Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Азия. Четвертый квартал 2025 года

27.04.2026

Версия 1.0

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 категорий угроз. В аналогичном мировом рейтинге вирусы находятся на шестом месте, в большинстве регионов — на шестом или седьмом.

В Юго-Восточной Азии показатель вирусов в 5,2 раза превышает среднемировой и является самым высоким значением 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 0,07%. Это значение выше среднемирового в 1,8 раза.

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

Доступность интернет-ресурсов на компьютерах ОТ

В четвертом квартале 2025 года Юго-Восточная Азия заняла второе место по доле компьютеров АСУ, на которых блокировались угрозы из интернета, и первое — по показателям ресурсов в интернете из списка запрещенных и веб-майнеров.

Интернет-ресурсы из списка запрещенных главным образом используются злоумышленниками для распространения вредоносного ПО, а также для фишинговых атак и в качестве инфраструктуры управления и контроля (C2). Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

Высокие показатели этой категории угроз, как правило, свидетельствуют:

- о слабом контроле выполнения политик ИБ (компьютеры АСУ имеют так или иначе доступ к интернету);
- о недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным интернет-ресурсам).

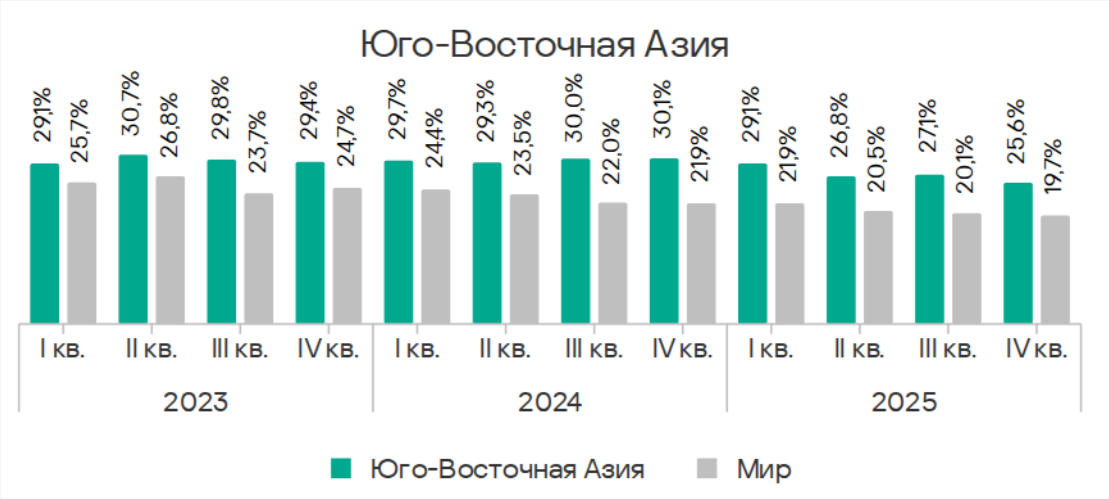
Особенностью региона является распространение через интернет не только традиционных для этого источника угроз, но и вирусов и вредоносных программ для AutoCAD. Эти категории угроз распространяются в Юго-Восточной Азии через все источники, но чаще в интернете.

Вьетнам, который лидирует в рейтингах стран по многим категориям угроз, занимает первое место и по показателю угроз из интернета.

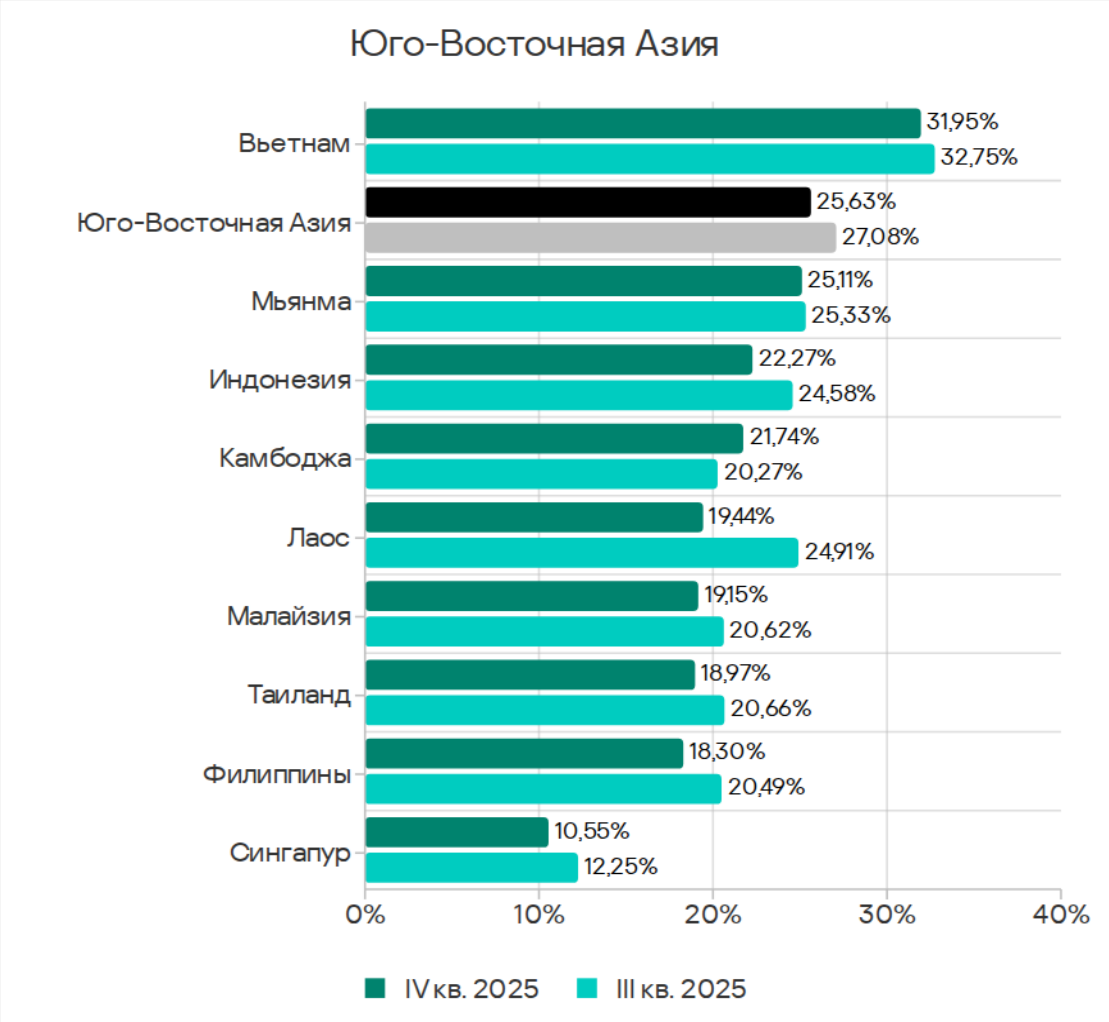
Статистика по всем угрозам

Юго-Восточная Азия занимает второе место в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с показателем 25,6%. Это значение больше среднемирового в 1,3 раза и в 3,0 раза больше минимального значения среди регионов, зафиксированного в Северной Европе.

После роста показателя региона в третьем квартале 2025 года, в четвертом доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Юго-Восточной Азии, уменьшилась.



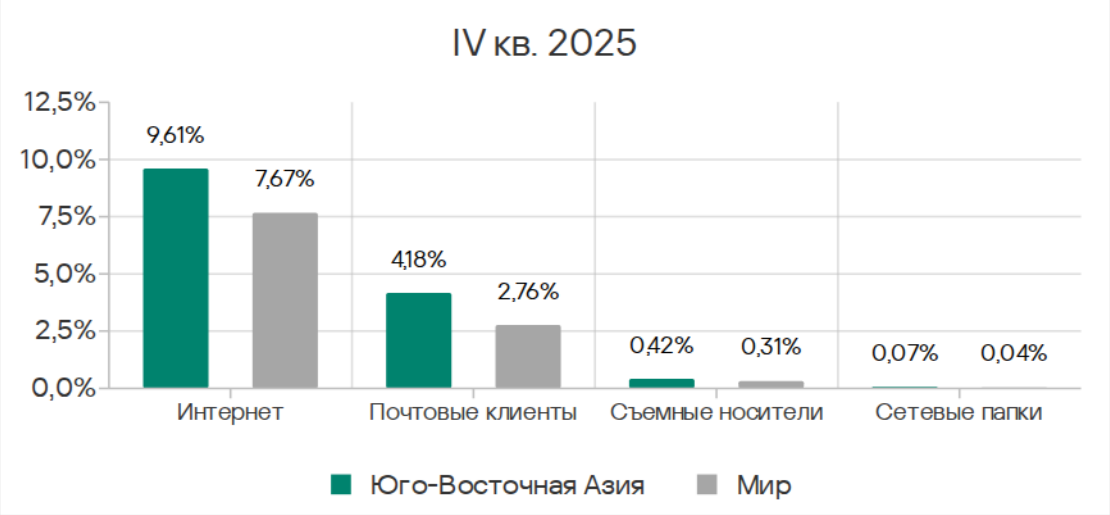
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 10,55% в Сингапуре до 31,95% во Вьетнаме. Показатели остальных стран — в диапазоне от 18% до 26%.



Источники угроз

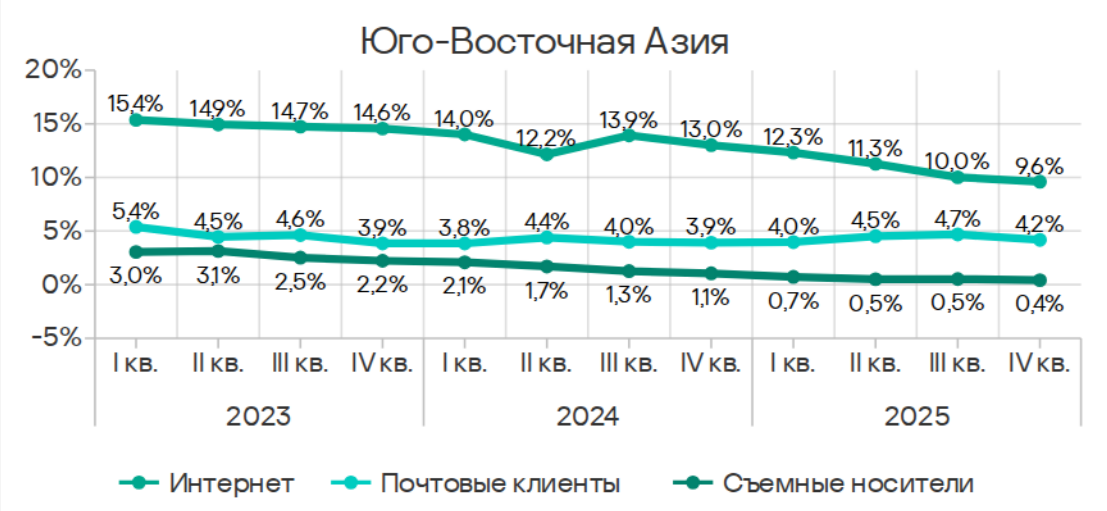
Доля компьютеров АСУ, на которых были заблокированы угрозы из разных источников, в регионе выше среднемировых показателей для всех источников угроз:

- интернет — в 1,3 раза;
- почтовые клиенты — в 1,5 раза;
- съемные носители — в 1,4 раза;
- сетевые папки — в 1,8 раза.



По показателям угроз из интернета и в сетевых папках Юго-Восточная Азия занимает второе место в соответствующих рейтингах регионов.

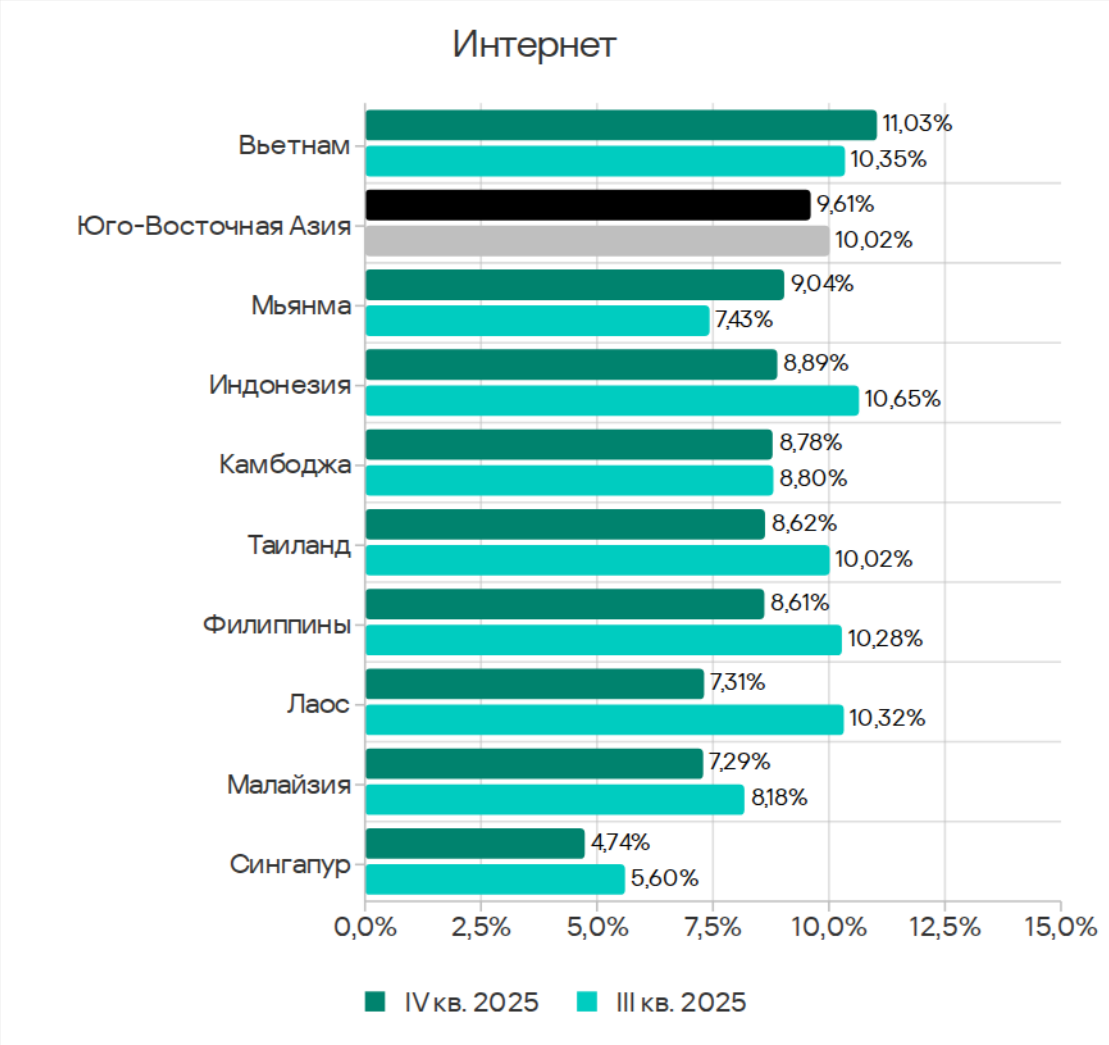
В четвертом квартале 2025 года показатель уменьшился у всех источников угроз.



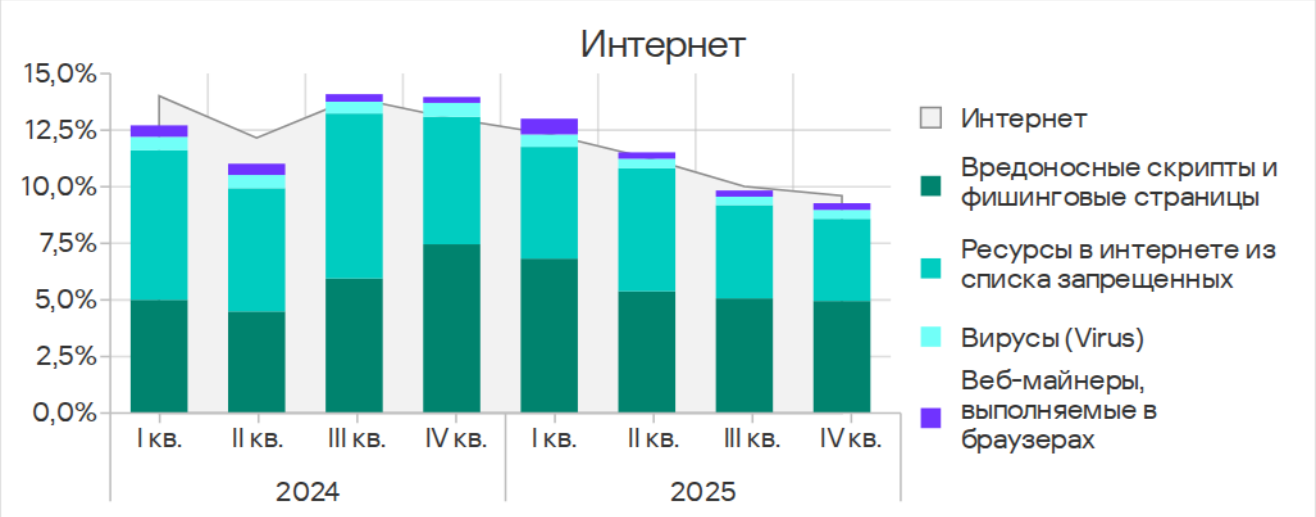
Интернет

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 2,4 раза.

Показатели стран региона варьируют от 4,74% в Сингапуре до 11,03% во Вьетнаме.



Основные категории угроз из интернета, которые блокируются на компьютерах АСУ в регионе: это вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вирусы и веб-майнеры. По показателям вирусов и веб-майнеров Юго-Восточная Азия лидирует среди регионов.

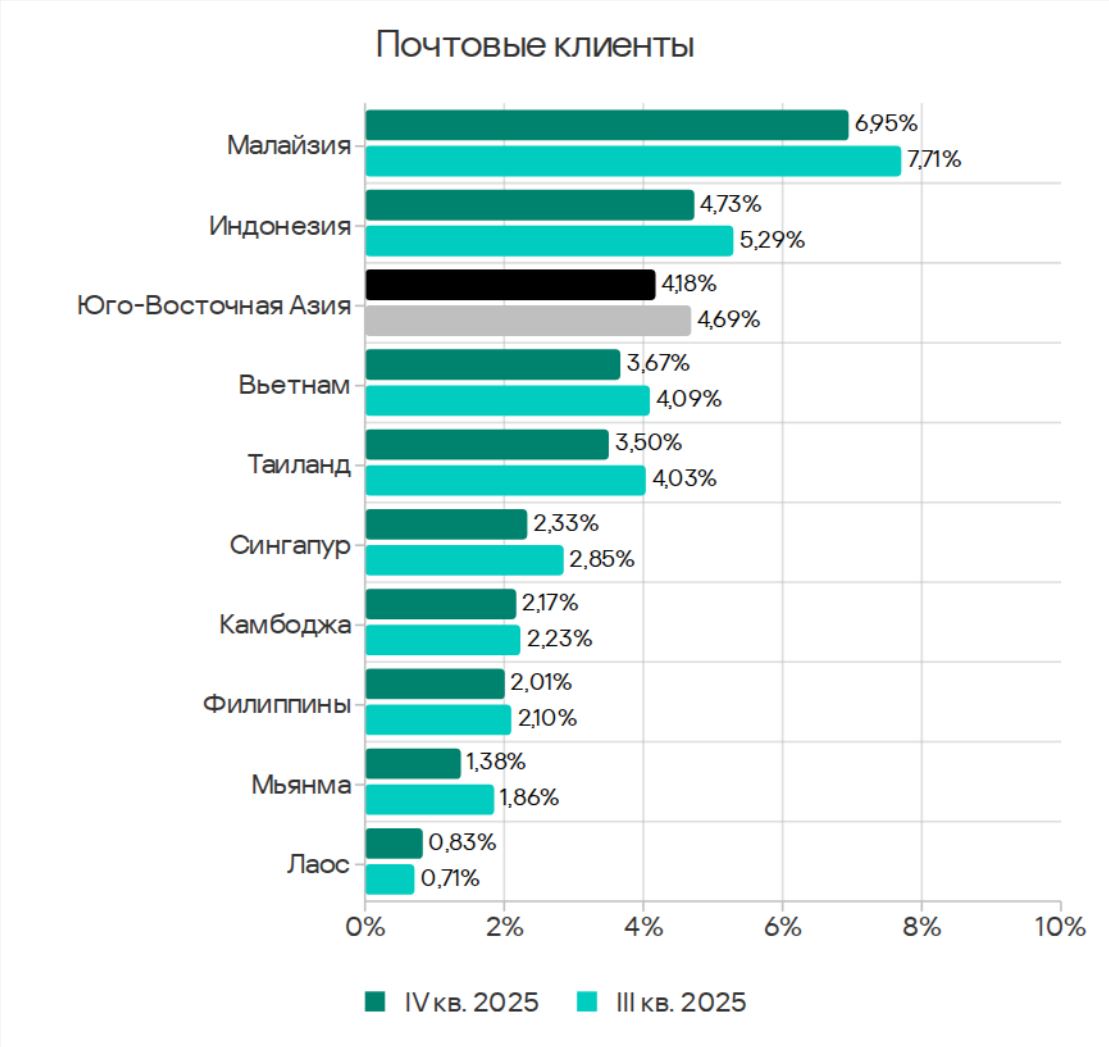


Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, Юго-Восточная Азия занимает четвертое место в рейтинге регионов с показателем 4,18%. Это в 6,5 раза больше, чем в Северной Европе, где значение минимальное.

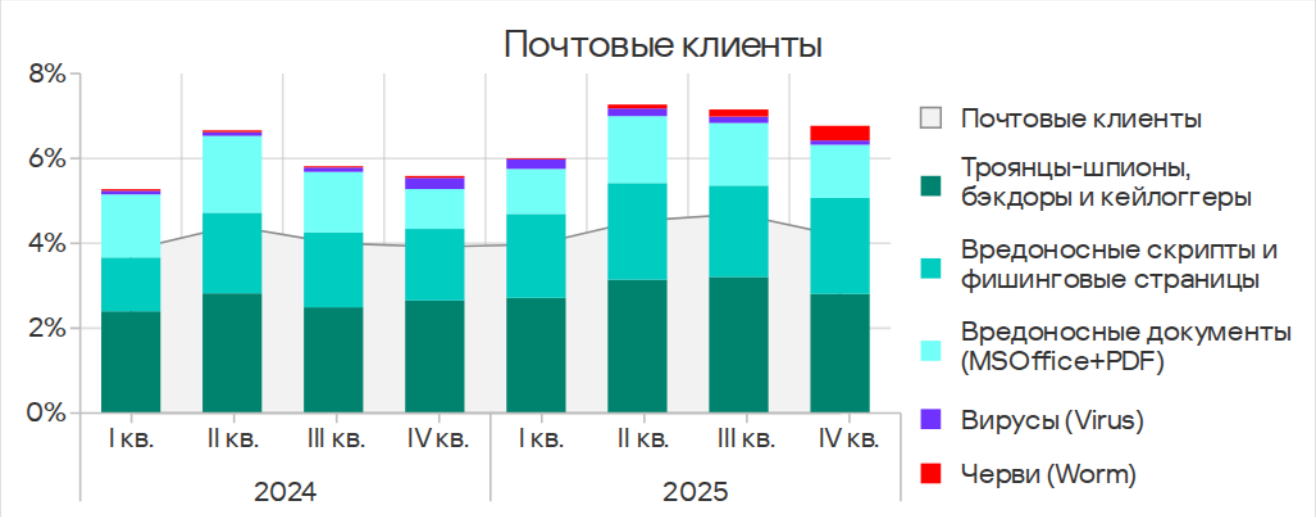
С 2024 года динамика показателя почтовых клиентов в регионе соответствует динамке среднемирового показателя. В четвертом квартале 2025 года он уменьшился после роста в течение трех предыдущих кварталов.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, с заметным отрывом лидирует Малайзия с 6,95%. Наименьшее значение в Лаосе — 0,83%.



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

Почта — основной канал распространения шпионских программ в регионе. В рейтинге регионов по показателю шпионских программ Юго-Восточная Азия находится на втором месте.



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, в ходе которых были атакованы организации во всех регионах мира. В Юго-Восточной Азии пик атаки пришелся на ноябрь.

Злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Под видом резюме (Curriculum Vitae) такие письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm). При запуске файла происходило заражение системы.

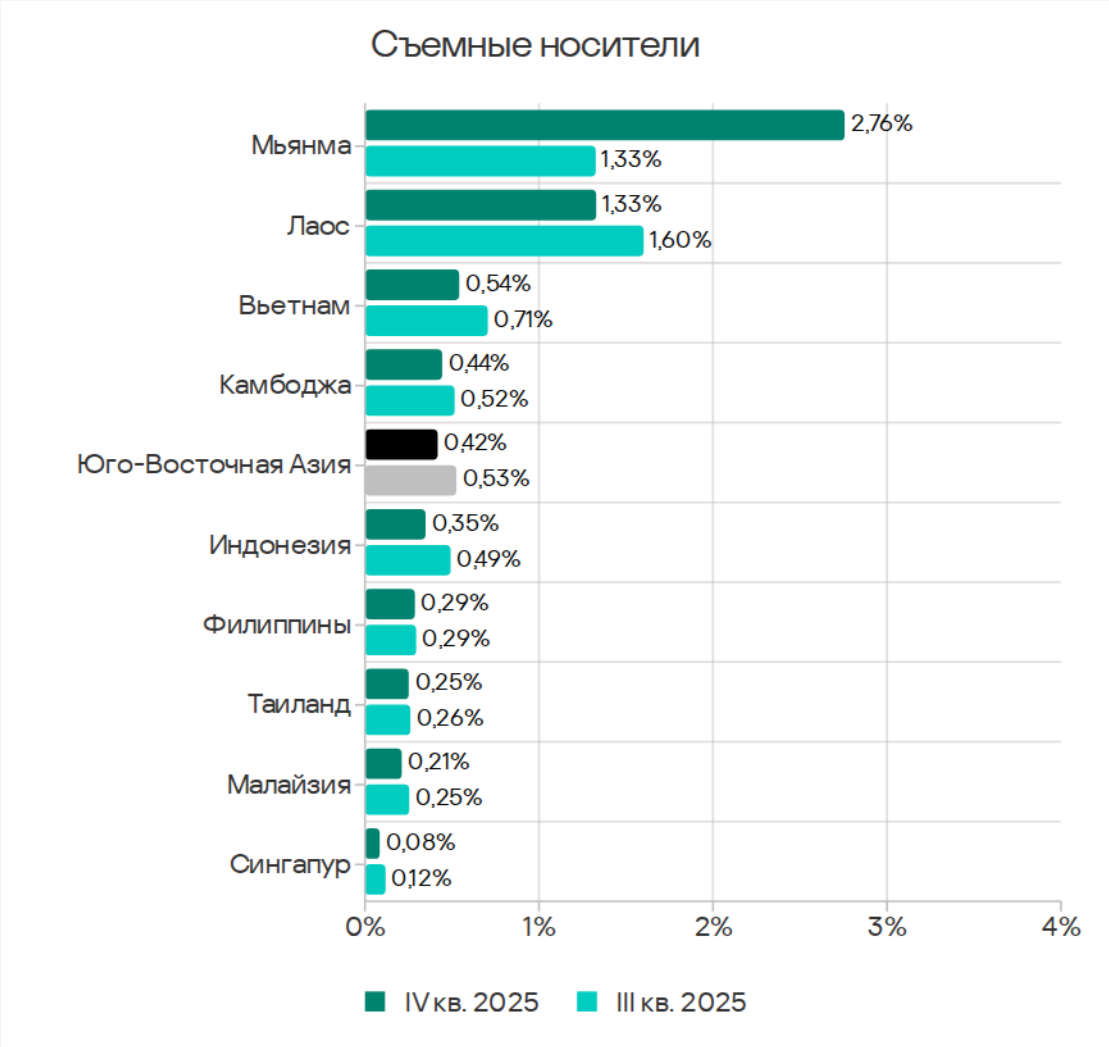
Как правило такие кампании направлены на доставку вредоносного ПО для кражи данных, а также на доставку программ-шпионов или инструментов для удаленного управления (RAT).

Съемные носители

Юго-Восточная Азия занимает шестое место в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей. Отметим, что первые шесть позиций в этом рейтинге занимают регионы Азии, Африка и Ближний Восток с показателями, которые попадают в диапазон от 0,42% до 1,41%, тогда как значения в остальных регионах не превышают 0,19%.

Доля компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, в Юго-Восточной Азии уменьшилась до 0,42%. Это в 8,9 раза больше значения в регионе Австралия и Новая Зеландия, который занимает последнее место в рейтинге.

Среди стран региона по этому показателю с отрывом от остальных лидируют Мьянма с 2,76% и Лаос с 1,33%. Наименьшее значение в Сингапуре — 0,08%.



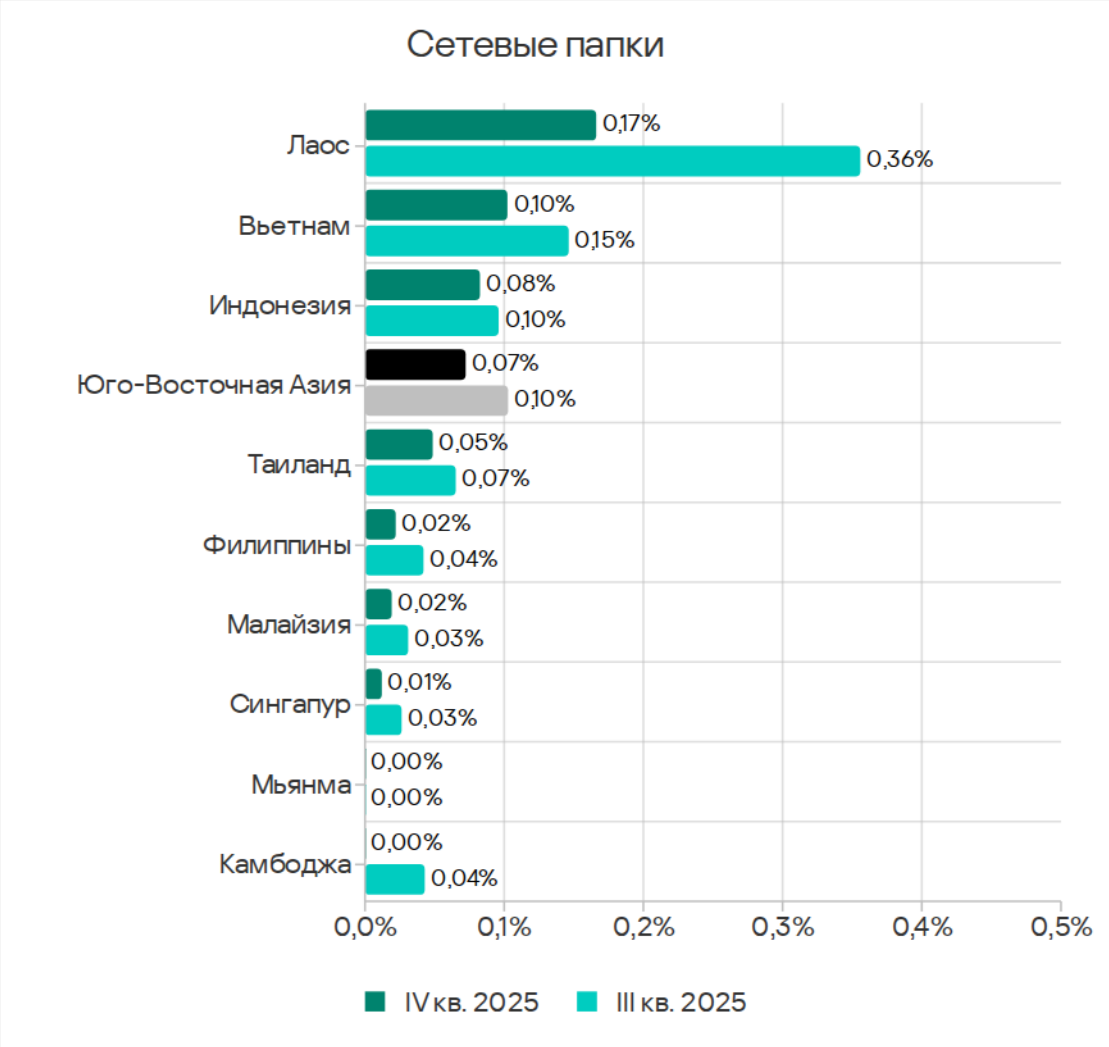
У Мьянмы и Лаоса, возглавляющих рейтинг по съемным носителям, наименьшие из всех стран региона показатели по угрозам в почтовых клиентах.

Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: вирусы, черви и шпионское ПО. По показателю вирусов 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 0,07%. С Северной Европой, которая занимает последнее место в рейтинге, показатели отличаются в 7,0 раза.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, в четвертом квартале 2025 года с заметным отрывом лидирует Лаос с 0,17%. Во всех странах региона, где были заблокированы угрозы в сетевых папках, показатели уменьшились.



Основными категориями угроз, которые распространяются через сетевые папки, в четвертом квартале 2025 года стали вирусы, вредоносное ПО для AutoCAD, черви. 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 майнеров — исполняемых файлов для ОС Windows и программ-вымогателей, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения.

Наиболее значительно региональные показатели превышали среднемировые у категорий угроз:

- веб-майнеры — в 1,5 раза;
- шпионские программы — в 1,5 раза;
- вирусы — в 5,3 раза;
- вредоносное ПО для AutoCAD — в 7,0 раза.

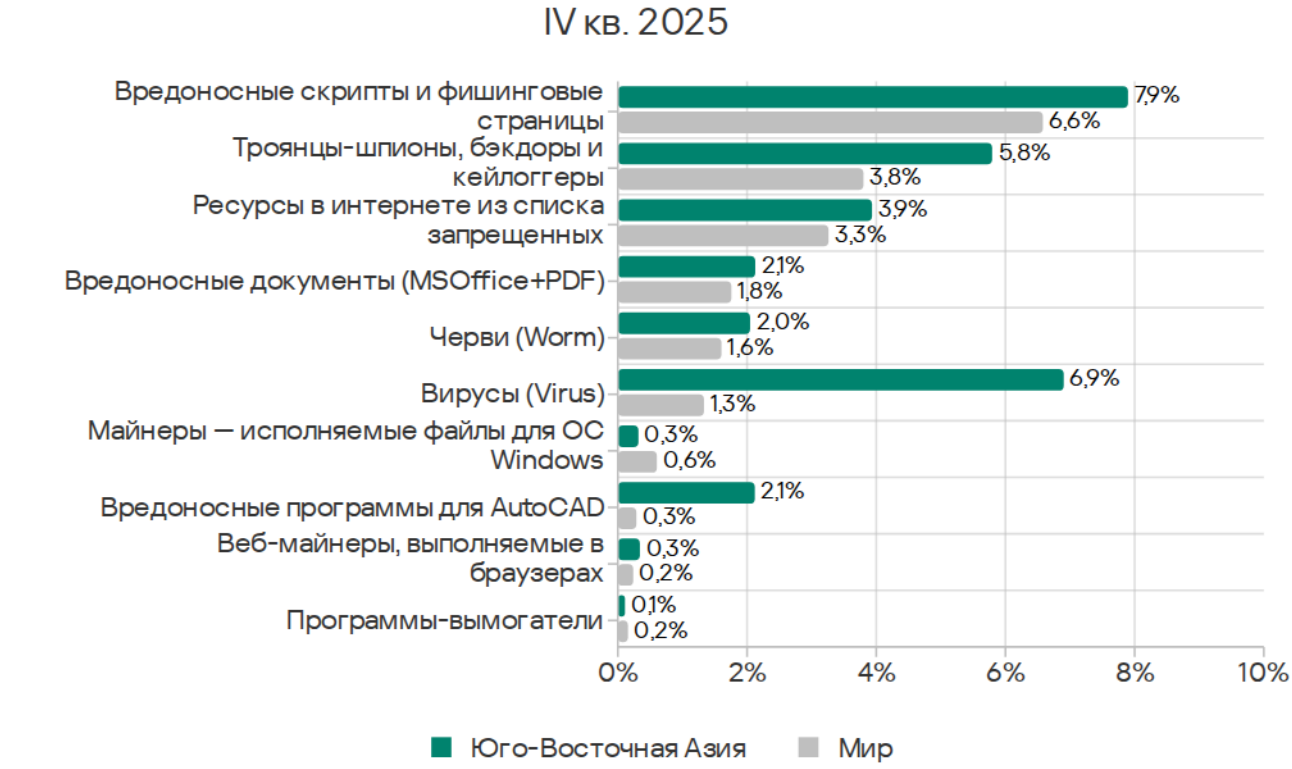
Юго-Восточная Азия в четвертом квартале 2025 года заняла первое место среди регионов по показателям категорий:

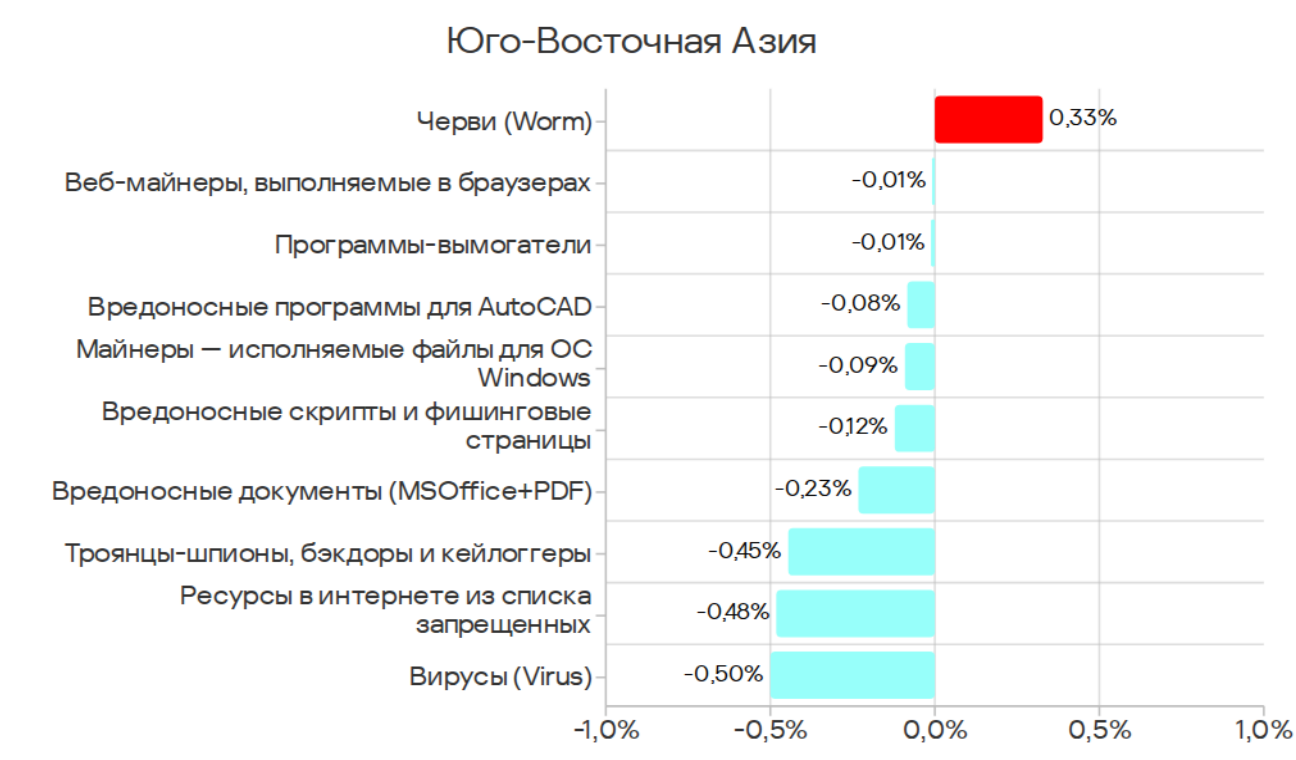
- ресурсы в интернете из списка запрещенных;
- веб-майнеры;
- вирусы;
- вредоносные программы для AutoCAD.

Отметим, что основным источником всех перечисленных выше угроз является интернет, а Юго-Восточная Азия находится на втором месте по показателю угроз из интернета.

По показателю шпионских программ регион на втором месте. Основной канал распространения этой угрозы — электронная почта.

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



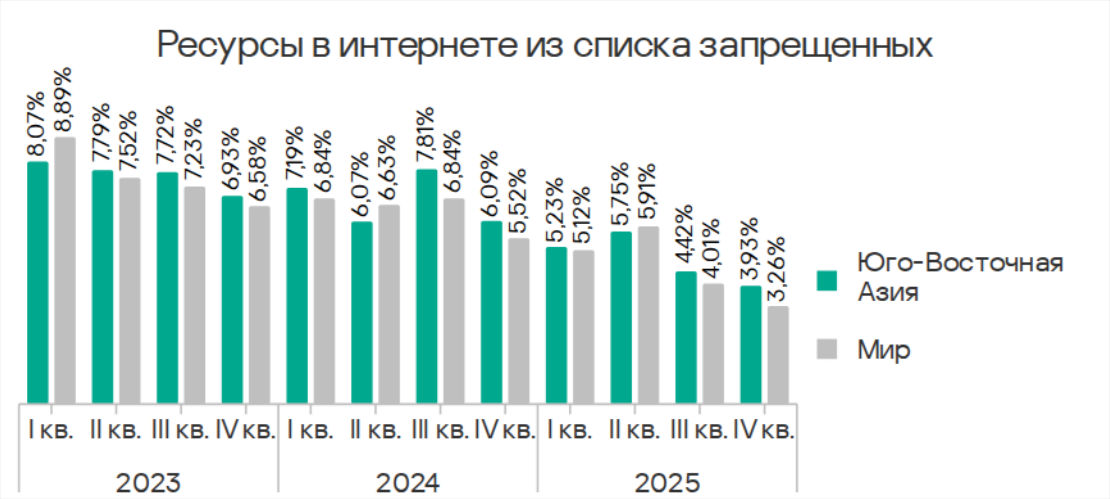


Из всех категорий угроз за квартал показатель вырос только у червей.

Ресурсы в интернете из списка запрещенных

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Юго-Восточная Азия в четвертом квартале 2025 года потеснила Африку и заняла первое место с 3,93%. Это в 2,2 раза больше показателя Северной Европы, которая замыкает рейтинг.

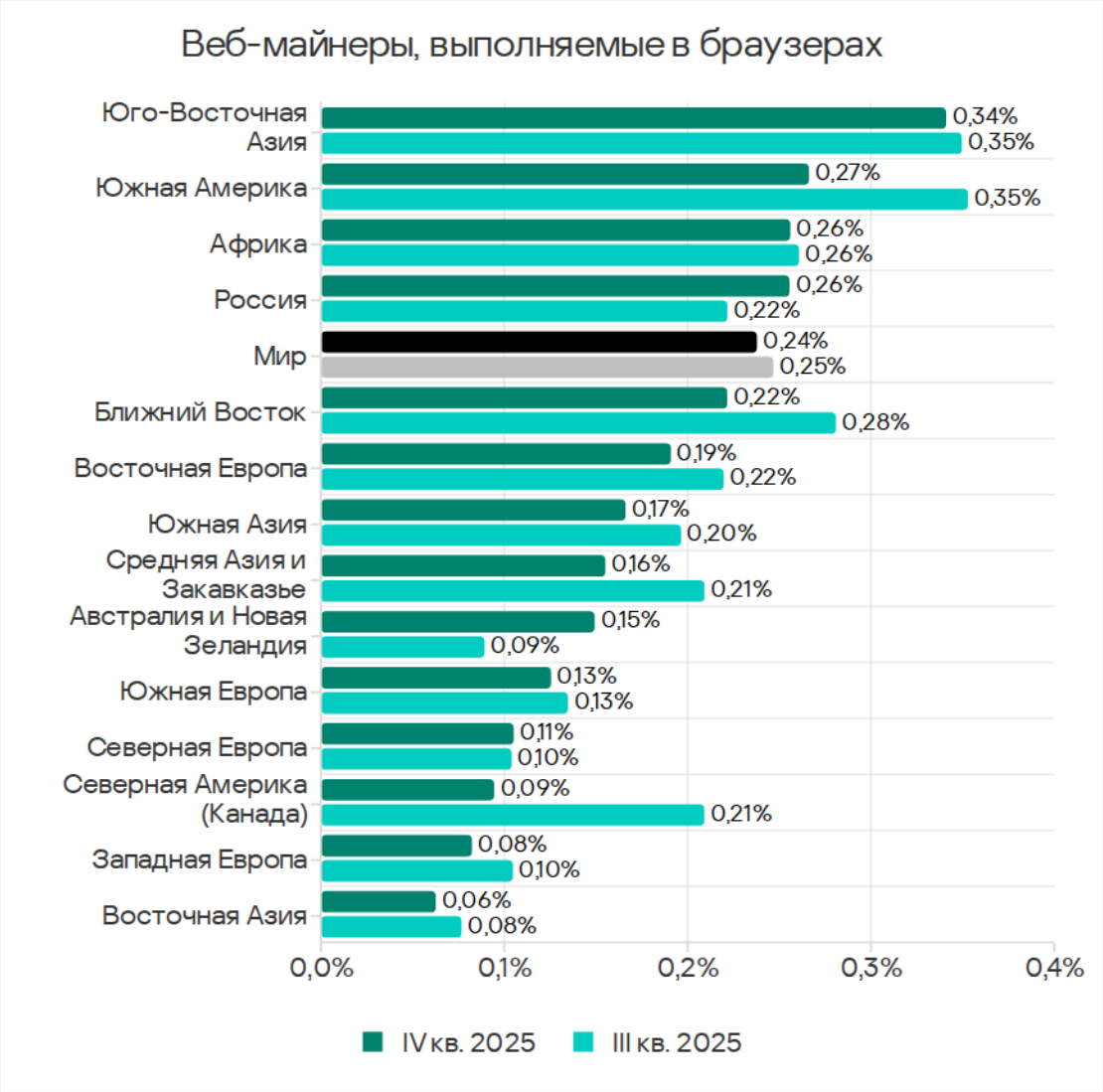
Показатель в Юго-Восточной Азии уменьшается второй квартал подряд.



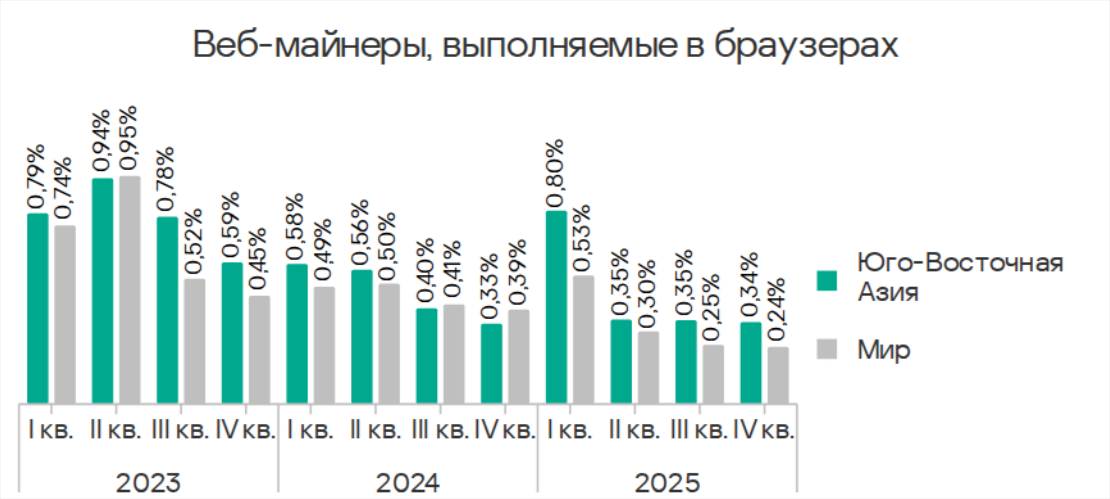
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, лидирует Вьетнам с 4,72%. В Сингапуре показатель – наименьший (1,51%).

Веб-майнеры, выполняемые в браузерах

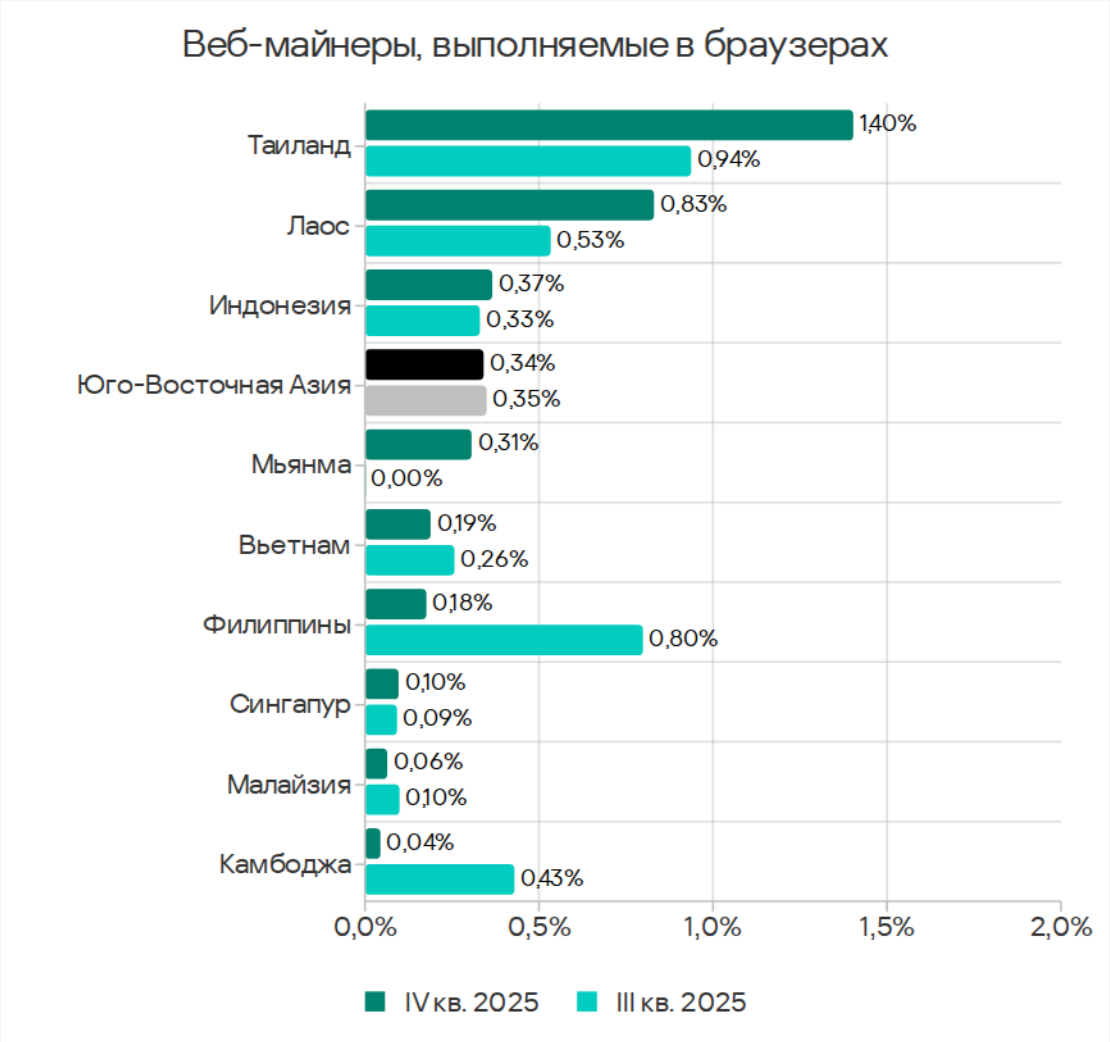
В четвертом квартале 2025 года по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, Юго-Восточная Азия лидирует с 0,34%. Это в 5,7 раза больше показателя в Восточной Азии, которая замыкает рейтинг.



Показатель в регионе колеблется.



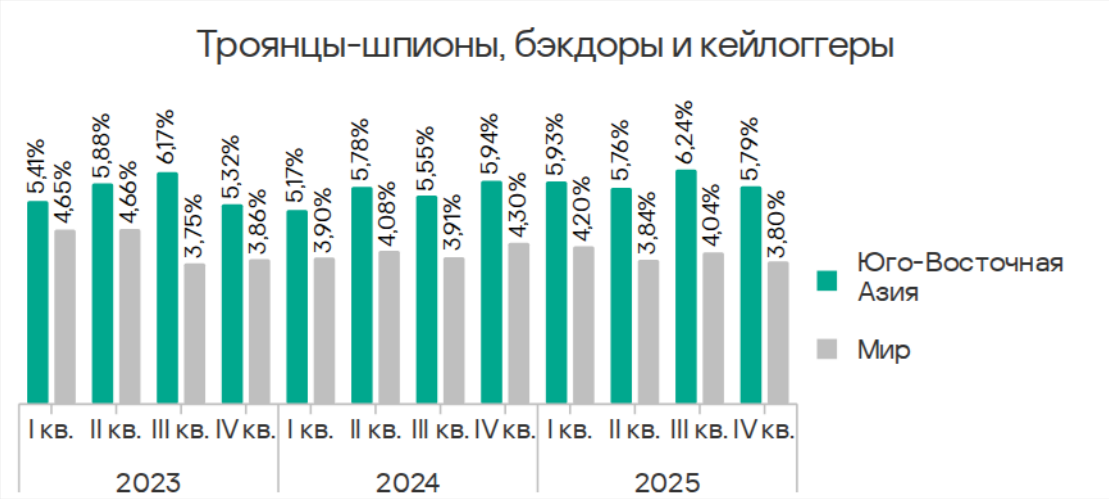
Среди стран региона по доле компьютеров АСУ, на которых блокируются веб-майнеры, с большим отрывом лидирует Таиланд с 1,40%.



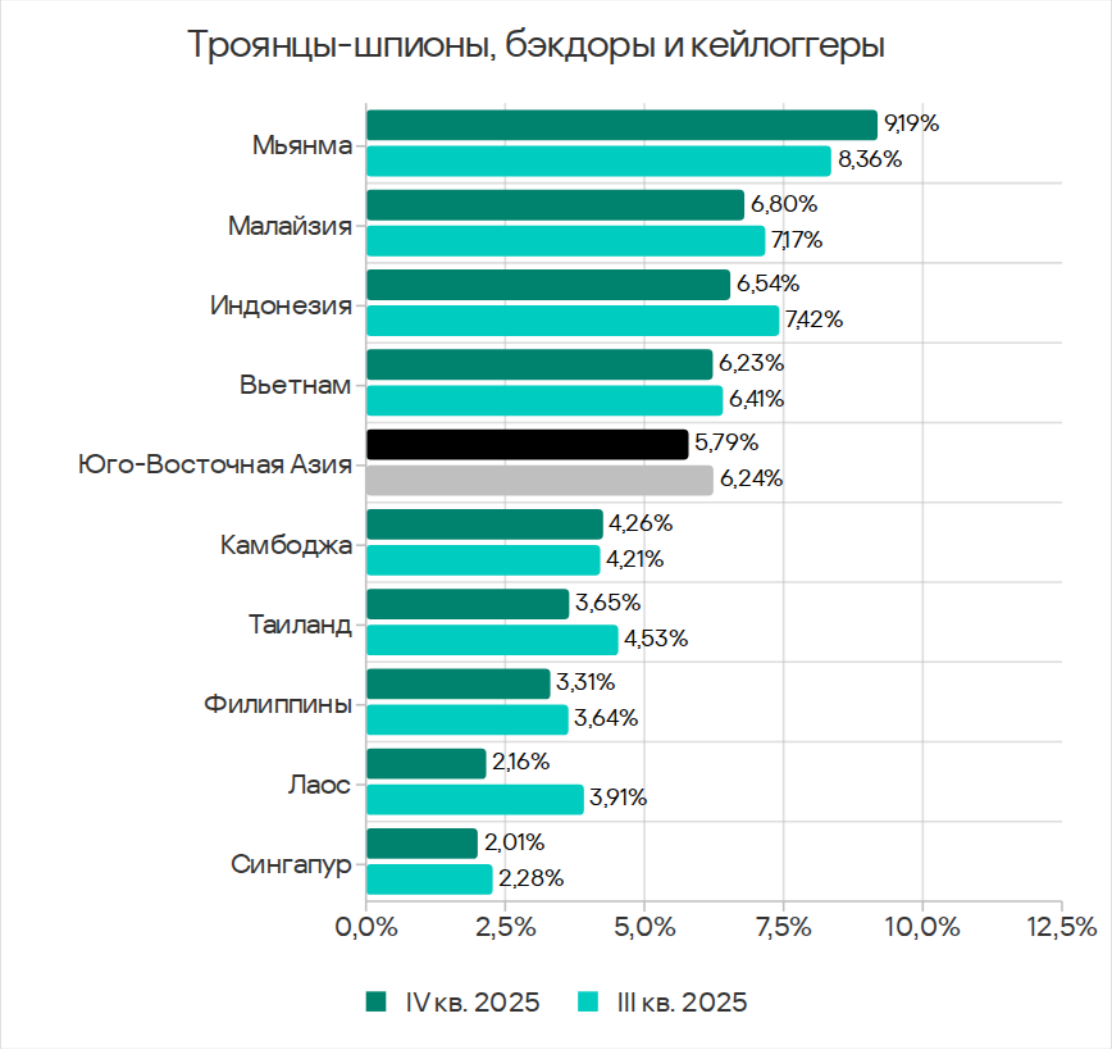
Шпионские программы

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются шпионские программы, Юго-Восточная Азия в четвертом квартале 2025 года занимает второе место с 5,79%. Это в 4,6 раза больше показателя Северной Европы, где значение показателя минимальное.

В 2025 году показатель в регионе был довольно стабильным.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы программы-шпионы, лидирует Мьянма с 9,19%. В Сингапуре показатель – наименьший (2,01%).



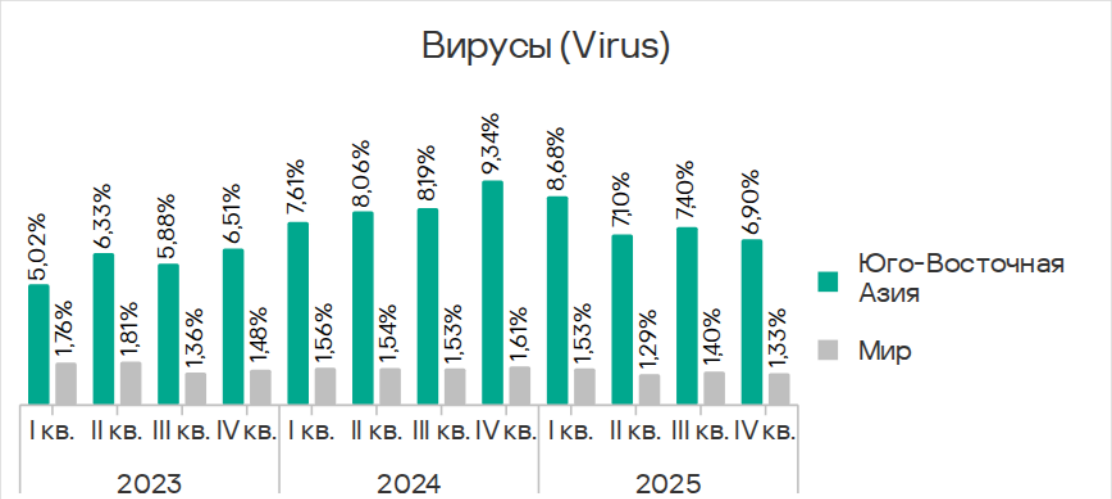
Шпионские программы в регионе блокируются во всех источниках угроз, но основной канал их распространения — электронная почта. Малайзия, Индонезия и Вьетнам, которые следуют за Мьянмой в рейтинге по шпионским программам, попали в топ-3 стран региона, лидирующих по угрозам из почтовых клиентов. А вот в Мьянме ситуация иная: страна находится на втором месте по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.

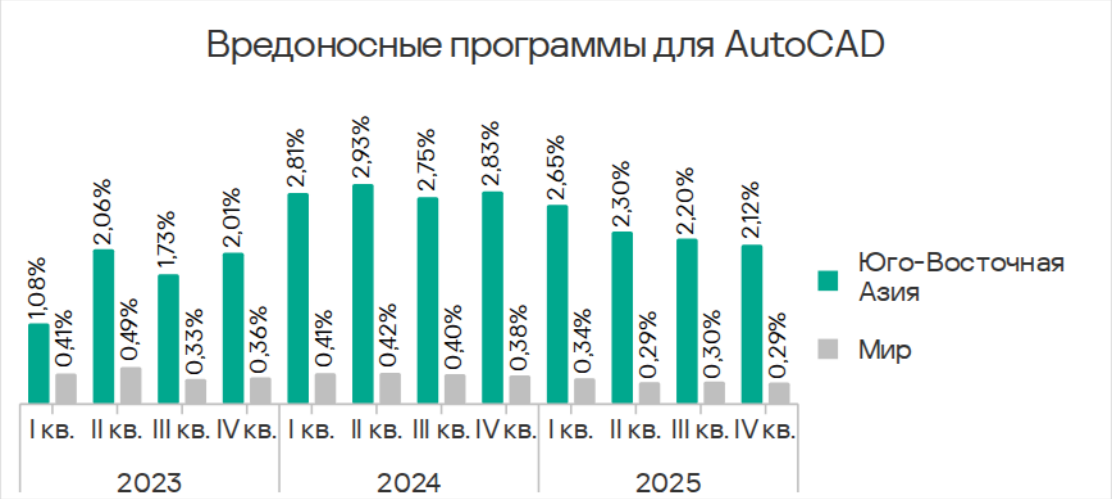
Вирусы и вредоносные программы для AutoCAD

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 отмечен явный тренд на их снижение. В четвертом квартале 2025 года и у

вирусов, и у вредоносных программ для AutoCAD показатель был наименьшим с начала 2024 года.

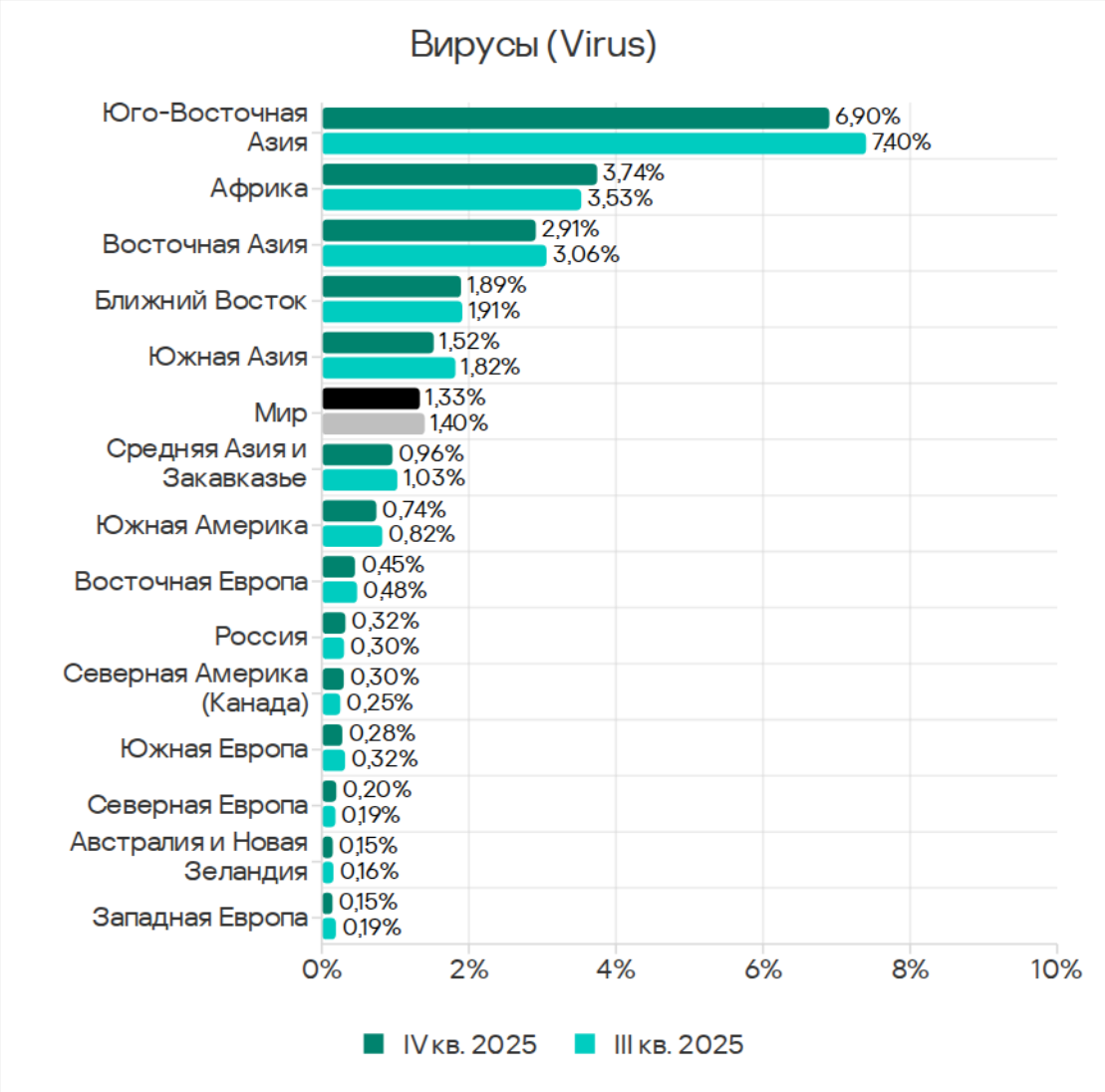




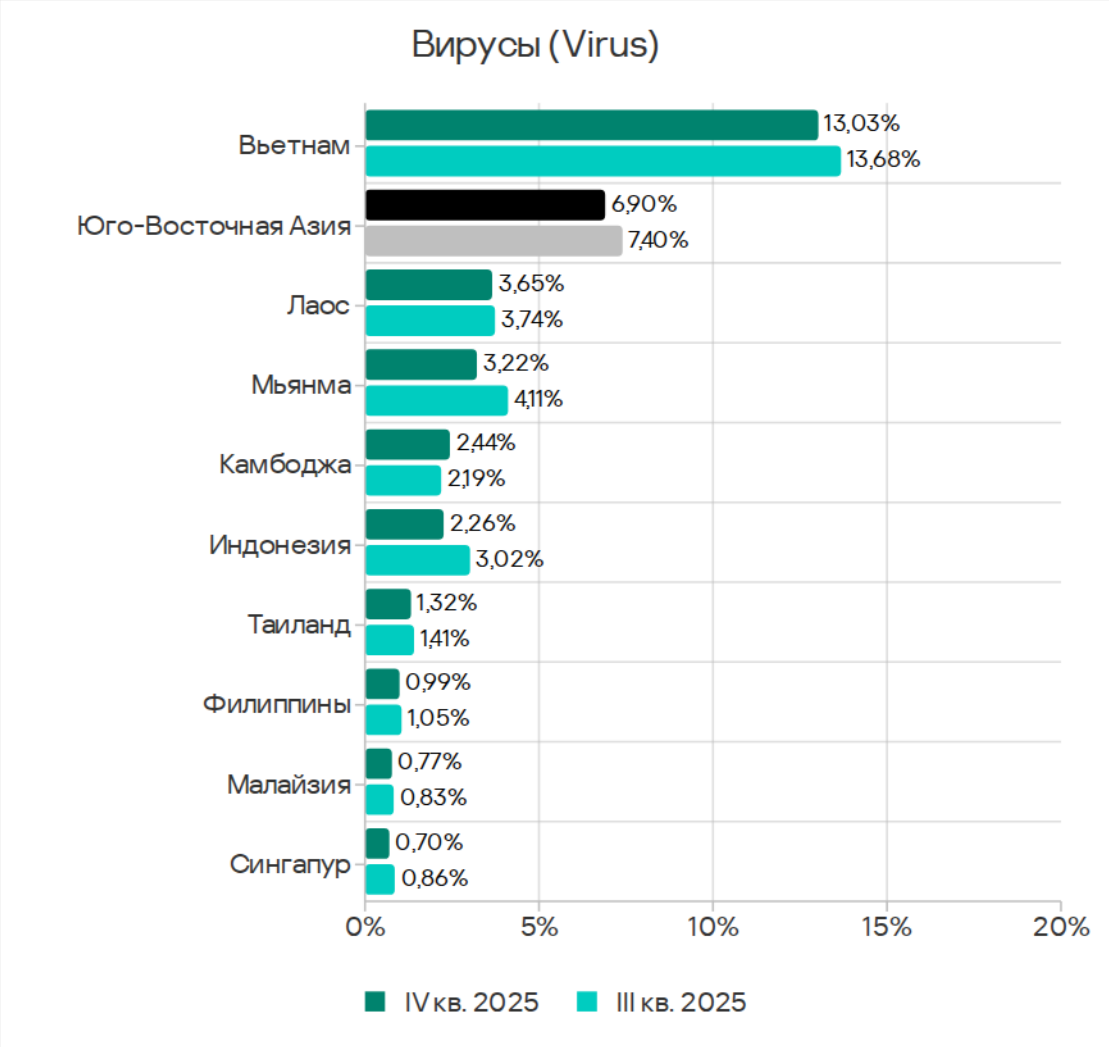
Вирусы

По доле компьютеров АСУ, на которых были заблокированы вирусы, Юго-Восточная Азия лидирует в соответствующем рейтинге с огромным отрывом от остальных регионов с 6,90%.

В Юго-Восточной Азии показатель больше, чем в Африке (следующий в рейтинге регион), в 1,8 раза, а по сравнению с Западной Европой, которая замыкает рейтинг, — в 46,0 раза.



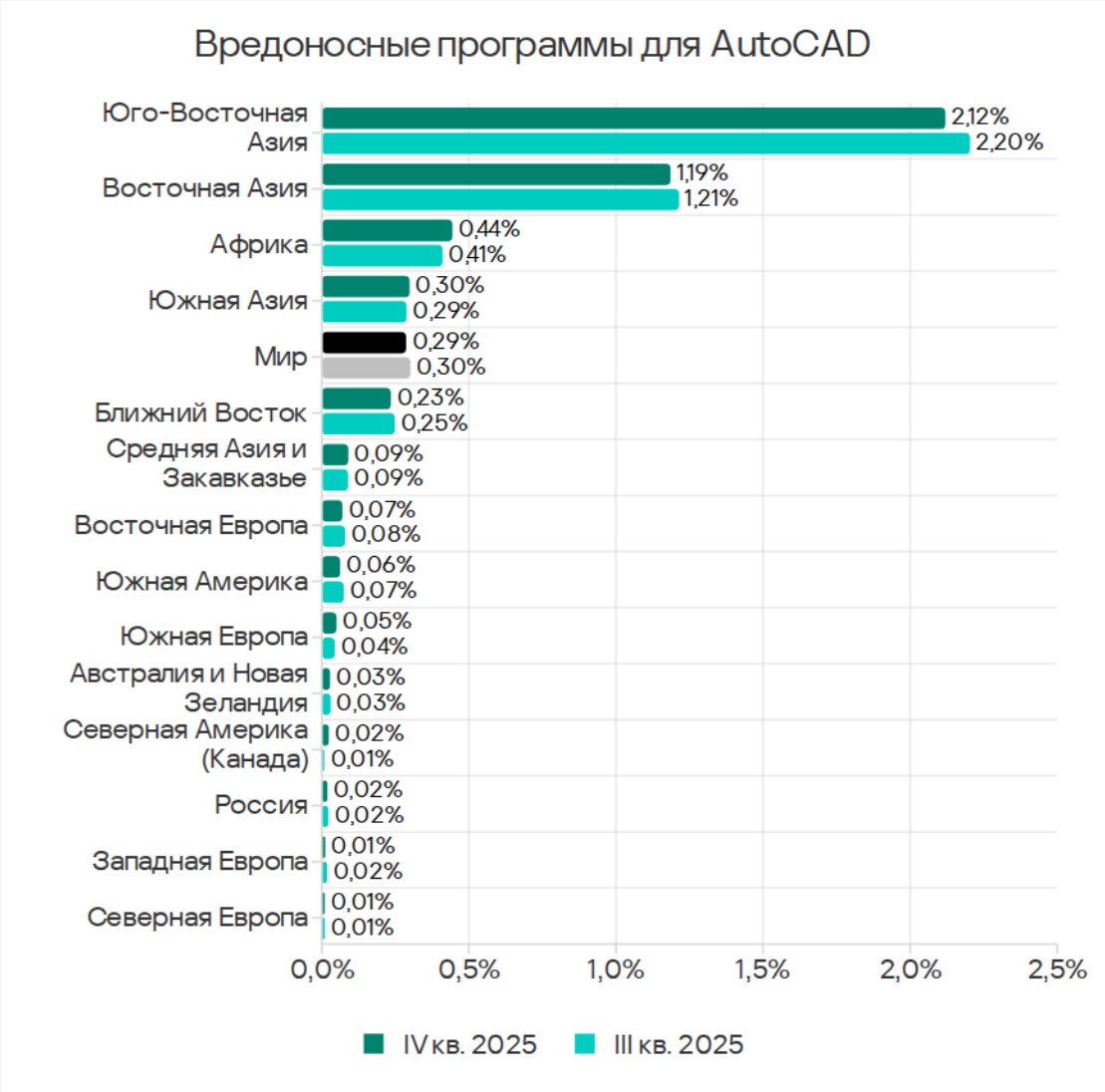
Столь яркое лидерство Юго-Восточной Азии обеспечивает Вьетнам с 13,0%. В этой стране показатель выше, чем у следующего в рейтинге Лаоса, в 3,6 раза. Наименьший показатель среди стран региона – в Сингапуре (0,70%).



