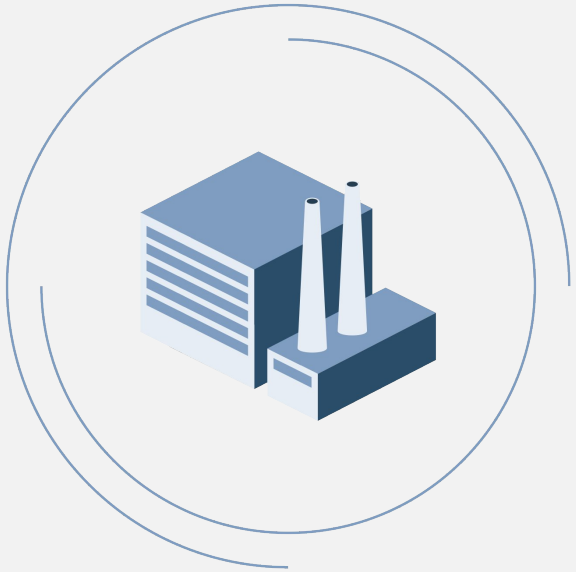
Межсетевой экран UserGate на защите корпоративного периметра

Роман Силиненко
Ведущий инженер

sales@usergate.ru
8 800 500 40 32

UserGate

Сращивание IT и OT влияют на производство



и на множество других областей

Управление зданиями

Энергетика

Логистика

Добыча ресурсов

Нефть и газ

Умный город

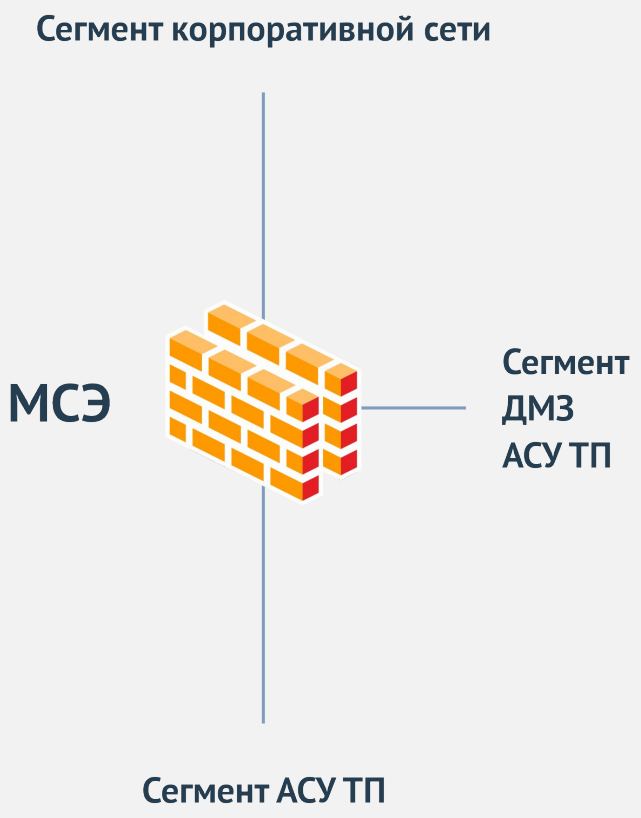
Водоснабжение

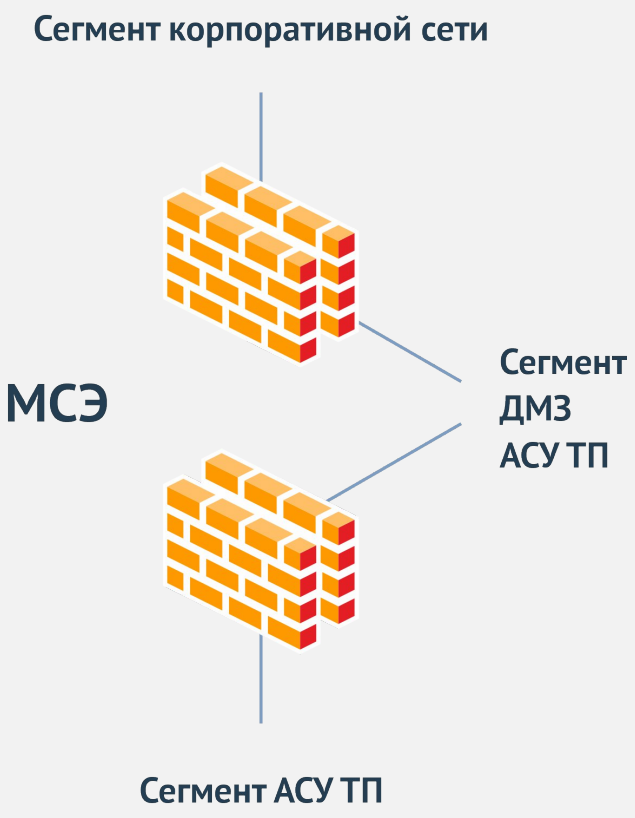
Химическая промышленность

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

UserGate

NIST
ISA 99
ГОСТ
МЭК
CpwE





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.

