КСБ-СОФТ

UserGate Client: комплексный подход к защите доступа и рабочих станций

Спикеры:

- **Андрей Дуюн** – менеджер по работе с партнерами UserGate
- **Кирилл Жарков** – ведущий инженер UserGate

Модератор:

- **Дмитрий Чирков** – специалист по работе с ключевыми клиентами КСБ-СОФТ

Обменивайтесь
сообщениями во вкладке «Чат»

Запись вебинара направим
Всем участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

План вебинара

- режимы работы UserGate Client
- VPN
- проверка состояния конечной станции с помощью NAC
- управление доступом пользователей
- аналитика и реагирование на инциденты ИБ на конечной станции
- ответы на вопросы и розыгрыш призов

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

70+
регионов внедрения

4000+
реализованных проектов

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

2015
UserGate – резидент Сколково

2016
выпуск нового UserGate как решения класса UTM

Сертификация новой платформы по требованиям ФСТЭК России

2018
создание экспертной лаборатории и начало разработки собственных аппаратных платформ

2019
открытие первого московского офиса UserGat

2020
открытие офиса UserGate в Хабаровске

начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

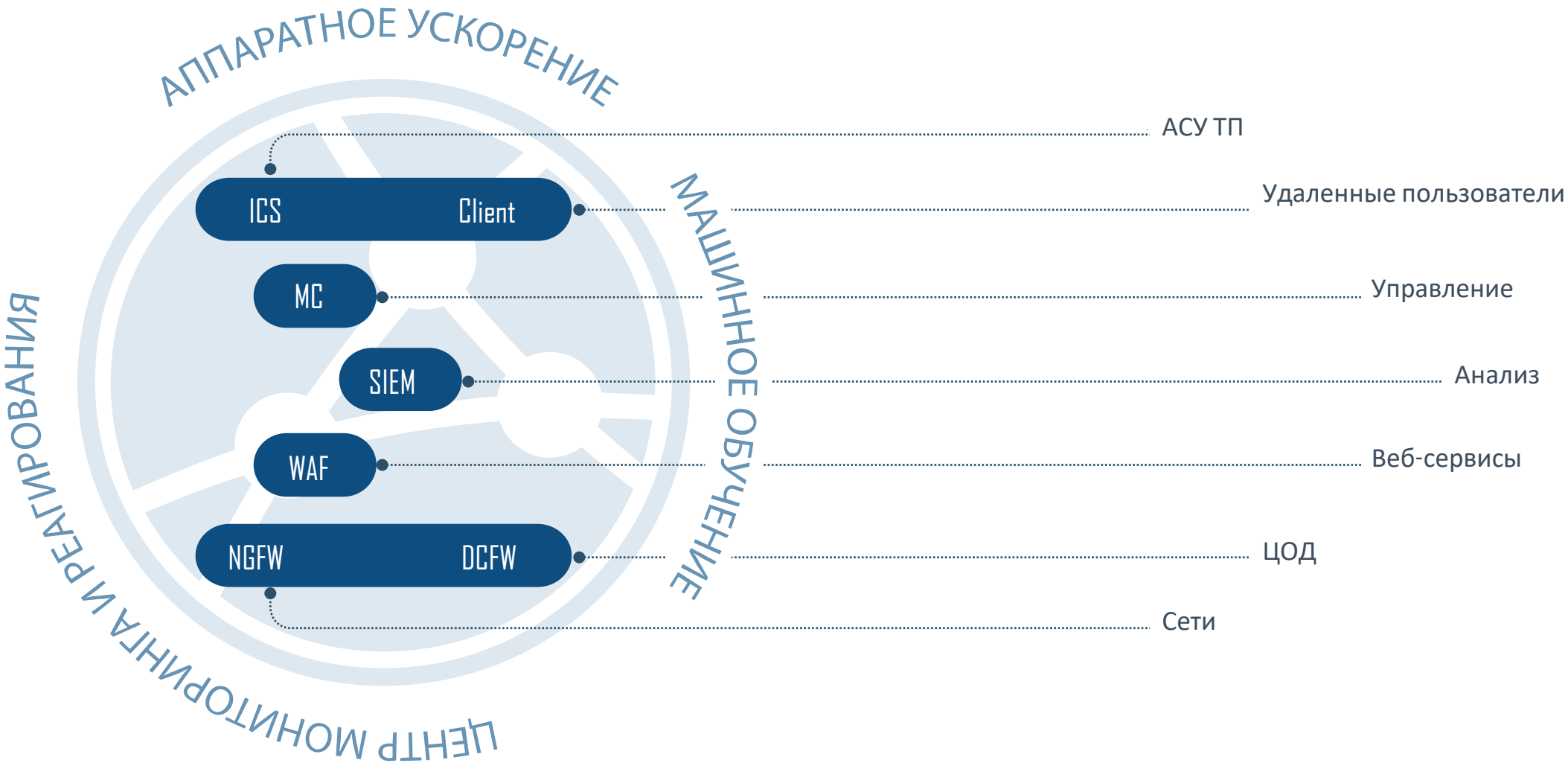
реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