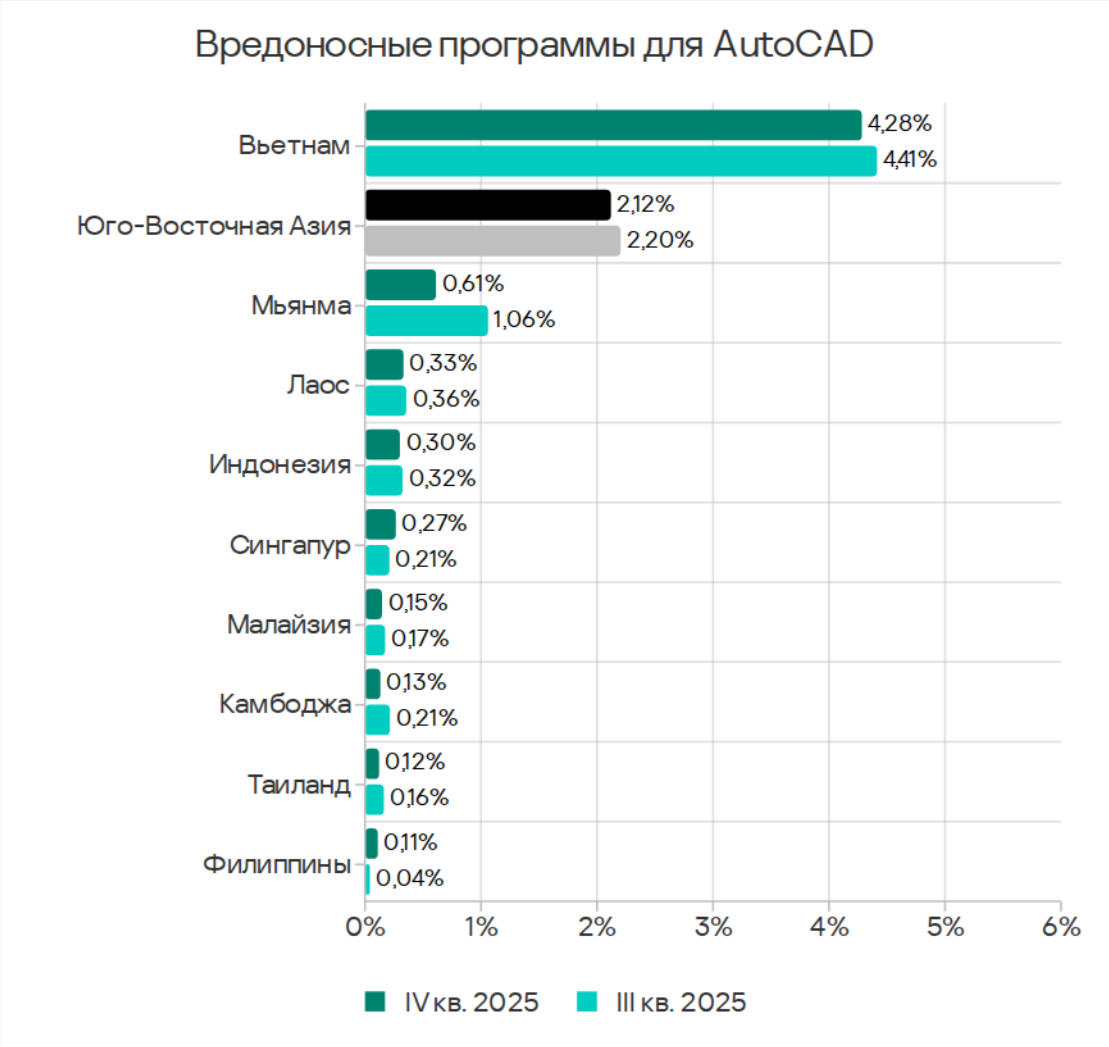
Вирусы в регионе блокируются во всех источниках угроз, но чаще всего – при скачивании из интернета. Примечательно, что самая распространенная категория вирусов во Вьетнаме – макровирусы для MS Excel (первые версии этих вирусов появились еще в 1997 году), а самая большая среди индустрий по доле обнаруженных вирусов – строительство. Похоже, что корень проблемы кроется в зараженных Excel-документах, хранящихся на сервисах для обмена файлами и на сайтах различных государственных служб Вьетнама, например, районных коммунальных и муниципальных служб.

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. Показатель в Юго-Восточной Азии – 2,12%, это больше минимального среди регионов значения — в Северной Европе — в 212 раз (!).



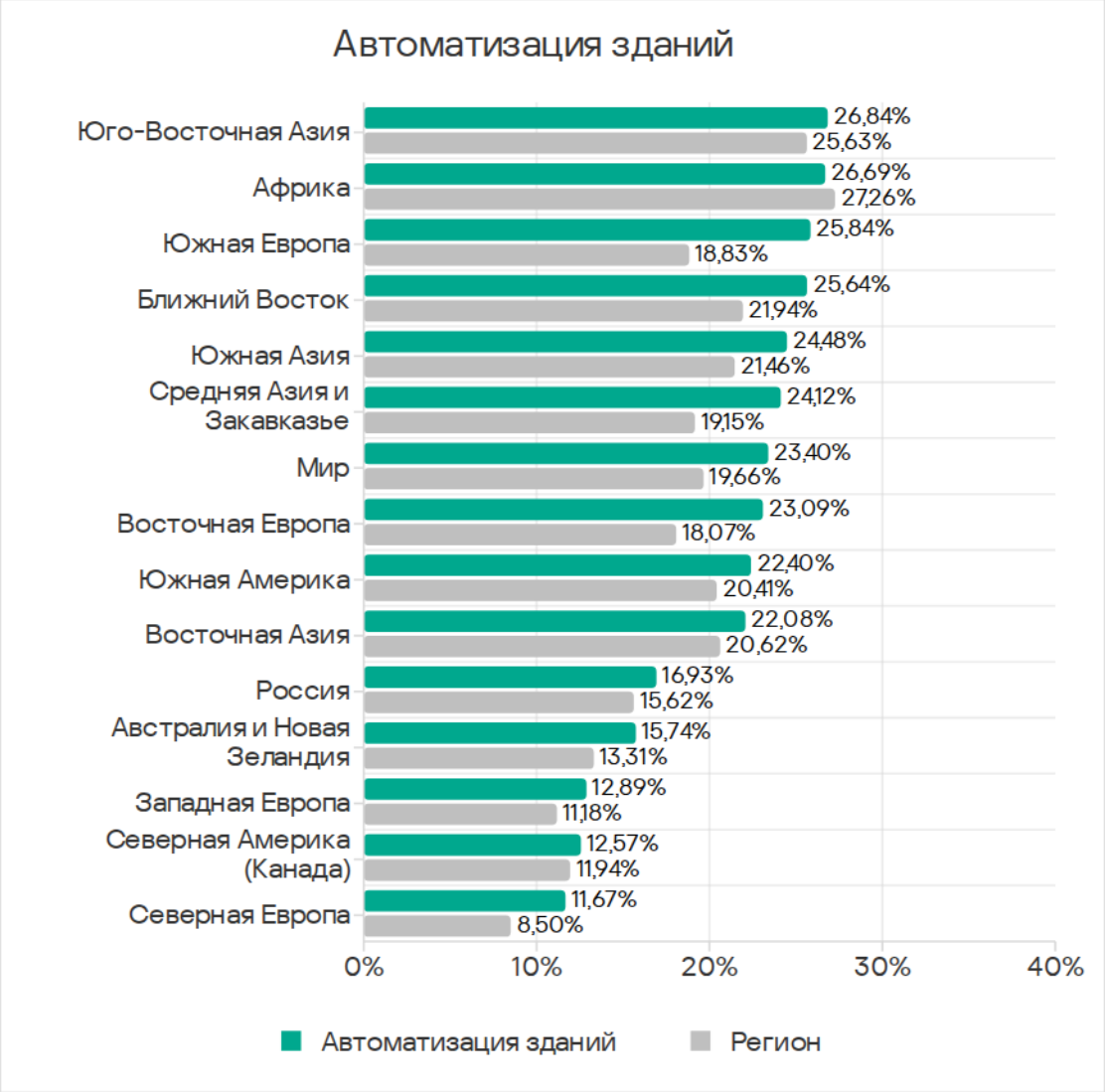
Лидерство региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, также обеспечивает Вьетнам с огромным для этой категории показателем 4,28%.



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

Отрасли

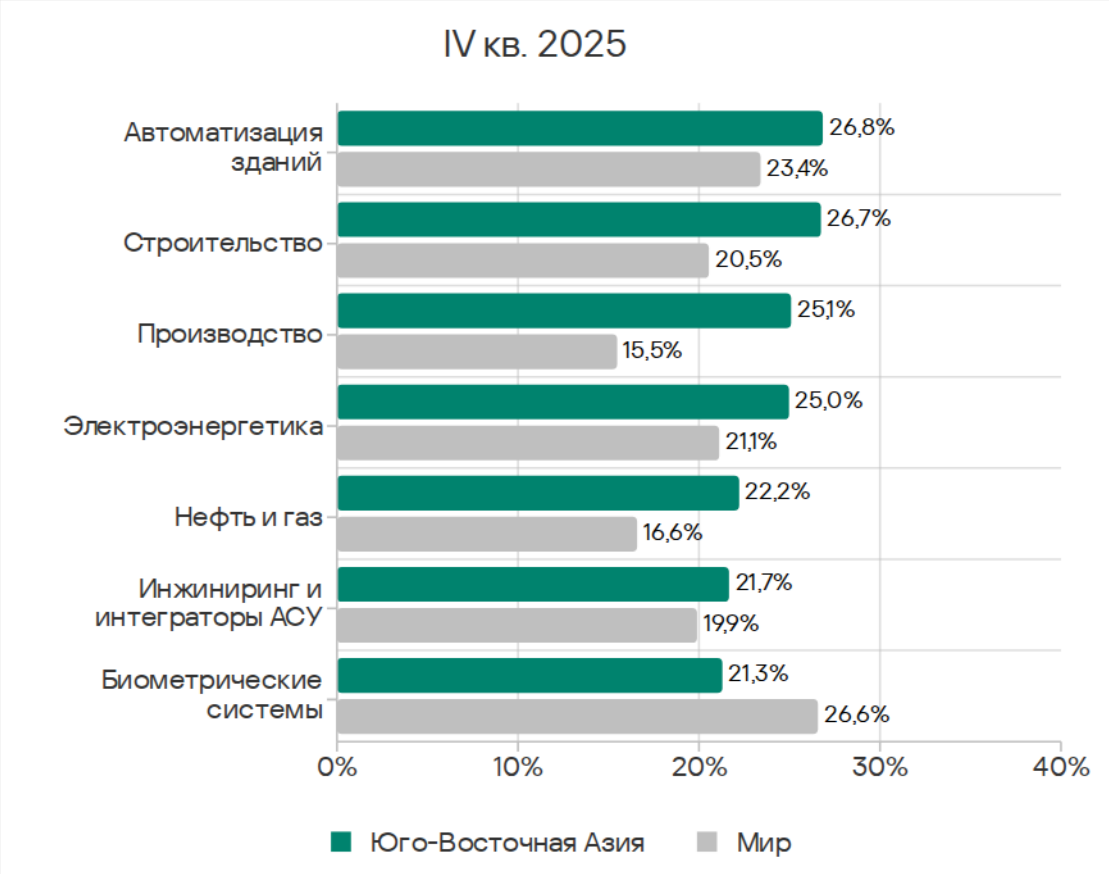
В четвертом квартале 2025 года среди регионов Юго-Восточная Азия лидирует по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в автоматизации зданий и производстве.



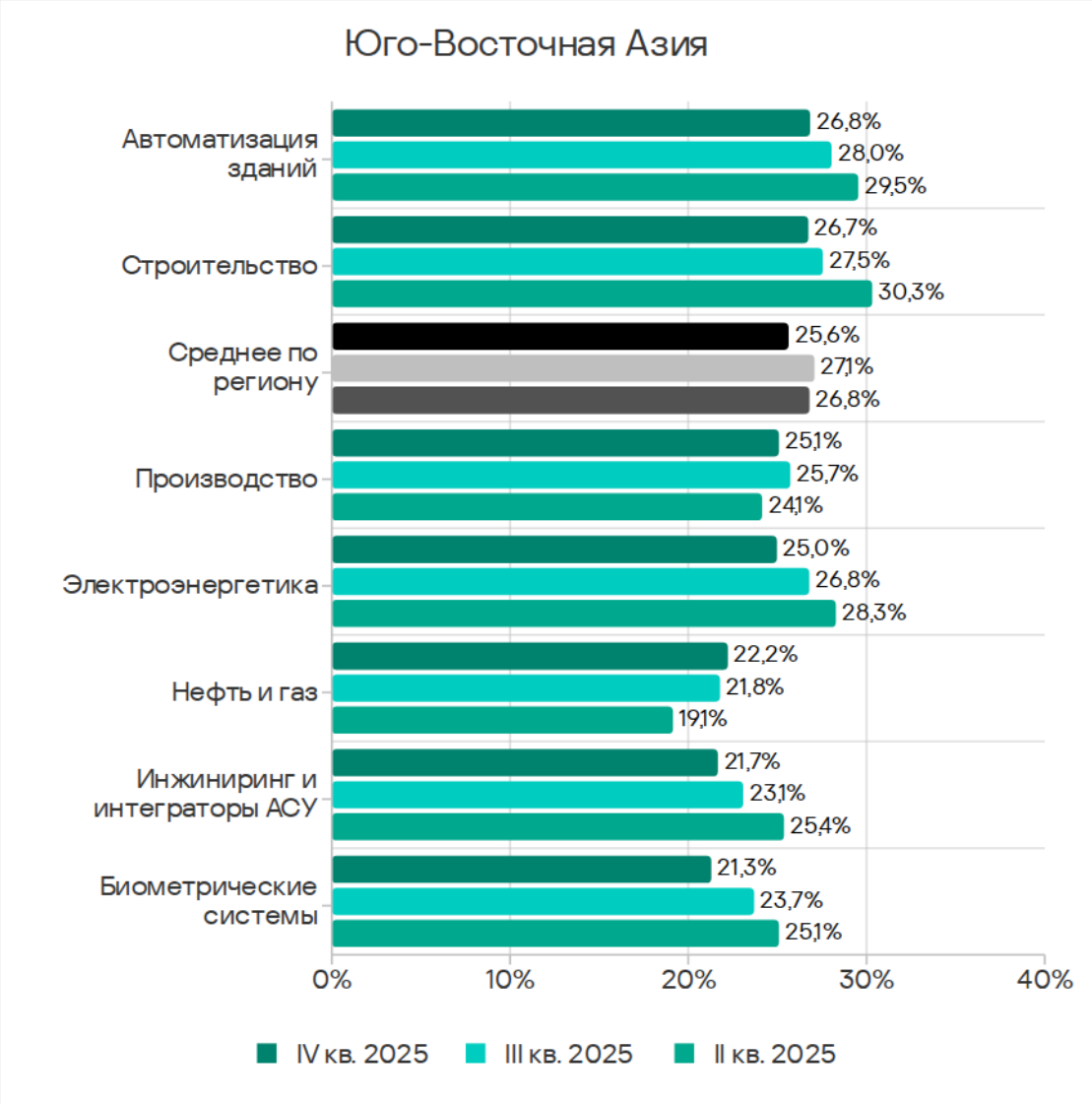
По показателям отраслей строительство, инжиниринг и интеграторы АСУ регион занимает второе место, по показателю электроэнергетической отрасли — третье.

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

В регионе показатели всех отраслей, кроме инфраструктуры биометрических систем, превышают аналогичные среднемировые. Больше всего разница у производственной (в 1,6 раза) и строительной (в 1,3 раза) отраслей.

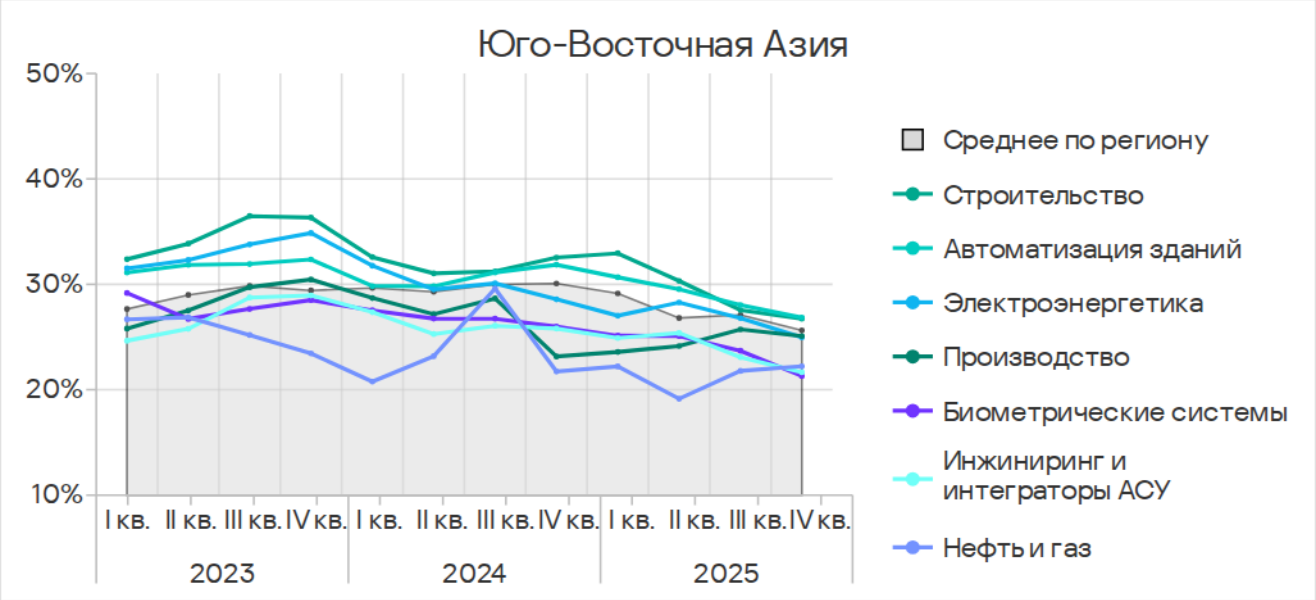


За квартал показатели всех отраслей, кроме нефти и газа, уменьшились.



Особенность региона — позиция инфраструктуры биометрических систем в рейтинге отраслей. В большинстве регионов она располагается в верхней части рейтинга и только в Юго-Восточной и Восточной Азии замыкает его.

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, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	7,34%	9,87%	9,77%	11,08%	10,79%	12,35%	8,74%	9,61%
Почтовые клиенты	6,99%	5,83%	3,72%	2,37%	5,48%	3,13%	5,65%	4,18%
Съемные носители	0,40%	0,40%	0,38%	0,54%	0,32%	0,22%	0,54%	0,42%
Сетевые папки	0,08%	0,06%	0,02%	0,03%	—	0,15%	0,06%	0,07%
Показатель отрасли в регионе	21,29%	26,84%	21,66%	24,97%	22,22%	26,74%	25,09%	

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

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	2,35%	3,83%	3,96%	5,26%	5,15%	5,31%	3,33%	3,93%
Вредоносные скрипты и фишинговые страницы	9,84%	9,51%	7,80%	7,89%	9,18%	8,64%	8,86%	7,90%
Вредоносные документы (MSOffice+PDF)	3,88%	2,96%	1,58%	1,91%	2,09%	2,25%	2,44%	2,13%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,07%	7,40%	4,78%	5,23%	6,60%	4,50%	8,20%	5,79%
Программы-вымогатели	0,32%	0,13%	0,09%	0,13%	—	0,20%	0,12%	0,11%
Майнеры — исполняемые файлы для ОС Windows	0,45%	0,38%	0,31%	0,54%	0,64%	0,66%	0,59%	0,32%
Веб-майнеры, выполняемые в браузерах	0,47%	0,37%	0,43%	0,52%	0,48%	1,00%	0,65%	0,34%
Вредоносные программы для AutoCAD	0,26%	0,75%	0,95%	1,47%	1,45%	4,23%	0,71%	2,12%
Черви (Worm)	1,93%	2,21%	1,49%	2,45%	0,64%	1,30%	2,44%	2,05%
Вирусы (Virus)	2,48%	6,17%	3,29%	6,03%	2,90%	7,27%	4,22%	6,90%
Показатель отрасли в регионе	21,29%	26,84%	21,66%	24,97%	22,22%	26,74%	25,09%	

Автоматизация зданий

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

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

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- третье место по показателю угроз в сетевых папках;

- первое место по доле компьютеров АСУ, на которых были заблокированы вирусы;
- второе место по показателю угроз следующих категорий: шпионские программы, веб-майнеры, вредоносные программы для AutoCAD;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов;
- третье место по показателю угроз из интернета, на съемных носителях и в сетевых папках;
- второе место по показателю угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, вирусы;
- третье место по показателю шпионских программ, программ-вымогателей и червей.

Строительство

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

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

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- второе место по показателю сетевых папок;
- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: ресурсы в интернете из списка запрещенных, вирусы и веб-майнеры;
- второе место по показателю вредоносных программ для AutoCAD;
- третье место по показателю шпионских программ.

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 показателю угроз следующих категорий: ресурсы в интернете из списка запрещенных, вирусы, вредоносные программы для AutoCAD, майнеры обеих категорий;
- второе место по показателю программ-вымогателей.

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 были заблокированы угрозы в почтовых клиентах,
- третье место по показателю угроз из интернета, на съемных носителях и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: вредоносные документы, шпионские программы, вирусы, веб-майнеры;
- второе место по показателю угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вредоносные программы для AutoCAD.

Среди отраслей в регионе производство занимает:

- второе место по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей;
- третье место по показателю угроз из почтовых клиентов;
- первое место по показателю шпионских программ,
- второе место по показателю червей и майнеров обеих категорий;
- третье место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вредоносные документы.

Электроэнергетика

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

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

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- первое место по доле компьютеров АСУ, на которых были заблокированы вирусы;
- второе место по показателю ресурсов в интернете из списка запрещенных и вредоносных программ для AutoCAD;
- третье место по показателю шпионских программ и веб-майнеров.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угроз на съемных носителях;
- второе место по показателю угроз из интернета,
- первое место по показателю червей;
- второе место по показателю ресурсы в интернете из списка запрещенных и вредоносных программ для AutoCAD;
- третье место по показателю вирусов и майнеров обеих категорий.

Инжиниринг и интеграторы АСУ

Юго-Восточная Азия находится на втором 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 были заблокированы угрозы в почтовых клиентах;
- третье место по показателю угроз из интернета;
- первое место по доле компьютеров АСУ, на которых были заблокированы веб-майнеры;
- второе место по показателю угроз следующих категорий: ресурсы в интернете из списка запрещенных, шпионские программы, вредоносные программы для AutoCAD;
- третье место по показателю вирусов.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

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

Биометрические системы

Юго-Восточная Азия находится на восьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

Среди регионов по показателям в инфраструктуре биометрических систем Юго-Восточная Азия занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах и сетевых папках;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD;

- третье место по показателю вредоносных документов, шпионских программ и веб-майнеров.

Среди отраслей в регионе биометрические системы занимают:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах;
- второе место по показателю угроз в сетевых папках;
- первое место по показателю угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, программы-вымогатели;
- второе место по показателю шпионских программ.

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 четвертое место среди регионов по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях. Показатель региона превышает среднемировой в 1,6 раза.

Южная Азия находится на пятом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.

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 пятом — по показателю программ-вымогателей. Эти категории угроз в регионе распространяются через все источники угроз, но преимущественно на съемных носителях.

Высокий уровень угроз из интернета

В четвертом квартале 2025 года в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Южная Азия поднялась с третьего на первое место. По росту этого показателя в четвертом квартале 2025 года регион находится на первом месте.

Индия и Афганистан — две страны региона, где показатель угроз из интернета за квартал увеличился. Если в Афганистане изменения были незначительными, то в Индии значение увеличилось в 1,34 раза.

По доле компьютеров АСУ, на которых угрозы блокировались из интернета, во всех отраслях, кроме строительства и электроэнергетики, Южная Азия на первом месте среди регионов.

Особенность квартала: вредоносные скрипты и фишинговые страницы

В четвертом квартале 2025 года в регионе отмечен резкий рост доли компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы. В результате в рейтинге регионов по этому показателю Южная Азия поднялась с восьмого на первое место.

За квартал показатель в Южной Азии вырос в 1,49 раза, по его росту регион также находится на первом месте.

Основным фактором столь значительного роста стала волна заражений веб-сайтов под управлением WordPress, популярных в Индии. В результате заражения посетители сайтов вместе с контентом получали вредоносный JS-код, который был предназначен для перенаправления пользователя на фишинговый сайт.

Больше всего в регионе показатель категории вредоносные скрипты и фишинговые страницы вырос в отраслях производство и инжиниринг и интеграторы АСУ. В этих же отраслях больше всего вырос показатель угроз из интернета.

Рост в регионе показателей и интернета, и вредоносных скриптов и фишинговых страниц обеспечила Индия, где их значение за квартал увеличилось в 1,34 и 1,87 раза соответственно.

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.

В четвертом квартале ситуация именно в этой стране привела к тому, что регион оказался на первом месте по показателям угроз из интернета и категории вредоносные скрипты и фишинговые страницы.

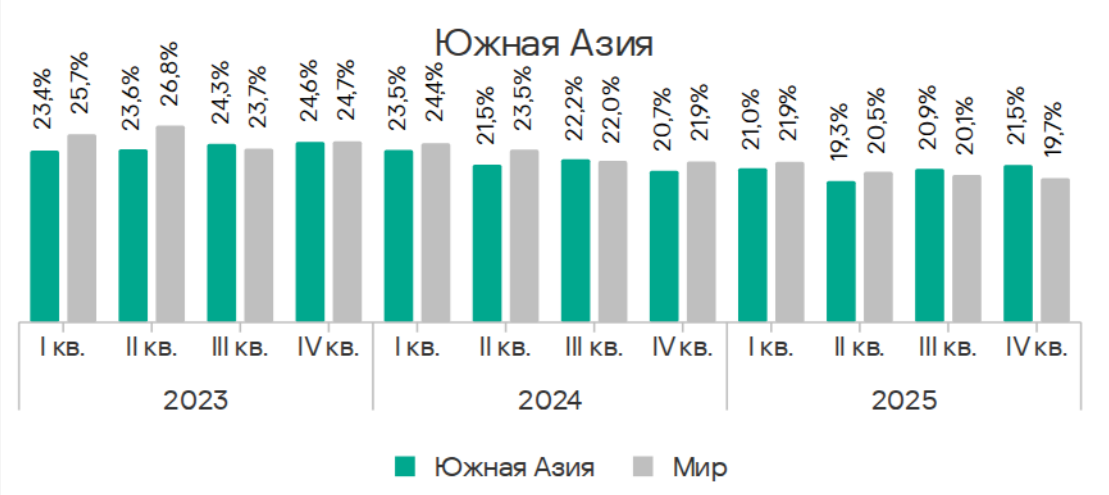
Ситуация с кибербезопасностью в Афганистане заметно отличается от других стран региона в отношении контроля подключения съемных носителей. Это заметно по показателям съемных носителей и самораспространяющегося ПО в разных странах — в Афганистане они заметно выше, чем в других странах региона. Такая же ситуация в Афганистане и с сетевыми папками.

Статистика по всем угрозам

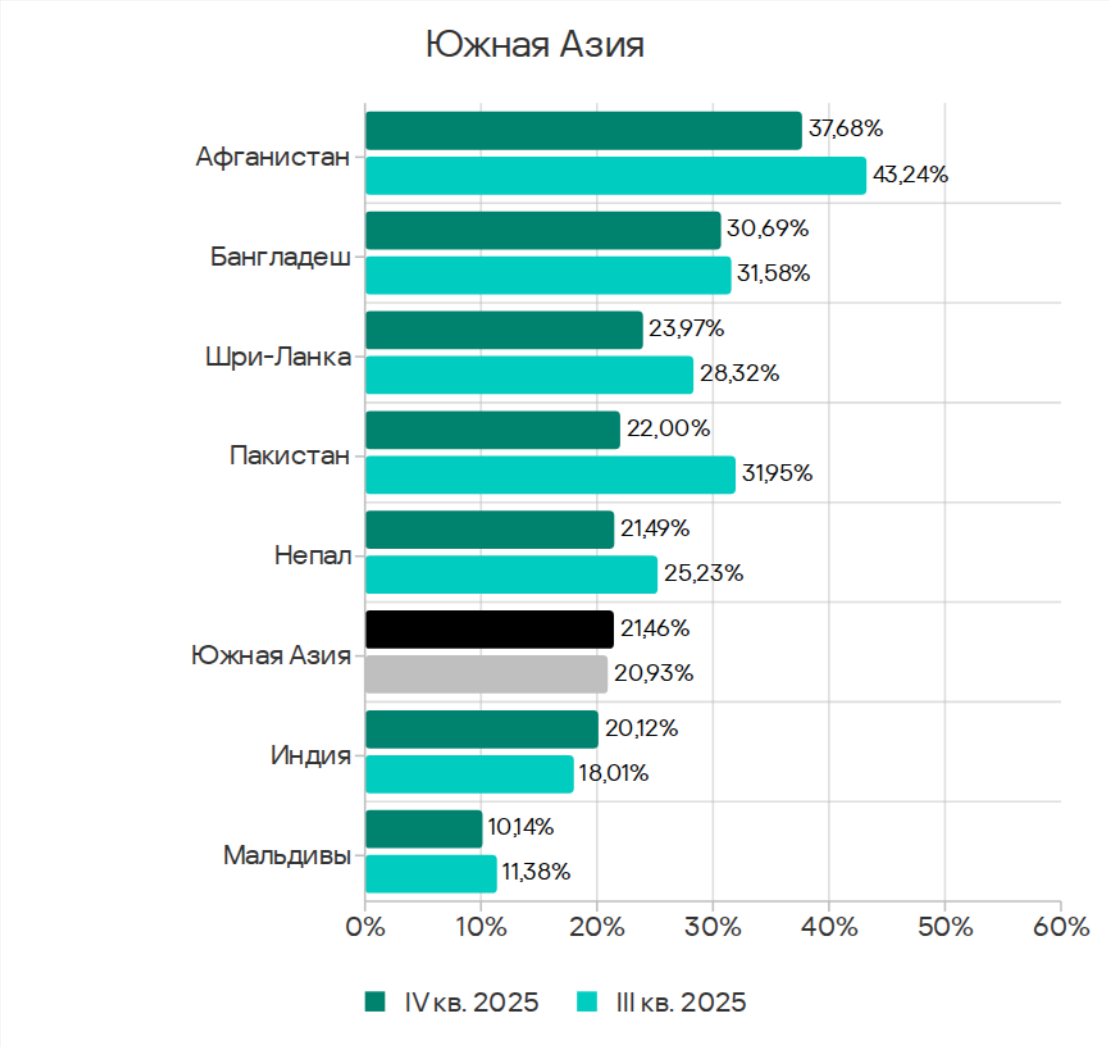
В четвертом квартале 2025 года Южная Азия в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, поднялась с пятого на четвертое место. Во втором квартале регион был на девятой позиции.

Южная Азия – один из четырех регионов, где доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал увеличилась. Показатель в регионе растет второй квартал подряд.

Значение в регионе — 21,5% — самое высокое с четвертого квартала 2024 года. Оно в 2,5 раза больше, чем в Северной Европе, которая замыкает этот рейтинг.



