UGaaS

Артур Салахутдинов
Руководитель направления MSSP

Artur.salah@usergate.ru
8 800 500 40 32 | доб. 9907

MaaS

UCaaS

PSSP

SaaS

UserGate как услуга

IDaaS

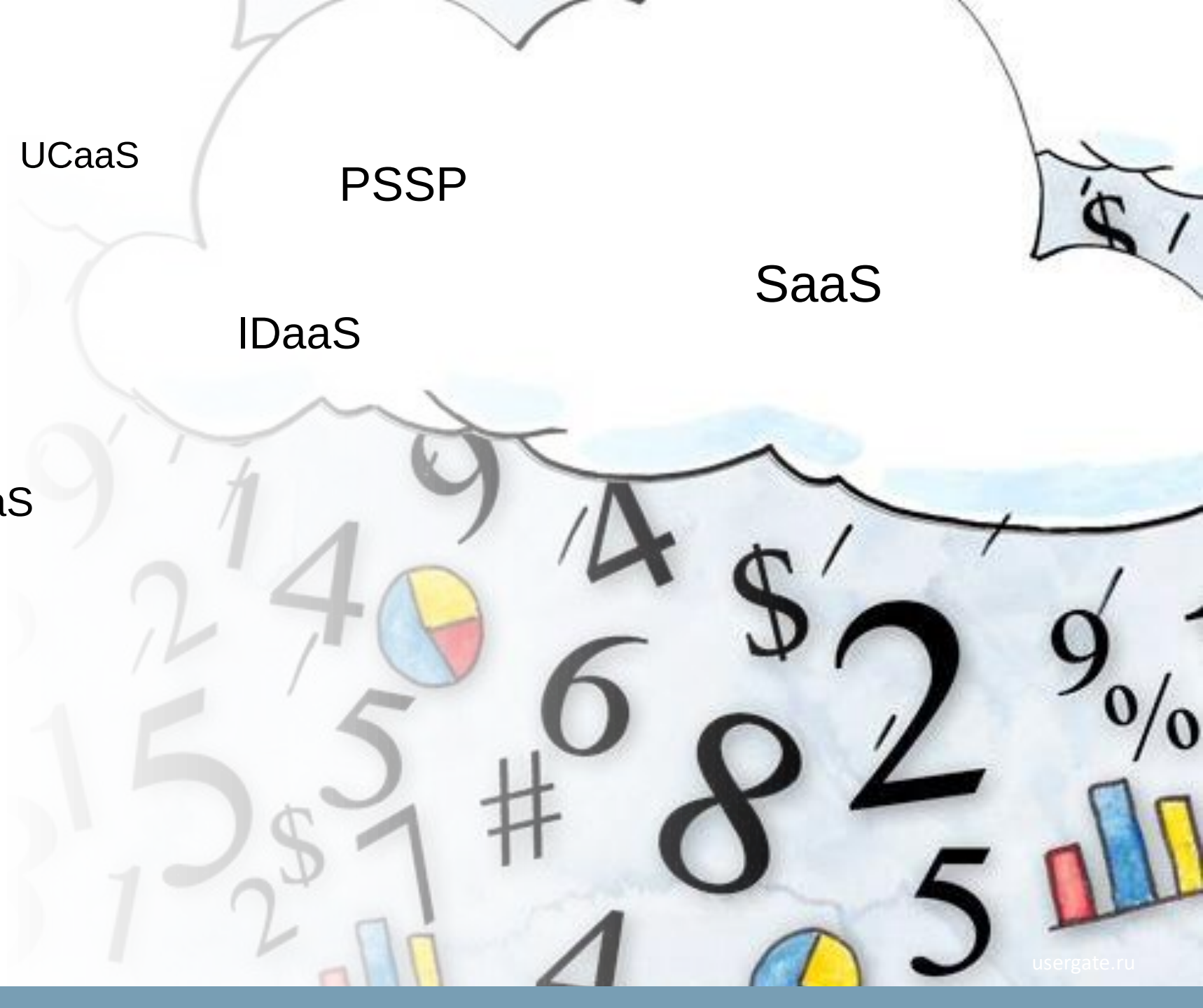
PaaS

DBaaS

FaaS

SOC

ITaaS



Целевая аудитория

1. KAV - СМБ (до 200 польз) и Пользователи интернет
2. Отраслевые ГК – (РосАтом, РосТех, РЖД и пр)
3. Распределенные ГОС-структуры
4. Средний СМБ – (Ритейл, Сети)

До 2010 года

Компания Entensys разрабатывала популярные программные решения под Windows-платформу для малого и среднего бизнеса (более 50 тысяч организаций)

2010 год

Произошла смена стратегии, началась разработка кроссплатформенного решения нового поколения, в том числе адаптированного для использования в виртуальных средах

2013 год

Был выпущен UserGate Web Filter, который стал использоваться крупнейшими операторами связи и провайдерами публичного WiFi, университетами, школами (около 14 тысяч школ)

2016 год

Выпущен UserGate UTM, комплексное решение по интернет-безопасности, разработанное как развитие уже опробованной на сетях операторов связи платформы

Настоящее время

Ребрендинг UserGate — российский разработчик программного обеспечения и микроэлектроники