2021
выход на рынок экосистемы безопасности UserGate SUMMA

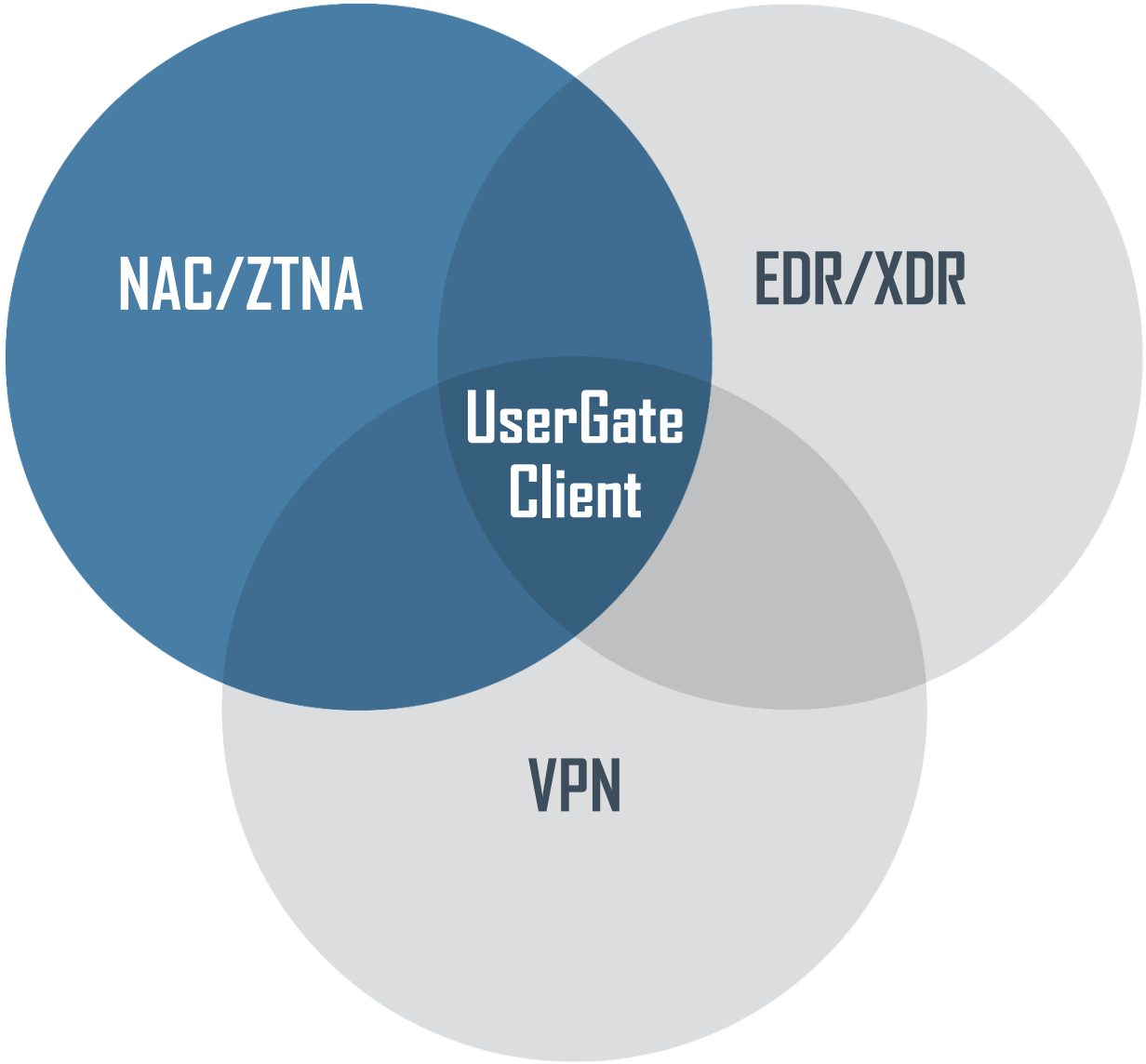
2022
открытие офиса в Санкт-Петербурге

UserGate SUMMA

100% видимость событий безопасности



Инструмент для разных концепций



UserGate Client – агент SUMMA

- Сообщает экосистеме компонентов безопасности UserGate SUMMA о состоянии устройства, работающих на нем приложениях и версиях ПО
- Управляет политиками используемых на устройстве приложений
- Предоставляет защиту уровня персонального межсетевого экрана
- Обеспечивает безопасное удаленное соединение (Virtual Private Network)
- Контролирует доступ в сеть на основе политик соответствия требованиям (Network Access Control
- Реализует подключение к корпоративной сети, построенное на принципах сетевого доступа с нулевым доверием (Zero Trust Network Access)
- Источник данных для SIEM-системы UserGate Log Analyzer

