

Практика импортозамещения в обеспечении сетевой безопасности критически важных объектов

Алексей Долгих

Руководитель отдела продаж

sales@usergate.ru

8 800 500 40 32 | +7 (983)129-12-84



Здравоохранение



Банки
и финансовые
организации



Горнодобывающая
промышленность



Наука



Энергетика
и топливно-
энергетический
комплекс



Транспорт



Металлургическая
промышленность



Сфера атомной
энергии



Химическая
промышленность



Связь



Ракетно-
космическая
промышленность



Оборонная
промышленность

Требования регуляторов

СИСТЕМЫ БЕЗОПАСНОСТИ ДОЛЖНЫ ОБЕСПЕЧИВАТЬ

Предотвращение неправомерного доступа к информации, обрабатываемой ЗОКИИ;

Восстановление функционирования ЗОКИИ, в том числе за счет создания и хранения резервных копий необходимой для этого информации;

Непрерывное взаимодействие с ГосСОПКА на информационные ресурсы РФ, которое осуществляется в соответствии со статьей 5 ФЗ «О безопасности КИИ РФ».

Для обеспечения безопасности **ЗОКИИ** должны применяться **сертифицированные** на соответствие требованиям по безопасности **средства защиты информации** или средства, прошедшие оценку соответствия в форме испытаний или приемки (в обязательном порядке должны пройти проверку на 6-й уровень доверия согласно 76-му приказу ФСТЭК России от 02.06.2020 г.) в соответствии с № 184-ФЗ «О техническом регулировании»

ПРИКАЗ №196 ФСБ РФ от 6 мая 2019 г.

«Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» общие требования к средствам защиты основываются на следующих пунктах: ...

3.3. Возможность осуществления модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

3.4. Обеспечение гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

Приказ ФСТЭК России от 28.05.2020 № 75

«Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования. Вступает в силу 26 сентября 20 г.

В соответствии с Требованиями по обеспечению безопасности ЗОКИИ Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239..., достаточным для обеспечения безопасности значимого объекта при его подключении к сети связи общего пользования является применение следующих средств защиты информации, прошедших оценку на соответствие требованиям по безопасности в форме обязательной сертификации, испытаний или приемки

СЗИ\КЗ	3 КЗ	2 КЗ	1 КЗ
Программно-аппаратный граничный маршрутизатор	✓	✓	✓
Выделенные физические интерфейсы для каждого сервиса		✓	✓
МЭ тип "А" на границе с ССОП (Интернет)	✓	✓	✓
Средство обнаружения (предотвращения) вторжений		✓	✓

