UserGate

UserGate SUMMA

Комплексная защита ИТ инфраструктуры

Евгений Митюшкин

Ведущий менеджер
по работе с клиентами

emitiushkin@usergate.ru

+7 (916) 411-50-39

UserGate

13 лет разработки и внедрения

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

Фронт-офис
в г. Москве расположен
в БЦ «ФилиГрад»

Новый офис разработки и сопровождения продаж в «Санкт-Петербург Плаза»

Новое в 7.1

Новые платформы

FG

C150-C151

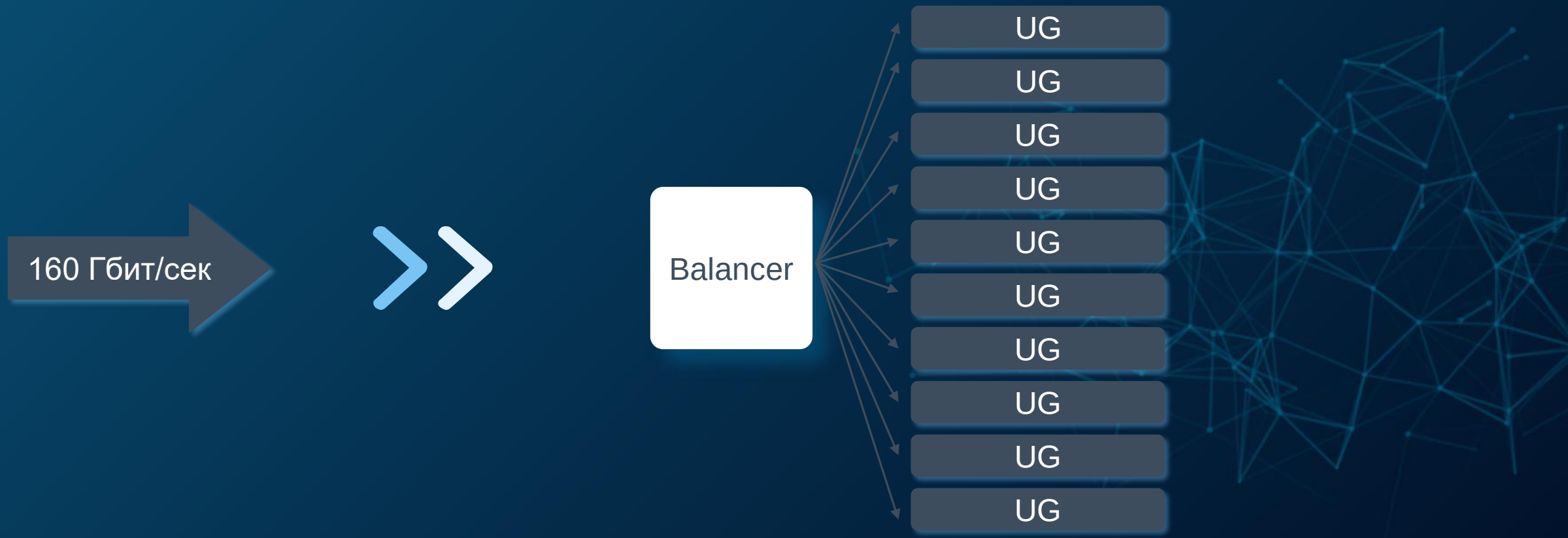
B50

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

Стекирование


160 Гбит/сек
Balancer
UG
UG
UG
UG
UG
UG
UG
UG
UG
UG

Новое в 7.1

- UserID
- Пользовательские сигнатуры COB
- Новый движок IPSv3
- IKEv2
- Темная тема
- UserGate Client
- UserGate SIEM Light (MVP)

CLI

Теперь в CLI можно конфигурировать абсолютно все, и даже немного больше, чем в веб-версии

Добавлены новые инструменты диагностики

```
Admin@UGOS>

+ traceroute      Print the route packets trace to network host
+ shutdown        Shutdown
+ show            Show
+ clear           Clear
+ ping            Ping
+ reboot          Reboot
+ date            Display date
+ exit            Logout
+ netcheck        Check HTTP/HTTPS connection
+ configure       Configuration mode
+ dig             Query domain name server
```

Система бэкапов

Уменьшен размер образа

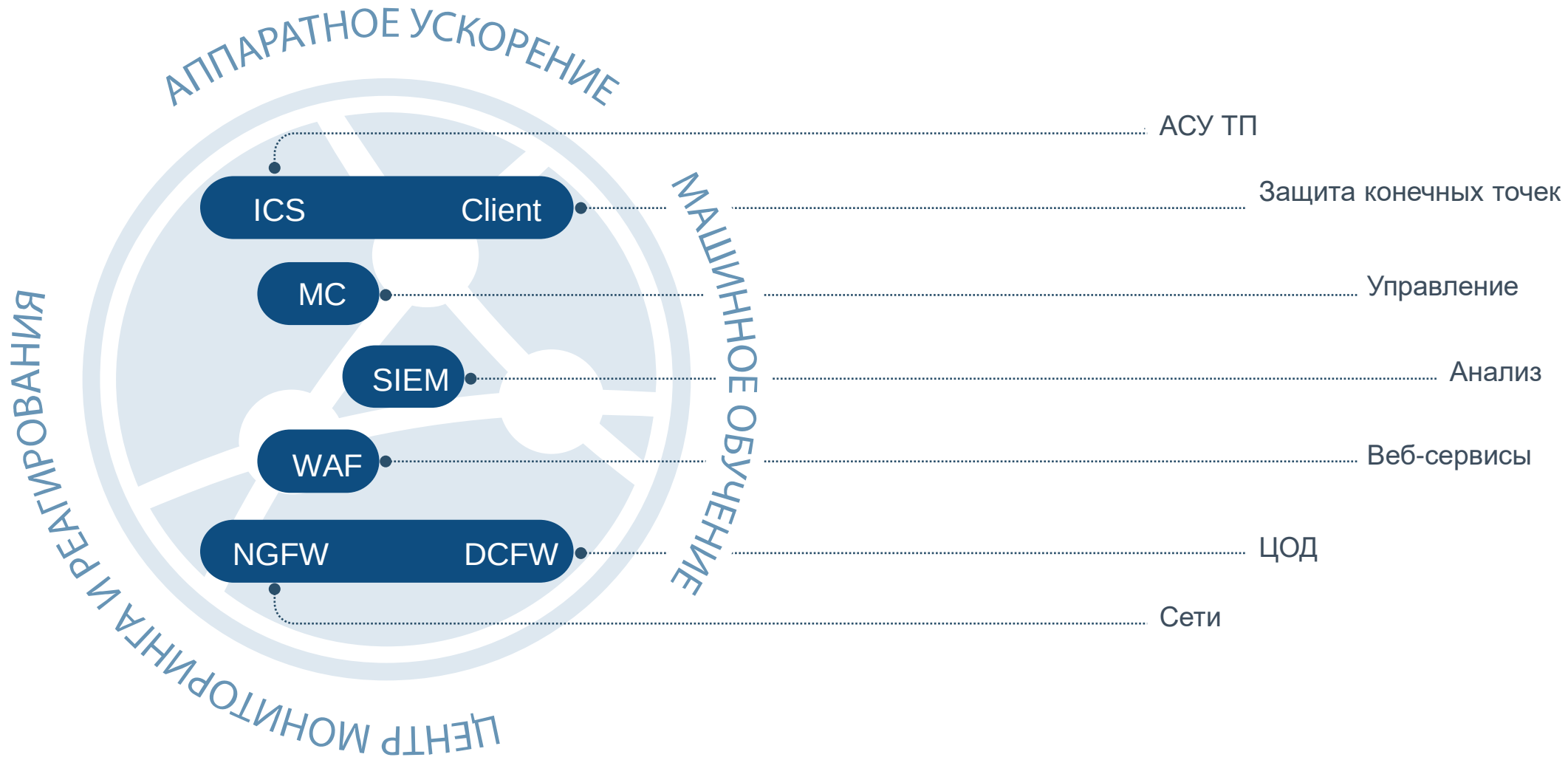
Проведение бэкапов без перезагрузки

Хранение бэкапов в памяти устройства

Что мы умеем?

UserGate SUMMA

100% видимость событий безопасности



NGFW

Security Web Gateway (SWG)

Intrusion Detection & Prevention System (COB/IDPS)

Zero Trust Network Access (ZTNA)

VPN

URL filtering

Proxy
Proxy + App Control

SSL-инспекция

Mail Security

Antivirus

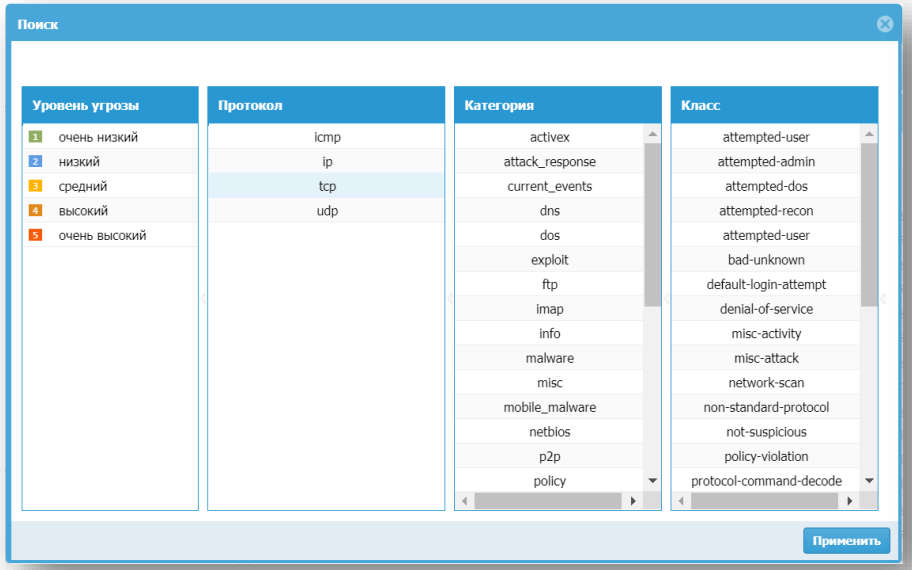
UserGate IDPS (COB)

