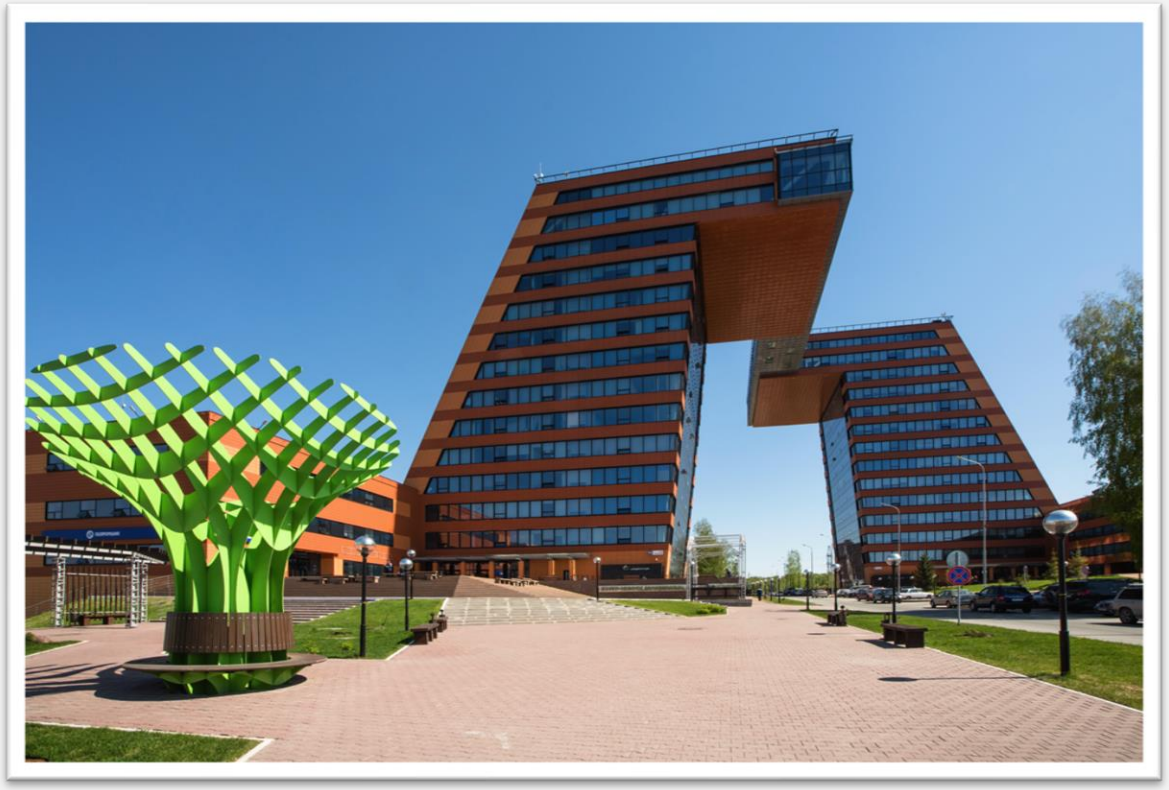
UserGate:
Интернет-безопасность для предприятий любого размера

Антон Рахманенков
ведущий менеджер
по работе с корпоративными клиентами

arakhmanenkov@usergate.com
8 800 500 40 32 | +7-916-720-40-08



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

Дополнительные офисы:
г. Москва, ИЦ «Сколково»
г. Хабаровск

Анализ и корреляция событий
(UserGate LogAn)

Межсетевой экран
(Enterprise Firewall, NGFW)

Система обнаружения и предотвращения вторжений
(IPS/IDS)

