Практика импортозамещения в обеспечении сетевой безопасности критически важных объектов

Алексей Долгих
ведущий менеджер
по работе с корпоративными клиентами

AD@usergate.ru
8 800 500 40 32 | +7 (983)129-12-84

17.09.2020 г.

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

UserGate

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 131-му приказу ФСТЭК России) в соответствии с № 184-ФЗ «О техническом регулировании»

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 131-му приказу ФСТЭК России) 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		✓	✓

UserGate

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

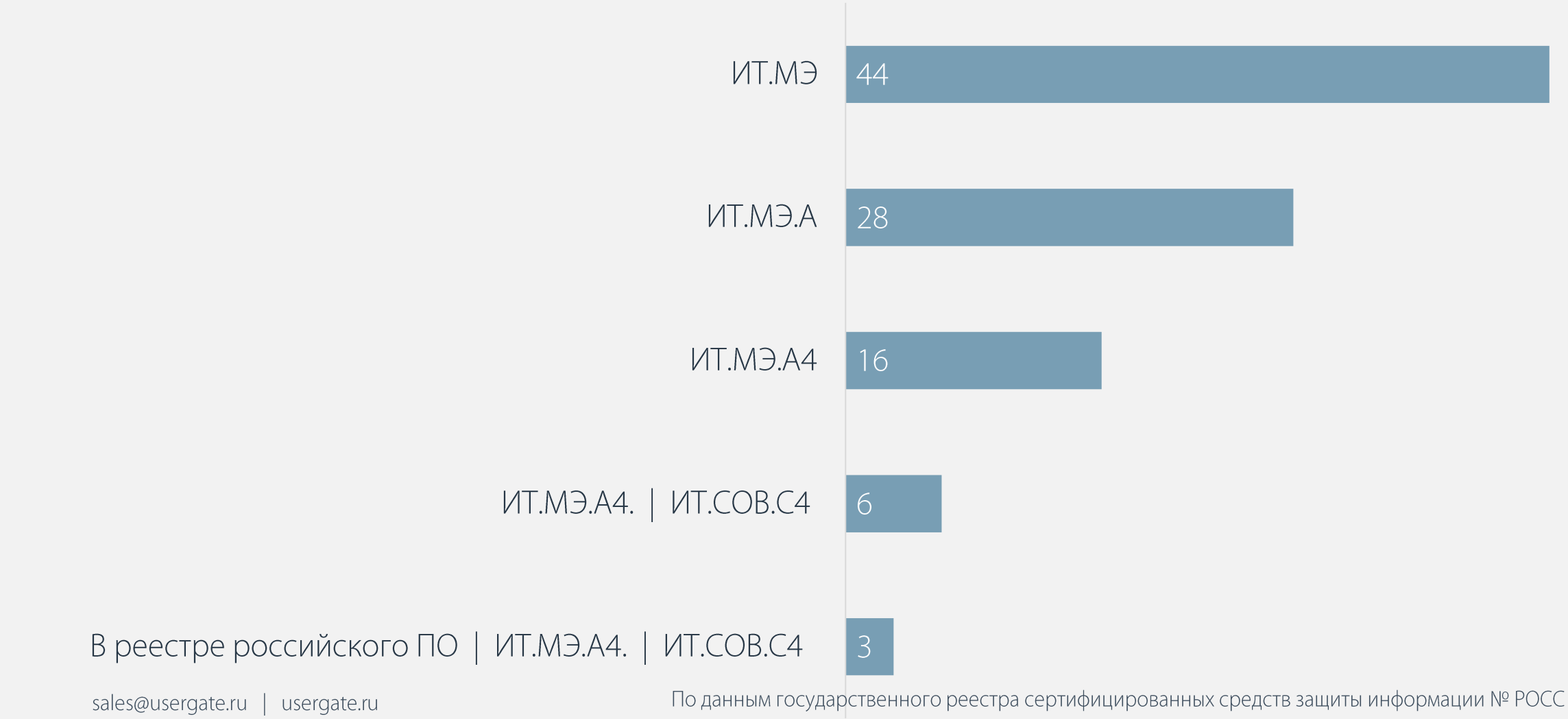
МЭ типа «Г»

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)