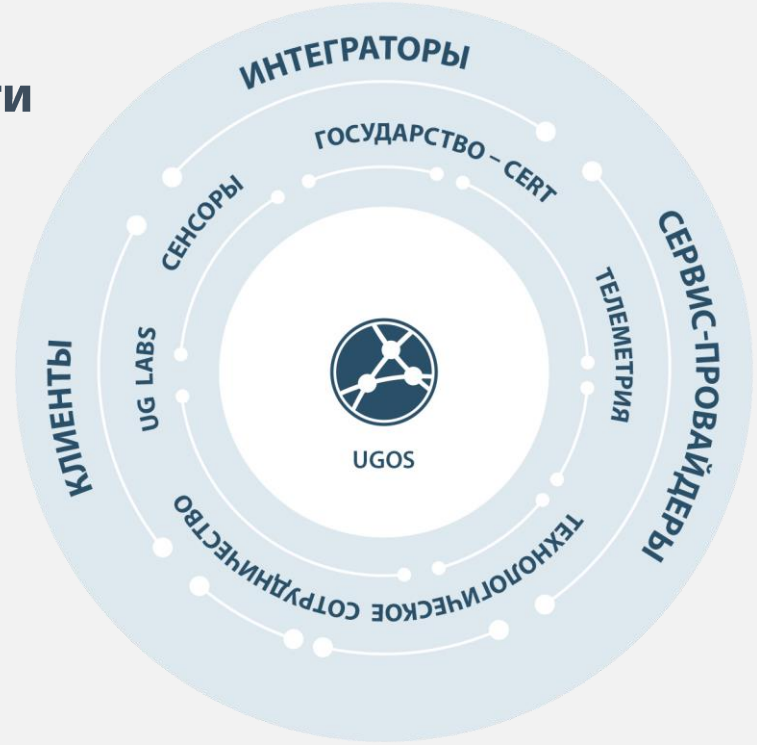
- Не уступает мировым лидерам
- Активное развитие партнерской сети/площадки сертификации
- Сертификат ФСТЭК России
- Участник проекта ГосСопка Импортозамещение

Центр мониторинга и реагирования UserGate (MRC-UG) – это команда специалистов по информационной безопасности, которая занимается исследованием сетевых угроз. Командой используются сведения из многочисленных открытых источников, получаются данные от всевозможных платных подписок, баз уязвимостей, а также за счет технологического партнерства с другими компаниями. MRC-UG обладает собственными ловушками (honeypots), на базе которых ведется изучение актуальной противоправной активности в интернете.

Источники информации об инцидентах безопасности

UserGate создает свои сигнатуры на основе:

- образцов вредоносного трафика;
- публичных proof of concept на уязвимости;
- информации от различных CERT;
- анализа собираемых IoC.



Защита от угроз
(Threat protection)

Межсетевой экран
(Enterprise Firewall, NGFW)

Анализ угроз
(Поддержка концепции SOAR)

Операционная система UGOS

Интернет-фильтрация
(Internet filtering)

Защита от атак, безопасность дата-центров
(IPS)

Виртуальная частная сеть
(VPN)

Безопасность почты
(Mail Security)

Высокая отказоустойчивость и кластеризация
(High Availability and Clustering)

Сертифицировано ФСТЭК РОССИИ

Поддержка АСУ ТП
(SCADA)