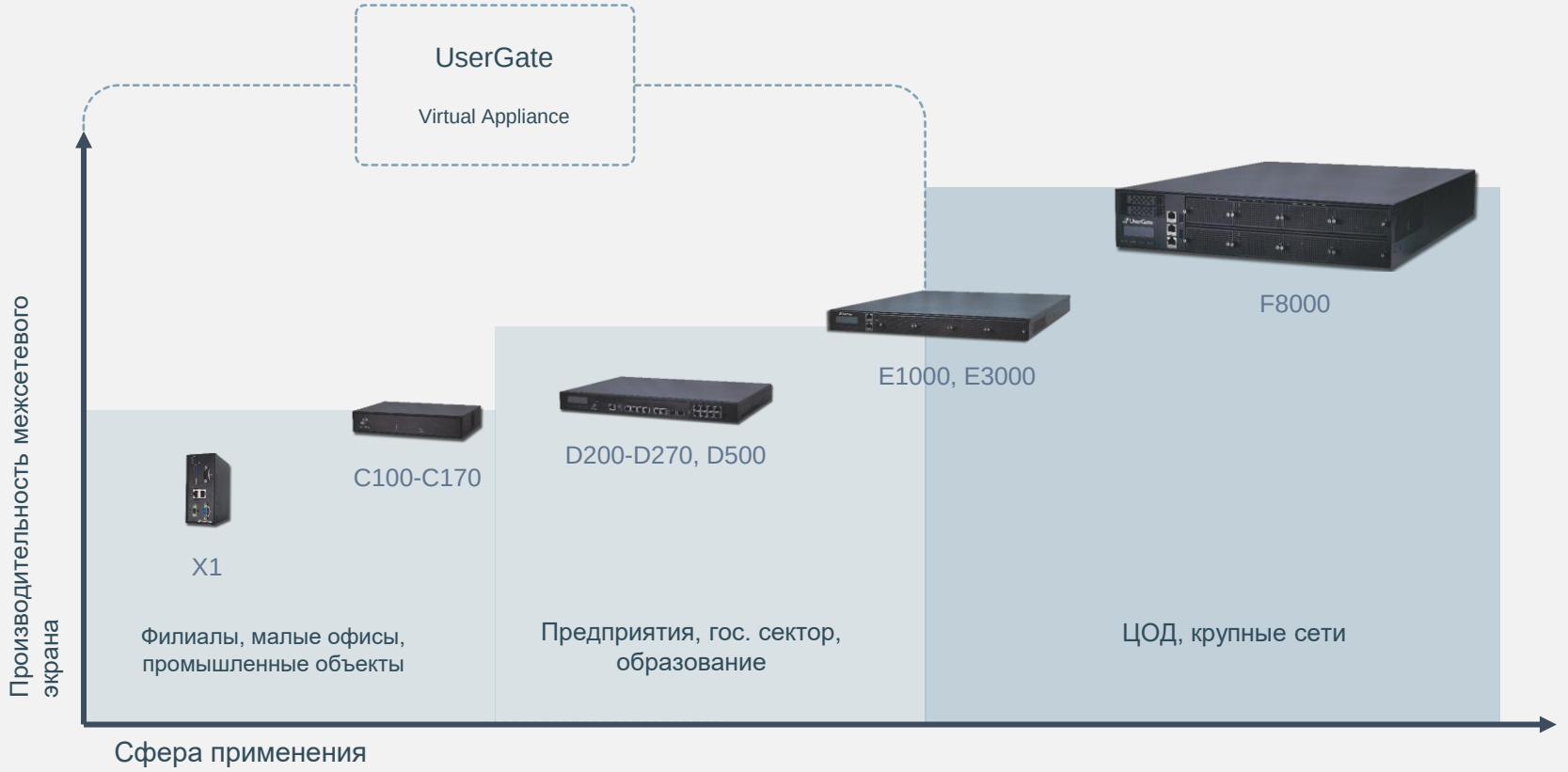
Операционная система UG OS

Прокси сервер
(Proxy)

Централизованное управление
(UserGate Management Center)

Собственные аппаратные платформы

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



Межсетевой экран NGFW

Безопасная публикация ресурсов и сервисов

Система обнаружения и предотвращения вторжений

Анализ команд в протоколах АСУ ТП

Интернет фильтрация

- Межсетевой экран нового поколения
- Системы обнаружения вторжений (IDS/IPS)
- Доступ к внутренним ресурсам через SSL VPN Portal
- Анализ и выгрузка информации об инцидентах безопасности (SIEM)
- Обратный прокси (Reverse proxy)
- Автоматизация реакции на угрозы безопасности информации (SOAR)
- Контроль приложений L7
- Антивирус с эвристическим анализом (опция)

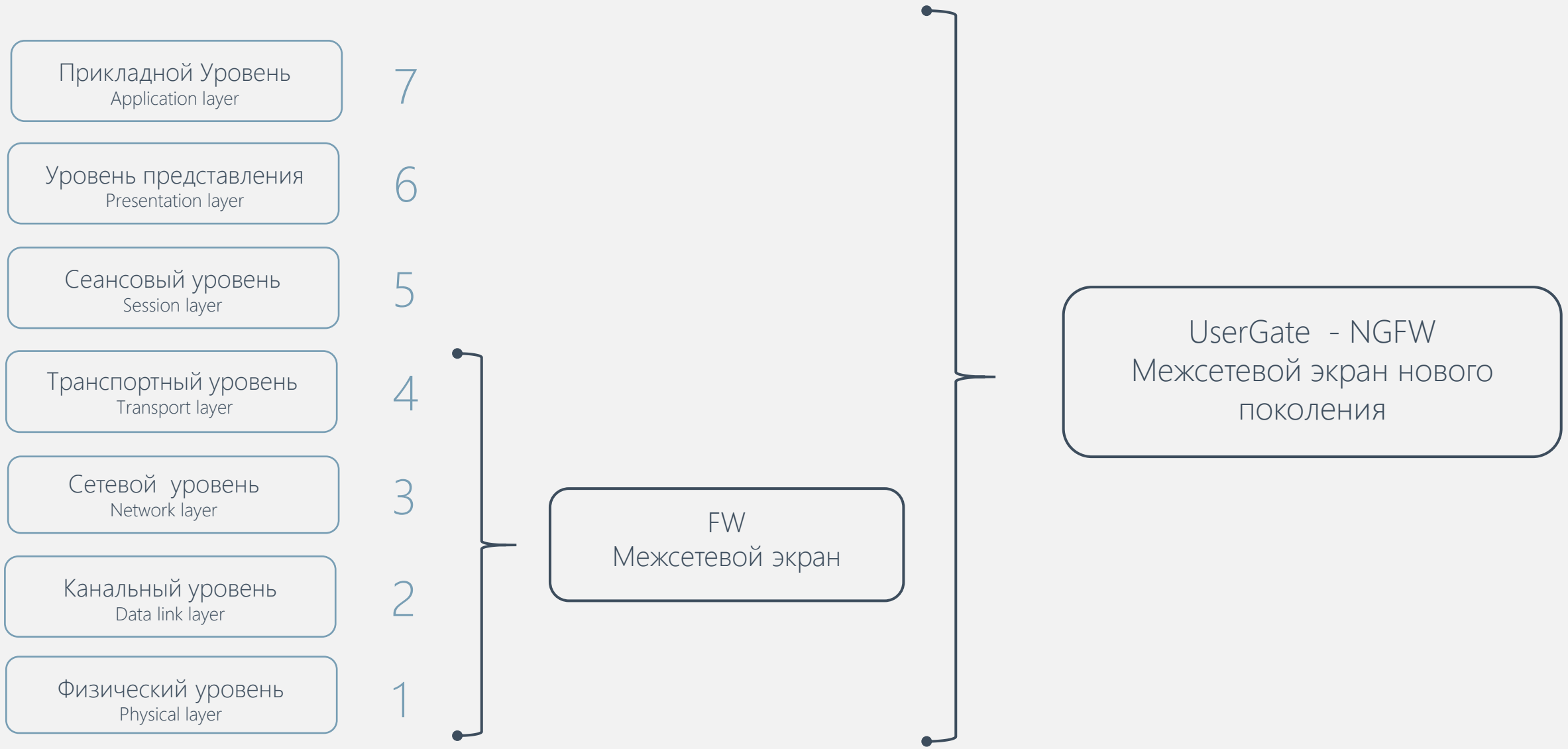
- Контроль доступа в интернет
- Дешифрование SSL
- Идентификация пользователей
- Виртуальная частная сеть (VPN)
- Поддержка АСУ ТП (SCADA)
- Удаленное администрирование
- Безопасная публикация внутренних ресурсов и сервисов
- Поддержка высокой отказоустойчивости и кластеризации