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

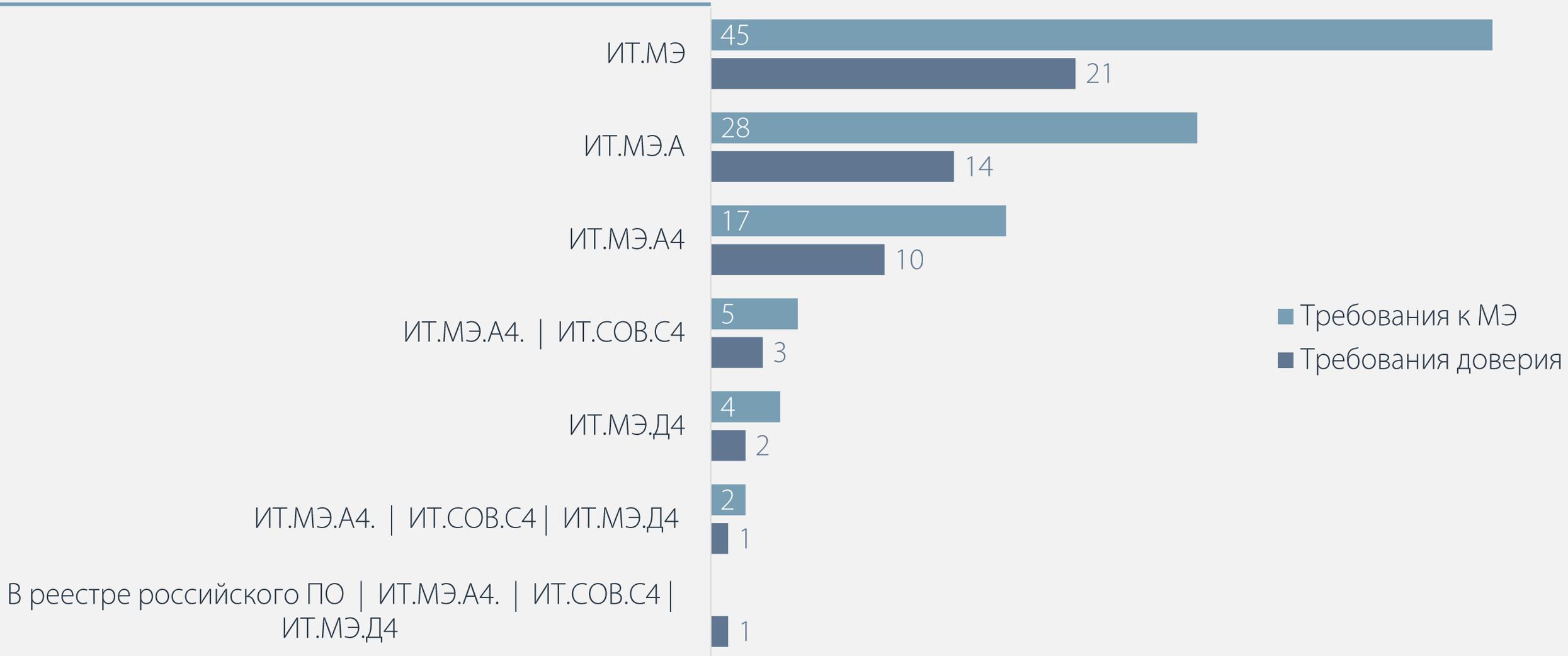
МЭ типа «Г»

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)

Сертификатов, выданных на серию в реестре ФСТЭК России*:

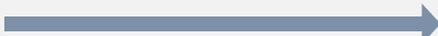


Соотношение сертификатов ФСТЭК России выданных на серию, с профилем защиты ИТ.МЭ.А4





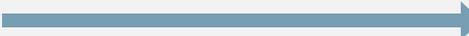
Всем производителям СЗИ необходимо было пройти процедуру подтверждения соответствия требованиям к УД до 01.01.2021



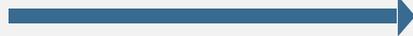
2021 г.
Требования доверия в 31 Приказе ФСТЭК России

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

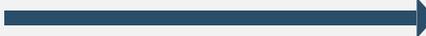
В автоматизированных системах управления 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия.



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



Межсетевой экран
NGFW



Система обнаружения
и предотвращения
вторжений



Безопасная
публикация
ресурсов
и сервисов



Анализ команд в
протоколах АСУ ТП





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.