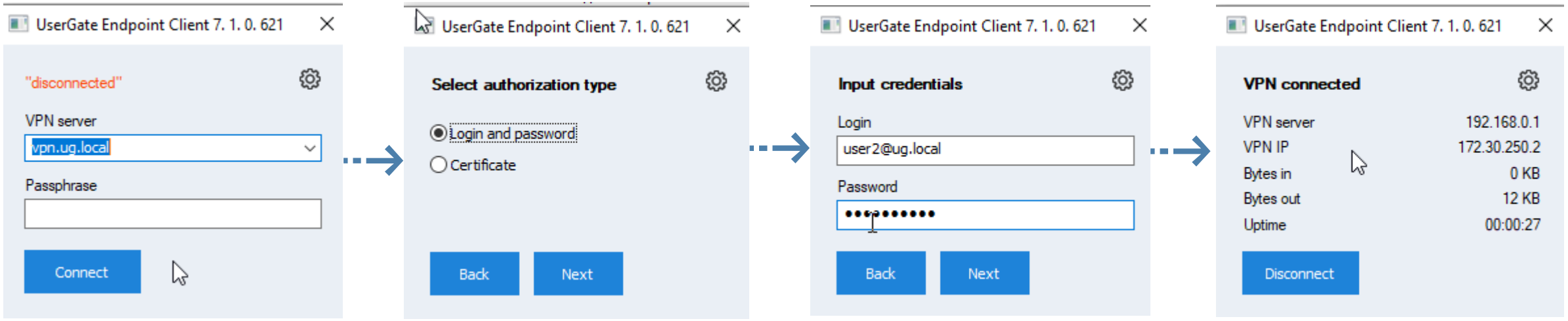
VPN

Возможности

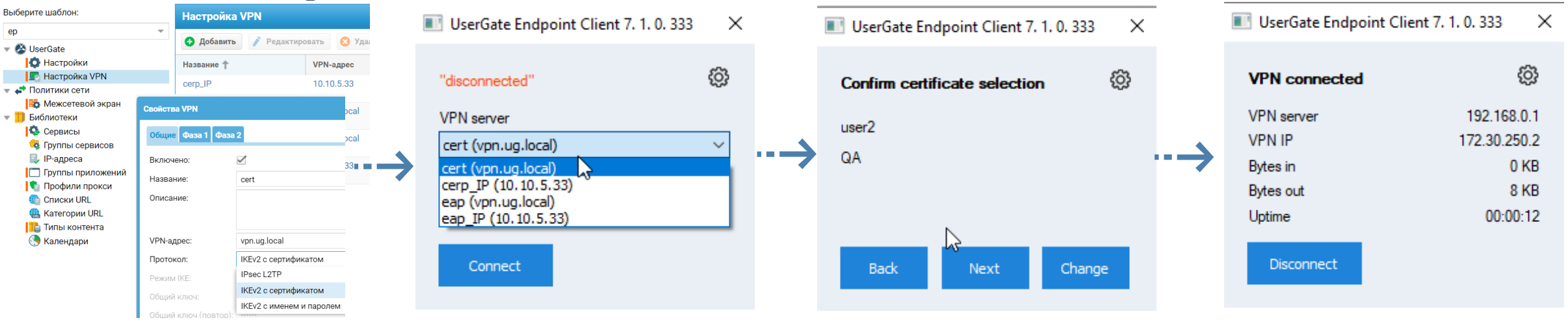
- Простая настройка со стороны клиента;
- IKEv2;
- Аутентификация по сертификатам;
- Split tunneling;
- MFA;

VPN – процесс подключения

Режим NGFW (автонастройка)

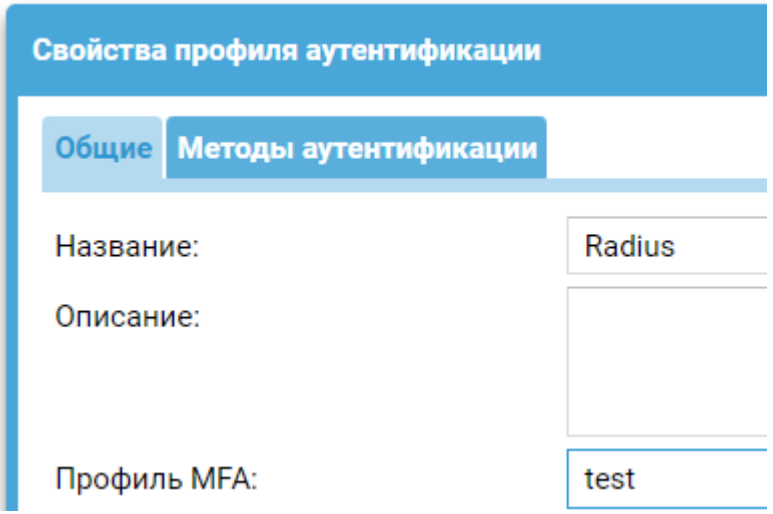


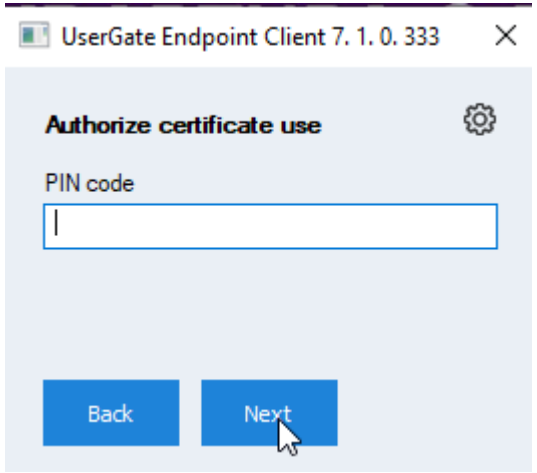
Режим Management Center



VPN – MFA


TOTP Initialization Page
Имя:
user4
Пароль:
Используйте этот ключ для инициализации TOTP Authenticator.
hymm azpz kdeu x374
Или используйте этот QR-код:
Login
Powered by UserGate