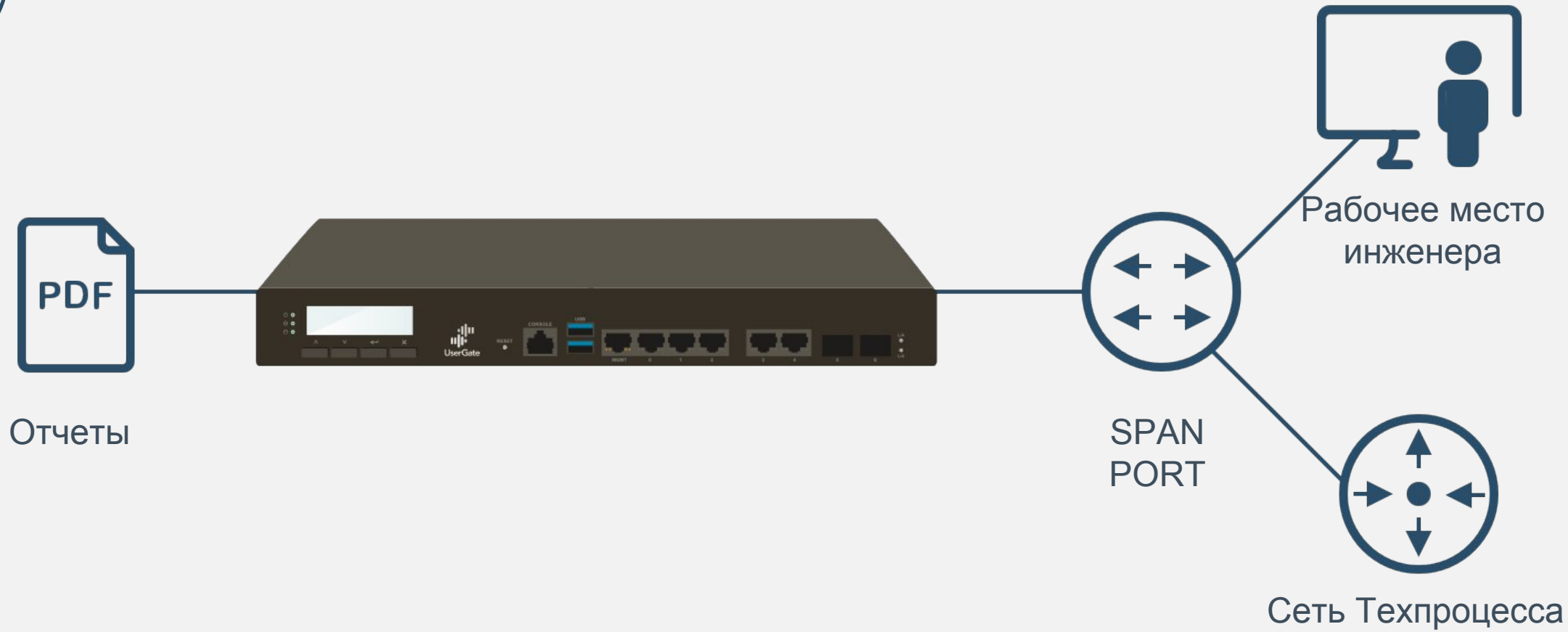
СОВ - Система обнаружения и предотвращения вторжений

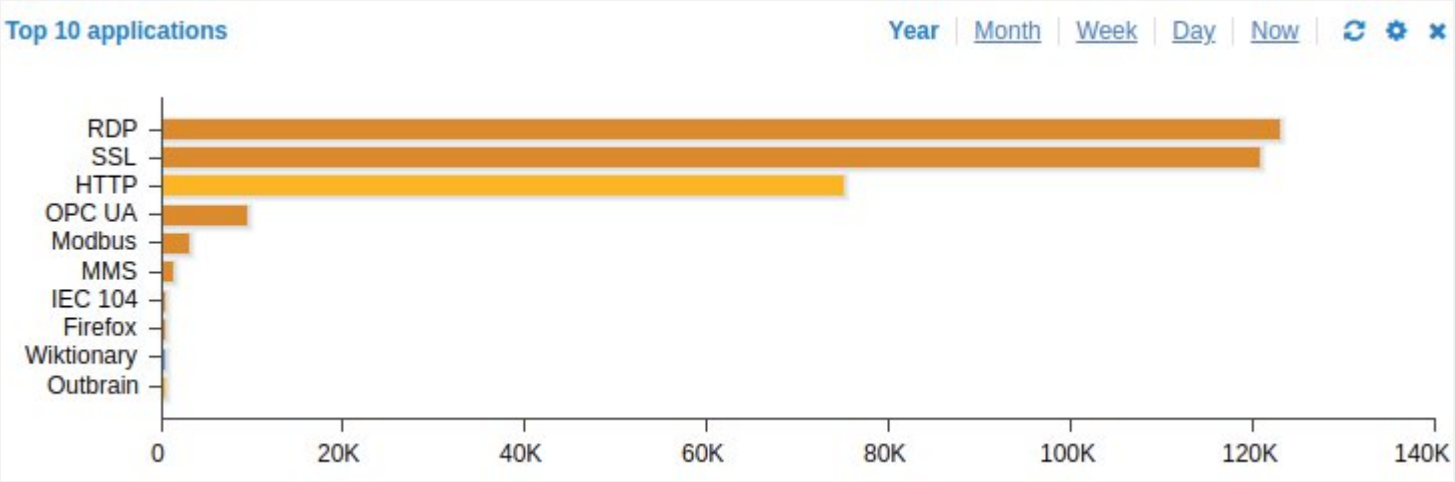
Сигнатуры IPS для протоколов АСУ ТП.