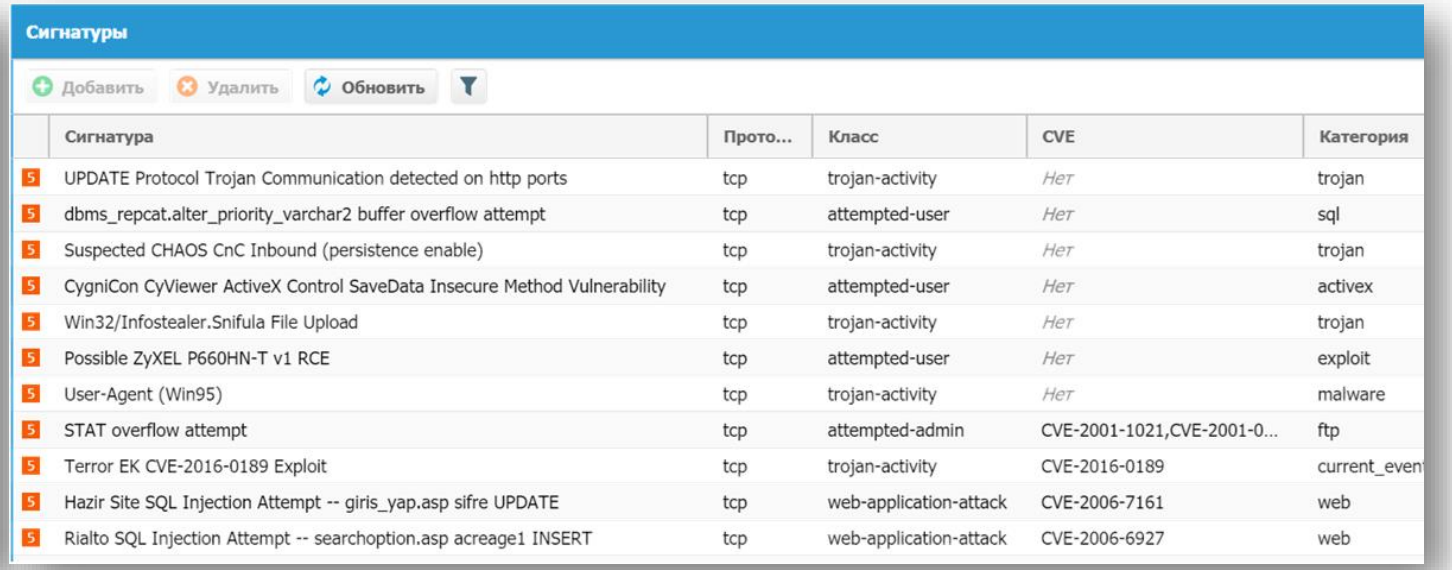
Модуль в составе UserGate NGFW

COB / IDPS

Система обнаружения и предотвращения вторжений

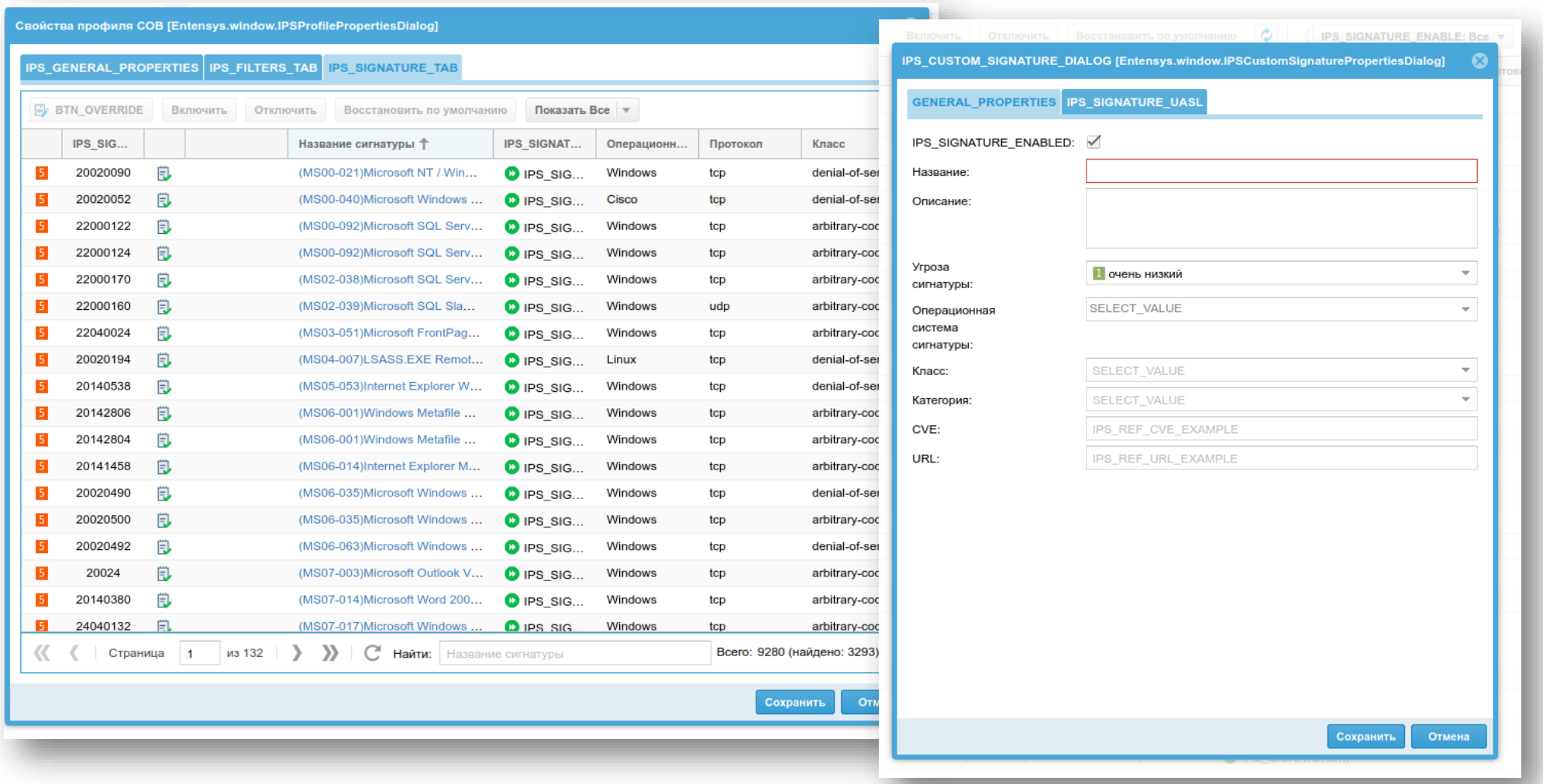
- Реагирование на атаки злоумышленников, использующих известные уязвимости.
- Распознаваниие вредоносной активности внутри сети.





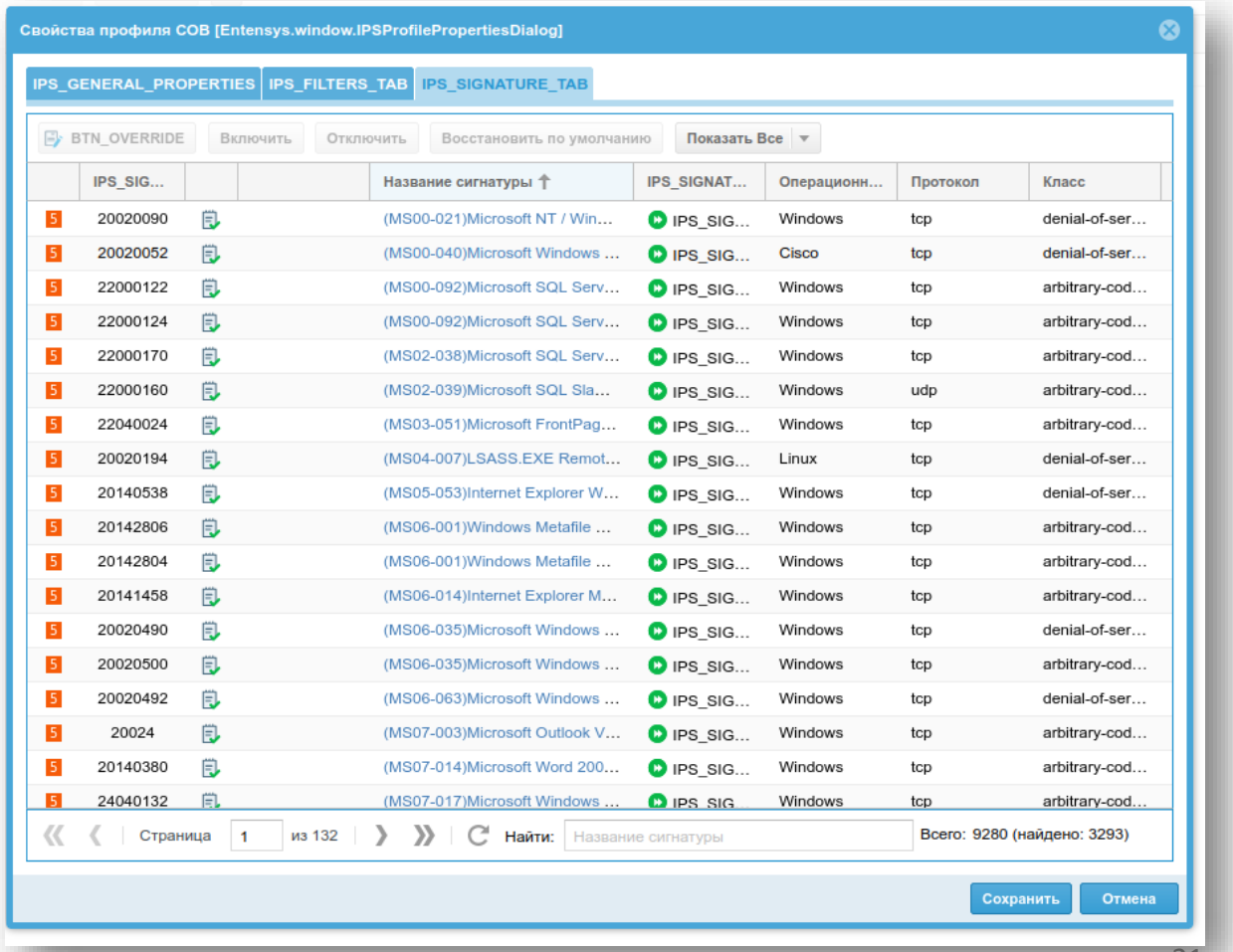
Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon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

Создание собственных сигнатур

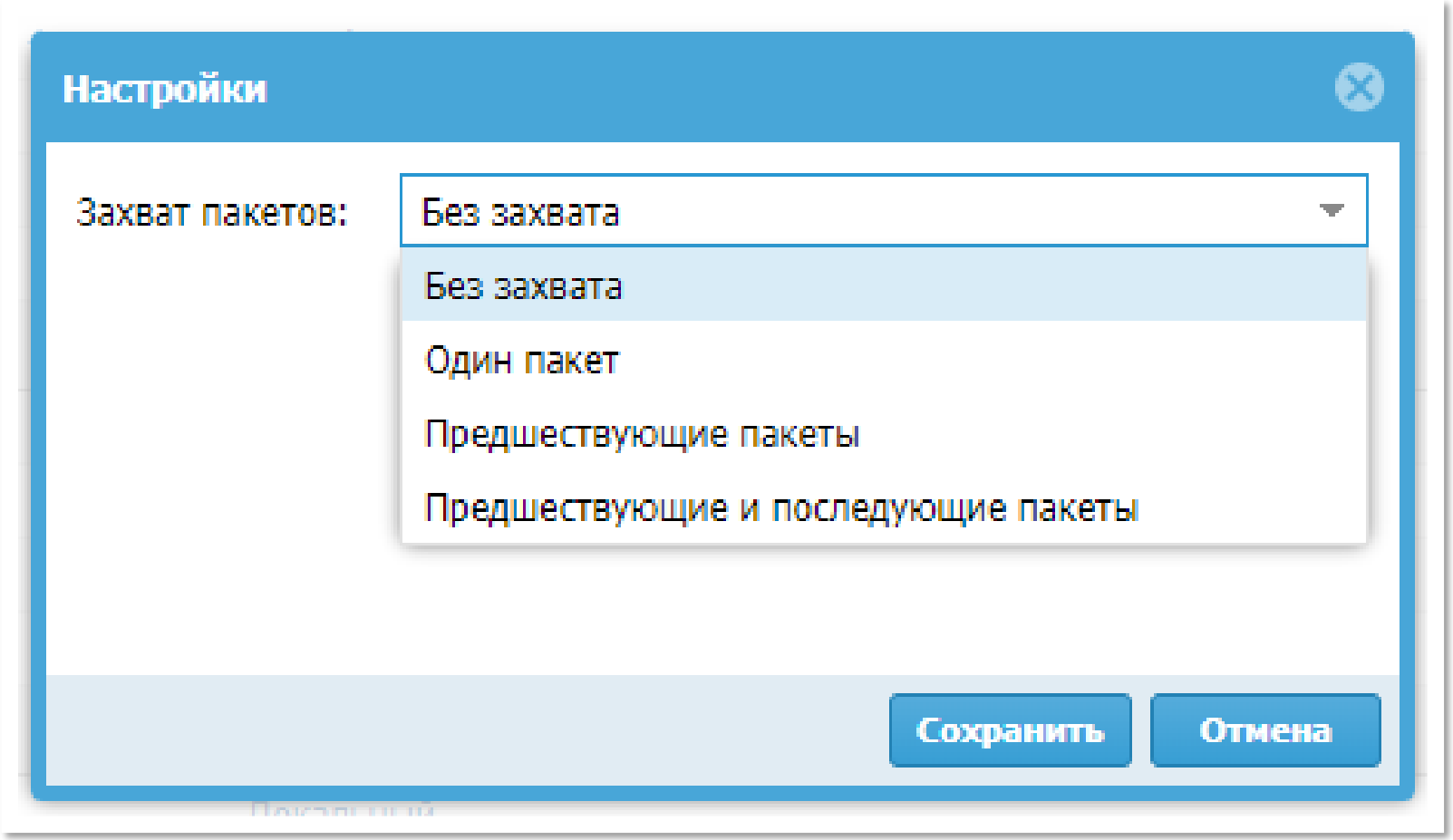


Создание своего профиля IDPS

с возможностью автоматического обновления при появлении новых сигнатур соответствующего типа



