UserGate

Безопасность корпоративных и технологических сетей. UserGate SUMMA

Антон Рахманенков

arakhmanenkov@usergate.ru
+7-916-720-40-08

О компании

Наш офис разработки находится в Технопарке Новосибирского Академгородка – в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

Дополнительные офисы: Москва, Санкт-Петербург, Хабаровск.

Важные даты UserGate

2001
запуск первой версии UserGate Proxy

2009
начало разработки первого российского NGFW UserGate

2010
создан внутренний стартап, в рамках которого началась разработка новой платформы

2012
UserGate – резидент Академпарка в Новосибирске

2015
UserGate – резидент Сколково

2016
выпуск нового UserGate как решения класса UTM

2018
создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2019
открытие первого московского офиса UserGate

2020
открытие офиса UserGate в Хабаровске

начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

2021
выход на рынок экосистемы безопасности UserGate SUMMA

2022
открытие офиса в Санкт-Петербурге

Философия UserGate

Основа для развития –
это лучшие технологии

Во время повсеместного использования открытого кода мы всегда полагаемся только на **собственные разработки** и полностью **контролируем свое решение**

В компании **UserGate** мы разрабатываем не только ПО, **мы разрабатываем всю платформу целиком**

Три уровня использования Open Source в разработке

1-й уровень

для тех, кто вообще ничего не умеет

1

Готовые продукты:

- pfSense
- OPNSense
- M0n0wall
- IPCop
- …

2-й уровень

для тех, кто сам научился собирать образы

2

Готовые продукты:

- Suricata
- Snort
- nDPI
- Squid
- OpenVPN
- OpenSSL
- …

3-й уровень
для профессионалов

3

Низкоуровневые библиотеки:

- Curl
- Python
- Apache
- Bash
- Telnet-server
- их сотни

Риски

Какие риски использования готовых продуктов:

- производительность (userspace);
- закладки (на уровне ядра);
- чужие списки фильтрации (иностранные);
- иностранные решения (ipoque DPI);
- блокирование источника кода;
- слабая поддержка кода в коммерческих проектах, скорость развития решения.

Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

Check Point

UserGate

CISCO

HUAWEI

paloalto NETWORKS

FORTINET

Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

Check Point

UserGate

CISCO

HUAWEI

paloalto NETWORKS

FORTINET

Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

UserGate → UserGate

Check Point

CISCO

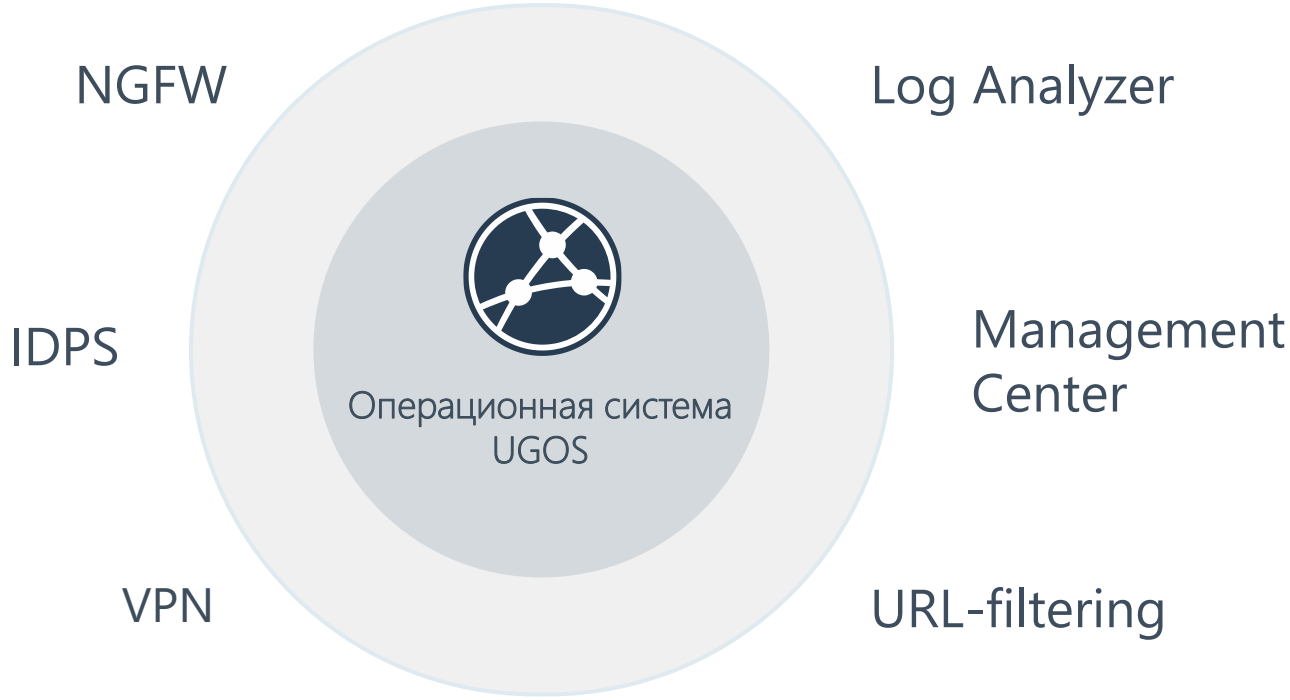
HUAWEI

paloalto NETWORKS

FORTINET

Операционная система UGOS

Уникальная архитектура UserGate и лежащая в ее основе операционная система UGOS позволяют обрабатывать и анализировать сетевой трафик на самых высоконагруженных каналах связи и добиваться эффективного масштабирования. В своих технологиях мы не используем Open Source.



Новое в 7.0

- CLI
- Система бэкапов
- SSL Forwarding
- UserGate Policy Language
- Cloud-init
- Новая архитектура процессоров - новые платформы
- Новый движок IPS

Аппаратные платформы UserGate

Промышленная платформа X10

Тип решения	X10
Блок питания	2шт.
Firewall throughput	2000 Mbit
NGFW (APP)	1200 Mbit
NGFW (IPS, APP, URLF)	280 Mbit
Temperature resistance	+40 до -70
New sessions per second	20000

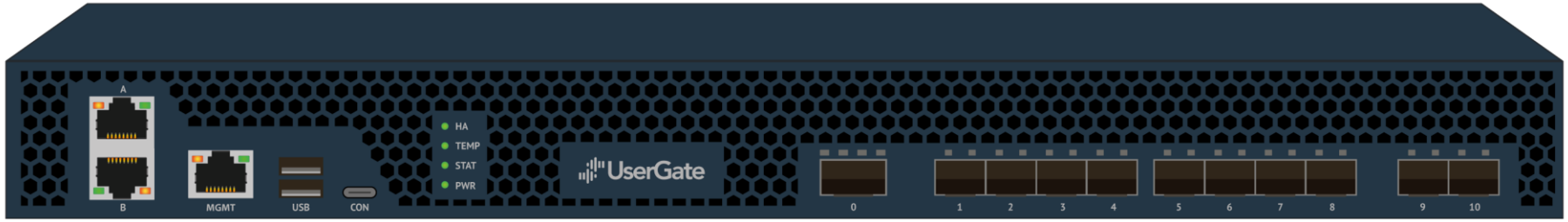
Модель X10

Собственная платформа C150

Тип решения	C150
Блок питания	2шт.
Firewall throughput	3000 Mbit
NGFW (APP)	1800 Mbit
NGFW (IPS, APP, URLF)	800 Mbit
New sessions per second	20000

