

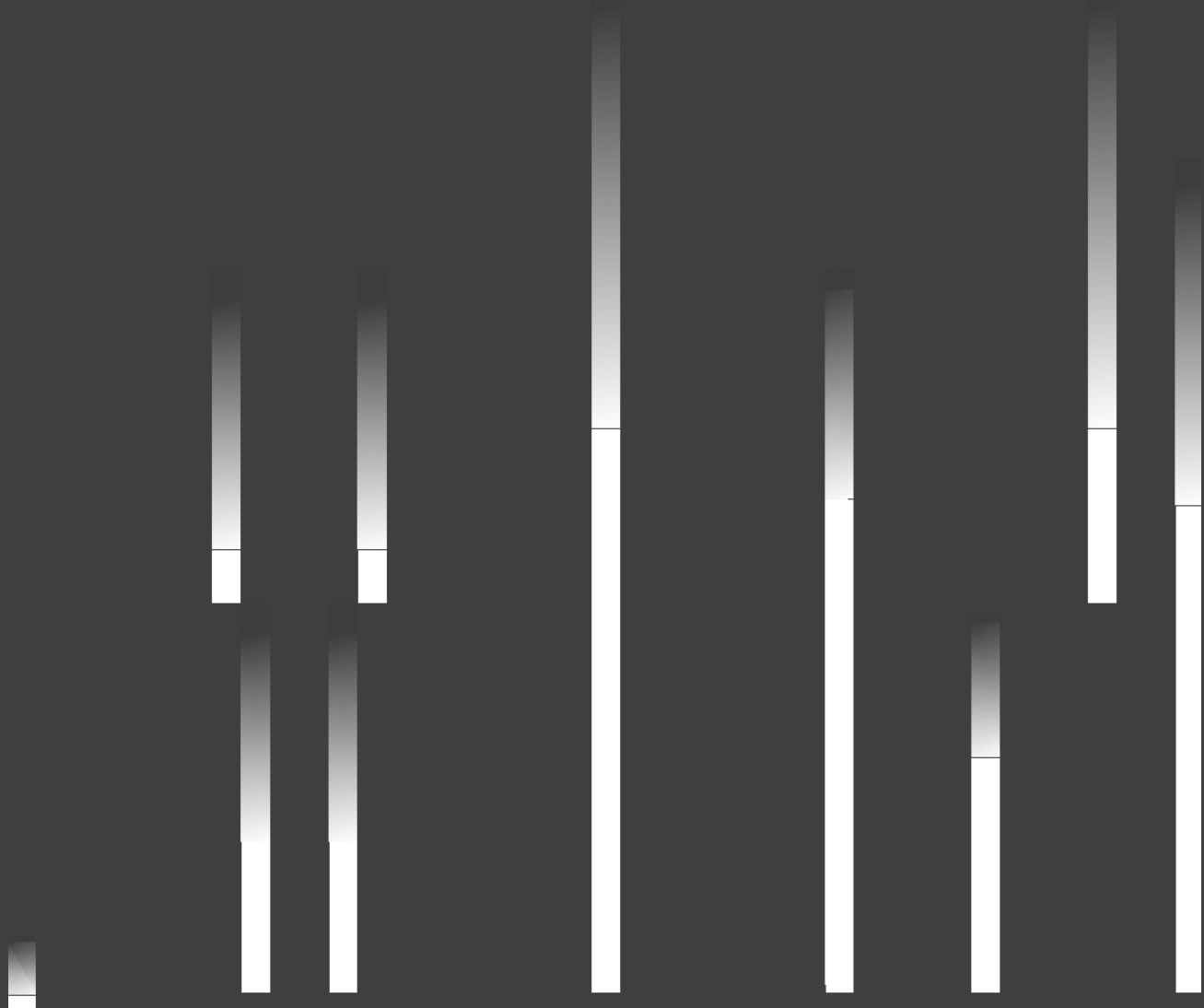
#CloudMTS

# Оперативная миграция ресурсов: сохраняем стабильность



**Александр Асаулко**

Менеджер по продукту #CloudMTS



#CloudMTS

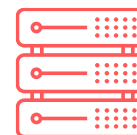
## Облачный бизнес МТС



**Решения в формате частных,  
публичных, гибридных  
облаков**



**Комплекс консалтинговых  
и профессиональных сервисов**



**14 ЦОД, доступ по всей  
России, собственные каналы  
связи**

#CloudMTS

## Облачный бизнес МТС

> 25

сервисов

4

страны  
присутствия

2000+

клиентов из разных  
отраслей бизнеса

**#CloudMTS – экосистема облачных сервисов МТС для крупного бизнеса и корпораций, включающая:**

Инфраструктурные решения в формате частных, публичных и гибридных облаков;

Корпоративные сервисы, а также комплекс консалтинговых и профессиональных услуг;

Услуги дата-центра, телеком-сервисы, решения по безопасности.



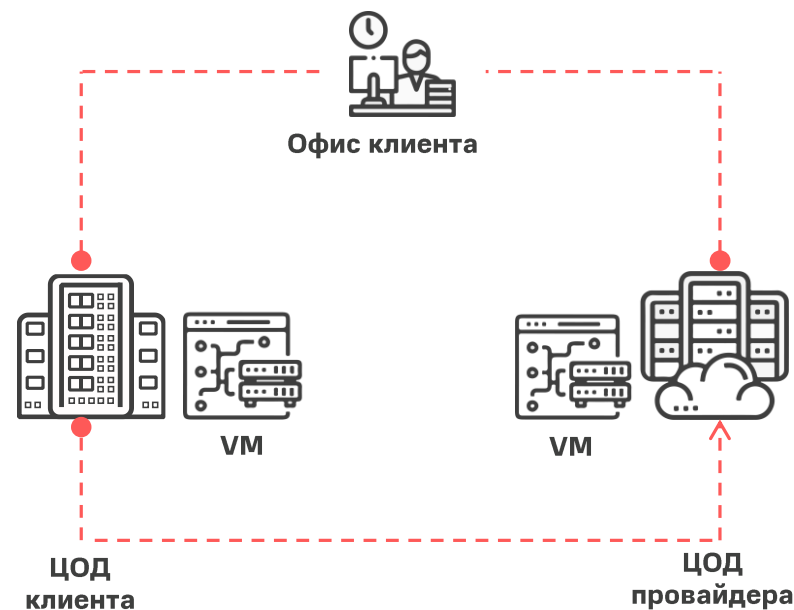
## Почему **выбирают** миграцию в облако провайдера?