Запись трафика в PCAP



Контент-фильтрация

Модуль в составе UserGate NGFW

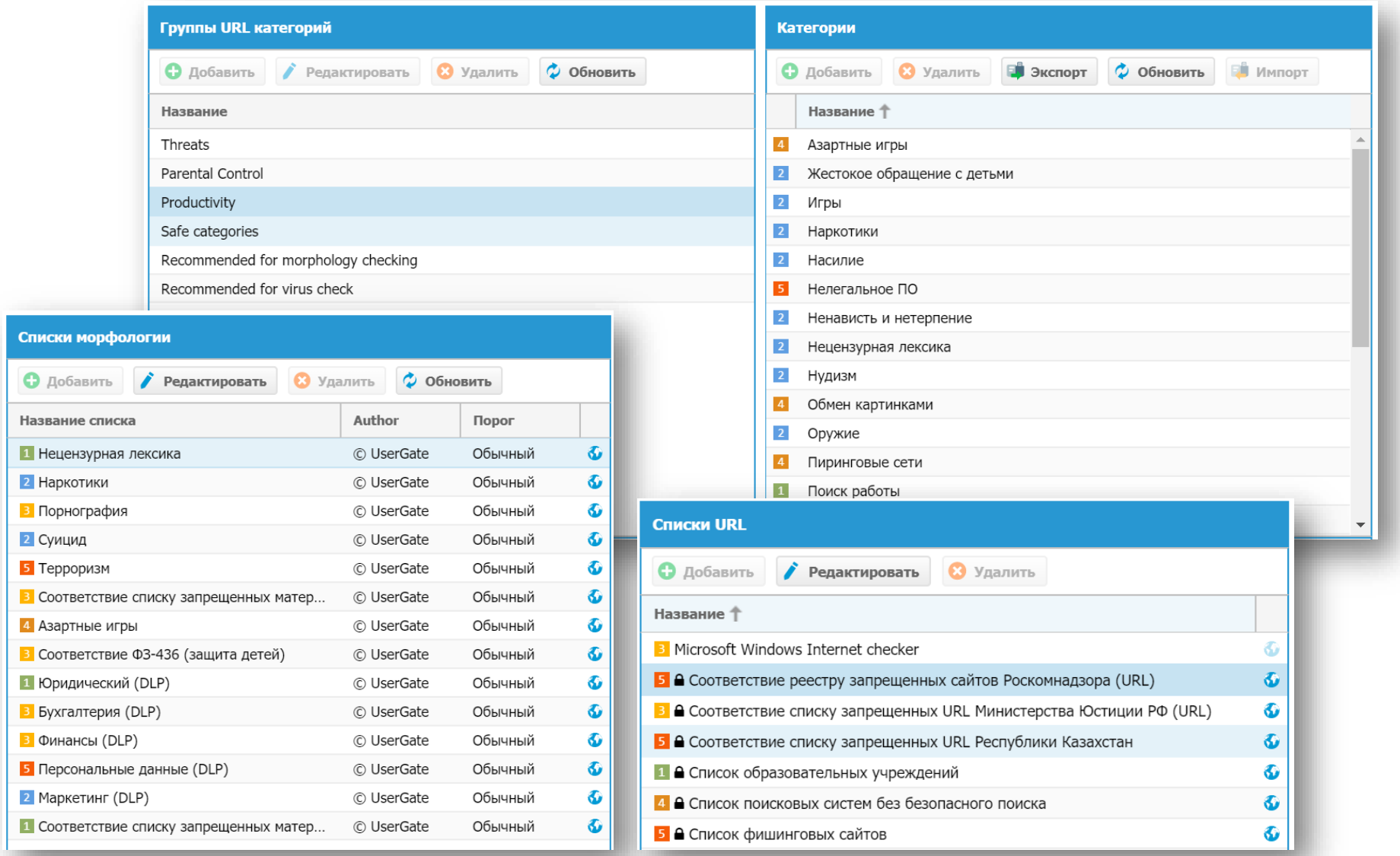
Механизмы фильтрации

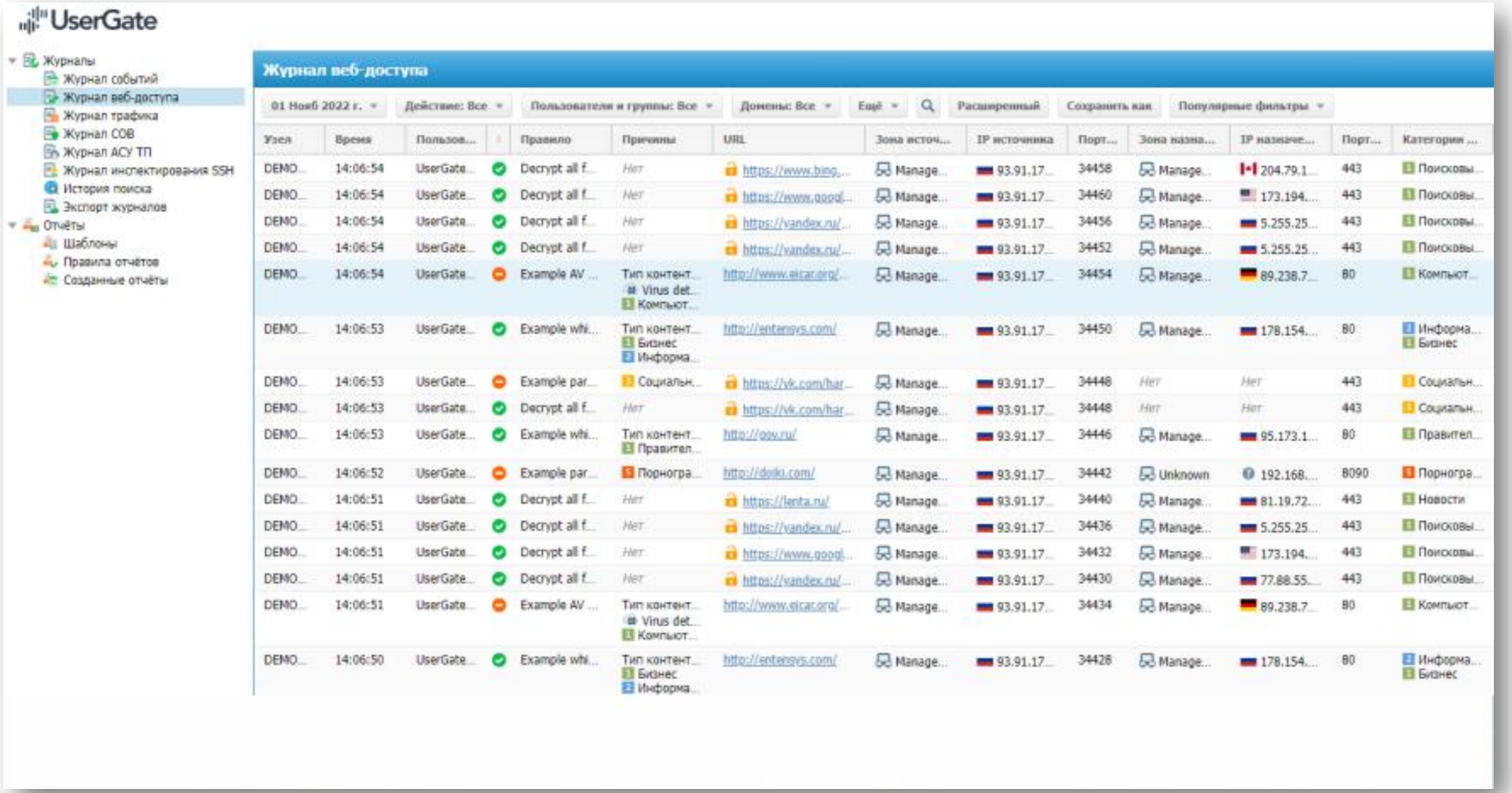
- Фильтрация по категориям
- Морфологический анализ
- Безопасный поиск
- Белые и черные списки
- Блокировка контекстной рекламы
- Запрет загрузки определенных видов файлов
- Антивирусная проверка трафика
- Интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3

Механизмы фильтрации

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

UserGate URL Filtering




UserGate
Журналы
Журнал событий
Журнал веб-доступа
Журнал трафика
Журнал СОВ
Журнал АСУ ТП
Журнал инспектирования SSH
История поиска
Экспорт журналов
Отчёты
Шаблоны
Правила отчётов
Созданные отчёты
Журнал веб-доступа
01 Нояб 2022 г.
Действие: Все
Пользователи и группы: Все
Домены: Все
Ещё
Расширенный
Сохранить как
Популярные фильтры
Узел
Время
Пользов...
Правило
Причины
URL
Зона источ...
IP источника
Порт...
Зона назна...
IP назначе...
Порт...
Категории ...
DEMO 14:06:54 UserGate Decrypt all f... Нет https://www.bing... Manage... 93.91.17... 34458 Manage... 204.79.1... 443 Поисковы...
DEMO 14:06:54 UserGate Decrypt all f... Нет https://www.googl... Manage... 93.91.17... 34460 Manage... 173.194.... 443 Поисковы...
DEMO 14:06:54 UserGate Decrypt all f... Нет https://yandex.ru/... Manage... 93.91.17... 34456 Manage... 5.255.25... 443 Поисковы...
DEMO 14:06:54 UserGate Decrypt all f... Нет https://yandex.ru/... Manage... 93.91.17... 34452 Manage... 5.255.25... 443 Поисковы...
DEMO 14:06:54 UserGate Example AV ... Тип контент... Virus det... Компьют... http://www.eicar.org/... Manage... 93.91.17... 34454 Manage... 89.238.7... 80 Компьют...
DEMO 14:06:53 UserGate Example whi... Тип контент... Бизнес Информа... http://entensys.com/ Manage... 93.91.17... 34450 Manage... 178.154.... 80 Информа... Бизнес
DEMO 14:06:53 UserGate Example par... Социальн... https://vk.com/har... Manage... 93.91.17... 34448 Нет Нет 443 Социальн...
DEMO 14:06:53 UserGate Decrypt all f... Нет https://vk.com/har... Manage... 93.91.17... 34448 Нет Нет 443 Социальн...
DEMO 14:06:53 UserGate Example whi... Тип контент... Правител... http://gov.ru/ Manage... 93.91.17... 34446 Manage... 95.173.1... 80 Правител...
DEMO 14:06:52 UserGate Example par... Порногра... http://deiki.com/ Manage... 93.91.17... 34442 Unknown 192.168.... 8090 Порногра...
DEMO 14:06:51 UserGate Decrypt all f... Нет https://lenta.ru/ Manage... 93.91.17... 34440 Manage... 81.19.72... 443 Новости
DEMO 14:06:51 UserGate Decrypt all f... Нет https://yandex.ru/... Manage... 93.91.17... 34436 Manage... 5.255.25... 443 Поисковы...
DEMO 14:06:51 UserGate Decrypt all f... Нет https://www.googl... Manage... 93.91.17... 34432 Manage... 173.194.... 443 Поисковы...
DEMO 14:06:51 UserGate Decrypt all f... Нет https://yandex.ru/... Manage... 93.91.17... 34430 Manage... 77.88.55... 443 Поисковы...
DEMO 14:06:51 UserGate Example AV ... Тип контент... Virus det... Компьют... http://www.eicar.org/... Manage... 93.91.17... 34434 Manage... 89.238.7... 80 Компьют...
DEMO 14:06:50 UserGate Example whi... Тип контент... Бизнес Информа... http://entensys.com/ Manage... 93.91.17... 34428 Manage... 178.154.... 80 Информа... Бизнес

