Приказа №935 не предполагает использование устройств съема аналогично операторам связи – отсутствуют точки установки

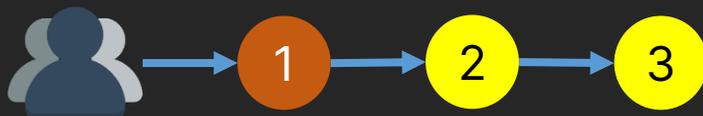


Сбор информации выполняется индивидуально с каждого сервиса и продукта, закрепляется в проектном решении по внедрению ТС ОРМ

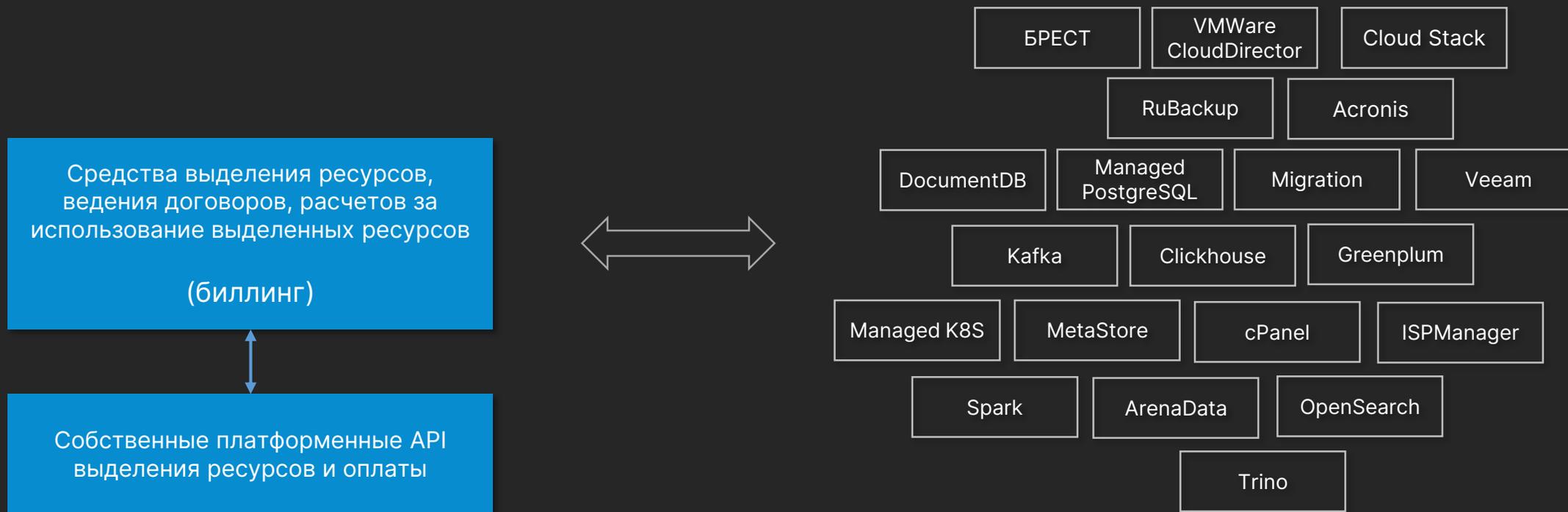


Более сложные (юридически и технически) – сервисы умного города (умный домофон, умный двор), предоставляемые провайдерами хостинга, также подпадают под Приказ №935

Сборка цепочек о фактах взаимодействия:



Сервисы «под капотом»: большой объем инфраструктурного и платформенного ПО



- ❖ Сбор информации с каждого сервиса об оказанных пользователям услугах наша основная работа при внедрении TC OPM
- ❖ Организация передачи обновлений информации из собственного ПО выполняет провайдер хостинга