Контроль доступа
в интернет

Гостевой портал

NEW
UserGate Management
Center

Контроль приложений
на уровне L7

Безопасная
публикация ресурсов
и сервисов

Идентификация
пользователей

NEW
UserGate
Log Analyzer

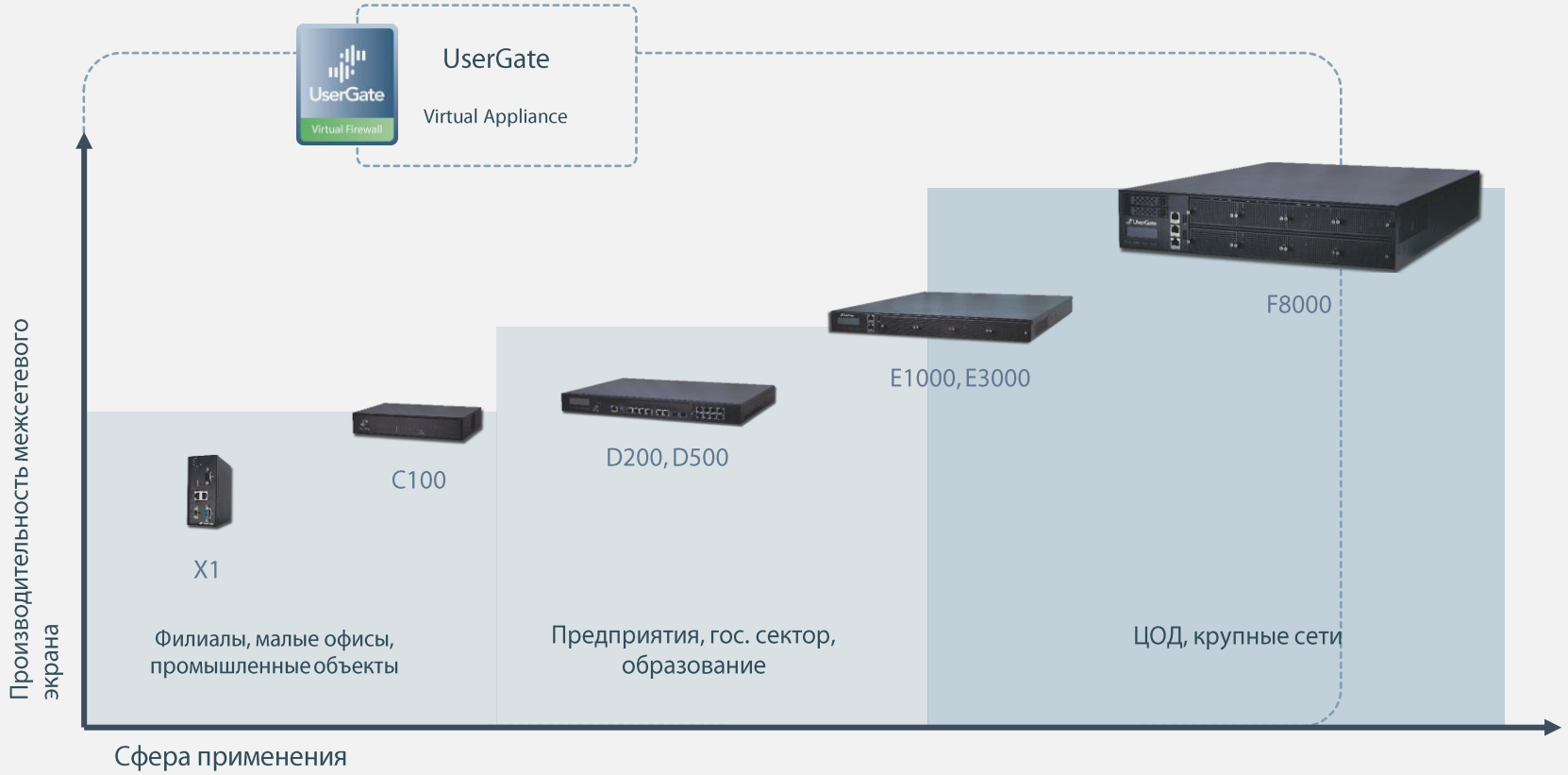
Дешифрование
SSL

Антивирусная
защита

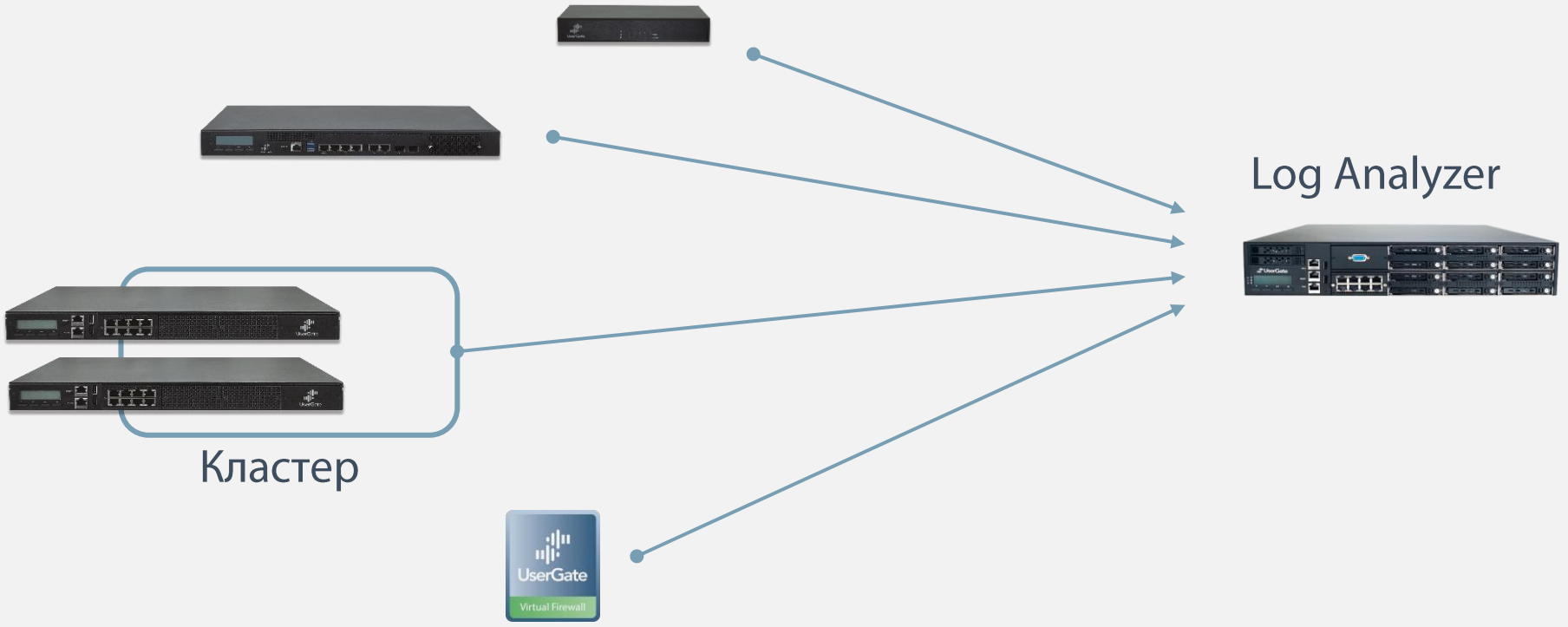
Контроль мобильных
устройств, поддержка
концепции BYOD

Работа решений линейки UserGate основана на одноименной платформе, доступной в виде виртуального решения (готового образа для VMware, Hyper-V и др. систем виртуализации) или в виде appliance, то есть программно-аппаратного комплекса.