UserGate Client

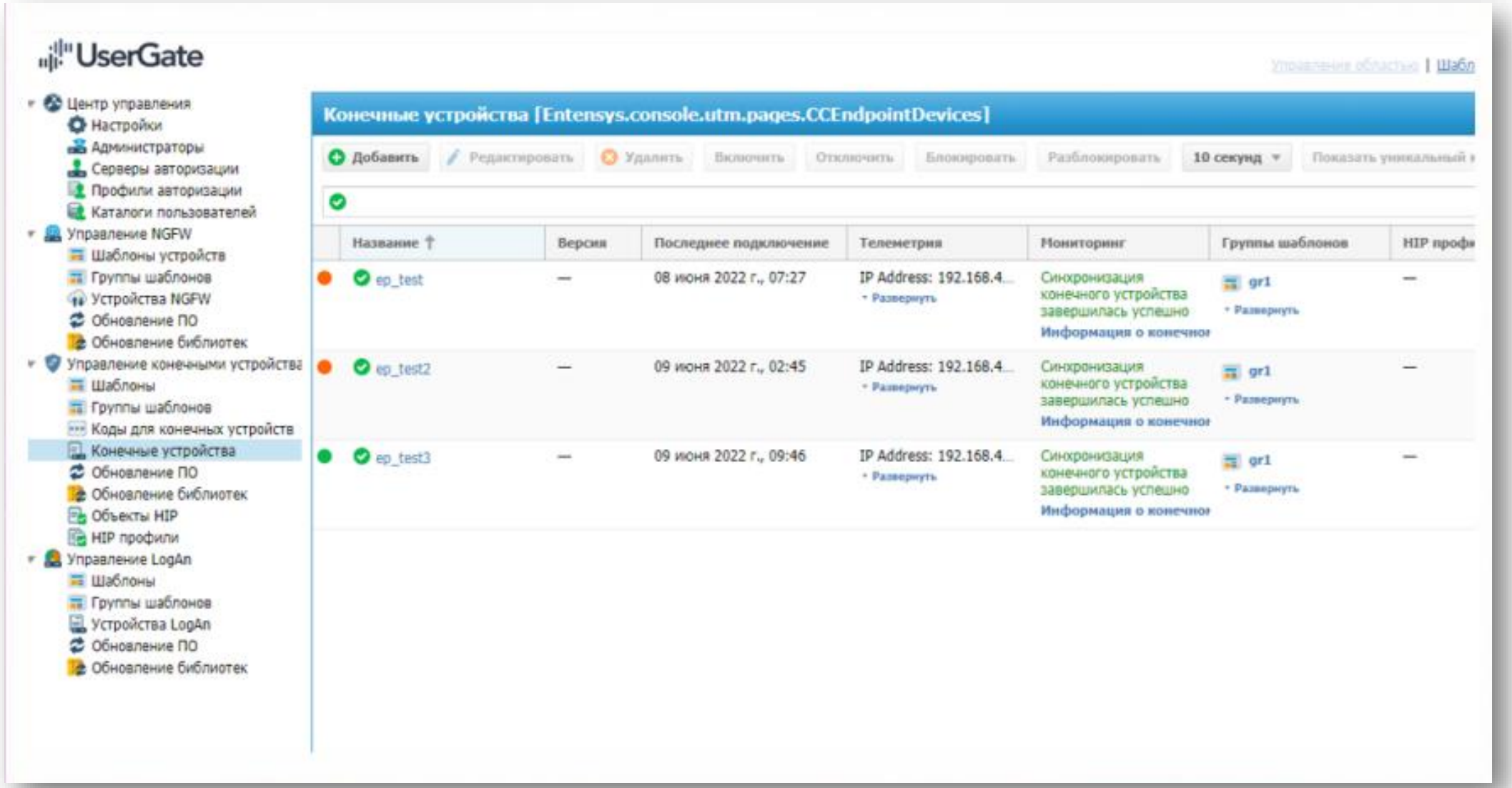
EDR

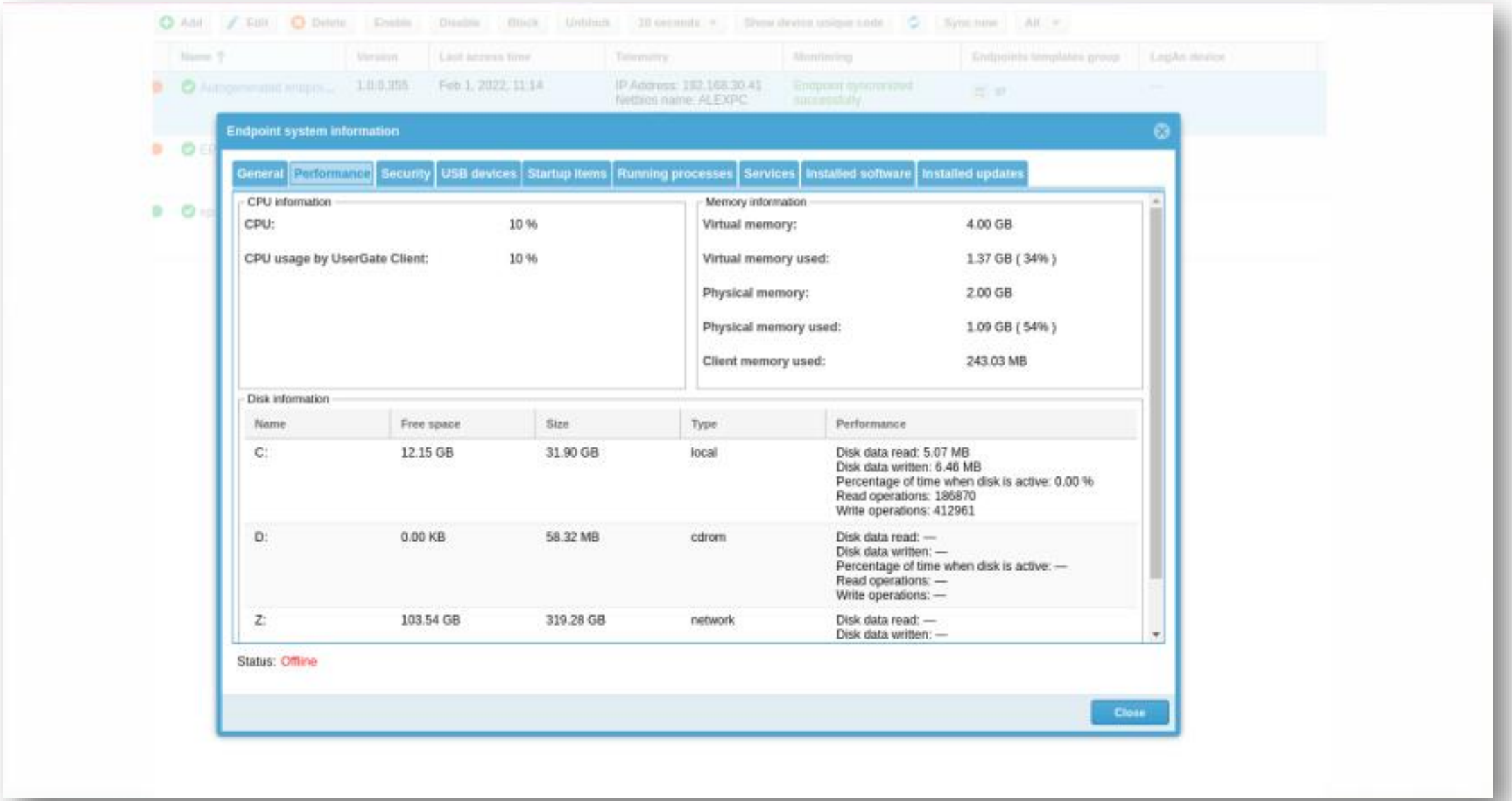
VPN

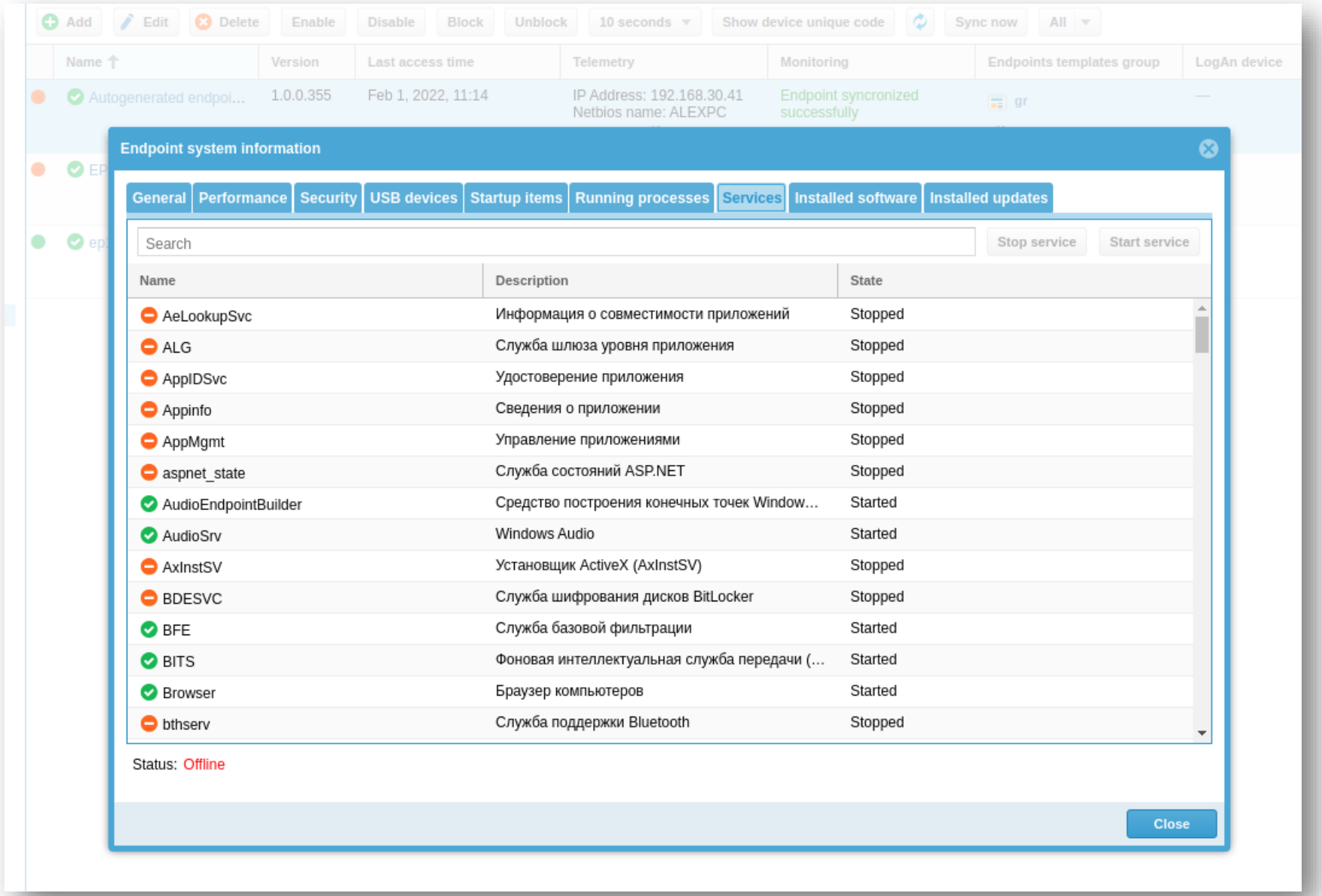
NAC

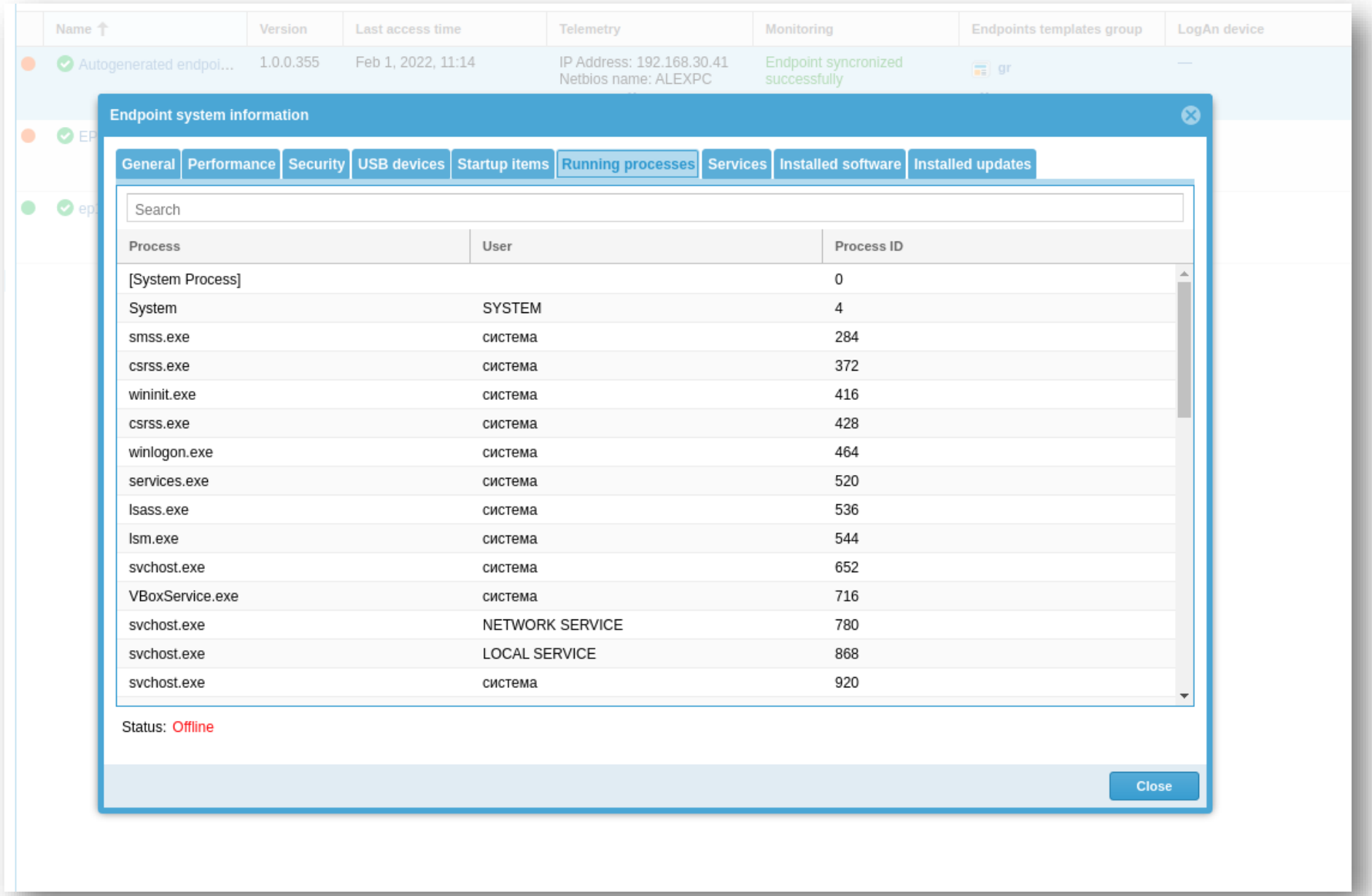
UserGate Client

- Межсетевой экран класса B
- Защита рабочих мест от сложных угроз: IoC и IoA
- Контроль состояния хоста (версии ПО, обновлений
- Наличие включенной защиты, процессов и служб)
- Контентная фильтрация
- VPN-клиент для удаленной работы
- Средство аутентификации (MFA)
- Сенсор для SIEM


UserGate
Центр управления
Настройки
Администраторы
Серверы авторизации
Профили авторизации
Каталоги пользователей
Управление NGFW
Шаблоны устройств
Группы шаблонов
Устройства NGFW
Обновление ПО
Обновление библиотек
Управление конечными устройства
Шаблоны
Группы шаблонов
Коды для конечных устройств
Конечные устройства
Обновление ПО
Обновление библиотек
Объекты HIP
HIP профили
Управление LogAn
Шаблоны
Группы шаблонов
Устройства LogAn
Обновление ПО
Обновление библиотек
Конечные устройства [Entensys.console.utm.pages.CCEndpointDevices]
Добавить
Редактировать
Удалить
Включить
Отключить
Блокировать
Разблокировать
10 секунд
Название
Версия
Последнее подключение
Телеметрия
Мониторинг
Группы шаблонов
HIP профи
ep_test
08 июня 2022 г., 07:27
IP Address: 192.168.4...
Развернуть
Синхронизация конечного устройства завершилась успешно
gr1
ep_test2
09 июня 2022 г., 02:45
ep_test3
09 июня 2022 г., 09:46

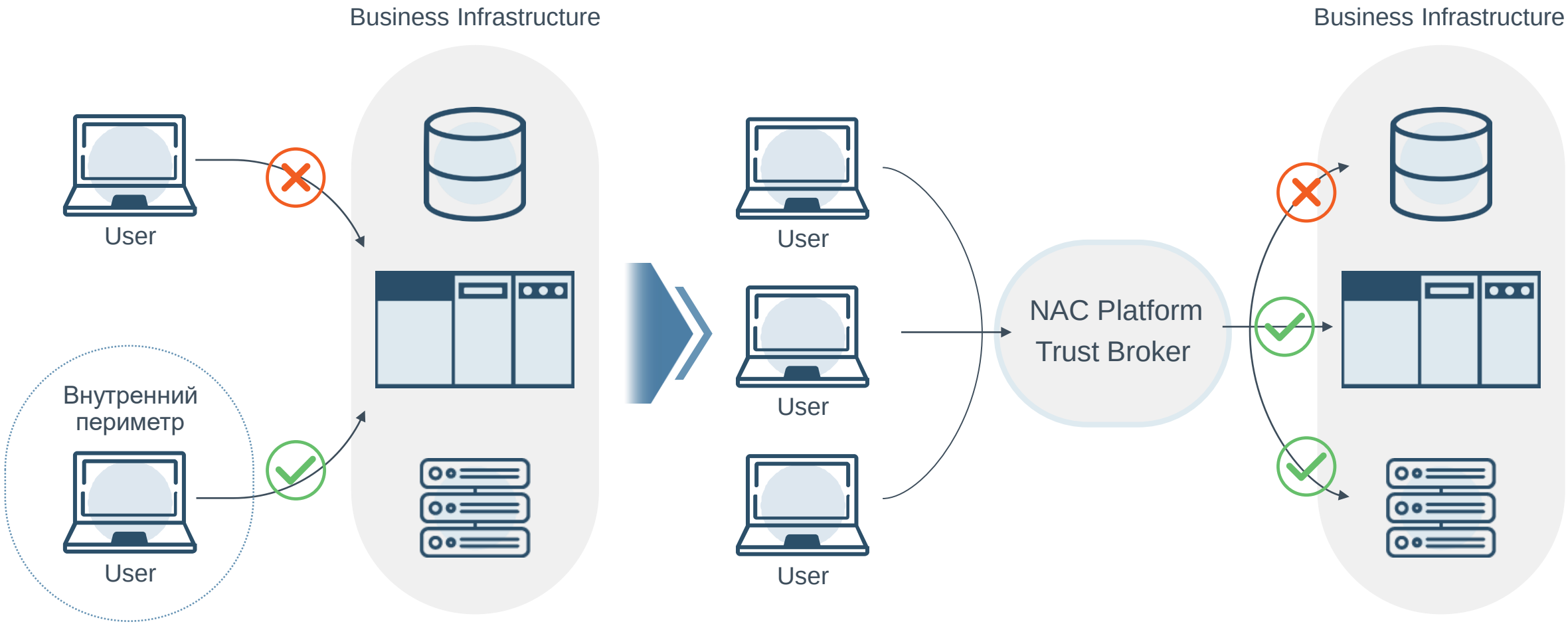

Endpoint system information
General
Performance
Security
USB devices
Startup items
Running processes
Services
Installed software
Installed updates
CPU information
CPU: 10 %
CPU usage by UserGate Client: 10 %
Memory information
Virtual memory: 4.00 GB
Virtual memory used: 1.37 GB (34%)
Physical memory: 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