UserGate - Next Generation Firewall

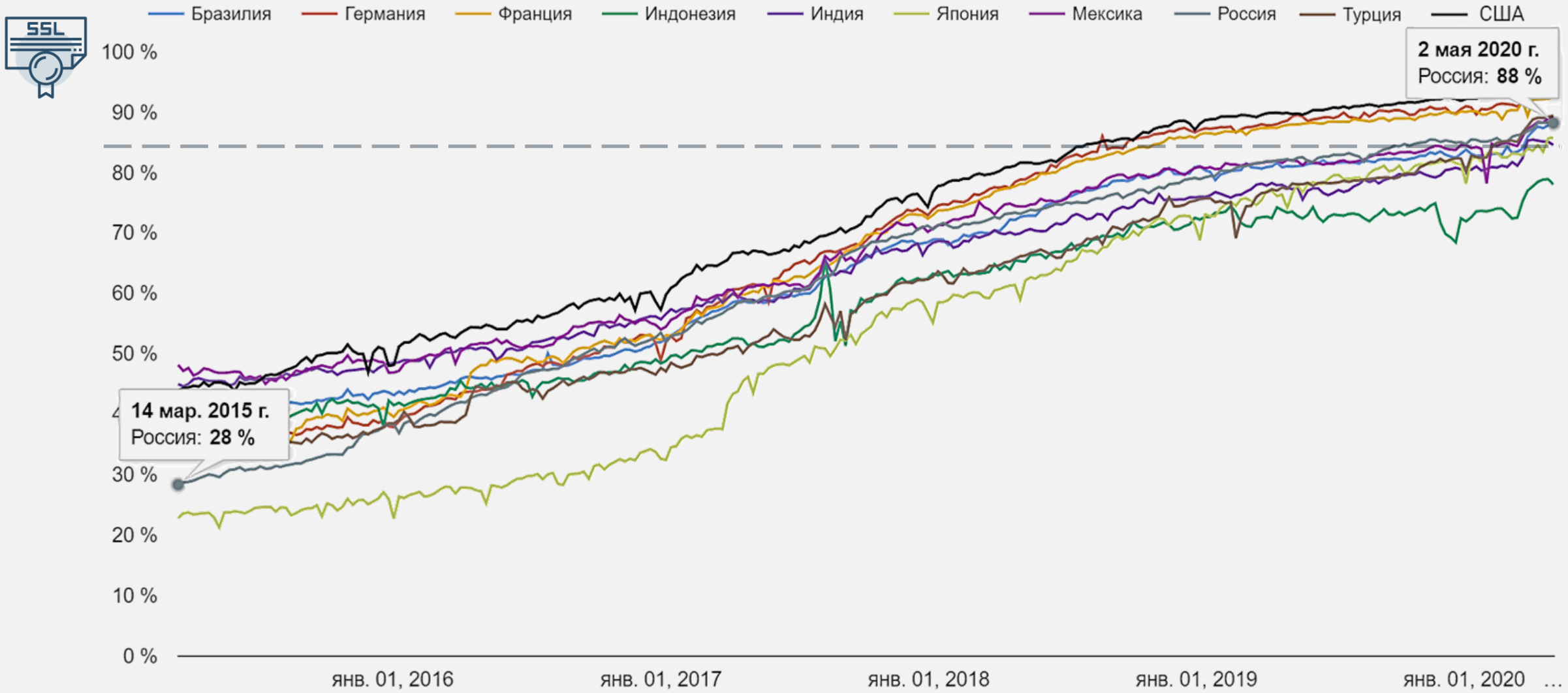
- Сегментирование сети, контроль и анализ трафика между сегментами
- Контроль приложений на L7 уровне по всем портам. Позволяет ограничить трафик для управления сетевыми протоколами и ограниченным набором утвержденных приложений/протоколов для администрирования/сигнализации.
- Идентификация и контроль действий пользователей АСУ ТП (операторов, администраторов, устройств)
- Политика доступа по времени суток вместе с идентификацией приложений и пользователей.
- Возможность централизованного развертывания различных политик и конфигураций на географически распределенных объектах.
- Поддержка ролевой модели доступа.
- Предоставление централизованных отчетов, которые облегчают экспертизу и соблюдение нормативных требований.