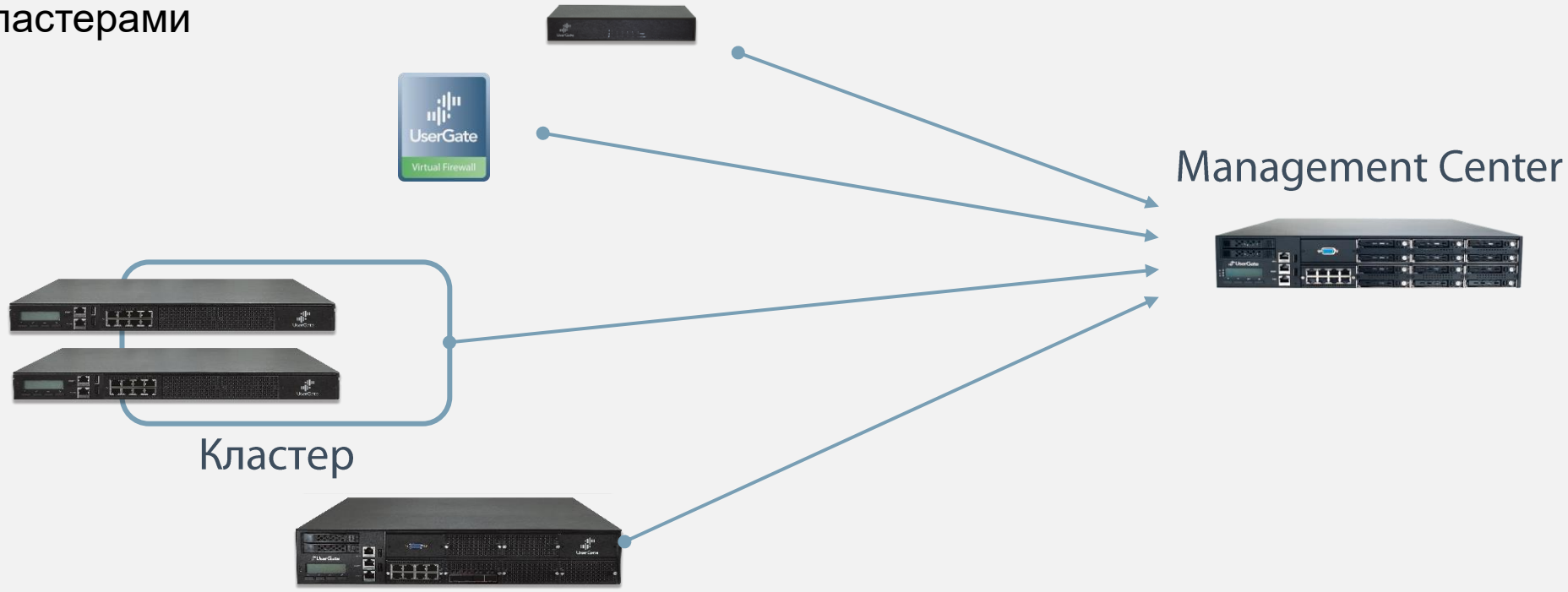
ПАК в MSSP не участвует.



- Сбор логов с устройств UserGate
- Сбор логов с любых сетевых устройств по SNMP
- Построение Dashboards
- Построение собственных отчетов



- Единый сервер управления
- Поддержка облачной платформы управления
- Применение общих политик и настроек
- Поддержка распределенного парка межсетевых экранов
- Создание управляемых областей
- Управление кластерами



Модель	VE100	VE250	VE500	VE1000	VE2000	VE4000	VE6000
Пользователей	100	250	500	1000	2000	4000	-
FW, Гбит/с	0,8	1600	1800	2000	2800	3000	3200
IPS (COB), Мбит/с	600	1300	1350	1400	1800	2100	2400
DCI, Мбит/с	150	1300	1500	1700	2000	2400	2700
Контроль Приложений L7, Мбит/с	700	1500	1700	1800	2500	2800	3100
Инспектирование SSL, Мбит/с	50	300	1100	1600	2000	2100	2700
IDS (COB), Мбпс	800	1700	2000	2500	3000	3200	3400

Каналы продаж

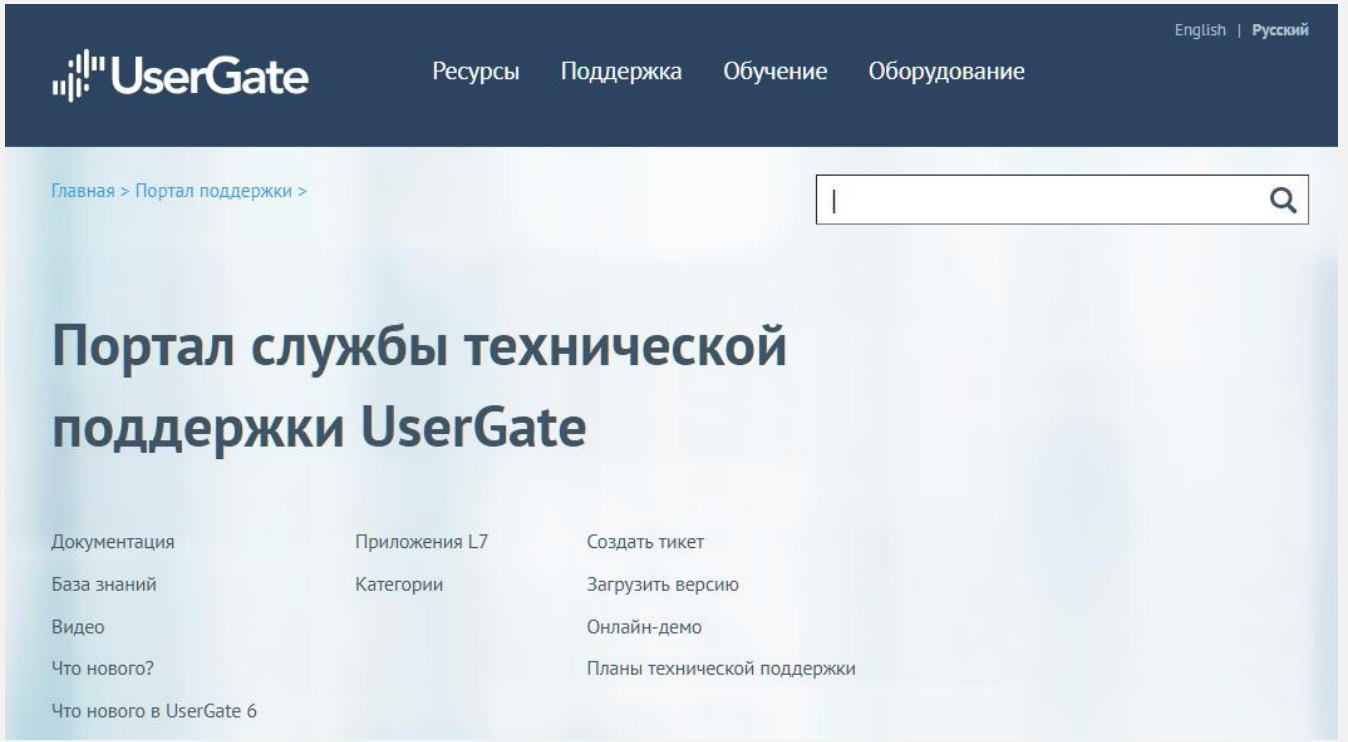
1. Интеграторы ИБ - Профессиональный Сервис

