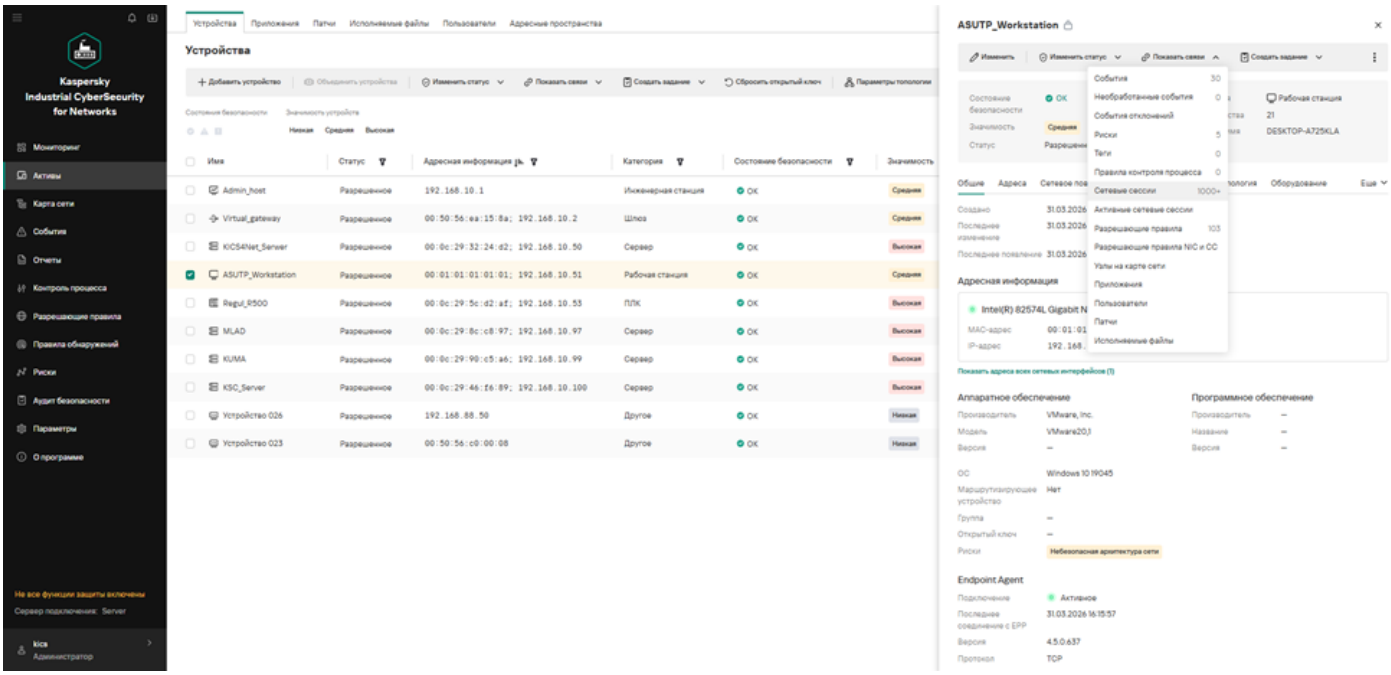
?????????? ?? ?????????? KICS for Networks ??? ????????????? ?????? ?????? ??????? ????????????????? ?????? ????? ???????????????? ???????? ????

Для формирования набора правил используется предварительно обученная система KICS for Networks. Качество обучения системы не имеет особого значения: важным условием является наличие в системе достаточного количества записей о сетевых сессиях. Идеальный вариант — наличие в системе данных о максимальном количестве сетевых сессий узлов защищаемого сегмента сети.

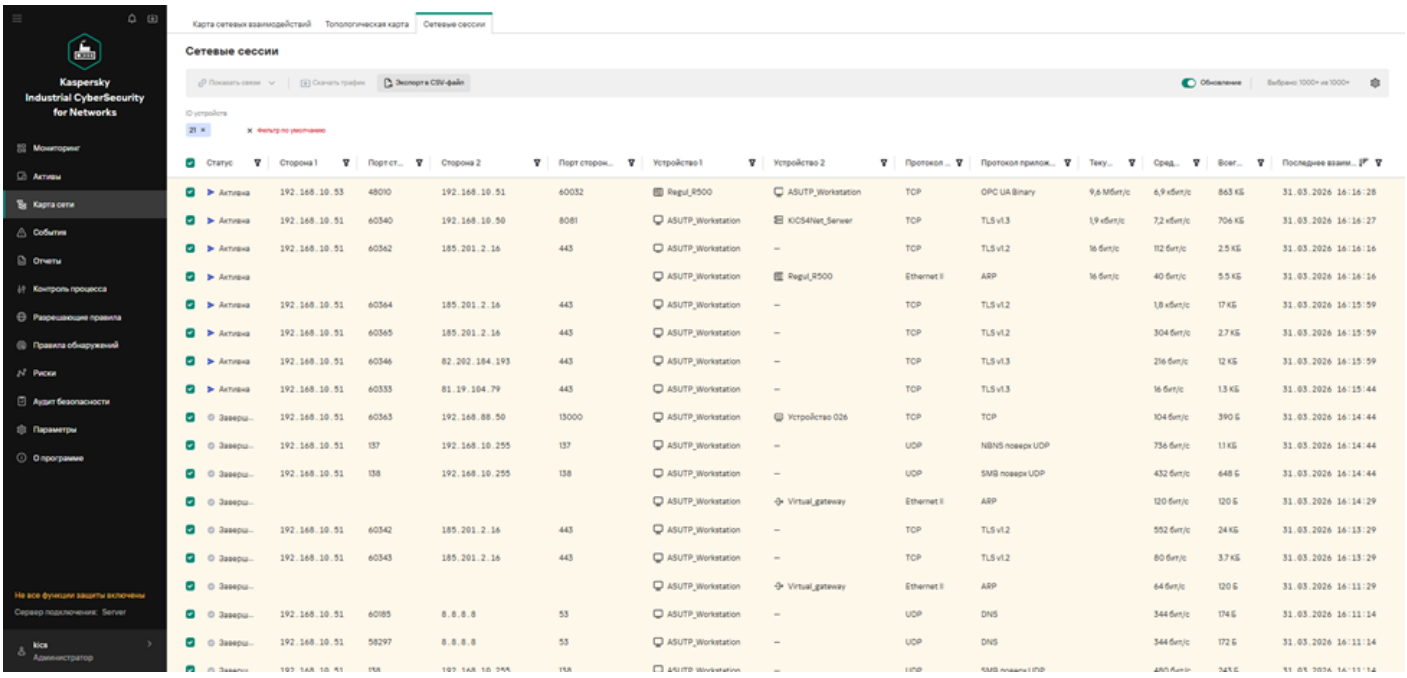
1. ??????????? ??????? ??????? ??????

На первом этапе необходимо сформировать перечень всех сетевых сессий (активных и завершённых) для конкретного защищаемого узла. Для этого в карточке актива следует перейти к выборке необходимых сетевых сессий, используя кнопку «Показать связи» → «Сетевые сессии».