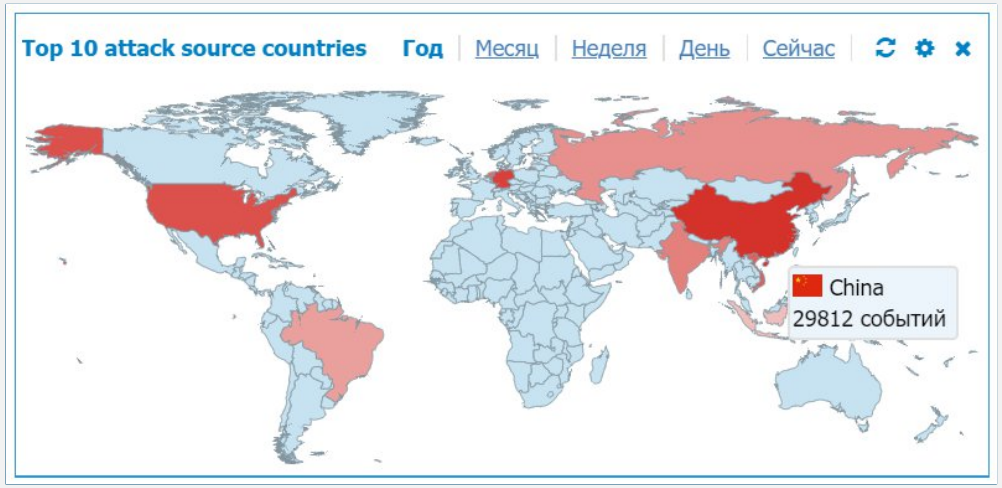
Защита систем, которое невозможно пропатчить (виртуальный патчинг)

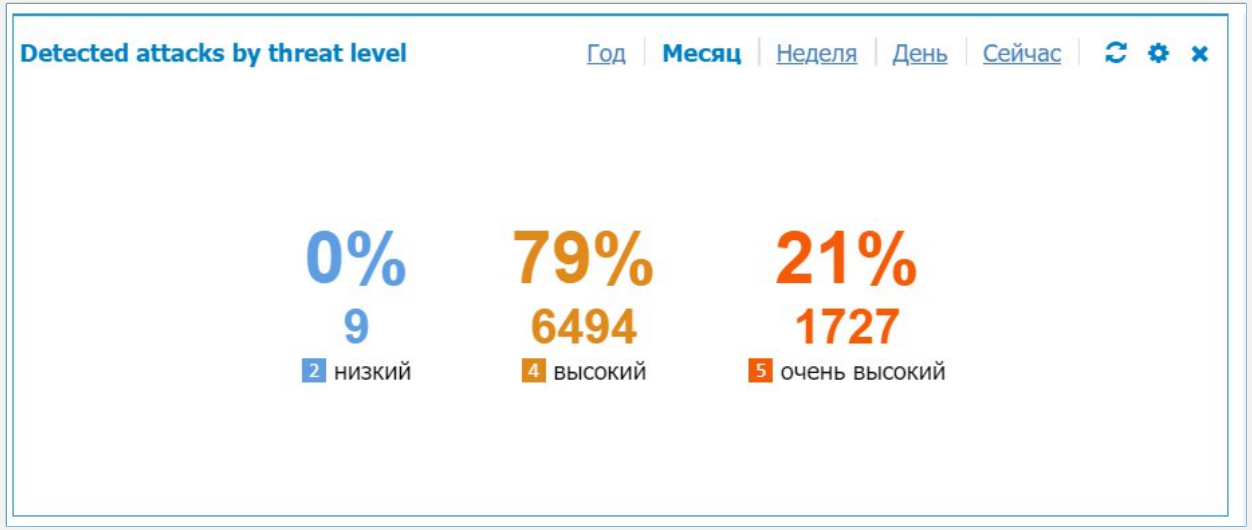
Category: scada ×

Signature	OS	Prot...	Class type	References	Category
Measuresoft ScadaPro Remote Command Executi...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2011-3497	scada
CitectSCADA/CitectFacilities ODBC Server Remot...	Other	tcp	targeted-activity	None	scada
Advantech WebAccess Dashboard Viewer uploadl...	Other	tcp	targeted-activity	None	scada
Advantech WebAccess Multiple Remote Code Exe...	Other	tcp	targeted-activity	None	scada
DATAC RealWin SCADA Server Remote Stack Buf...	Other	tcp	targeted-activity	None	scada
SCADA 3S CoDeSys Gateway Server Directory Tr...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2012-4705	scada
Scadatec Procyon Telnet Service Remote Buffer O...	Other	tcp	targeted-activity	None	scada
Multiple Schneider Electric Products Stack Based ...	Other	tcp	targeted-activity	None	scada
AzeoTech DAQFactory NETB Datagram Parsing B...	None	tcp	targeted-activity	None	scada
CoDeSys Gateway Server CVE-2012-4705 Directo...	Other	tcp	targeted-activity	None	scada
7T Interactive Graphical SCADA System Multiple ...	Other	tcp	targeted-activity	None	scada
ABB MicroSCADA wserver.exe CreateProcessA() ...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	None	scada
ICONICS WebHMI ActiveX Control Stack Buffer O...	None	tcp	targeted-activity	None	scada
Interactive Graphical SCADA System Remote Co...	Other	tcp	targeted-activity	None	scada
Siemens SIMATIC WinCC Default Password Secu...	Other	tcp	default-login-att...	CVE: 2010-2772	scada