Высокий риск утечки важных данных – нужно повысить безопасность ИТ-инфраструктуры.

Необходимо консолидировать территориально разрозненные ИТ-системы и обеспечить доступ к данным из любого региона России.

Требуется расширить ресурсы или модернизировать оборудование – сложно обосновать бюджет, нет места в серверной, дорогая техническая поддержка.

Низкое качество сервиса в арендованном дата-центре или частое отключение электроэнергии в серверной бизнес-центра.



## Сценарии миграции в облако

### Миграция на уровне виртуальных машин

Переезд виртуальной машины и запуск ее в облаке провайдера

### Миграция на уровне приложений

Погружение в детали и миграция конкретно взятого / взятых приложений (например, Exchange, Active Directory, БД)

### Миграция на уровне операционной системы

Погружение внутрь виртуальной машины, установка агента, загрузка в облако провайдера и последующее восстановление

### Миграция с помощью ВаaS-решений

Клиенты самостоятельно мигрирует и восстанавливает виртуальную машину в облаке без участия сотрудников провайдера



#CloudMTS



## Клиентский кейс «Русхимсеть»

ЗАО «РУСХИМСЕТЬ» — первый национальный универсальный химический дистрибьютор в России и странах СНГ.

**17**

офисов по всей России

**4**

зарубежных  
дочерних компании

**28**

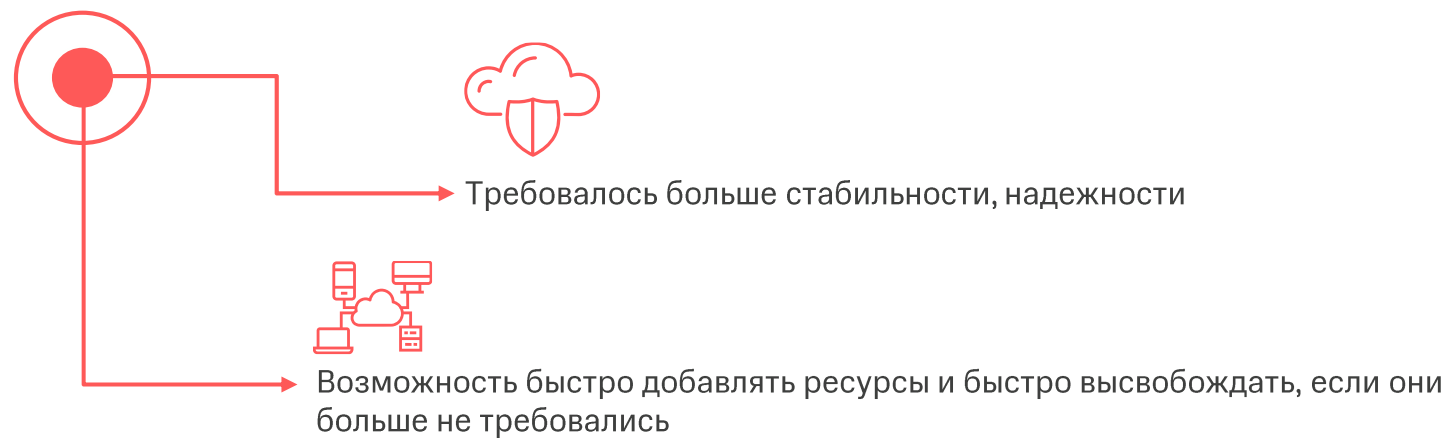
логистических центра



## Идея **перехода** к провайдеру

Компания столкнулась с проблемой морального и физического устаревания оборудования. Неоднократно случались сбои в работе отдельных систем. Это порождало простои и потери для бизнеса.

Приняли решение: вкладываться в модернизацию частного облака нет смысла. Нужно переходить к провайдеру.



## Как готовились к миграции

### ШАГ 1

#### Аудит инфраструктуры

Команда изучила ИТ-ландшафт, чтобы понять, в каком состоянии находятся сервисы. Составлен список систем и их взаимодействий. Подготовлен план миграции.

### ШАГ 4

#### Согласование бюджета

В среднем публичное облако оказалось в 2-3 раза «экономнее» приватного варианта.

### ШАГ 2

#### Первичное планирование

Очертили круг сервисов, которые в конечном итоге будут вынесены на облачную площадку.

### ШАГ 5

#### Утверждение ИТ-конфигурации в облаке

Поскольку ИТ-инфраструктура переносилась на площадку провайдера, требовалось заранее согласовать и утвердить облачную конфигурацию.

### ШАГ 3

#### Оптимизация запросов

Требовалось определиться, какие сервисы стоит перенести в облако, а также оптимизировать запросы и проработать способы их решения.

### ШАГ 6

#### Окончательный план миграции

Миграция разбита на два этапа. В первую очередь в облако перенесли системы 1С, далее остальные компоненты инфраструктуры.



## Полученные **результаты**

### **Критические элементы ИТ-инфраструктуры в облаке**

В облаке - 1С, система электронного документооборота, почта, рабочие места, IP-телефония.

### **Дисковая подсистема перестала быть слабым звеном**

Ранее дисковая подсистема была узким местом, поскольку не справлялась с текущими нагрузками. Теперь ее производительность выросла в 10 раз.

### **Увеличение скорости работы ИТ-систем**

Минимум на 30% повысилась скорость работы ИТ-систем.

### **Гарантия стабильности и надежности**

Получили гарантированную стабильность, быстродействие, масштабируемость.

### **Облако для baas-задач**

«Русхимсеть» использует облачные технологии для создания резервных копий приложений и баз данных.

### **Экономия на ИТ**

На 25% сократились ежемесячные затраты, связанные с эксплуатацией оборудования.