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
Search
Stop service
Start service
Name
Description
State
AeLookupSvc
Информация о совместимости приложений
Stopped
ALG
Служба шлюза уровня приложения
Stopped
AppIDSvc
Удостоверение приложения
Stopped
Appinfo
Сведения о приложении
Stopped
AppMgmt
Управление приложениями
Stopped
aspnet_state
Служба состояний ASP.NET
Stopped
AudioEndpointBuilder
Средство построения конечных точек Window...
Started
AudioSrv
Windows Audio
Started
AxInstSV
Установщик ActiveX (AxInstSV)
Stopped
BDESVC
Служба шифрования дисков BitLocker
Stopped
BFE
Служба базовой фильтрации
Started
BITS
Фоновая интеллектуальная служба передачи (...
Started
Browser
Браузер компьютеров
Started
bthserv
Служба поддержки Bluetooth
Stopped
Status: Offline
Close


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
Search
Process
User
Process ID
[System Process] 0
System SYSTEM 4
smss.exe система 284
csrss.exe система 372
wininit.exe система 416
csrss.exe система 428
winlogon.exe система 464
services.exe система 520
lsass.exe система 536
lsm.exe система 544
svchost.exe система 652
VBoxService.exe система 716
svchost.exe NETWORK SERVICE 780
svchost.exe LOCAL SERVICE 868
svchost.exe система 920
Status: Offline
Close

Задача NAC

Заменить фактор доверенности нахождения
на фактор доверенности состояния устройства



Фактор доверенности нахождения

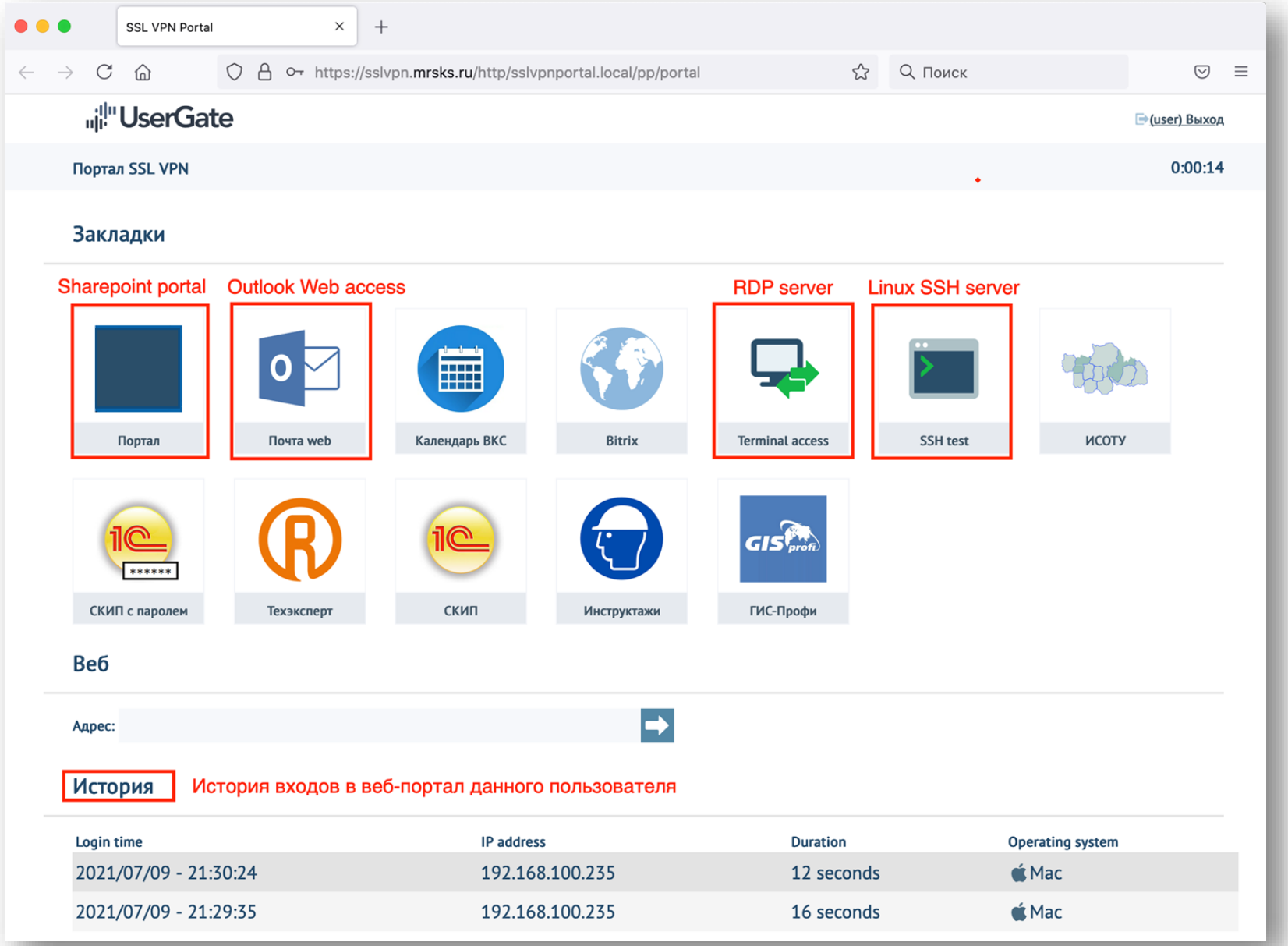
Фактор доверенности состояния устройства

Безопасный доступ

Безопасная публикация ресурсов и сервисов

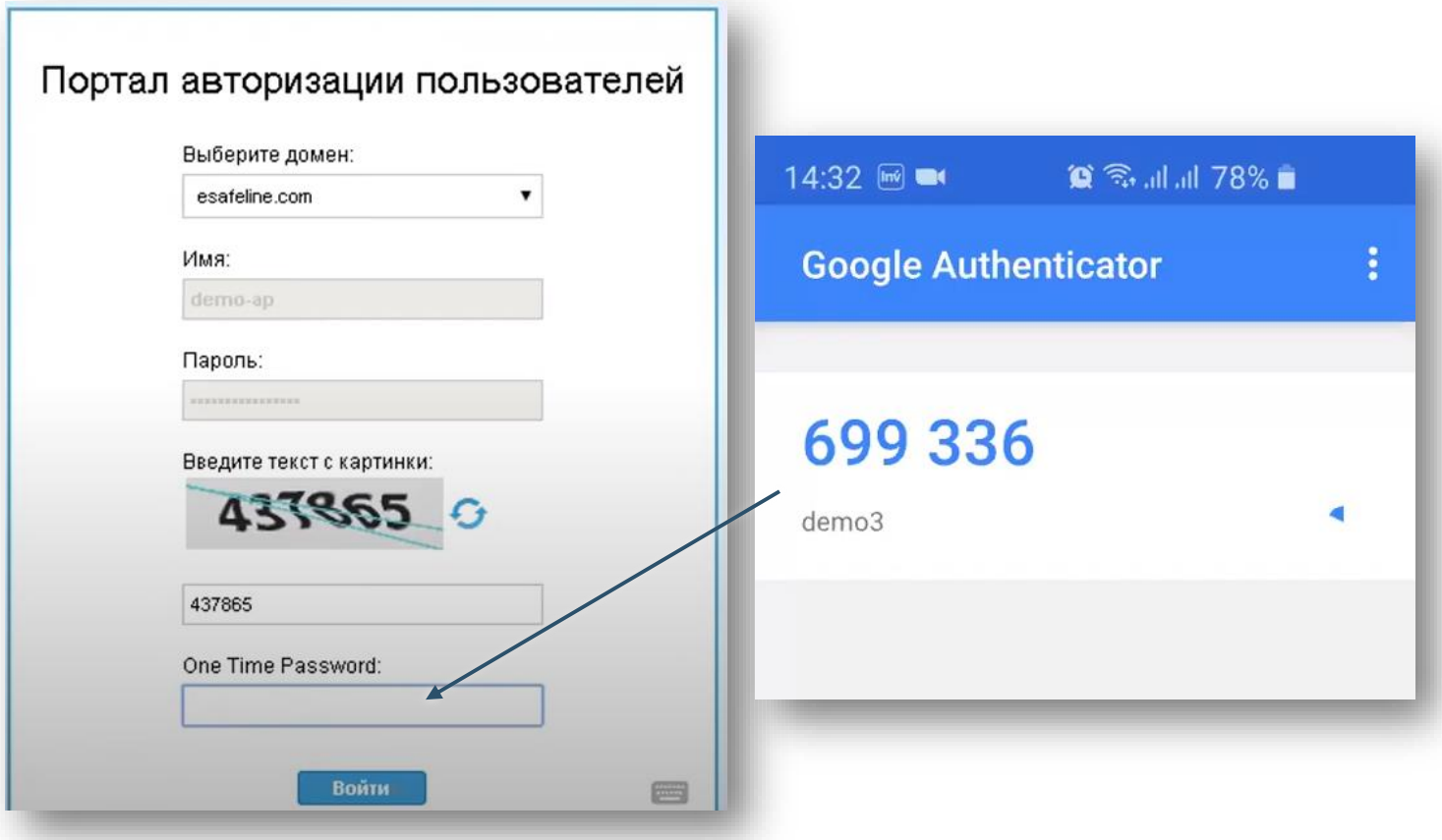
Reverse Proxy
Обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

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.


SSL VPN Portal
https://sslvpn.mrsks.ru/http/sslvpnportal.local/pp/portal
Поиск
UserGate
(user) Выход
Портал SSL VPN
0:00:14
Закладки
Sharepoint portal
Outlook Web access
RDP server
Linux SSH server
Портал
Почта web
Календарь ВКС
Bitrix
Terminal access
SSH test
ИСОТУ
СКИП с паролем
Техэксперт
СКИП
Инструктажи
ГИС-Профи
Веб
Адрес:
История
История входов в веб-портал данного пользователя
Login time
IP address
Duration
Operating system
2021/07/09 - 21:30:24
192.168.100.235
12 seconds
Mac
2021/07/09 - 21:29:35
192.168.100.235
16 seconds
Mac