Модель C150

Платформа UserGate FG



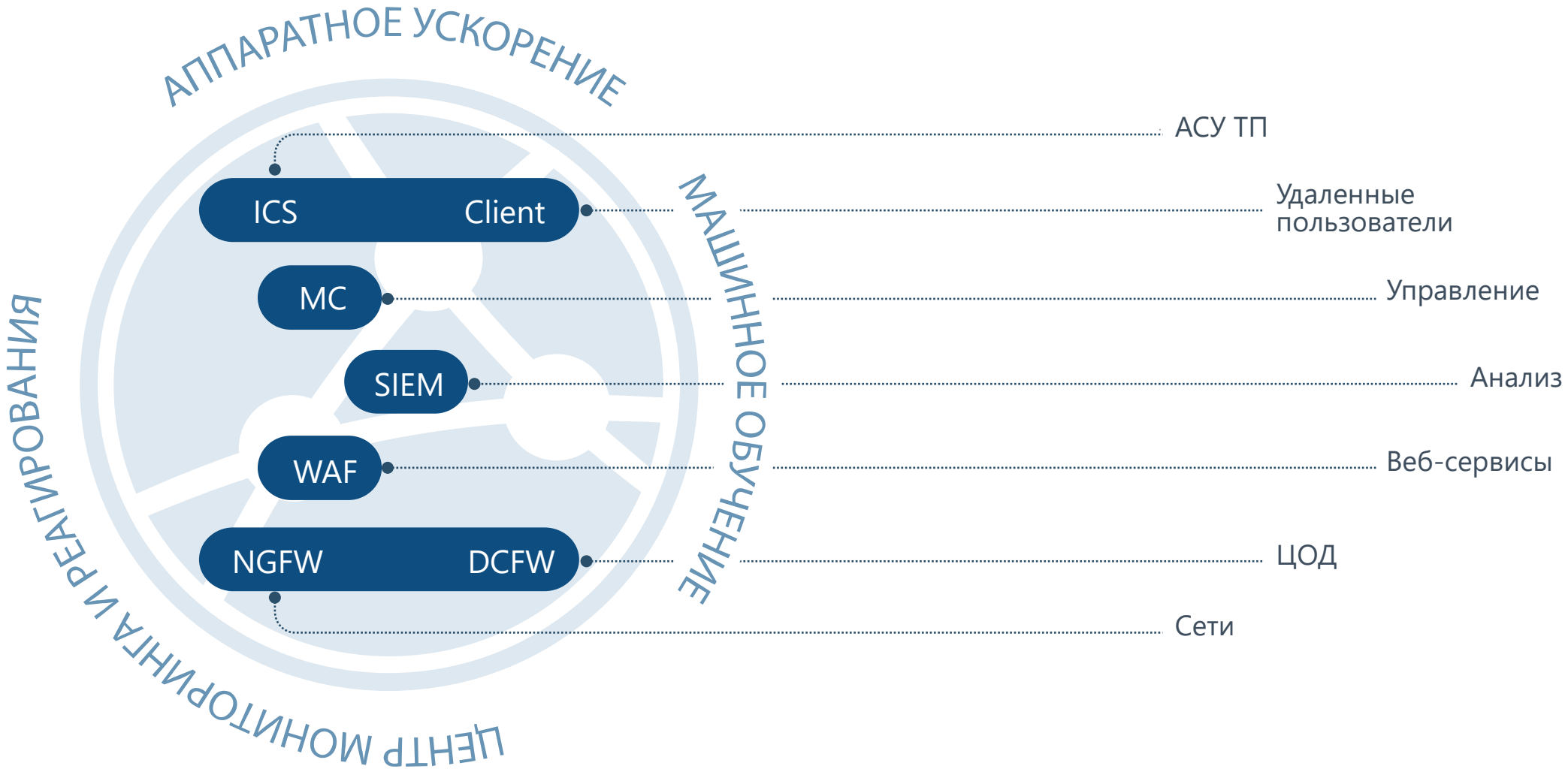
- аппаратная обработка трафика на ПЛИС
- производительность МЭ более 100+ Gbps, пакеты 64 байта, трафик реальных приложений
- производительность PPS ~ 120 Mpps
- Wire speed – производительность МЭ = скорости сетевого интерфейса
- собственная разработка
- доверие к ПАК Минпромторга России

Сетевые порты:

- 10 x 10 Gbps SFP+
- 1 x 100 Gbps QSFP28
- 2 x 1 Gbps BASE-T
- IPMI
- SSD: от 128 Гб
- RAM: от 64 Гб
- БП: 2 с горячей заменой

UserGate SUMMA

UserGate SUMMA



UserGate Client

UserGate Client

Программное обеспечение класса (EDR) для конечных устройств предоставляет дополнительную информацию о конечной точке и позволяют контролировать устройство внутри и за пределами периметра.

- Сообщает экосистеме компонентов безопасности UserGate SUMMA о состоянии устройства, работающих на нем приложениях и версиях ПО.
- Управляет политиками используемых на устройстве приложений.
- Контролирует доступ в сеть на основе политик соответствия требованиям (Network Access Control, NAC).
- Реализует подключение к корпоративной сети, построенное на принципах сетевого доступа с нулевым доверием (Zero Trust Network Access, ZTNA).

UserGate Log Analyzer

UserGate Log Analyzer

Выделенный сервер сбора и хранения логов, журналирования и анализа событий

- Уменьшение нагрузки на шлюзы UserGate.
- Создание кастомных отчетов.
- Объединение журналов с нескольких шлюзов для общего анализа.
- Функции SIEM и IRP.