2. Непубличные (ведомственные) корпоративные операторы\интеграторы

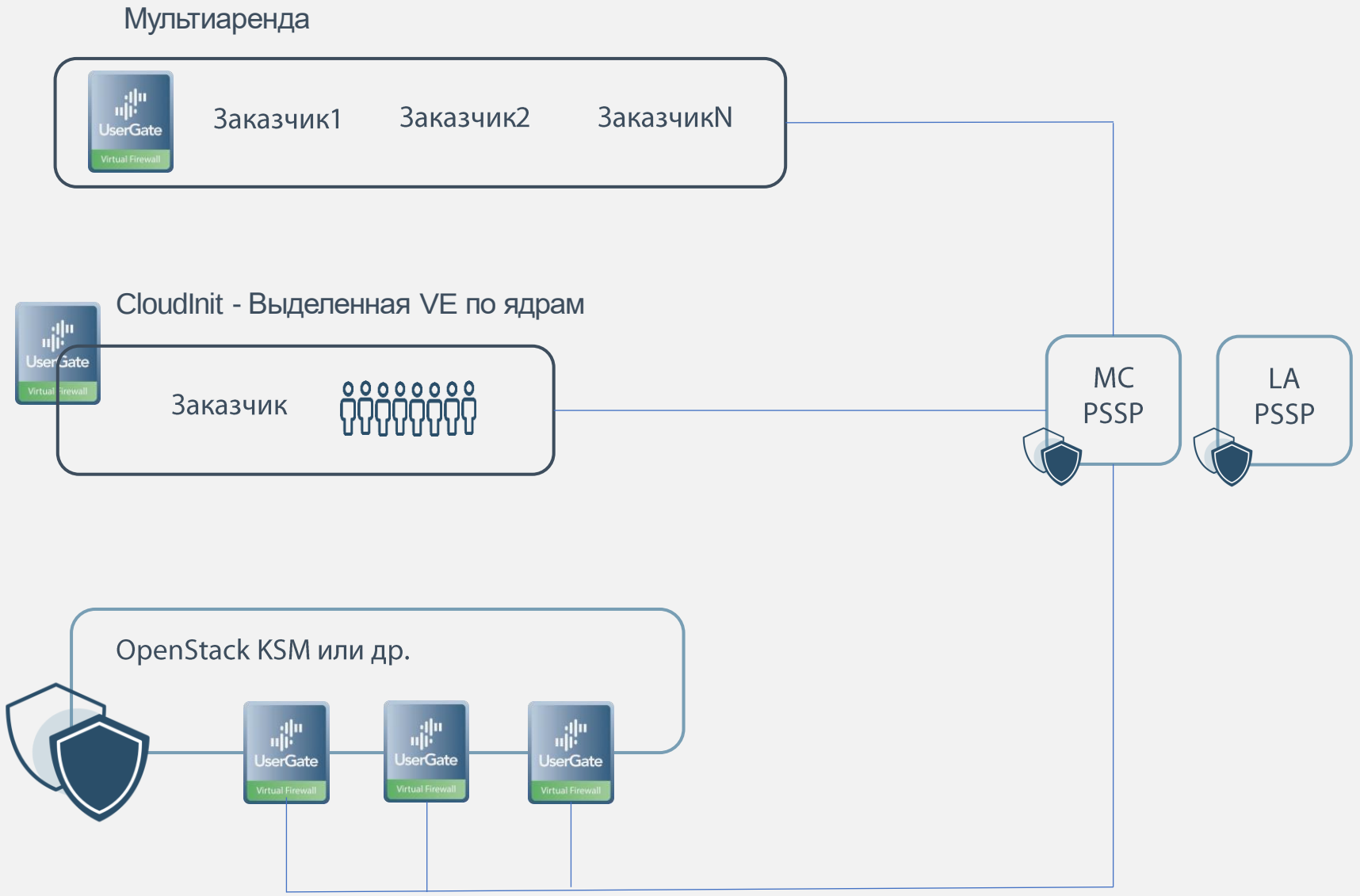
3. Провайдеры:
   - Поставщики инфраструктуры (ЦОД)
   - Телко

Нет ограничений!