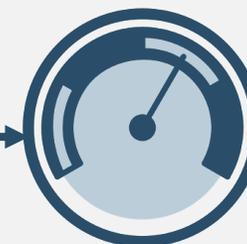




UserGate



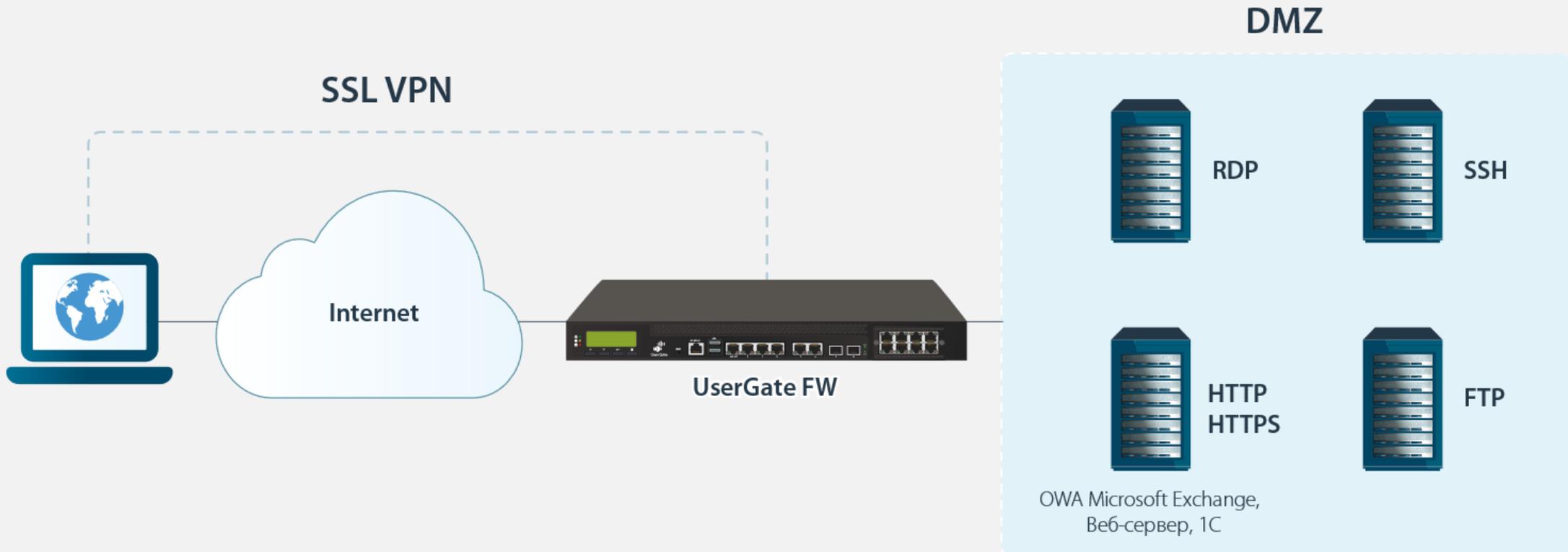
CLIENT



SERVER



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

Портал авторизации пользователей

Выберите домен:
esafeline.com

Имя:
demo-ар

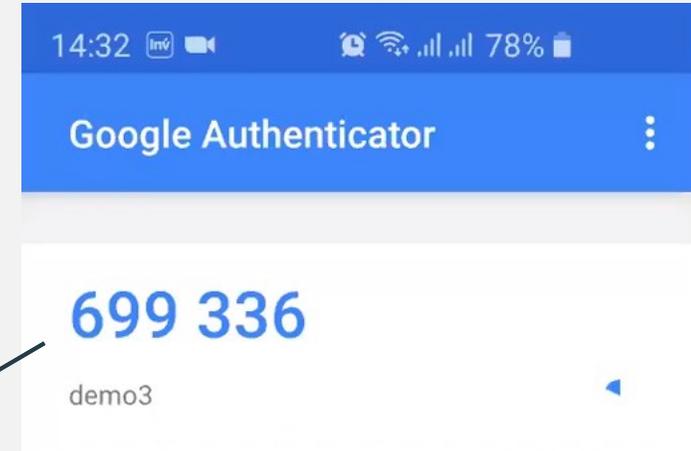
Пароль:

Введите текст с картинки:
 

437865

One Time Password:

Войти





СОВ - Система обнаружения и предотвращения вторжений

Сигнатуры IPS для протоколов АСУ ТП.

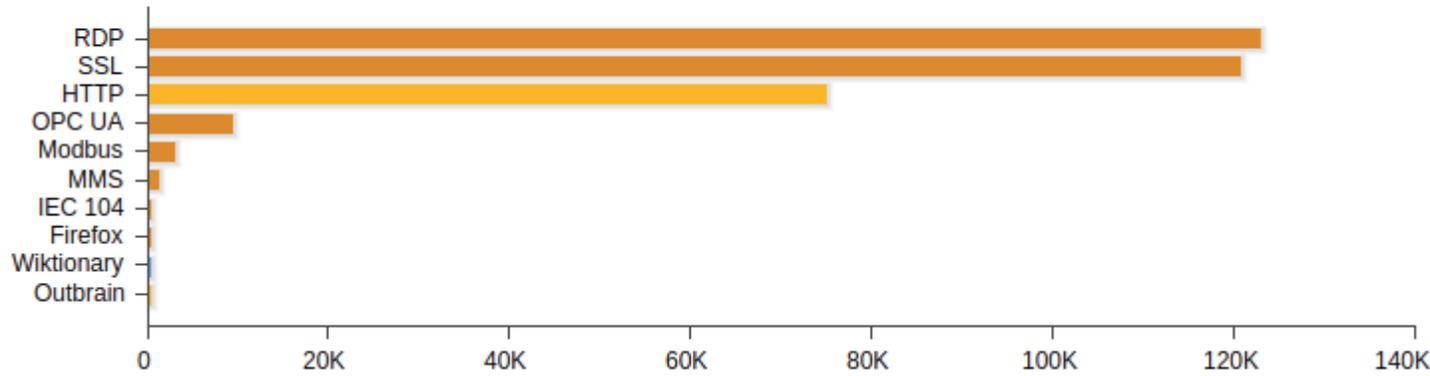
Защита систем, которое невозможно пропатчить (виртуальный патчинг)