#CloudMTS



**Александр Асаулко**

Менеджер по продукту #CloudMTS

**+79885724753**

[aleksandr.asaulko@mts.ru](mailto:aleksandr.asaulko@mts.ru)

[www.cloud.mts.ru](http://www.cloud.mts.ru)



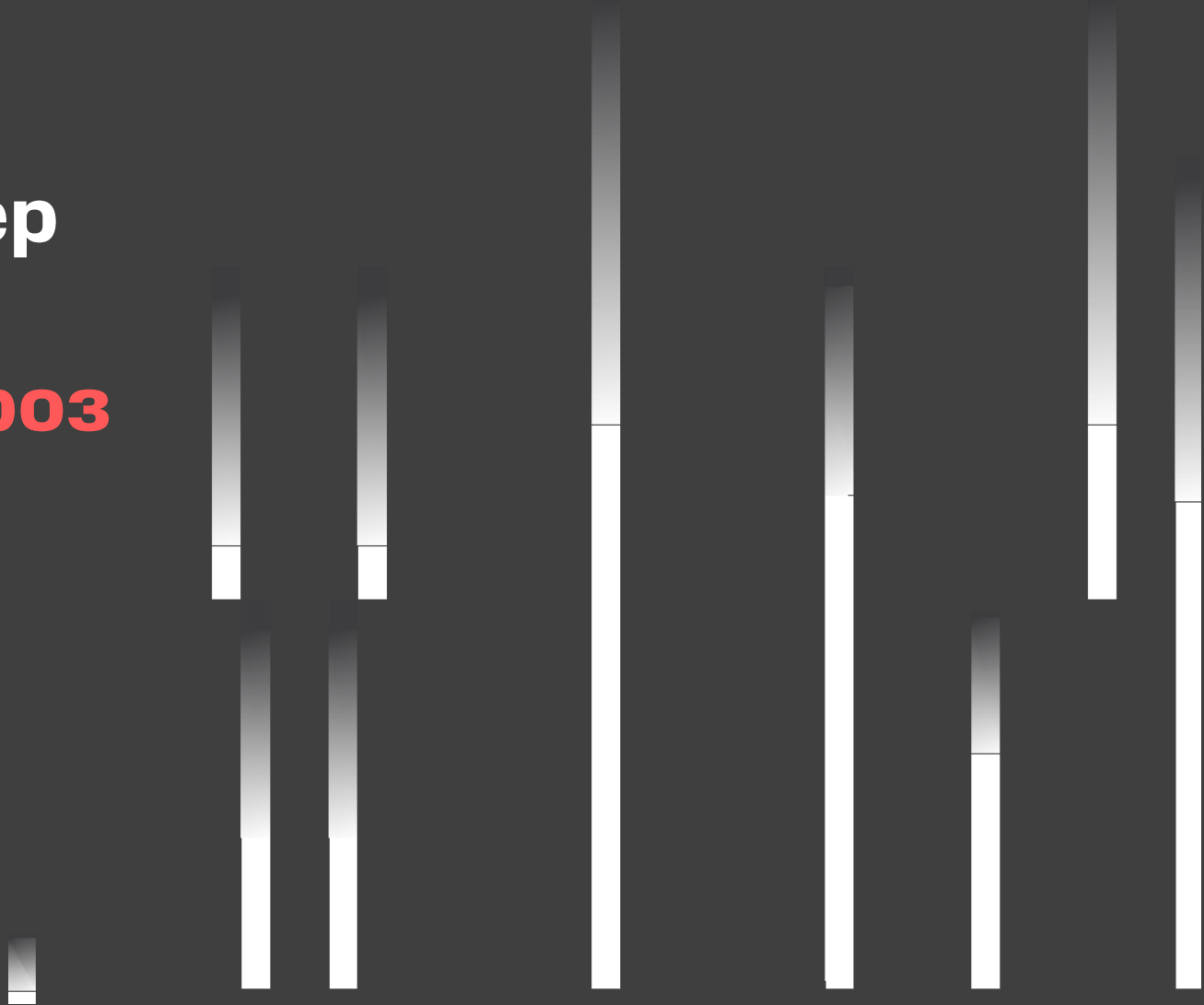
#CloudMTS

# Как облачный провайдер помогает комплексно защититься от киберугроз



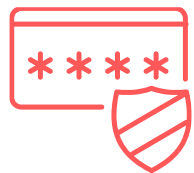
**Александр Карпузиков**

Менеджер по продукту #CloudMTS



#CloudMTS

## Портфель услуг ИБ #CloudMTS



**Защищенный  
сегмент IaaS 152-ФЗ**



**Антивирусная  
защита VM**



**Security Operation Center**



**Защита  
от DDoS-атак**



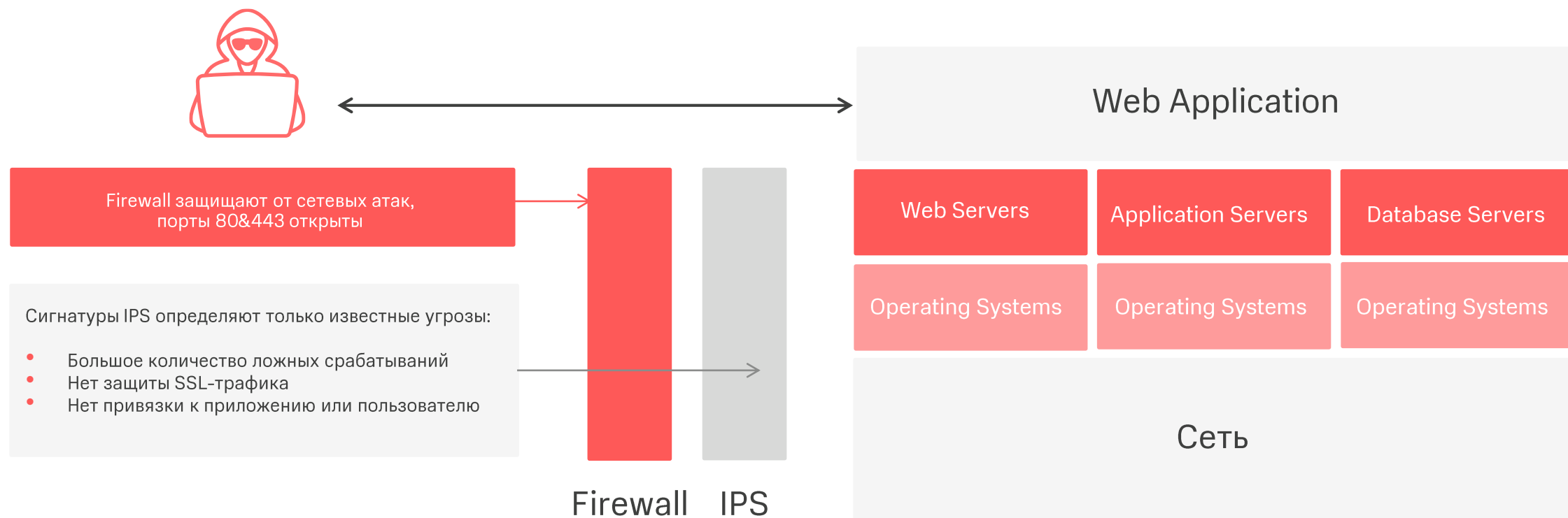
**Защита веб-приложений  
и сайтов (WAF)**