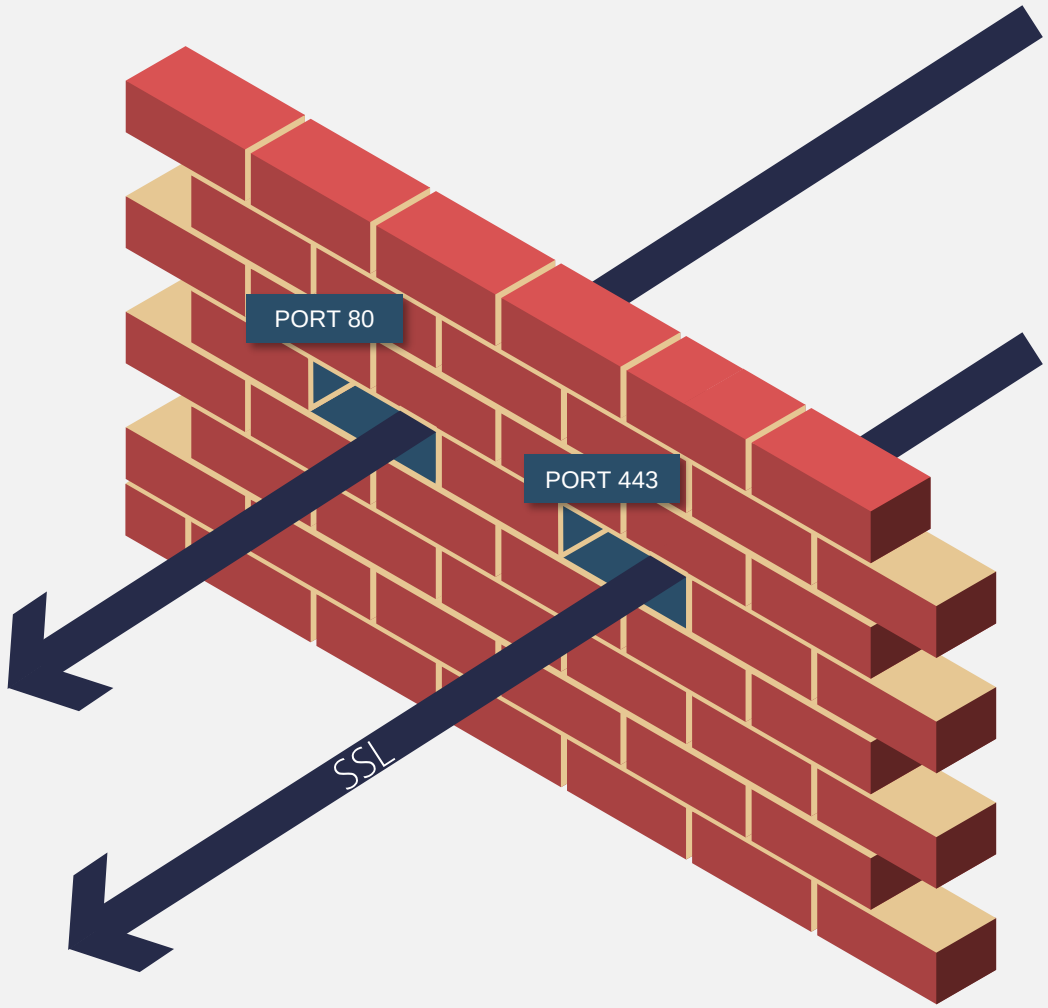
Аутентификация пользователей и применение к пользователям правил межсетевого экранирования, контентной фильтрации, контроля приложений с поддержкой таких средств и протоколов аутентификации, как Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, MFA.

Администраторы могут применить определенные политики безопасности к любому пользователю, группе пользователей или, например, ко всем неизвестным пользователям.


