



UserGate SUMMA. Комплексный подход к обеспечению информационной безопасности

Кишина Валерия

Менеджер по работе с клиентами
vkishina@usergate.com

8 800 500 40 32 | +7 (983) 130-18-72



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

Дополнительные офисы:
г. Москва, г. Санкт-Петербург,
г. Хабаровск.



О компании 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

2019

открытие первого московского офиса UserGate

2018

создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2016

выпуск нового UserGate как решения класса UTM

2015

UserGate – резидент Сколково

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

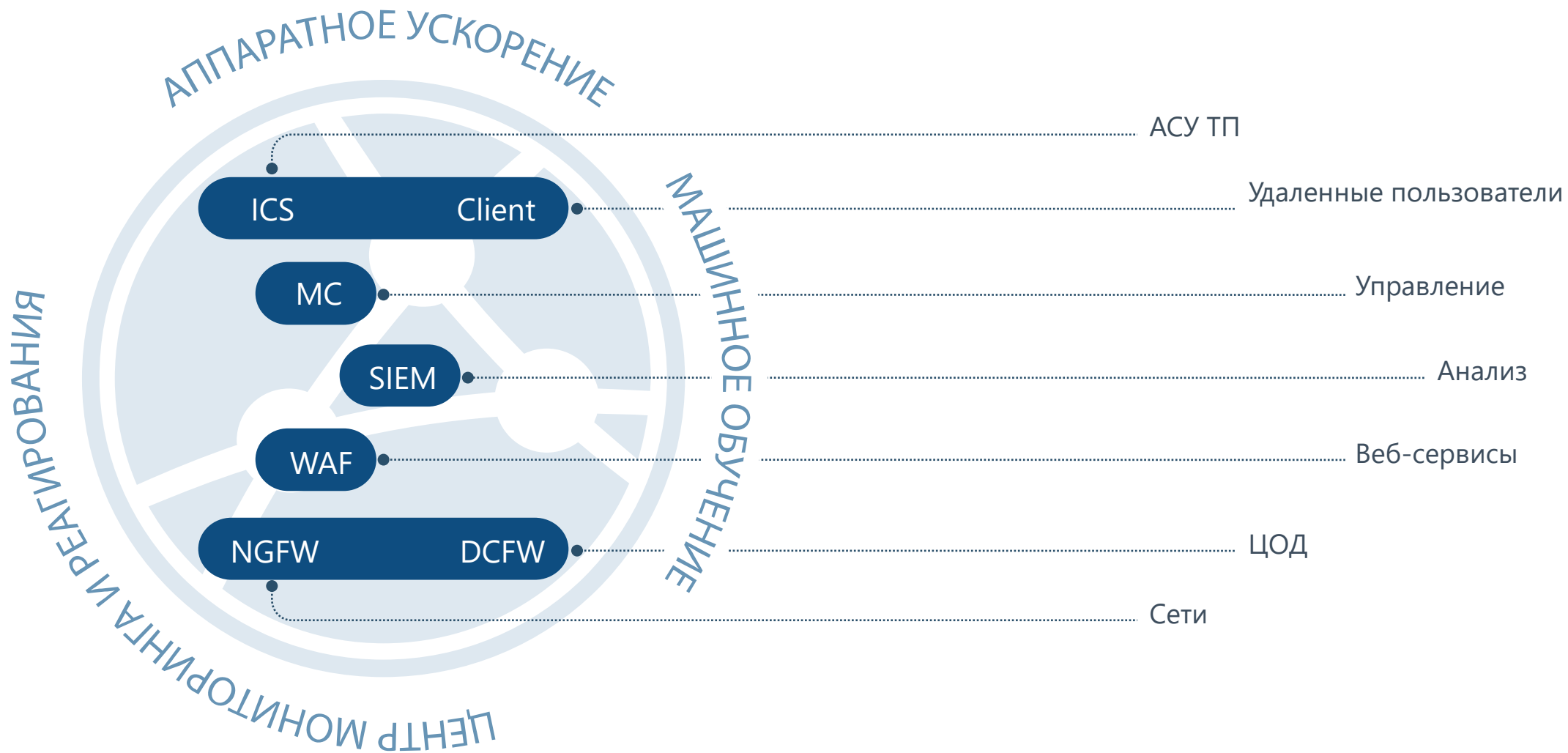
2022

открытие офиса в Санкт-Петербурге



UserGate SUMMA

100% видимость событий безопасности



UserGate NGFW

Межсетевой экран следующего поколения



Next-Generation Firewall

- Высокая скорость обработки трафика
- Идентификация пользователей
- Применение гибких политик к пользователям
- Контроль приложений на L7 уровне по всем портам
- Интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и поддержкой TLS ГОСТ
- Инспекция SSH
- Защита от DoS-атак



IDPS (COB)





Система обнаружения вторжений

Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

The screenshot displays the interface of an intrusion detection system. On the left, there is a search filter panel with four columns: 'Уровень угрозы' (Threat Level), 'Протокол' (Protocol), 'Категория' (Category), and 'Класс' (Class). The 'Уровень угрозы' column has five options: 1 (очень низкий), 2 (низкий), 3 (средний), 4 (высокий), and 5 (очень высокий). The 'Протокол' column has three options: icmp, ip, and tcp. The 'Категория' column has a scrollable list of categories including activex, attack_response, current_events, dns, dos, exploit, ftp, imap, info, malware, misc, mobile_malware, netbios, p2p, and policy. The 'Класс' column has