- 3 линии ТП
- Поддержка вендора стандартная
- Поддержка Партнера PSSP 1-2 и Звендора Партнеру
- Требования к партнеру:
    a) Наличие специалистов 1,2й линии Технической поддержки
    b) Сертифированный Администратор UserGate
    c) Демостенд



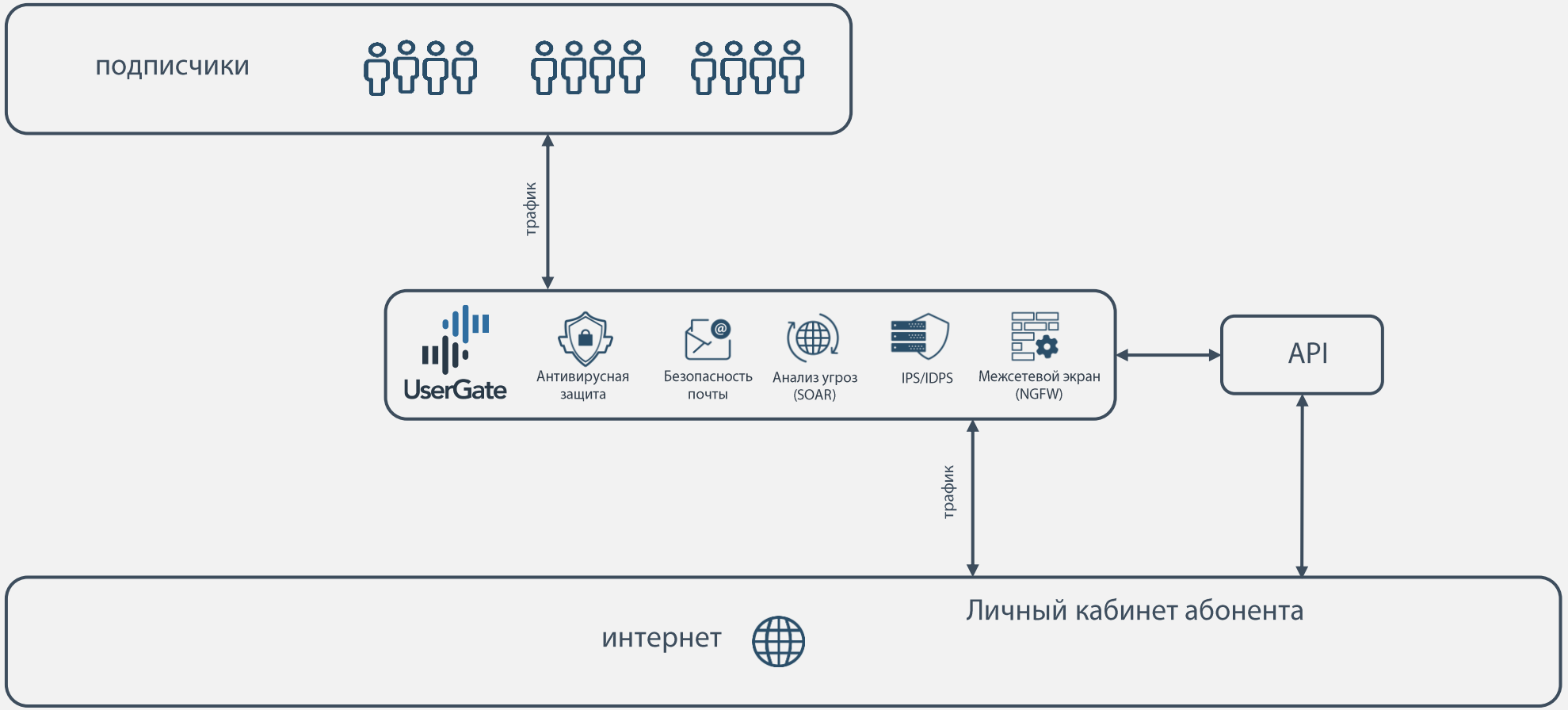
- PSSP: ТПЗ линия, обслуживание инфраструктуры заказчика
- Самостоятельное администрирование и по заявкам
- Сбор и хранение логов, долговременная статистика
- В персп. + СИЕМ
- В персп. – Сумма






PSSP (Профессиональные сервисы ИБ)						
				Logan	Managment Center	Собственная Техническая поддержка
DCI	МЭ FG	NGFW	USG			
URL фильтр	Классический FW	Классический FW	Классический FW	Долговременное хранение	Единая Консоль управления	1-2 линия ТП
Антивирус		IDPS	IDPS	Отчетность	Заявки\доступ	UG 3л ТП
Реклама		DPI	DPI	SOAR		Инфраструктура
			DCI			
			ASpam			

- Стандарт – стандартные UTM и поддержка производителя
- Профессионал – Стандарт + дополнительные решения
- Спонсор – оплата годовой выбранной конфигурации вперед


подписчики
трафик
UserGate
Антивирусная защита
Безопасность почты
Анализ угроз (SOAR)
IPS/IDPS
Межсетевой экран (NGFW)
API
трафик
интернет
Личный кабинет абонента