#CloudMTS

**WAF Premium**

01

## Фокус более 75% атак направлен на веб-приложения



## Что интересно злоумышленникам?

**Кража персональных данных** и другой конфиденциальной информации

**Хищение денежных средств пользователей**

**Атаки на пользователей сайта** путём заражения страниц сайта вирусами и размещения ссылок, содержащих инструменты взлома

**Понижение позиций ресурса в поисковых системах**

и нарушение рекламной политики путём манипуляций с кодом сайта

**Нарушение работоспособности веб-приложений**, включая удаление или искажение файлов, баз данных и т.п.

**Подмена содержания страниц** (размещение противозаконного или ложного контента, в том числе, поддельных новостей, неправильных цен на товары, ложной контактной информации, адресов электронной почты и т.д.)

**Выполнение мошеннических действий** от лица пользователей

Ботнет активности (рекламный бюджет уходит на нецелевые клики, сбиваются аналитические метрики по продажам)

**Проникновение в инфраструктуру**

## Кому нужна защита с помощью WAF

Все вертикали бизнеса, использующие интернет в качестве среды взаимодействия с пользователями и заказчиками (сайт, веб-приложения чаты и т.д.)

Бизнес-процессы построены (оптимизированы) благодаря веб-приложениям/сайтам



Банки, страховые и финансовые организации



Госсектор, бюджетные организации (фед. и рег.)



ТЭК, предприятия



Транспорт



Все бизнесы интернет-индустрии, интернет магазины и различные сайты (игровые, развлекательные, новостные и т.д.)





# Причина появления **WAF Premium**

## Предпосылки:

Обычно сервис-провайдерами предоставляется инструмент фильтрации

В зону ответственности не входит эксплуатация решения, мониторинг и реагирование на атаки, внесение правил блокировки

## Что мы предлагаем в комплексной услуге **WAF Premium**:

### 1. Конфигурирование

Управление конфигурацией защищаемых веб-приложений.

Тонкая настройка прохождения трафика через узлы фильтрации с учетом специфики защищаемых веб-приложений

### 2. Эксплуатация

Выявление ложных срабатываний механизмов фильтрации и корректировка профиля защиты.

Актуализация профиля защиты с учетом специфики трафика.

Масштабирование компонентов по мере роста нагрузки на веб-приложение.

### 3. Мониторинг и реагирование на инциденты

Мониторинг и реагирование на инциденты в режиме 24/7.

Предоставление отчетов по зафиксированным инцидентам и обращениям в техническую службу по запросу заказчика.



# Функциональные возможности услуги

## Нейтрализация рисков из списка OWASP TOP 10

WAF Premium задействует разнообразные механизмы защиты — от сигнатурного и динамического анализа трафика до настраиваемых правил безопасности

## Предотвращение ботнет-активности

WAF Premium определяет и блокирует подозрительную активность по цифровому отпечатку браузера — набору таких признаков как часовой пояс, в котором находится пользователь, а также язык, список расширений и версия браузера

## Выявление уязвимостей и предотвращение их эксплуатации

WAF Premium выявляет уязвимости с помощью пассивного сканера, а механизм виртуального патчинга позволяет оперативно предотвращать эксплуатацию найденных ошибок, не дожидаясь следующего релиза веб-приложения

## Поведенческий анализ

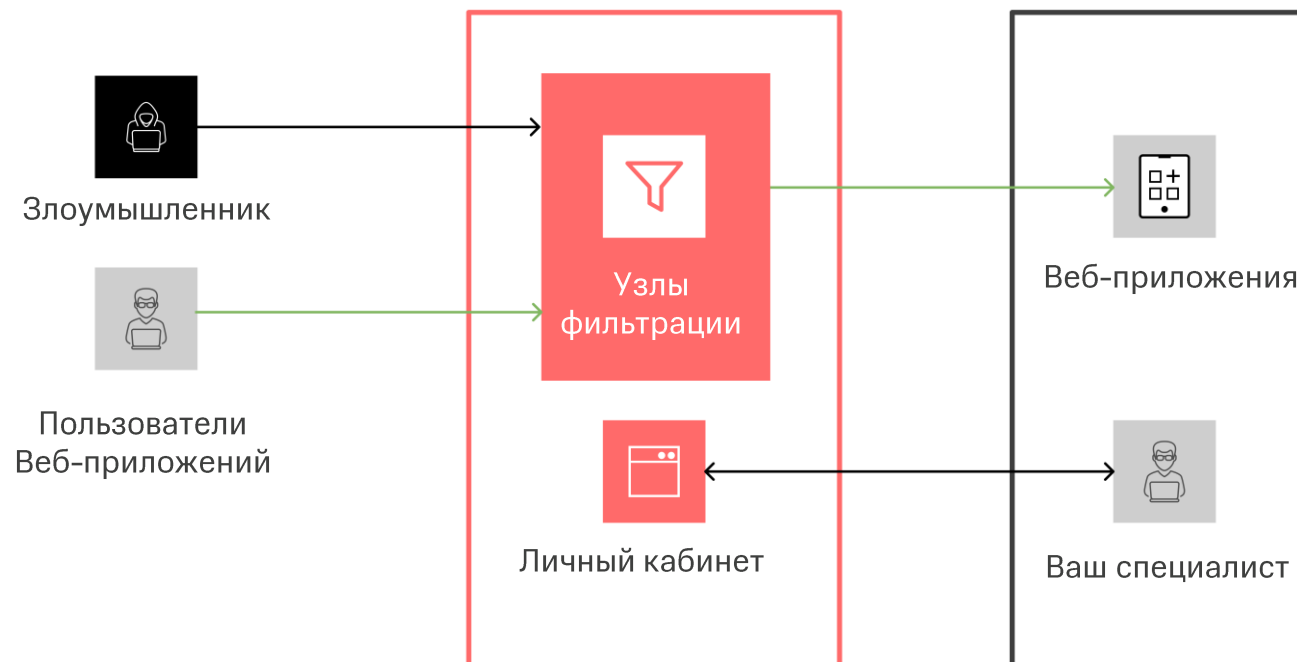
WAF Premium защищает от атак методом перебора (brute-force) и сканирования каталогов (dirbusting) по именам файлов на серверах веб-приложений. Эту задачу выполняют технологии поведенческого анализа, которые обнаруживают аномальное поведение, и алгоритмы ограничения частоты запросов (rate limiting)

## Выявление попыток использования скомпрометированных учетных записей

WAF Premium предотвращает атаки типа credential stuffing, используя собственные базы данных и настраиваемые правила корреляции

## Принципы работы услуги

- Трафик пользователей, поступающий заказчику из интернета и направленный на защищаемое веб-приложение, проходит через узлы фильтрации WAF Premium
- Входящие запросы проверяются в соответствии с настроенной политикой защиты. Если они содержат в себе следы веб-атаки (вредоносной активности), трафик помечается как зловредный и блокируется, прежде чем достичь веб-приложения



#CloudMTS

IaaS Ф3-152

02

#CloudMTS

## Основной вопрос клиента — владельца ИСПДн

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

**«ДА!»**

## Реализация ИСПДн: плюсы облачного решения



### Реализация на собственной Инфраструктуре

Высокие единовременные затраты и стоимость владения

Уникальность каждой системы защиты ПДн

Долгий срок реализации (проект, поставка, внедрение)

Необходимость мониторинга и изучения законодательства

Необходимость разработки документации на ИСПДн

Необходимость иметь в штате высококвалифицированных специалистов



### Реализация на облачной Инфраструктуре

Низкие единовременные затраты и стоимость владения

Отработанное типовое решение в облачной инфраструктуре

Оперативное развертывание (от 1 дня)

Мониторинг и обеспечение соответствия законодательству — зона ответственности исполнителя

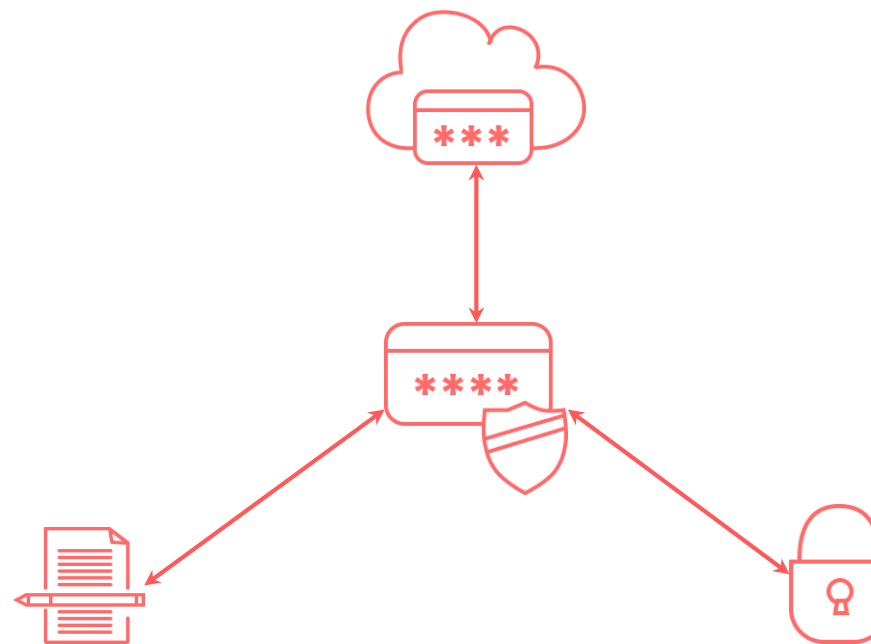
Все необходимые шаблоны документов предоставляет исполнитель

Сертифицированные специалисты исполнителя

## IaaS 152-ФЗ

Безопасная обработка персональных данных в защищенном облаке, полностью соответствующем требованиям ФЗ-152

**Предоставление в пользование виртуальной ИТ-инфраструктуры**, удовлетворяющей требованиям законодательства РФ по защите информации, для размещения информационных систем персональных данных клиента



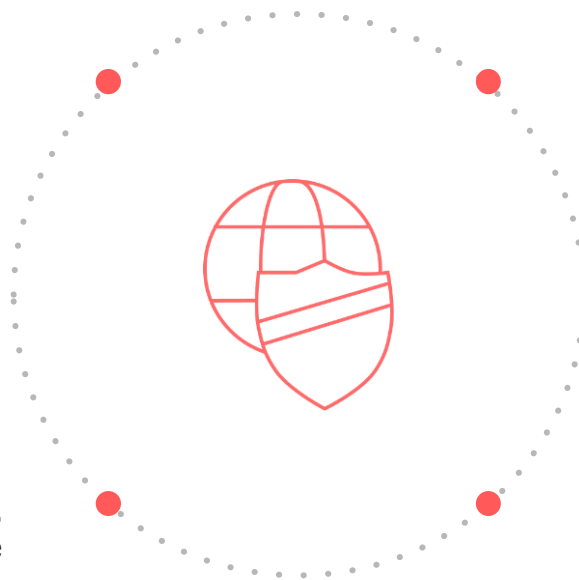
Возможность заключения **официального договора-поручения на обработку ПДн** и помощь в подготовке необходимой документации

**Отдельный защищенный аттестованный сегмент** облака для размещения мощностей заказчика и обработки ПДн

## Что **получает клиент** в защищенном сегменте #CloudMTS

Гарантию выполнения требований  
21 приказа ФСТЭК  
на уровне средств связи  
и инфраструктуры — аттестат  
на облако (на продукты IaaS)

Набор типовой документации,  
частную модель угроз для ИСПДн в облаке



СЗИ и СКЗИ для реализации ИСПДн на уровне  
виртуальных машин и локальной вычислительной  
сети по схеме аренды

Поддержку в случае проведения проверок  
РКН, ФСТЭК



#CloudMTS

**SOC**

03

## Security Operations Center (SOC)



**Центр обеспечения безопасности (SOC)** объединяет технологии (программные и аппаратные) и людей для обеспечения комплексной защиты от киберугроз **при помощи мониторинга и реагирования (в режиме 24/7)** на события (инциденты) информационной безопасности **(ИБ)**.