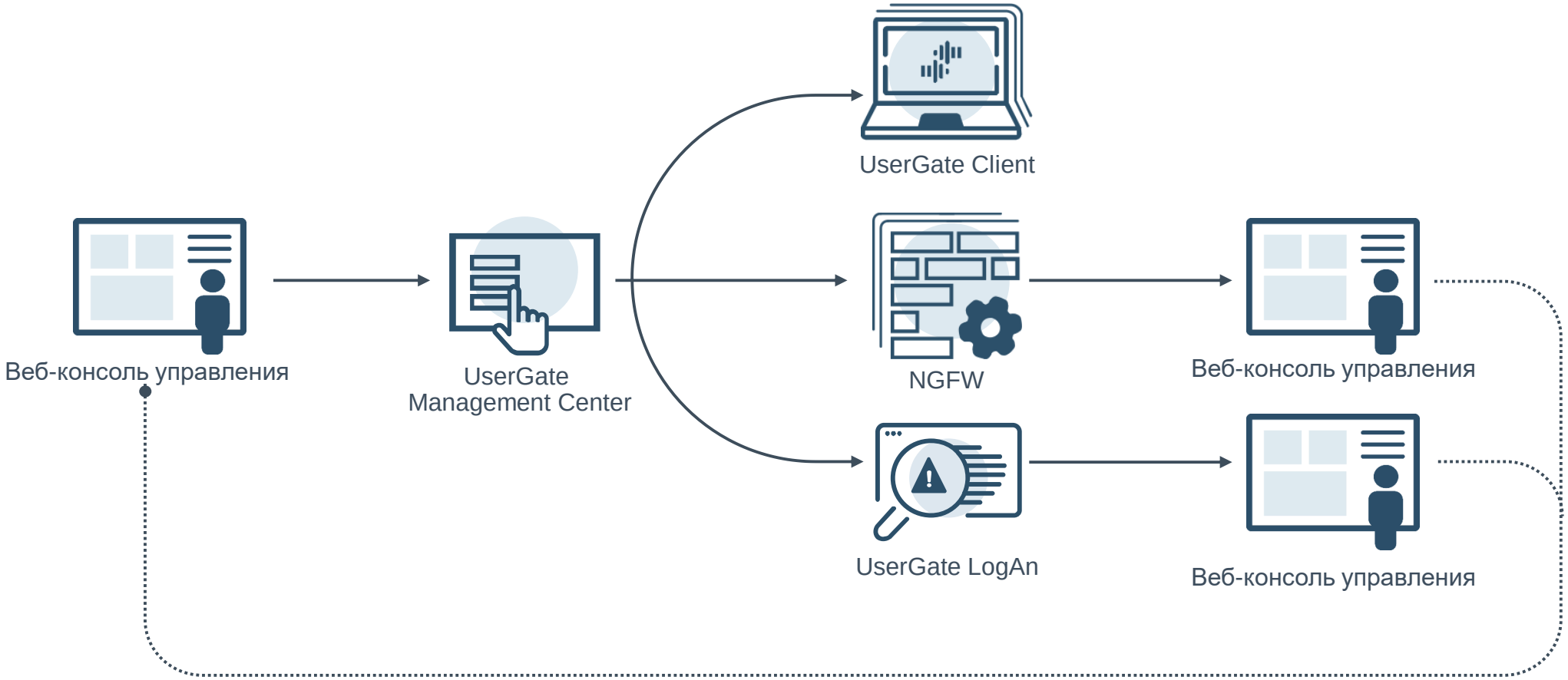
Многофакторная аутентификация

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

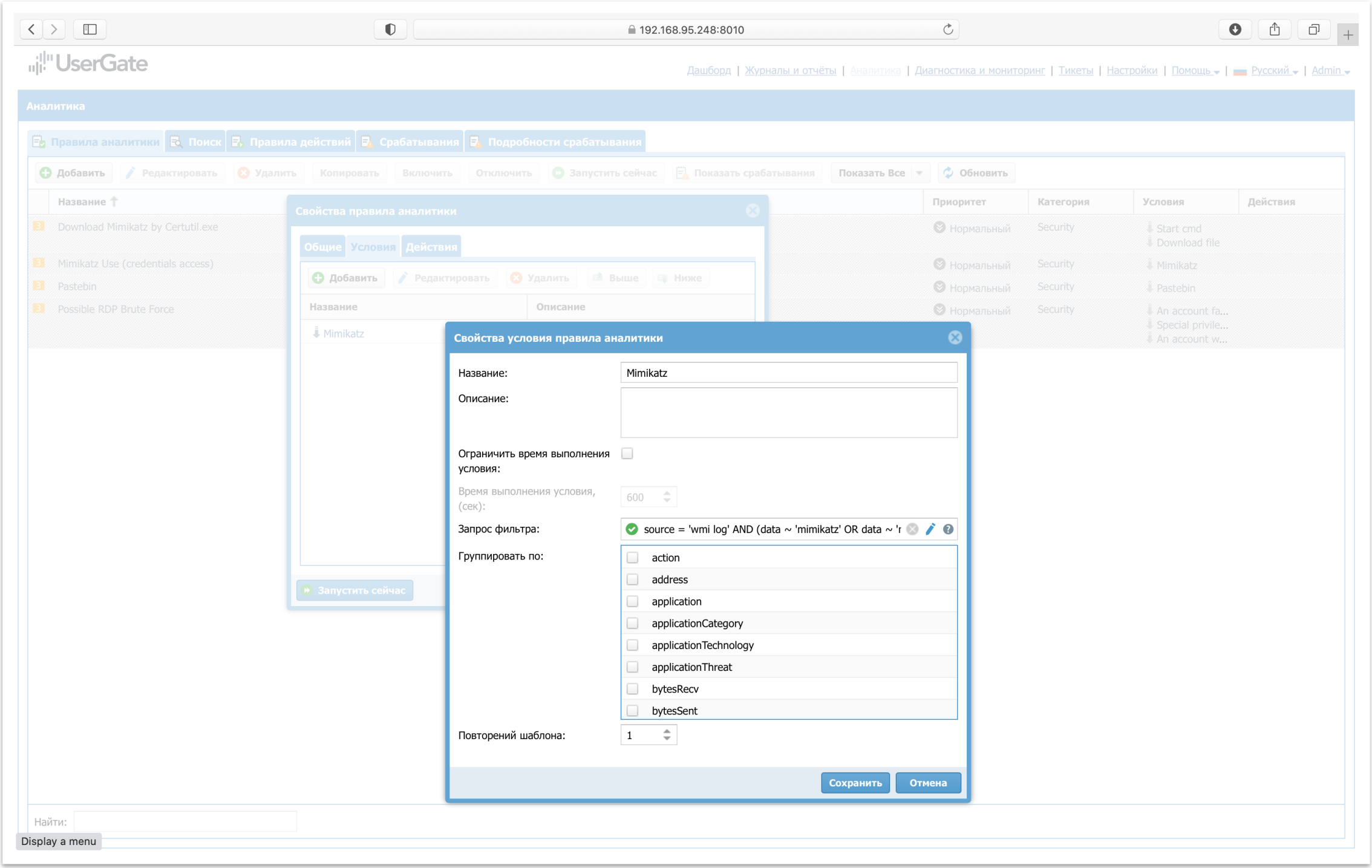


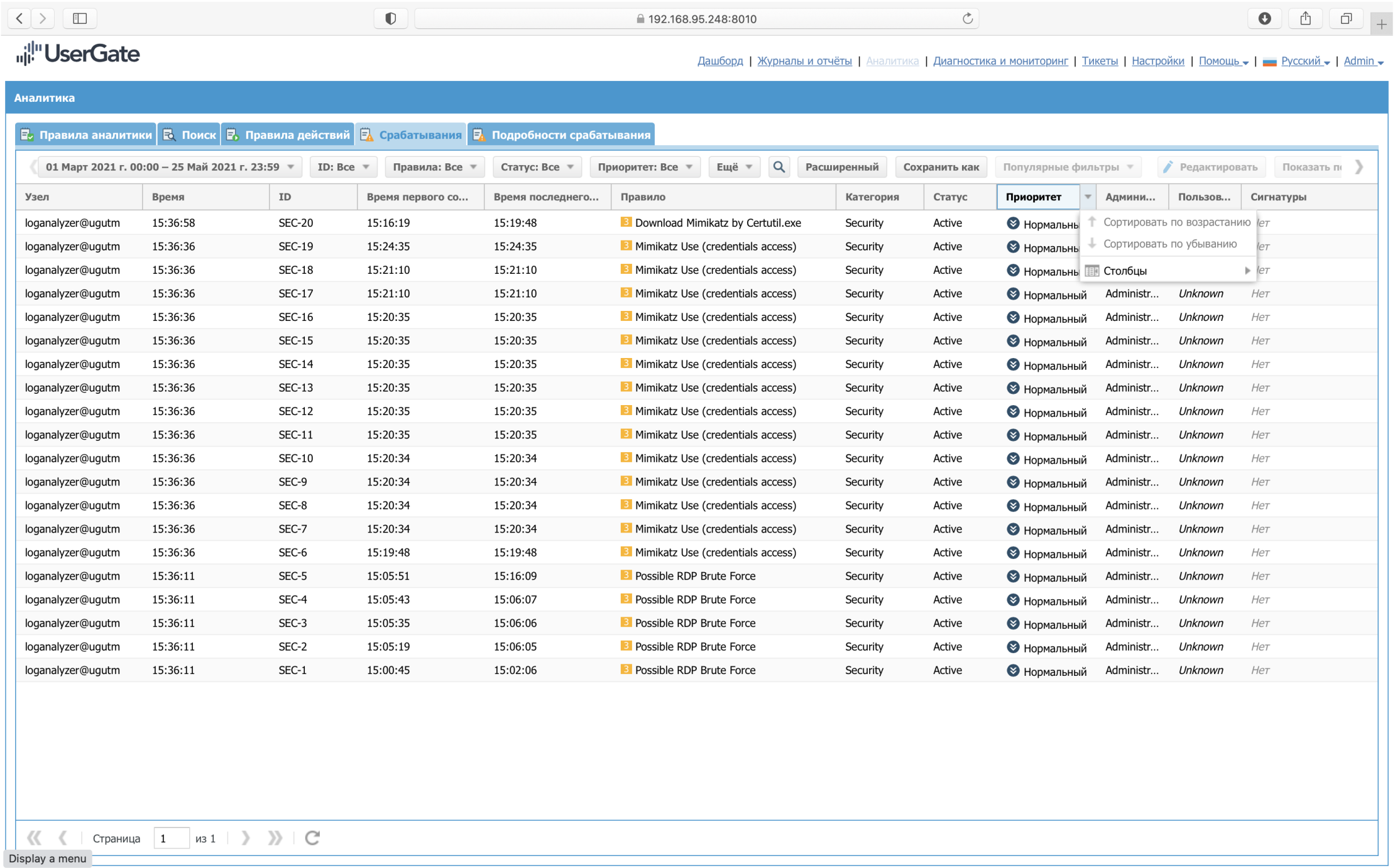
UserGate Management Center

Веб-консоль управления

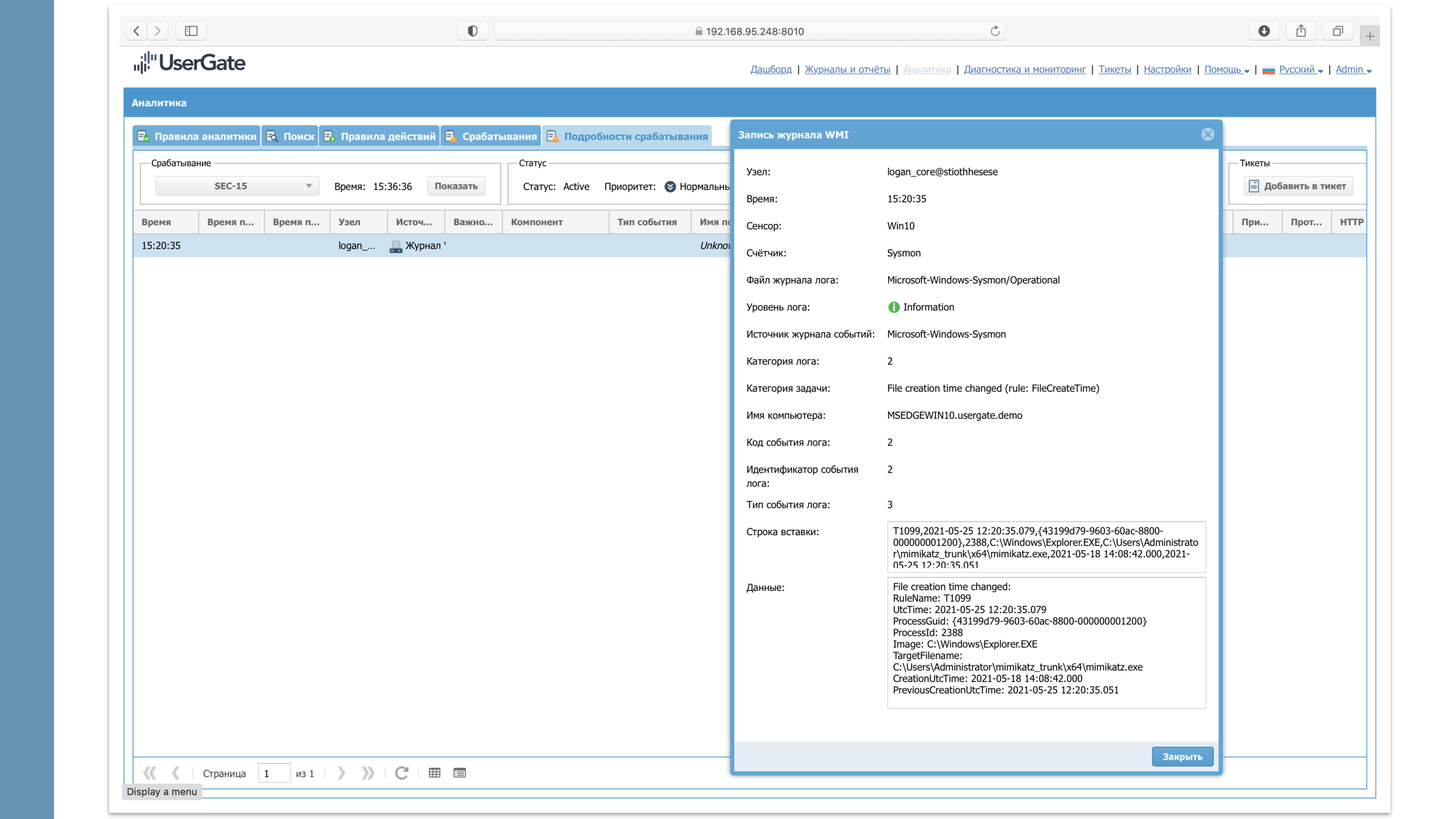


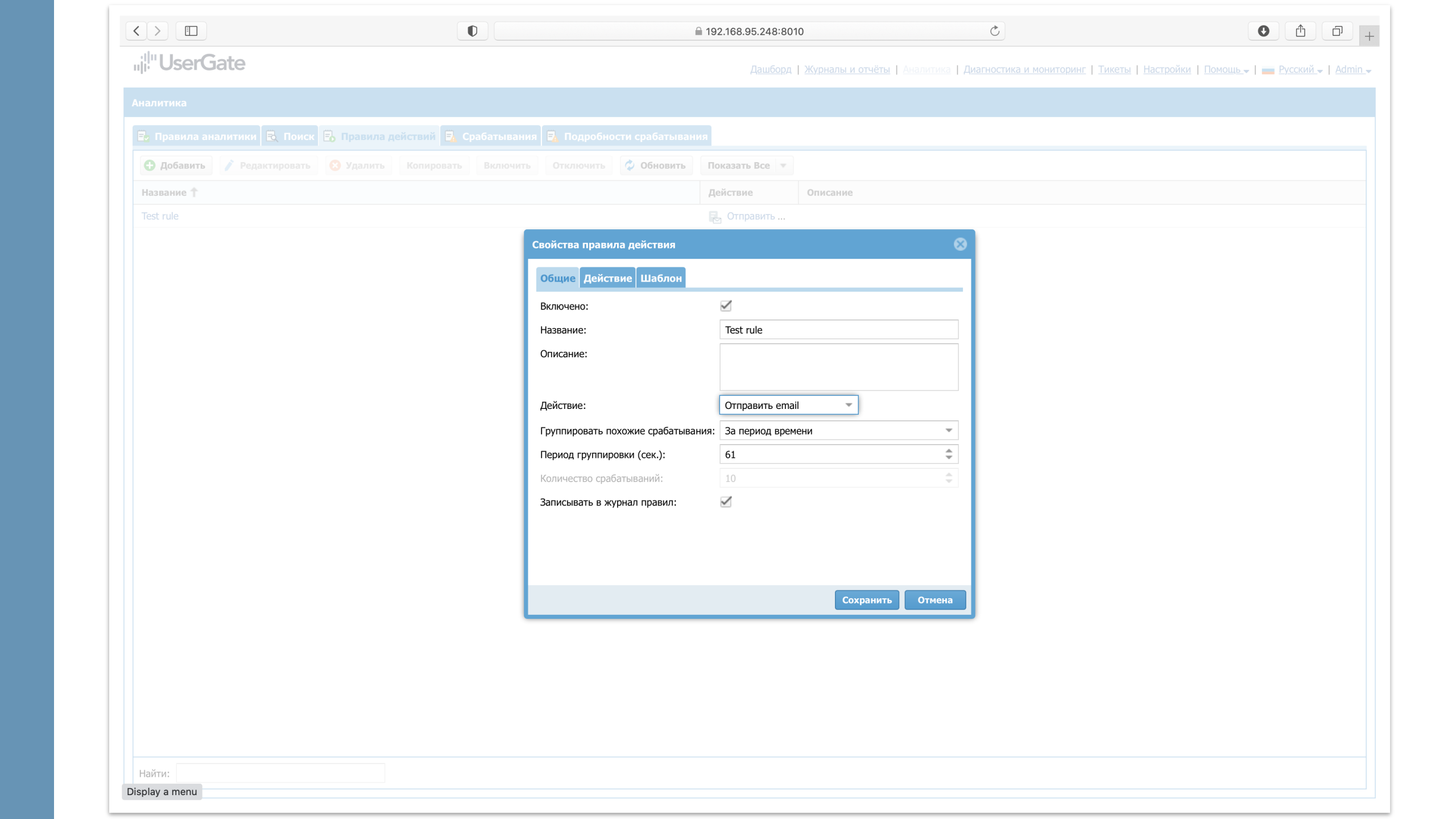
UserGate LogAnalyzer

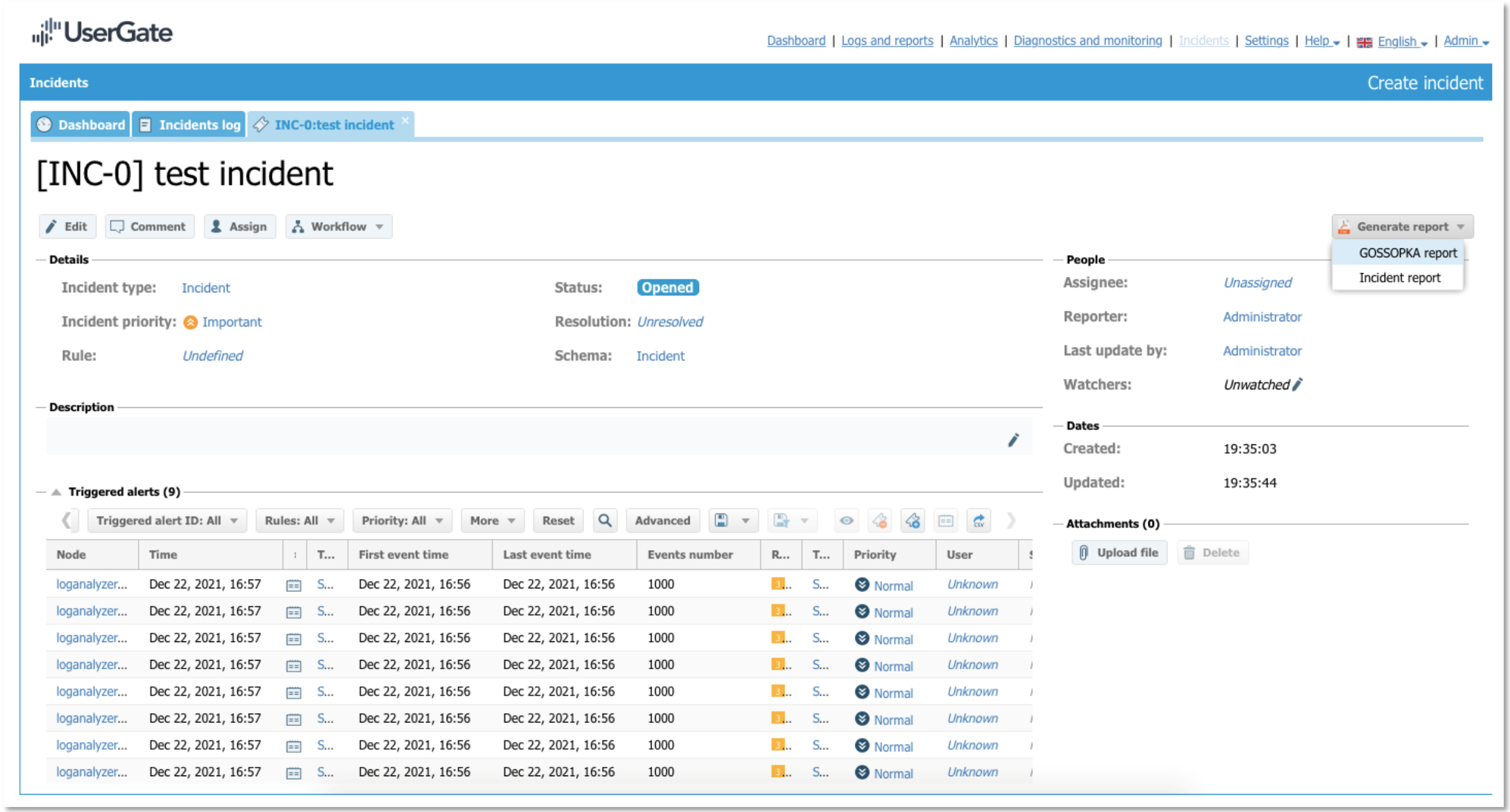

192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Запустить сейчас
Показать срабатывания
Показать Все
Обновить
Название
Приоритет
Категория
Условия
Действия
Download Mimikatz by Certutil.exe
Нормальный
Security
Start cmd
Download file
Mimikatz Use (credentials access)
Нормальный
Security
Mimikatz
Pastebin
Нормальный
Security
Pastebin
Possible RDP Brute Force
Нормальный
Security
An account fa...
Special privile...
An account w...
Свойства правила аналитики
Общие
Условия
Действия
Добавить
Редактировать
Удалить
Выше
Ниже
Название
Описание
Mimikatz
Запустить сейчас
Свойства условия правила аналитики
Название:
Mimikatz
Описание:
Ограничить время выполнения условия:
Время выполнения условия, (сек):
600
Запрос фильтра:
source = 'wmi log' AND (data ~ 'mimikatz' OR data ~ 'r
Группировать по:
action
address
application
applicationCategory
applicationTechnology
applicationThreat
bytesRecv
bytesSent
Повторений шаблона:
1
Сохранить
Отмена
Найти:
Display a menu



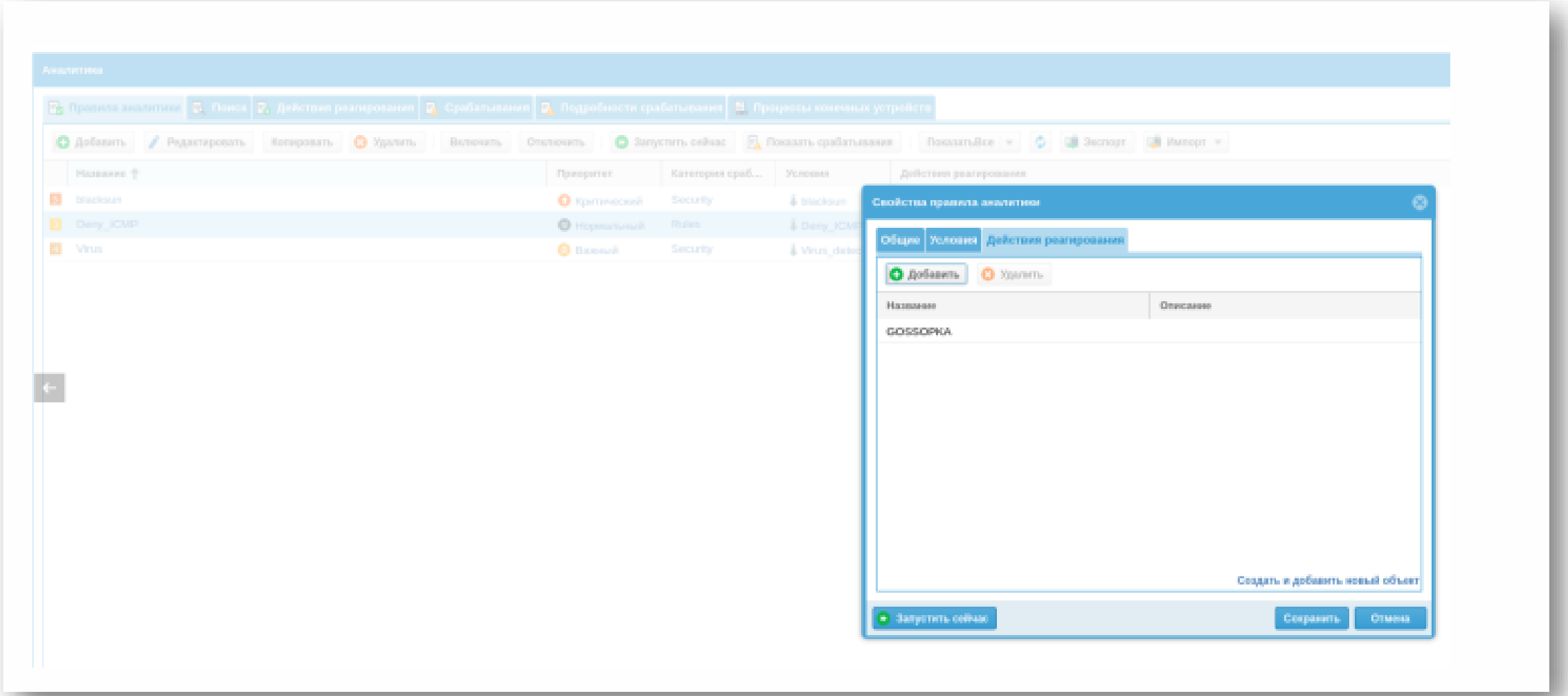
Узел	Время	ID	Время первого со...	Время последнего...	Правило	Категория	Статус	Приоритет	Админи...	Пользов...	Сигнатуры
loganalyzer@ugutm	15:36:58	SEC-20	15:16:19	15:19:48	Download Mimikatz by Certutil.exe	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-19	15:24:35	15:24:35	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-18	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-17	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-16	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-15	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-14	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-13	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-12	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-11	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-10	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-9	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-8	