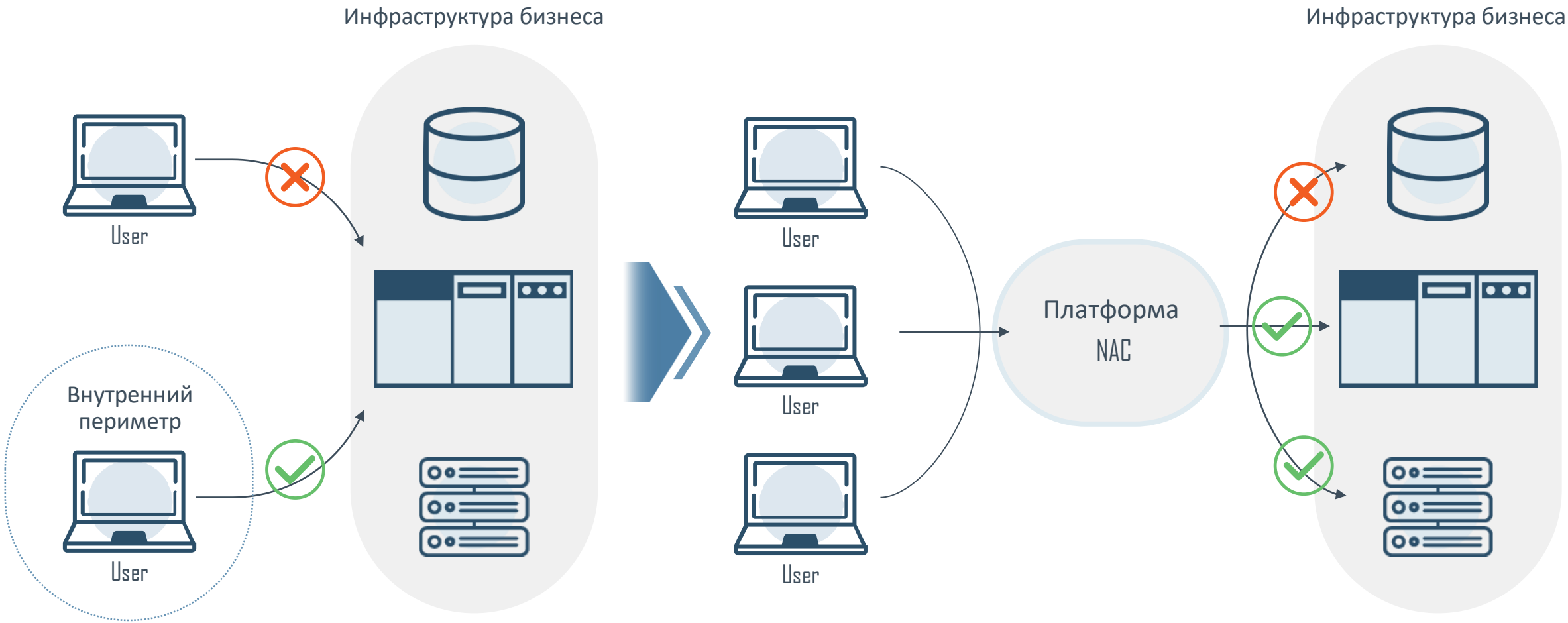

Свойства профиля аутентификации
Общие
Методы аутентификации
Название:
Radius
Описание:
Профиль MFA:
test


UserGate Endpoint Client 7. 1. 0. 333
Authorize certificate use
PIN code
Back
Next

NAC

Задача NAC

Заменить фактор доверенности нахождения
на фактор доверенности состояния устройства