Вопросы НСД и исполнений решения – требования Приказа №935

Реализация в виде программных модулей в составе ИС провайдера хостинга

Отдельный аппаратно-программный комплекс

Комбинированное исполнение



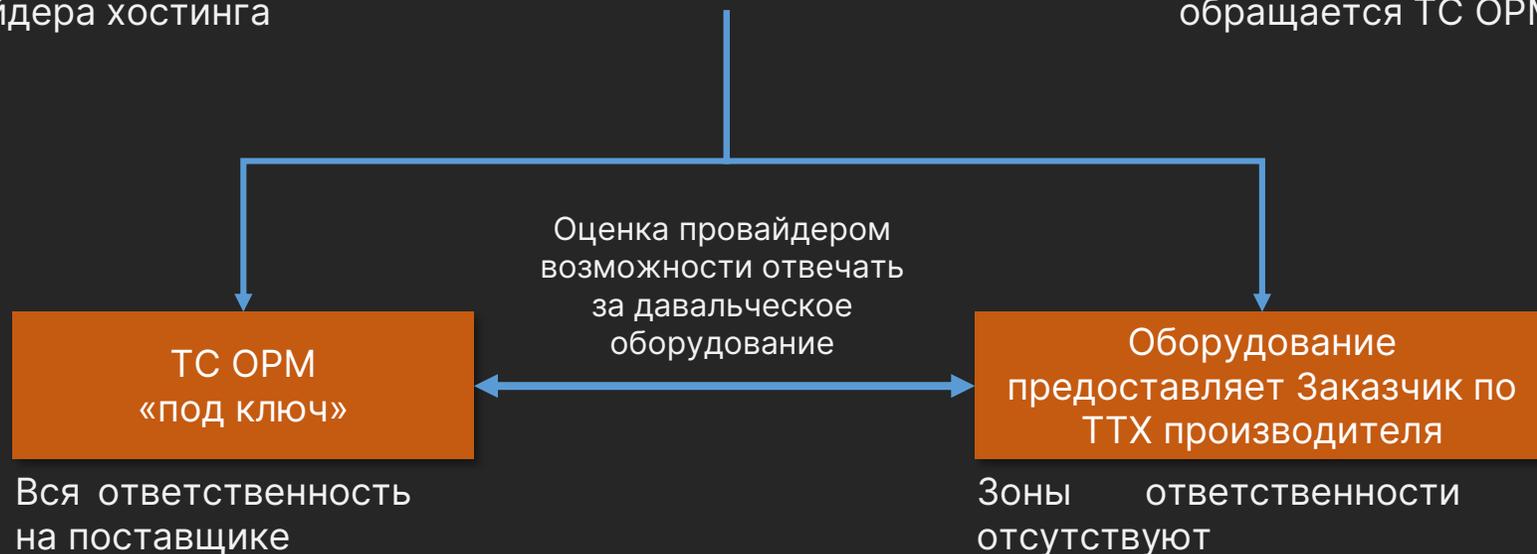
Все вопросы защиты критериев поиска – на всем персонале провайдера хостинга



Максимальное обеспечение безопасности



Защита только части внутренних ресурсов к которым обращается ТС ОРМ





ТС ОРМ «Ящер-935»: реализация действующего регулирования

- ❖ ТС ОРМ интегрируется в текущую операционную деятельность, условно – как SIEM специального назначения, работу которого необходимо планировать аналогично другим видам деятельности
- ❖ При вводе в эксплуатацию нового сервиса необходимо расширение адаптеров данных получения информации с инфраструктурного ПО нового сервиса

Варианты исполнения ТС ОРМ «Ящер-935»



ВИМАНА
Научно-технический центр

Небольшие
компании и ИП



Пьедестальная
платформа/4U

Средние компании



Стандартная
1/2U платформа

2-4 сервера

Крупные компании



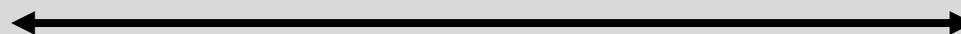
Стандартная
1/2U платформа

4-10 серверов

Федеральные компании



Максимально
компактная
реализация



Стандартные 19' x86 сервера

Российское ОСР
v3
оборудование



ВИМАНА

Научно-технический центр

Запрос расчета проекта
ТС ОРМ «Ящер-935» по адресу:

