

Ландшафт угроз для систем промышленной автоматизации

Азия. Третий квартал 2025 года

Юго-Восточная Азия	4
Основные проблемы кибербезопасности в регионе	4
Статистика по всем угрозам.....	4
Источники угроз.....	6
Интернет.....	7
Почтовые клиенты	8
Съемные носители	10
Сетевые папки.....	11
Категории угроз	12
Шпионские программы	14
Вирусы и вредоносные программы для AutoCAD.....	15
Отрасли.....	20
Источники и категории вредоносного ПО в отраслях: «горячие точки»	24
Восточная Азия.....	30
Основные проблемы кибербезопасности в регионе	30
Статистика по всем угрозам.....	33
Источники угроз.....	34
Интернет.....	35
Почтовые клиенты	36
Съемные носители	38
Сетевые папки.....	39
Категории угроз	41
Шпионские программы	43
Черви.....	44
Вирусы и вредоносные программы для AutoCAD.....	45
Угроза квартала: вредоносные скрипты и фишинговые страницы.....	48
Отрасли.....	49
Источники и категории вредоносного ПО в отраслях: «горячие точки»	54
Южная Азия	60
Основные проблемы кибербезопасности в регионе	60
Статистика по всем угрозам.....	61
Источники угроз.....	62

Интернет.....	63
Почтовые клиенты	64
Съемные носители	65
Сетевые папки.....	67
Категории угроз	68
Ресурсы в интернете из списка запрещенных	69
Черви.....	70
Вирусы и вредоносные программы для AutoCAD.....	72
Программы-вымогатели.....	74
Отрасли.....	75
Источники и категории вредоносного ПО в отраслях: «горячие точки»	77
Средняя Азия и Закавказье	82
Основные проблемы кибербезопасности в регионе	82
Статистика по всем угрозам.....	83
Источники угроз.....	84
Интернет.....	85
Почтовые клиенты	86
Съемные носители	87
Категории угроз	89
Майнеры – исполняемые файлы для ОС Windows	91
Черви.....	93
Программы-вымогатели.....	95
Отрасли.....	96
Источники и категории вредоносного ПО в отраслях: «горячие точки»	98
Методика подготовки статистики.....	105

Юго-Восточная Азия

Основные проблемы кибербезопасности в регионе

Наличие значительной части незащищенной инфраструктуры, которая становится источником вторичного заражения (распространения) вредоносного ПО

В Юго-Восточной Азии высокие показатели самораспространяющегося ПО.

Регион занимает первое место в мире по доле компьютеров АСУ, на которых были заблокированы вирусы и вредоносные программы для AutoCAD. В обоих случаях он лидирует с большим отрывом.

Вредоносные программы для AutoCAD в большинстве случаев распространяются так же, как вирусы. Это объясняет столь высокую долю для этой категории вредоносного ПО.

В Юго-Восточной Азии вирусы занимают второе место в региональном рейтинге категорий вредоносных программ по доле компьютеров АСУ, на которых они были заблокированы. Это самая высокая позиция вирусов в региональных рейтингах. Региональный показатель в 5,3 раза превышает среднемировой и является самым высоким значением в мире.

Среди всех категорий угроз, в мировом рейтинге в третьем квартале 2025 года по доле компьютеров АСУ, на которых была заблокирована угроза, программы для AutoCAD находятся на седьмом месте из 10. Во всех регионах, кроме Южной, Восточной и Юго-Восточной Азии, эта категория занимает последнее место. А в региональном рейтинге Юго-Восточной Азии – шестое, с показателем, который в 7,3 раза превышает среднемировой и является самым высоким в мире.

Недостатки сегментации сети предприятий в регионе

Юго-Восточная Азия занимает второе место среди регионов по доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, с 0,10%. Это значение выше среднемирового в 2,5 раза.

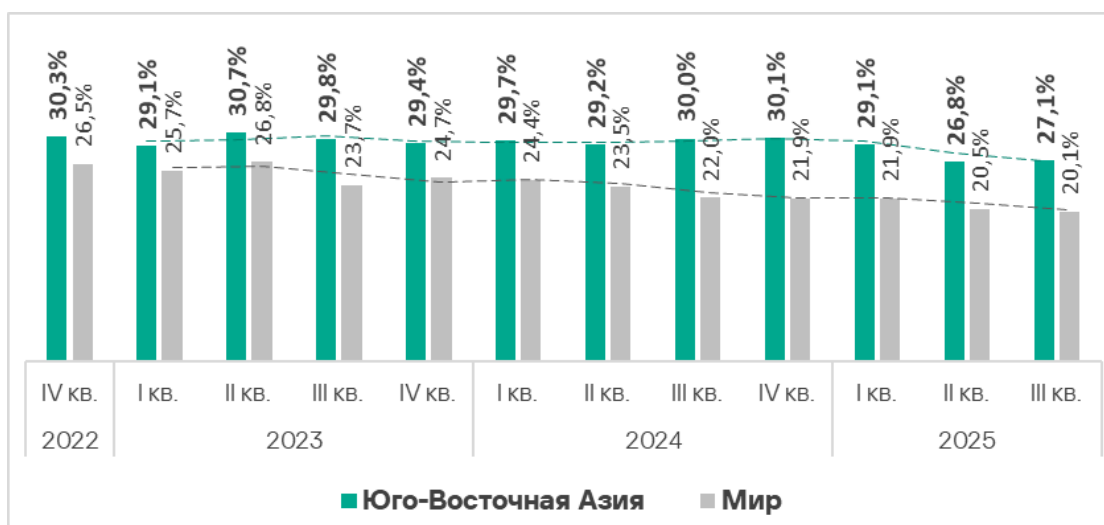
Преимущественно это результат ситуации во Вьетнаме, который с большим отрывом лидирует среди стран региона и по вирусам, и по вредоносному ПО для AutoCAD, а также по угрозам в сетевых папках.

Статистика по всем угрозам

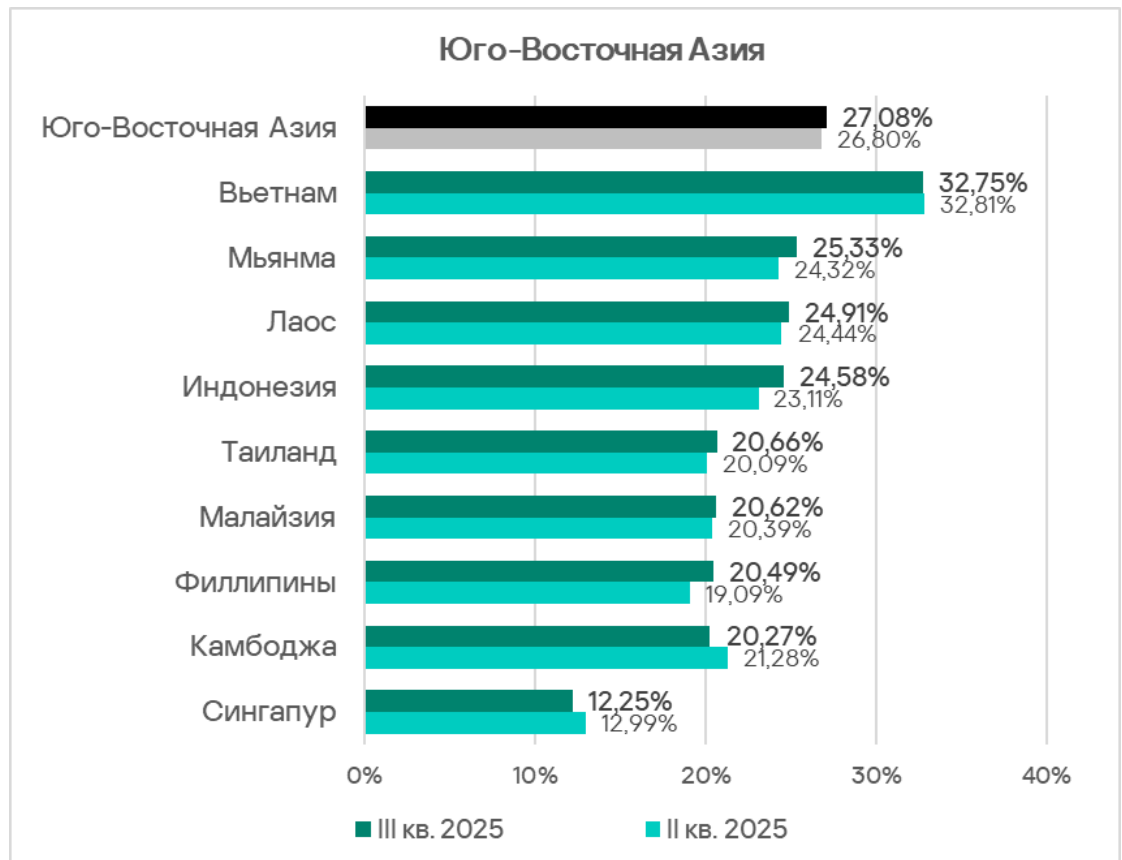
Юго-Восточная Азия занимает второе место в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с

показателем 27,1%. Это значение больше среднемирового в 1,3 раза и в 2,9 раза больше минимального значения среди регионов, зафиксированного в Северной Европе.

После уменьшения показателя региона в двух предыдущих кварталах, в третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Юго-Восточной Азии, увеличилась, но не вернулась к значениям конца 2024 года.



В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 12,25% в Сингапуре до 32,75% во Вьетнаме. Показатели остальных стран — в диапазоне от 20% до 26%.

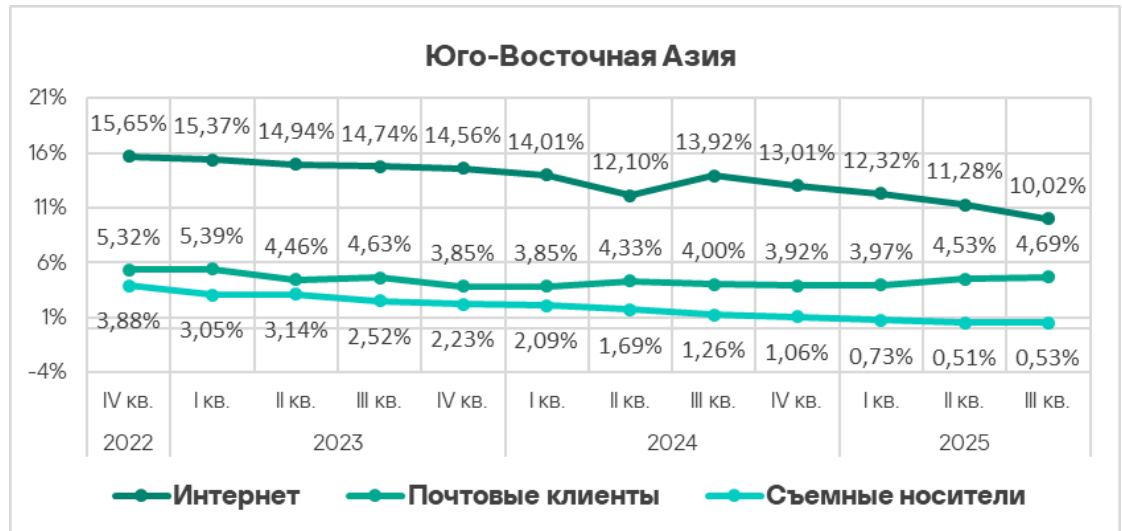


Источники угроз

Доля компьютеров АСУ, на которых были заблокированы угрозы из разных источников, по всем источникам в регионе выше среднемировых показателей. Доля компьютеров АСУ, где источником угрозы стали почтовые клиенты и съемные носители, в регионе выше, чем в мире, в 1,6 раз для каждого из этих источников. Региональный показатель сетевых папок превышает среднемировой в 2,5 раза.



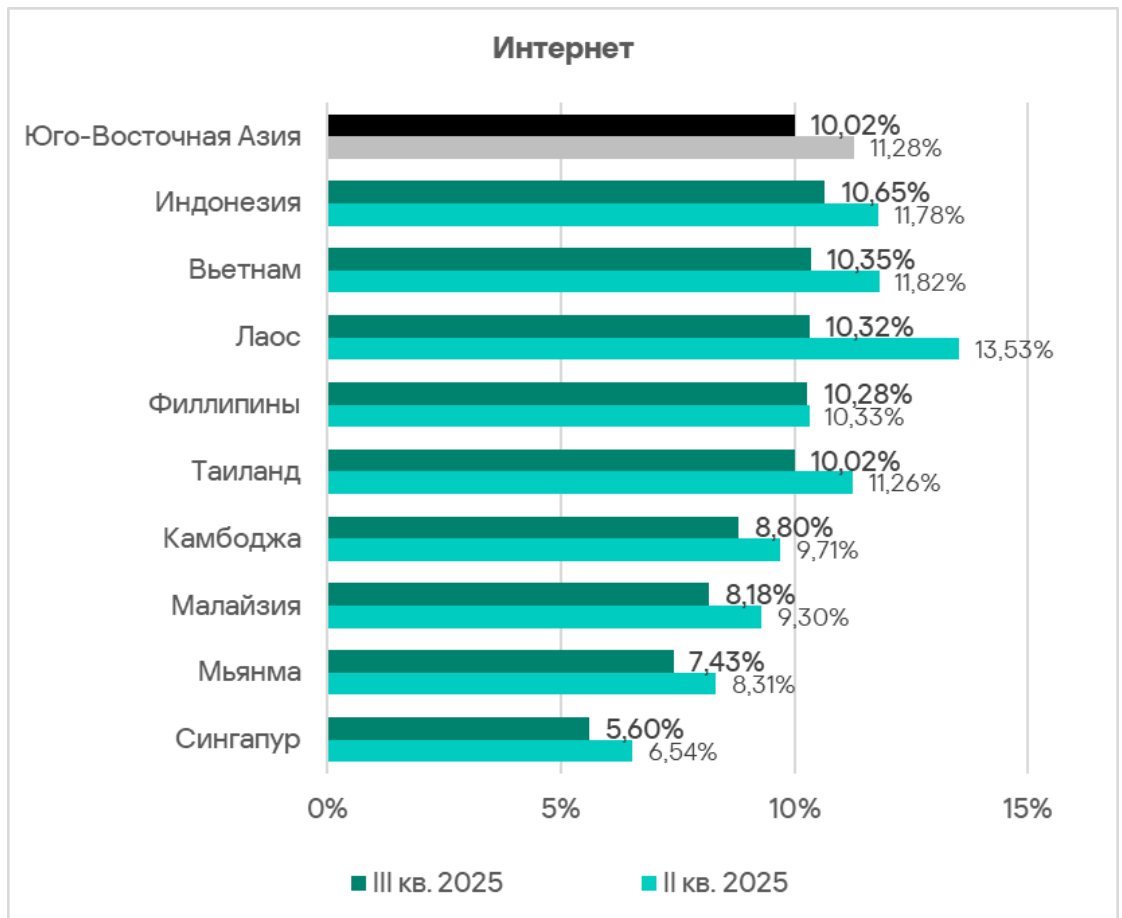
В третьем квартале 2025 года показатель вырос у почтовых клиентов и немного подрос у съемных носителей.



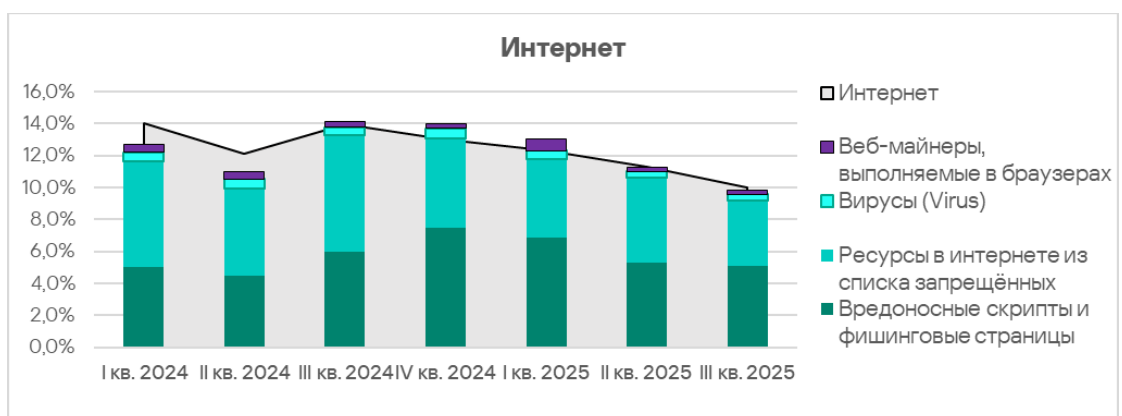
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Юго-Восточная Азия занимает второе место в рейтинге регионов с показателем, который превышает минимальный — у Северной Европы — в 2,2 раза.

Показатели стран региона варьируют от 5,60% в Сингапуре до 10,65% в Индонезии.



Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе, — это вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вирусы и веб-майнеры.

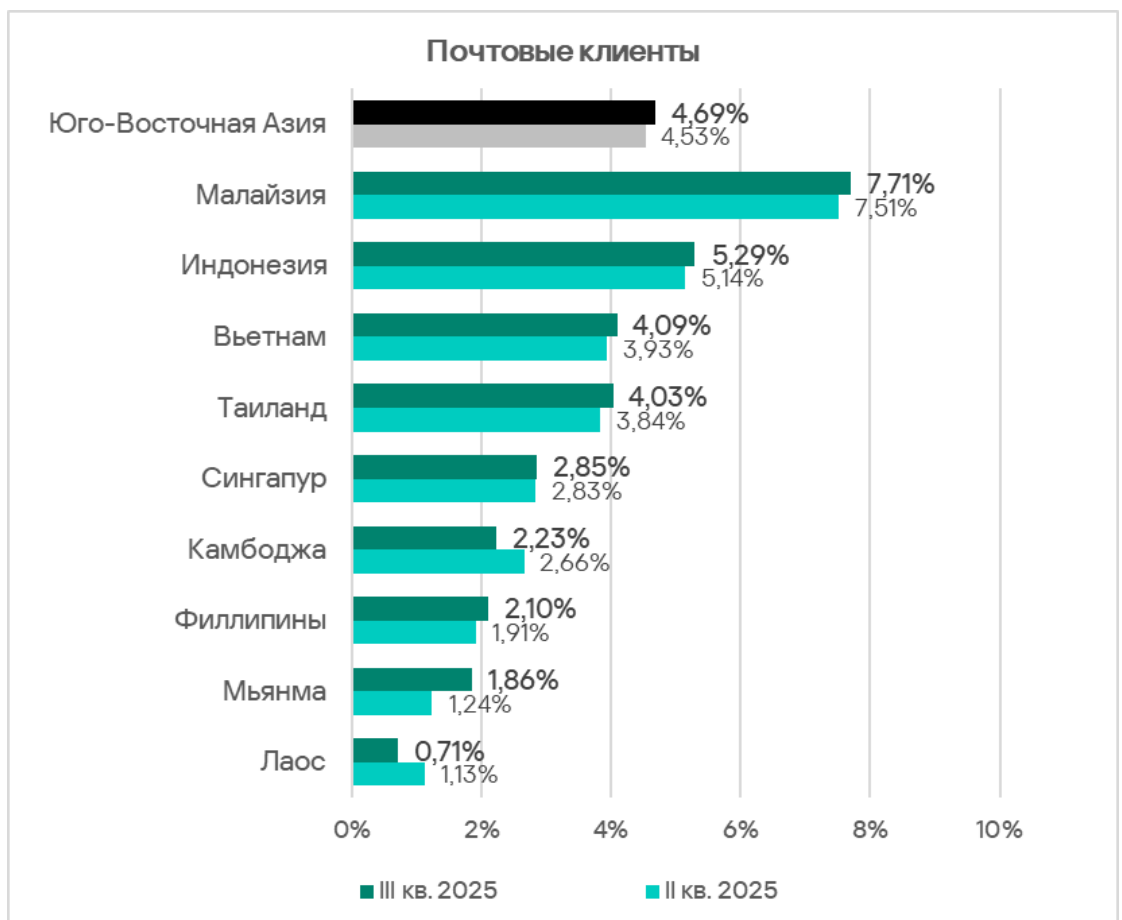


Почтовые клиенты

Почтовые клиенты — источник угроз в регионе, показатель которого растет третий квартал подряд.

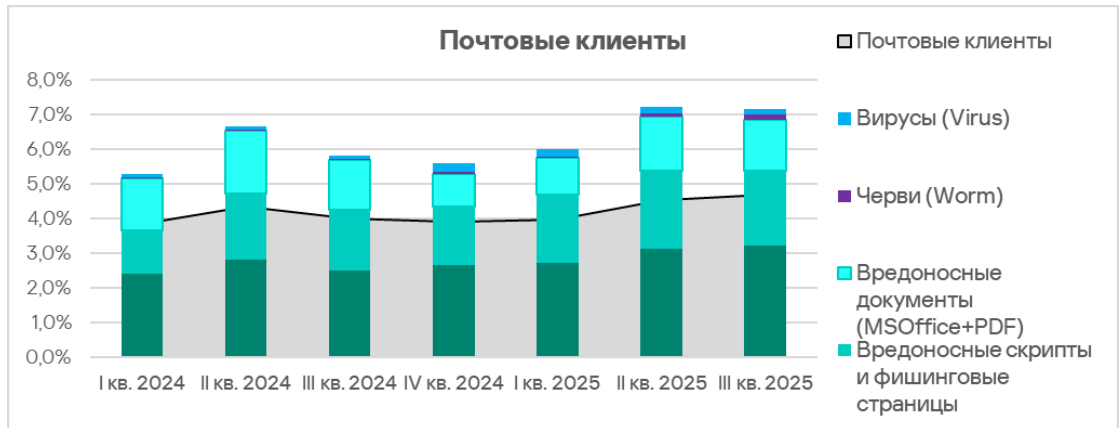


Среди стран региона по этому показателю с заметным отрывом лидирует Малайзия с 7,71%. Минимальная доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, – в Лаосе (0,71%). В отличие от большинства стран региона (все, кроме Камбоджи), в Лаосе показатель за квартал уменьшился.



Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ: шпионское ПО, вредоносные скрипты и фишинговые

страницы, вредоносные документы. В рейтинге регионов по шпионским программам Юго-Восточная Азия находится на втором месте.

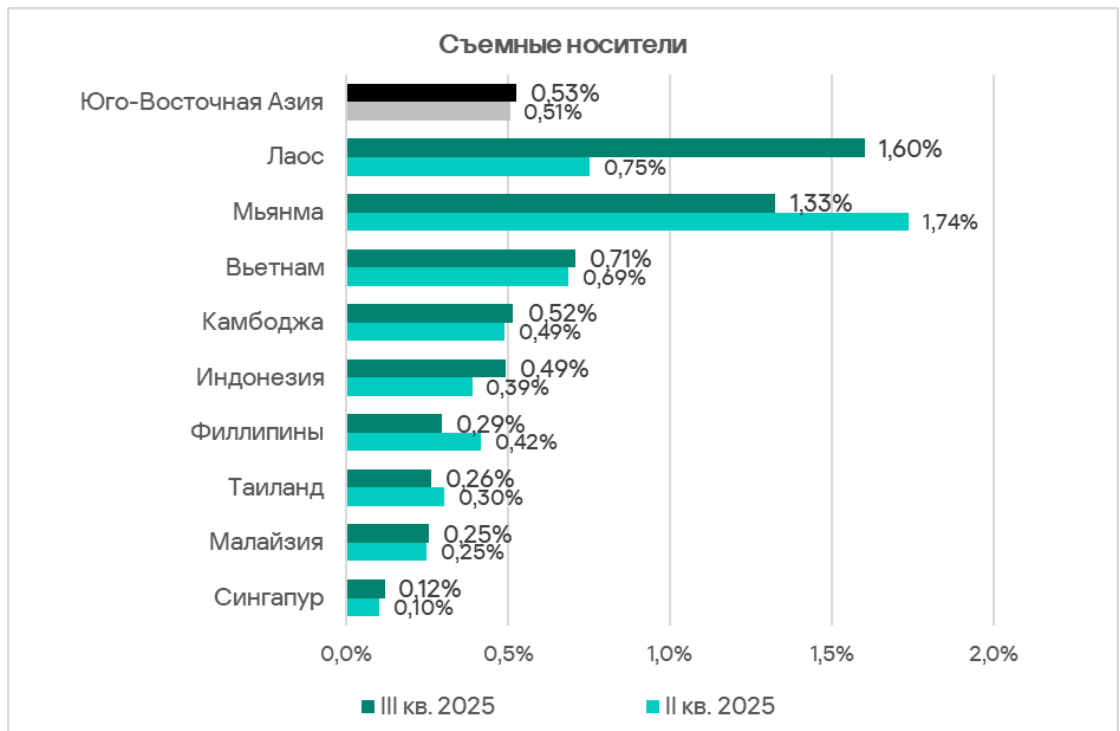


Съемные носители

Юго-Восточная Азия занимает пятое место в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей. Первые шесть позиций в этом рейтинге занимают Африка (лидирует с большим отрывом), регионы Азии и Ближний Восток. Показатели не только Африки, но и всех этих регионов, заметно больше значений в остальных регионах.

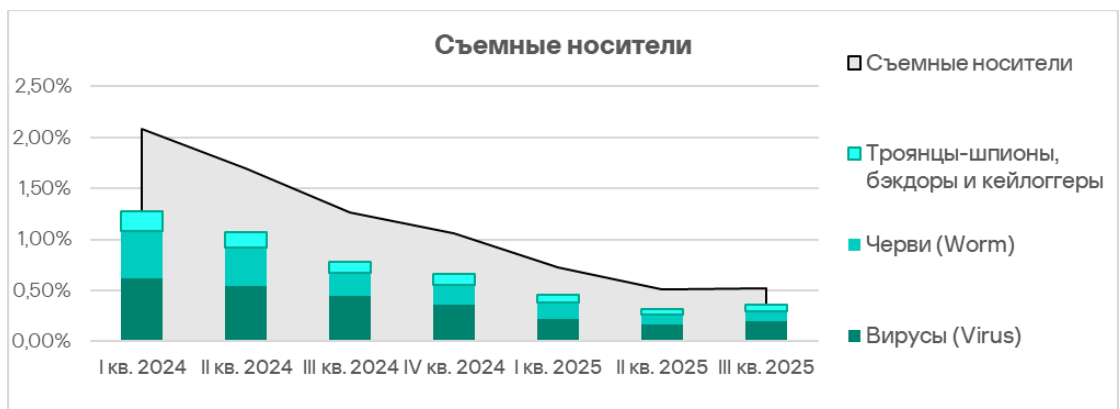
Показатель в Юго-Восточной Азии вырос до 0,53% и превышает значение в регионе Австралия и Новая Зеландия, который занимает последнее место в рейтинге, в 10,6 раза.

Среди стран региона по этому показателю с отрывом от остальных лидируют Лаос с 1,60% (в этой стране показатель за квартал вырос в 2,1 раза), и Мьянма с 1,33%. Наименьшее значение в Сингапуре — 0,12%.



У обеих стран, возглавляющих рейтинг по съемным носителям, — Лаоса и Мьянмы — наименьшие из всех стран региона показатели по угрозам в почтовых клиентах.

Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: вирусы, черви и шпионское ПО. По вирусам Юго-Восточная Азия с большим отрывом лидирует среди регионов.



Сетевые папки

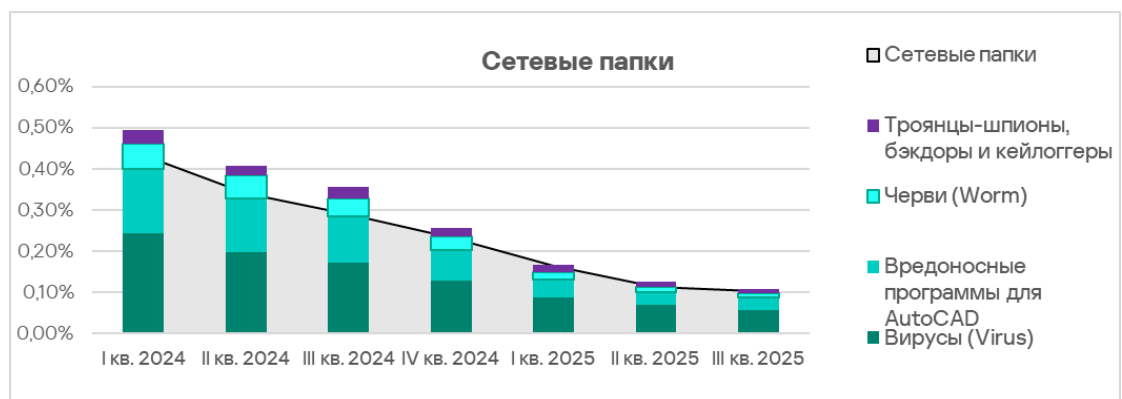
Юго-Восточная Азия занимает второе место среди регионов по доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, с 0,10%, уступая только Восточной Азии.

Показатели двух регионов-лидеров заметно превышают остальные. У Юго-Восточной Азии он превышает значение следующего в рейтинге региона — Ближнего Востока — в 1,7 раза. С Северной Европой, которая занимает последнее место в рейтинге, показатели отличаются в 17,2 раза.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, в третьем квартале 2025 года с заметным отрывом лидирует Лаос с 0,36%.



Основными категориями угроз, которые распространяются через сетевые папки, являются вирусы, вредоносное ПО для AutoCAD, черви и шпионские программы. По показателю вредоносного ПО для AutoCAD Юго-Восточная Азия с большим отрывом лидирует среди регионов.



Категории угроз

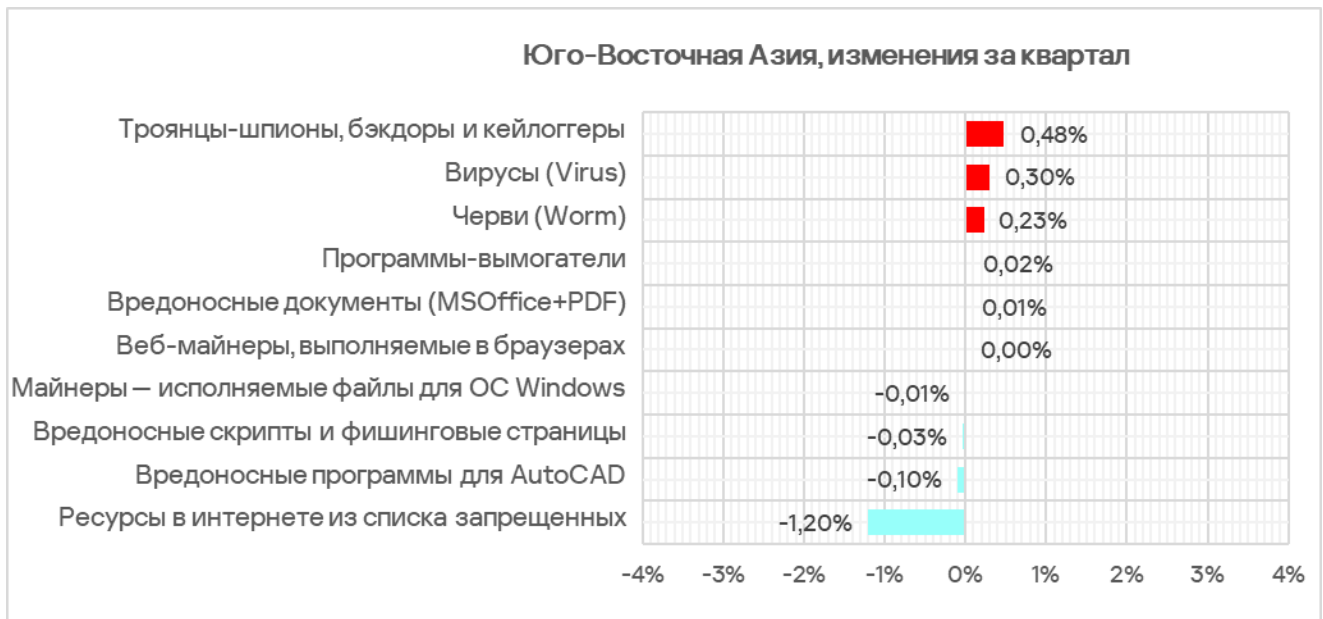
В Юго-Восточной Азии у всех категорий угроз, кроме трех (ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows и программы-вымогатели), доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения.

Наиболее значительно региональные показатели превышают среднемировые у категорий угроз:

- шпионские программы – в 1,5 раза;
- вирусы – в 5,3 раза;
- вредоносное ПО для AutoCAD – в 7,3 раза.

В Юго-Восточной Азии в рейтинге категорий угроз вирусы находятся на втором месте. Это единственный регион, где эта категория угроз находится насколько высоко.

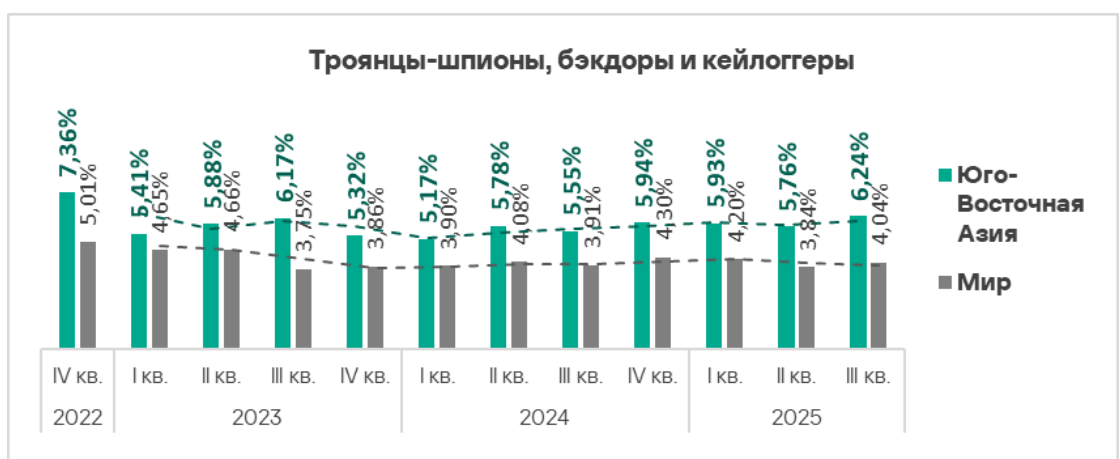




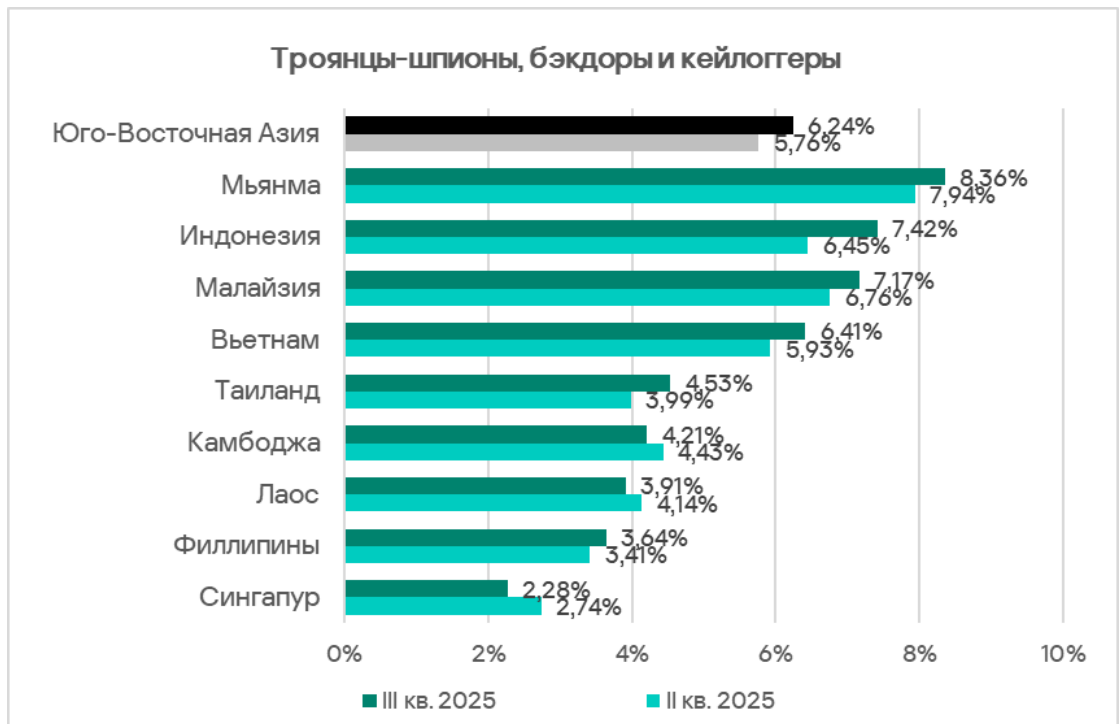
Из всех категорий угроз за квартал показатель вырос у трех: шпионские программы, вирусы и черви.

Шпионские программы

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются шпионские программы, Юго-Восточная Азия в третьем квартале 2025 года поднялась на одну позицию и заняла второе место с 6,24%. Это в 4,5 раза больше показателя Северной Европы, где значение показателя минимальное.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы программы-шпионы, лидирует Мьянма с 8,36%. В Сингапуре показатель наименьший – 2,28%. Показатель вырос во всех странах, кроме Сингапура, Лаоса и Камбоджи.

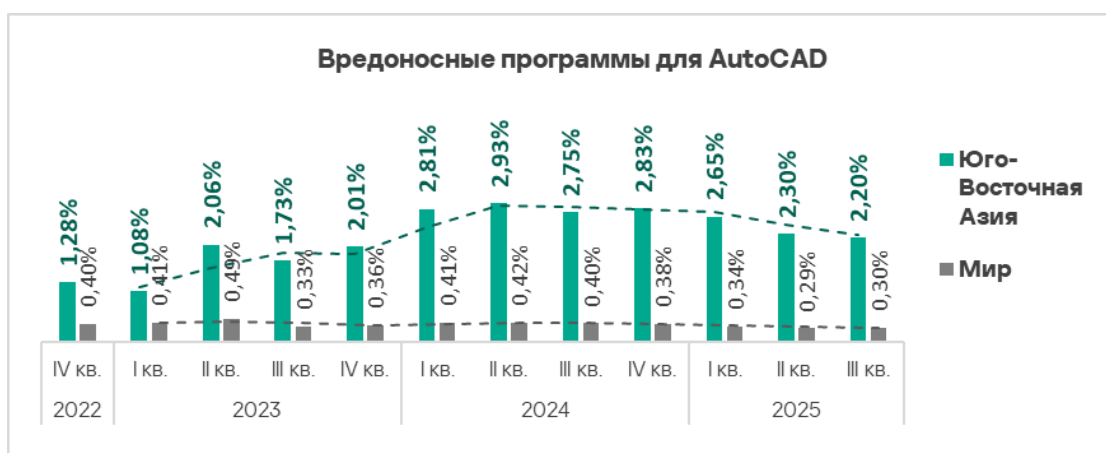
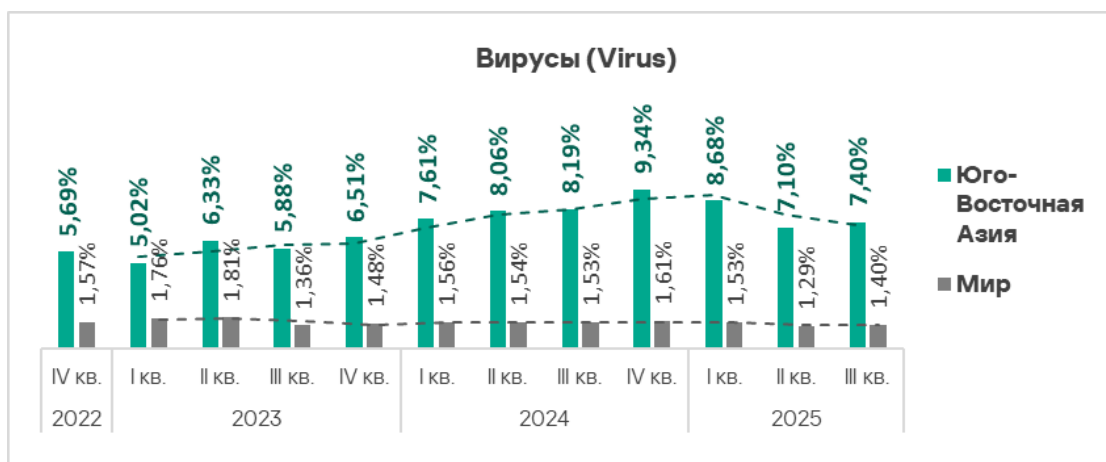


Шпионские программы в регионе блокируются во всех источниках угроз, но основной канал их распространения — электронная почта. Малайзия, Индонезия и Вьетнам, которые следуют за Мьянмой в рейтинге по шпионским программам, оказались в тройке стран региона, лидирующих и по угрозам из почтовых клиентов. А вот в Мьянме ситуация иная: страна находится на втором месте по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.

Вирусы и вредоносные программы для AutoCAD

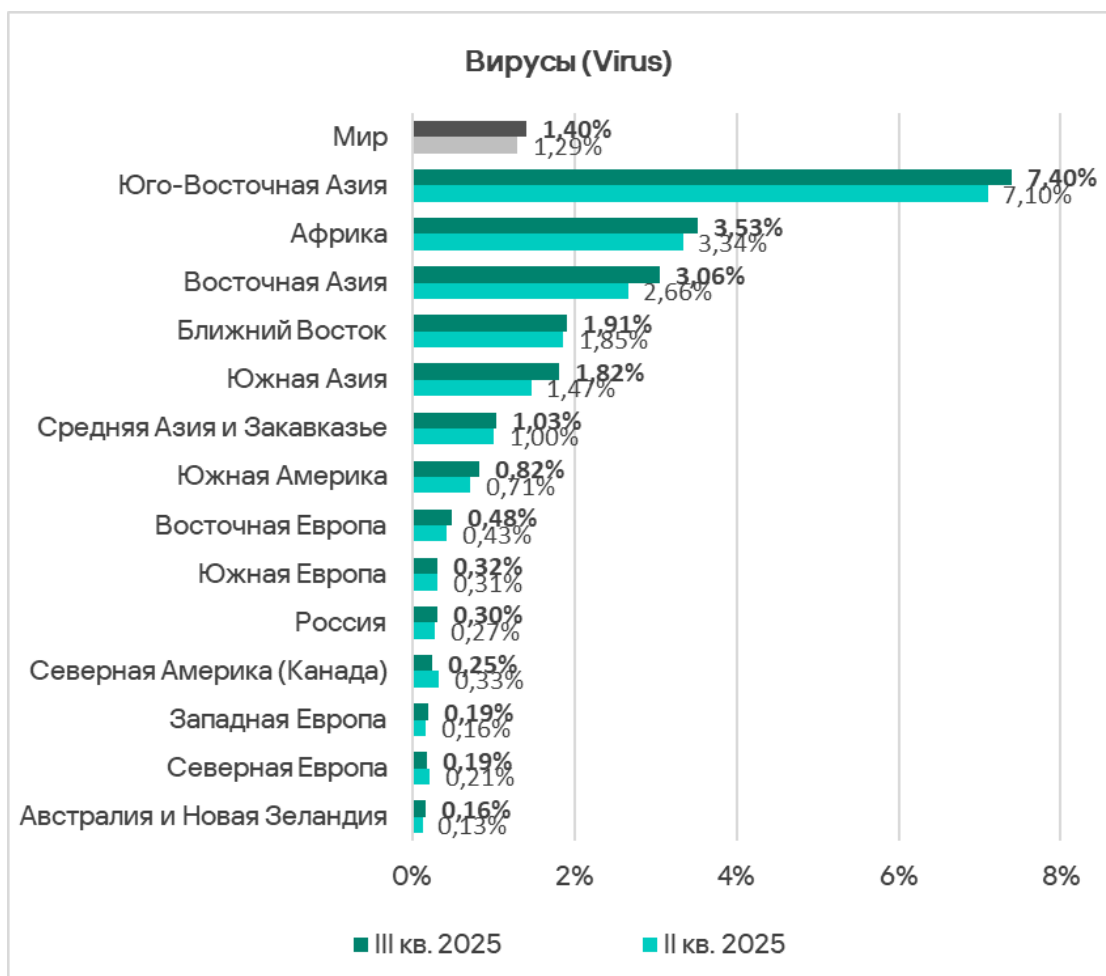
Вредоносные программы для AutoCAD в большинстве случаев, как и вирусы, распространяются путем заражения пользовательских файлов. Поэтому у этих двух категорий угроз много общего.

Показатели обеих категорий заметно выросли в 2024 году, но в 2025 году они ниже, чем годом ранее.



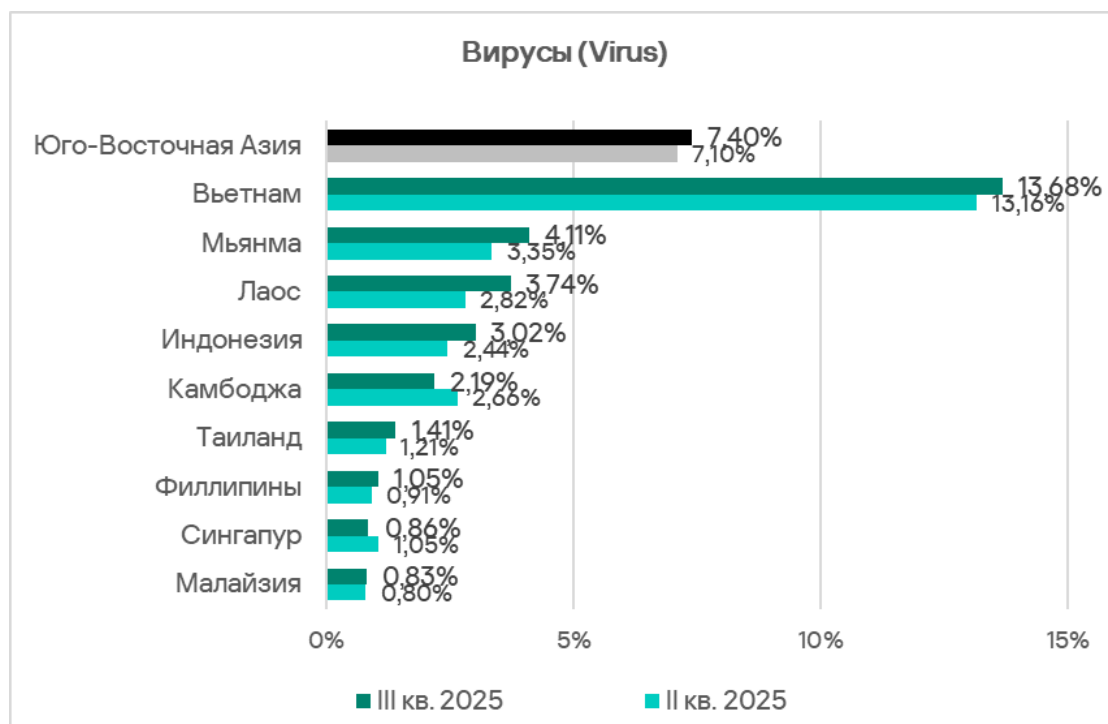
Вирусы

По доле компьютеров АСУ, атакованных вирусами, Юго-Восточная Азия лидирует в соответствующем рейтинге регионов с огромным отрывом.



В Юго-Восточной Азии показатель больше, чем в Африке (следующий в рейтинге регион), в 2,1 раза, а по сравнению с регионом Австралия и Новая Зеландия, который замыкает рейтинг, — в 46,3 раза.

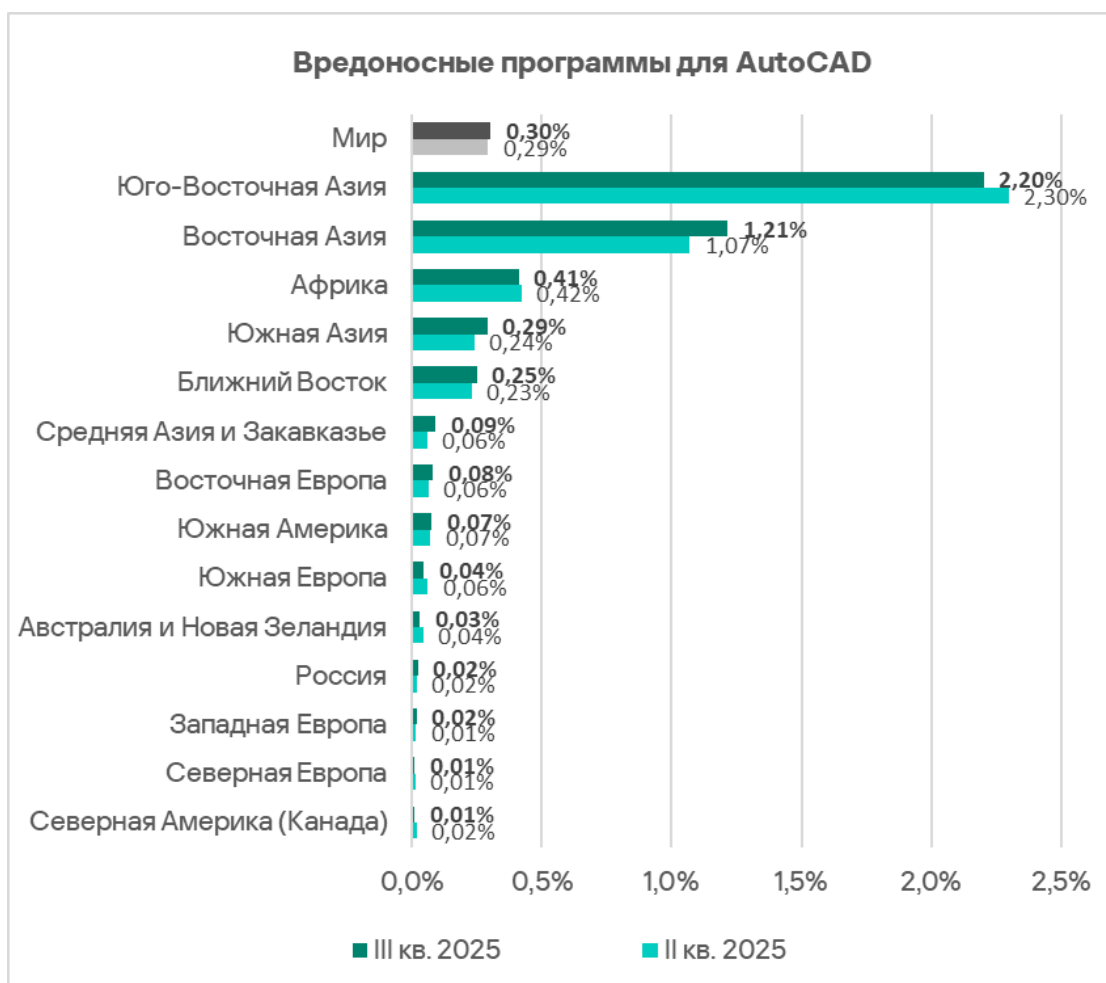
Столь яркое лидерство Юго-Восточной Азии обеспечивает Вьетнам с 13,6%. В этой стране показатель выше, чем у следующей в рейтинге Мьянмы, в 3,3 раза.



Вирусы в регионе блокируются во всех источниках угроз. Отметим, что Вьетнам находится на второй позиции в рейтингах стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и в сетевых папках, и на третьей — по показателям почтовых клиентов и съемных носителей.

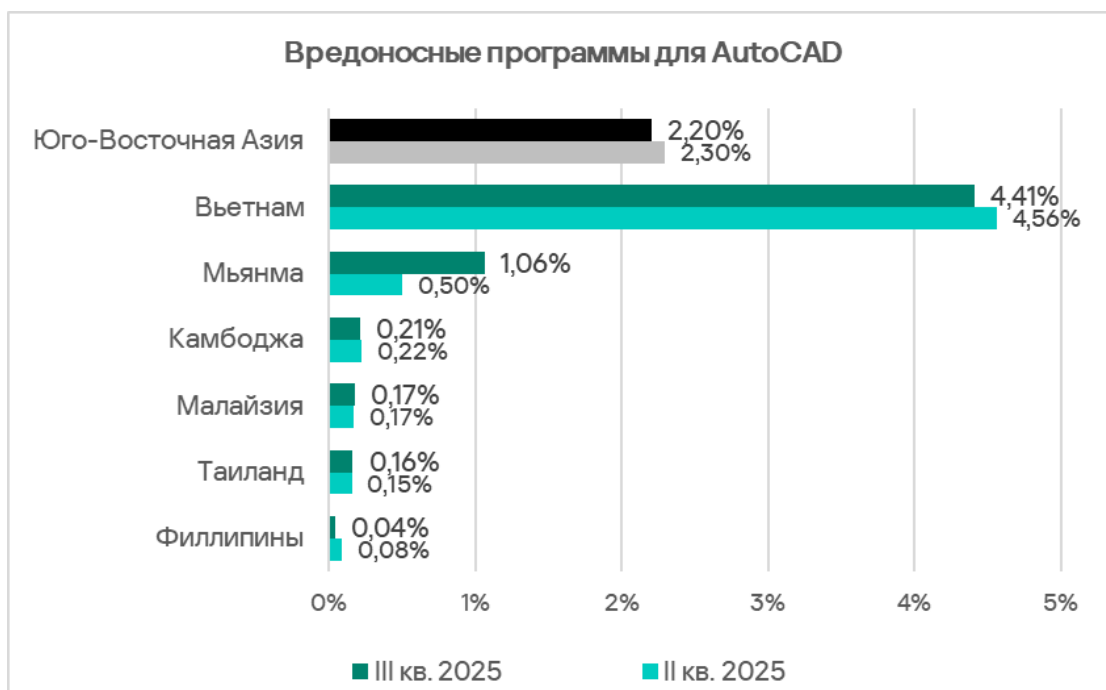
Вредоносное ПО для AutoCAD

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, Юго-Восточная Азия также лидирует в соответствующем рейтинге регионов с большим отрывом.



В Юго-Восточной Азии показатель больше минимального среди регионов — в Северной Америке (Канада) — в 220 раз (!).

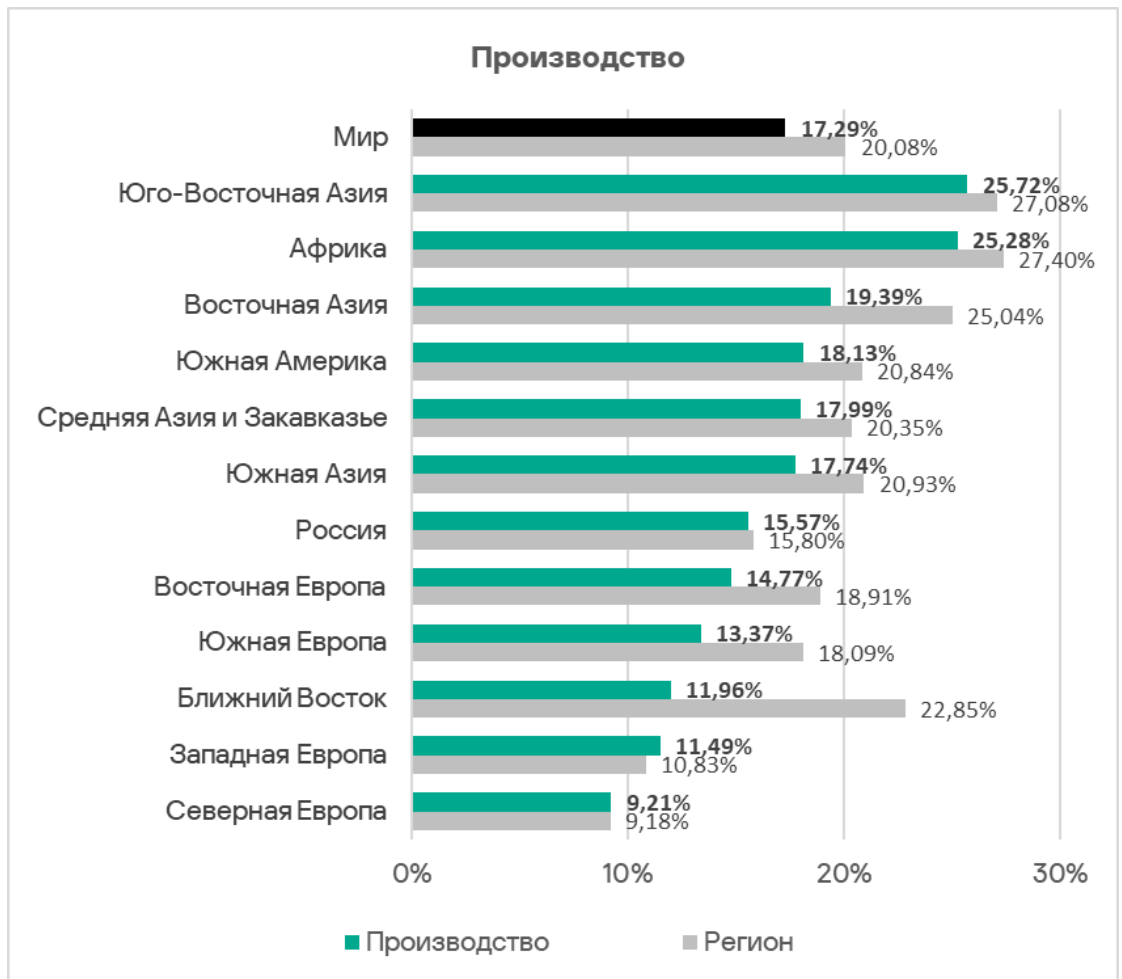
Лидерство региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, также обеспечивает Вьетнам с огромным для этой категории показателем 4,41%.



Отрасли

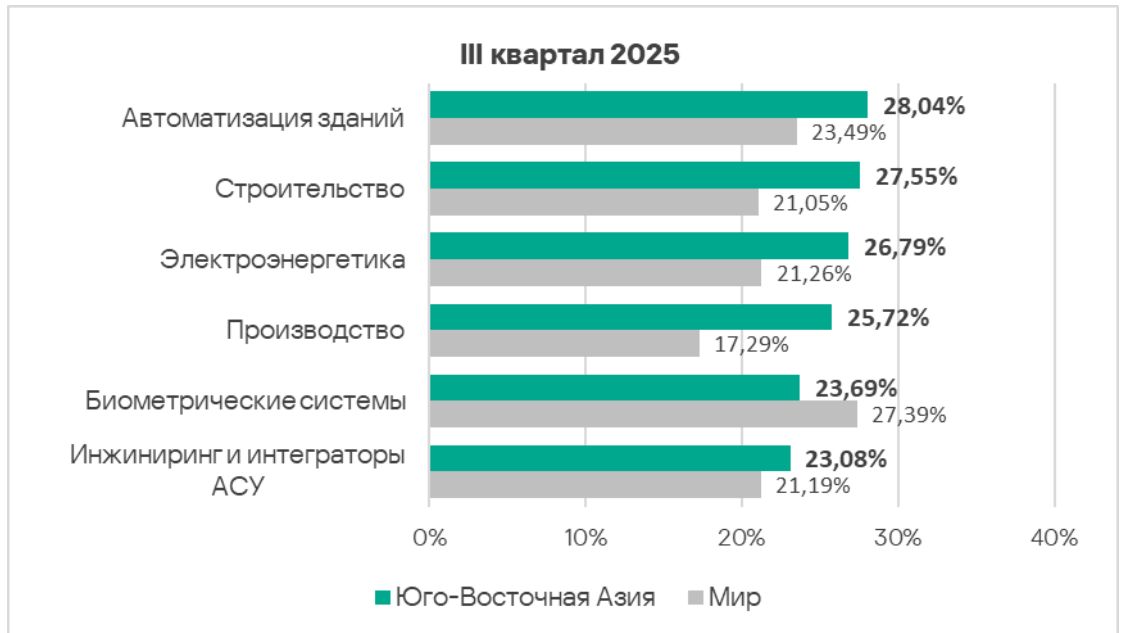
В третьем квартале 2025 года среди регионов Юго-Восточная Азия лидирует по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отраслях автоматизация зданий и производство.





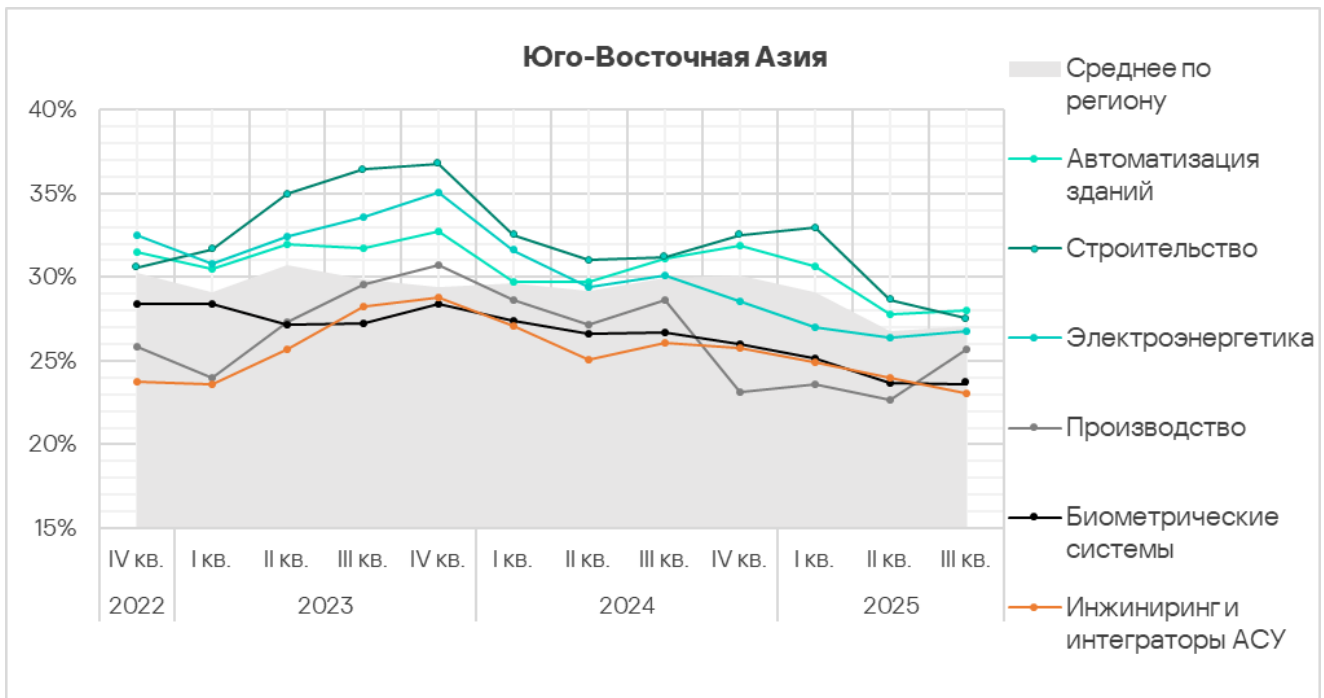
В третьем квартале 2025 года в Юго-Восточной Азии по доле компьютеров АСУ, на которых блокируются вредоносные объекты, среди рассмотренных в отчете отраслей автоматизация зданий обогнала строительство.

В регионе показатели всех отраслей превышают аналогичные среднемировые. Больше всего разница у отрасли производство — в 1,5 раза.



За квартал увеличились показатели у отраслей автоматизация зданий, электроэнергетика, производство. Больше всего — показатель производственной отрасли.

Все рассмотренные отрасли с четвертого квартала 2023 года демонстрируют положительную динамику долгосрочных трендов (показатели снижаются) с периодическими колебаниями.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

Показатели источников угроз в отраслях в Юго-Восточной Азии, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	8,47%	9,97%	11,61%	10,67%	9,40%	9,76%	10,02%
Почтовые клиенты	8,24%	6,65%	2,50%	4,13%	6,27%	5,52%	4,69%
Съемные носители	0,56%	0,50%	0,55%	0,42%	0,65%	0,42%	0,53%
Сетевые папки	0,05%	0,09%	0,03%	0,05%	0,00%	0,00%	0,10%
Показатель отрасли в регионе	23,69%	28,04%	26,79%	23,08%	27,55%	25,72%	

Показатели категорий угроз в отраслях в Юго-Восточной Азии, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	3,35%	4,10%	5,81%	4,93%	4,08%	4,81%	4,42%
Вредоносные скрипты и фишинговые страницы	10,08%	9,47%	8,20%	7,86%	9,34%	7,07%	8,02%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,93%	8,10%	5,68%	5,36%	6,74%	5,09%	6,24%
Черви (Worm)	2,00%	1,61%	2,50%	1,25%	2,37%	0,71%	1,72%
Майнеры - исполняемые файлы для ОС Windows	0,61%	0,46%	0,83%	0,44%	0,53%	0,28%	0,41%
Вредоносные документы (MSOffice + PDF)	4,20%	3,36%	1,85%	1,90%	2,60%	1,56%	2,36%
Вирусы (Virus)	2,66%	6,66%	6,14%	3,34%	4,08%	3,54%	7,40%
Программы-вымогатели	0,28%	0,18%	0,29%	0,08%	0,30%	0,42%	0,12%
Веб-майнеры, выполняемые в браузерах	0,59%	0,40%	0,68%	0,40%	0,53%	0,14%	0,35%
Вредоносные программы для AutoCAD	0,26%	0,79%	1,38%	1,02%	0,59%	0,99%	2,20%
Показатель отрасли в регионе	23,69%	28,04%	26,79%	23,08%	27,55%	25,72%	

Автоматизация зданий

Юго-Восточная Азия – лидер среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

В глобальном рейтинге по индустриям во всех регионах отрасль автоматизация зданий в Юго-Восточной Азии занимает:

- второе место по доле компьютеров, на которых были заблокированы вирусы.

Среди регионов по показателям в отрасли Юго-Восточная Азия занимает:

- второе место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, и третье – по показателю угроз в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателям угроз следующих категорий: шпионские программы, веб-майнеры, вредоносные программы для AutoCAD.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов и в сетевых папках;
- второе место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, вирусы.

Строительство

Юго-Восточная Азия находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

В глобальном рейтинге по индустриям во всех регионах строительство в Юго-Восточной Азии занимает:

- первое место по показателю угроз из интернета;
- первое место по доле компьютеров, на которых были заблокированы вирусы;
- второе место по доле компьютеров, на которых было заблокировано вредоносное ПО для AutoCAD;
- четвертое место по доле компьютеров, на которых были заблокированы веб-майнеры.

Среди регионов по показателям в отрасли Юго-Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, и второе – по показателю сетевых папок;
- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, веб-майнеры, вредоносные программы для AutoCAD.

Среди отраслей в регионе строительство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и в сетевых папках;
- первое место по показателям следующих категорий угроз: вирусы, вредоносные программы для AutoCAD, веб-майнеры;
- второе место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, майнеры – исполняемые файлы для ОС Windows.

Электроэнергетика

Юго-Восточная Азия находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

В глобальном рейтинге по индустриям во всех регионах электроэнергетика в Юго-Восточной Азии занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы вирусы;
- пятое место по показателю угроз из интернета.

Среди регионов по показателям в отрасли Юго-Восточная Азия занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателям шпионских программ и вредоносных программ для AutoCAD, третье — по показателям майнеров обеих категорий и ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе электроэнергетика занимает:

- второе место по доле компьютеров АСУ, на которых блокировались угрозы из интернета, третье место по показателям угроз на съемных носителях;
- первое место по показателям ресурсов в интернете из списка запрещенных;
- второе место по показателям следующих категорий угроз: веб-майнеры, вредоносные программы для AutoCAD, программы-вымогатели.

Производство

Юго-Восточная Азия – лидер среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди регионов по показателям в отрасли Юго-Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, второе – по показателю угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются угрозы следующих категорий: вредоносные скрипты и фишинговые страницы, шпионские программы, вирусы, веб-майнеры;

- второе место по показателям следующих категорий угроз: вредоносные документы, программы-вымогатели, вредоносные программы для AutoCAD. Также регион занимает третье место по показателям ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей;
- третье место по показателю угроз из почтовых клиентов;
- второе место по показателю червей;
- третье место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, вредоносные документы и шпионские программы.

Биометрические системы

Юго-Восточная Азия находится на седьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в ОТ-инфраструктуре биометрические системы.

Среди регионов по показателям в ОТ-инфраструктуре биометрические системы Юго-Восточная Азия занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах;
- первое место по доле компьютеров АСУ, на которых блокируются веб-майнеры;
- второе место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD, и третье — по показателям вредоносных документов и шпионских программ.

Среди отраслей в регионе ОТ-инфраструктура биометрические системы занимает:

- первое место по доле компьютеров АСУ, на которых блокировались угрозы в почтовых клиентах;
- второе место по показателю съемных носителей, третье — по показателю угроз в сетевых папках;
- первое место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы;
- третье место по показателям программ-вымогателей, червей, майнеров обеих категорий.

Инжиниринг и интеграторы АСУ

Юго-Восточная Азия находится на третьем месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди регионов по показателям в отрасли Юго-Восточная Азия занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, в почтовых клиентах и сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются веб-майнеры;
- второе место по показателям шпионских программ, вирусов и вредоносных программ для AutoCAD, и третье — по показателям ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- третье место по показателю угроз из интернета;
- третье место по показателю следующих категорий угроз: ресурсы в интернете из списка запрещенных и вредоносные программы для AutoCAD.

Восточная Азия

Основные проблемы кибербезопасности в регионе

Отсутствие или неэффективность мер защиты периметра технологической сети

В Восточной Азии стабильно высокий для региона показатель шпионских программ, в прошлом квартале эта категория угроз даже занимала первое место в рейтинге категорий вредоносного ПО по доле компьютеров АСУ в регионе, на которых оно было заблокировано.

Обнаружение шпионского ПО на компьютере АСУ обычно указывает на то, что вектор первоначального заражения сработал, будь то переход по вредоносной ссылке, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует об отсутствии или о неэффективности мер защиты периметра технологической сети (таких как контроль безопасности сетевых коммуникаций и выполнения политики использования съемных носителей).

Наличие части незащищенной технологической инфраструктуры, которая становится источником вторичного заражения (распространения) вредоносного ПО

В Восточной Азии высокие показатели ПО, распространяющегося через сетевые папки.

По доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, Восточная Азия находится на первом месте среди регионов. Через сетевые папки, как правило, распространяются вирусы и вредоносное ПО для AutoCAD, которые схожи в этом плане, — и те, и другие заражают пользовательские файлы.

В глобальном рейтинге по всем индустриям во всех регионах по показателю вредоносного ПО для AutoCAD сфера строительства в Восточной Азии занимает первое место, нефтегазовый сектор — второе место, а электроэнергетика — четвертое. По показателю угроз, заблокированных при обращении к данным на съемных носителях электроэнергетика в Восточной Азии занимает третье место.

Нефтегазовая, производственная и строительная отрасли в Восточной Азии занимают первые три места в глобальной рейтинге всех индустрий во всех регионах по показателю угроз, заблокированных при обращении к сетевым папкам.

Высокие показатели обнаружения самораспространяющегося ПО на уровне отрасли, страны или региона, вероятно, указывают на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных устройств. Эти незащищенные компьютеры становятся источниками распространения вредоносного ПО.

Ситуацию могут ухудшать и слабая сегментация сети предприятия, и отсутствие контроля использования съемных носителей информации.

Отсутствие контроля использования съемных носителей информации

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Восточная Азия занимает второе место среди регионов, уступая только Африке. Именно на съемных носителях в регионе чаще всего блокируются черви. Распространяются на них и шпионские программы, и вирусы.

Частые попытки заражения защищенных систем при подключении USB-накопителей могут свидетельствовать:

- о низкой степени информатизации предприятия (отсутствии защищенных внутренних систем хранения и передачи файлов);
- о существовании значительной незащищенной части инфраструктуры предприятия, которая является источником заражения накопителей;
- об общей низкой культуре информационной безопасности.

Скорость внедрения мер и средств кибербезопасности уступает темпам развития быстро развивающихся отраслей

По доле компьютеров АСУ, на которых были заблокированы угрозы в отрасли, Восточная Азия в третьем квартале 2025 года лидирует среди регионов по показателю электроэнергетики с 30,01% и отрасли инжиниринг и интеграторы АСУ с 29,31%. По показателю отрасли производство регион находится на третьем месте в соответствующем рейтинге.

Восточная Азия — [крупнейший мировой потребитель электроэнергии](#). Потребление и, соответственно, генерация в регионе [растут практически непрерывно](#). Поэтому неудивительны высокие значения показателя доступности ОТ-систем сектора для киберугроз. Ведь при вводе в эксплуатацию новых объектов адекватные меры киберзащиты обычно применяются с существенным запозданием.

Яркие различия в странах региона

Ситуация с кибербезопасностью в разных странах и территориях региона существенно отличается. Это хорошо заметно, в частности, по рейтингам

стран по показателям компьютеров АСУ, где вредоносные объекты были заблокированы из разных источников:

- Макао и Гонконг лидируют по угрозам из интернета;
- Тайвань и Гонконг — по угрозам из почты;
- континентальный Китай лидирует по угрозам на съемных носителях и в сетевых папках, что обуславливает высокие позиции региона по показателям вирусов и вредоносных программ для AutoCAD.

Что касается рейтингов по категориям угроз, то по угрозам, которые распространяются в интернете и в почте (ресурсы в интернете из списка запрещенных и вредоносные документы), лидирует Гонконг. Монголия традиционно лидирует по показателям майнеров, Макао — по показателям программ-вымогателей.

В рейтингах по остальным угрозам лидирует континентальный Китай.

Япония занимает последние места в большинстве рейтингов.

Особенность квартала

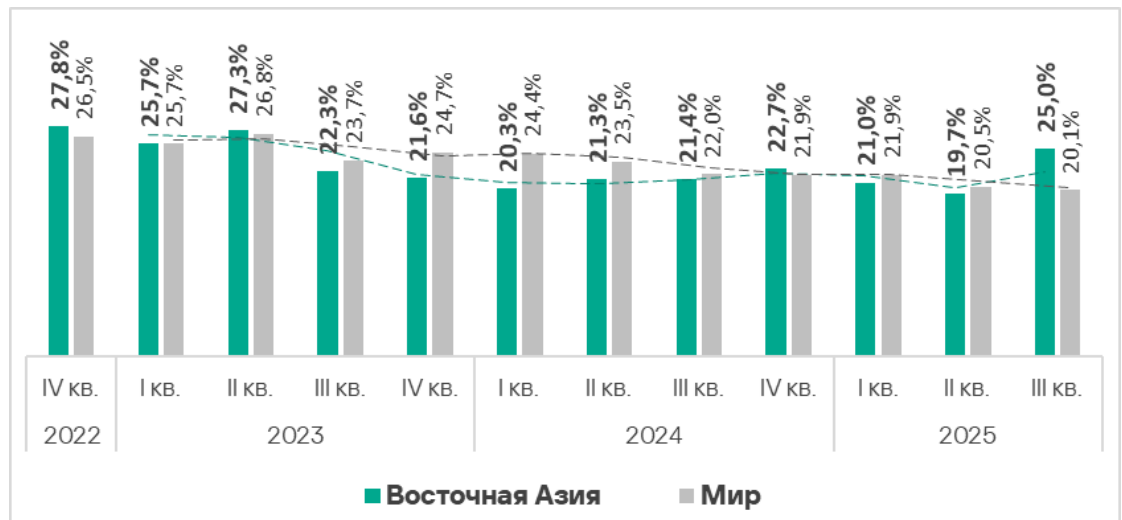
В третьем квартале 2025 года в регионе отмечен резкий рост доли компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы. Рост этого показателя повлиял на позицию региона в рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, – Восточная Азия поднялась с седьмого на третье место.

Столь резкий рост связан с всплеском блокировок вредоносных скриптов на компьютерах в сфере инжиниринга и интеграторов АСУ в континентальном Китае. Вредоносное ПО было обнаружено в памяти кастомизированных клиентских приложений Torrent и MediaGet, а также в папках указанного ПО. Обнаруженные вредоносные скрипты предназначены для кражи информации о системе. Распространение вредоносных скриптов, вероятно, связано с рекламными интеграциями различных приложений, например, в альтернативных инсталляционных пакетах какого-либо ПО, помимо самого приложения, могут также присутствовать другие неясные приложения.

Эти вредоносные скрипты были заблокированы при обнаружении в расшифрованном виде на диске и в памяти уже после проникновения на компьютер, поэтому точный источник этих скриптов не установлен. Как следствие, драматичный рост доли атакованных компьютеров АСУ в Восточной Азии никак не отразился на показателях источников угроз в регионе.

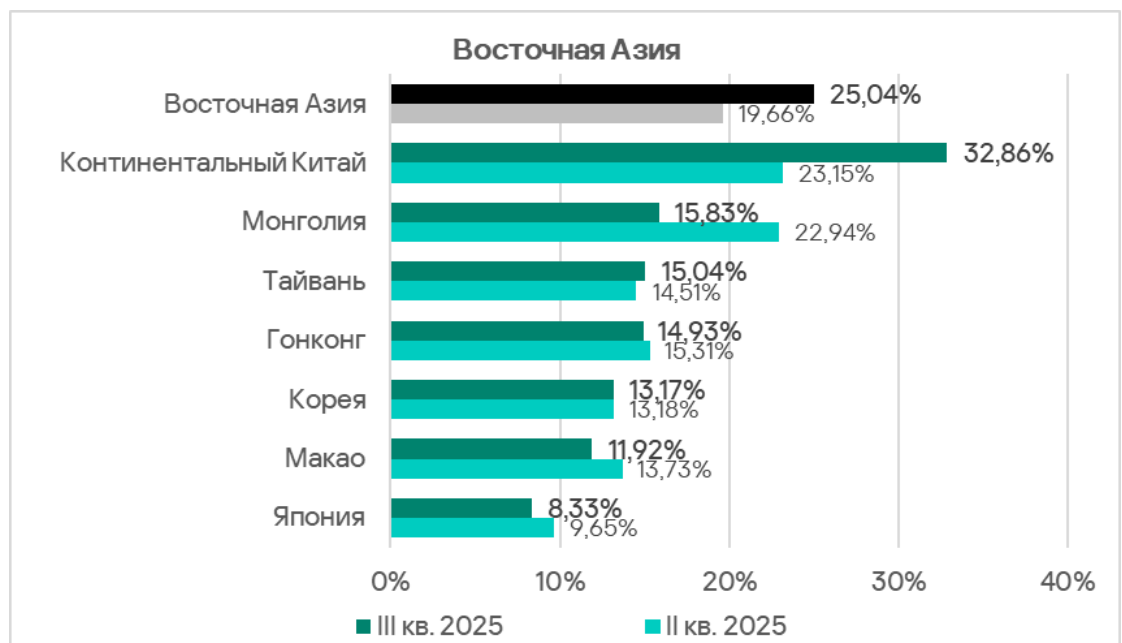
Статистика по всем угрозам

В третьем квартале 2025 года Восточная Азия в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, поднялась с седьмого на третье место. Показатель региона вырос в 1,3 раза – с 19,7% до 25,0%. Это значение превышает минимальный показатель – в Северной Европе – в 2,7 раза.



По росту показателя за квартал (5,3 п. п.) Восточная Азия лидирует с большим отрывом от остальных регионов.

В странах и на территориях региона показатель варьирует от 8,33% в Японии до 32,86% в континентальном Китае.

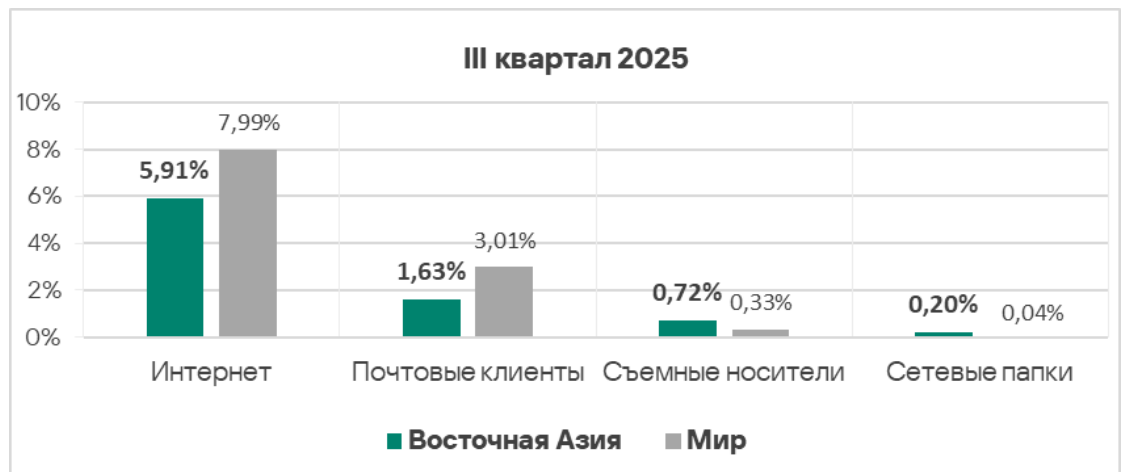


За квартал значения выросли только в континентальном Китае и на Тайване. Но если разница квартальных показателей на Тайване составила 0,53 п. п., то в континентальном Китае — необычно высокие 9,71 п. п. Таким образом, рост показателя Восточной Азии обеспечил в основном континентальный Китай. Как уже было сказано выше, этот рост связан с распространением вредоносных скриптов в сфере инжиниринга и интеграции АСУ.

Источники угроз

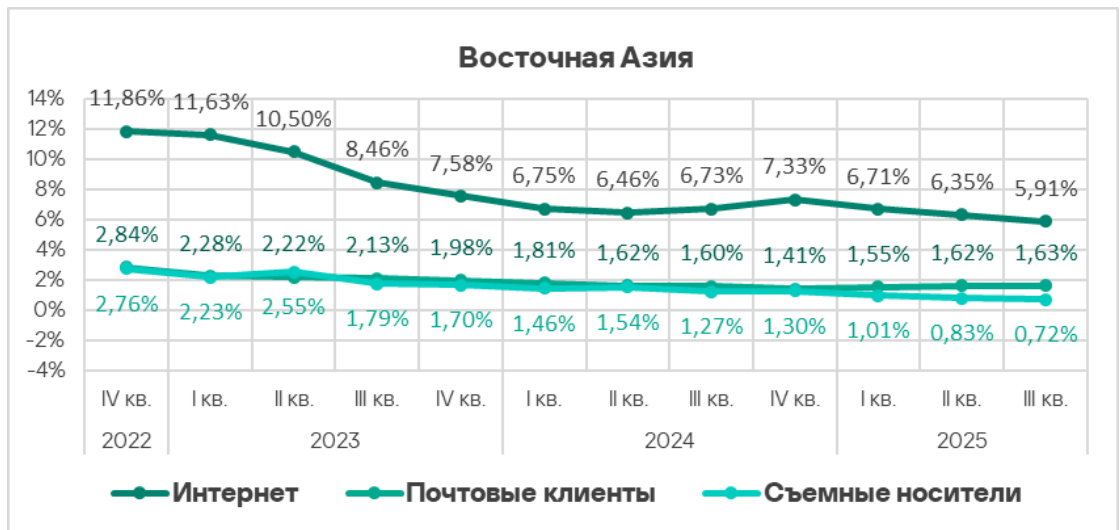
В третьем квартале 2025 года у Восточной Азии выше, чем среднемировые, показатели по двум источникам угроз:

- съемные носители — в 2,2 раза, второе место среди регионов;
- сетевые папки — в 5,0 раза, первое место среди регионов.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз, кроме почтовых клиентов, показатель которых вырос на незначительные 0,01 п. п.

В целом, все основные источники угроз в рамках долгосрочных трендов демонстрируют тенденцию к снижению.

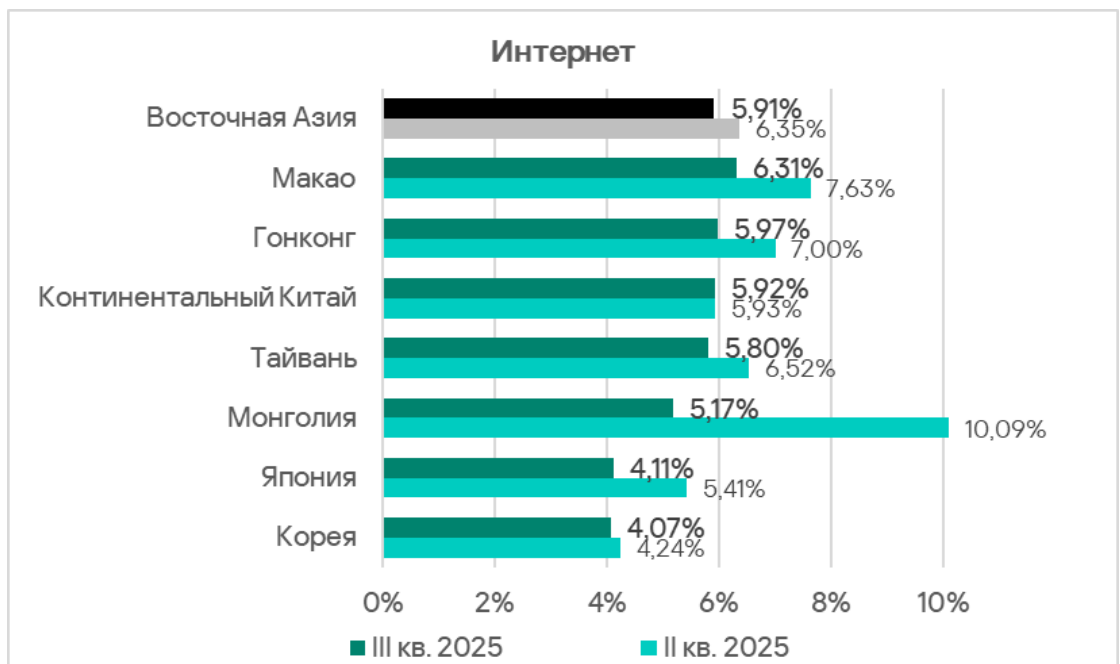


Интернет

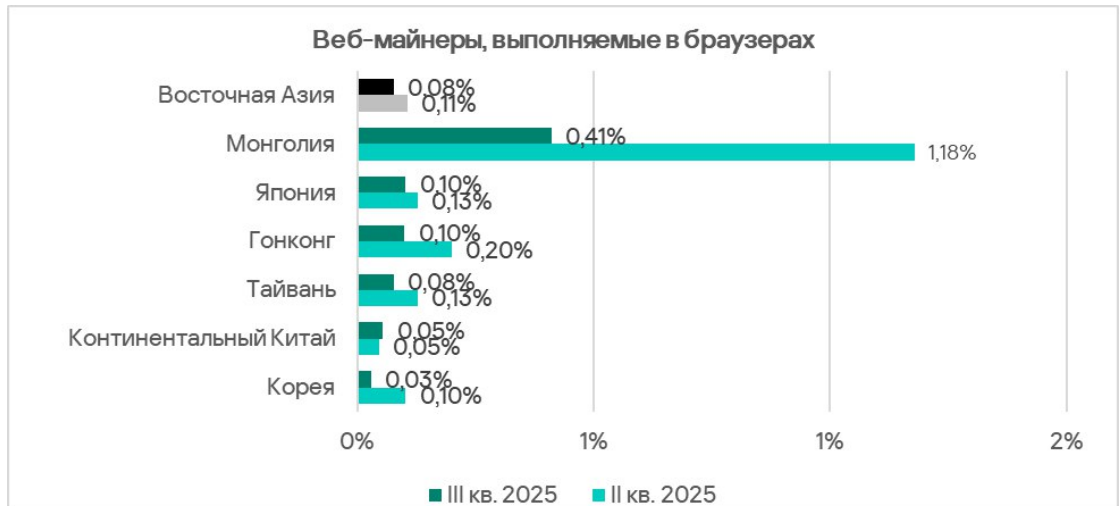
По доле компьютеров АСУ, на которых блокируются угрозы из интернета, Восточная Азия заняла 12-е место в соответствующем рейтинге регионов.

Показатель по угрозам из интернета снижается в регионе третий квартал подряд и достиг наименьшего значения за три последних года — 5,91%. Это больше, чем минимальное среди регионов значение — в Северной Европе — в 1,3 раза.

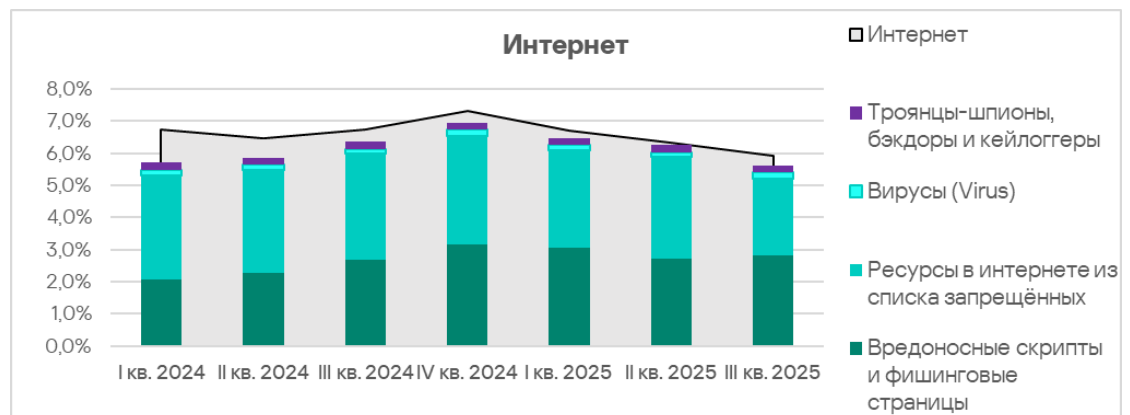
Доля компьютеров АСУ, на которых блокируются угрозы из интернета, в странах и территориях региона варьирует от 4,07% в Корее до 6,31% в Макао.



В Монголии, которая лидировала в аналогичном рейтинге в прошлом квартале, показатель снизился почти вдвое, в том числе из-за резкого падения доли компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и веб-майнеры.



Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вирусы и шпионские программы.

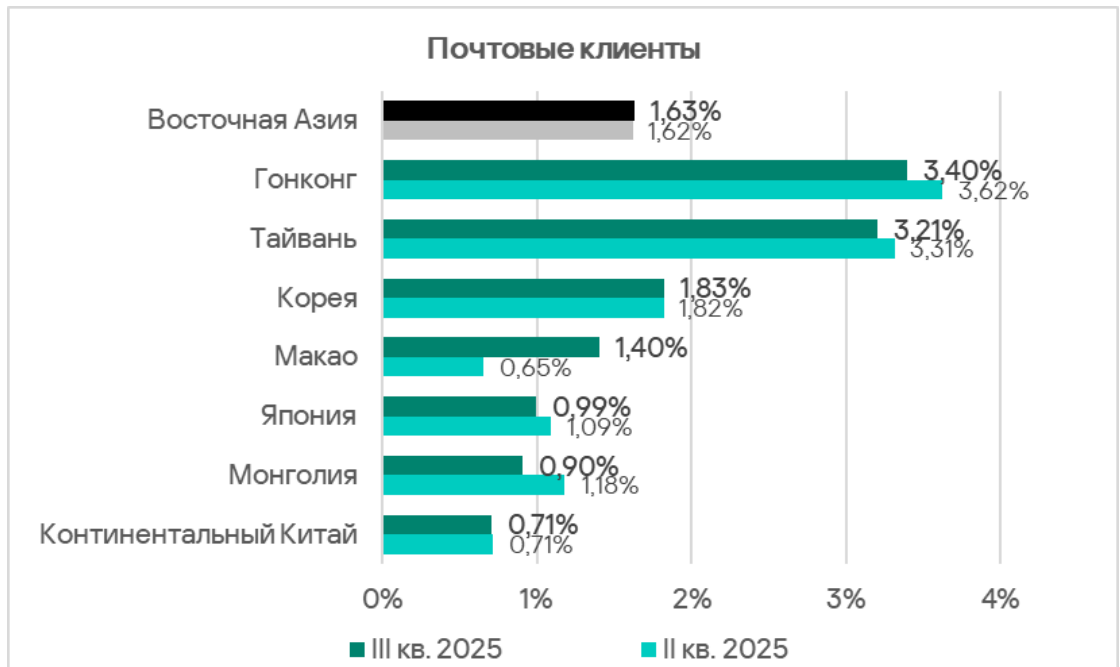


По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в регионе лидирует Гонконг.

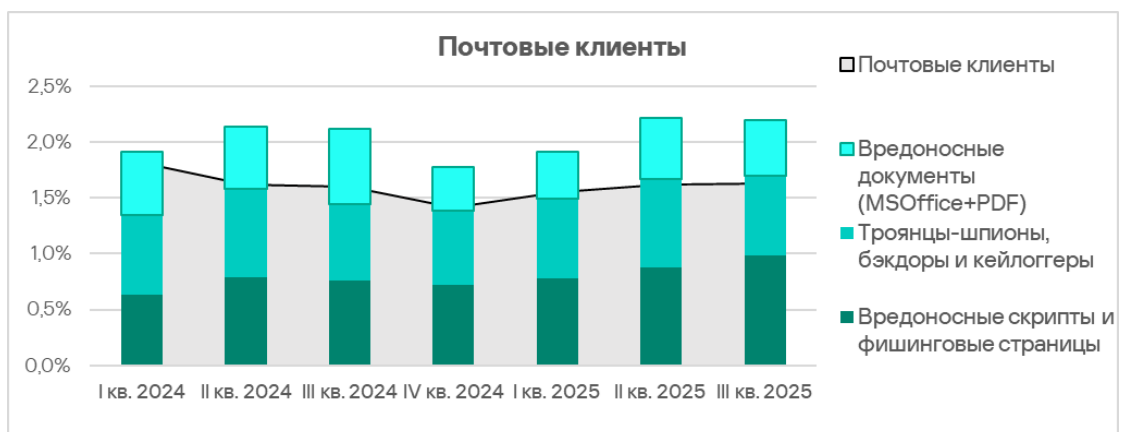
Почтовые клиенты

По доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, Восточная Азия среди регионов занимает 11-е место с 1,63%. Это в 2,1 раза больше, чем в России, где показатель наименьший.

Среди стран и территорий региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидируют Гонконг с 3,40% и Тайвань с 3,21%. Минимальный показатель в континентальном Китае — 0,71%.



Основные категории угроз из почтовых клиентов, заблокированные на компьютерах АСУ, — это вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы. Шпионские программы распространяются во всех источниках угроз, но почта — основной.

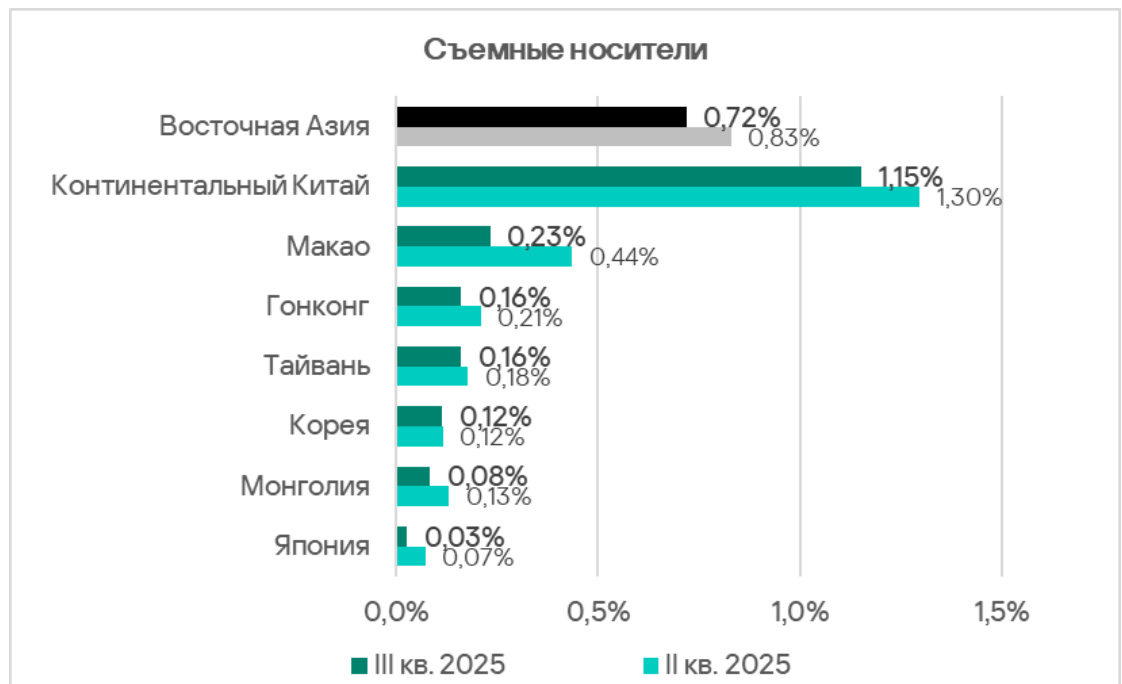


Гонконг лидирует и по показателю угрозы, которая распространяется преимущественно через почту, — вредоносные документы. Показатель этой категории угроз непрерывно растет в Гонконге уже год.

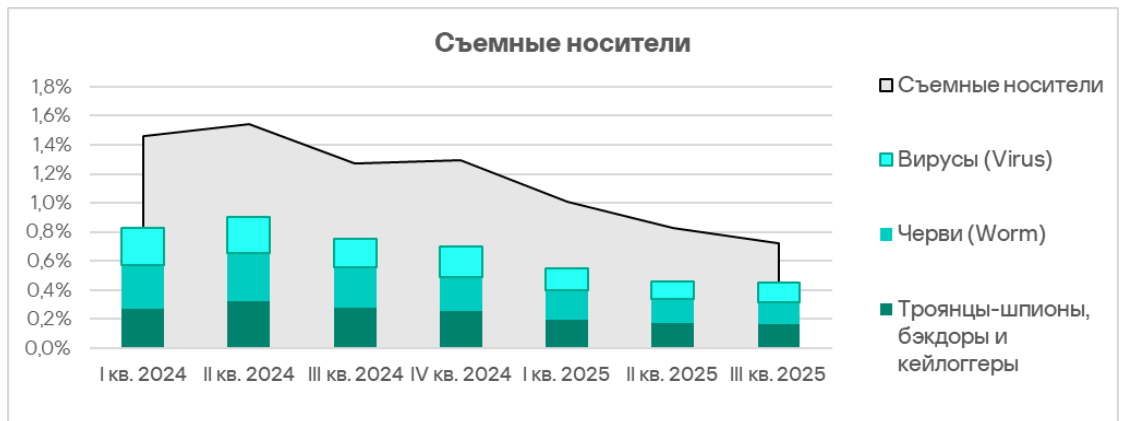
Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Восточная Азия занимает второе место среди регионов, уступая только Африке. Показатель региона (0,72%) – в 14,4 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает этот рейтинг.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует континентальный Китай с 1,15%. Показатели остальных стран и территорий варьируют от 0,03% в Японии до 0,23% в Макао.

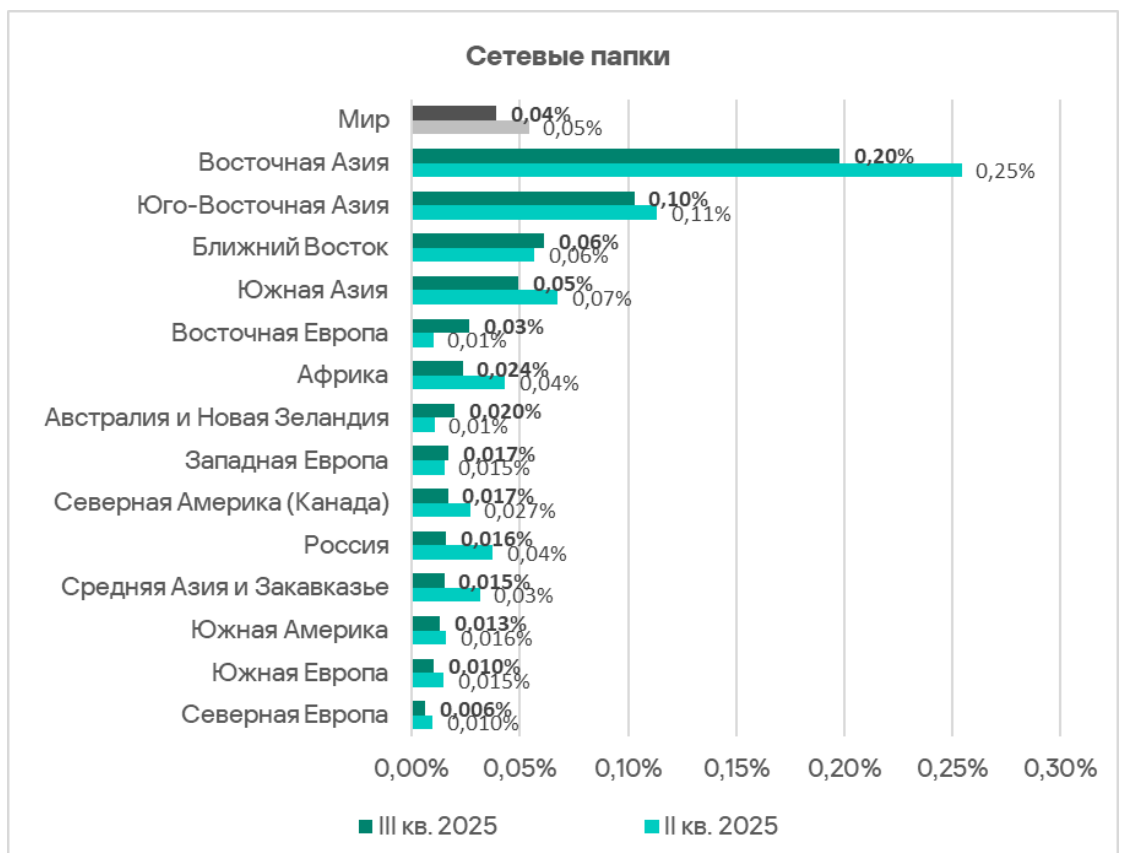


Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ: шпионское ПО, черви и вирусы. Отметим, что континентальный Китай лидирует по показателям всех этих категорий угроз.

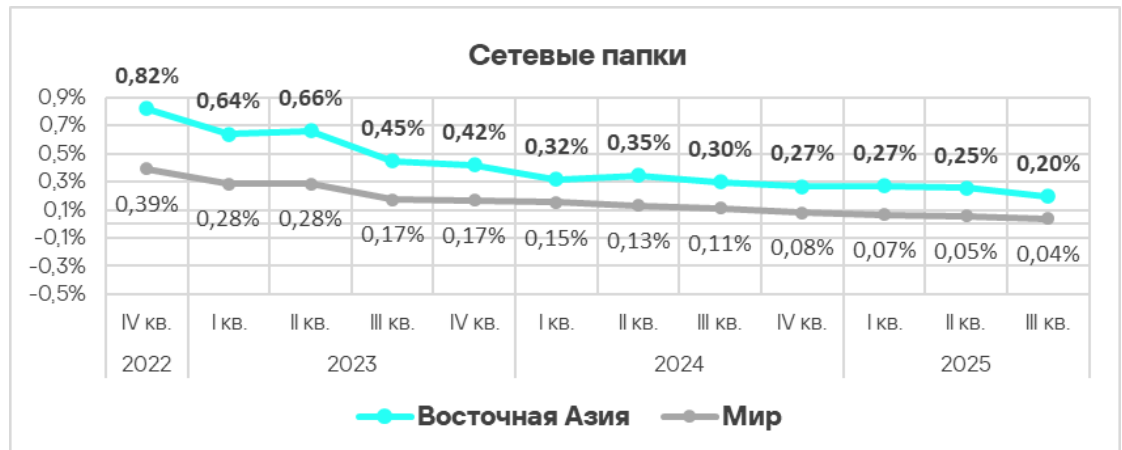


Сетевые папки

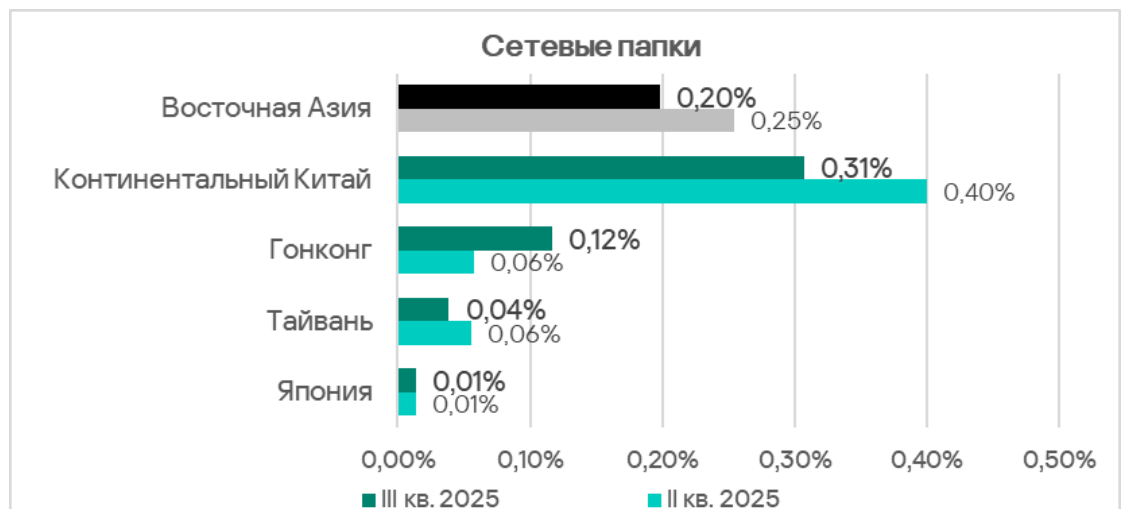
Восточная Азия по-прежнему занимает первое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. В третьем квартале 2025 года показатель региона (0,20%) превышает в 5,0 раза среднемировой и в 33,0 раза показатель в Северной Европе, где он наименьший среди регионов.



Доля компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, в Восточной Азии демонстрирует нисходящий тренд. Показатель в третьем квартале 2025 года был минимальным за последние три года.

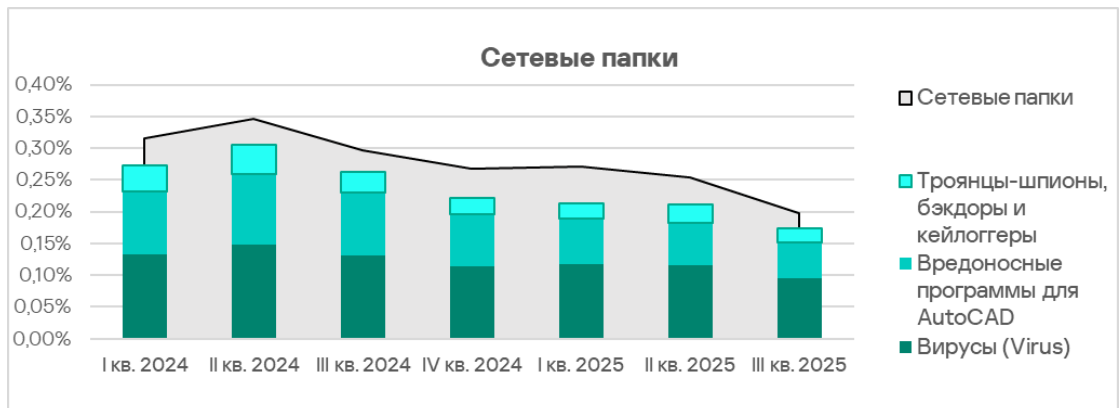


Лидерство Восточной Азии по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, обеспечивает континентальный Китай, лидирующий среди стран и территорий региона с 0,31%.



Отметим, что угрозы в сетевых папках были обнаружены не во всех странах региона.

Основными категориями угроз, которые распространяются через сетевые папки, являются вирусы, вредоносные программы для AutoCAD и шпионские программы.



Вирусы в регионе распространяются через все источники угроз, преимущественно через интернет и съемные носители. Однако показатель сетевых папок для этой угрозы высок и сопоставим с показателем съемных носителей.

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, Восточная Азия находится на втором месте среди регионов. И по вирусам, и по вредоносному ПО для AutoCAD, в регионе лидирует континентальный Китай.

Категории угроз

Как и в большинстве регионов, в третьем квартале 2025 года в Восточной Азии в рейтинге по доле компьютеров АСУ, на которых блокировались угрозы определенной категории, лидируют вредоносные скрипты и фишинговые страницы, потеснившие с первого места шпионские программы. Среди регионов Восточная Азия лидирует по росту показателя категории вредоносные скрипты и фишинговые страницы.



По сравнению со среднемировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы:

- вредоносные скрипты и фишинговые страницы – в 1,4 раза, по этому показателю Восточная Азия занимает второе место среди регионов;
- шпионские программы – в 1,1 раза;

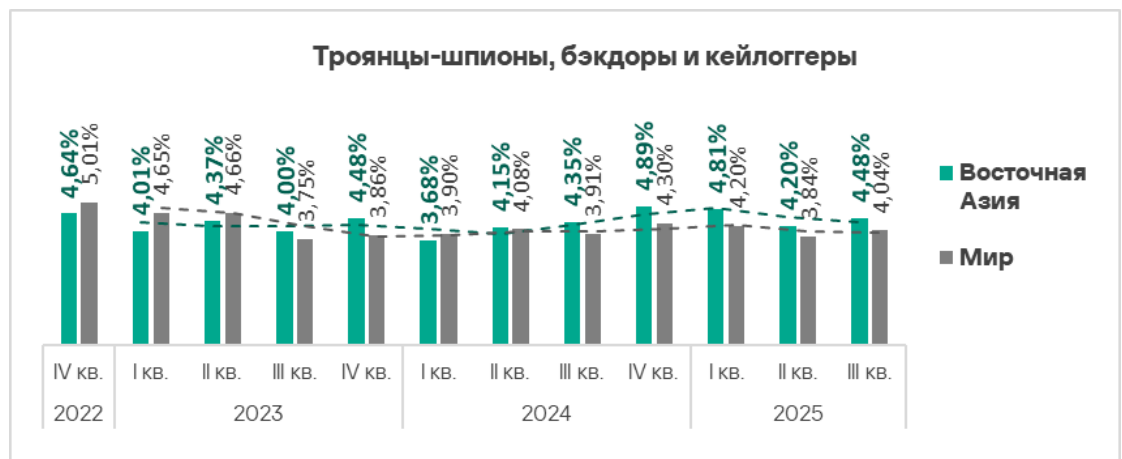
- черви — в 1,2 раза;
- вирусы — в 2,2 раза, третье место среди регионов;
- вредоносное ПО для AutoCAD — в 4,0 раза, второе место среди регионов.

Шпионские программы

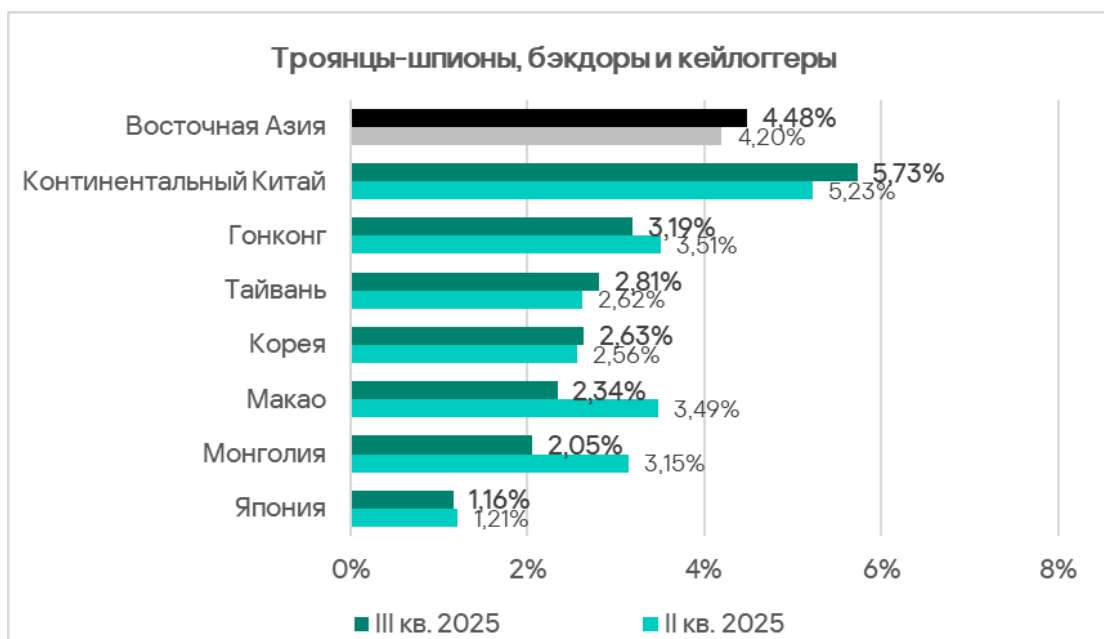
Среди регионов по доле компьютеров АСУ, на которых блокируются шпионские программы, Восточная Азия занимает седьмое место.

Доля компьютеров АСУ, на которых блокируется шпионское ПО, в регионе довольно стабильна и относительно высока, эта категория в прошлом квартале занимала первое место в региональном рейтинге.

Предыдущие два квартала показатель снижался. В третьем квартале 2025 года он подрос до 4,48%. Это в 3,2 раза больше, чем в Северной Европе, где значение наименьшие среди регионов



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются шпионские программы, с отрывом лидирует континентальный Китай с 5,73%. В Японии показатель — наименьший (1,16%).



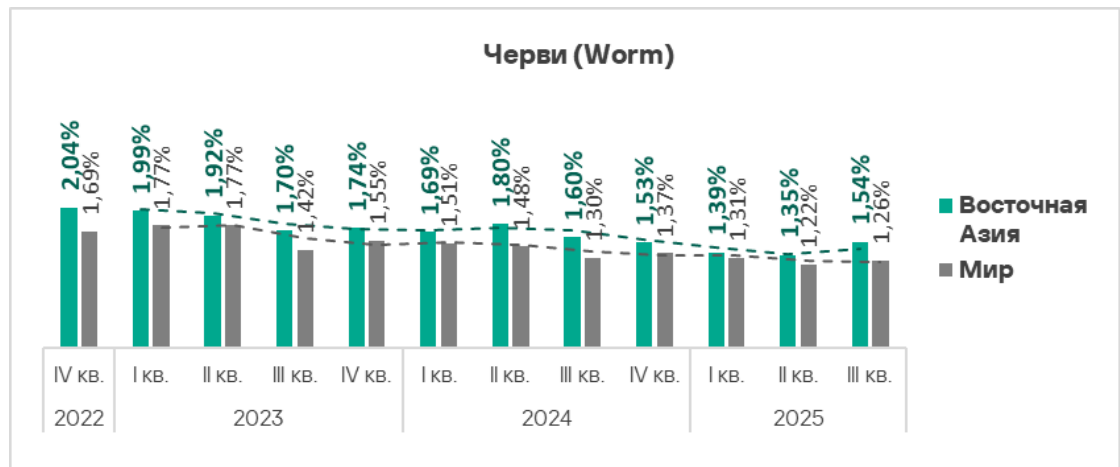
В регионе шпионские программы распространяются через все источники, в третьем квартале 2025 года преимущественно через почтовые клиенты.

Континентальный Китай, который лидирует в этом рейтинге, также находится на первых местах по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей и в сетевых папках. Гонконг и Тайвань лидируют по угрозам из почты.

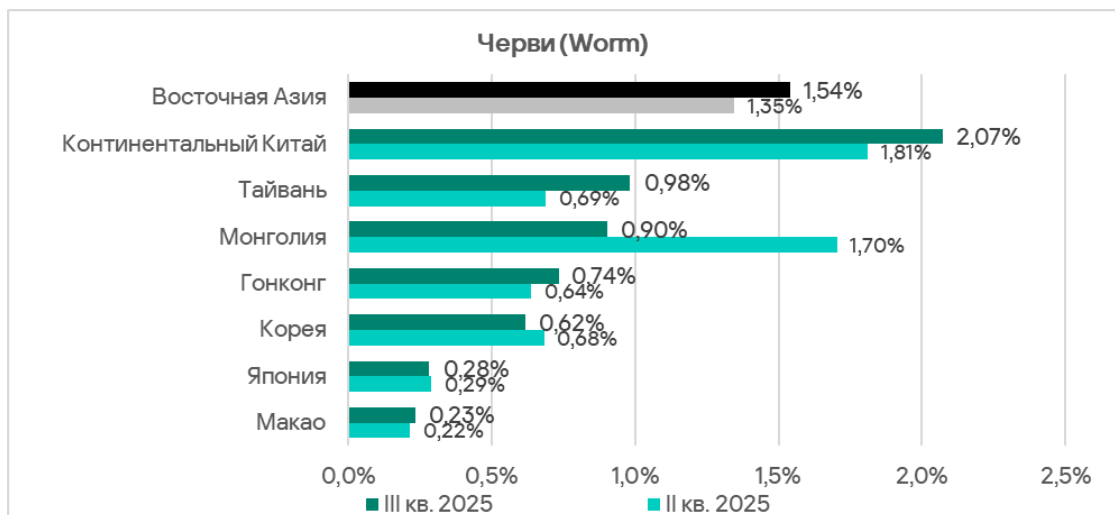
Черви

По доле компьютеров АСУ, на которых блокируются черви, Восточная Азия занимает среди регионов пятое место с 1,54%. Это в 7,0 раза больше, чем в Северной Европе, где показатель наименьший среди всех регионов.

Доля компьютеров АСУ, на которых блокируются черви, в Восточной Азии снижалась три предыдущих квартала, но в третьем квартале 2025 года она подросла до показателя, сопоставимого с показателем четвертого квартала 2024 года.



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются черви, лидирует континентальный Китай с 2,07%. В Монголии, которая в прошлом квартале занимала второе место в этом рейтинге, показатель заметно снизился.



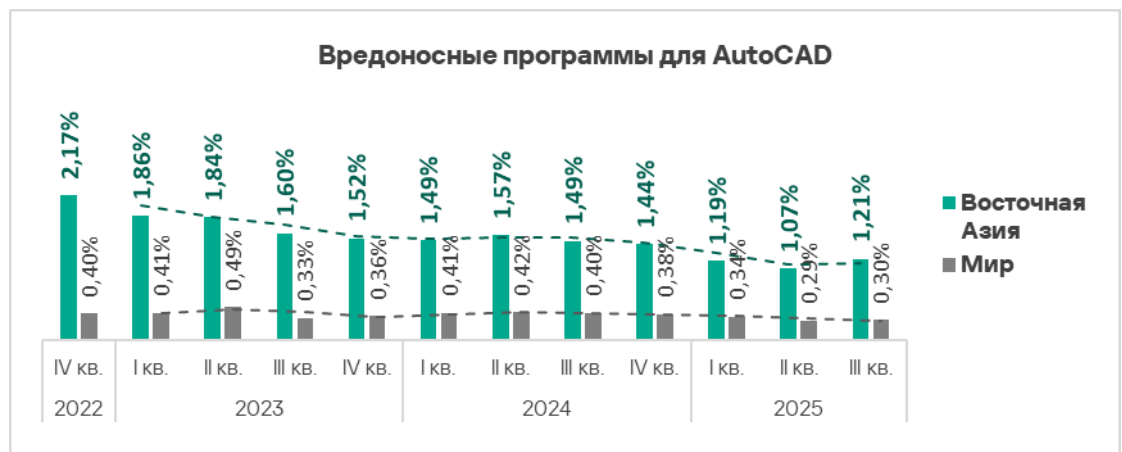
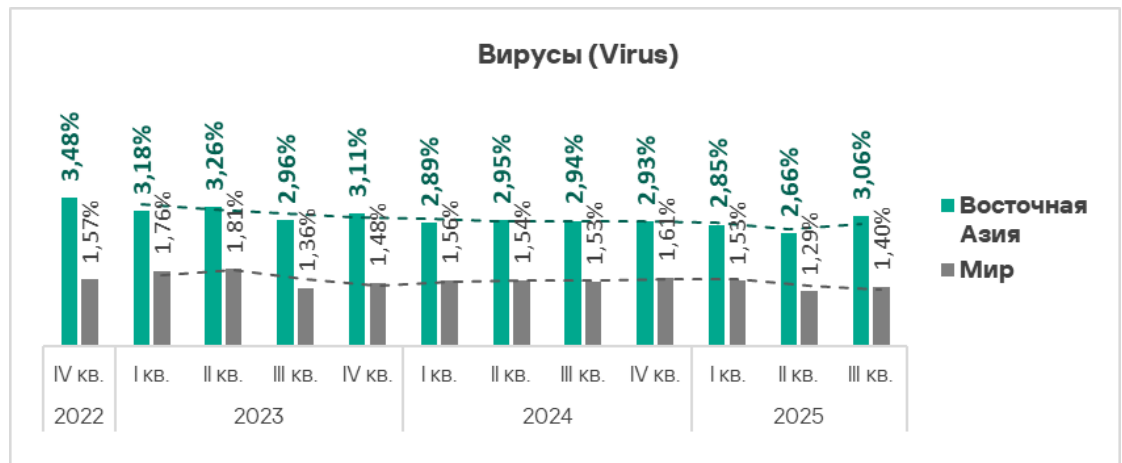
Распространяются черви через все источники угроз, преимущественно на съемных носителях. Континентальный Китай, который лидирует в рейтинге по червям, занимает первое место также по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Вирусы и вредоносные программы для AutoCAD

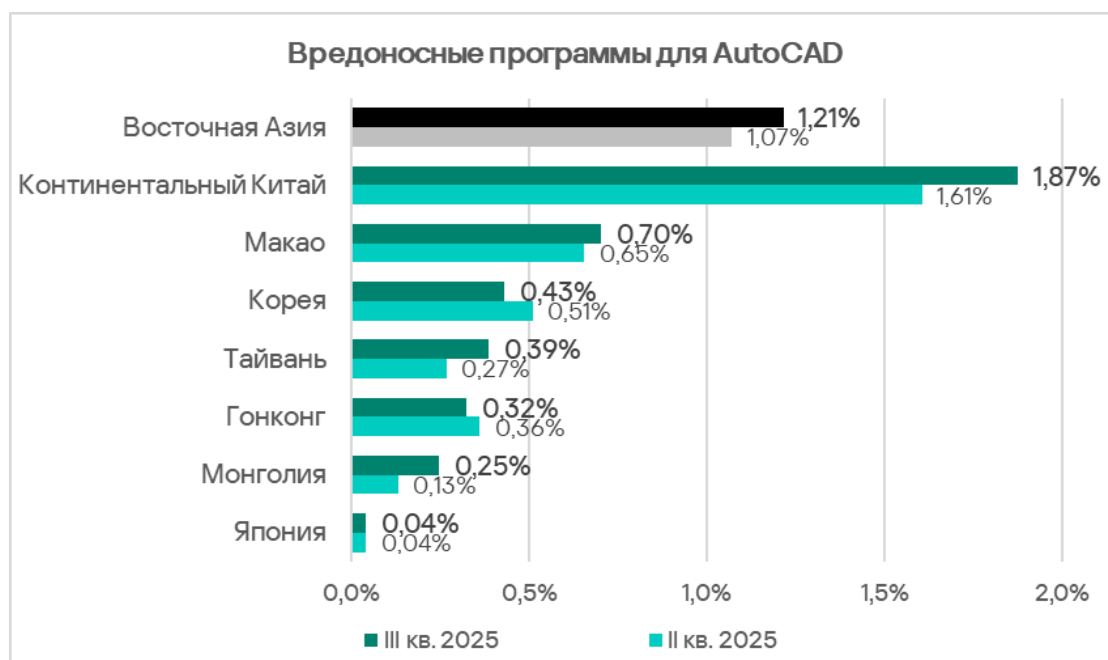
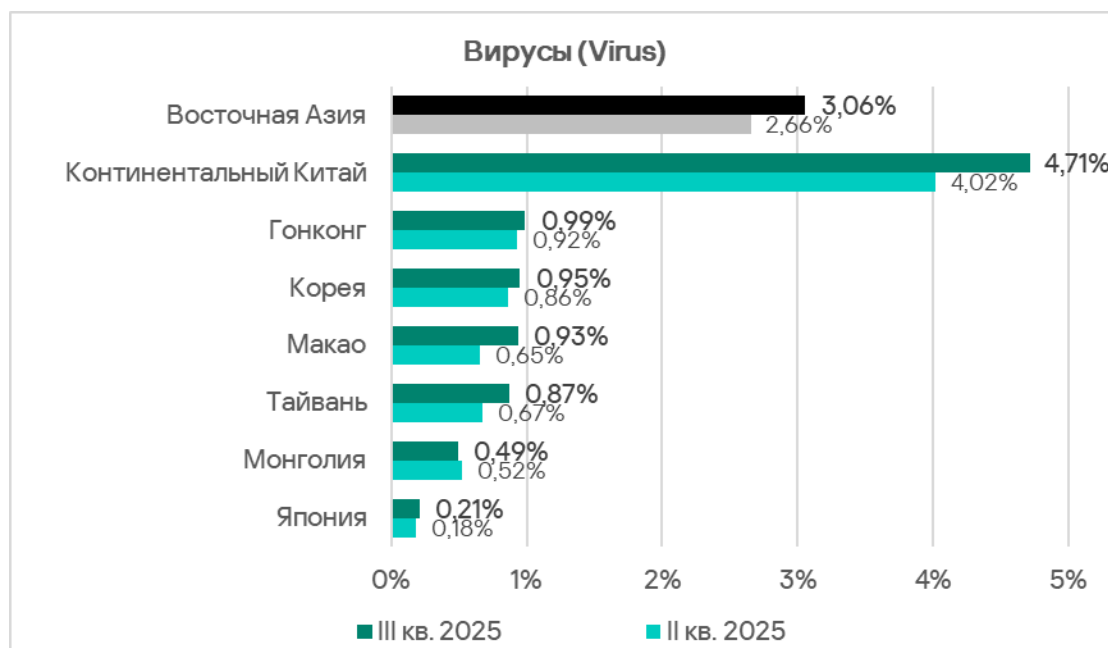
Восточная Азия занимает третье место среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, и второе место по показателям вредоносных программ для AutoCAD, уступая в этом рейтинге только Юго-Восточной Азии.

В Восточной и Юго-Восточной Азии ситуация с вредоносным ПО для AutoCAD схожая: в большинстве случаев оно распространяется так же, как вирусы. Эта особенность объясняет столь высокий процент для этой категории вредоносного ПО.

Показатели обеих категорий за квартал выросли.



Лидерство региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы обеих категорий, обеспечивает континентальный Китай, который лидирует с большим отрывом и по вирусам, и по вредоносным программам для AutoCAD.

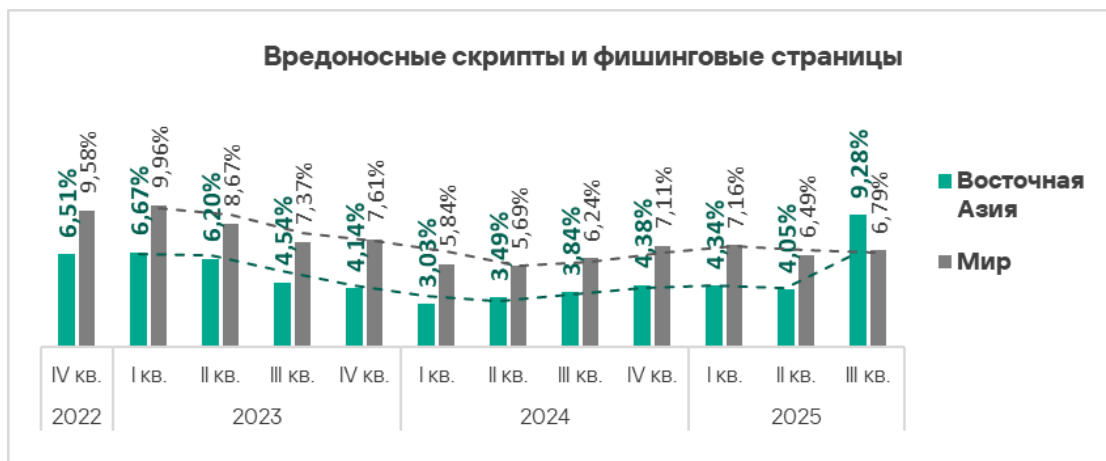


Вирусы в регионе распространяются через все источники угроз. Лидирует как источник вирусов интернет, съемные носители на втором месте, а показатель сетевых папок для этой угрозы сопоставим с показателем почтовых клиентов.

Основной источник вредоносных программ для AutoCAD — сетевые папки. Континентальный Китай лидирует по показателю этого источника угроз.

Угроза квартала: вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Восточная Азия в соответствующем рейтинге регионов поднялась с 13-го на второе (после Африки) место. Показатель в регионе увеличился на 5,23 п. п. и достиг 9,28% — это в 3,6 раза больше, чем в Северной Европе, где он наименьший.



Отметим, что в третьем квартале показатель вредоносных скриптов вырос в восьми регионах, но по его росту Восточная Азия лидирует.

Рост показателя в регионе обусловлен тем, что в континентальном Китае на компьютерах в сфере инжиниринга и интеграторов АСУ распространялись вредоносные скрипты-шпионы, обнаруженные в контексте кастомизированных клиентов Torrent и MediaGet (в памяти и на диске). В результате доля компьютеров АСУ, на которых была заблокирована эта категория угроз, в континентальном Китае выросла на 8,68 п. п. — до 11,89%, и он с большим отрывом лидирует по этому показателю среди стран и территорий региона.



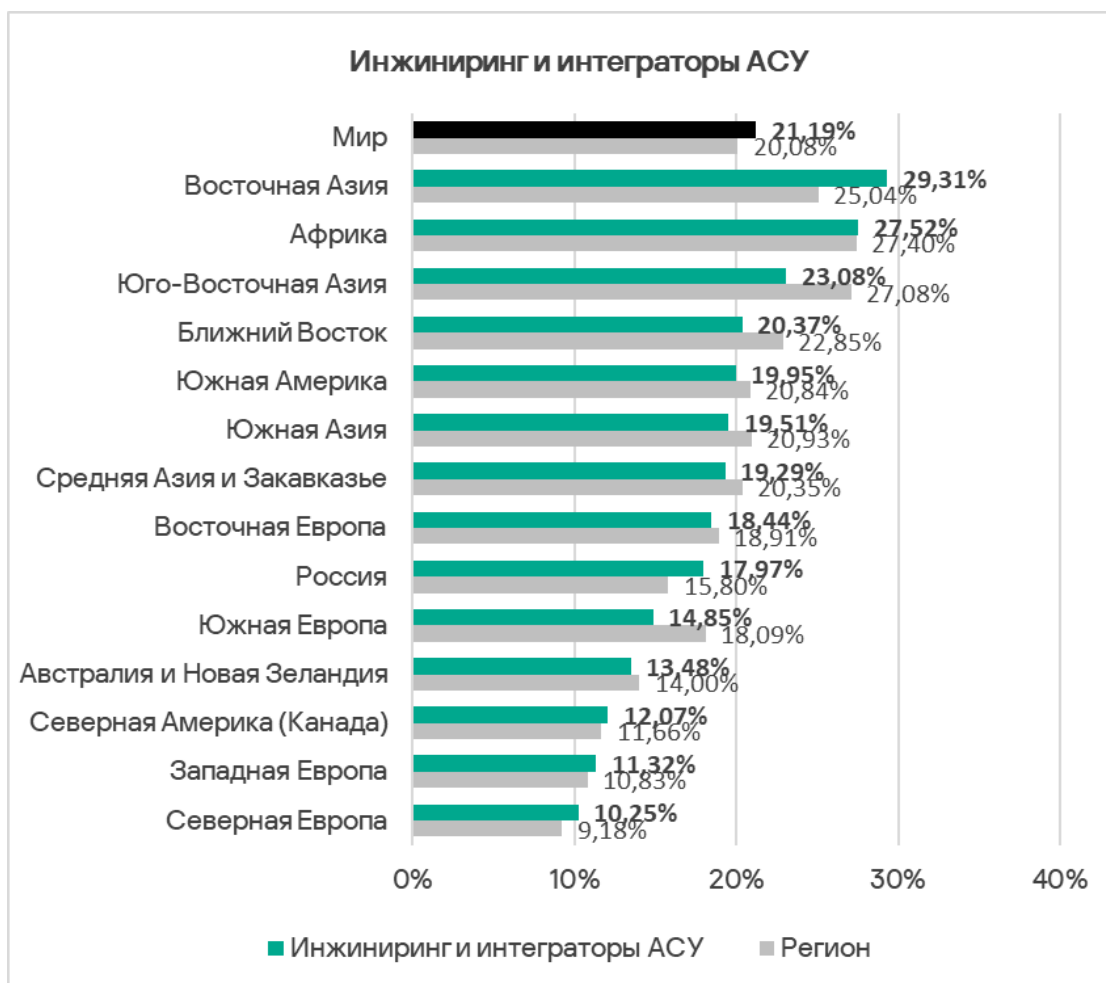
Отрасли

В третьем квартале 2025 года Восточная Азия лидирует среди регионов по показателю двух отраслей: электроэнергетика и инжиниринг и интеграторы АСУ.

Показатель отрасли электроэнергетика в Восточной Азии (30,01%) — в 3,3 раза больше, чем в регионе Северная Америка (Канада), где он наименьший.

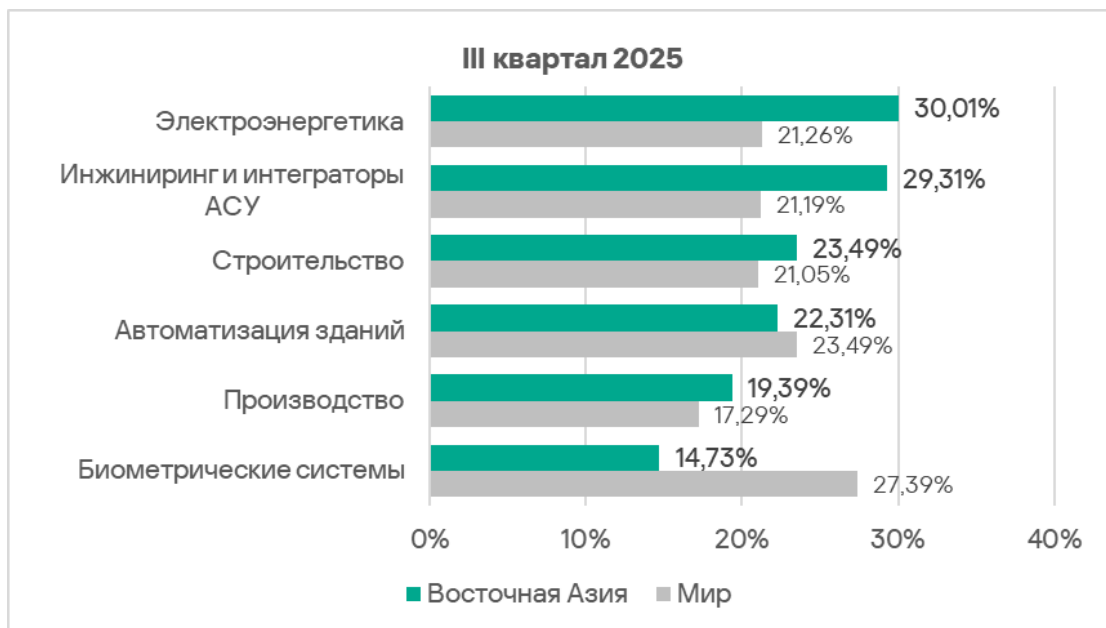


Показатель отрасли инжиниринг и интеграторы АСУ в регионе (29,31%) — в 2,9 раза больше, чем в Северной Европе, где значение наименьшее.



По показателю производственной отрасли Восточная Азия занимает третье место среди регионов.

В Восточной Азии наиболее часто встречающейся с угрозами отраслью из рассмотренных в отчете является электроэнергетика.



По сравнению с соответствующими среднемировыми значениями более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:

- электроэнергетика — в 1,4 раза;
- инжиниринг и интеграторы АСУ — в 1,4 раза;
- строительство — в 1,1 раза;
- производство — в 1,1 раза.

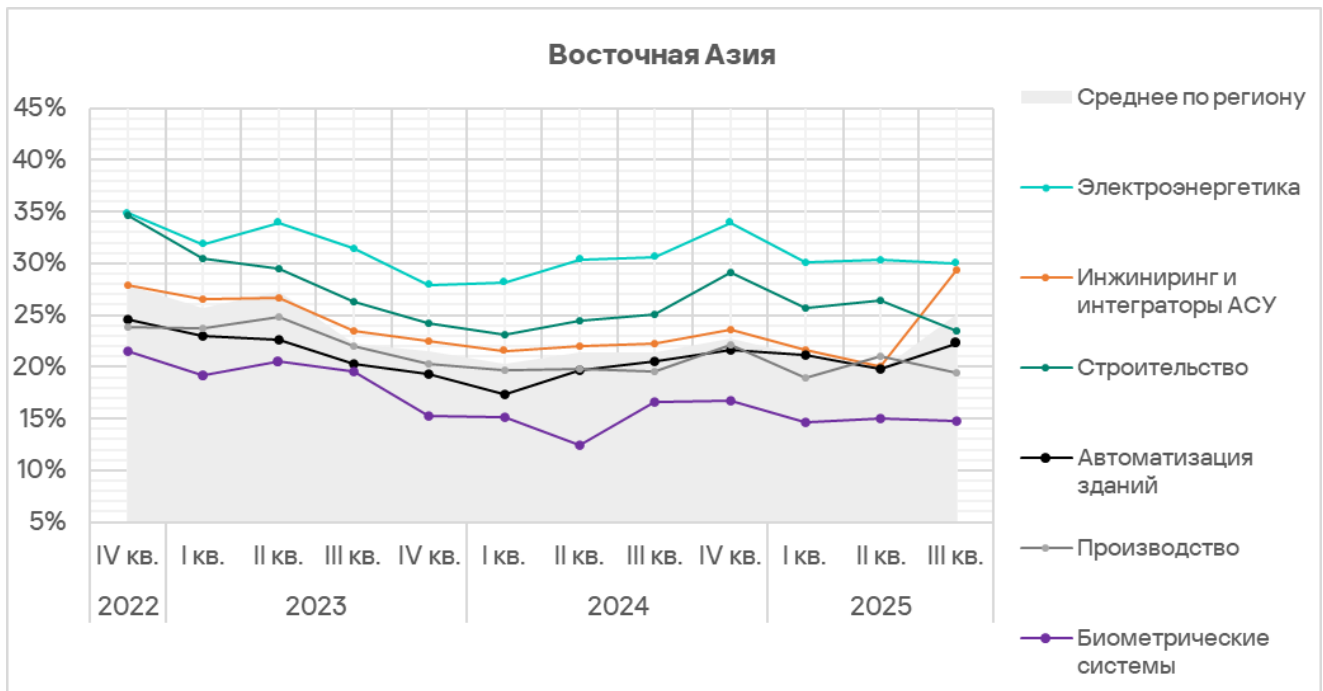
В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась в двух отраслях: автоматизация зданий и инжиниринг и интеграторы АСУ.



Показатель отрасли инжиниринг и интеграторы АСУ вырос на значимые 9,26 п. п. в следствии обнаружения шпионских скриптов, о которых мы упоминали выше. Именно это привело к росту в этой отрасли доли компьютеров АСУ, на которых блокировались угрозы.

Самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, сохраняется в электроэнергетике на протяжении всего рассматриваемого периода. При этом ее значение существенно превышает не только среднее по региону, но и среднемировое. Эта отрасль в регионе активно развивается, а при вводе в эксплуатацию новых объектов адекватные меры киберзащиты обычно применяются с заметным запозданием.

Еще одна особенность региона — позиция ОТ-инфраструктуры биометрические системы в рейтинге отраслей. В большинстве регионов она в верхней части рейтинга, а в Восточной Азии замыкает его.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

Показатели источников угроз в отраслях в Восточной Азии, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	4,40%	6,08%	8,84%	5,92%	7,91%	6,65%	5,91%
Почтовые клиенты	4,84%	3,02%	1,06%	1,62%	1,93%	1,59%	1,63%
Съемные носители	0,00%	0,88%	1,78%	0,64%	0,80%	1,29%	0,72%
Сетевые папки	0,00%	0,24%	0,34%	0,21%	0,46%	0,50%	0,20%
Показатель отрасли в регионе	14,73%	22,31%	30,01%	29,31%	23,49%	19,39%	

Показатели категорий угроз в отраслях в Восточной Азии, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	1,10%	2,30%	4,04%	2,63%	3,03%	6,82%	2,56%
Вредоносные скрипты и фишинговые страницы	6,81%	5,93%	6,68%	12,86%	6,65%	8,64%	9,28%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,71%	6,44%	8,98%	4,32%	4,41%	8,18%	4,48%
Черви (Worm)	0,44%	2,30%	3,01%	1,48%	2,98%	2,73%	1,54%
Майнеры - исполняемые файлы для ОС Windows	0,22%	0,32%	0,29%	0,20%	0,30%	0,45%	0,19%
Вредоносные документы (MSOffice + PDF)	2,86%	2,94%	2,95%	1,86%	2,03%	1,36%	1,75%
Вирусы (Virus)	1,54%	2,61%	5,19%	3,73%	3,82%	7,27%	3,06%
Программы-вымогатели	0,22%	0,32%	0,37%	0,15%	0,25%	0,45%	0,15%
Веб-майнеры, выполняемые в браузерах	0,22%	0,16%	0,06%	0,07%	0,20%	0,00%	0,08%
Вредоносные программы для AutoCAD	0,00%	1,20%	2,50%	1,39%	1,39%	6,36%	1,21%
Показатель отрасли в регионе	14,73%	22,31%	30,01%	29,31%	23,49%	19,39%	

Электроэнергетика

Восточная Азия – лидер среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

В глобальном рейтинге по индустриям во всех регионах электроэнергетика в Восточной Азии занимает:

- третье место по показателю угроз на съемных носителях;
- третье место по показателю угроз в сетевых папках;
- третье место по доле компьютеров, на которых блокировалось вредоносное ПО для AutoCAD;
- пятое место по доле компьютеров, на которых блокировалось шпионское ПО.

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях и в сетевых папках;

- первое место по доле компьютеров АСУ, на которых блокируются вредоносные документы, шпионские программы, вредоносные программы для AutoCAD;
- второе место по показателям вирусов и программ-вымогателей, третье — по показателям червей.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и по показателям угроз на съемных носителях, и третье место — по показателям сетевых папок;
- первое место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, вредоносные документы, шпионские программы, черви, программы-вымогатели;
- второе место по показателям вирусов и вредоносных программ для AutoCAD.

Инжиниринг и интеграторы АСУ

Восточная Азия – лидер среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

В глобальном рейтинге по индустриям во всех регионах отрасль инжиниринг и интеграция АСУ в Восточной Азии занимает:

- пятое место по показателю угроз в сетевых папках;
- третье место по доле компьютеров, на которых блокировались вредоносные скрипты и фишинговые страницы.

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, и второе место – по показателю съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются следующие категории угроз: вредоносные скрипты и фишинговые страницы, вирусы, вредоносные программы для AutoCAD;
- третье место по показателям шпионских программ и червей.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- первое место по показателю вредоносных скриптов и фишинговых страниц;
- третье место по показателю вредоносных программ для AutoCAD.

Строительство

Восточная Азия находится на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

В глобальном рейтинге по индустриям во всех регионах строительная отрасль в Восточной Азии занимает:

- второе место по показателю угроз в сетевых папках;
- пятое место по доле компьютеров, на которых блокировались вирусы.

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, и второе – по показателю съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются вредоносные документы и вредоносные программы для AutoCAD;
- второе место по показателям шпионских программ и третье – по показателям вирусов.

Среди отраслей в регионе строительство занимает:

- второе место по угрозам из интернета и угрозам в сетевых папках и третье – по показателю угроз из почтовых клиентов;
- первое место по показателям следующих категорий угроз: вирусы, вредоносные программы для AutoCAD, майнеры обеих категорий;
- второе место по показателям категорий: вредоносные скрипты и фишинговые страницы, шпионские программы, ресурсы в интернете из списка запрещенных.

Автоматизация зданий

Восточная Азия находится на восьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

В глобальном рейтинге по индустриям во всех регионах отрасль автоматизация зданий в Восточной Азии занимает:

- четвертое место по показателю угроз в сетевых папках.

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, и второе – по показателю съемных носителей;

- первое место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по угрозам из почты и третье – по угрозам на съемных носителях.;
- второе место по показателям следующих категорий угроз: вредоносные документы, майнеры – исполняемые файлы для ОС Windows, программы-вымогатели.
- третье место по показателям категорий шпионские программы и черви.

Производство

Восточная Азия находится на третьем месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

В глобальном рейтинге по индустриям во всех регионах производственная отрасль в Восточной Азии занимает:

- первое место по показателю угроз в сетевых папках.

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, и второе – по показателю съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются черви и вредоносные программы для AutoCAD;
- второе место по показателям шпионских программ и вирусов;
- третье место по показателю программ-вымогателей.

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, второе – по показателю съемных носителей и третье – по угрозам из интернета;
- второе место по показателю червей;
- третье место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, вирусы, программы-вымогатели и майнеры обеих категорий.

Биометрические системы

Восточная Азия находится на последнем месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в ОТ-инфраструктуре биометрические системы.

Среди отраслей в регионе ОТ-инфраструктура биометрические системы занимает:

- первое место по угрозам в почтовых клиентах;
- второе место в регионе по показателю веб-майнеров;
- третье место — по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы и вредоносные документы.

Южная Азия

Основные проблемы кибербезопасности в регионе

Отсутствие контроля использования съемных носителей информации.

Наличие части незащищенной технологической инфраструктуры, которая становится источником вторичного заражения (распространения) вредоносного ПО.

Южная Азия занимает третье место среди регионов по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях. Показатель региона превышает среднемировой в 1,9 раза.

Южная Азия находится на четвертом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. Показатель по этому источнику угроз в регионе превышает среднемировое значение в 1,3 раза.

Съемные носители и сетевые папки в регионе становятся источником самораспространяющегося вредоносного ПО, вредоносных программ для AutoCAD и программ-вымогателей.

Южная Азия находится на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, на четвертом — по показателю вредоносных программ для AutoCAD, на третьем — по показателю программ-вымогателей. Эти категории угроз в регионе распространяются через все источники угроз, но преимущественно на съемных носителях.

Высокий уровень угроз из интернета

Южная Азия находится на третьем месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета.

Различия в странах региона

На все показатели региона большое влияние оказывает Индия. Эта страна находится в конце большинства рейтингов по источникам и по категориям угроз с долей атакованных компьютеров АСУ, которая заметно ниже, чем в большинстве других стран региона, и меньше среднего по региону.

Ситуация с кибербезопасностью в Афганистане заметно отличается от других стран региона в отношении контроля подключения съемных носителей. Это заметно по показателям съемных носителей и самораспространяющегося ПО в разных странах — в Афганистане они

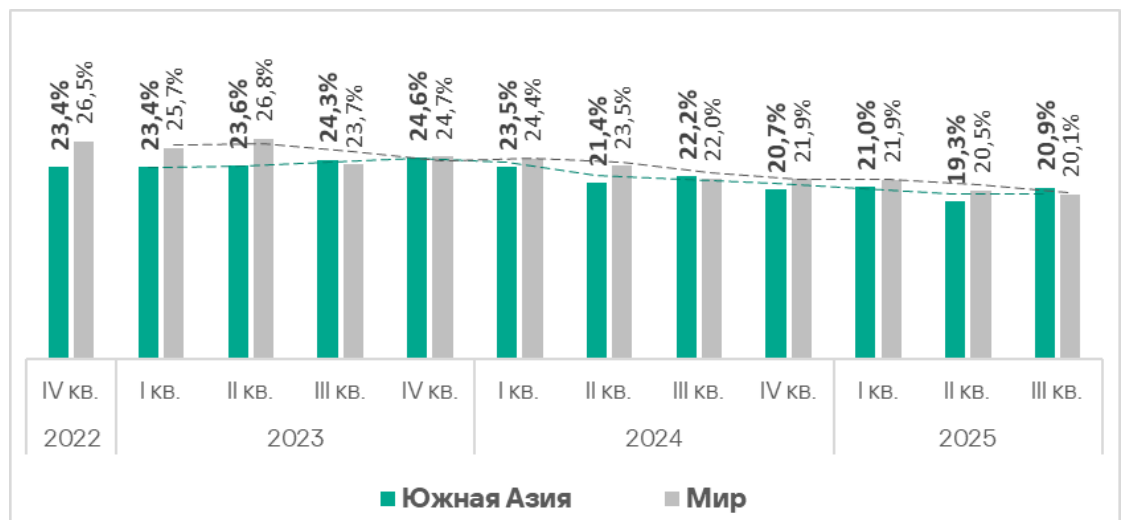
заметно выше, чем в других странах региона. Такая же ситуация в Афганистане и с сетевыми папками.

Статистика по всем угрозам

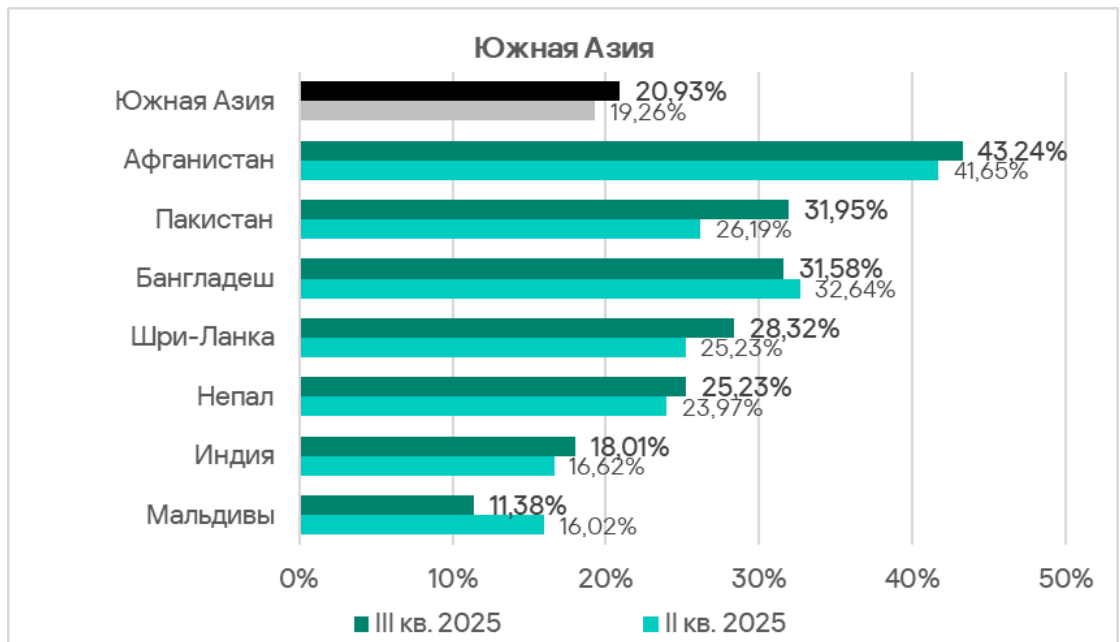
В третьем квартале 2025 года Южная Азия в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, поднялась с девятого на пятое место.

Показатель в регионе за квартал увеличился на 1,6 п. п. до 20,9%. Это в 2,3 раза больше, чем в Северной Европе, которая замыкает этот рейтинг.

Регион демонстрирует плавный нисходящий тренд с некоторыми колебаниями.



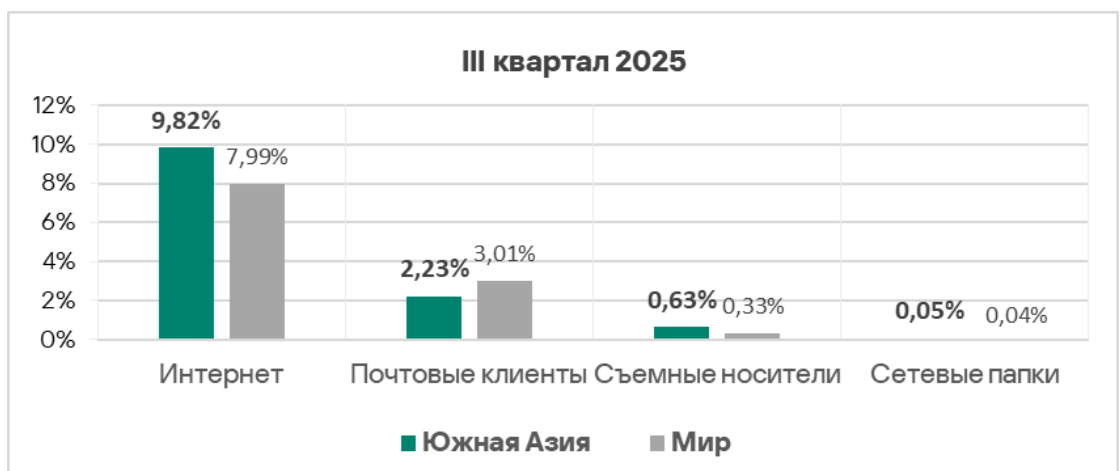
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 11,38% на Мальдивах до 43,24% в Афганистане. Показатель за квартал вырос во всех странах, кроме Бангладеш и Мальдив.



Источники угроз

В третьем квартале 2025 года у Южной Азии выше, чем среднемировые, показатели по всем источникам угроз, кроме почтовых клиентов:

- интернет — в 1,2 раза, третье место среди регионов;
- съемные носители — в 1,9 раза, третье место среди регионов;
- сетевые папки — в 1,3 раза, четвертое место среди регионов.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз.

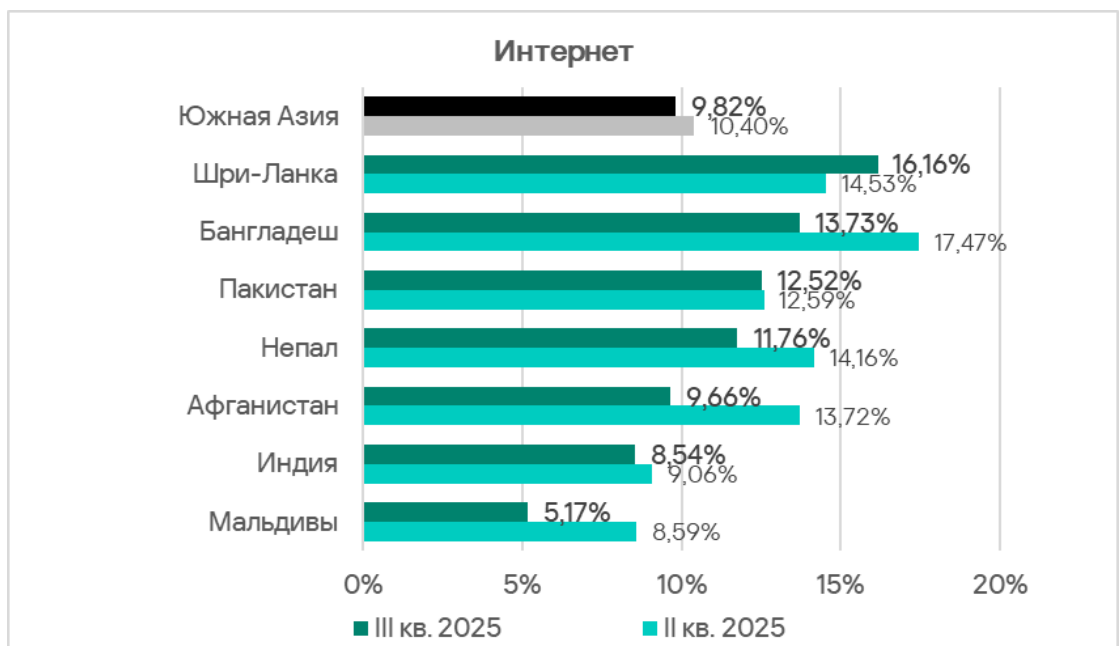
В целом, все основные источники угроз в рамках долгосрочных трендов демонстрируют тенденцию к снижению.



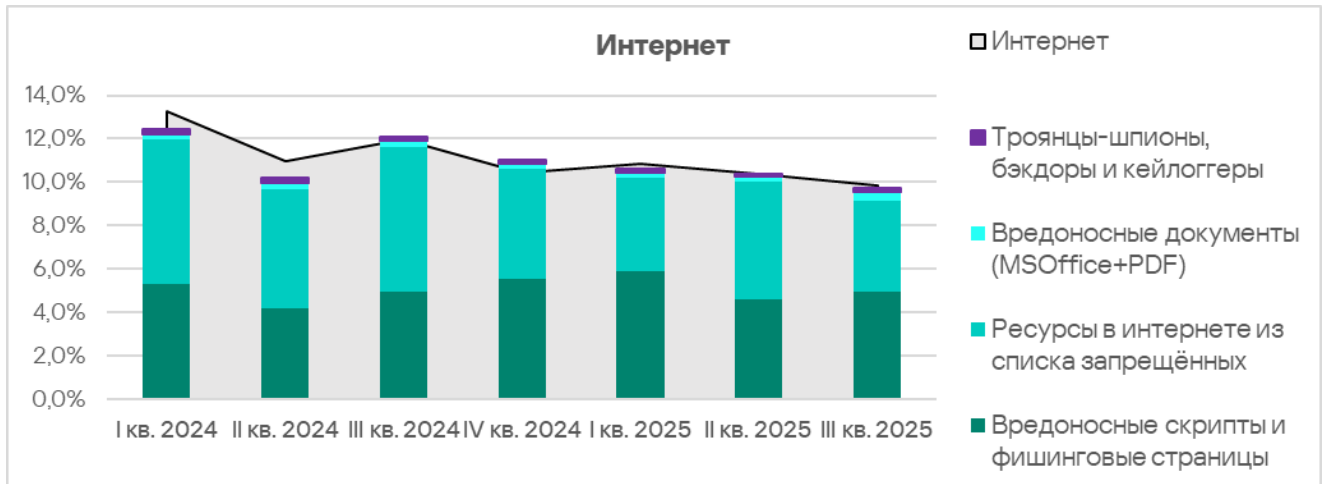
Интернет

В третьем квартале 2025 года Южная Азия по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, заняла третье место среди регионов с 9,82%. Этот показатель в 2,1 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов. Это также наименьший показатель в регионе за последние три года.

Показатели стран региона варьируют от 5,17% на Мальдивах до 16,16% в Шри-Ланке. Шри-Ланка — единственная страна региона, где показатель угроз из интернета за квартал увеличился.



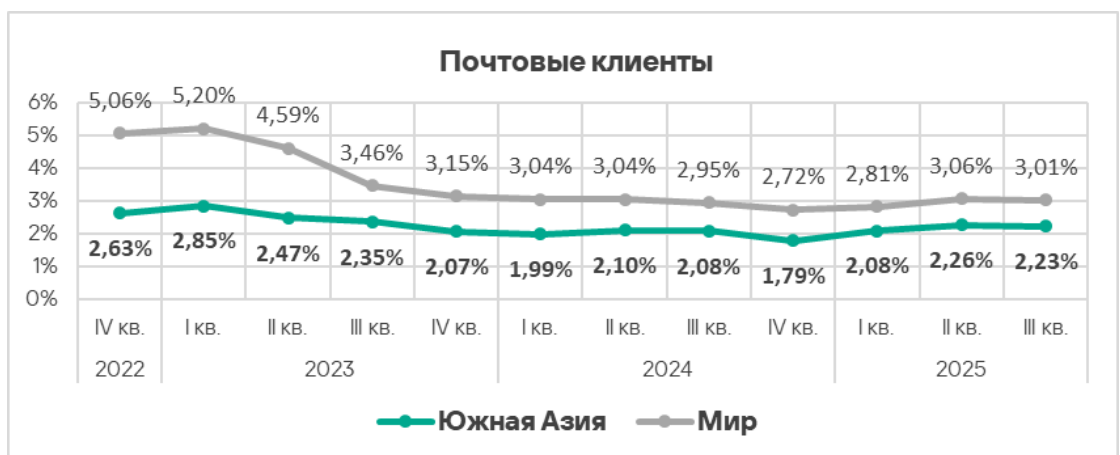
Основные категории угроз из интернета, которые блокировались на компьютерах АСУ в регионе в третьем квартале 2025 года: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вредоносные документы и шпионские программы.



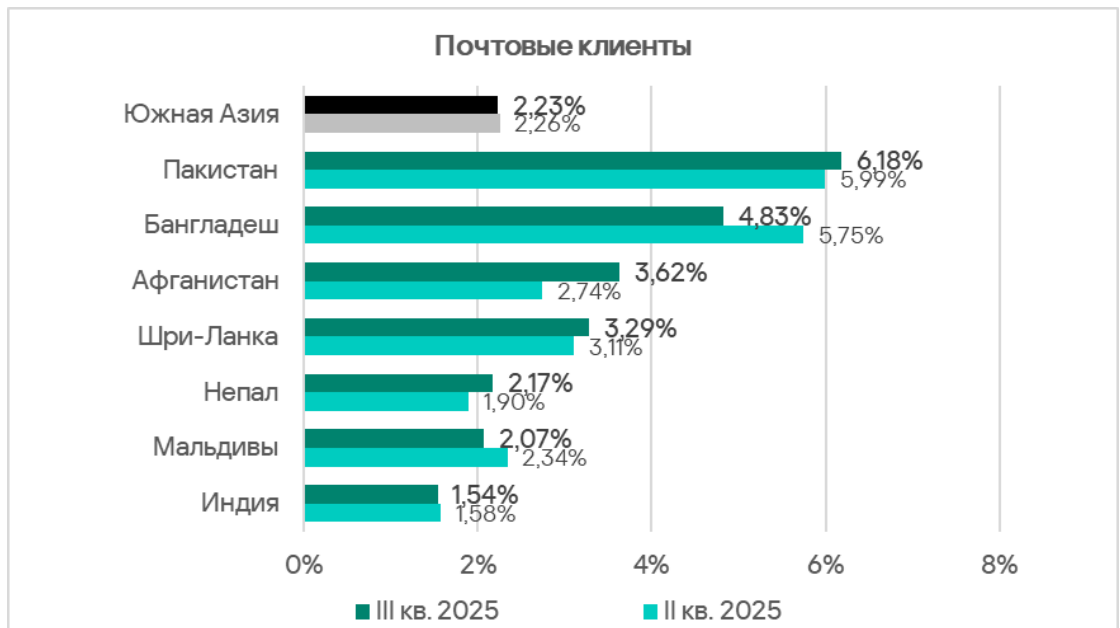
По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в регионе также лидирует Шри-Ланка.

Почтовые клиенты

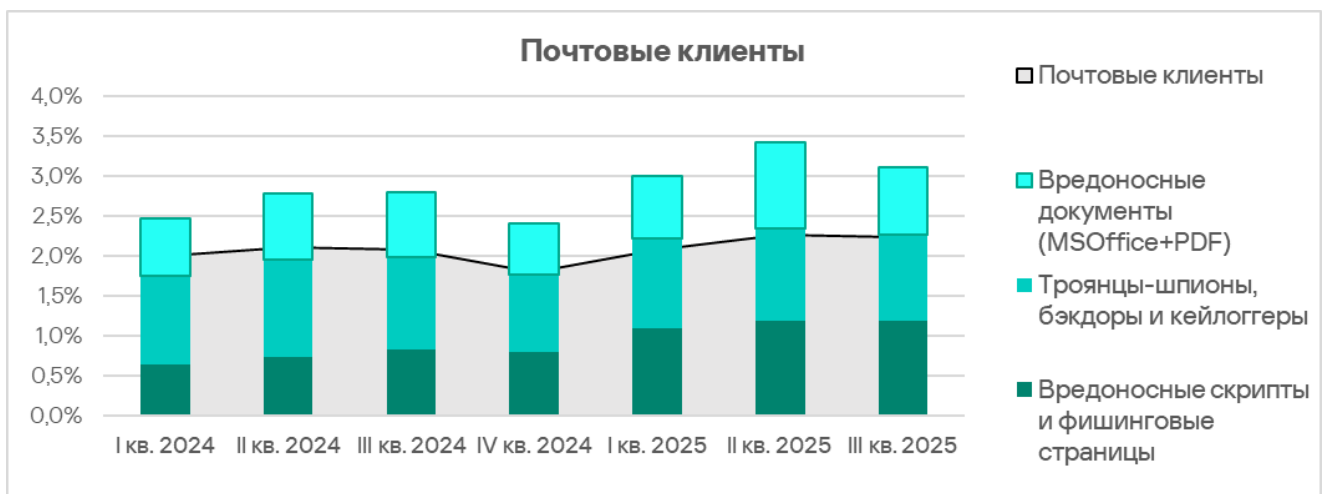
По доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, Южная Азия среди регионов занимает девятое место с 2,23%. Это в 2,9 раза больше, чем в России, где показатель наименьший.



Среди стран региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидируют Пакистан с 6,18% и Бангладеш с 4,83%. Наименьший показатель — в Индии (1,54%). Показатель в Пакистане растет третий квартал подряд.



Основные категории угроз из почтовых клиентов, заблокированные на компьютерах АСУ: вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы.



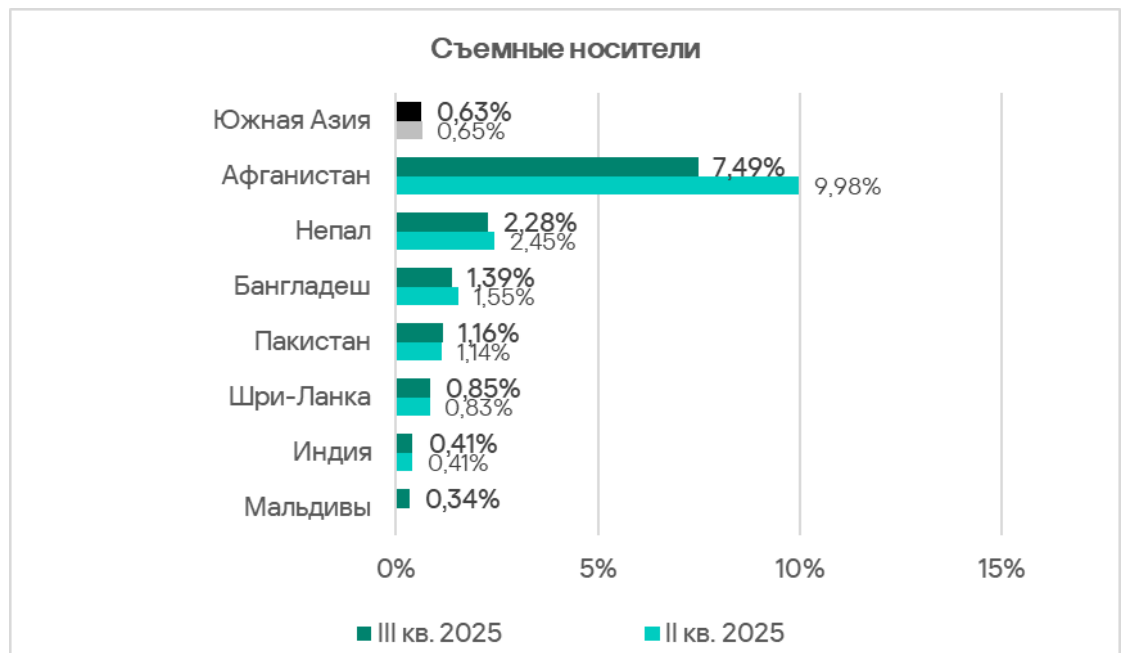
Пакистан и Бангладеш находятся среди лидеров и по показателям угроз, распространяемых через почту. Эти страны лидируют по показателям вредоносных документов, входят в топ-3 по вредоносным скриптам и фишинговым страницам. Бангладеш лидирует по шпионским программам.

Съемные носители

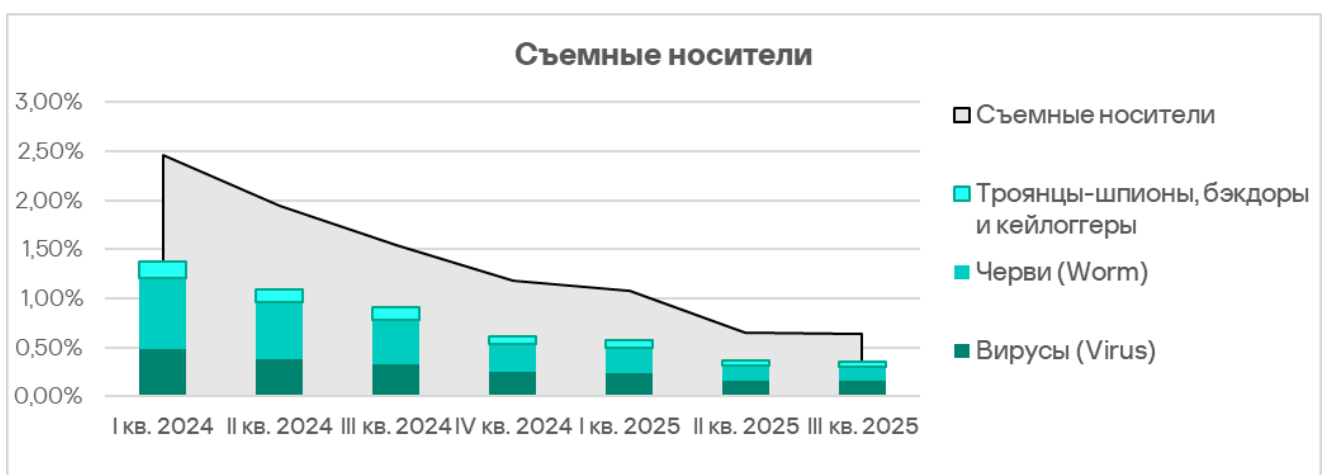
По доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях, Южная Азия заняла третье место среди регионов с 0,63%. Это в

12,6 раза больше, чем показатель в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с большим отрывом лидирует Афганистан с 7,94%. Показатели остальных стран варьируются от 0,34% на Мальдивах до 2,28% в Непале.



Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ: вирусы, черви и шпионское ПО.

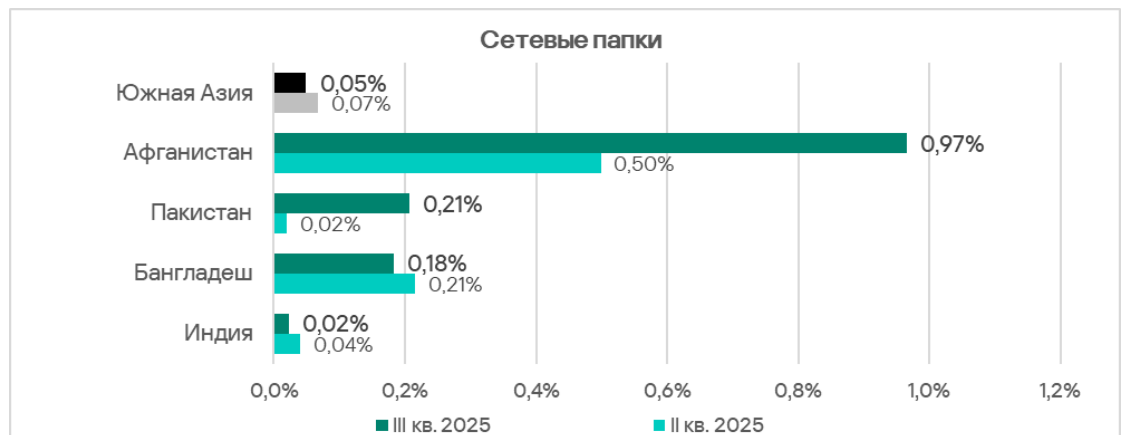


Афганистан также лидирует (и тоже с большим отрывом) по доле компьютеров АСУ, на которых были заблокированы черви.

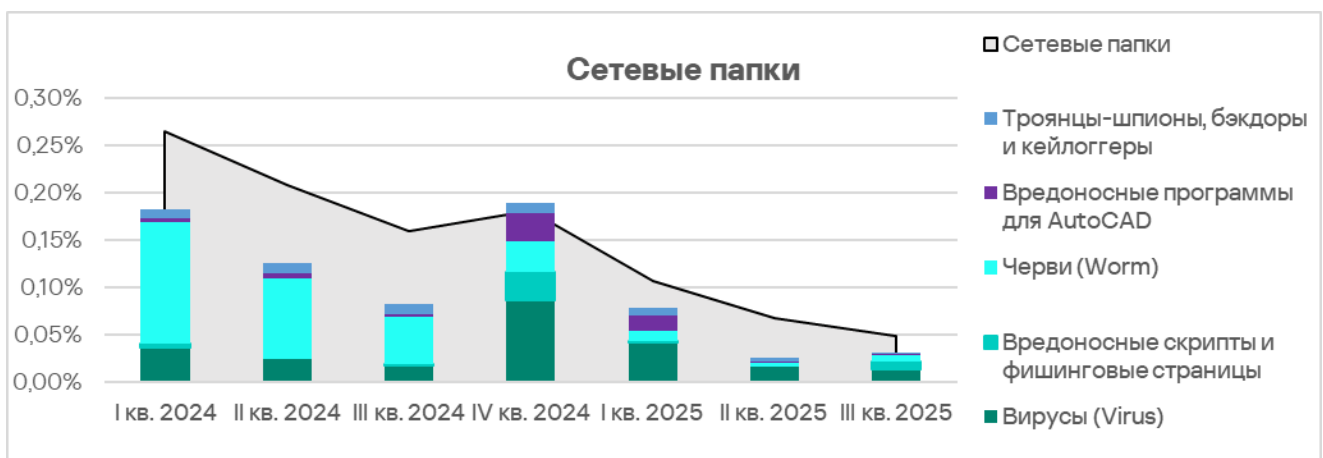
Сетевые папки

Южная Азия занимает четвертое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках с 0,05%. В третьем квартале 2025 года показатель региона превышает в 8,2 раза показатель Северной Европы, которая замыкает соответствующий рейтинг.

Высокую позицию Южной Азии в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, в третьем квартале 2025 года региону обеспечил Афганистан с 0,97%. В Шри-Ланке, которая лидировала по этому показателю во втором квартале 2025 года, в третьем квартале угроз в сетевых папках не обнаружено (как и в Непале).



Основными категориями угроз, которые распространяются в регионе через сетевые папки, в третьем квартале 2025 года стали вирусы, вредоносные скрипты и черви.



Категории угроз

Как и в большинстве регионов, в третьем квартале 2025 года в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были обнаружены, в Южной Азии лидируют вредоносные скрипты и фишинговые страницы. Эта же категория лидирует в регионе по росту показателя за квартал.





По сравнению со среднемировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы:

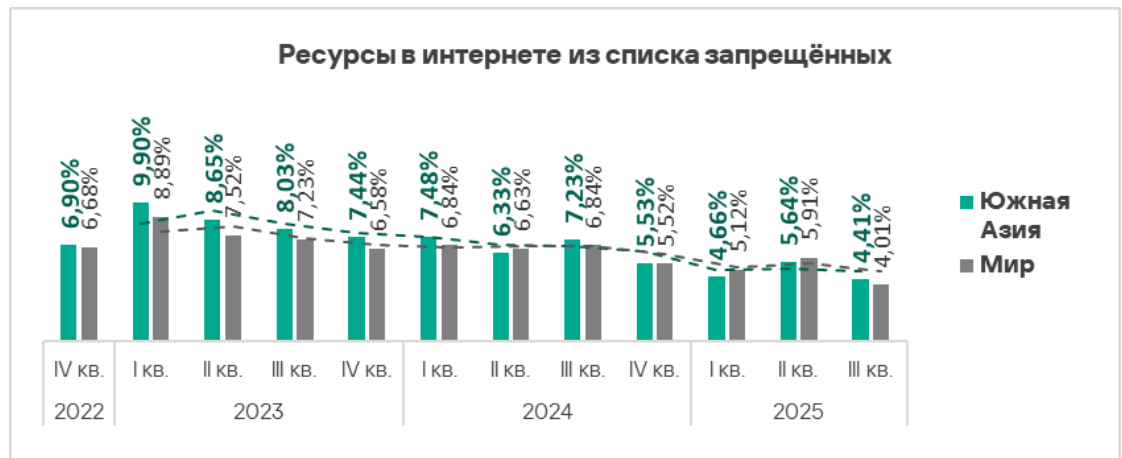
- ресурсы в интернете из списка запрещенных — в 1,1 раза, у Южной Азии третье место по показателю этой категории угроз среди регионов;
- черви — в 1,1 раза;
- вирусы — в 1,3 раза;
- программы-вымогатели — в 1,4 раза, третье место по показателю этой категории угроз среди регионов.

Кроме того, Южная Азия находится на четвертом месте среди регионов по показателю вредоносных программ для AutoCAD.

Ресурсы в интернете из списка запрещенных

Южная Азия занимает третье место среди регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных с 4,41%. Этот показатель в 1,9 раза больше, чем в Австралии и Новой Зеландии, где он наименьший среди регионов.

Динамика показателя в регионе в целом соответствует динамике среднемирового показателя.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, лидирует Шри-Ланка с 6,88%.



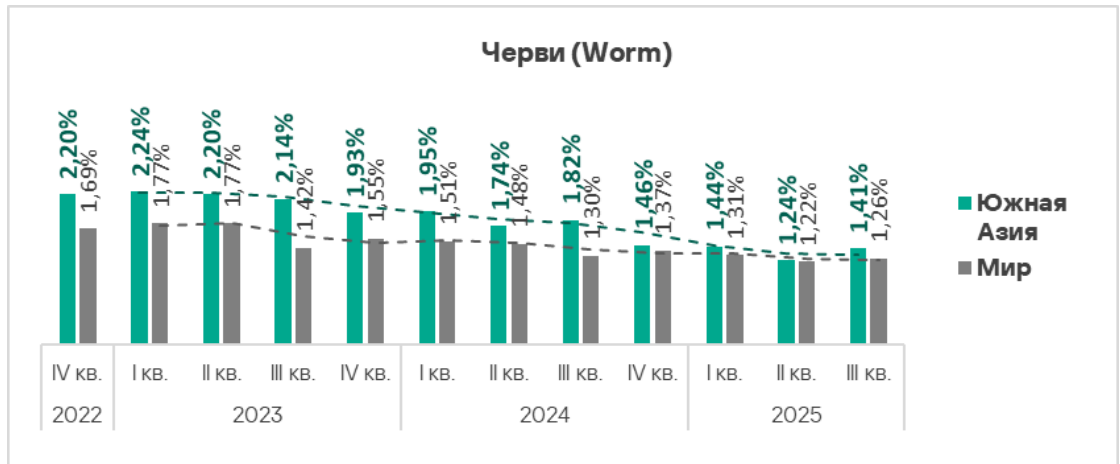
Единственный источник распространения этой категории угроз — интернет. Шри-Ланка также занимает первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета.

Черви

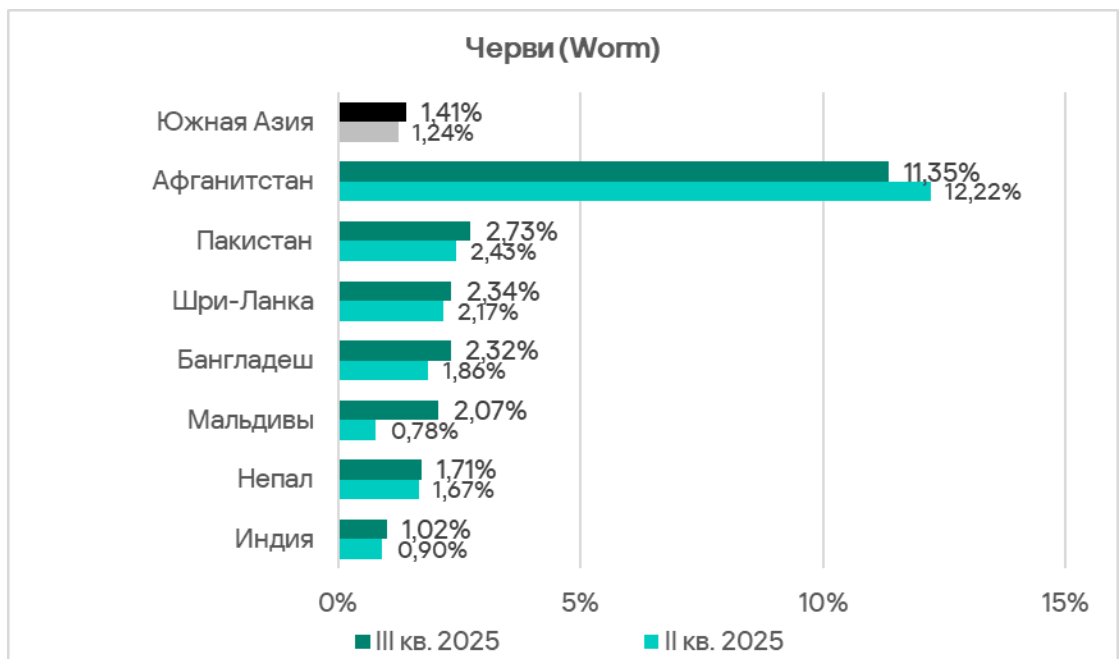
Южная Азия занимает седьмое место среди регионов по доле компьютеров АСУ, на которых были заблокированы черви.

В третьем квартале 2025 года показатель червей в регионе вырос до 1,41% — это в 6,4 раза больше, чем в Северной Европе, где он наименьший среди

регионов. По росту показателя червей Южная Азия занимает третье место среди регионов.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы черви, лидирует Афганистан с огромным для этой категории угроз показателем 11,35%.



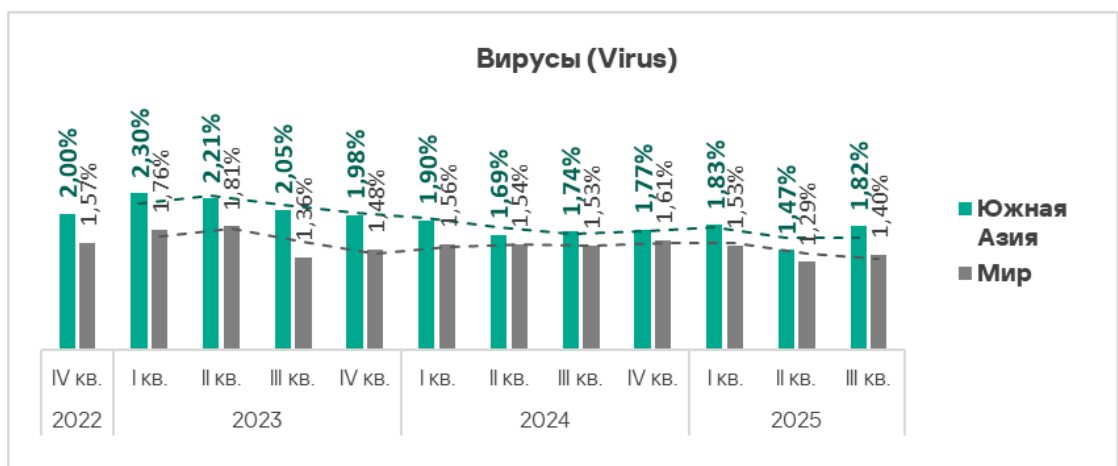
Черви в регионе распространяются через все источники угроз, чаще всего их блокируют при подключении съемных носителей. По показателю этого источника угроз в регионе также лидирует Афганистан, и тоже с большим отрывом от остальных стран.

Вирусы и вредоносные программы для AutoCAD

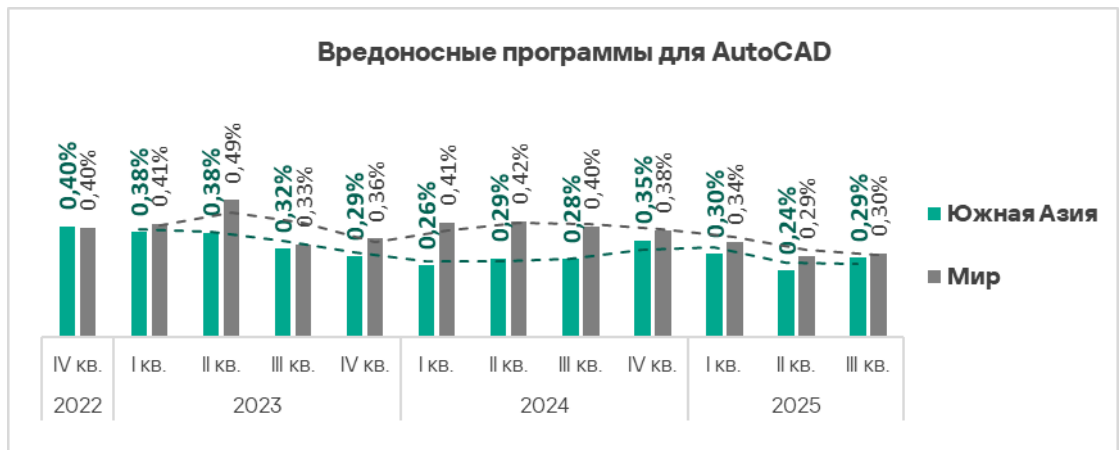
Южная Азия занимает пятое место среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, и четвертое место по показателям вредоносных программ для AutoCAD.

Как и в Восточной и Юго-Восточной Азии, в Южной Азии вредоносное ПО для AutoCAD в большинстве случаев распространяется так же, как и вирусы. Эта особенность объясняет столь высокий процент для этой категории вредоносного ПО.

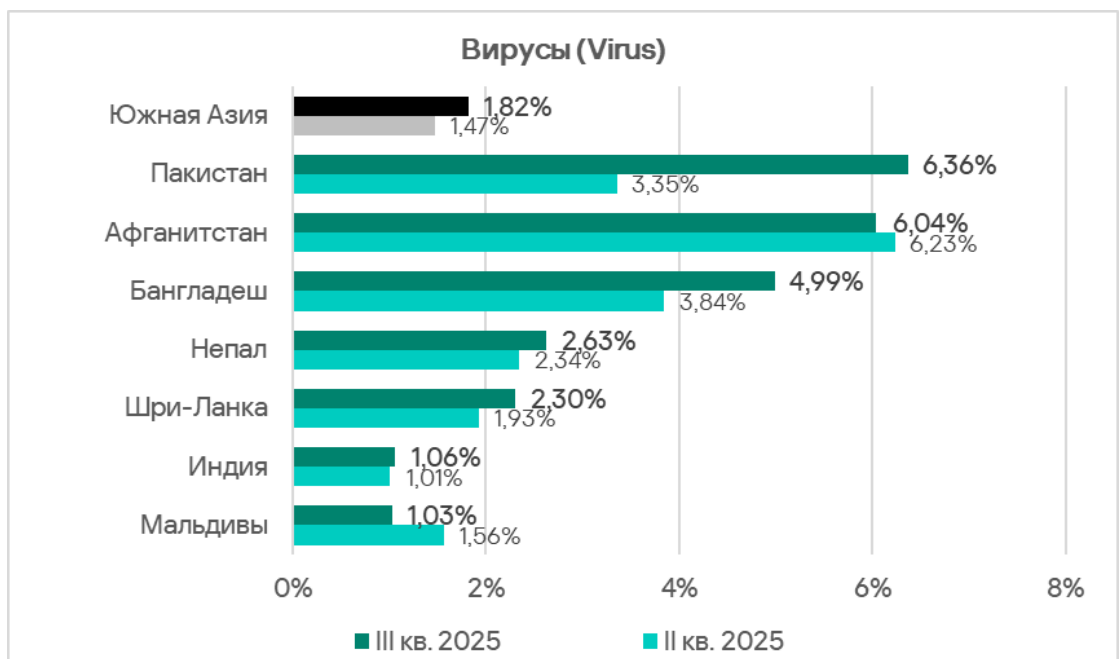
Показатель вирусов в Южной Азии колеблется с тенденцией к снижению. В третьем квартале 2025 года показатель вирусов в регионе вырос до 1,82% — это в 11,4 раза больше, чем в Австралии и Новой Зеландии, где он наименьший среди регионов. По росту этого показателя Южная Азия занимает второе место среди регионов.



Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, в Южной Азии также увеличилась за квартал — до 0,29%. Этот показатель в 29,0 раза больше, чем в Северной Америке (Канада), которая замыкает соответствующий рейтинг регионов.

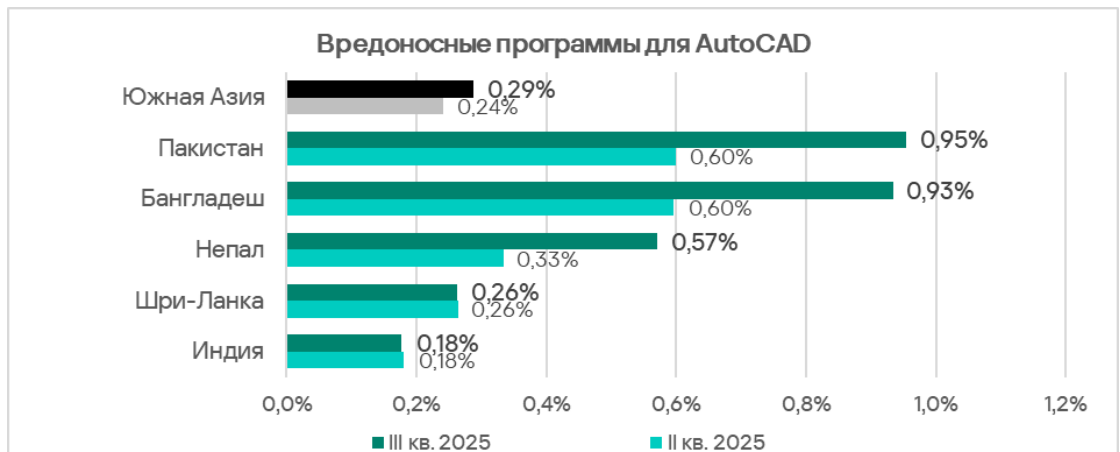


Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вирусы, лидирует Пакистан с 6,36%. За квартал показатель этой страны увеличился почти вдвое, и она опередила постоянного лидера этого рейтинга — Афганистан.



Вирусы в регионе распространяются через все источники угроз, но основной канал — съемные носители. По доле компьютеров АСУ, на которых блокировались угрозы при подключении съемных носителей, в регионе лидирует Афганистан.

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, первенство держат две страны — Пакистан с 0,95% и Бангладеш с 0,93%. В обеих странах показатель за квартал вырос с 0,6%.



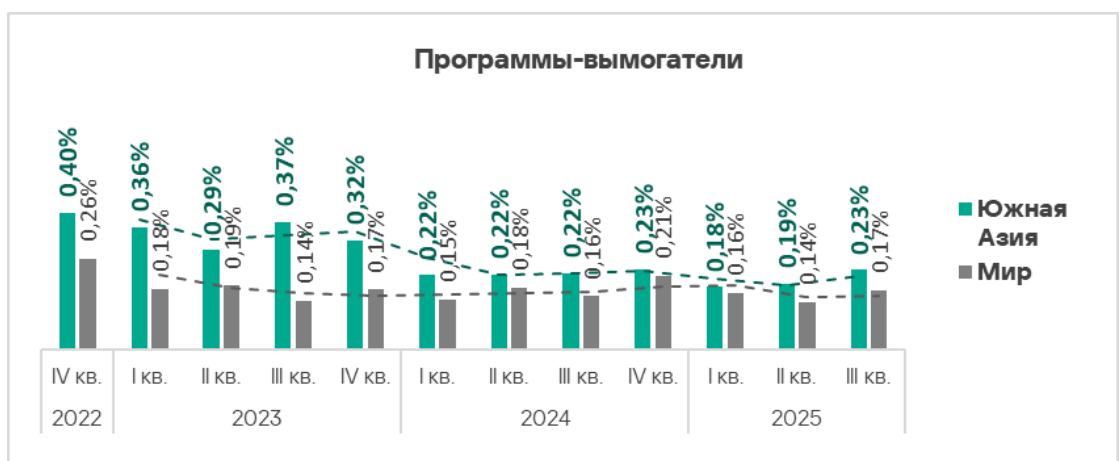
Как и вирусы, вредоносные программы для AutoCAD в регионе распространяются через все источники угроз, но преимущественно на съемных носителях.

Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Южная Азия находится на третьем месте среди регионов, пропустив выше только Африку и Ближний Восток.

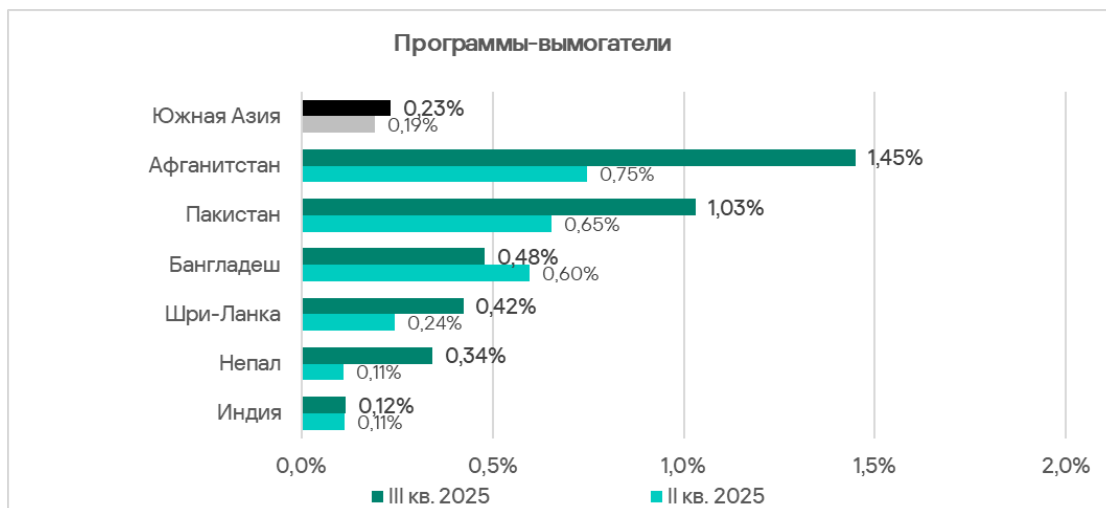
Показатель Южной Азии (0,23%) — в 4,6 раза больше, чем в Северной Европе, где он наименьший.

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в регионе растет второй квартал подряд.



Среди стран региона по доле компьютеров АСУ, на которых блокируются программы-вымогатели, лидирует Афганистан с 1,45%. Высокое значение также у следующего в рейтинге Пакистана — 1,03%.

За квартал показатель вырос во всех странах, кроме Бангладеш. В Афганистане он увеличился почти вдвое.



В Южной Азии программы-вымогатели чаще всего распространяются на съемных носителях. Среди стран региона по показателю этого источника угроз также лидирует Афганистан.

Отрасли

Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является ОТ-инфраструктура биометрические системы.

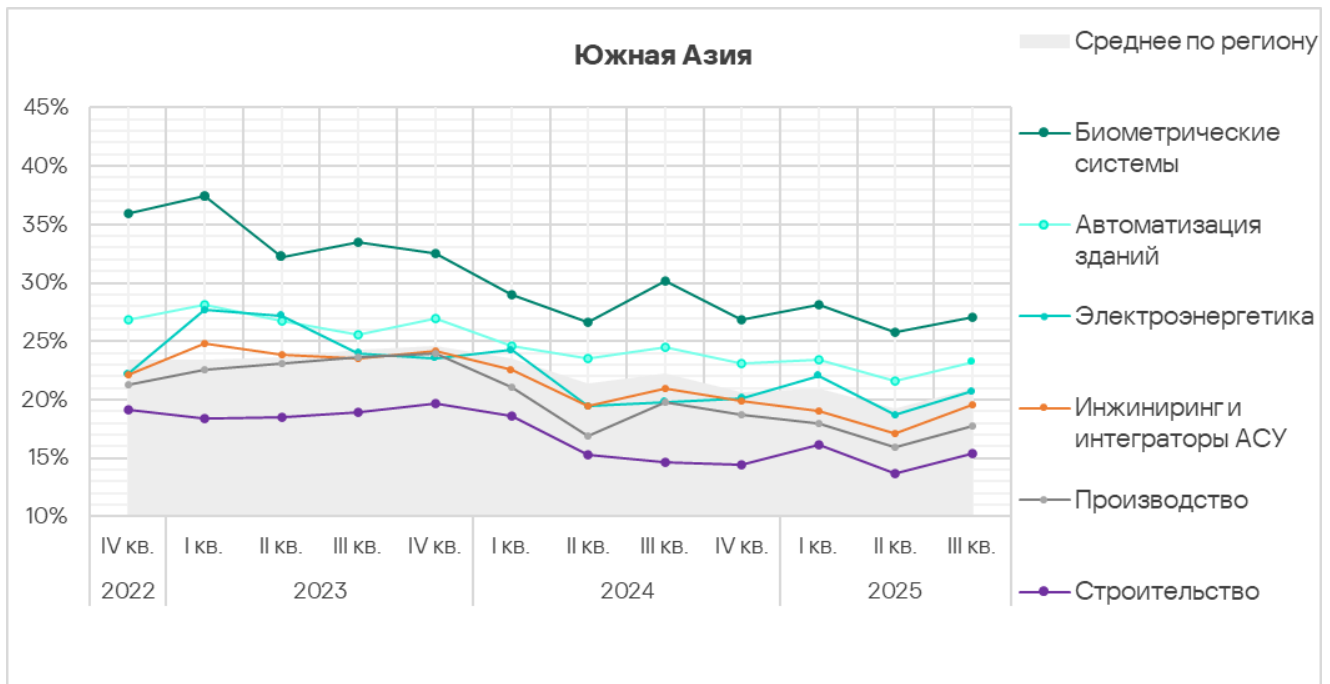
По сравнению с соответствующими среднемировыми значениями показатели меньше во всех отраслях, кроме производства.



В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась во всех рассматриваемых отраслях.



Все рассмотренные отрасли с четвертого квартала 2023 года демонстрируют положительную динамику долгосрочных трендов (показатели снижаются) с периодическими колебаниями.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

Показатели источников угроз в отраслях в Южной Азии, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	11,21%	10,52%	8,08%	9,90%	7,60%	7,53%	9,82%
Почтовые клиенты	5,08%	3,23%	2,73%	0,98%	2,10%	1,41%	2,23%
Съемные носители	1,82%	0,78%	0,54%	0,38%	0,20%	0,67%	0,63%
Сетевые папки	0,08%	0,09%	0,00%	0,02%	0,05%	0,00%	0,05%
Показатель отрасли в регионе	27,05%	23,21%	20,73%	19,51%	15,36%	17,74%	

Показатели категорий угроз в отраслях в Южной Азии, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	4,92%	4,44%	4,09%	4,68%	3,44%	4,10%	4,41%
Вредоносные скрипты и фишинговые страницы	11,59%	8,53%	5,35%	5,75%	5,05%	4,77%	7,03%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,12%	4,07%	3,41%	1,81%	1,67%	2,76%	2,97%
Черви (Worm)	3,26%	1,72%	2,73%	0,94%	0,48%	1,81%	1,41%
Майнеры — исполняемые файлы для ОС Windows	0,91%	0,45%	0,15%	0,36%	0,18%	0,34%	0,41%
Вредоносные документы (MSOffice+PDF)	3,48%	2,19%	1,56%	0,91%	0,86%	0,87%	1,57%
Вирусы (Virus)	3,86%	2,13%	2,58%	1,46%	1,47%	2,42%	1,82%
Программы-вымогатели	0,45%	0,34%	0,10%	0,11%	0,13%	0,20%	0,23%
Веб-майнеры, выполняемые в браузерах	0,30%	0,23%	0,00%	0,19%	0,20%	0,07%	0,20%
Вредоносные программы для AutoCAD	0,23%	0,18%	0,24%	0,36%	1,04%	0,34%	0,29%
Показатель отрасли в регионе	27,05%	23,21%	20,73%	19,51%	15,36%	17,74%	

У отраслей в регионе высокий показатель угроз из интернета – у большинства по источнику, так и по категориям угроз (ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы).

Биометрические системы

Южная Азия находится на четвертом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в ОТ-инфраструктуре биометрические системы.

В глобальном рейтинге среди всех индустрий во всех регионах ОТ-инфраструктура биометрические системы в Восточной Азии занимает:

- второе место по показателю угроз на съемных носителях;
- третье место по доле компьютеров, на которых были заблокированы черви.

Среди регионов по показателям в отрасли Южная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и на съемных носителях;
- второе место по показателю сетевых папок;

- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателю червей;
- третье место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вредоносные программы для AutoCAD и майнеры обеих категорий.

Среди отраслей в регионе отрасль биометрические системы занимает:

- первое место по всем источникам угроз, кроме сетевых папок;
- второе место по показателю угроз в сетевых папках;
- первое место по показателям всех категорий угроз, кроме вредоносных программ для AutoCAD.

Автоматизация зданий

Южная Азия находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

Среди регионов по показателям в отрасли Южная Азия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- третье место по показателю съемных носителей, четвертое — по показателю угроз в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных;
- четвертое место по показателям следующих категорий угроз: вредоносные программы для AutoCAD и программы-вымогатели.

Среди отраслей в регионе автоматизация зданий занимает:

- первое место по показателю угроз в сетевых папках. По остальным источникам угроз — второе место в рейтингах;
- второе место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, программы-вымогатели и майнеры обеих категорий;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Электроэнергетика

Южная Азия находится на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

Среди регионов по показателям в отрасли Южная Азия находится на четвертом месте по доле компьютеров АСУ, на которых блокируются черви, вирусы и вредоносные программы для AutoCAD.

Среди отраслей в регионе электроэнергетика занимает:

- третье место по показателю угроз в почтовых клиентах;
- второе место по показателям вирусов и червей;
- третье место по показателям шпионских программ и вредоносных документов.

Инжиниринг и интеграторы АСУ

Южная Азия находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди регионов по показателям в отрасли Южная Азия занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- четвертое место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, вирусы и вредоносные программы для AutoCAD.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- третье место по показателю угроз из интернета;
- второе место по показателю следующих категорий угроз: ресурсы в интернете из списка запрещенных, вредоносные программы для AutoCAD;
- третье место по показателю следующих категорий угроз: вредоносные скрипты и фишинговые страницы, майнеры – исполняемые файлы для ОС Windows.

Производство

Южная Азия находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди регионов по показателям в отрасли Южная Азия занимает:

- третье место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей;
- четвертое место по показателю угроз из интернета;
- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных;
- третье место по показателям вредоносных программ для AutoCAD, четвертое — по показателям вирусов и программ-вымогателей.

Среди отраслей в регионе производство занимает:

- третье место по угрозам на съемных носителях;
- третье место по показателю следующих категорий угроз: вирусы, черви, программы-вымогатели, вредоносные программы для AutoCAD.

Строительство

Южная Азия находится на девятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

Среди регионов по показателям в отрасли Южная Азия находится на четвертом месте по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках.

Среди отраслей в регионе строительство занимает:

- третье место по показателю угроз в сетевых папках;
- первое место по показателю вредоносных программ для AutoCAD;
- третье место по показателю веб-майнеров.

Средняя Азия и Закавказье

Основные проблемы кибербезопасности в регионе

Отсутствие контроля использования съемных носителей информации

В Средней Азии и Закавказье традиционно высока доля компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей. В третьем квартале 2025 года соответствующий показатель в регионе был в 1,5 раза выше, чем в среднем по миру.

Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы, майнеры — исполняемые файлы для ОС Windows и шпионское ПО.

По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы, Средняя Азия и Закавказье лидирует среди всех регионов, по показателю червей она находится на втором месте после Африки. Показатели этих категорий выше среднемировых в 2,1 и 1,7 раза соответственно

Частые попытки заражения защищенных систем при подключении USB-накопителей могут указывать на:

- низкую степень информатизации предприятия (отсутствие защищенных внутренних систем хранения и передачи файлов);
- существование незащищенной части инфраструктуры предприятия, которая является источником самораспространяющегося ПО;
- общую низкую культуру информационной безопасности.

Отсутствие контроля за установкой пользователями ПО на компьютеры АСУ

В рейтинге регионов по показателю майнеров — исполняемых файлов для ОС Windows Средняя Азия и Закавказье занимает первое место. Основной канал распространения такого вредоносного ПО — интернет.

В третьем квартале 2025 года в Средней Азии и Закавказье доля компьютеров АСУ, на которых блокировались майнеры — исполняемые файлы для ОС Windows, была самой высокой среди регионов во всех индустриях.

Небольшое исследование показало, что в регионе программы для майнинга криптовалют, по всей видимости, нередко устанавливаются на компьютеры АСУ их легитимными пользователями. Однако зачастую, скачивая из сети такое ПО, сотрудники предприятий не подозревают, что его конфигурация

была модифицирована злоумышленниками — в результате добытые майнингом средства уходят совсем не тем, кто это ПО для майнинга установил.

Также следует учитывать, что вредоносные майнеры — исполняемые файлы давно используют техники самораспространения червей: кражу данных аутентификации, поиск и кражу небезопасно сохраненных секретов, эксплуатацию локальных и сетевых уязвимостей. Поэтому их присутствие в технологической сети нельзя считать незначительной угрозой.

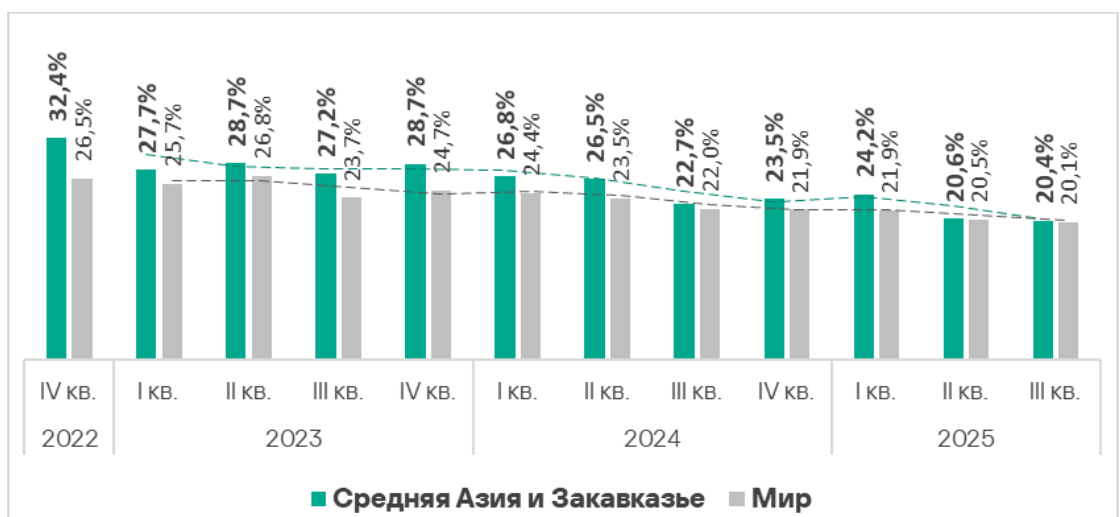
Стабильно высокий уровень показателя программ-вымогателей

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье занимает четвертое место с показателем, который в 1,2 раза выше среднемирового. Эта категория угроз в регионе в третьем квартале 2025 года распространялась как в интернете, так и в электронной почте, и на съемных носителях. По показателю программ-вымогателей Средняя Азия и Закавказье занимает первое место среди регионов в отраслях электроэнергетика и инжиниринг и интеграторы АСУ, второе место — в ОТ-инфраструктуре биометрические системы, третье место — в нефтегазовой отрасли.

Статистика по всем угрозам

В третьем квартале 2025 года Средняя Азия и Закавказье занимает седьмое место в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с 20,4%. Это в 2,2 раза больше, чем в Северной Европе, где показатель наименьший среди регионов.

Показатель в регионе постепенно уменьшается, в третьем квартале 2025 года он был наименьшим за три последних года.

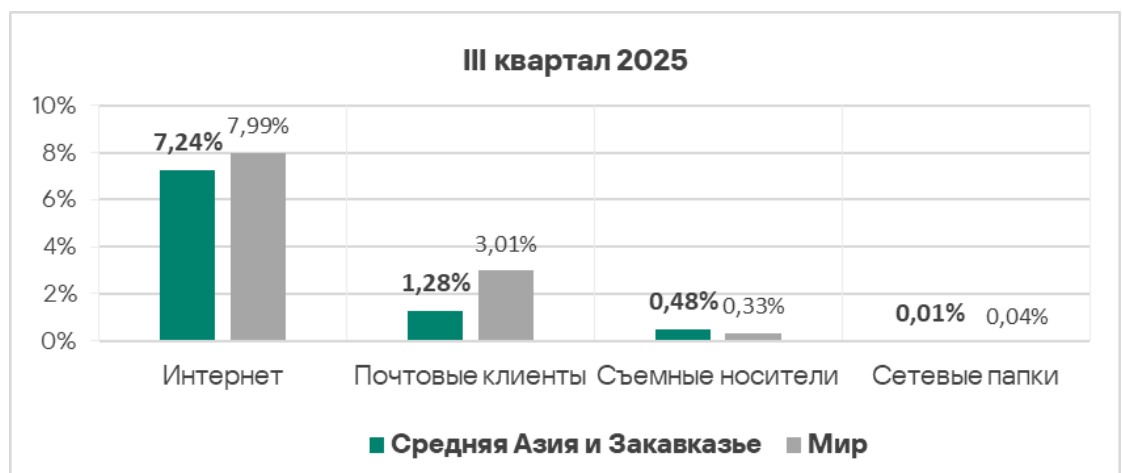


В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 12,86% в Грузии до 39,16% в Туркмении.

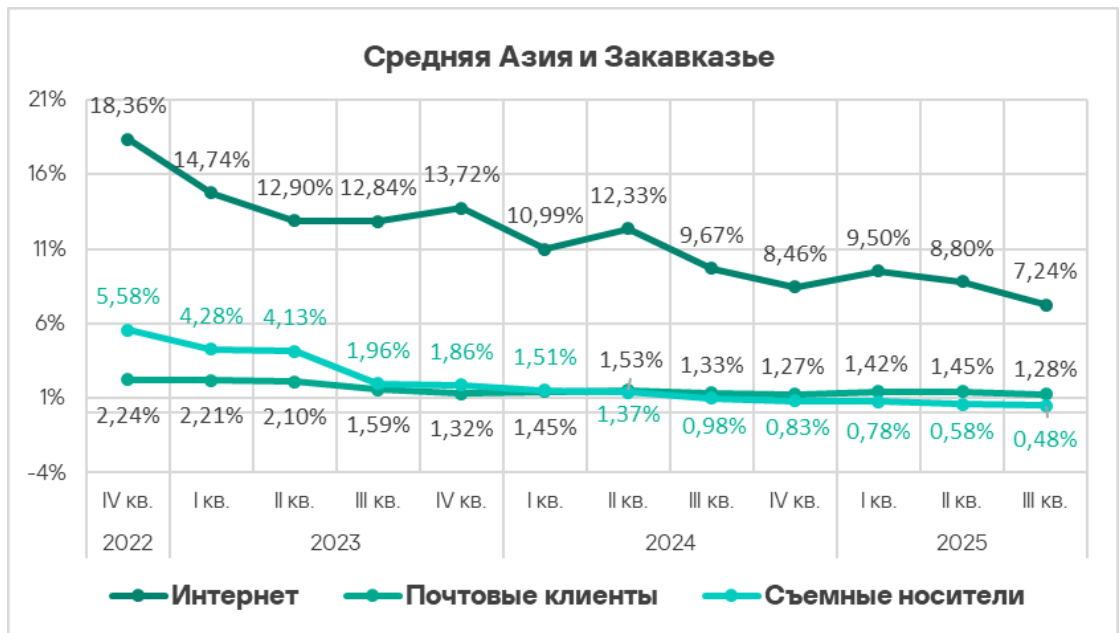


Источники угроз

В Средней Азии и Закавказье среди всех источников угроз выше среднемирового показателя только доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, — в 1,5 раза.



В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз.



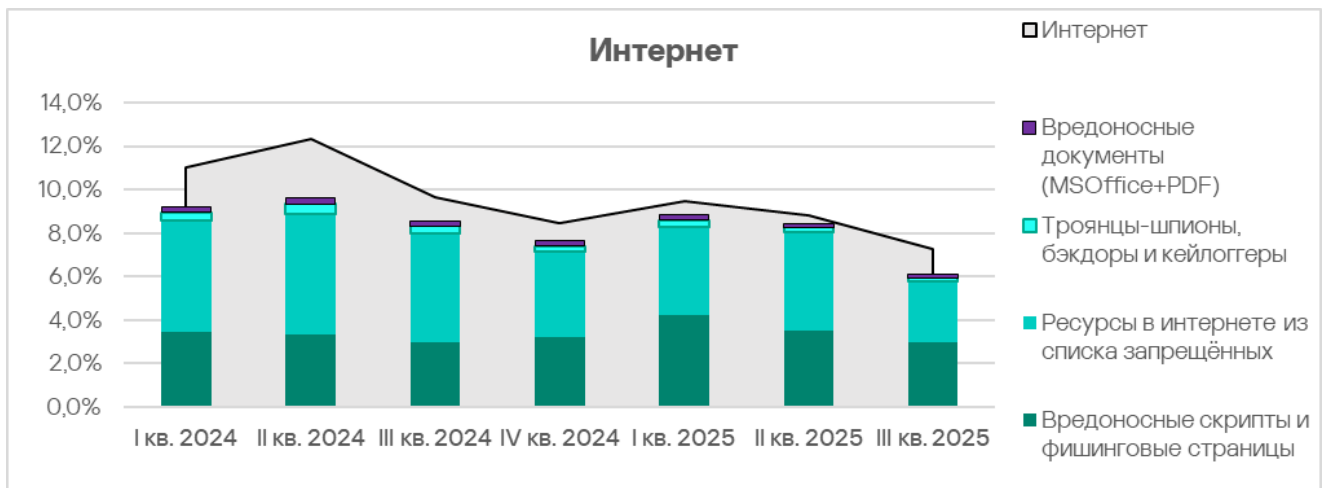
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Средняя Азия и Закавказье занимает седьмое место в рейтинге регионов с показателем 7,24%, который превышает минимальный — у Северной Европы — в 1,6 раза.

Показатели стран региона варьируют от 3,30% в Туркмении до 12,11% в Узбекистане. Узбекистан — единственная страна в регионе, где показатель вырос.



Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе, — это ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, шпионские программы и вредоносные документы.



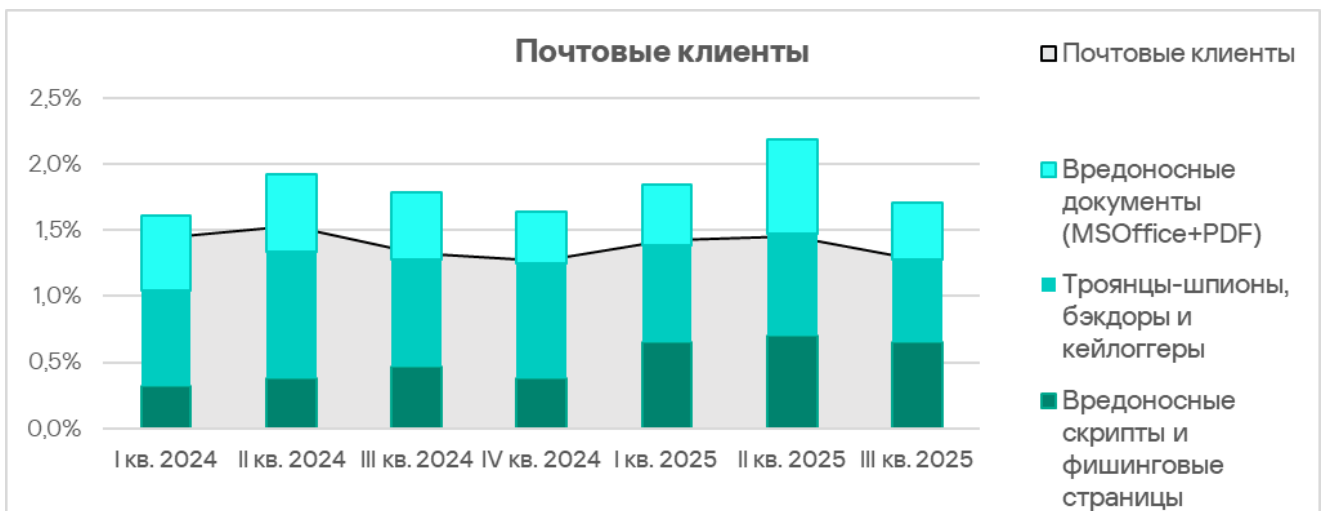
Почтовые клиенты

Регион Средняя Азия и Закавказье по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, занимает 12-е место в соответствующем рейтинге с 1,28%. Этот показатель в 1,6 раза выше, чем в России, которая этот рейтинг замыкает.

Среди стран региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидирует Азербайджан с 2,27%. Минимальный показатель в Туркмении – 0,24%.



Основные категории угроз из электронной почты, которые блокируются на компьютерах АСУ, – это вредоносные скрипты и фишинговые страницы, шпионское ПО, вредоносные документы.



Съемные носители

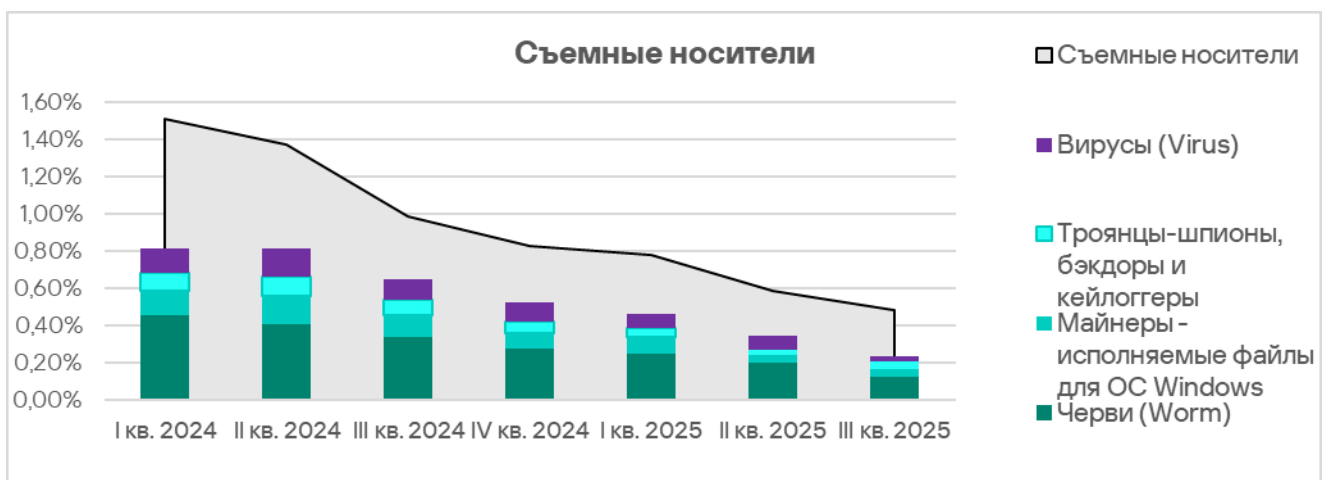
На первых шести позициях в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей:

Африка, Ближний Восток и регионы Азии. Средняя Азия и Закавказье — на шестом месте с 0,48%. Это в 9,6 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает этот рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует Туркмения с 3,95%. Отметим, что эта страна была последней в рейтинге по почтовым клиентам.



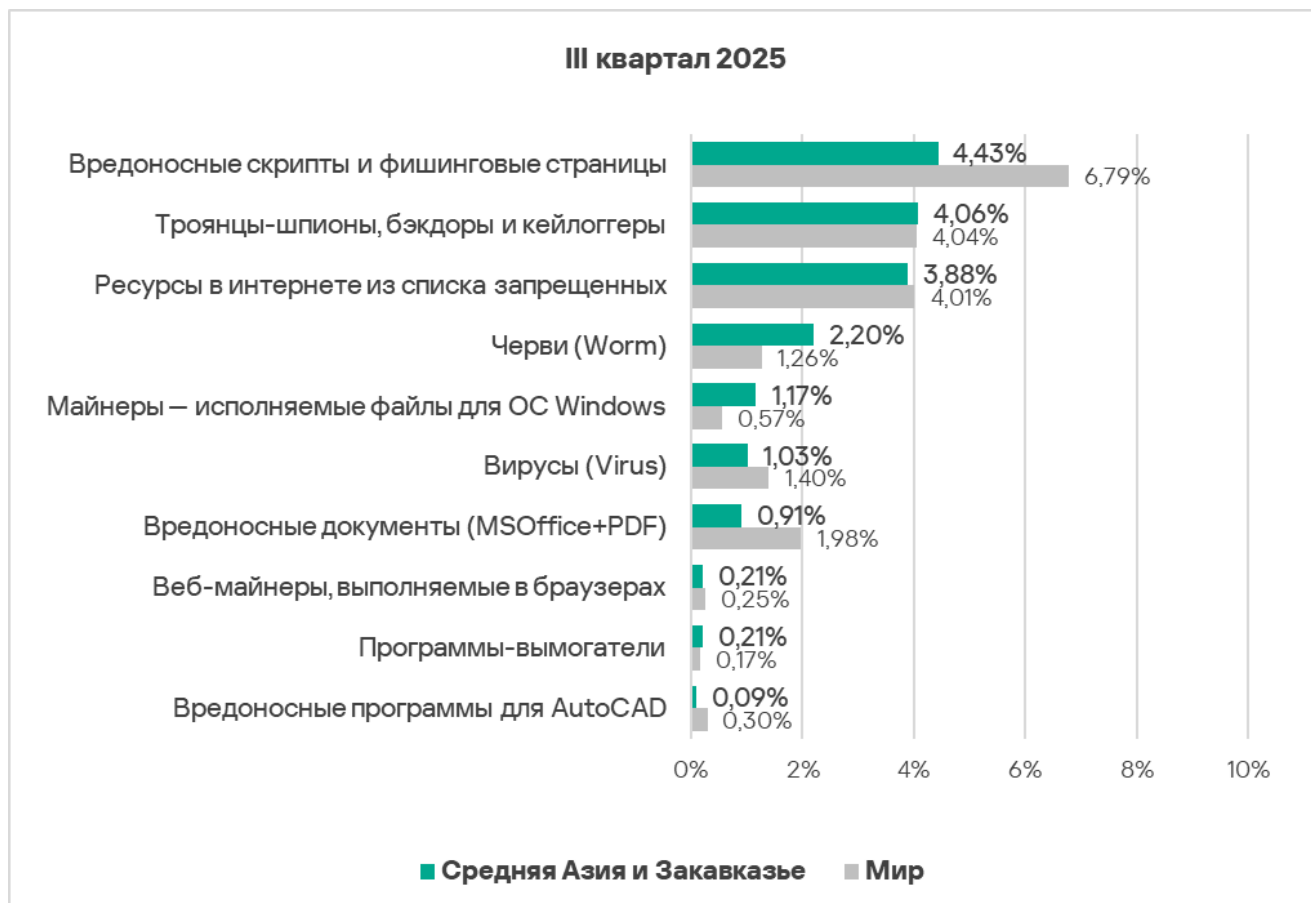
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы, майнеры — исполняемые файлы для ОС Windows и шпионское ПО.

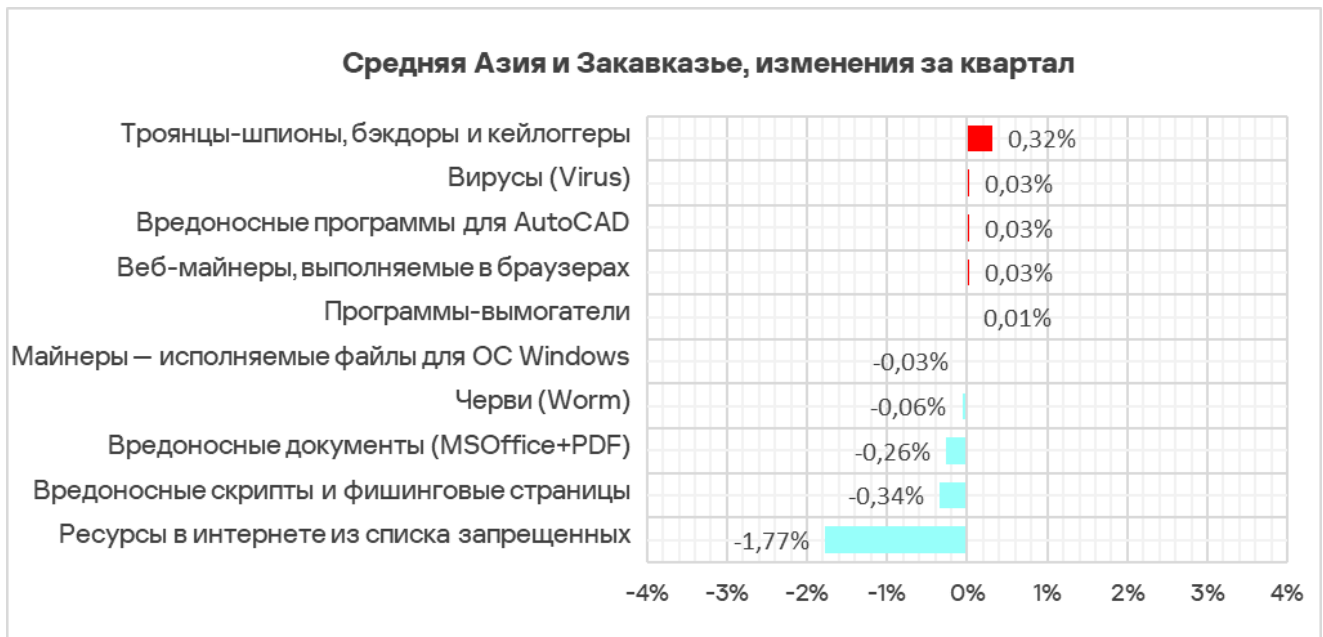


По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы, Средняя Азия и Закавказье лидирует среди остальных

регионов. По показателю червей регион находится на втором месте после Африки.

Категории угроз

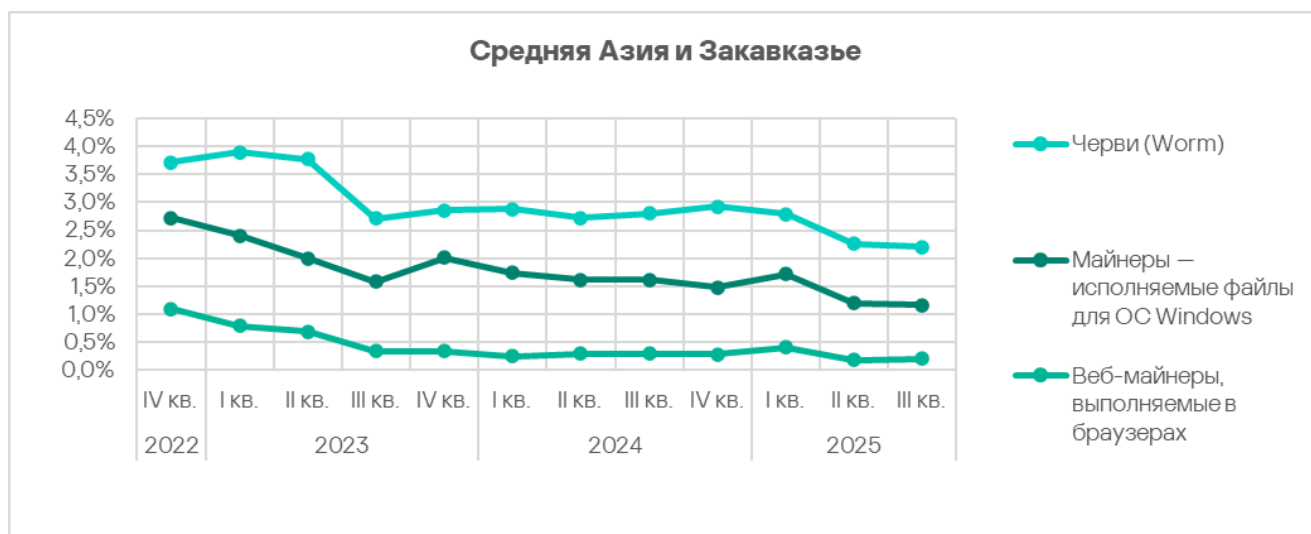




Из всех категорий угроз за квартал больше всего показатель вырос у шпионских программ, показатель в регионе даже чуть превысил среднемировой.

По сравнению со среднемировыми показателями, кроме шпионских программ, в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории угроз:

- майнеры – исполняемые файлы для ОС Windows – в 2,1 раза; Средняя Азия и Закавказье лидирует среди регионов по этому показателю;
- черви – в 1,7 раза; регион находится на втором месте в соответствующем рейтинге;
- программы-вымогатели – в 1,2 раза; четвертое место в рейтинге регионов по этому показателю.

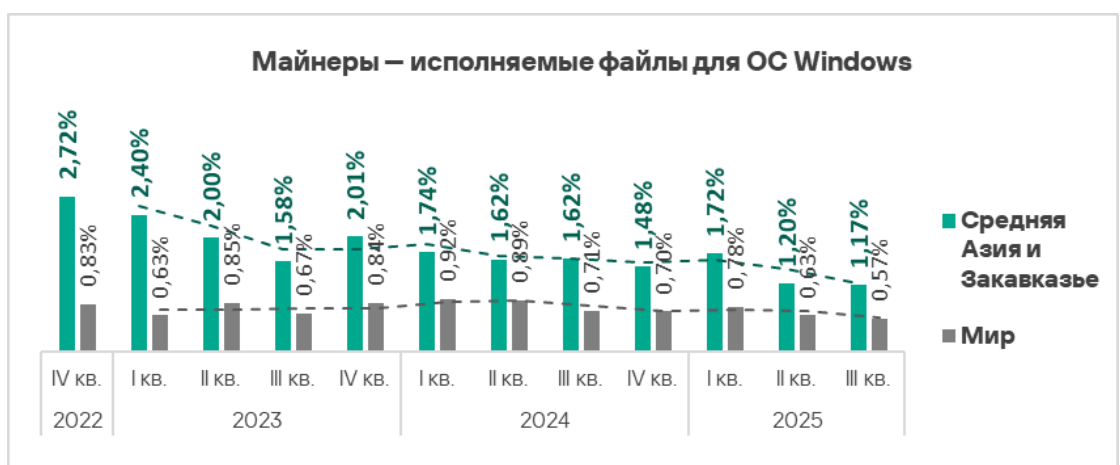


Майнеры – исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows, Средняя Азия и Закавказье лидирует среди регионов с 1,17%. Этот показатель в 9,0 раза больше, чем в регионе Австралия и Новая Зеландия, где он наименьший из всех среди регионов.



Доля компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы для ОС Windows, уменьшается второй квартал подряд и достигла минимального значения за три года.



Среди стран региона по доле компьютеров АСУ, на которых блокируются майнеры в формате исполняемых файлов, лидируют Таджикистан с 2,88% и

Туркмения с 2,82%. В обеих странах-лидерах показатели за квартал заметно уменьшились.

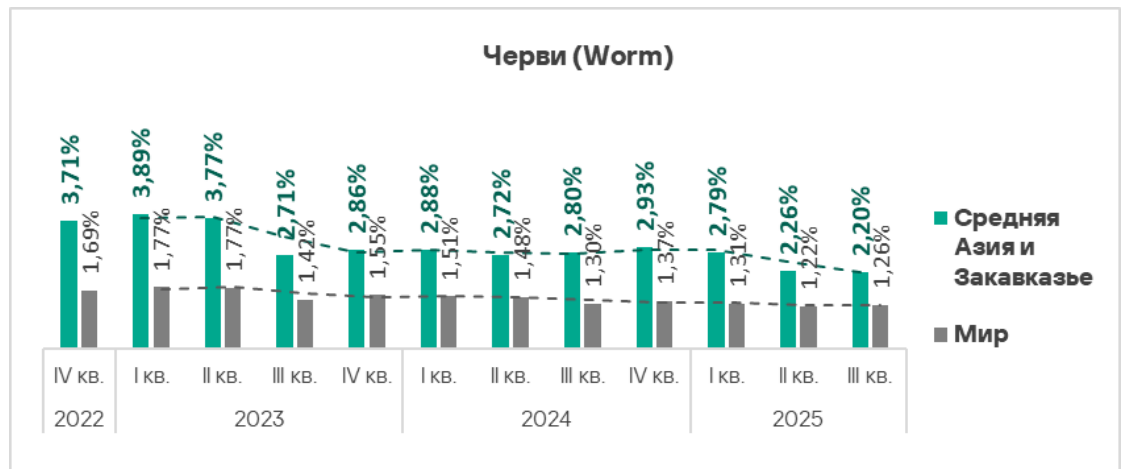


Распространяются такие угрозы через интернет и на съемных носителях. Таджикистан находится на втором месте в рейтинге стран региона по угрозам из интернета, Туркмения лидирует по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Черви

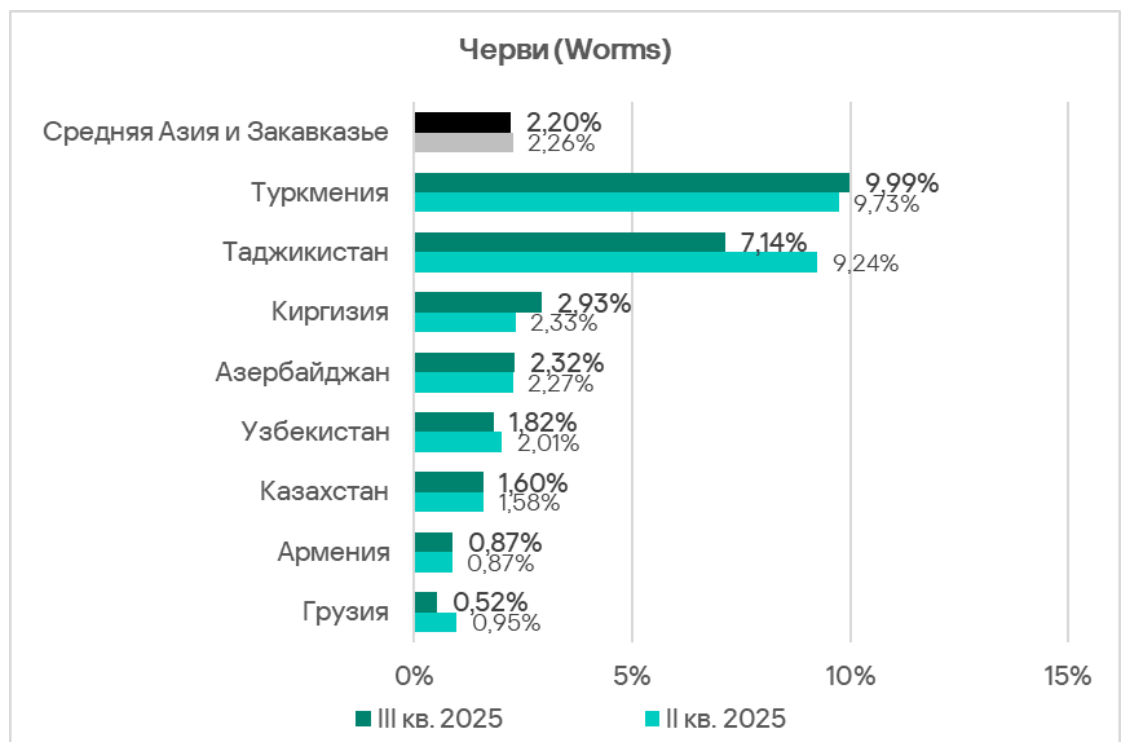
По доле компьютеров АСУ, на которых блокируются черви, Средняя Азия и Закавказье занимает среди регионов второе место, уступая только Африке. Показатель в регионе (2,20%) — в 10,0 раза больше, чем в Северной Европе, где он наименьший среди всех регионов.

Показатель червей снижается в Средней Азии и Закавказье третий квартал подряд. В третьем квартале 2025 года он оказался наименьшим за последние три года.



В Средней Азии и Закавказье в рейтинге категорий угроз черви занимают четвертое место. На такой высокой позиции в региональном рейтинге черви, кроме Средней Азии и Закавказья, находятся только в России.

Среди стран региона по доле компьютеров АСУ, на которых заблокированы черви, лидирует Таджикистан с 9,99%.



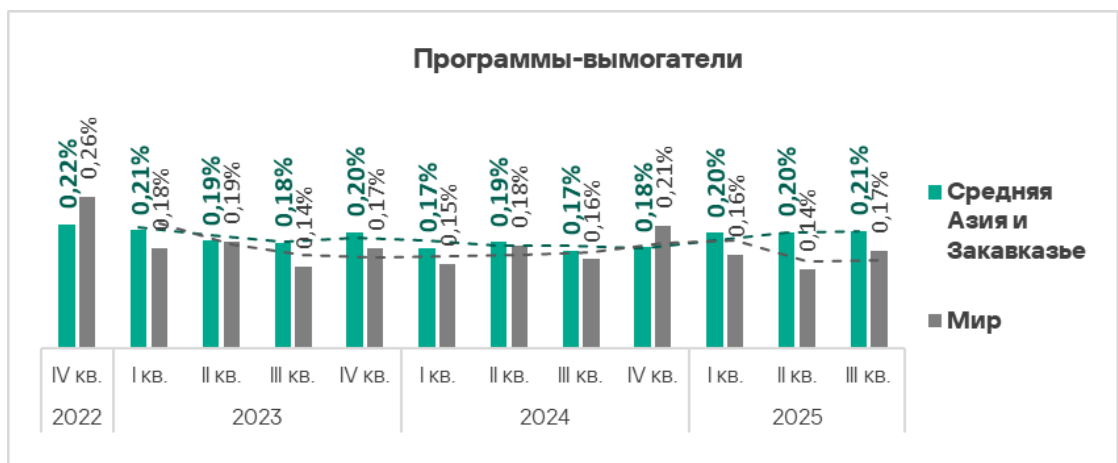
Распространяются такие угрозы преимущественно на съемных носителях. Туркмения и Таджикистан, лидирующие в этом рейтинге, на первых местах и в рейтинге по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Отметим также, что Таджикистан и Туркмения лидируют в рейтинге по майнерам — исполняемым файлам для ОС Windows.

Программы-вымогатели

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье среди регионов занимает четвертое место с 0,21%. Этот показатель больше, чем в Северной Европе, которая замыкает соответствующий рейтинг, в 4,2 раза.

Показатель программ-вымогателей в Средней Азии и Закавказье довольно стабилен и немного подрос за квартал.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы-вымогатели, с большим отрывом от остальных лидирует Таджикистан с 1,07%.



Отрасли

Из отраслей региона, рассмотренных в отчете, чаще встречается с угрозами ОТ-инфраструктура биометрические системы.

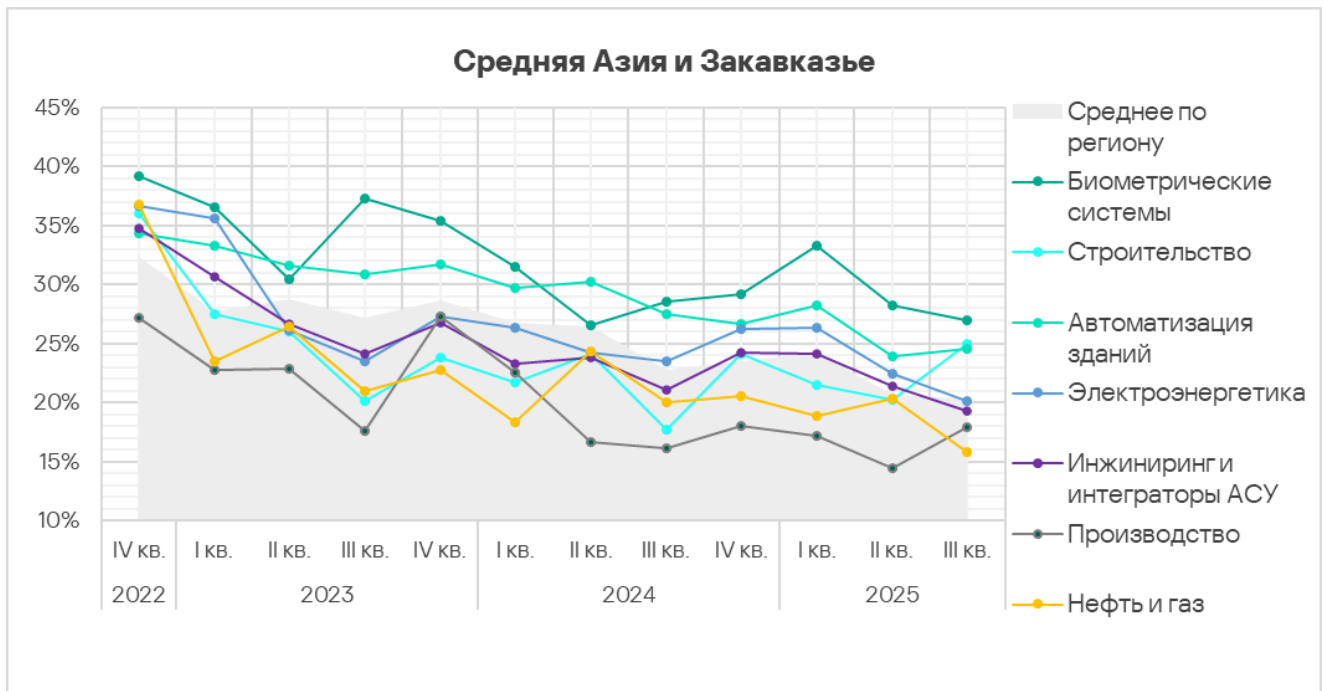


У отраслей строительство, автоматизация зданий и производство показатель выше среднемирового, больше всего разница в отрасли

строительство — в 1,2 раза. Именно в этих отраслях показатель за квартал вырос.



Тренды во всех отраслях демонстрируют в целом положительную динамику (показатели снижаются), хотя у некоторых отраслей заметны колебания.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

Показатели источников угроз в отраслях в Средней Азии и Закавказье, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	11,21%	10,52%	8,08%	9,90%	12,40%	7,60%	7,53%	7,24%
Почтовые клиенты	5,08%	3,23%	2,73%	0,98%	5,81%	2,10%	1,41%	1,28%
Съемные носители	1,82%	0,78%	0,54%	0,38%	0,39%	0,20%	0,67%	0,48%
Сетевые папки	0,08%	0,09%	0,00%	0,02%	0,00%	0,05%	0,00%	0,01%
Показатель отрасли в регионе	26,98%	24,62%	20,11%	19,29%	15,80%	25,03%	17,99%	

Показатели категорий угроз в отраслях в Средней Азии и Закавказье, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	5,18%	4,33%	6,18%	4,28%	4,42%	5,16%	3,96%	3,88%
Вредоносные скрипты и фишинговые страницы	7,08%	5,51%	5,65%	5,14%	4,15%	5,41%	6,12%	4,43%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,08%	6,13%	4,34%	3,66%	2,14%	2,77%	4,32%	4,06%
Черви (Worm)	3,00%	2,93%	3,15%	1,48%	1,74%	2,26%	2,88%	2,20%
Майнеры - исполняемые файлы для ОС Windows	1,91%	1,44%	1,45%	1,19%	1,47%	1,89%	1,08%	1,17%
Вредоносные документы (MSOffice + PDF)	3,54%	1,44%	1,18%	0,96%	0,13%	0,38%	0,36%	0,91%
Вирусы (Virus)	1,63%	1,44%	1,45%	1,14%	0,94%	1,76%	2,52%	1,03%
Программы-вымогатели	0,54%	0,29%	0,53%	0,44%	0,13%	0,13%	0,00%	0,21%
Веб-майнеры, выполняемые в браузерах	0,27%	0,26%	0,79%	0,29%	0,54%	0,88%	0,36%	0,21%
Вредоносные программы для AutoCAD	0,00%	0,05%	0,13%	0,10%	0,00%	0,63%	0,00%	0,09%
Показатель отрасли в регионе	26,98%	24,62%	20,11%	19,29%	15,80%	25,03%	17,99%	

Для всех отраслей основной источник угроз — интернет. Как следствие, актуальны такие категории угроз как опасные ссылки из списка запрещенных, вредоносные скрипты и фишинговые страницы.

Регион Средняя Азия и Закавказье лидирует по доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows. Эта угроза актуальна для всех отраслей в регионе.

Во всех рассмотренных в отчете отраслях региона показатель категории угроз майнеры — исполняемые файлы для ОС Windows в Средней Азии и Закавказье — самый высокий среди регионов.

Еще одна актуальная угроза — черви.

Показатель червей в Средней Азии и Закавказье — второй по величине среди регионов во всех отраслях, кроме автоматизации зданий (первое место), электроэнергетики (первое место) и отрасли инжиниринг и интеграторы АСУ (четвертое место).

Высок в отраслях региона и показатель программ-вымогателей.

По показателю программ-вымогателей Средняя Азия и Закавказье занимает первое место среди регионов в отраслях электроэнергетика и инжиниринг и

интеграторы АСУ, второе место — в ОТ-инфраструктуре биометрические системы, третье — в нефтегазовой отрасли.

Биометрические системы

Средняя Азия и Закавказье находятся на пятом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в ОТ-инфраструктуре биометрические системы.

В глобальном рейтинге среди всех индустрий во всех регионах ОТ-инфраструктура биометрические системы в Средней Азии и Закавказье занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы;
- третье место по доле компьютеров АСУ, на которых были заблокированы программы-шифровальщики.

Среди регионов по показателям в ОТ-инфраструктуре биометрические системы регион занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в интернете;
- четвертое место по показателям съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и майнеры – исполняемые файлы для ОС Windows;
- второе место по показателям программ-вымогателей и третье — по показателям червей.

Среди отраслей в регионе ОТ-инфраструктура биометрические системы занимает:

- первое место по доле компьютеров АСУ, на которых блокировались угрозы в почтовых клиентах;
- второе место по угрозам в интернете и на съемных носителях;
- первое место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, программы-вымогатели, майнеры – исполняемые файлы для ОС Windows;
- второе место по показателям ресурсов в интернете из списка запрещенных и червей;
- третье место по показателю вирусов.

Строительство

Средняя Азия и Закавказье находятся на четвертом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

В глобальном рейтинге среди всех индустрий во всех регионах строительство в Средней Азии и Закавказье занимает:

- первое место по доле компьютеров АСУ, на которых блокировались веб-майнеры;
- второе место по доле компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы.

Среди регионов по показателям в отрасли регион Средняя Азия и Закавказье занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях;
- четвертое место по показателям угроз из интернета и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются майнеры обеих категорий;
- второе место по показателю червей и четвертое – по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионах строительство занимает:

- первое место по доле компьютеров АСУ, на которых блокировались угрозы в интернете;
- третье место по показателю съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокировались веб-майнеры и вредоносные программы для AutoCAD;
- второе место по показателям майнеров в формате исполняемых файлов и вирусам;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Автоматизация зданий

Средняя Азия и Закавказье находятся на четвертом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

В глобальном рейтинге среди всех индустрий во всех регионах отрасль автоматизация зданий в Средней Азии и Закавказье занимает:

- пятое место по доле компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы.

Среди регионов по показателям в отрасли Средняя Азия и Закавказье занимают:

- первое место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows и черви;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе автоматизация зданий – единственная, где на компьютерах АСУ блокировались угрозы в сетевых папках. Кроме того, она занимает:

- второе место по угрозам в почтовых клиентах;
- второе место по доле компьютеров АСУ, на которых блокировались вредоносные документы и шпионские программы;
- третье место по показателю червей.

Электроэнергетика

Средняя Азия и Закавказье находятся на седьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

В глобальном рейтинге среди всех индустрий во всех регионах электроэнергетика в Средней Азии и Закавказье занимает:

- второе место по доле компьютеров АСУ, на которых блокировались веб-майнеры;
- четвертое место по доле компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы для ОС Windows, черви и программы-вымогатели.

Среди регионов по показателям в отрасли Средняя Азия и Закавказье занимают:

- первое место по доле компьютеров АСУ, на которых блокируются майнеры обеих категорий, черви и программы-вымогатели;
- второе место по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе электроэнергетика занимает:

- третье место по доле компьютеров АСУ, на которых блокировались угрозы в интернете и в почтовых клиентах;

- первое место по доле компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных и черви;
- второе место по показателям веб-майнеров, программ-вымогателей и вредоносных программ для AutoCAD;
- третье место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы и шпионские программы.

Инжиниринг и интеграторы АСУ

Средняя Азия и Закавказье находятся на седьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди регионов по показателям в отрасли Средняя Азия и Закавказье занимают:

- первое место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows и программы-вымогатели;
- четвертое место по показателю червей.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- третье место по доле компьютеров АСУ, на которых блокировались программы-вымогатели и вредоносные программы для AutoCAD.

Производство

Средняя Азия и Закавказье находятся на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди регионов по показателям в отрасли Средняя Азия и Закавказье занимают:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows;
- второе место по показателям веб-майнеров и червей, третье – по показателям шпионских программ и вирусов и четвертое – по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых блокировались угрозы на съемных носителях;
- первое место по показателю вирусов;
- второе место по доле компьютеров АСУ, на которых блокировались вредоносные скрипты и фишинговые страницы.

Нефть и газ

Средняя Азия и Закавказье находятся на четвертом месте по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в нефтегазовой отрасли.

В глобальном рейтинге среди всех индустрий во всех регионах нефтегазовая отрасль Средней Азии и Закавказье занимает:

- третье место по доле компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы.

Среди регионов по показателям в отрасли Средняя Азия и Закавказье занимают:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов;
- второе место по показателю угроз из интернета и третье – по показателю угроз на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows;
- второе место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, веб-майнеры и черви;
- третье место по показателю программ-вымогателей.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- третье место по доле компьютеров АСУ, на которых блокировались майнеры обеих категорий.

Методика подготовки статистики

В отчете представлены результаты анализа статистических данных, полученных с помощью распределенной антивирусной сети [Kaspersky Security Network \(KSN\)](#). Данные получены от тех пользователей KSN, которые добровольно подтвердили свое согласие на их анонимную передачу и обработку с целью, описанной в Соглашении KSN для установленного на их компьютере продукта «Лаборатории Касперского».

Подключение к сети KSN дает нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счет обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за ее объема и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT¹.

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

- серверы управления и сбора данных (SCADA);
- серверы автоматизации зданий;
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human machine interface (HMI);
- компьютеры, используемые для администрирования технологических сетей и сетей автоматизации зданий;
- компьютеры программистов АСУ/ПЛК.

Компьютеры, передающие нам статистику, принадлежат организациям из разных отраслей. Наиболее широко представлены химическая промышленность, металлургия, инжиниринг и интеграторы АСУ,

¹ Организациям, в отношении любых данных которых наложены ограничения на их передачу вонне периметра организации, рекомендуем рассмотреть вариант использования сервиса [Kaspersky Private Security Network](#).

нефтегазовая отрасль, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность и фармацевтическая отрасль. Сюда же входят системы инжиниринговых компаний и интеграторов АСУ, работающих с предприятиями в самых разных отраслях, а также системы управления зданиями, физической безопасности и обработки биометрических данных.

Атакowanными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год – в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете доли машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение исследуемого периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение исследуемого периода мы получали обезличенную информацию.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com