Прикладной Уровень
Application layer
7
Уровень представления
Presentation layer
6
Сеансовый уровень
Session layer
5
Транспортный уровень
Transport layer
4
Сетевой уровень
Network layer
3
Канальный уровень
Data link layer
2
Физический уровень
Physical layer
1
FW
Межсетевой экран
UserGate - NGFW
Межсетевой экран нового поколения

Процент страниц, загружаемых по HTTPS в Chrome по странам/регионам

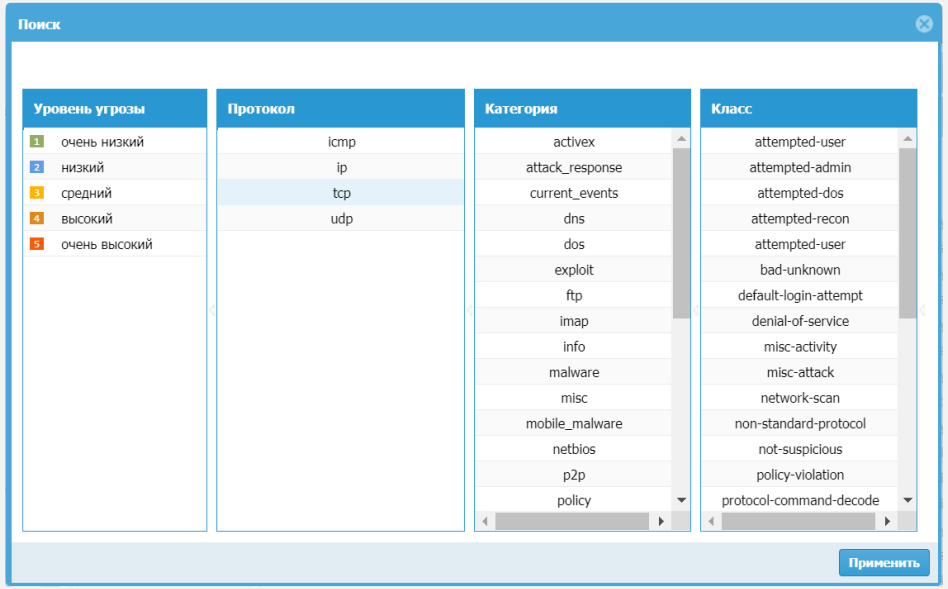


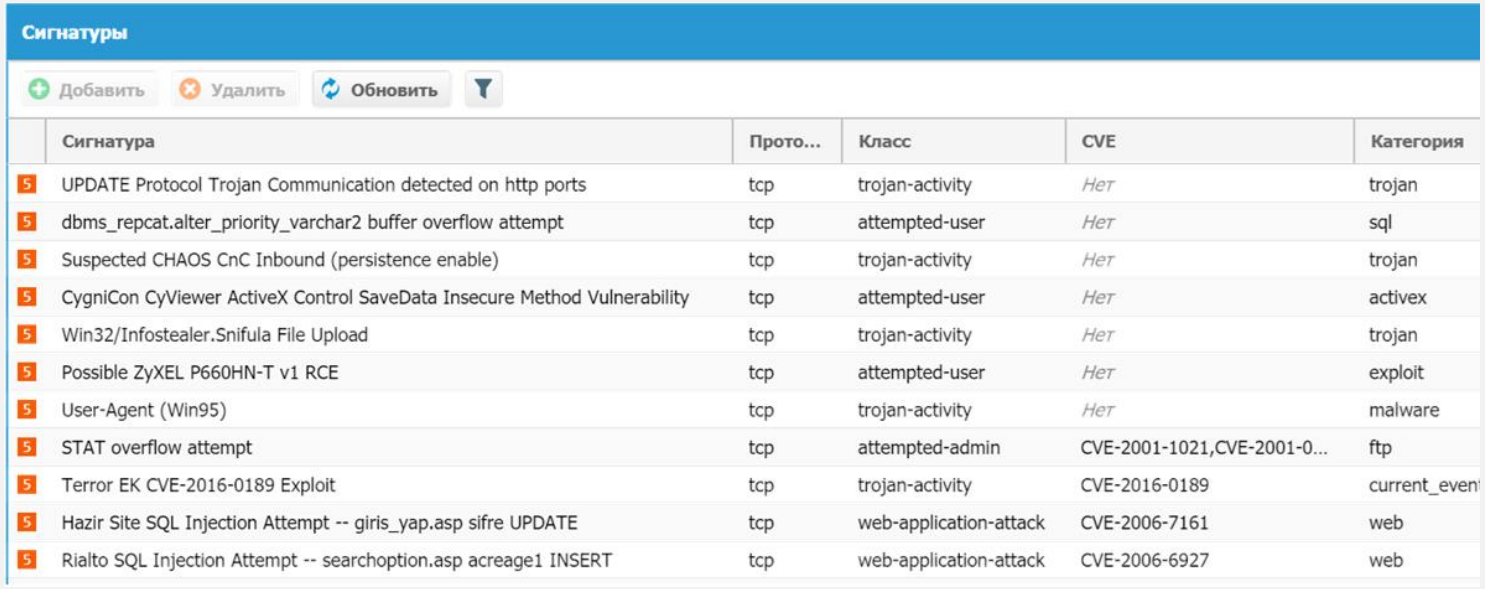


kaspersky Yandex Яндекс.Диск zoom Viber Gmail by Google eset @mail.ru Microsoft Office Update ssh COMMUNICATIONS SECURITY AMMYY JUST DO IT REMOTELY SSL

СОВ - Система обнаружения и предотвращения вторжений (IPS - Intrusion Prevention System)