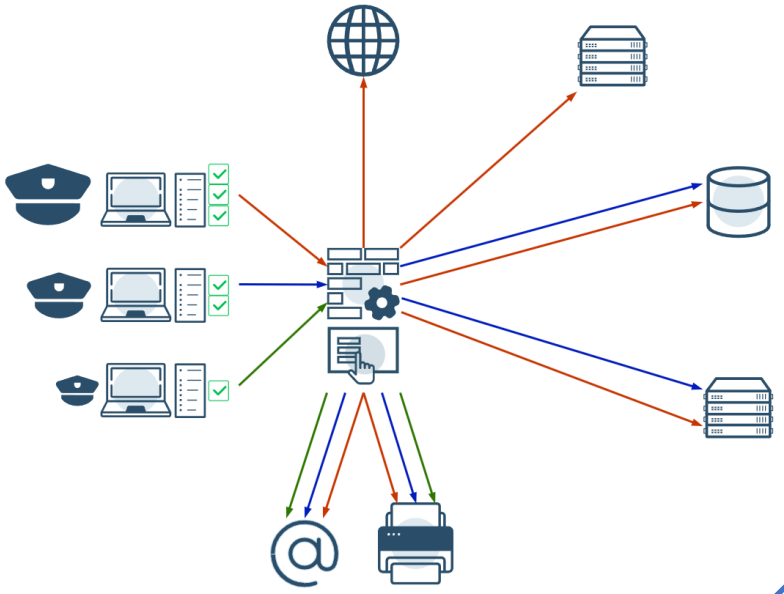


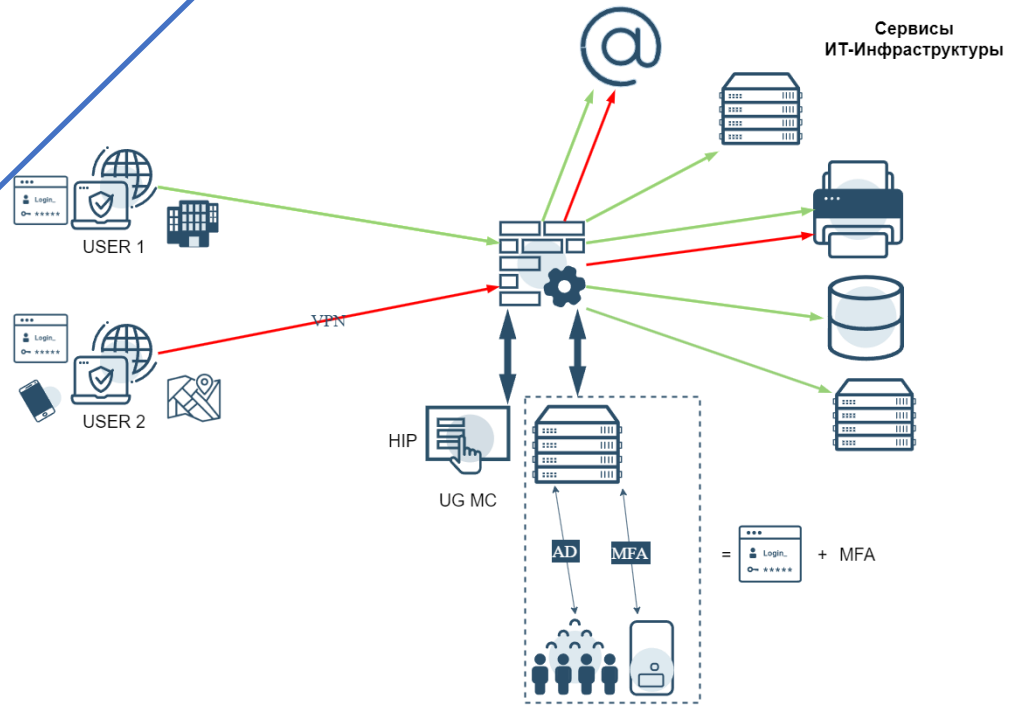
Фактор доверенности нахождения

Фактор доверенности состояния устройства

Применение NAC

Групповые политики доступа

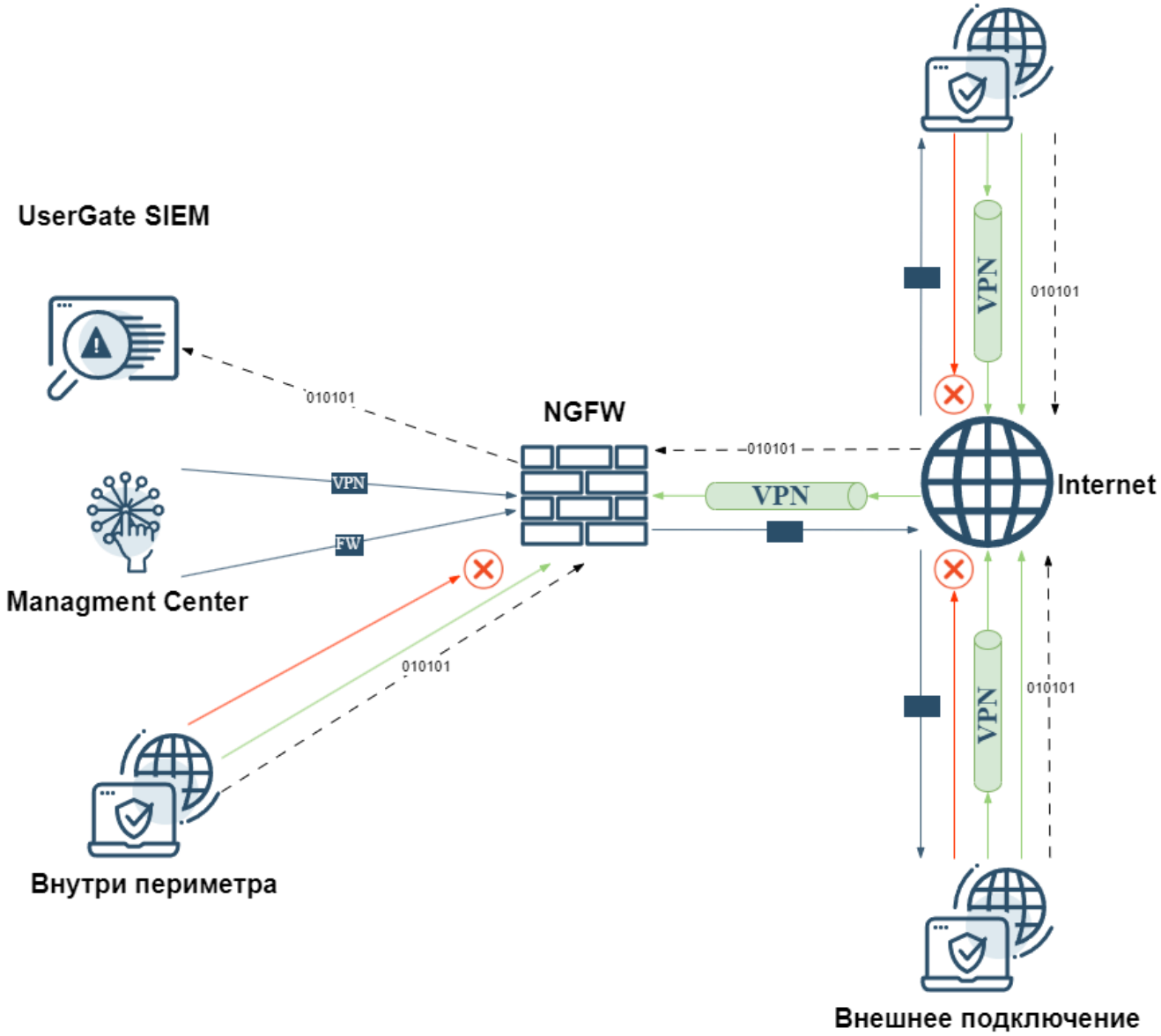




Доступ в офисе и вне офиса

EDR

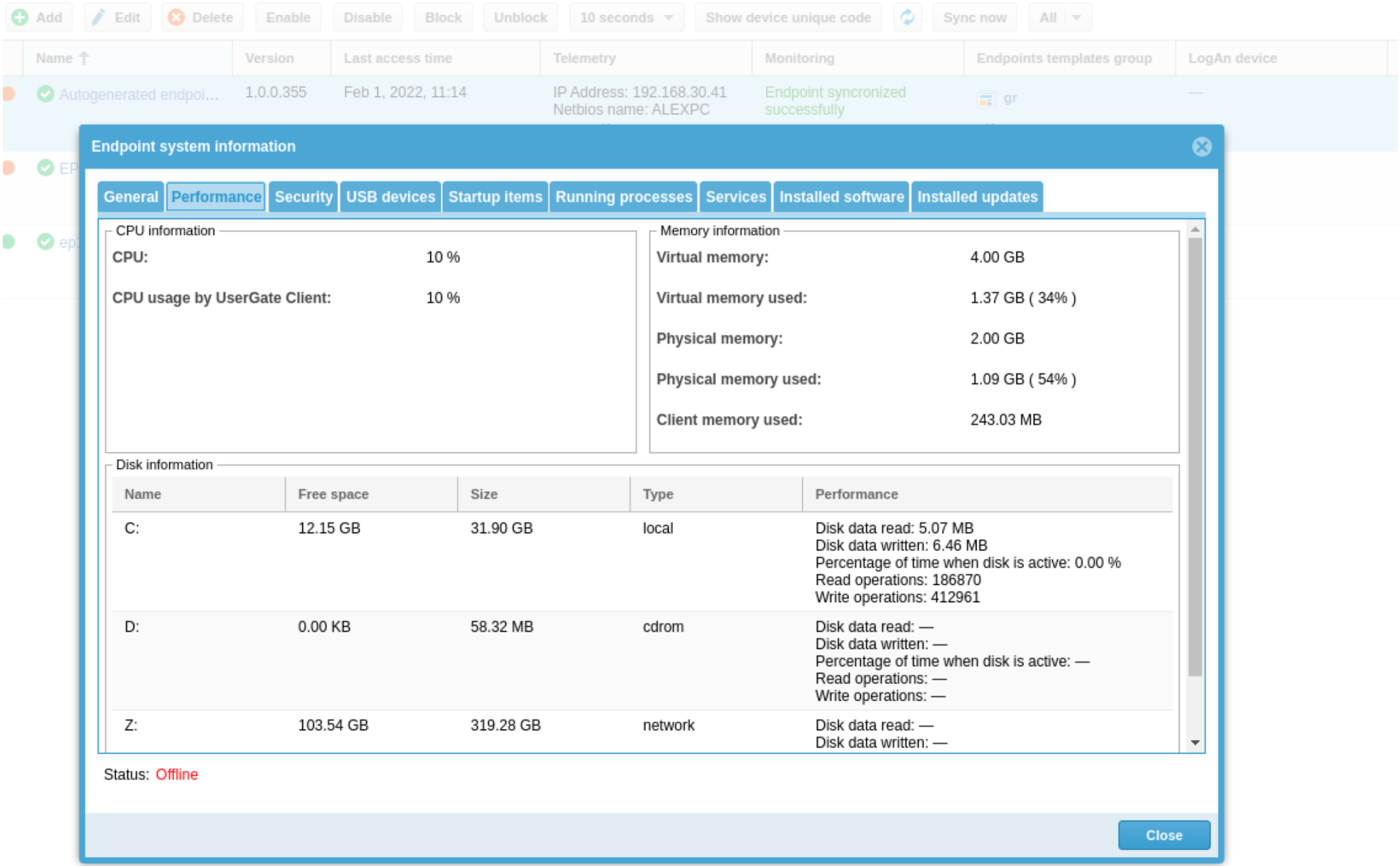