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-7	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-6	15:19:48	15:19:48	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-5	15:05:51	15:16:09	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-4	15:05:43	15:06:07	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-3	15:05:35	15:06:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-2	15:05:19	15:06:05	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-1	15:00:45	15:02:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет


192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Срабатывание
SEC-15
Время: 15:36:36
Показать
Статус
Статус: Active
Приоритет: Нормальны
Тикеты
Добавить в тикет
Время
Время п...
Время п...
Узел
Источ...
Важно...
Компонент
Тип события
Имя по
При...
Прот...
HTTP
15:20:35
logan_...
Журнал '
Unknou
Страница 1 из 1
Display a menu
Запись журнала WMI
Узел: logan_core@stiothhesese
Время: 15:20:35
Сенсор: Win10
Счётчик: Sysmon
Файл журнала лога: Microsoft-Windows-Sysmon/Operational
Уровень лога: Information
Источник журнала событий: Microsoft-Windows-Sysmon
Категория лога: 2
Категория задачи: File creation time changed (rule: FileCreateTime)
Имя компьютера: MSEDGEWIN10.usergate.demo
Код события лога: 2
Идентификатор события лога: 2
Тип события лога: 3
Строка вставки: T1099,2021-05-25 12:20:35.079,{43199d79-9603-60ac-8800-000000001200},2388,C:\Windows\Explorer.EXE,C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe,2021-05-18 14:08:42.000,2021-05-25 12:20:35.051
Данные: File creation time changed:
RuleName: T1099
UtcTime: 2021-05-25 12:20:35.079
ProcessGuid: {43199d79-9603-60ac-8800-000000001200}
ProcessId: 2388
Image: C:\Windows\Explorer.EXE
TargetFilename:
C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe
CreationUtcTime: 2021-05-18 14:08:42.000
PreviousCreationUtcTime: 2021-05-25 12:20:35.051
Закрыть


192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Обновить
Показать Все
Название
Действие
Описание
Test rule
Отправить ...
Свойства правила действия
Общие
Действие
Шаблон
Включено:
Название:
Test rule
Описание:
Действие:
Отправить email
Группировать похожие срабатывания:
За период времени
Период группировки (сек.):
61
Количество срабатываний:
10
Записывать в журнал правил:
Сохранить
Отмена
Найти:
Display a menu