PDF
Отчеты
UserGate
SPAN
PORT
Рабочее место
инженера
Сеть Техпроцесса

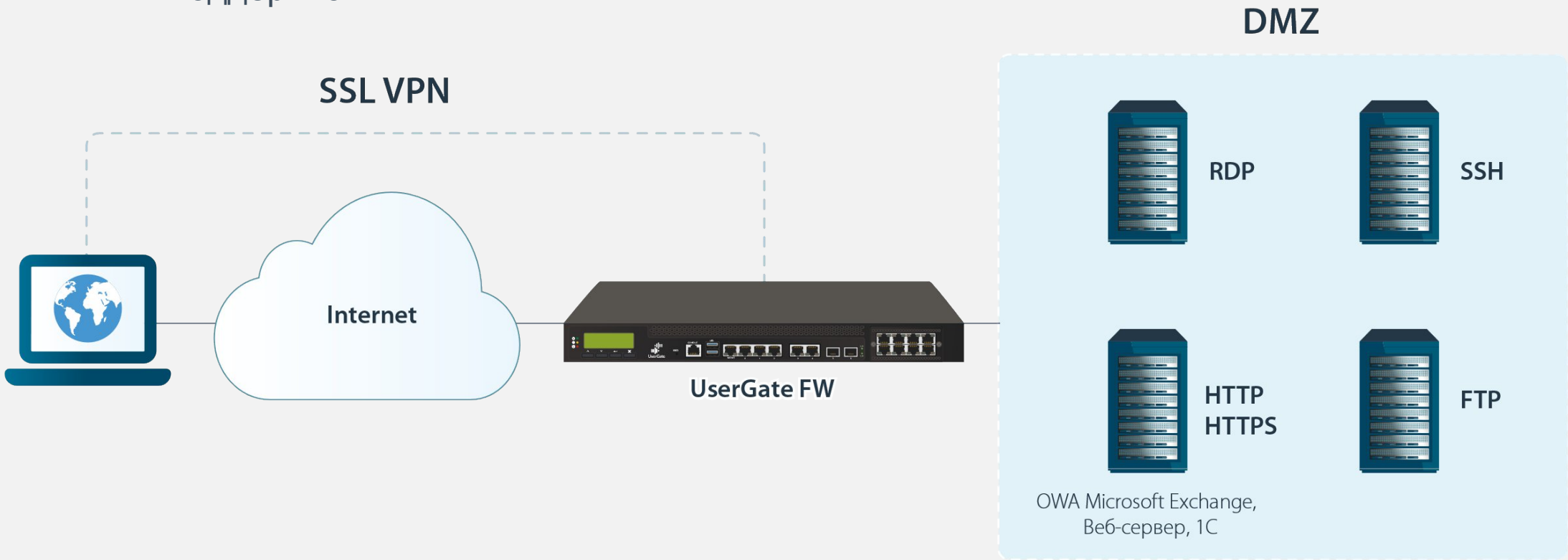




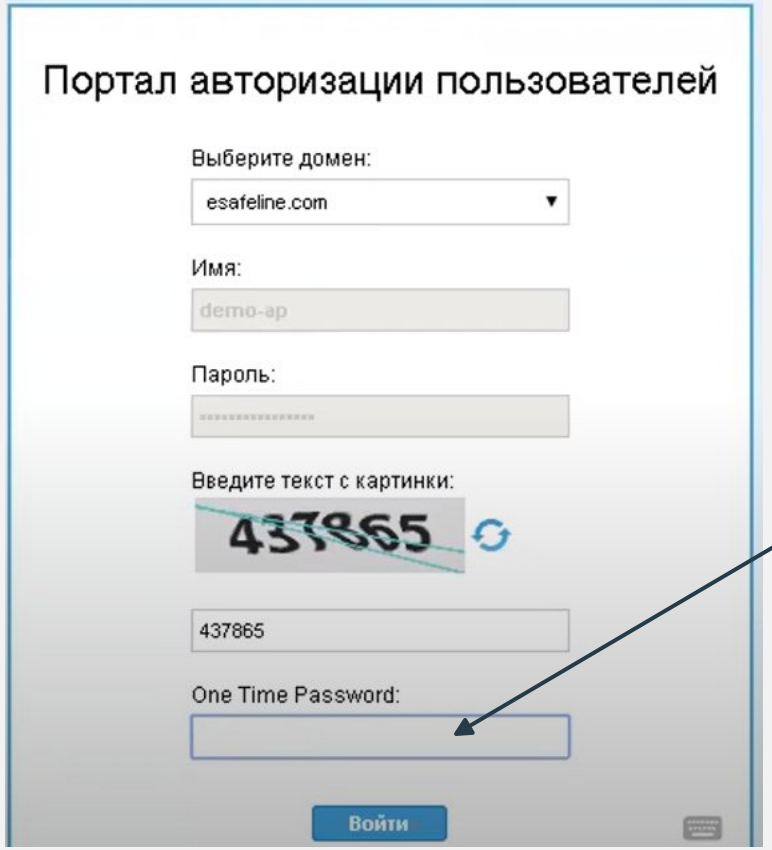


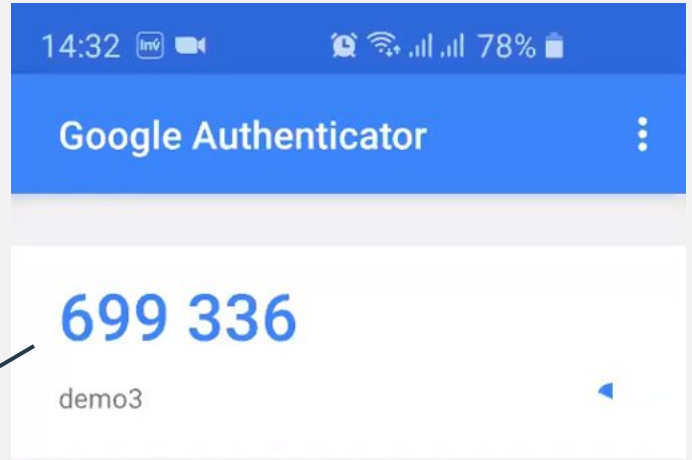
Время		Сигнатура	IP источника	IP назначения
07:13:58		4 Suspicious inbound to M...	103.94.123.206	138.68.85.159
07:13:55		4 Suspicious inbound to M...	221.194.44.208	138.68.85.159
07:13:51		4 Suspicious inbound to M...	125.161.72.33	138.68.85.159
07:12:52		5 ntpdx overflow attempt	51.159.59.122	138.68.85.159
07:08:02		5 Suspicious User Agent (...	138.68.85.159	178.248.232.27
07:08:02		5 Suspicious User Agent (...	138.68.85.159	81.19.72.59
06:52:35		5 Potential MySQL bot sca...	87.251.74.9	138.68.85.159

SSL VPN (Веб-портал) – позволяет удаленным сотрудникам, подрядчикам 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.



- MFA (TOTP, SMS, Email)
- Настройка политик доступа к отдельным сервисам по пользователям и группам
- Доступ через браузер
- SSO





iec 104
modbus
dnp3
opc ua

UserGate UTM имеет возможность контроля автоматизированной системы управления технологическим производством (АСУ ТП, SCADA).

Администратор может контролировать поток управляющих команд, настроив правила обнаружения, блокировки и\или журналирования конкретных команд либо присутствия в трафике конкретного протокола.

Стандарт	Контроль на уровне L7	Контроль команд в протоколе
МЭК-61850	✔	✔
IEC 60870-5 ГОСТ Р МЭК 60870-5 IEC 60870-5-104 ГОСТ Р МЭК 60870-5-104	✔	✔
Modbus	✔	✔
DNP3 он же IEEE Std 1815-2010	✔	✔
OPC UA	✔	✔
Ваш протокол	Добавляется по запросу	

Межсетевой экран NGFW

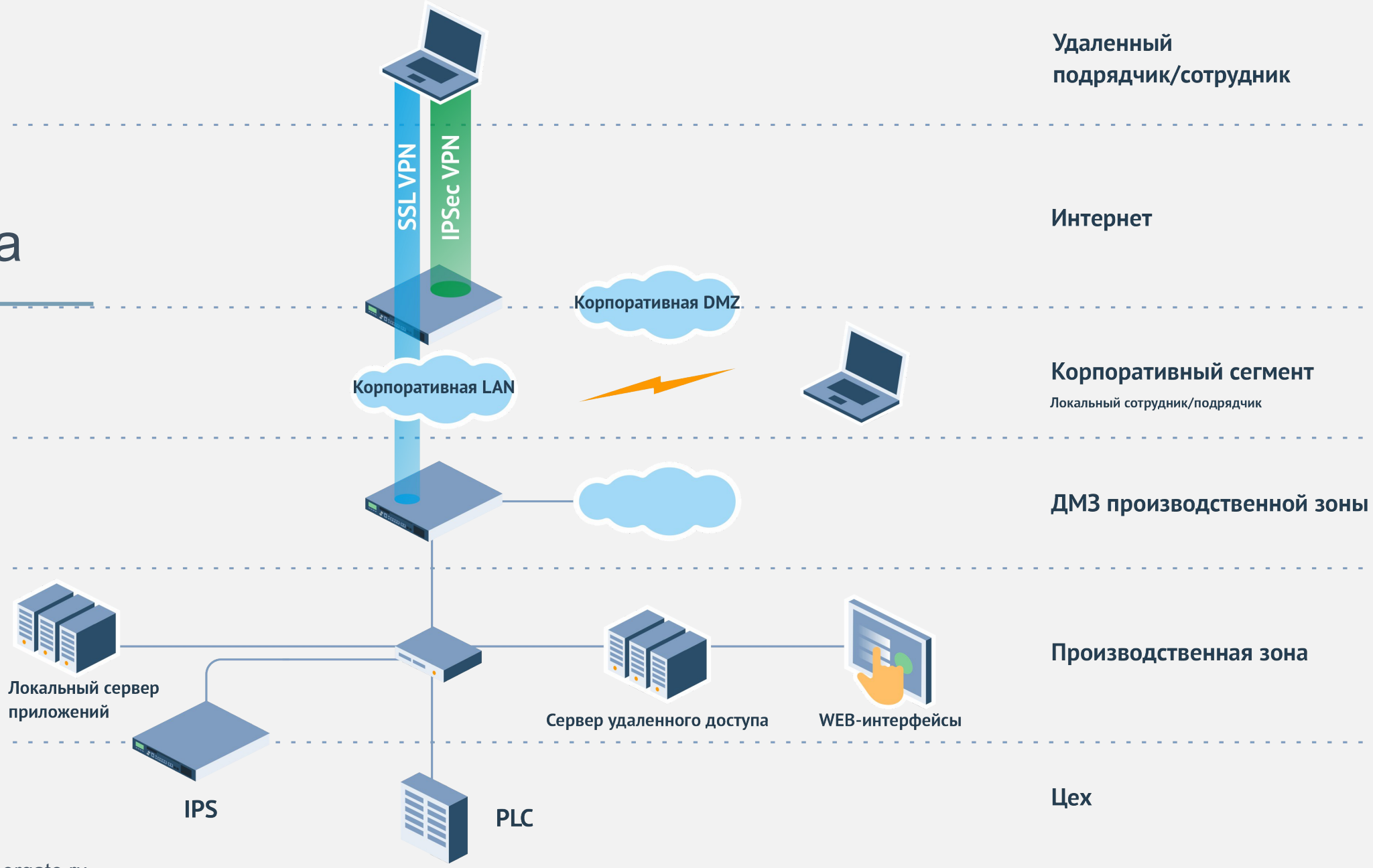
Система обнаружения и предотвращения вторжений