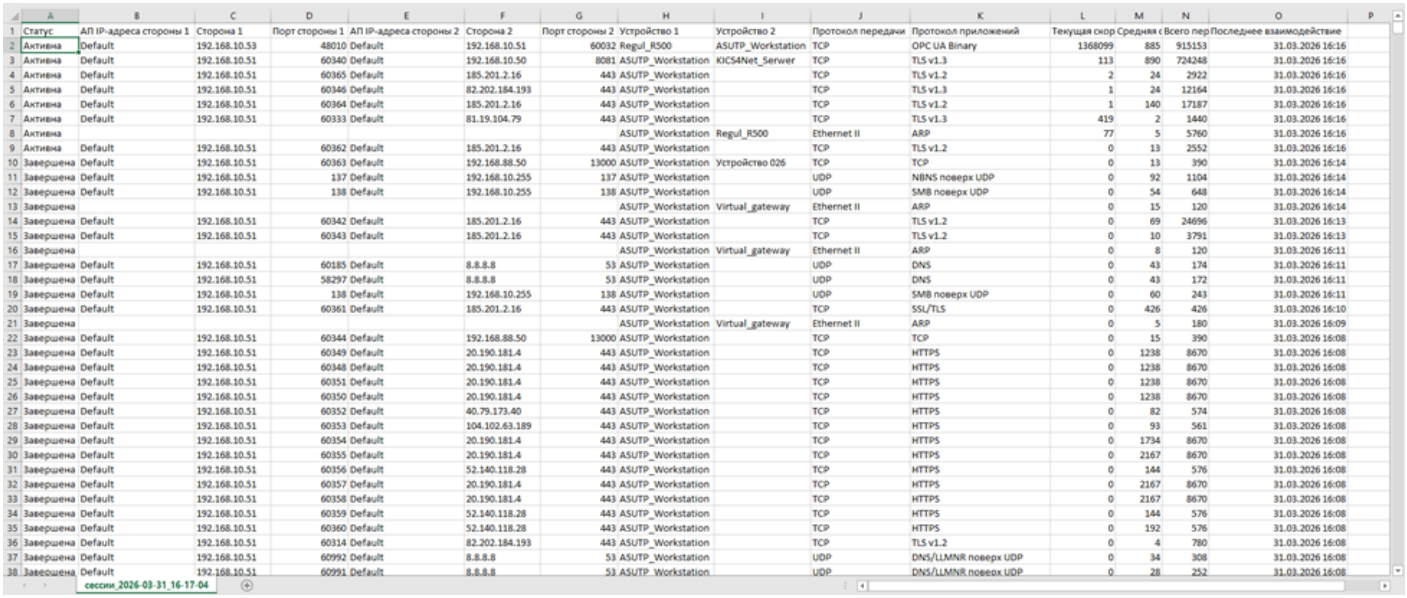
2. ??????? ??????

На следующем этапе необходимо выполнить экспорт всех сетевых сессий в CSV-файл. В разделе «Сетевые сессии» выберите все записи и нажмите кнопку «Экспортировать в CSV-файл».



3. ?????????? ????? ??? ???????

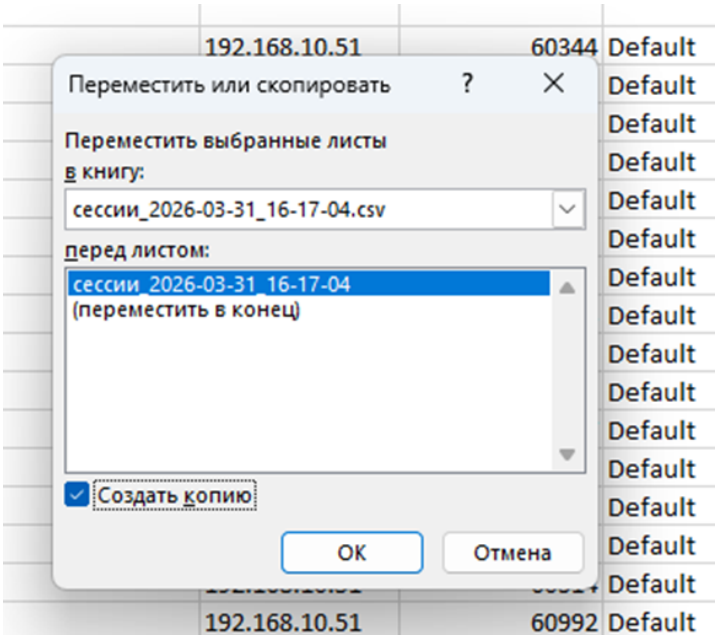
Откройте сформированный файл.



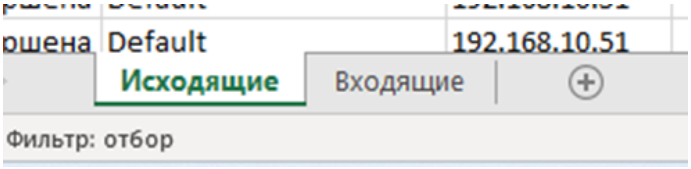
Статус	АП IP-адреса стороны 1	Сторона 1	Порт стороны 1	АП IP-адреса стороны 2	Сторона 2	Порт стороны 2	Устройство 1	Устройство 2	Протокол передачи	Протокол приложений	Текущая скор	Средняя с	Всего пер	Последнее взаимодействие
Активна	Default	192.168.10.53	48010	Default	192.168.10.51	60032	Regul_R500	ASUTP_Workstation	TCP	OPC UA Binary	1368099	885	915153	31.03.2026 16:16
Активна	Default	192.168.10.51	60340	Default	192.168.10.50	8081	ASUTP_Workstation	KICS4Net_Serwer	TCP	TLS v1.3	113	890	724248	31.03.2026 16:16
Активна	Default	192.168.10.51	60365	Default	185.201.2.16	443	ASUTP_Workstation		TCP	TLS v1.2	2	24	2922	31.03.2026 16:16
Активна	Default	192.168.10.51	60346	Default	82.202.184.193	443	ASUTP_Workstation		TCP	TLS v1.3	1	24	12164	31.03.2026 16:16
Активна	Default	192.168.10.51	60364	Default	185.201.2.16	443	ASUTP_Workstation		TCP	TLS v1.2	1	140	17187	31.03.2026 16:16
Активна	Default	192.168.10.51	60333	Default	81.19.104.79	443	ASUTP_Workstation		TCP	TLS v1.3	419	2	1440	31.03.2026 16:16
Активна							ASUTP_Workstation	Regul_R500	Ethernet II	ARP	77	5	5760	31.03.2026 16:16
Активна	Default	192.168.10.51	60362	Default	185.201.2.16	443	ASUTP_Workstation		TCP	TLS v1.2	0	13	2552	31.03.2026 16:16
Завершена	Default	192.168.10.51	60363	Default	192.168.88.50	13000	ASUTP_Workstation	Устройство 026	TCP	TCP	0	13	390	31.03.2026 16:14
Завершена	Default	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP	0	92	1104	31.03.2026 16:14
Завершена	Default	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP	0	54	648	31.03.2026 16:14
Завершена							ASUTP_Workstation	Virtual_gateway	Ethernet II	ARP	0	15	120	31.03.2026 16:14
Завершена	Default	192.168.10.51	60342	Default	185.201.2.16	443	ASUTP_Workstation		TCP	TLS v1.2	0	69	24696	31.03.2026 16:13
Завершена	Default	192.168.10.51	60343	Default	185.201.2.16	443	ASUTP_Workstation		TCP	TLS v1.2	0	10	3791	31.03.2026 16:13
Завершена							ASUTP_Workstation	Virtual_gateway	Ethernet II	ARP	0	8	120	31.03.2026 16:11
Завершена	Default	192.168.10.51	60185	Default	8.8.8.8	53	ASUTP_Workstation		UDP	DNS	0	43	174	31.03.2026 16:11
Завершена	Default	192.168.10.51	58297	Default	8.8.8.8	53	ASUTP_Workstation		UDP	DNS	0	43	172	31.03.2026 16:11
Завершена	Default	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP	0	60	243	31.03.2026 16:11
Завершена	Default	192.168.10.51	60361	Default	185.201.2.16	443	ASUTP_Workstation		TCP	SSL/TLS	0	426	426	31.03.2026 16:10
Завершена							ASUTP_Workstation	Virtual_gateway	Ethernet II	ARP	0	5	180	31.03.2026 16:09
Завершена	Default	192.168.10.51	60344	Default	192.168.88.50	13000	ASUTP_Workstation		TCP	TCP	0	15	390	31.03.2026 16:08
Завершена	Default	192.168.10.51	60349	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	1238	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60348	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	1238	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60351	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	1238	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60350	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	1238	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60352	Default	40.79.173.40	443	ASUTP_Workstation		TCP	HTTPS	0	82	574	31.03.2026 16:08
Завершена	Default	192.168.10.51	60353	Default	104.102.63.189	443	ASUTP_Workstation		TCP	HTTPS	0	93	561	31.03.2026 16:08
Завершена	Default	192.168.10.51	60354	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	1734	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60355	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	2167	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60356	Default	52.140.118.28	443	ASUTP_Workstation		TCP	HTTPS	0	144	576	31.03.2026 16:08
Завершена	Default	192.168.10.51	60357	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	2167	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60358	Default	20.190.181.4	443	ASUTP_Workstation		TCP	HTTPS	0	2167	8670	31.03.2026 16:08
Завершена	Default	192.168.10.51	60359	Default	52.140.118.28	443	ASUTP_Workstation		TCP	HTTPS	0	144	576	31.03.2026 16:08
Завершена	Default	192.168.10.51	60360	Default	52.140.118.28	443	ASUTP_Workstation		TCP	HTTPS	0	192	576	31.03.2026 16:08
Завершена	Default	192.168.10.51	60314	Default	82.202.184.193	443	ASUTP_Workstation		TCP	TLS v1.2	0	4	780	31.03.2026 16:08
Завершена	Default	192.168.10.51	60992	Default	8.8.8.8	53	ASUTP_Workstation		UDP	DNS/LLMNR поверх UDP	0	34	308	31.03.2026 16:08
Завершена	Default	192.168.10.51	60991	Default	8.8.8.8	53	ASUTP_Workstation		UDP	DNS/LLMNR поверх UDP	0	28	252	31.03.2026 16:08

сессии_2026-03-31_16-17-04

Для удобства дальнейшей работы создайте копию единственной вкладки.

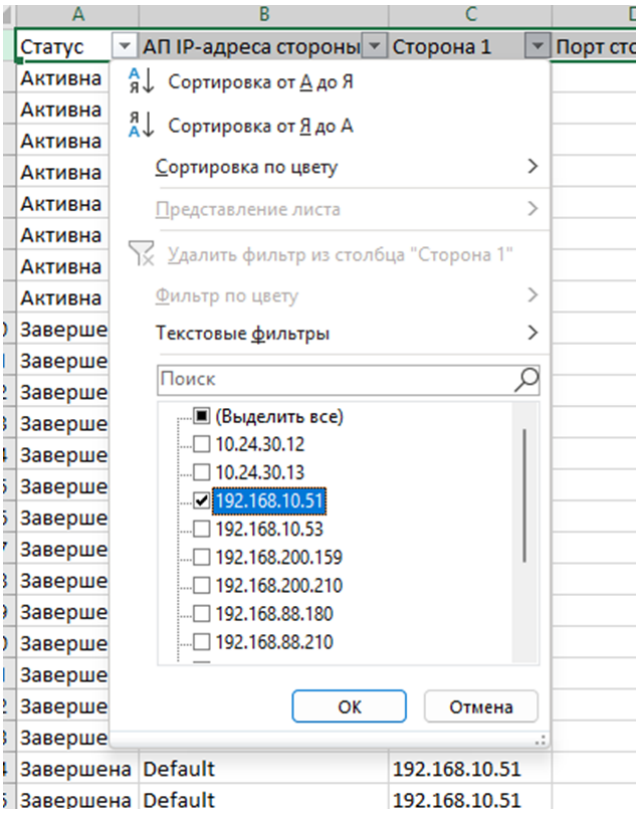


Присвойте вкладкам названия, соответствующие целевым наборам разрешённых входящих и исходящих соединений (например, «Исходящие», «Входящие»).