UserGate Management Center

UserGate Management Center

Единая точка управления

- Централизованно настраиваются все параметры работы межсетевых экранов.
- Создание управляемой области.
- Создание шаблона или несколько шаблонов, каждый из которых опишет свою часть настроек межсетевых экранов.
- Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку управляемых устройств UserGate.
- Добавление управляемого устройства и применение к нему группы шаблонов.

ICS, безопасность промышленных сетей

Угрозы IT и OT

Угрозы IT	Угрозы OT
Конфиденциальность	▪ Человеческие жертвы ▪ Техногенные катастрофы
Целостность	▪ Повреждение оборудования ▪ Простои производства
Доступность	Конфиденциальность данных

Сегментирование

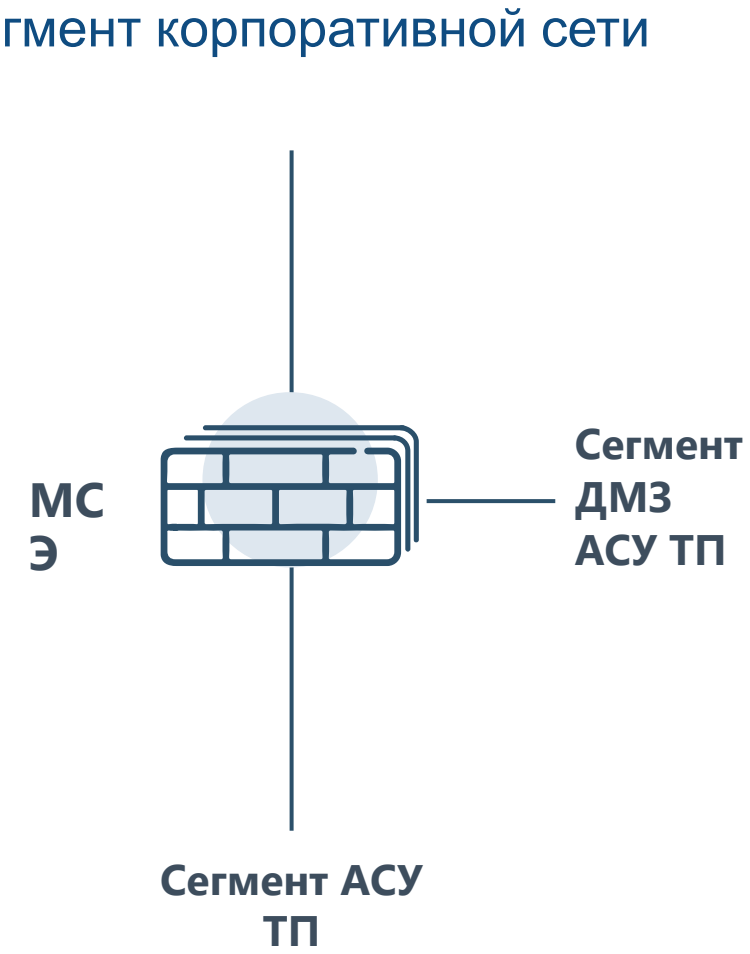
NIST

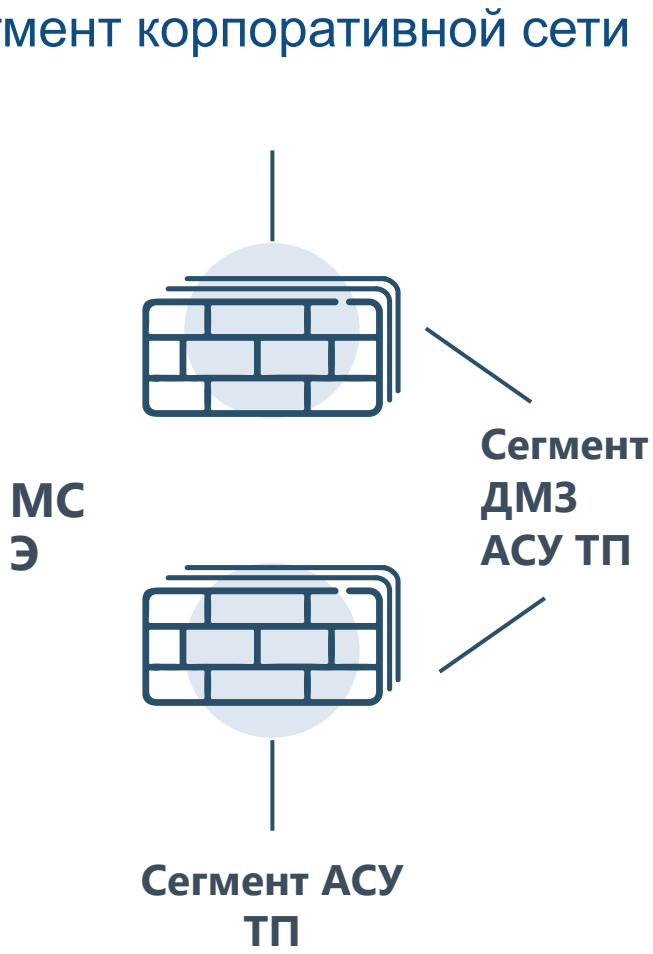
ISA 99

ГОСТ

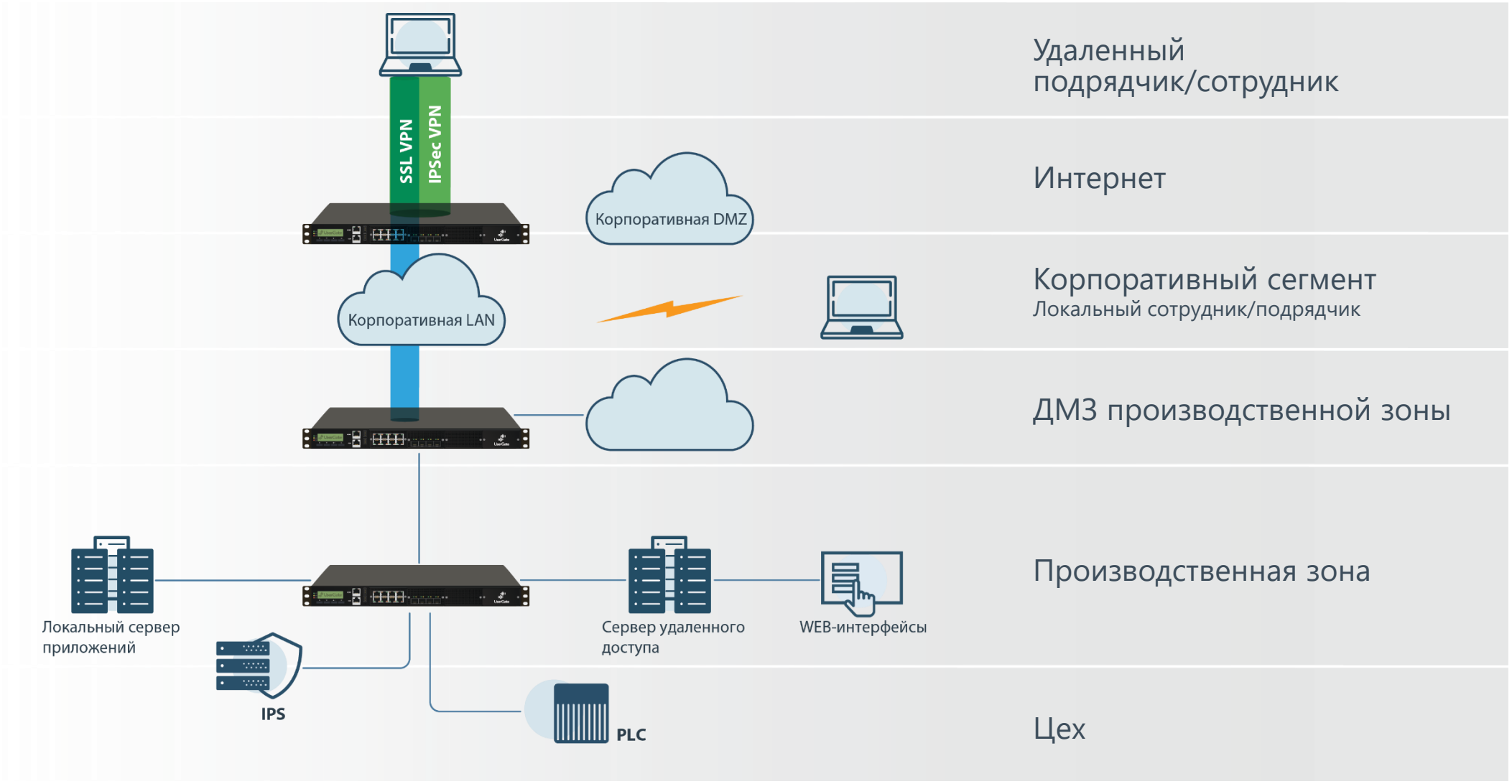
МЭК

CpwE





Общая архитектура



Законодательство, бумажная безопасность

Законодательство