Возможности EDR



Настройка HIP

Сбор информации с устройства, объекты HIP

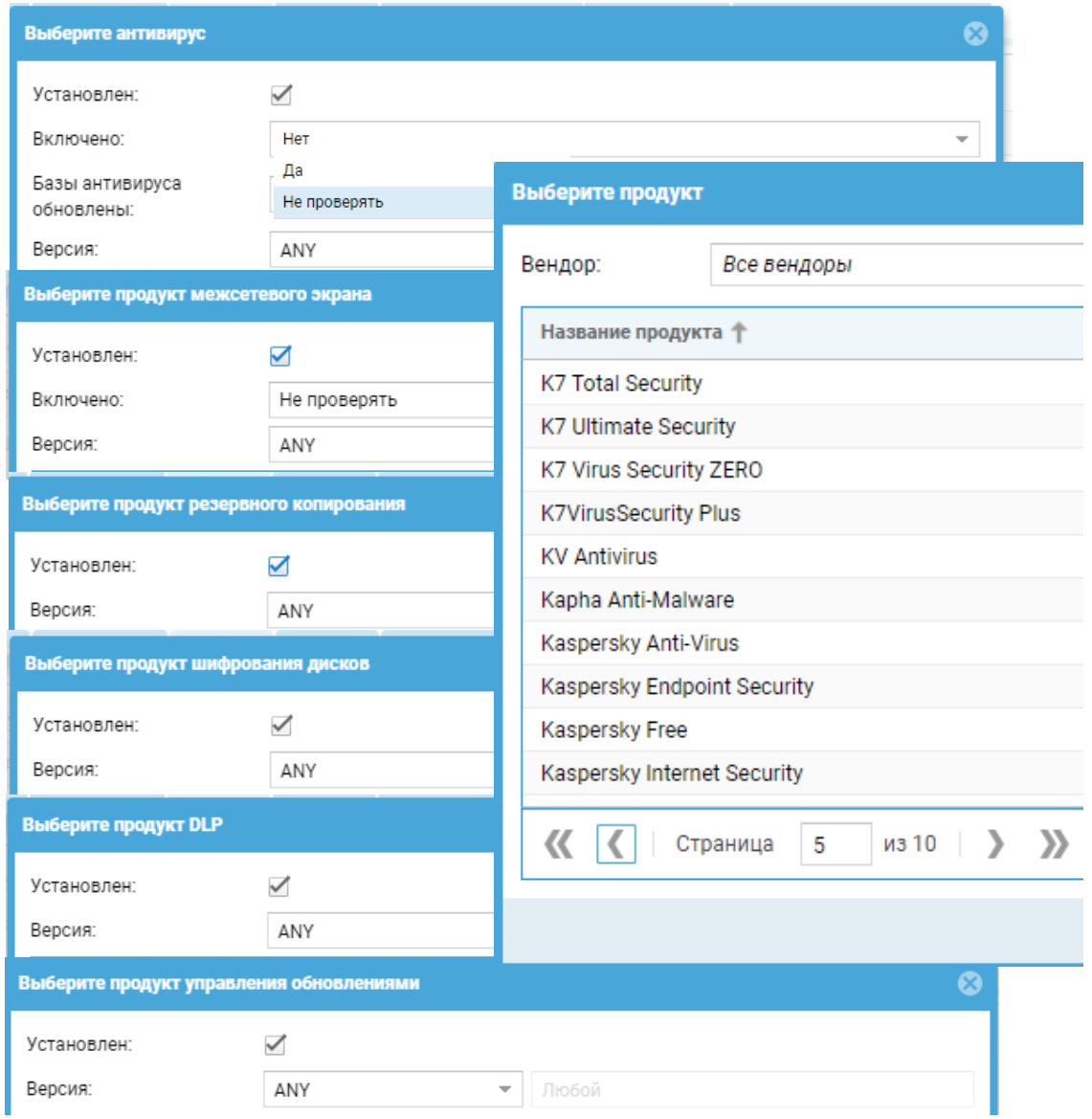
- состояние, память и производительность;
- соответствие политикам безопасности;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- приложения;
- ключи реестра;
- программное обеспечение;
- установленные обновления.