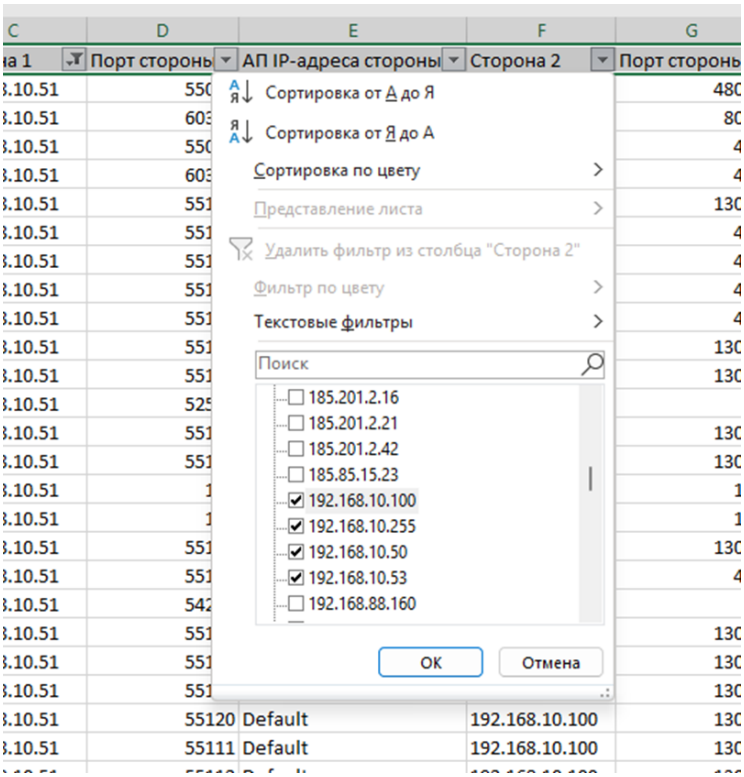


4. ???????????? ??????? ????????? ??????????

На вкладке «Исходящие» создайте фильтр данных, в котором для столбца «Сторона 1» выберите защищаемый узел.



Аналогично создайте фильтр данных, в котором для столбца «Сторона 2» выберите узлы, взаимодействие с которыми разрешено или предусмотрено для защищаемого узла проектной документацией. В случае отсутствия проектной документации перечень узлов, с которыми разрешено взаимодействие, определяется экспертно.



Полученная выборка представляет собой перечень фактических взаимодействий из числа разрешённых.

	C	D	E	F	G	H	I	J	K
ны	Сторона 1	Порт стороны	АП IP-адреса стороны	Сторона 2	Порт стороны	Устройство 1	Устройство 2	Протокол передач	Протокол приложений
	192.168.10.51	55135	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55125	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55133	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55123	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55124	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55122	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55117	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55118	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55119	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55120	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55111	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55112	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55113	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55114	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55115	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	55116	Default	192.168.10.100	13000	ASUTP_Workstation	KSC_Server	TCP	TLS v1.3
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	SMB поверх UDP
	192.168.10.51	137	Default	192.168.10.255	137	ASUTP_Workstation		UDP	NBNS поверх UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	138	Default	192.168.10.255	138	ASUTP_Workstation		UDP	UDP
	192.168.10.51	60340	Default	192.168.10.50	8081	ASUTP_Workstation	KICS4Net_Serwer	TCP	TLS v1.3
	192.168.10.51	60341	Default	192.168.10.50	8081	ASUTP_Workstation	KICS4Net_Serwer	TCP	TLS v1.3
	192.168.10.51	60341	Default	192.168.10.50	8081	ASUTP_Workstation	KICS4Net_Serwer	TCP	TLS v1.3
	192.168.10.51	60336	Default	192.168.10.50	8081	ASUTP_Workstation	KICS4Net_Serwer	TCP	TLS v1.3
	192.168.10.51	55063	Default	192.168.10.53	48010	ASUTP_Workstation	Regul_R500	TCP	OPC UA Binary
	192.168.10.51	55062	Default	192.168.10.53	48010	ASUTP_Workstation	Regul_R500	TCP	OPC UA Binary
	192.168.10.51	60031	Default	192.168.10.53	48010	ASUTP_Workstation	Regul_R500	TCP	TCP
	192.168.10.51	51534	Default	192.168.10.53	48010	ASUTP_Workstation	Regul_R500	TCP	TCP

5. ?????? ?????? ? ???????????? ??????

Выборка должна быть проанализирована на предмет использования в соединениях динамических портов:

- для ОС Windows — 49152–65535;
- для ОС Linux — 32768–60999;
- для проприетарных протоколов и стороннего ПО — используемые диапазоны.