## Цель и составляющие SOC

**SOC** занимается контролем защиты ИТ-инфраструктуры и снижением рисков, за счет использования экспертов кибер-безопасности и современных технологий обнаружения, анализа и предотвращения инцидентов (систем **SIEM** - Security information and event management и технологий кибер-разведки **Threat Intelligence**)

**SOC** строится на базе **технологий** мониторинга и реагирования на угрозы, поддерживается **людьми** (специалистами ИБ) и позволяет контролировать **процессы ИБ**, которые начинаются с обнаружения угроз и заканчиваются их предотвращением.

### SOC



Люди



Технологии



Процессы



## Про SOC МТС

### С 2005 года

существует  
Корпоративный SOC

### С 2016 года

предоставляем услуги  
Коммерческим  
заказчикам

### Клиенты

несколько десятков  
клиентов в различных  
сферах деятельности

### Сотрудники

высококвалифицированный  
штат сотрудников SOC

### SOC

один из крупнейших  
SOC не только в России,  
но и в Европе

### SIEM

реализация крупного  
промышленного SIEM  
как сервис

### Лицензия

лицензия ФСТЭК ТЗКИ №2012  
на услуги по мониторингу  
информационной  
безопасности средств  
и систем информатизации  
(пункт «в»)

### 700 млн.

обрабатывается  
около 700 млн. событий  
в сутки

### 24/7

мониторинг  
и реагирование на  
инциденты 24/7

### Сертификат

Сертификат ISO 27001  
«Предоставление услуг  
мониторинга и реагирования  
на инциденты информационной  
безопасности»

## Иерархия **защиты** с помощью SOC

Отдельные инструменты ИБ обеспечивают защиту от профильных частных угроз, однако **не защищают заказчика комплексно от инцидентов ИБ**



## Купил SIEM – получил SOC?

**SIEM** это технология, которая позволяет собирать события безопасности с различных источников (в том числе средств безопасности), обрабатывать и хранить их.

### **SIEM НЕ ВКЛЮЧАЕТ:**

**Сотрудников по безопасности**

**Процессы, следующих направлений:**

- Поддержка инфраструктуры SOC;
- Мониторинг событий безопасности;
- Расследование инцидентов;
- Постоянное усовершенствование SOC.





Обнаружение • Предупреждение • Ликвидация •

## Подключение к ГОССОПКА

Постоянное усовершенствование SOC. МТС является Корпоративным центром **ГосСОПКА** (**Государственная Система Обнаружения, Предупреждения и ликвидации последствий Компьютерных Атак**)

Во главе **ГосСОПКА** стоит Национальный координационный центр по компьютерным инцидентам (**НКЦКИ**)

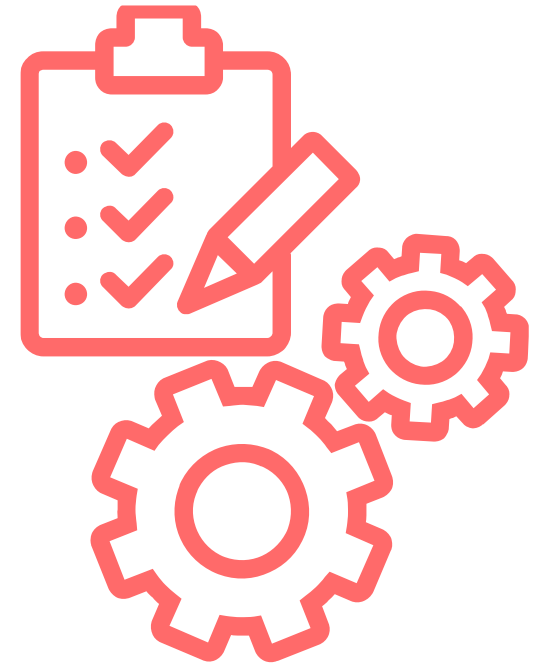
Субъекты критической информационной инфраструктуры (**КИИ**) **обязаны сообщать НКЦКИ** о произошедших компьютерных инцидентах (Федеральный закон от 26.07.2017 №187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»)

Является **дополнительной опцией** при подключении SOC

## Тарификация и набор **опций SOC**

В основе стоимости услуги лежит *количество обрабатываемых событий*  
**(Events per second - EPS)**

- В качестве **дополнительных опций** (в составе клиентского договора SOC):
- Контроль уязвимостей внешнего периметра / сканирование на уязвимости
- Проведение анализа и расследования инцидентов ИБ
- Подключение к **ГосСОПКА**





#CloudMTS



**Александр Карпузиков**

Менеджер по продукту #CloudMTS

**+ 7 915 486 36 15**

[akarpuzikov@mts.ru](mailto:akarpuzikov@mts.ru)

[www.cloud.mts.ru](http://www.cloud.mts.ru)