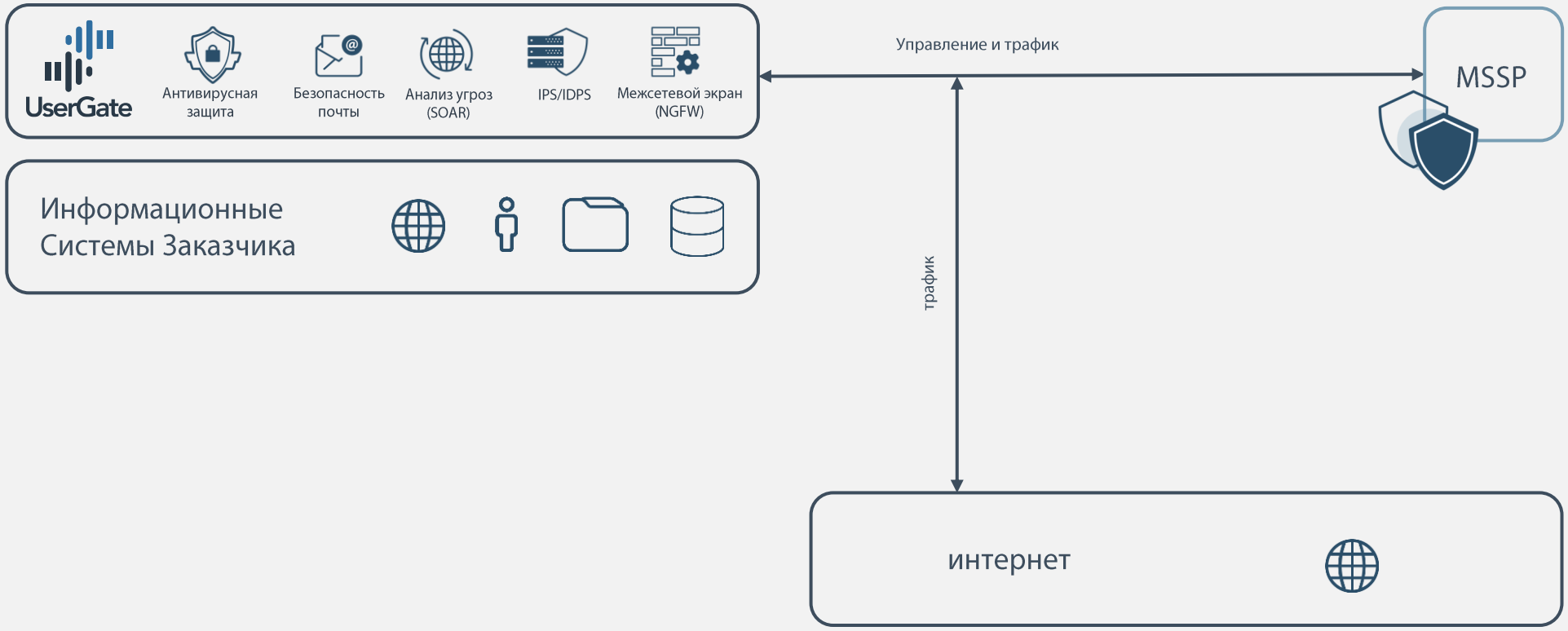
DCI:

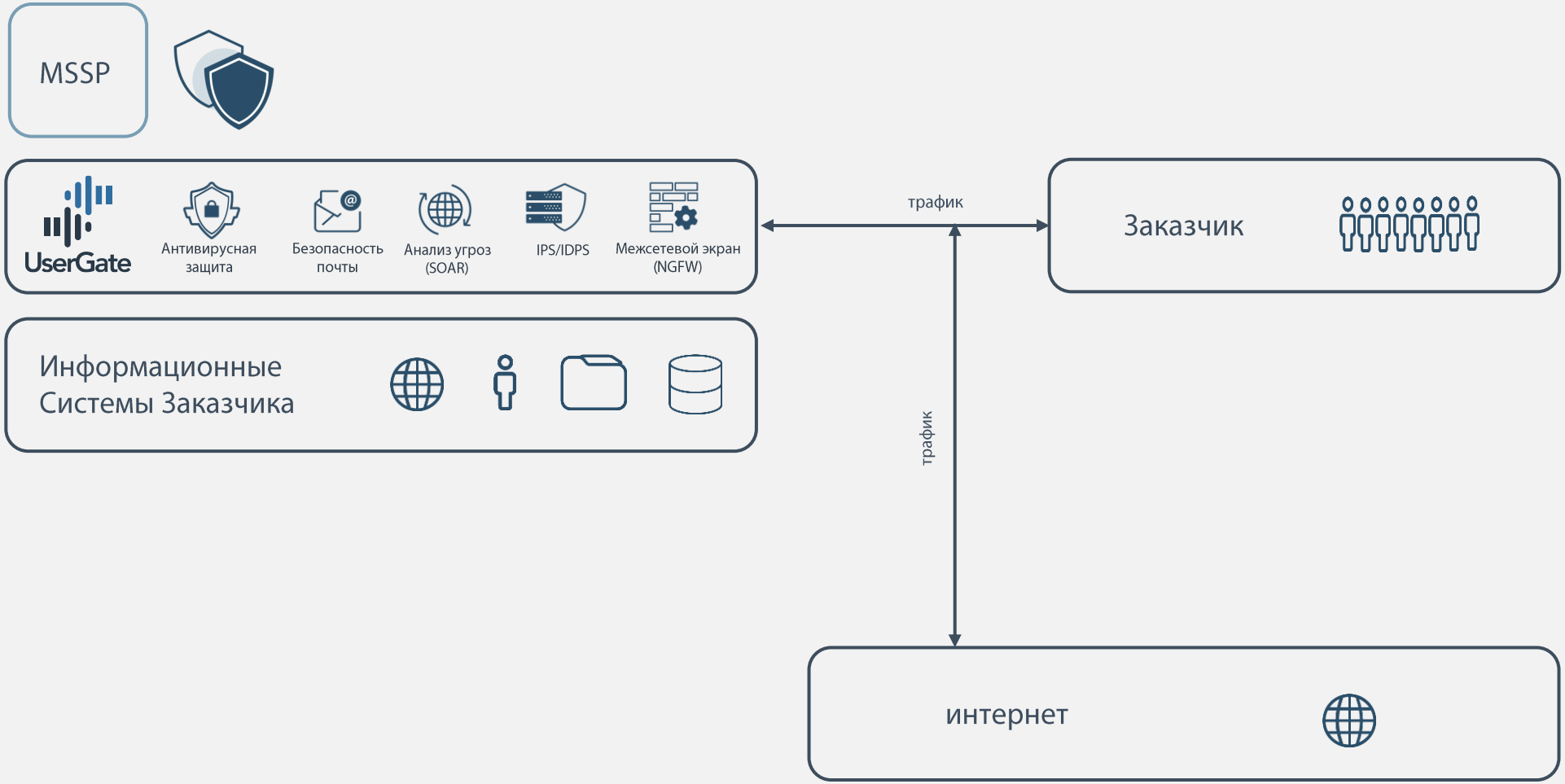
- Категоризация URL (внутридоменная) под различные тарифы и группы пользователей:
- Образование (ФЗ 436, 114, 139, 252)
- Списки РКН