Безопасная публикация ресурсов и сервисов

Анализ команд в протоколах АСУ ТП

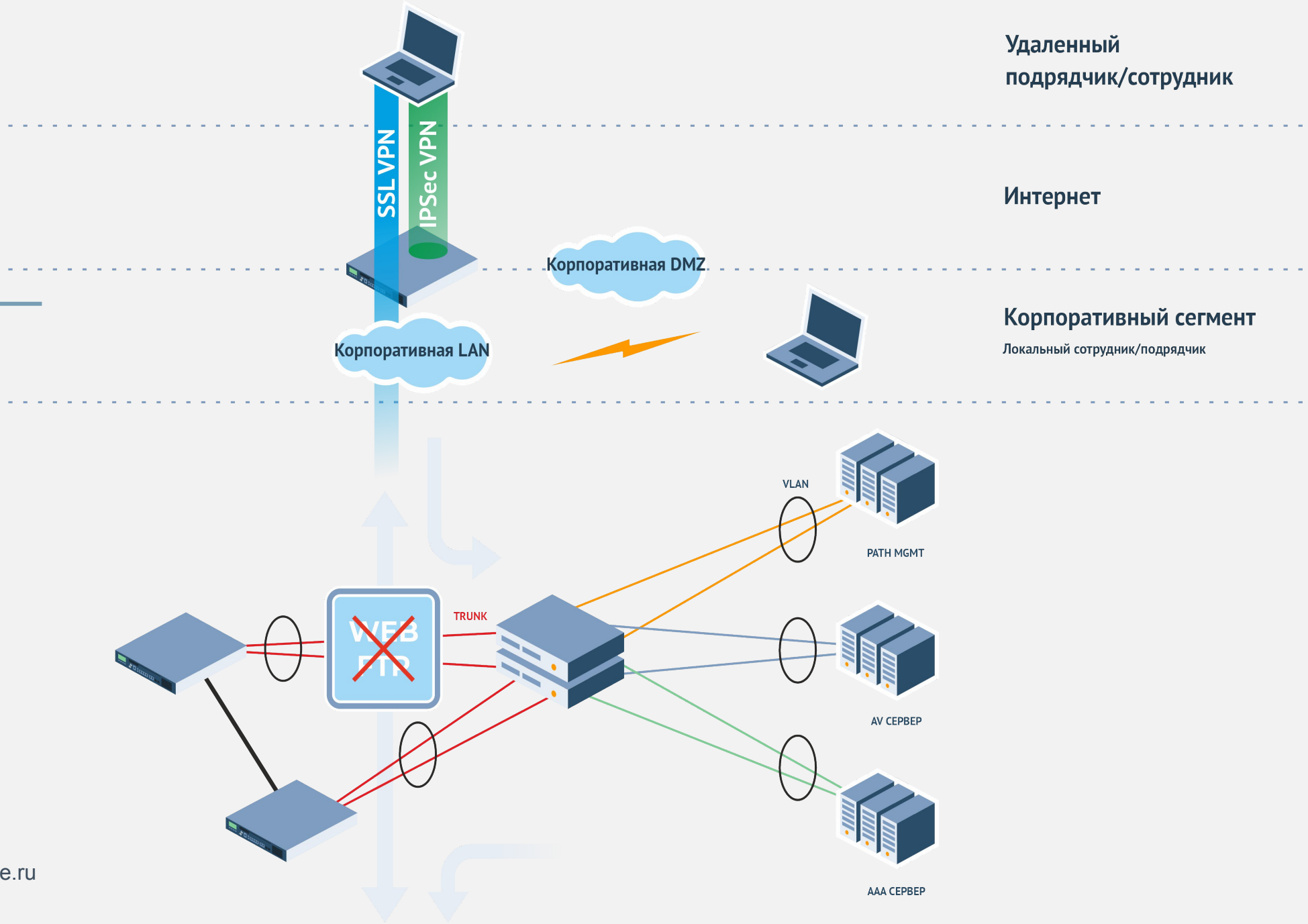
UserGate

Общая Архитектура

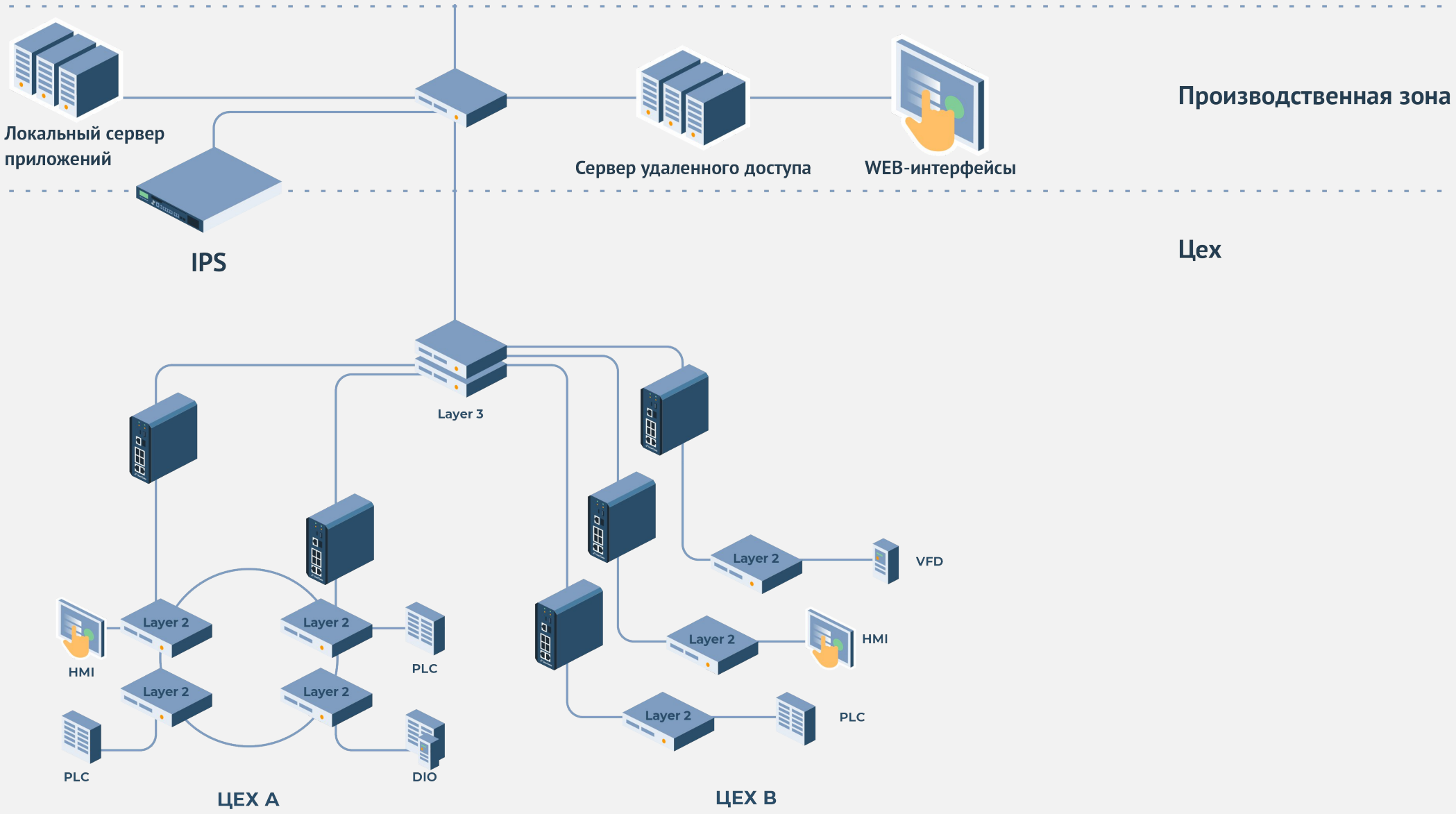


UserGate

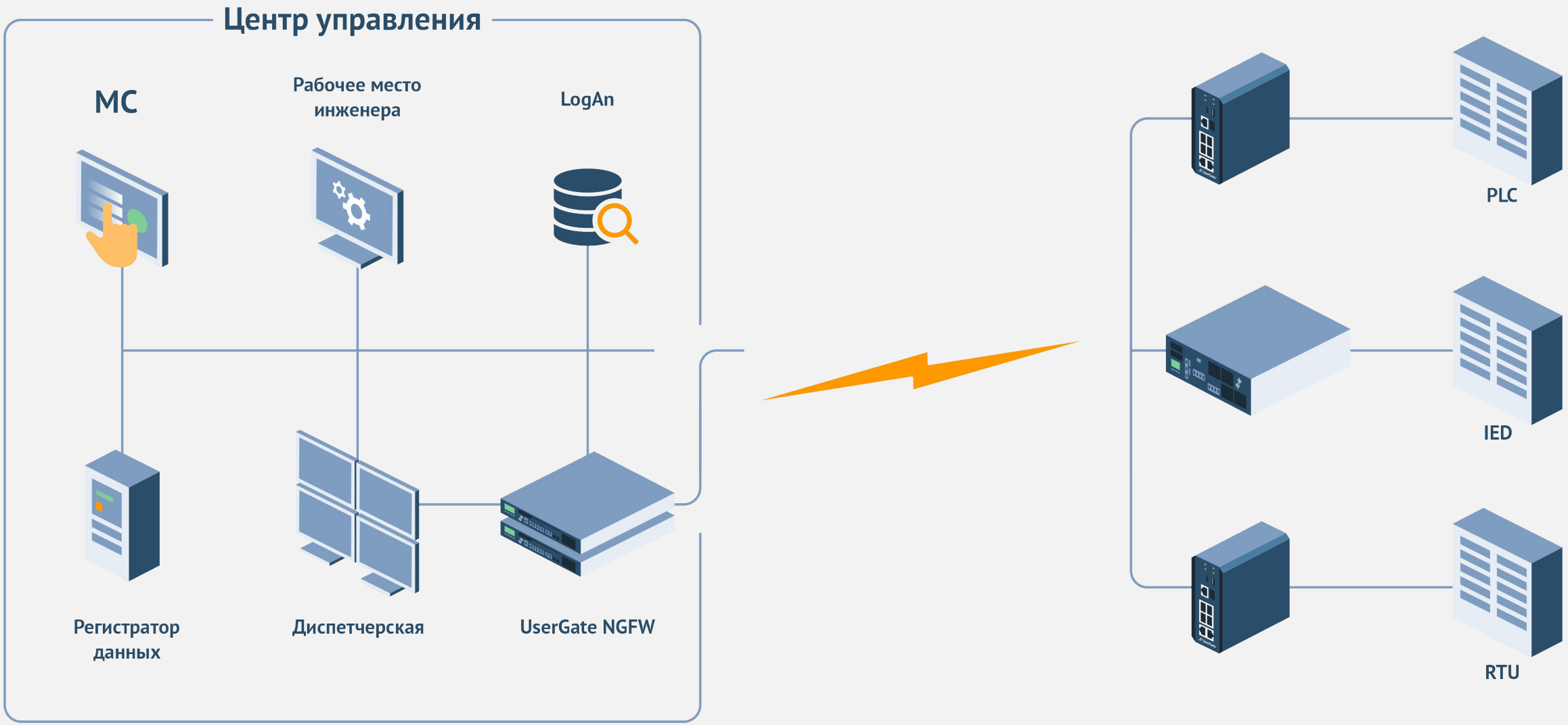
Общая Архитектура

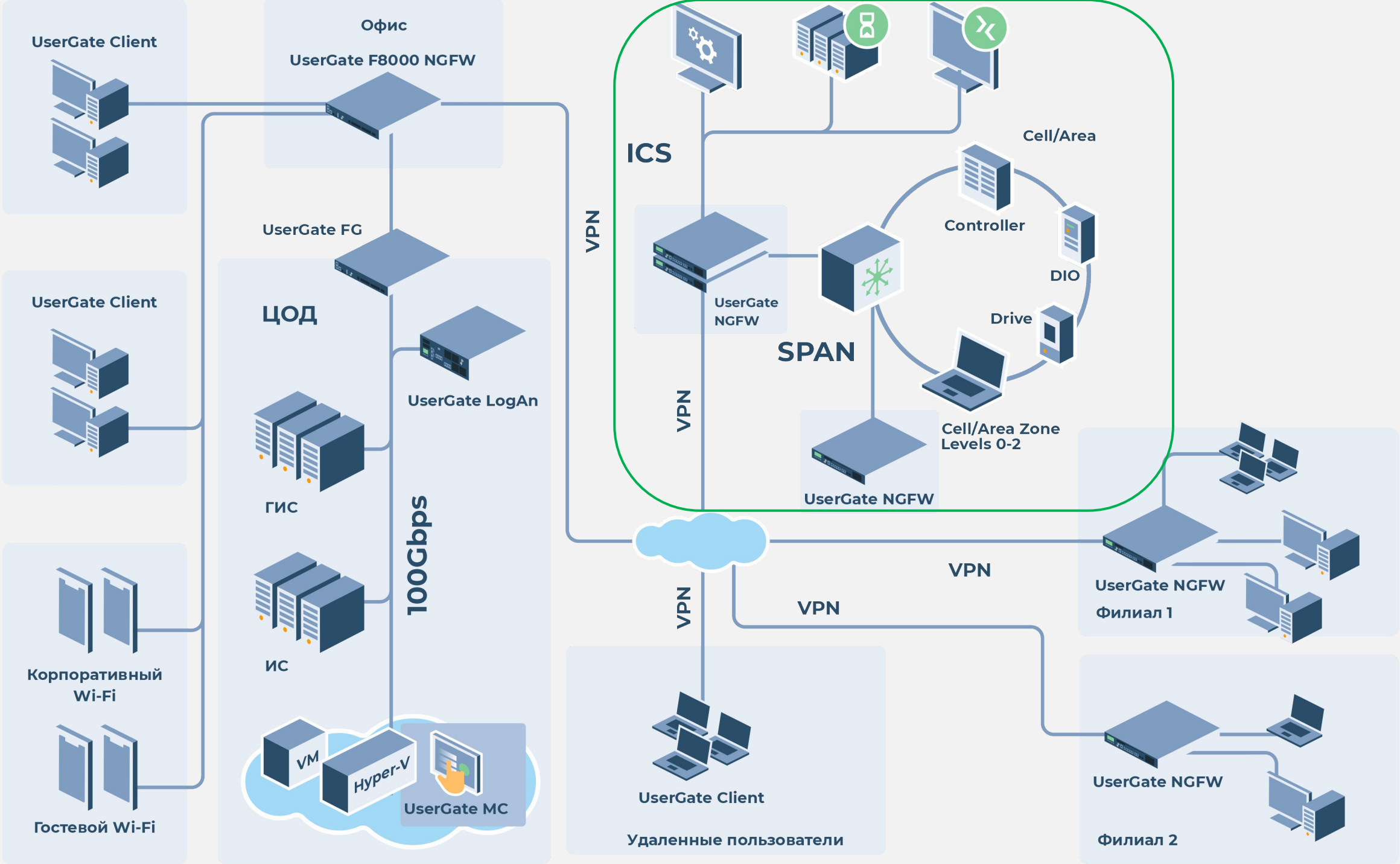


sales@usergate.ru | usergate.ru


UserGate
Производственная зона
Локальный сервер приложений
IPS
Сервер удаленного доступа
WEB-интерфейсы
Цех
Layer 3
Layer 2
HMI
PLC
DIO
VFD
ЦЕХ A
ЦЕХ B

Распределенная Архитектура




UserGate Client
Офис
UserGate F8000 NGFW
UserGate FG
UserGate Client
ЦОД
UserGate LogAn
ГИС
ИС
100Gbps
Корпоративный Wi-Fi
Гостевой Wi-Fi
VM
Hyper-V
UserGate MC
VPN
ICS
Cell/Area
Controller
DIO
Drive
UserGate NGFW
SPAN
VPN
Cell/Area Zone Levels 0-2
UserGate NGFW
VPN
VPN
VPN
UserGate NGFW
Филиал 1
UserGate Client
Удаленные пользователи
UserGate NGFW
Филиал 2

Новые платформы UserGate NGFW для АСУ ТП

sales@usergate.ru | usergate.ru

Реестр сертифицированных средств защиты информации ФСТЭК России

МЭ типа «А»

применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы.

МЭ типа «Б»

применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы

МЭ типа «В»

применяемый на узле (хосте) информационной системы

МЭ типа «Г»

применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера

МЭ тип «Д»

применяемый в автоматизированной системе управления технологическими или производственными процессами. МЭ типа «Д» может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы)

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

UserGate

Спасибо за внимание

Роман Силиненко
Ведущий инженер

sales@usergate.ru
8 800 500 40 32