Для выполнения требований 17 (ГИС), 21 (ПДн), 31 (АСУ ТП) и 239 (ЗО КИИ) приказов ФСТЭК России необходимо использовать только те СЗИ, которые прошли процедуру соответствия требованиям к УД. Для 239 приказа это требование в полную силу вступает с 2023 года.

250 Приказ Президента РФ запрещает использовать средства защиты информации, странами происхождения которых являются недружественные иностранные государства либо производителями которых являются организации, находящиеся под юрисдикцией таких государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

В Госдуму внесен законопроект «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных.

ФСТЭК России

UserGate первым на отечественном рынке ИБ получил **четыре из пяти профилей** защиты
в рамках одного сертификата ФСТЭК России № 3905.

- **Требования к МЭ**
  Профиль защиты МЭ типа А 4-го класса защиты
  Профиль защиты МЭ типа Б 4-го класса защиты
  Профиль защиты МЭ типа Д 4-го класса защиты
  Профиль защиты МЭ типа Г 4-го класса защиты

- **Требования к СОВ**
  Профиль защиты СОВ уровня сети 4-го класса защиты

Уровень доверия 4:

- классы защиты СЗИ 4
- ЗО КИИ 1 категории
- ГИС 1 класса
- АСУ ТП 1 класса
- ИСПДн 1 уровня
- ИСОП II класса

№ 3905

Реестр Министерства промышленности и торговли РФ

Модель С150

Союз «Торгово - промышленная палата Новосибирской области» (Союз «ТПП Новосибирской области»)

Услуги Союза «Торгово-промышленная палата Новосибирской области» соответствуют международным стандартам качества ISO 9001:2015

ИНН 5404102991, Россия, 630073, Новосибирск, пр. К. Маркса, 1, тел.: (383) 346 41 50, (383) 346 54 01, nsk@ntpp.ru, www.ntpp.ru

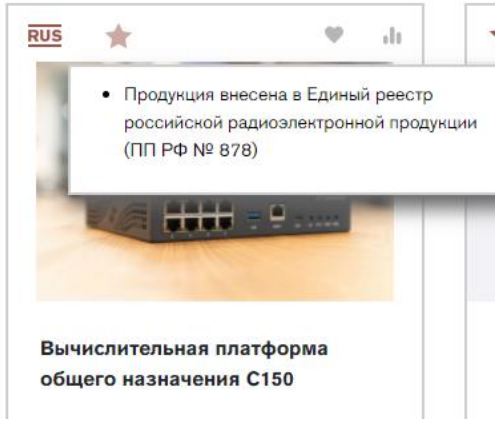
ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

к сертификату о происхождении товара формы СТ-1 № 2016000233 от 23.03.2022 г., в соответствии с которым Российская Федерация является страной происхождения товара (промышленной продукции)

№	Наименование производимой промышленной продукции	Код промышленной продукции по ОК 034 2014 (КПЕС 2008)	Код промышленной продукции по ТН ВЭД ЕАЭС	Реквизиты документа[1], содержащего требования к производимой промышленной продукции
1.	Вычислительная платформа общего назначения С150	26.20.40.140	8473 30	РНЦД.465235.001 ТУ