- Удаление рекламы/замена на свою

- Антивирусная проверка

- Приоритезация критичного трафика, исключение паразитного


UserGate
Антивирусная защита
Безопасность почты
Анализ угроз (SOAR)
IPS/IDPS
Межсетевой экран (NGFW)
Информационные Системы Заказчика
Управление и трафик
MSSP
трафик
интернет

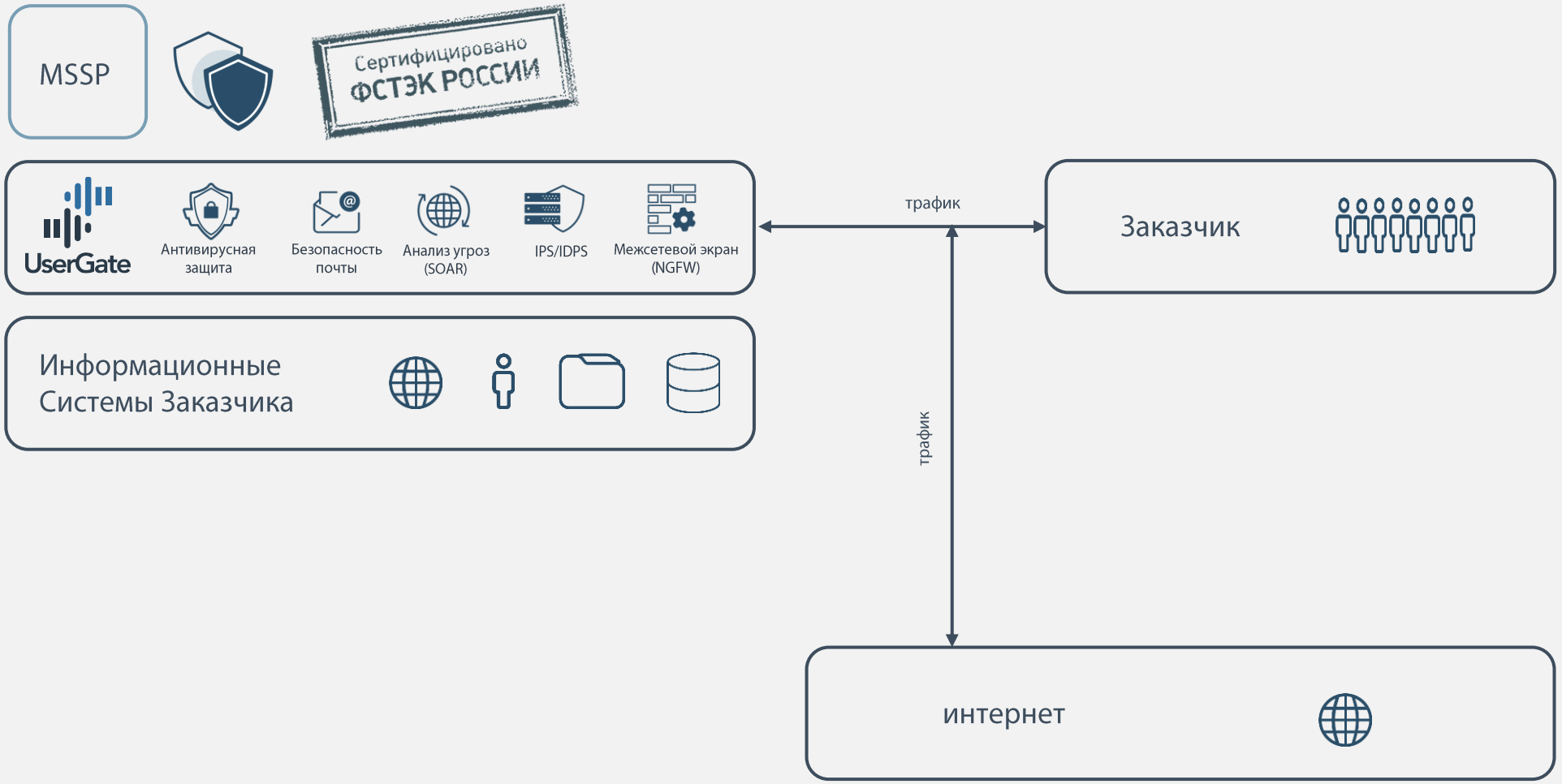

MSSP
UserGate
Антивирусная защита
Безопасность почты
Анализ угроз (SOAR)
IPS/IDPS
Межсетевой экран (NGFW)
трафик
Заказчик
Информационные Системы Заказчика
трафик
интернет

СЕРТИФИКАТ ФСТЭК России № 3905

Реестр

Данный уровень сертификации дает возможность использования решения в составе автоматизированных систем до класса защищенности 1Г, информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС)
до 1 класса (уровня) защищенности включительно,
т. е. не обрабатывающих гостайну. Решение полностью удовлетворяют требованиям 17 и 21 приказов ФСТЭК России для обработки персональных данных 1-4 категорий.

- 1) Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- 2) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- 3) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- 4) Приказ ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
- 5) Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
- 6) Национальный стандарт РФ ГОСТ Р 57580.1-2017 «Безопасность
- финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
- 7) Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
- 8) Стандарт безопасности данных индустрии платежных карт (PCI DSS).


MSSP
Сертифицировано
ФСТЭК РОССИИ
UserGate
Антивирусная защита
Безопасность почты
Анализ угроз (SOAR)
IPS/IDPS
Межсетевой экран (NGFW)
трафик
Заказчик
Информационные Системы Заказчика
трафик
интернет

Артур Салахутдинов
Руководитель направления MSSP

Artur.salah@usergate.ru
8 800 500 40 32 | доб. 9907