a scrollable list of classes including attempted-user, attempted-admin, attempted-dos, attempted-recon, attempted-user, bad-unknown, default-login-attempt, denial-of-service, misc-activity, network-scan, non-standard-protocol, not-suspicious, policy-violation, and protocol-command-decode. A 'Применить' (Apply) button is at the bottom right of the filter panel.

On the right, there is a 'Сигнатуры' (Signatures) section with a table of detected signatures. The table has five columns: 'Сигнатура' (Signature), 'Прото...' (Protocol), 'Класс' (Class), 'CVE', and 'Категория' (Category). The table contains 12 rows of data, each with a red '5' icon in the first column.

Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon CyViewer ActiveX Control SaveData Insecure Method Vulnerability	tcp	attempted-user	Нет	activex
Win32/Infostealer.Snifula File Upload	tcp	trojan-activity	Нет	trojan
Possible ZyXEL P660HN-T v1 RCE	tcp	attempted-user	Нет	exploit
User-Agent (Win95)	tcp	trojan-activity	Нет	malware
STAT overflow attempt	tcp	attempted-admin	CVE-2001-1021,CVE-2001-0...	ftp
Terror EK CVE-2016-0189 Exploit	tcp	trojan-activity	CVE-2016-0189	current_even
Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UPDATE	tcp	web-application-attack	CVE-2006-7161	web
Rialto SQL Injection Attempt -- searchoption.asp acreage1 INSERT	tcp	web-application-attack	CVE-2006-6927	web



Контентная фильтрация



Механизмы фильтрации

- фильтрация по категориям;
- морфологический анализ;
- безопасный поиск;
- белые и черные списки;
- блокировка контекстной рекламы;
- запрет загрузки определенных видов файлов;
- антивирусная проверка трафика;
- интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и TLS ГОСТ.



- крупнейшая база электронных ресурсов – более 600 миллионов сайтов;
- 80+ категорий;
- ежедневное обновление списка сайтов;
- повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории.