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

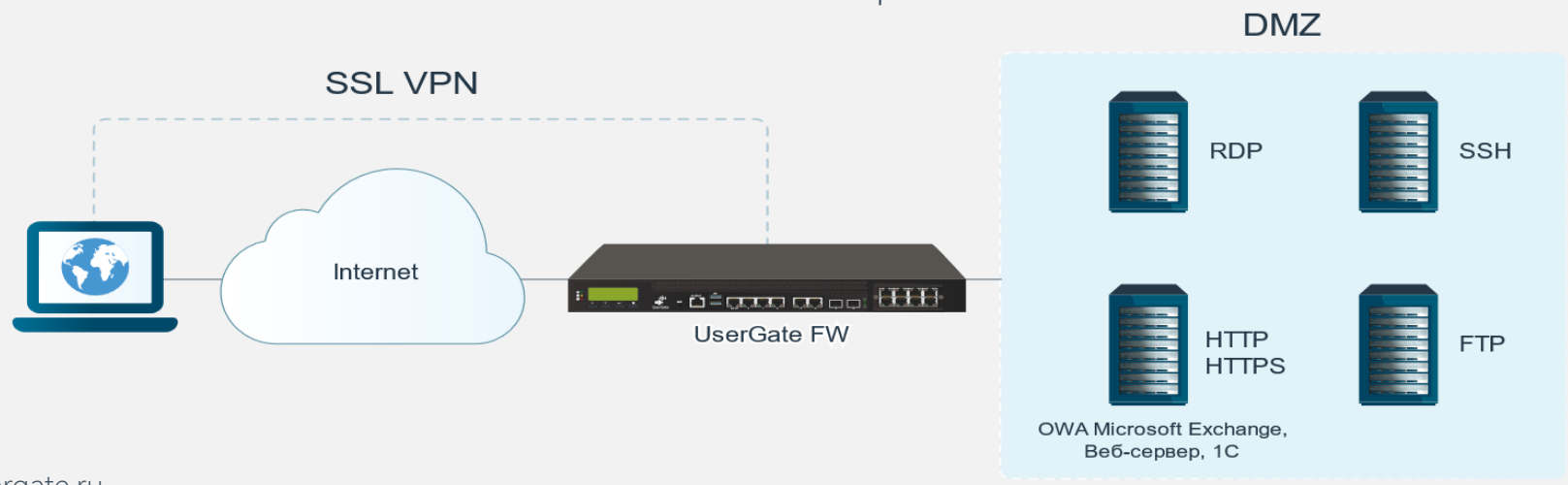




Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon 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

Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

SSL VPN (Веб-портал) – позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML в том числе с поддержкой MFA.



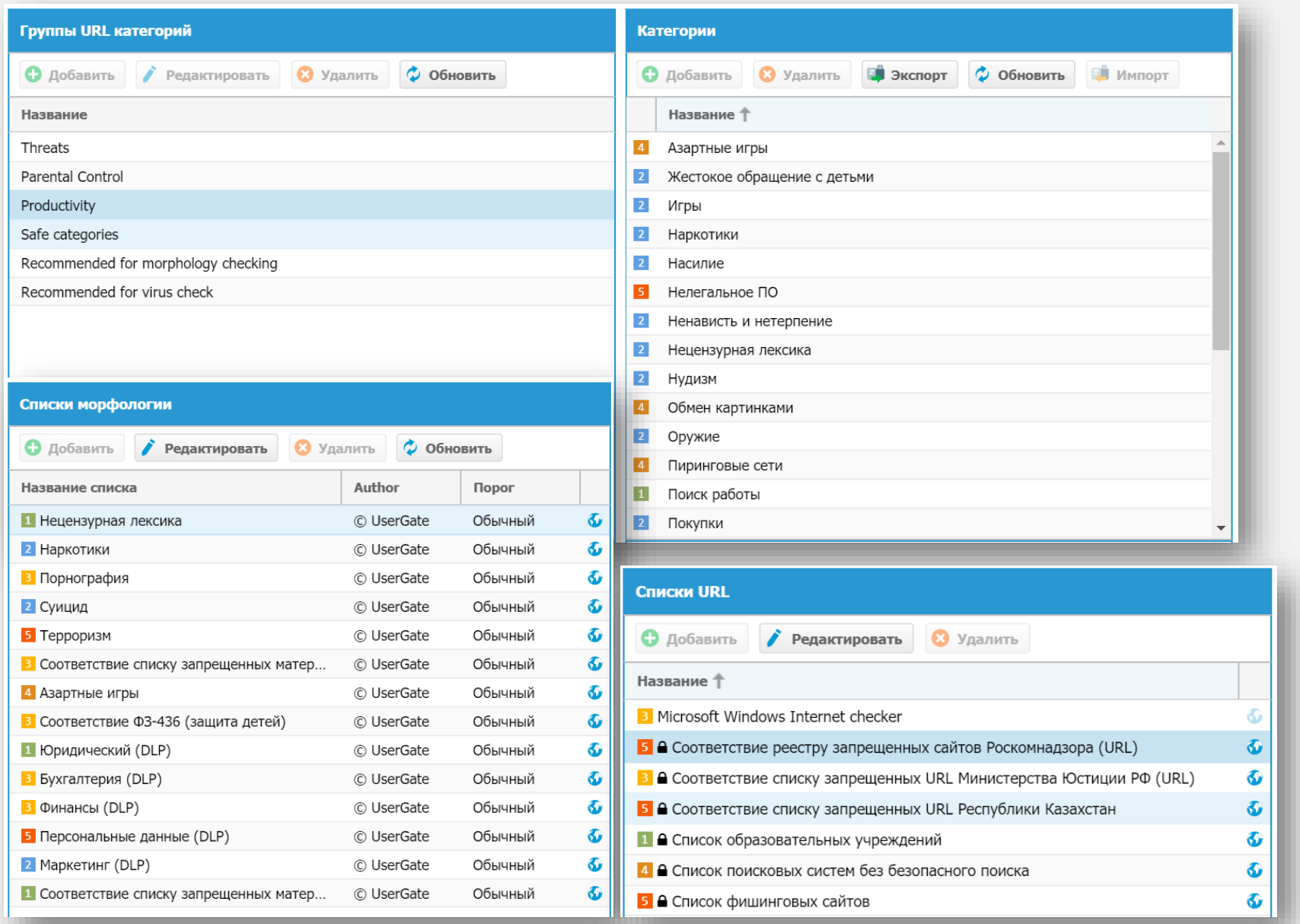
- Разделение технологических и корпоративных сетей
- Мониторинг и анализ SCADA-протоколов
- Варианты работы как в разрыв, так и в span