UserGate
Dashboard | Logs and reports | Analytics | Diagnostics and monitoring | Incidents | Settings | Help | English | Admin
Incidents
Create incident
Dashboard
Incidents log
INC-0:test incident
[INC-0] test incident
Edit
Comment
Assign
Workflow
Generate report
GOSSOPKA report
Incident report
Details
Incident type: Incident
Incident priority: Important
Rule: Undefined
Status: Opened
Resolution: Unresolved
Schema: Incident
People
Assignee: Unassigned
Reporter: Administrator
Last update by: Administrator
Watchers: Unwatched
Description
Dates
Created: 19:35:03
Updated: 19:35:44
Triggered alerts (9)
Triggered alert ID: All
Rules: All
Priority: All
More
Reset
Advanced
Attachments (0)
Upload file
Delete
Node
Time
First event time
Last event time
Events number
Priority
User
loganalyzer...
Dec 22, 2021, 16:57
Dec 22, 2021, 16:56
1000
Normal
Unknown

Интеграция с ГосСОПКА



Центр реагирования и мониторинга

UserGate MRC

Контроль приложений

1000+ уникальных сигнатур для детектирования различных программных продуктов по 20 категориям

Обнаружение и предотвращение вторжений

Более 10000 сигнатур, направленных на детектирование современных атак

Корреляции и аналитика

Анализ журналов событий различных систем для детектирования цепочек комплексных атак

Защита веб-приложений

Списки контентной фильтрации, 10M+ доменов в базе URLF по 87 категориям, правила WAF

Отчеты об угрозах

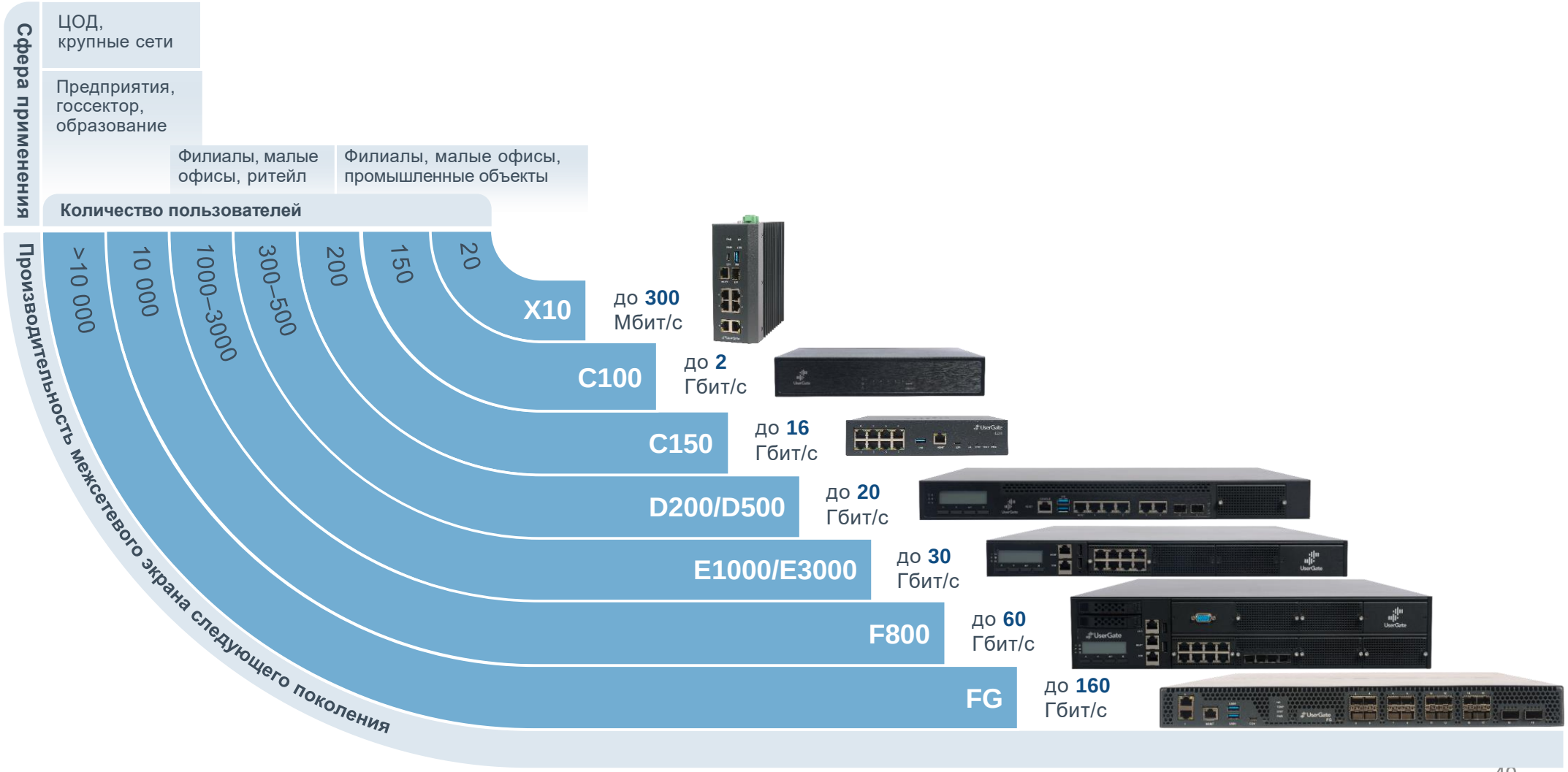
Информирование пользователей о резонансных угрозах, способах их обнаружения и предотвращения.

Индикаторы компрометации

IP-адреса ботнет-сетей, домены и IP-адреса C&C серверов, фишинговые сайты, хэши вредоносного ПО

UserGate NGFW

Модельный ряд аппаратных платформ



UserGate SUMMA

соответствие требованиям Законодательства РФ

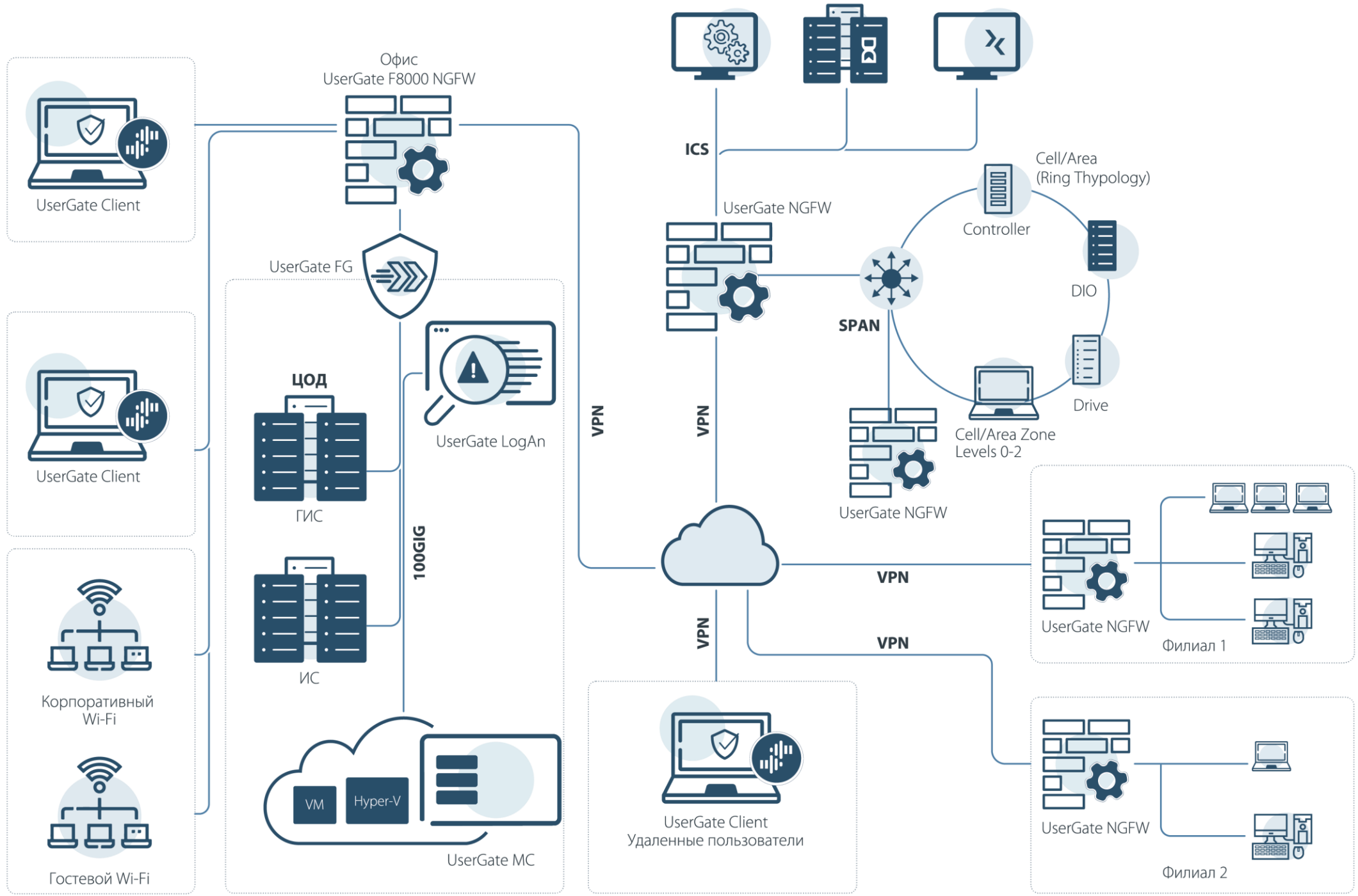
UserGate первым на отечественном рынке ИБ получил **четыре из пяти профилей** защиты в рамках одного сертификата ФСТЭК России № 3905.

- **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:

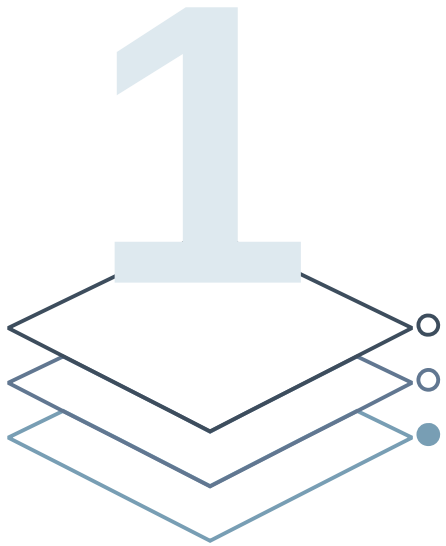
- классы защиты СЗИ 4
- ЗО КИИ 1 категории
- ГИС 1 класса
- АСУ ТП 1 класса
- ИСПДн 1 уровня
- ИСОП II класса


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

NGFW vs UTM

1 уровень

«Для тех, кто вообще ничего не умеет»

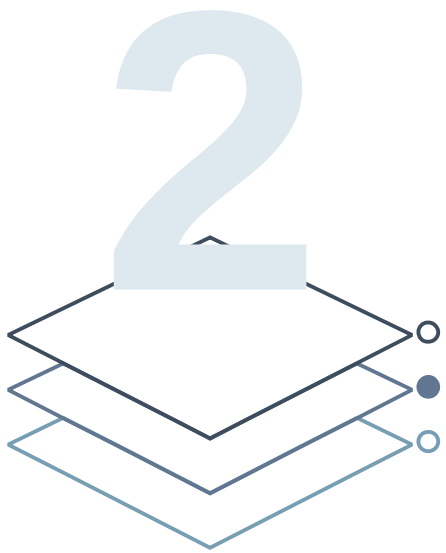


Готовые продукты:

- pfSense
- OPNSense
- M0n0wall
- IPCop
- …

2 уровень

«Для тех, кто сам научился собирать образы»

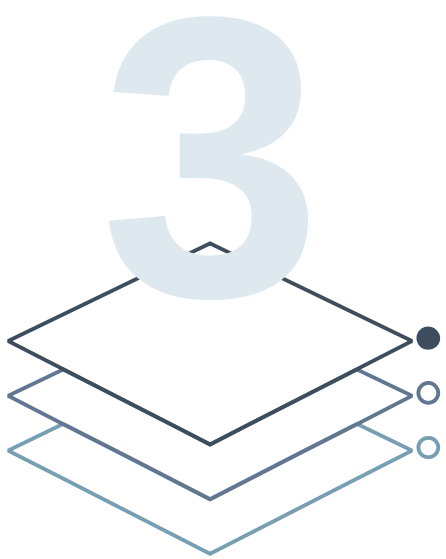


Готовые продукты:

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

3 уровень

«Для профессионалов»

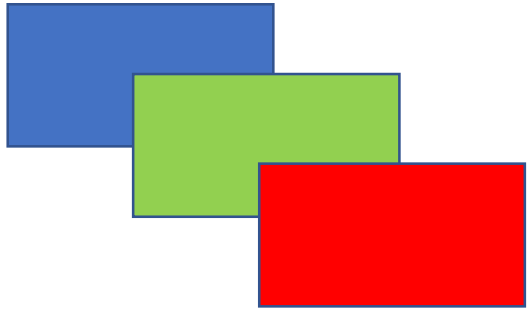


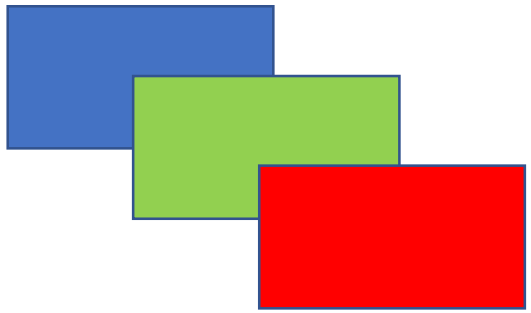
Низкоуровневые библиотеки:

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

	Чужие платформы	Свои платформы
Проприетарное ПО		CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	CHECK POINT	CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	CHECK POINT	CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	UserGate CHECK POINT	UserGate CISCO HUAWEI paloalto NETWORKS FORTINET
Open-source		

Нас выбирают

































UserGate

Спасибо за внимание!

Евгений Митюшкин

Ведущий менеджер
по работе с клиентами

emitiushkin@usergate.ru

+7 (916) 411-50-39