Группы URL категорий			
+ Добавить ✎ Редактировать ✖ Удалить ↻ Обновить			
Название			
Threats			
Parental Control			
Productivity			
Safe categories			
Recommended for morphology checking			
Recommended for virus check			

Списки морфологии			
+ Добавить ✎ Редактировать ✖ Удалить ↻ Обновить			
Название списка	Author	Порог	
1 Нецензурная лексика	© UserGate	Обычный	🔄
2 Наркотики	© UserGate	Обычный	🔄
3 Порнография	© UserGate	Обычный	🔄
2 Суицид	© UserGate	Обычный	🔄
5 Терроризм	© UserGate	Обычный	🔄
3 Соответствие списку запрещенных матер...	© UserGate	Обычный	🔄
4 Азартные игры	© UserGate	Обычный	🔄
3 Соответствие ФЗ-436 (защита детей)	© UserGate	Обычный	🔄
1 Юридический (DLP)	© UserGate	Обычный	🔄
3 Бухгалтерия (DLP)	© UserGate	Обычный	🔄
3 Финансы (DLP)	© UserGate	Обычный	🔄
5 Персональные данные (DLP)	© UserGate	Обычный	🔄
2 Маркетинг (DLP)	© UserGate	Обычный	🔄
1 Соответствие списку запрещенных матер...	© UserGate	Обычный	🔄

Категории	
+ Добавить ✖ Удалить 📄 Экспорт ↻ Обновить 📂 Импорт	
Название ↑	
4	Азартные игры
2	Жестокое обращение с детьми
2	Игры
2	Наркотики
2	Насилие
5	Незаконное ПО
2	Ненависть и нетерпение
2	Нецензурная лексика
2	Нудизм
4	Обмен картинками
2	Оружие
4	Пиринговые сети
1	Поиск работы
2	Покупки

Списки URL	
+ Добавить ✎ Редактировать ✖ Удалить	
Название ↑	
3	Microsoft Windows Internet checker
5	Соответствие реестру запрещенных сайтов Роскомнадзора (URL)
3	Соответствие списку запрещенных URL Министерства Юстиции РФ (URL)
5	Соответствие списку запрещенных URL Республики Казахстан
1	Список образовательных учреждений
4	Список поисковых систем без безопасного поиска
5	Список фишинговых сайтов

Про SSL-инспекцию





Про SSL-инспекцию

Обязательно:

- Проверка всей цепочки сертификатов!!!
- Выбор алгоритма шифрования (только strong)
- TLS 1.3, TLS ГОСТ
- Проверка движком IDPS

<input checked="" type="checkbox"/>	TLS GOST2012256 with 28147 CNT IMIT
<input checked="" type="checkbox"/>	TLS GOSTR341001 with 28147 CNT IMIT

Профиль SSL:

Записывать в журнал правил:

Атрибуты:

- Блокировать сайты с некорректными сертификатами
- Проверять по списку отозванных сертификатов
- Блокировать сертификаты с истекшим сроком действия
- Блокировать самоподписанные сертификаты

Протоколы SSL

Минимальная версия TLS:

Максимальная версия TLS:

Наборы алгоритмов шифрования

[Установка алгоритмов шифрования для стандартных протоколов](#)

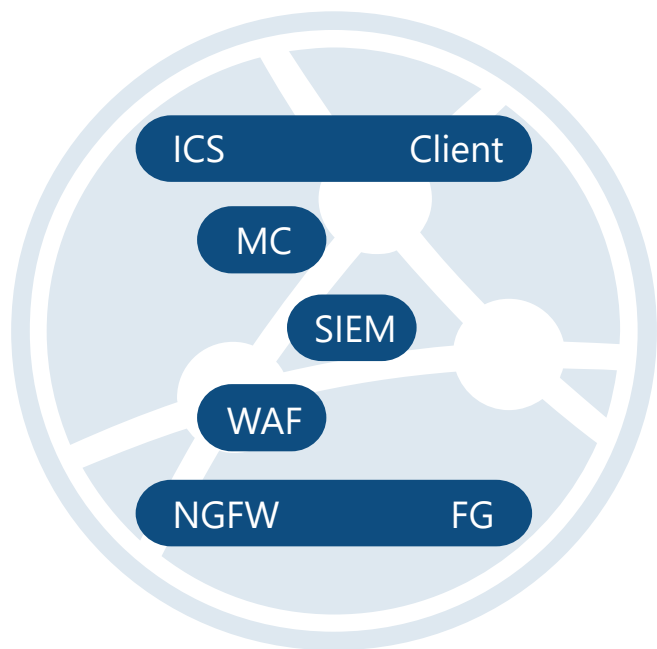
<input checked="" type="checkbox"/>	TLS ECDHE ECDSA with AES 256 CBC SHA384
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS ECDHE ECDSA with 3DES EDE CBC SHA
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS DHE DSS with AES 128 GCM SHA256
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS ECDH ECDSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS ECDH ECDSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 128 GCM SHA256
<input checked="" type="checkbox"/>	TLS DHE DSS with AES 256 GCM SHA384