Стандарт	Контроль на уровне L7	Контроль команд в протоколе
МЭК-61850	MMS	Собственный прокси для MMS для контроля взаимодействие между терминалами и системой управления АСУТП
IEC 60870-5 ГОСТ Р МЭК 60870-5 IEC 60870-5-104 ГОСТ Р МЭК 60870-5-104	IEC 104	Полностью реализован. Поддержка полного контроля передаваемых команд, значений и т.п.. Собственный прокси для IEC 104.
Modbus	Modbus	Полностью реализова. Собственный прокси.
DNP3 он же IEEE Std 1815-2010	Планируется в ближайшее время.	Полностью реализован. Собственный прокси.
OPC UA	OPC UA	Реализован только в виде сигнатуры для приложения L7. Позволяет журналировать, запрещать, разрешать использование данного протокола без возможности контроля передаваемых команд, адресов и т.п.

Различные механизмы фильтрации:

- фильтрация по категориям (UserGate URL filtering 4.0)
- морфологический анализ
- безопасный поиск
- белые и черные списки
- блокировка контекстной рекламы
- запрет загрузки определенных видов файлов
- антивирусная проверка трафика

- Собственная крупнейшая база электронных ресурсов – более 500 миллионов сайтов
- Более 80 категорий
- Ежедневное обновление списка сайтов
- Повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории



ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

- **Защита сервисов и приложений**
  Если у заказчика есть какие-либо сервисы (наличие ЦОДа), которые должны быть доступны снаружи для потребителей, их нужно защищать.
- **Защита периметра сети**
  Построение основного защищающего контура в организации.
- **Фильтрация контента**
  Блокировка опасного, незаконного и вредного для продуктивной работы контента

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

- **Защита чувствительных Информационных Систем**
  Если у заказчика есть информационная система, подлежащая обязательному категорированию (персональные данные, медицинские системы и т.д.), то он обязан защищать ее сертифицированными средствами защиты (152-ФЗ, 17 и 21 приказы ФСТЭК России)
- **Защита Критических Объектов**
  Если заказчик попадает под действие 187-ФЗ (О Защите КИИ), то он обязан использовать сертифицированные средства защиты на критических сегментах.
- **Отчетность и журналирование**
  Контроль за всеми событиями в сети для мониторинга и последующей аналитики.

UGOS

v.6

VRF

IDPS

SSL BROKER

SSH DECRYPTION

APP CONTROL

200+
НОВЫХ ФИЧ.

USERGATE LOGAN

SOAR

CUSTOM REPORTS

МАСШТАБИРУЕМОСТЬ

SENSORS SUPPORT

USERGATE MANAGEMENT CENTER

DEPLOYMENTS

ГИБКИЕ ШАБЛОННЫЕ ПОЛИТИКИ

ЦЕНТРАЛЬНОЕ УПРАВЛЕНИЕ

ГРАНУЛЯРНЫЕ ПОЛИТИКИ

ПОДДЕРЖКА ОБЛАЧНОЙ МОДЕЛИ

UserGate

UserGate Log Analyzer

Выделенная система сбора, хранения и журналирования логов

- Уменьшение нагрузки на шлюзы UserGate
- Обработка журналов и создание отчетов
- Объединение журналов с нескольких шлюзов для общего анализа
- Увеличение глубины журналирования
- Увеличение размера хранилища на серверах LogAn