#CloudMTS

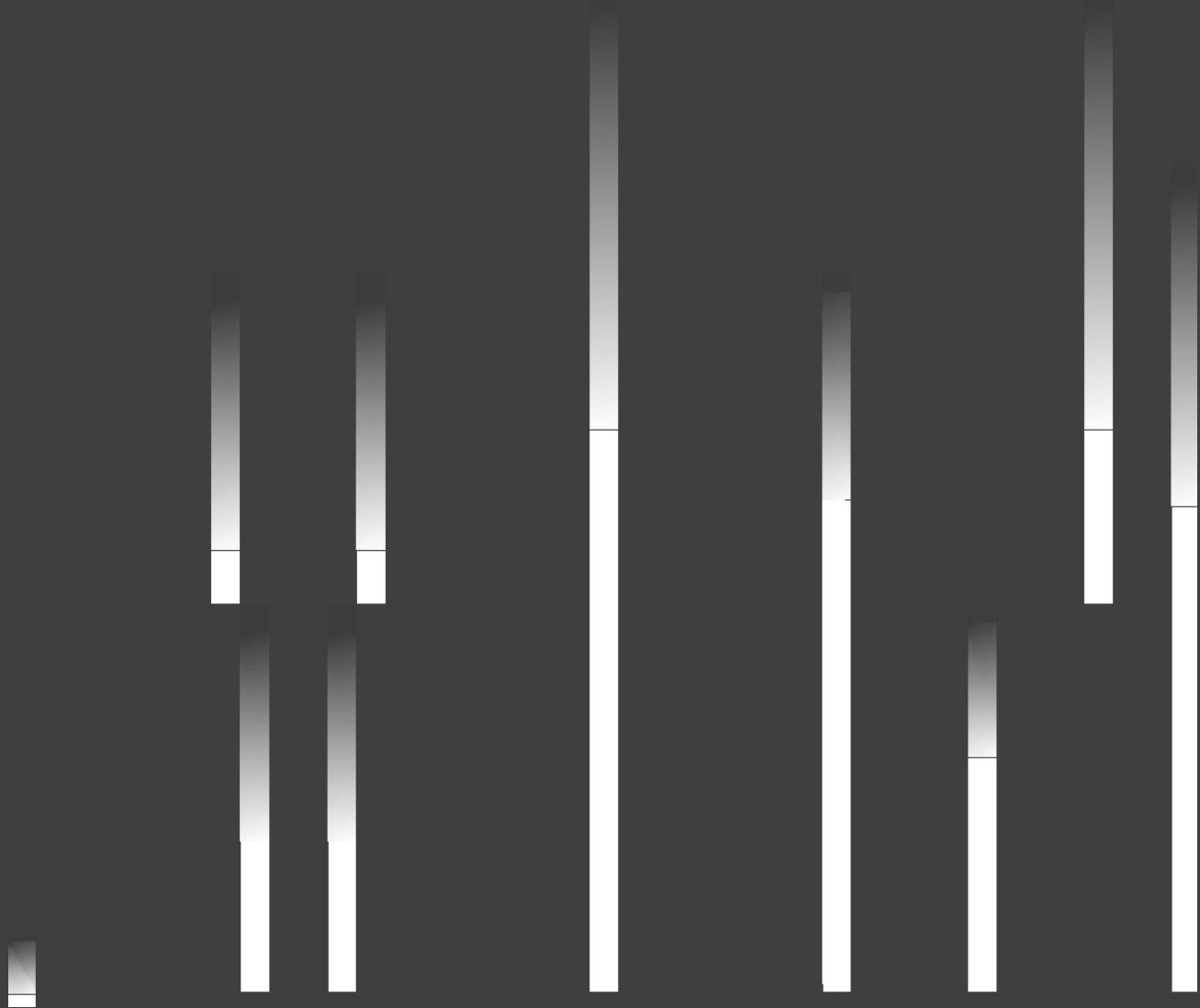
# Работа приложений 1С в новой реальности

Автоматизация, инфраструктура, сервисы 1С MTS Cloud



**Майя Чубукова**

Руководитель направления 1С #CloudMTS



#CloudMTS

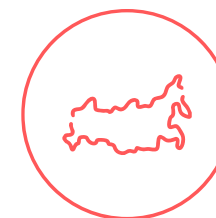
## Экспертиза 1С #CloudMTS



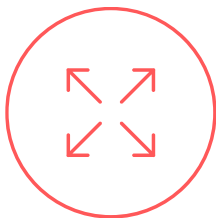
**МТС официальный  
партнер фирмы 1С**



**Собственная команда  
сертифицированных  
специалистов 1С**



**Наличие ЦОД  
по всей стране**



**Комплексное решение  
вопросов по облачной  
инфраструктуре**



**Выделенная линия  
консультаций 1С**



# **1С – универсальная платформа для автоматизации бизнес-процессов**

- 1С – российский разработчик ПО для автоматизации бизнес-процессов
- Продукты 1С находятся в реестре отечественного ПО
- Платформа сертифицирована по защите персональных данных
- 85 % рабочих мест России – автоматизировано на базе 1С
- Решения 1С покрывают практически все бизнес-процессы предприятия и максимально удобно для интеграции

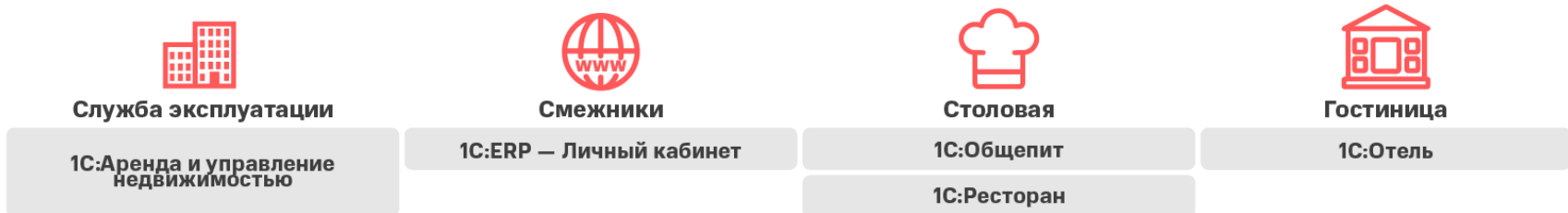
Управление



Операционная деятельность



Вспомогательные службы



ОТРАСЛЕВЫЕ МОДУЛИ

## Сервис 1С для бизнеса





- **1С Аналитика** - это BI-система , является частью платформы «1С:Предприятие 8», есть мобильный клиент
- **1С Кабинет сотрудника** – сервис 1С, с помощью которого можно подключать сотрудников к кадровым документам в личном кабинете. Есть мобильный клиент
- **1С: Распознавание первичных документов** – сервис, который берет на себя работу по превращению бумажных документов в документы базы 1С
- **1С СПАРК** – сервис проверки контрагентов и скоринга
- **1С ЭДО** – сервис обмена электронными юридически значимыми документами
- **1С Отчетность** – сервис электронного обмена с налоговыми органами
- **1С Шина** - это программный продукт (ESB), обеспечивающий обмен данными между различными информационными системами
- **1С Документооборот** – программный продукт для автоматизации внутреннего и внешнего документооборота предприятия. Есть мобильный клиент, встроенный почтовый клиент и коммуникатор
- **1С УНФ** – программный продукт для автоматизации управленческого учета малых предприятий