Формы поставки



Продукты UserGate SUMMA доступны в виртуальном исполнении



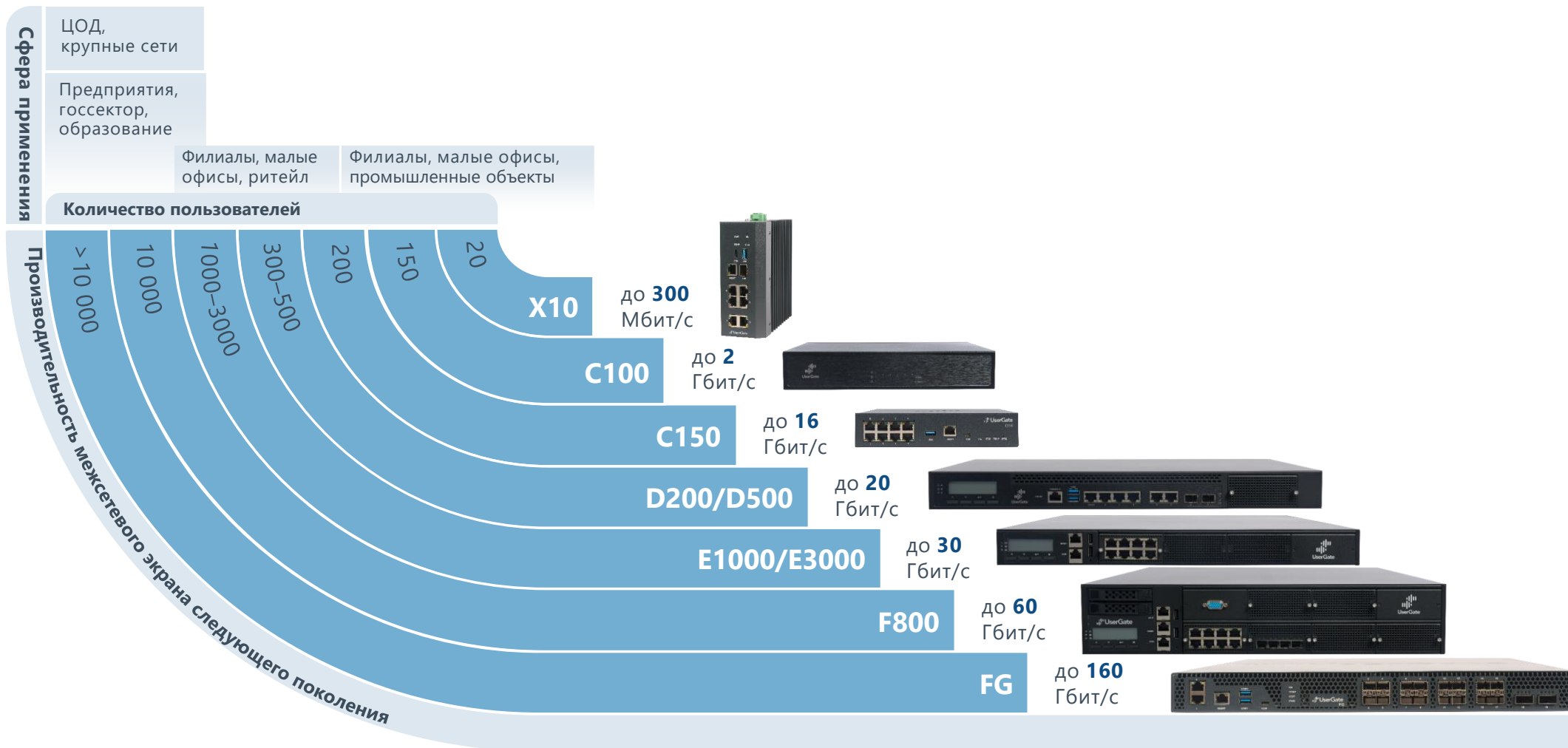
Гипервизоры:





UserGate NGFW

Модельный ряд аппаратных платформ



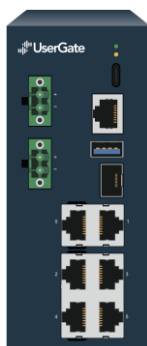
A decorative graphic on the right side of the slide, consisting of a network of light blue lines and dots, resembling a molecular structure or a data network, set against a dark blue background.

Собственные разработки железа



Собственные аппаратные платформы

МПТ



Модель X10

- FW до 2,5 Гб/с
- ARM 4 cores
- 6 портов 1GbE с поддержкой bypass
- 1 порт SFP
- два блока питания
- от – 40 °С до +70 °С
- крепление на DIN-рейку



Модель C150

- FW до 8 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- два блока питания
- от 0 °С до +70 °С



Новые платформы



FG



C150



B50

A decorative graphic on the right side of the slide, consisting of a complex network of light blue lines and dots, resembling a molecular structure or a data network, set against a dark blue background.

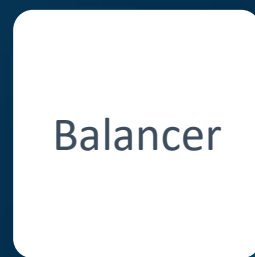
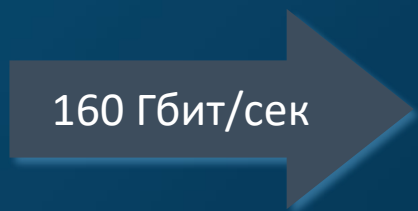
Высокопроизводительный FW

UserGate FG

- »» CPS - 80 000 сессий в секунду
- »» CC - 11 000 000 TCP сессий
- »» UDP 1518 byte - 150+ гбит/с
- »» EMIX - 65 гбит/с (цифра из ограничения тестового стенда)
- »» CPS - 35 000, 10 000 правил
- »» 80M PPS



2x100 + 16x10, wirespeed





Реализованные проекты



Защита инфраструктуры крупного государственного телеком-оператора

- Обеспечение безопасности сетевой инфраструктуры от интернет-угроз;
- Контроль доступа пользователей к внешним ресурсам и приложениям;
- Контроль доступа удаленных пользователей к информационным ресурсам заказчика;
- Создание легко масштабируемой системы информационной безопасности;



ООО «АльфаСтрахование — ОМС»

Контентная фильтрация web-трафика

- Переход с иностранного вендора;
- Оптимизация оборудования;
- Безопасный выход в интернет;
- Фильтрация трафика.



Нас выбирают





Новое в 7.1





Новое в 7.1

- » UserID
- » Пользовательские сигнатуры IDPS&L7
- » Новый движок IPSv3
- » IKEv2
- » Темная тема
- » UserGate Client
- » UserGate SIEM Light (MVP)



Пилотирование UserGate



DEMO

Отправьте заявку на пилотирование или
запросите демонстрацию решений
UserGate

sales@usergate.ru

8 (800) 500-40-32



**Спасибо
за внимание!**

Кишина Валерия

Менеджер по работе с клиентами

vkishina@usergate.ru

8 800 500 40 32 | +7 (983)-130-1872