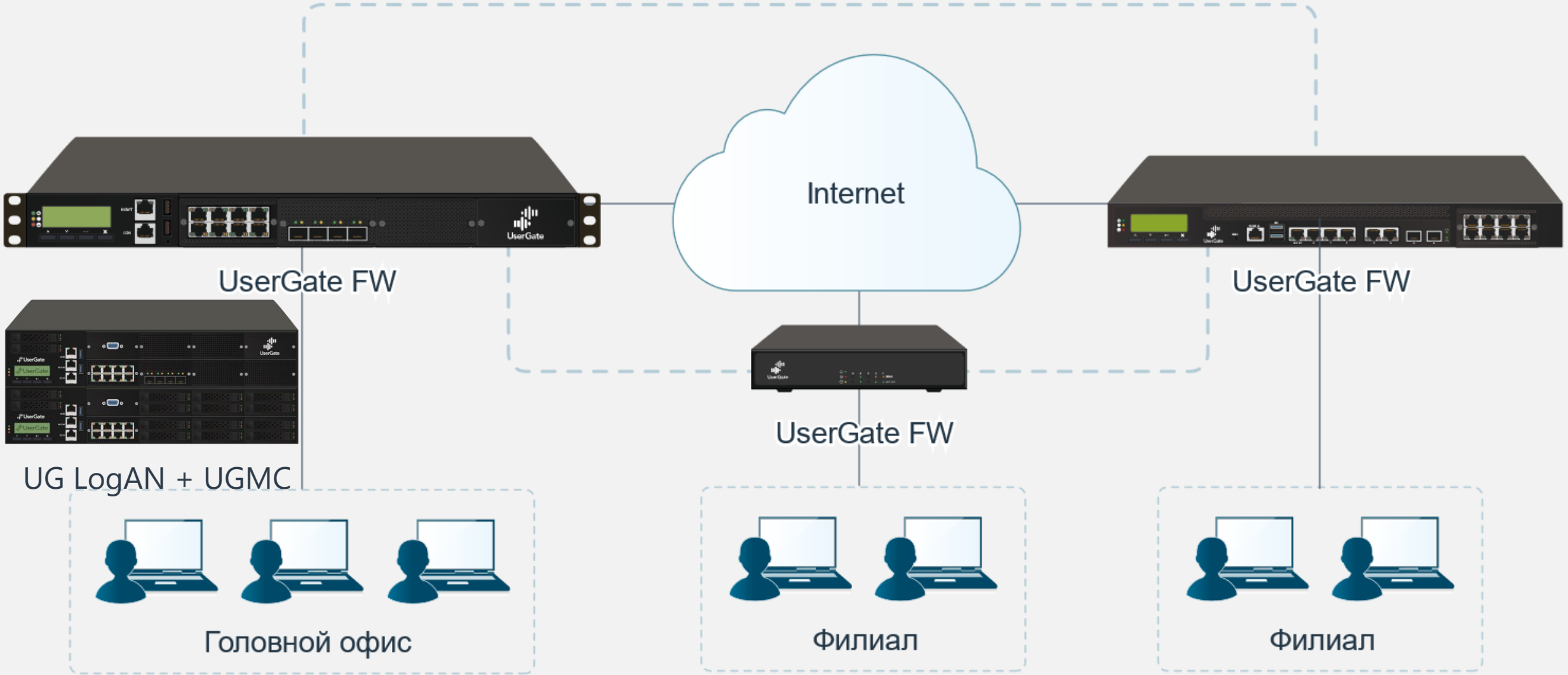
UserGate

UserGate Management Center

Выделенная система управления NGFW

С помощью UGMC централизованно настраиваются все параметры работы межсетевых экранов UserGate - сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие настройки. UserGate Management Center позволяет систематизировать подход к составлению настроек через применение шаблонов, а также прозрачно применить эти настройки на выбранной части парка межсетевых экранов.

sales@usergate.ru | usergate.ru


Internet
UserGate FW
UserGate FW
UserGate FW
UG LogAN + UGMC
Головной офис
Филиал
Филиал

UserGate

Законодательство

Всем производителям СЗИ необходимо было пройти процедуру подтверждения соответствия требованиям к УД до 01.01.2021

2021 г.
Требования доверия в 31 Приказе ФСТЭК России

...в автоматизированных системах управления 1 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия.

В автоматизированных системах управления 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия.

Согласно обновленным требованиям, для УД5 и выше с 01.01.22 сведения о платформе должны быть включены в единый реестр российской радиоэлектронной продукции (Реестр)

Для выполнения требований 17 и 21 приказов ФСТЭК России необходимо использовать только те СЗИ, которые прошли процедуру соответствия требованиям к УД. Для 239 приказа это требование вступает в силу с 01.01.23

Для УД5 и выше с 01.01.28, кроме включения сведений о платформе, в Реестре должны быть сведения о процессорах или микроконтроллерах, элементах памяти, сетевых картах, графических адаптерах

https://regulation.gov.ru/projects#npa=113431

UserGate

Новый сертификат

СЕРТИФИКАТ ФСТЭК России № 3905

Решение UserGate имеет действующий сертификат ФСТЭК России по 4 уровню доверия до 26.03.2026 г.

- 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».
- 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;
- АСУТП 1 класса;
- ИСПДн 1 уровня;
- ИСОП II класса

Текст для поиска: Д4 доверия(4)

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство
3905	26.03.2018	26.03.2026	изделие «Универсальный шлюз безопасности «UserGate»	Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Профиль защиты МЭ(Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

1

FORCEPOINT POWERED BY Raytheon
FORTINET
STONESOFT
Barracuda
KerioControl
BlueCoat
McAfee SECURE™
Microsoft Forefront
Check Point SOFTWARE TECHNOLOGIES LTD.

МИНФИН
РОССИИ

UserGate

Благодарим за внимание

Антон Рахманенков

ведущий менеджер
по работе с корпоративными клиентами

arakhmanenkov@usergate.com
8 800 500 40 32 | +7-916-720-40-08