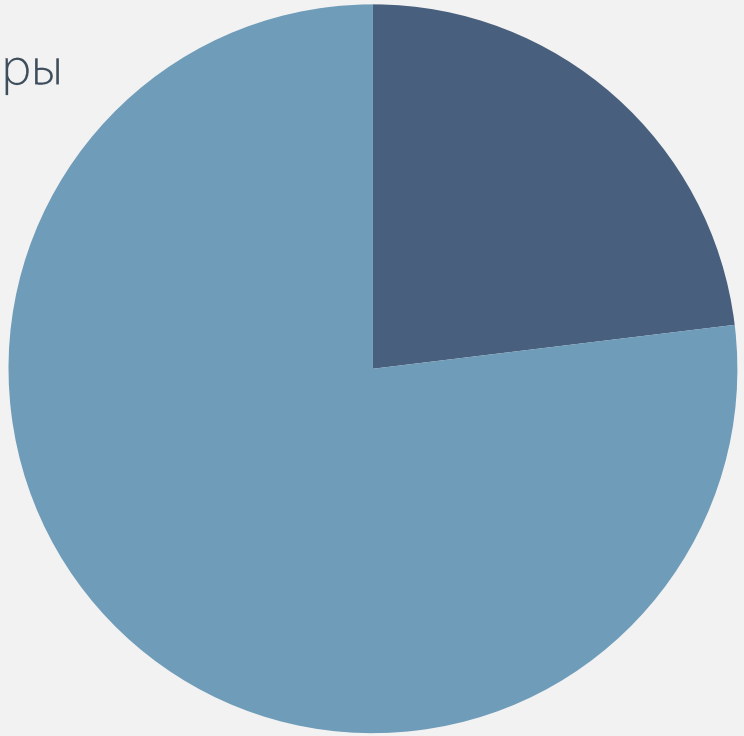
Сертификатов, выданных на серию в реестре ФСТЭК России*:



По данным государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 от 03.08.2020 сертификатов, выданных на серию в реестре ФСТЭК России:

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

Российские вендоры
13 сертификатов



Иностранные вендоры
3 сертификата

По данным государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 от 03.08.2020 сертификатов, выданных на серию в реестре ФСТЭК России:

Всем производителям СЗИ необходимо прохождение контроля по требованиям к УД до 1 января 2021 года

По новым требованиям к УД для УД5 и выше с 1 января 2022 года необходимо присутствие платформы в едином реестре российской радиоэлектронной продукции (Реестр)

Для УД5 и выше с 1 января 2028 года необходимо присутствие платформы в Реестре, а также используемых процессоров, микроконтроллеров и памяти

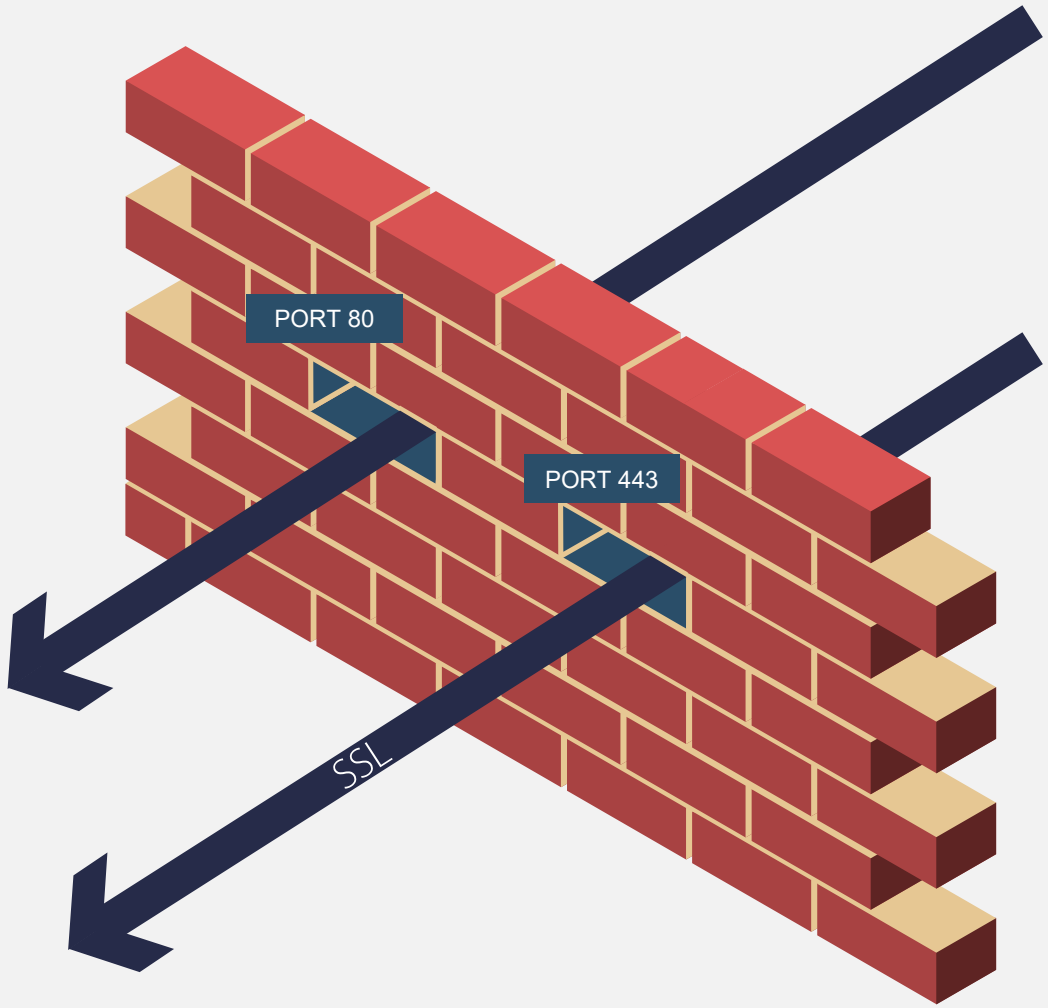
Межсетевой экран NGFW

Система обнаружения и предотвращения вторжений

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.
- Идентификация и контроль действий пользователей АСУ ТП (Операторов и Администраторов)
- Аналитика и отчетность


PORT 80
PORT 443
SSL


GW IP: UG
UserGate
CLIENT
Rule: NAT
INTERNET


UserGate
CLIENT
SERVER

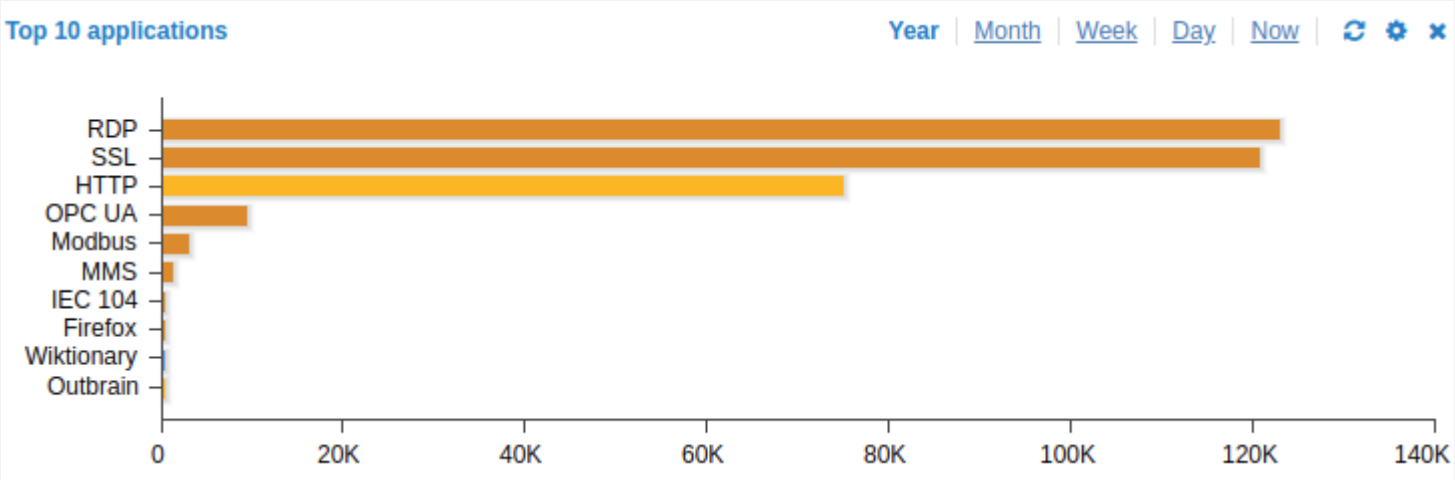
СОВ - Система обнаружения и предотвращения вторжений

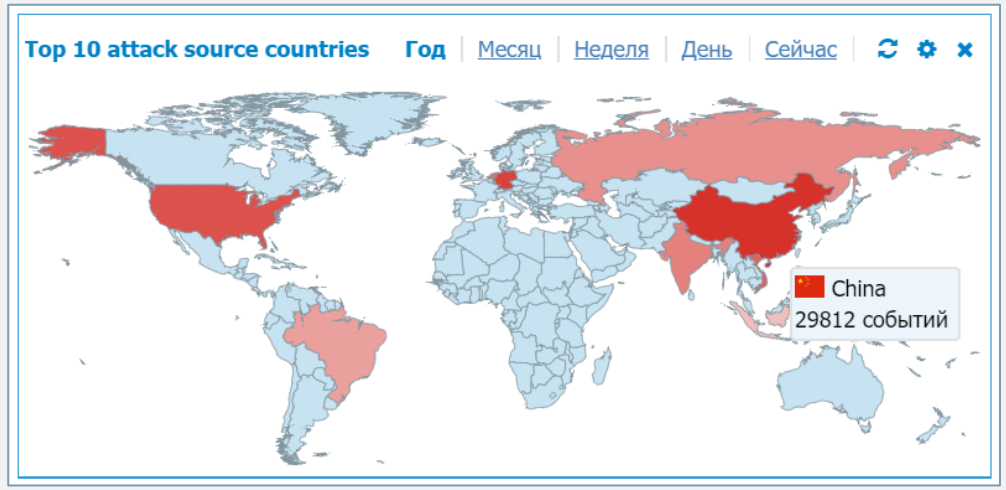
Сигнатуры IPS для протоколов АСУ ТП.

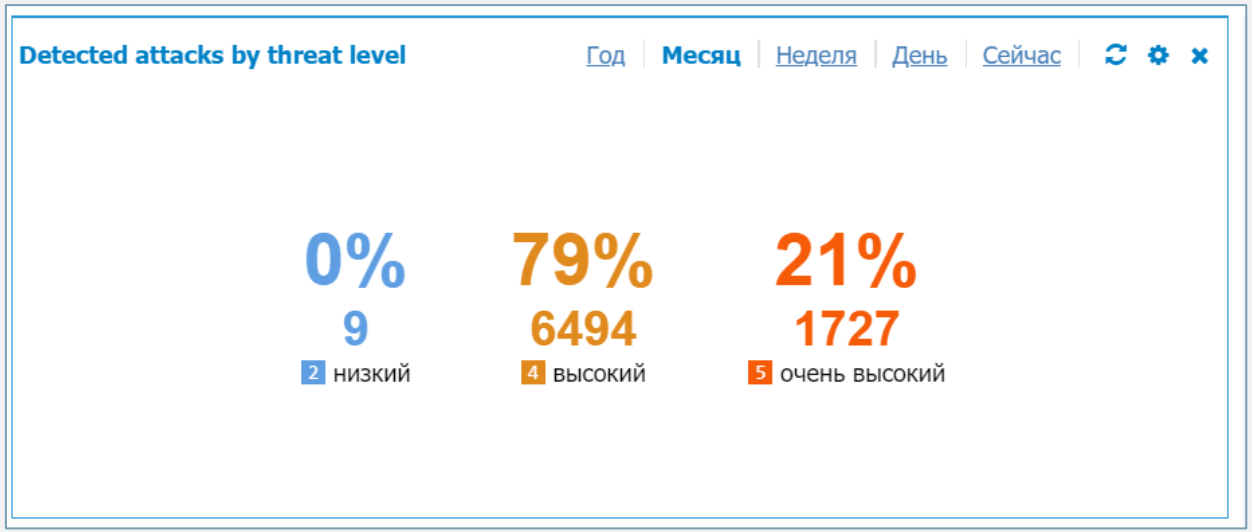
Category: scada ×

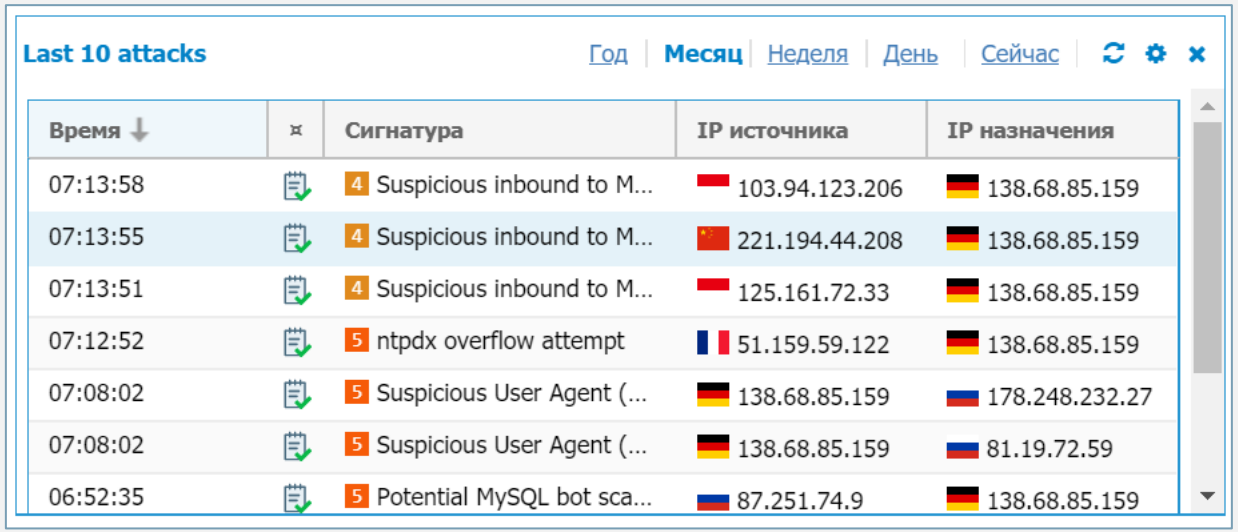
Signature	OS	Prot...	Class type	References	Category
Measuresoft ScadaPro Remote Command Executi...	BSD, Linux, Ma...	tcp	arbitrary-code-e...	CVE: 2011-3497	scada
CitectSCADA/CitectFacilities ODBC Server Remot...	Other	tcp	targeted-activity	*None*	scada
Advantech WebAccess Dashboard Viewer uploadI...	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


UserGate
PDF
STATISTICS
SPAN
PORT
CLIENT
R1


Top 10 applications
Year | Month | Week | Day | Now
RDP
SSL
HTTP
OPC UA
Modbus
MMS
IEC 104
Firefox
Wiktionary
Outbrain
0
20K
40K
60K
80K
100K
120K
140K


Top 10 attack source countries
Год | Месяц | Неделя | День | Сейчас
China
29812 событий


Detected attacks by threat level
Год | Месяц | Неделя | День | Сейчас
0%
9
2 низкий
79%
6494
4 высокий
21%
1727
5 очень высокий


Last 10 attacks
Год | Месяц | Неделя | День | Сейчас
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

iec 104 | modbus | dnp3

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

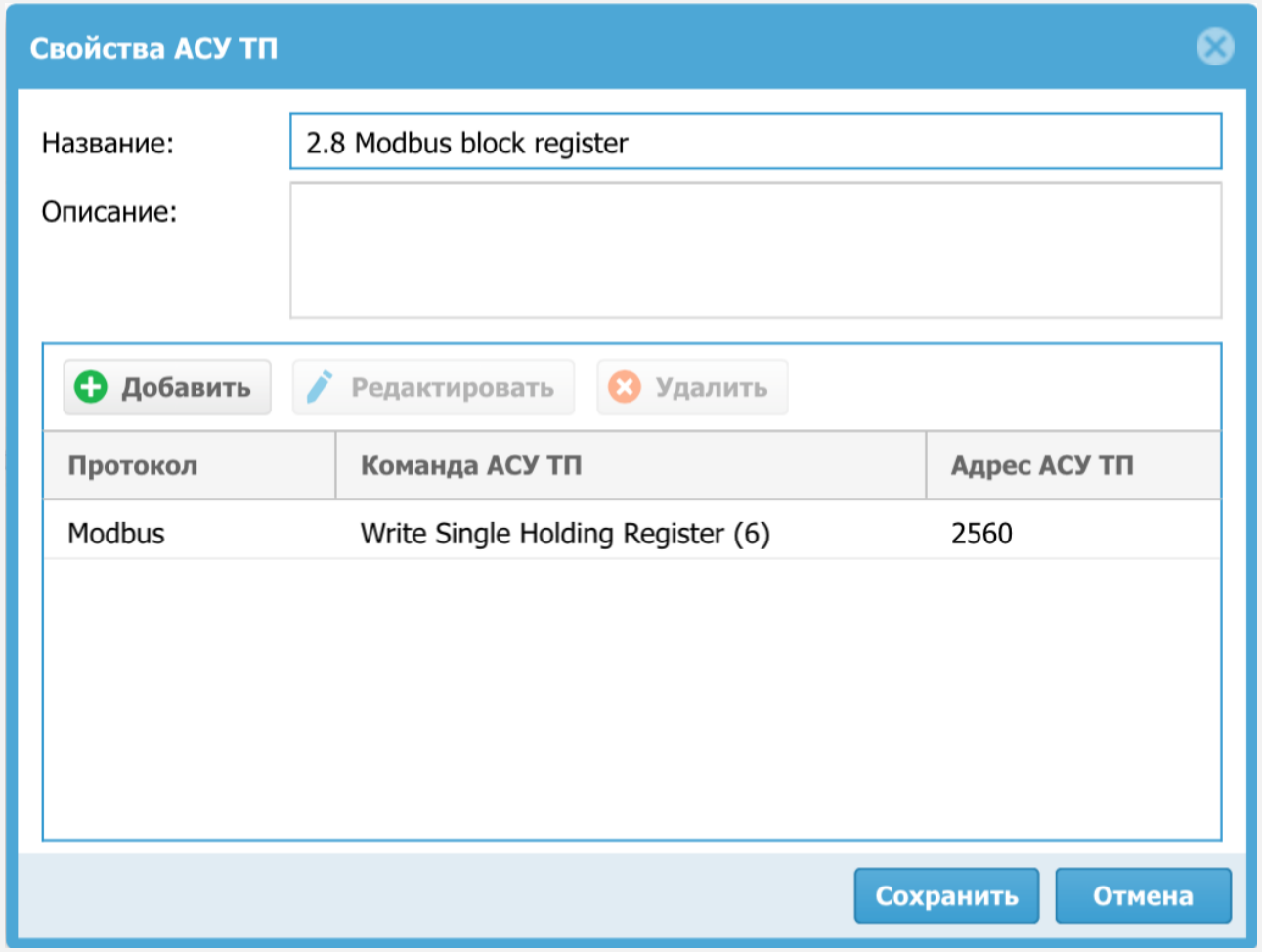
Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий.

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



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

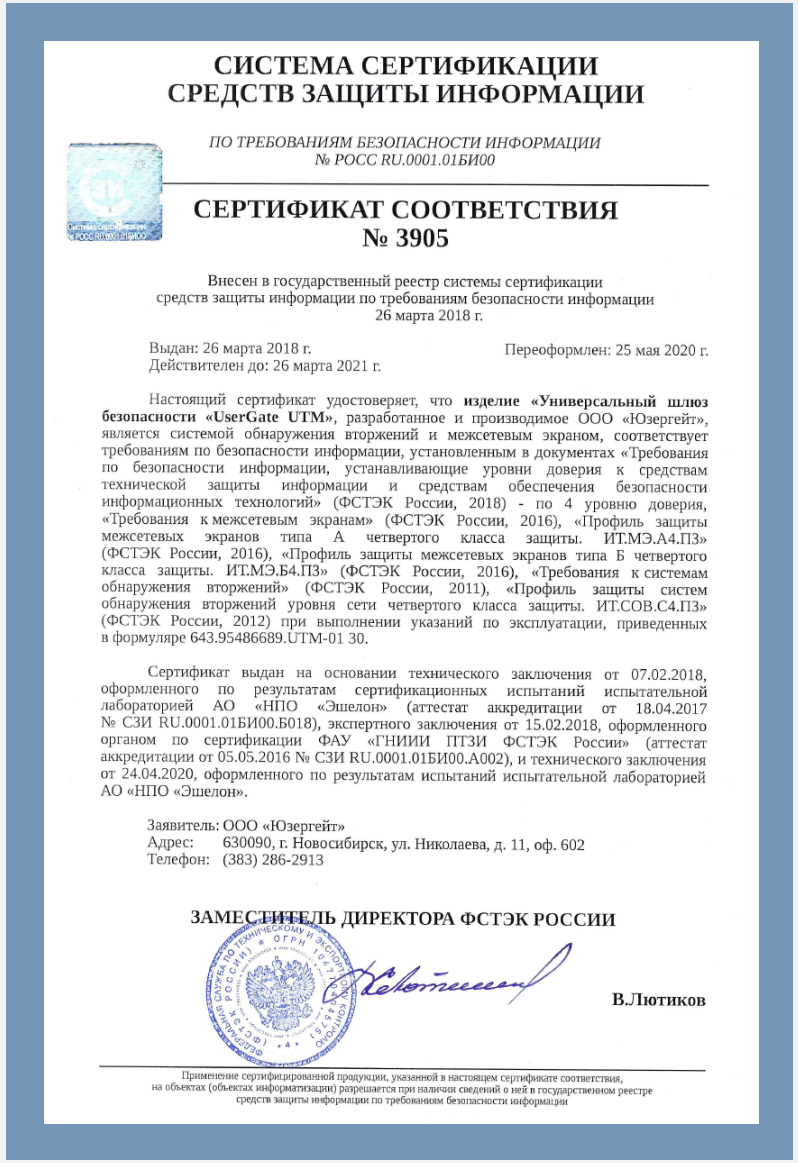
СЕРТИФИКАТ ФСТЭК России № 3905

Решение UserGate имеет действующий ФСТЭК России по 4 уровню доверия;

- Требования к МЭ «Профиль защиты МЭ типа А 4-го класса защиты», «Профиль защиты МЭ типа Б 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



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 26 марта 2018 г.

Выдан: 26 марта 2018 г. Переоформлен: 25 мая 2020 г.
Действителен до: 26 марта 2021 г.

Настоящий сертификат удостоверяет, что **изделие «Универсальный шлюз безопасности «UserGate UTM»**, разработанное и производимое ООО «Юзергейт», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 643.95486689.UTM-01 30.

Сертификат выдан на основании технического заключения от 07.02.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), экспертного заключения от 15.02.2018, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технического заключения от 24.04.2020, оформленного по результатам испытаний испытательной лабораторией АО «НПО «Эшелон».

Заявитель: ООО «Юзергейт»
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602
Телефон: (383) 286-2913

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

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.

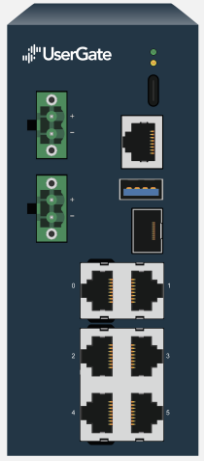
3

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

2 квартал 2021 г.

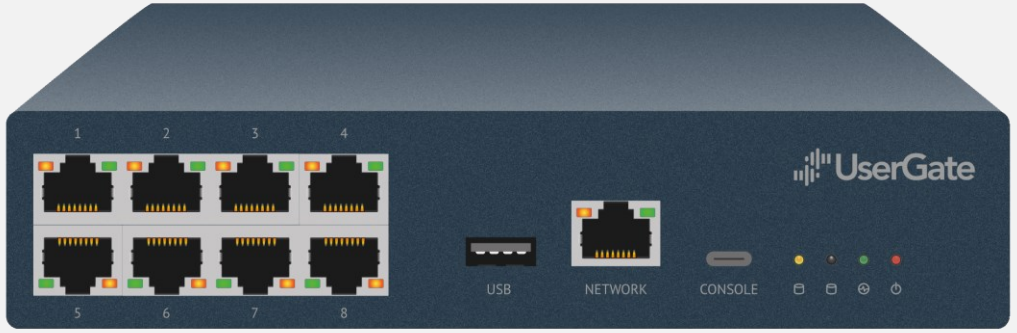
Собственные аппаратные платформы

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 °C
- 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 °C

UserGate

Спасибо за внимание

Алексей Долгих

ведущий менеджер
по работе с корпоративными клиентами

AD@usergate.ru
8 800 500 40 32 | +7 (983)129-12-84