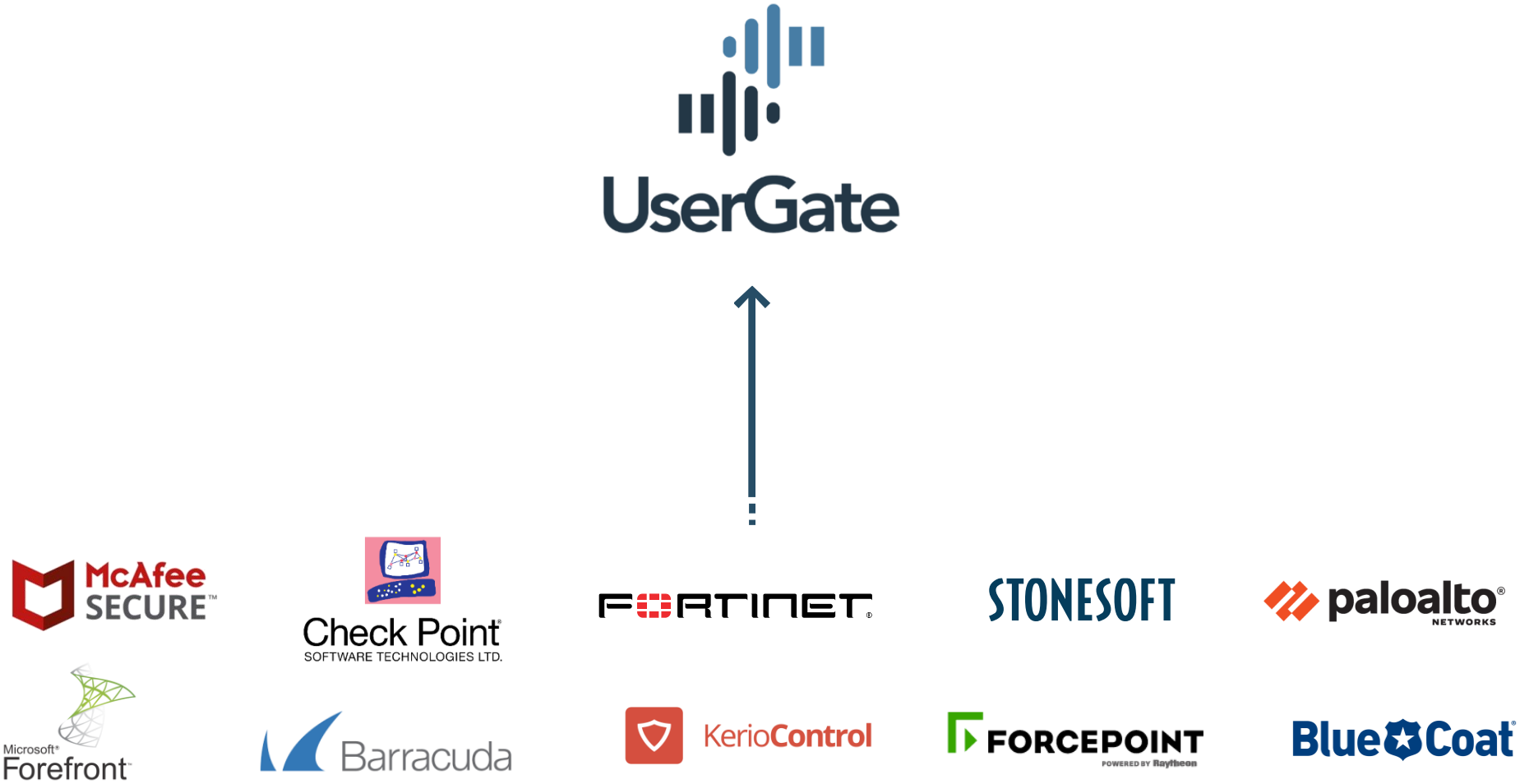
Срок действия: заключение действительно в течение 1 года со дня его выдачи.

Директор Департамента радиоэлектронной промышленности Ю.В. Плясунов



Немного о рынке

Переход со сторонних решений



Нас выбирают

ПЕНСИОННЫЙ ФОНД РОССИЙСКОЙ ФЕДЕРАЦИИ
РОССЕТИ
Ростелеком
РусГидро
ГАЗПРОМ МЕЖРЕГИОНГАЗ
РОСНЕФТЬ
Транснефть

ВТБ
ПСБ
абсолют банк
АО «СО ЕЭС»
УрГУПС

KNAUF
УВЗ УралВагонЗавод
ФОСАГРО
FESCO
ГалоПолимер
горки город
S7

MEGAFON
29TH WINTER UNIVERSIADE KRASNOYARSK 2019
ТВЦ
ГЕМОТЕСТ медицинская лаборатория
lady & gentleman CITY

Пилотирование UserGate

DEMO

Отправьте заявку на пилотирование или запросите демонстрацию решений UserGate

sales@usergate.ru
8 (800) 500-40-32

UserGate

Благодарим за внимание!

Антон Рахманенков

arakhmanenkov@usergate.ru
+7-916-720-40-08