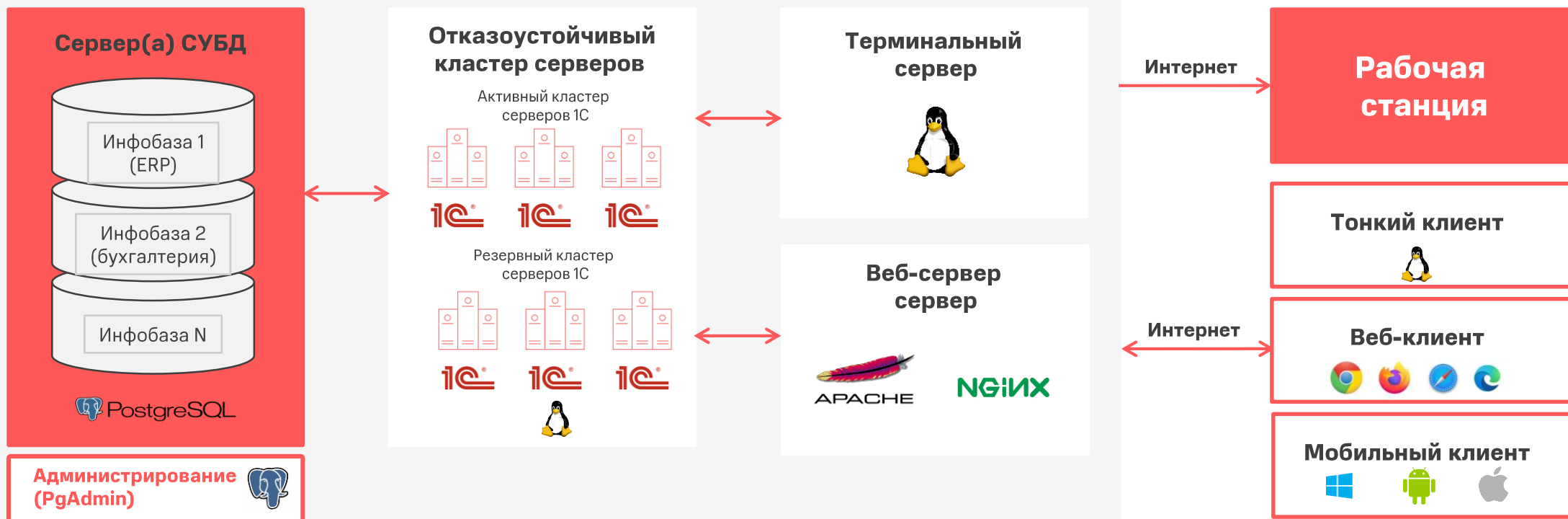
## Технологии платформы 1С

Веб-клиент	Тонкий клиент	Мобильный клиент
Мобильный клиент с автономным режимом	Мобильная платформа	Бизнес-процессы
СУБД 1С, MS SQL, PostgreSQL	Интернет (HTTP, REST, FTP, SMTP, POP3, IMAP, SOAP, OData)	Отказоустойчивый кластер
Механизм ботов	Встроенный мессенджер, чаты, видеозвонки, показ экрана	Корпоративные стили
Аутентификация: OC, OpenID, 2FA	Криптографическая защита	Кроссплатформенность (Windows, Linux, macOS)
Интеграционные возможности (XML, JSON)	Интеграция с мессенжерами Telegram, VK	Автоматический REST API

# ИТ- инфраструктура

## Виртуальная инфраструктура в облаке (PROD, DEV, TEST)

Мониторинг (ElasticSearch, ClickHouse, Zabbix, 1C:ЦУП, 1C:ЦКК)    







## Нюансы перехода 1С с продуктов MS на Open Source

	Продукты MS	Продукты OpenSource
Стоимость	Платно	PostgreSQL (от 1С) - бесплатно
Производительность 1С	Высокая производительность из коробки	Требует специальных знаний к настройке высокопроизводительных систем
Удобство	GUI +	GUI +/-
Наличие специалистов	Большое количество специалистов	Меньше специалистов на рынке
Ограничения		Интеграции (требуется пересмотр работы всех узлов интеграции , в частности не работает COM соединение) Блоки по использованию офисного ПО

## Продукты #CloudMTS для приложений 1С

### Вендорские сервисы

- Лицензии 1С
- ИТС сопровождение
- Сервисы 1С

### Оптимизация приложений 1С

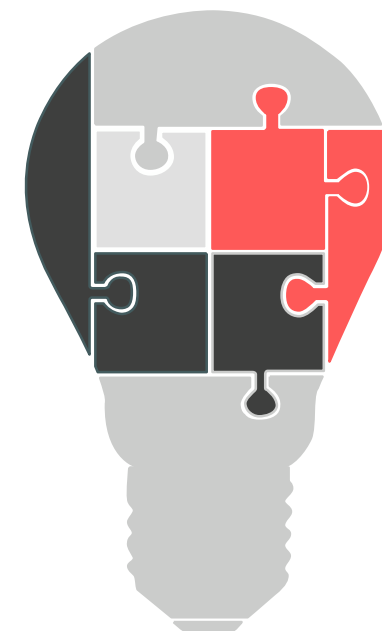
- Аудит производительности
- Настройка и мониторинг метрик
- Работы по ускорению работы приложений

### Сопровождение пользователей

- Абонентское обслуживание
- Линия консультаций

### Проектный офис

- Внедрение типовых конфигураций 1С
- Адаптация 1С
- Проекты автоматизации



## Хостинг 1С. PaaS-платформа и сервисы для размещения 1С заказчиков в облаке МТС

### Состав готового пакета:

- Вычислительные ресурсы для оптимальной работы приложений 1С;
- Настройка инфраструктуры, разворот и публикация баз клиента в облаке;
- Администрирование инфраструктуры и серверов 1С;
- Резервное копирование;
- Линия консультаций по работе с приложениями 1С;
- Автообновление типовых баз до актуальных релизов;
- Возможность использования СУБД PostgreSQL;
- Замена ключей 1С на программные.





## Тарифы Хостинг 1С

Параметры	Стандарт	Стандарт +
Работа пользователей через веб и тонкий клиент	+	+
Работа пользователей через TS (терминальный сервер)	-	+
Базовое количество обращений на ЛК*, шт.	3	3
Базовое количество ИБ** на обслуживании, шт.	5	5
Базовое количество места на 1 пользователя, ГБ	10	10
Работа с версиями 1С предыдущих поколений	-	+
Стоимость за пользователя (с НДС)	от 1 500, 00 ₽	от 2 700,00 ₽

#CloudMTS



**Майя Чубукова**

Руководитель направления 1С  
Департамент облачного бизнеса #CloudMTS

**+ 7 906 732 41 38**

[mchubukova@mts.ru](mailto:mchubukova@mts.ru)

[www.cloud.mts.ru](http://www.cloud.mts.ru)



#CloudMTS

**Спасибо!**