Add
Edit
Delete
Enable
Disable
Block
Unblock
10 seconds
Show device unique code
Sync now
All
Name
Version
Last access time
Telemetry
Monitoring
Endpoints templates group
LogAn device
Autogenerated endpoi...
1.0.0.355
Feb 1, 2022, 11:14
IP Address: 192.168.30.41
Netbios name: ALEXPC
Endpoint syncronized successfully
gr
Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
CPU information
CPU: 10 %
CPU usage by UserGate Client: 10 %
Memory information
Virtual memory: 4.00 GB
Virtual memory used: 1.37 GB (34%)
Physical memory: 2.00 GB
Physical memory used: 1.09 GB (54%)
Client memory used: 243.03 MB
Disk information
Name
Free space
Size
Type
Performance
C:
12.15 GB
31.90 GB
local
Disk data read: 5.07 MB
Disk data written: 6.46 MB
Percentage of time when disk is active: 0.00 %
Read operations: 186870
Write operations: 412961
D:
0.00 KB
58.32 MB
cdrom
Disk data read: —
Disk data written: —
Percentage of time when disk is active: —
Read operations: —
Write operations: —
Z:
103.54 GB
319.28 GB
network
Disk data read: —
Disk data written: —
Status: Offline
Close

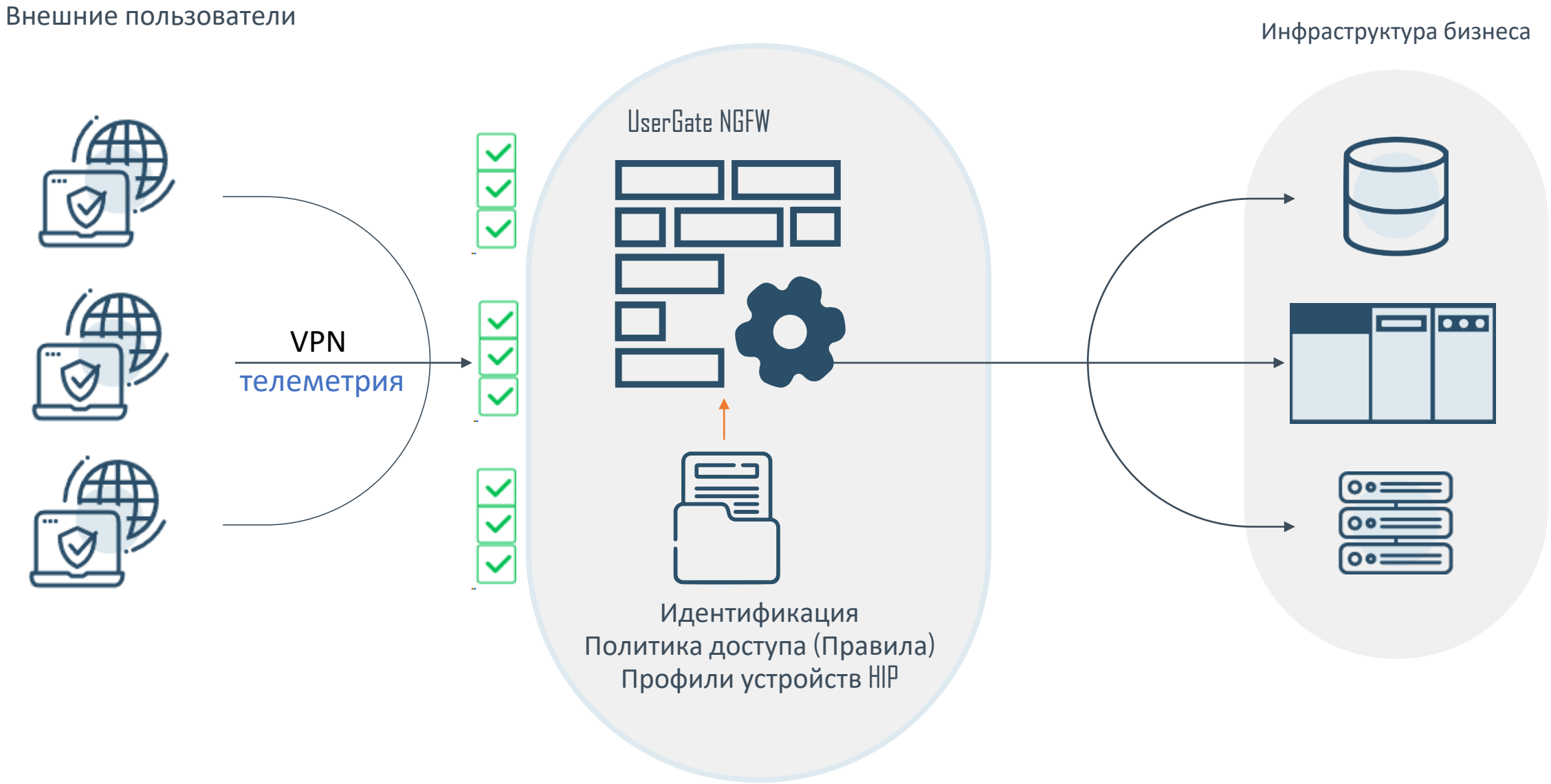
HIP – настройка

В проверке установленных продуктов доступно:

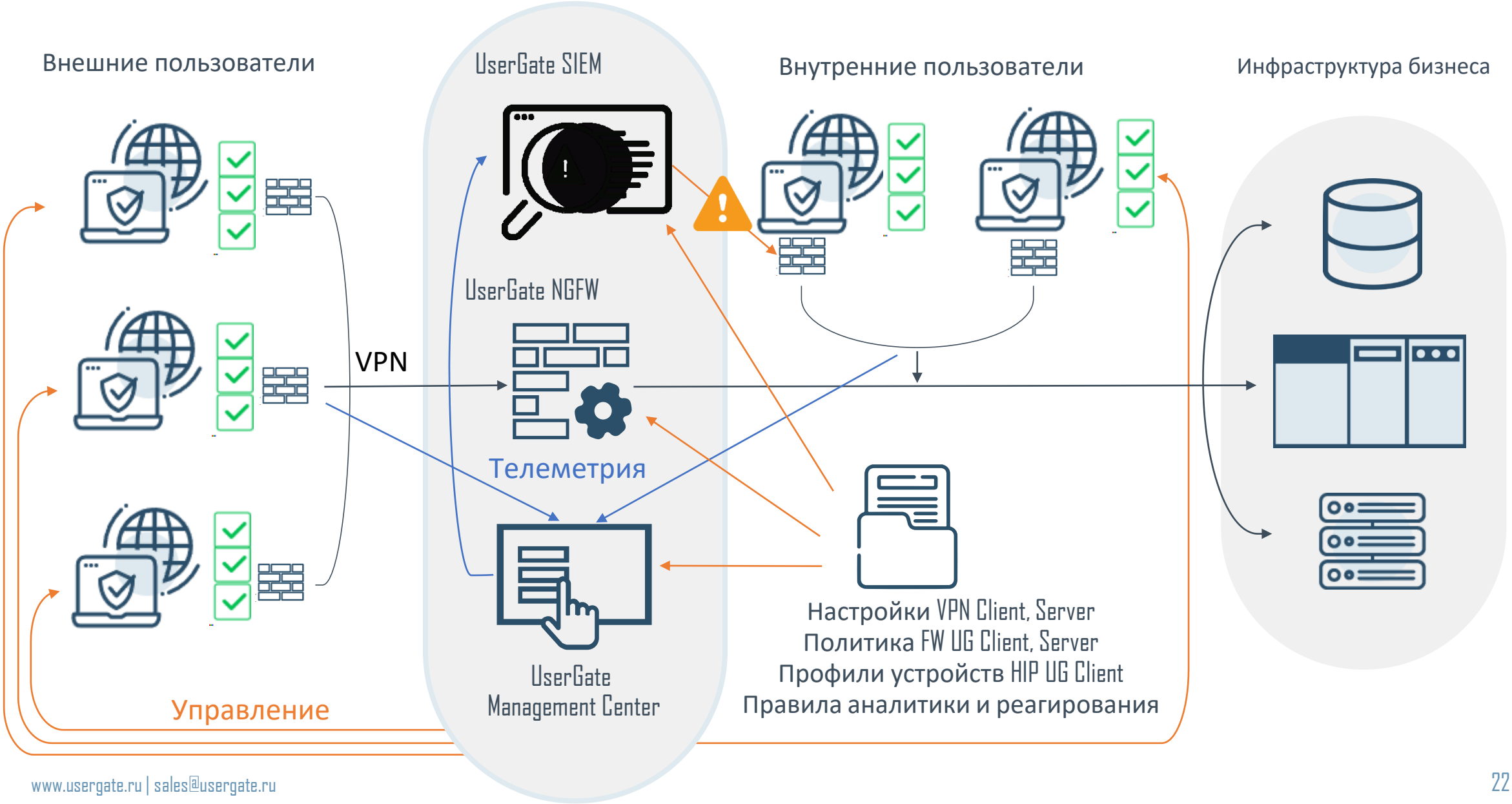
- антивирус (более 100);
- межсетевой экран (более 50);
- резервное копирование (более 50);
- шифрование диска (более 30);
- DLP (более 10);
- управление обновлениями.



Режим NGFW


Внешние пользователи
Инфраструктура бизнеса
UserGate NGFW
VPN
телеметрия
Идентификация
Политика доступа (Правила)
Профили устройств HIP

Режим МС


Внешние пользователи
UserGate SIEM
Внутренние пользователи
Инфраструктура бизнеса
UserGate NGFW
VPN
Телеметрия
UserGate
Management Center
Настройки VPN Client, Server
Политика FW UG Client, Server
Профили устройств HIP UG Client
Правила аналитики и реагирования
Управление

UserGate Client – сравнение

Функции		UG client (MC режим)	UG client (NGFW режим)	Сторонние VPN клиенты (Win, Android, etc.)
VPN		**Endpoint лицензия MC Лицензия пользователя в NGFW**	**Лицензия пользователя NGFW**	**Лицензия пользователя NGFW**
IKEv1	Аутентификация L2TP	✓	✓	✓
IKEv2	Аутентификация по сертификатам	✓	✓	✓
	Аутентификация EAP MS-CHAPv2	✓	✓	✓
	MFA	✓	✓	
	Split-tunneling	✓	✓	
HIP		**Endpoint лицензия MC NAC подписка MC**	**Лицензия пользователя NGFW NAC подписка NGFW**	
	Блокировка на клиенте	✓		
	Блокировка на NGFW		✓	
	Поддержка работы из-за NAT	✓		
Локальный FW на клиенте		**Endpoint лицензия MC**		
Мониторинг логов клиента		**Endpoint лицензия MC**		
Аналитика и реагирование		**SIEM лицензия Logan**		
Пред-настроенные правила аналитики		**Подписка на экспертизу SIEM**		

Демонстрация

ПРИГЛАШАЕМ ПОСЕТИТЬ

ИНФОФОРУМ

7-8 февраля, Москва

Доклад в секции 3: Цифровая безопасность - новые вызовы. Защита КИИ – **7 февраля**

Александр Кирий: "SOCRAT: ключевые особенности и философия подходов"

Международный ТБ ФОРУМ Технологии и Безопасность

13-15 февраля, Москва

Доклад в секции АСУ ТП КИИ – **13 февраля**

Татьяна Егорова: "Кибербезопасность объектов КИИ: насущные проблемы и пути их решения"

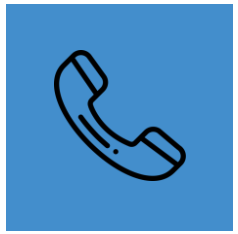
Доклад в секции РБПО – **15 февраля**

Степан Харитонов: "Один в поле не воин или как не заплутать на пути внедрения SDL"

Работайте с нами!

https://ksb-soft.ru/

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9



8 800 3333-872

info@ksb-soft.ru

Телеграм-канал
«Мнение интегратора»