Category: scada x						
	Signature	OS	Prot...	Class type	References	Category
5	Measuresoft ScadaPro Remote Command Executi...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2011-3497	scada
5	CitectSCADA/CitectFacilities ODBC Server Remot...	Other	tcp	targeted-activity	None	scada
5	Advantech WebAccess Dashboard Viewer uploadl...	Other	tcp	targeted-activity	None	scada
5	Advantech WebAccess Multiple Remote Code Exe...	Other	tcp	targeted-activity	None	scada
5	DATAc RealWin SCADA Server Remote Stack Buf...	Other	tcp	targeted-activity	None	scada
5	SCADA 3S CoDeSys Gateway Server Directory Tr...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2012-4705	scada
5	Scadatec Procyon Telnet Service Remote Buffer O...	Other	tcp	targeted-activity	None	scada
5	Multiple Schneider Electric Products Stack Based ...	Other	tcp	targeted-activity	None	scada
5	AzeoTech DAQFactory NETB Datagram Parsing B...	None	tcp	targeted-activity	None	scada
5	CoDeSys Gateway Server CVE-2012-4705 Directo...	Other	tcp	targeted-activity	None	scada
5	7T Interactive Graphical SCADA System Multiple ...	Other	tcp	targeted-activity	None	scada
5	ABB MicroSCADA wserver.exe CreateProcessA() ...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	None	scada
5	ICONICS WebHMI ActiveX Control Stack Buffer O...	None	tcp	targeted-activity	None	scada
5	Interactive Graphical SCADA System Remote Co...	Other	tcp	targeted-activity	None	scada
5	Siemens SIMATIC WinCC Default Password Secu...	Other	tcp	default-login-att...	CVE: 2010-2772	scada



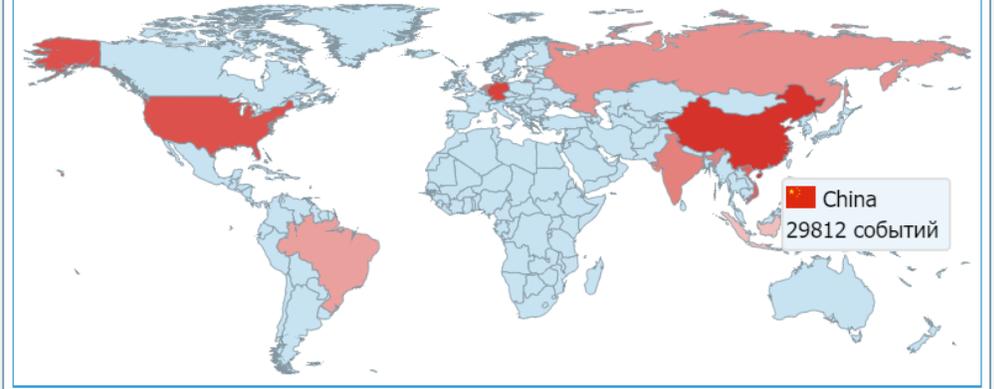
Top 10 applications

Year | Month | Week | Day | Now | Refresh | Settings | Close



Top 10 attack source countries

Год | Месяц | Неделя | День | Сейчас | Refresh | Settings | Close



Detected attacks by threat level

Год | Месяц | Неделя | День | Сейчас | Refresh | Settings | Close

0%
9
2 низкий

79%
6494
4 высокий

21%
1727
5 очень высокий

Last 10 attacks

Год | Месяц | Неделя | День | Сейчас | Refresh | Settings | Close

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



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

iec 104 | modbus | dnp3

Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий.

Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

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.



iec 104 | modbus | dnp3

Создаем профиль для протокола Modbus

Свойства АСУ ТП

Название:

Описание:

+ Добавить ✎ Редактировать ✖ Удалить

Протокол	Команда АСУ ТП	Адрес АСУ ТП
Modbus	Write Single Holding Register (6)	2560

Сохранить Отмена



iec 104 | modbus | dnp3

Создаем правило АСУ ТП и указываем профиль

Правила АСУ ТП							
+ Добавить ✎ Редактировать ✖ Удалить ↔ Переместить 📄 Копировать 🔍 Включить 🔍 Отключить 🔄 Обновить Показать Все ▾							
#	Название	Действие	Исходная ...	Адрес источника	Сервис	Назначение	Профили АСУ ТП
1	2.8 Block register	🛑 Блокировать	Любая	Любой	Modbus	Любой	2.8 Modbus block register
2	2.6 Block write	🛑 Блокировать	Любая	Любой	Modbus	Любой	Modbus 2.6
3	IEC104 type 45	▶ Пропускать	DMZ Trusted	Любой	SCADA	Любой	ASDU type 45
4	Modbus	▶ Пропускать	DMZ Trusted	Любой	Modbus	Любой	Modbus all



iec 104 | modbus | dnp3

Результат работы правила фиксируется в журнале

Журнал АСУ ТП

02 Дек 2019 г.	Действие: Блокировать	Правила: All	Ещё	Расширенный	Сохранить как	Популярные фильтры	
Время	⌘	Правило	Зона источ...	Порт назн...	Протокол	Команда АСУ ТП	Адрес АСУ ТП
08:45:04	⊖	2.8 Block register	DMZ	502	Modbus	Write Single Holding Register (6)	2560

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

1

~~Получения профиля защиты
МЭ (Д четвертого класса
защиты. ИТ.МЭ.Д4.ПЗ)~~

~~До конца 2020 г.~~

2

~~Продление действующего
сертификата
на 5 летний срок~~

~~До конца 2020 г.~~

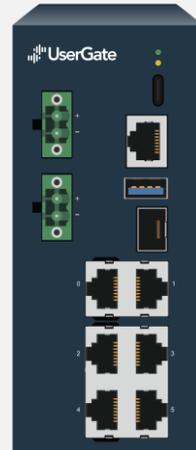
3

Сертификация во ФСТЭК
России аппаратных
платформ собственной
разработки и включение их в
единый реестр российской
радиоэлектронной
продукции

3 квартал 2021 г.

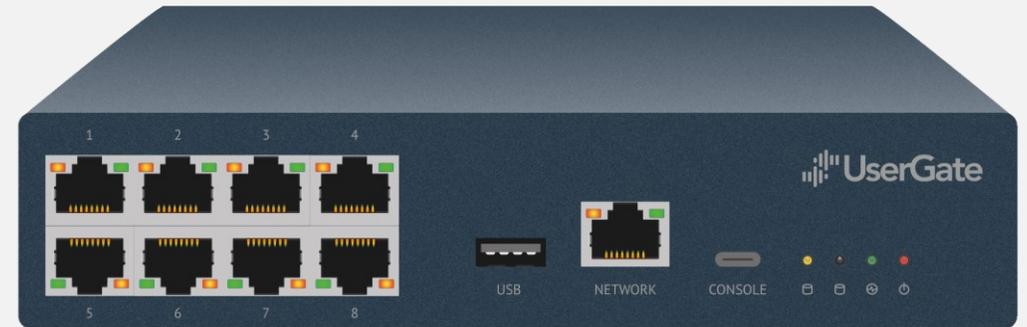
Собственные аппаратные платформы

Модель X1



- МЭ до 2,5 Гб/с
- ARM 4 cores
- 6 портов 1GbE с поддержкой bypass
- 1 порт SFP
- Два блока питания
- От -40 до + 70 °С
- Крепление на DIN рейку

Модель C100



- МЭ до 2,5 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- Два блока питания
- От 0 до +70 °С



ПРАВИТЕЛЬСТВО
МОСКВЫ



ПЕНСИОННЫЙ ФОНД
РОССИЙСКОЙ ФЕДЕРАЦИИ



lady & gentleman
CITY



МИНФИН
РОССИИ



Спасибо за внимание

Алексей Долгих

Руководитель отдела продаж

sales@usergate.ru

8 800 500 40 32 | +7 (983)129-12-84