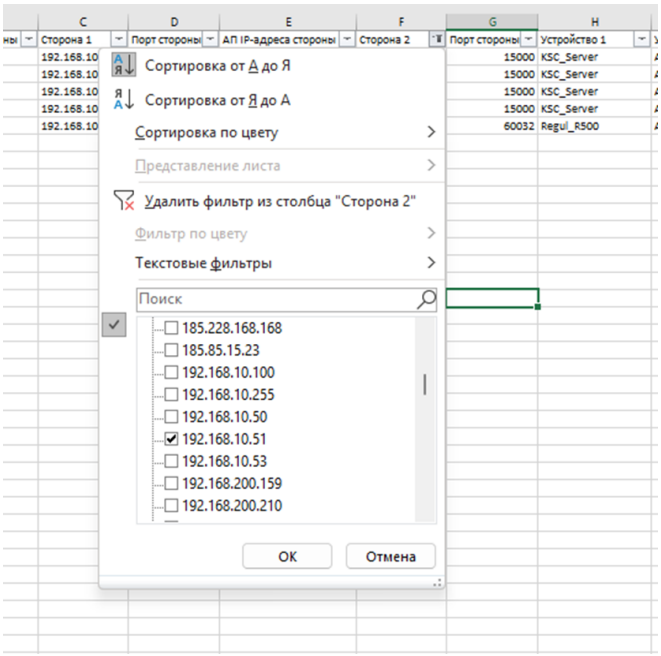
Для таких случаев при формировании набора правил в соответствующих правилах необходимо указывать действующие диапазоны портов. Если определить диапазон портов невозможно, допускается фильтрация только по IP-адресу (наименее безопасный вариант).

Для взаимодействий, в которых порт определяется однозначно, правило формируется по соответствующему порту. Для служебных взаимодействий (например, по портам 137, 138) правила могут не формироваться, если соответствующий функционал (например, NetBIOS для портов 137, 138) не используется в защищаемой системе.

При работе с выборкой сессий дубликаты записей удаляются или скрываются инструментами Excel.

6. ???????????? ?????? ??? ???????? ?????????????

Правила для входящих взаимодействий формируются аналогичным образом.



На этапе фильтрации данных защищаемый узел выступает в качестве стороны 2.

Сторона 1	Порт стороны	АП IP-адреса стороны	Сторона 2	Порт стороны	Устройство 1	Устройство 2	Протокол переда	Протокол приложений
192.168.10.100	56343	Default	192.168.10.51	15000	KSC_Server	ASUTP_Workstation	UDP	UDP
192.168.10.100	49634	Default	192.168.10.51	15000	KSC_Server	ASUTP_Workstation	UDP	UDP
192.168.10.100	44560	Default	192.168.10.51	15000	KSC_Server	ASUTP_Workstation	UDP	UDP
192.168.10.100	57398	Default	192.168.10.51	15000	KSC_Server	ASUTP_Workstation	UDP	UDP
192.168.10.53	48010	Default	192.168.10.51	60032	Regul_R500	ASUTP_Workstation	TCP	OPC UA Binary

7. ????

По результатам анализа и оценки сформированных выборок взаимодействий составляется набор правил для средств периметральной защиты (программно-аппаратных или программных межсетевых экранов), позволяющий реализовывать функционал защищаемой системы при минимальном количестве разрешённых взаимодействий. Стоит отметить, что для настройки современных межсетевых экранов, работающих по принципу Stateful (в том числе функционал "Сетевой экран" KICS for Nodes), создания правил для обратного трафика не требуется, достаточно создания разрешающего правила от стороны, инициировавшей сессию, до узла назначения, обратые пакеты будут пропущены через МЭ автоматически.

Сторона 1	Порт стороны 1	Сторона 2	Порт стороны 2
192.168.10.51	49152 – 65535	192.168.10.53	48010
192.168.10.51	49152 – 65535	192.168.10.50	8081
192.168.10.51	49152 – 65535	192.168.10.100	13000
192.168.10.51	137	192.168.10.255	137
192.168.10.51	138	192.168.10.255	138
192.168.10.100	49152 – 65535	192.168.10.51	15000
192.168.10.53	48010	192.168.10.51	49152 – 65535

ВАЖНО! Включение средств периметральной защиты систем промышленной автоматизации в режиме блокирования отдельных сетевых взаимодействий должно осуществляться только после проведения соответствующих приемочных испытаний и проверки отсутствия деструктивного воздействия на работоспособность защищаемых систем.

Revision #5
Created 1 April 2026 15:52:46 by Alexey Panyukhin
Updated 1 July 2026 08:19:24 by Alexey Panyukhin