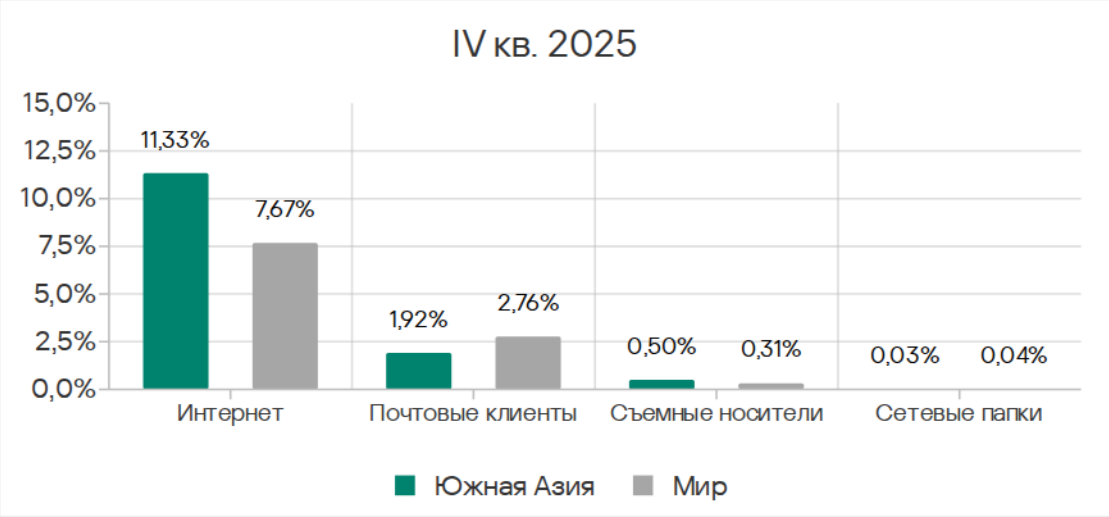
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 10,14% на Мальдивах до 37,68% в Афганистане.



Источники угроз

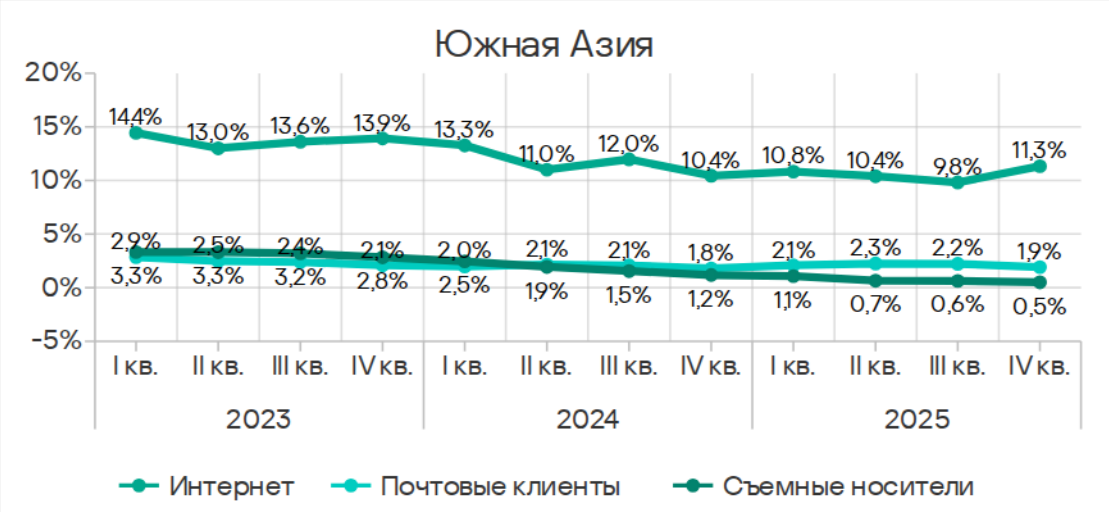
В четвертом квартале 2025 года у Южной Азии выше, чем среднемировые, показатели по двум источникам угроз:

- интернет — в 1,5 раза, первое место среди регионов;
- съемные носители — в 1,6 раза, четвертое место среди регионов.



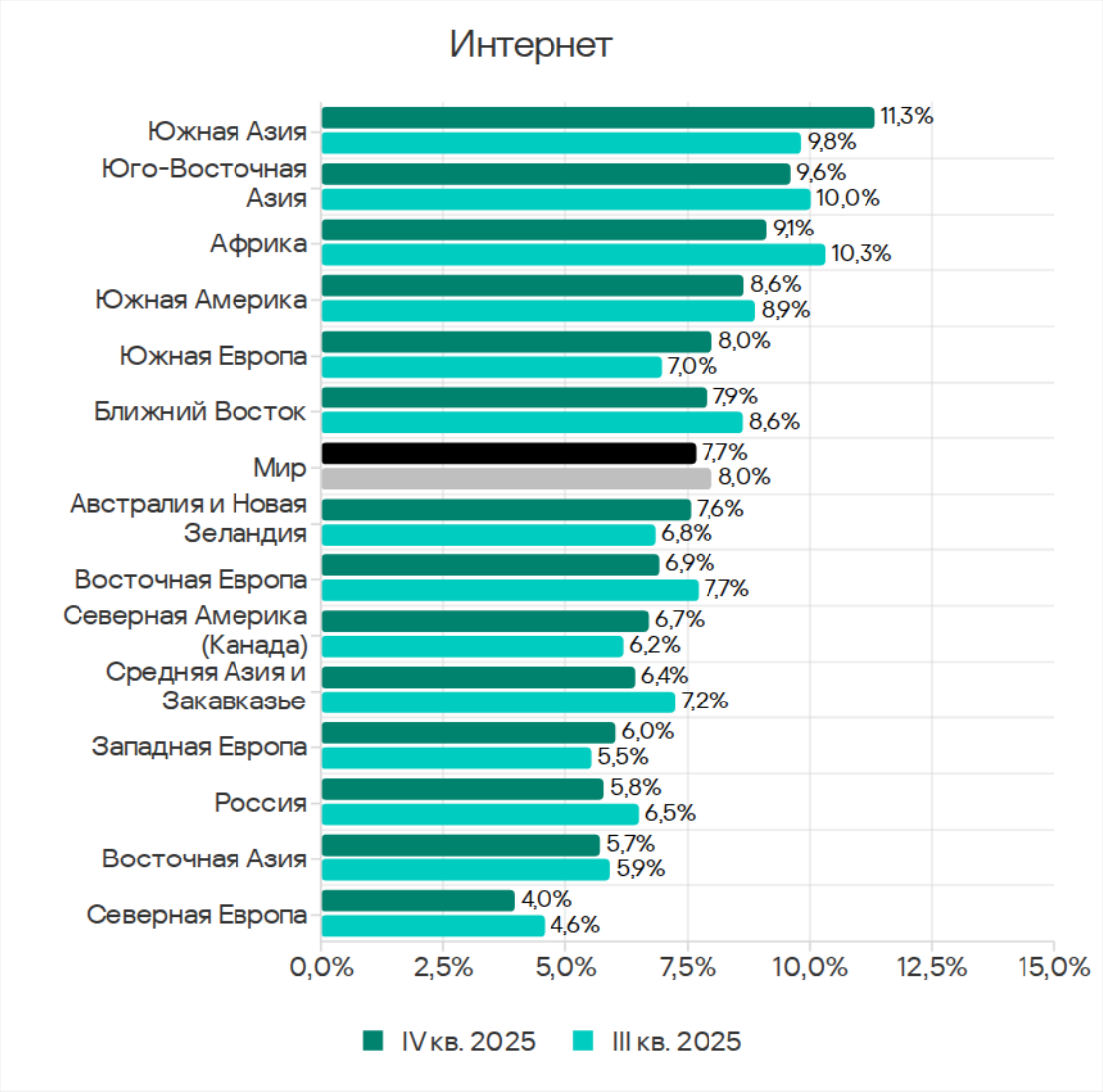
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, из всех источников угроз увеличилась только у интернета.

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

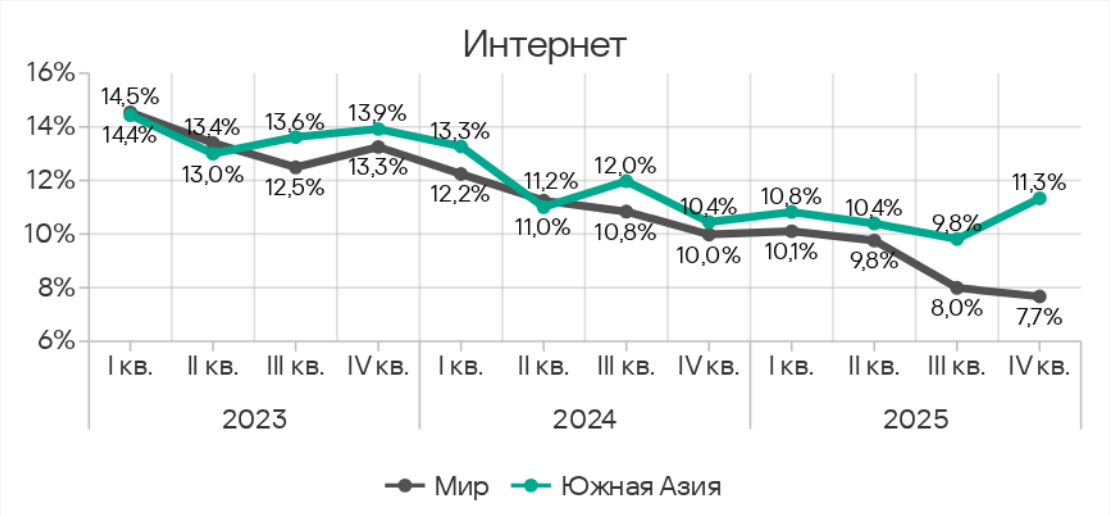


Интернет

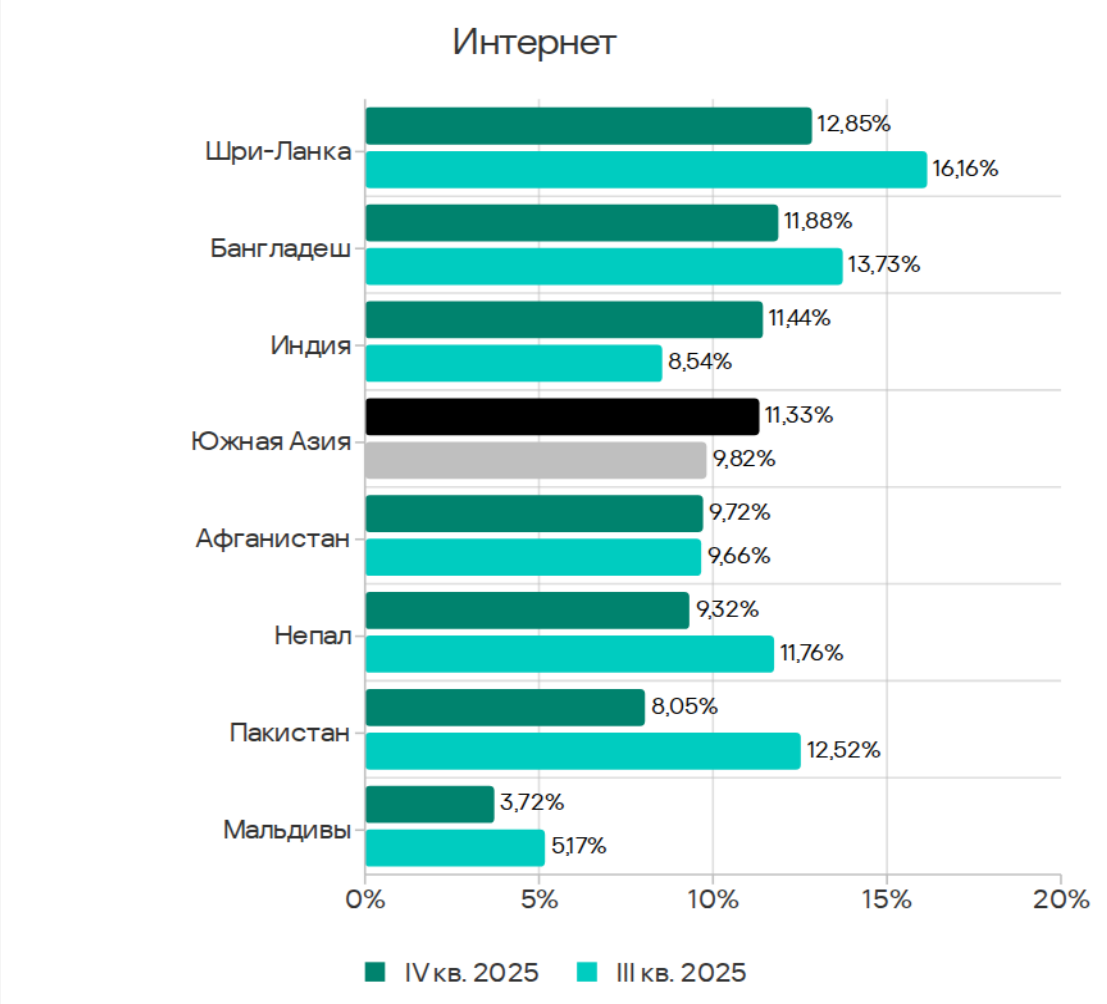
В четвертом квартале 2025 года Южная Азия по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, поднялась с третьего на первое место среди регионов с 11,33%. Этот показатель в 2,9 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.



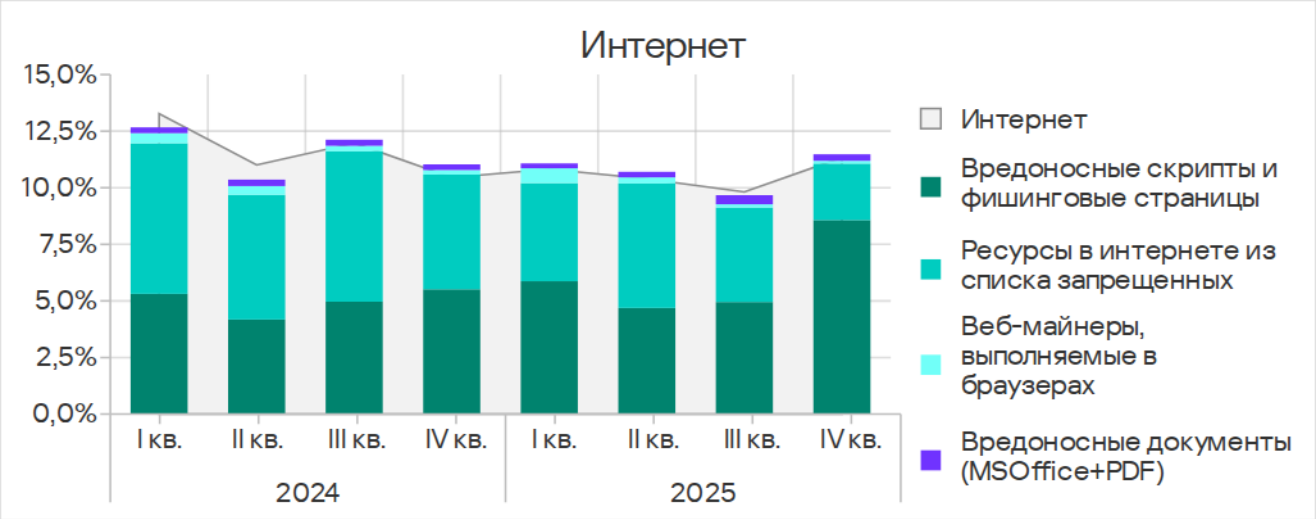
По росту доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, в четвертом квартале Южная Азия заняла первое место среди регионов. Показатель четвертого квартала 2025 года в Южной Азии – самый высокий с четвертого квартала 2024 года.



Показатели стран региона варьируют от 3,72% на Мальдивах до 12,85% в Шри-Ланке. Индия и Афганистан — две страны региона, где доля компьютеров АСУ, на которых блокируются угрозы из интернета, за квартал увеличилась, причем в Индии — в 1,34 раза.



Основные категории угроз из интернета, которые были заблокированы на компьютерах АСУ в регионе в четвертом квартале 2025 года: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, вредоносные документы.



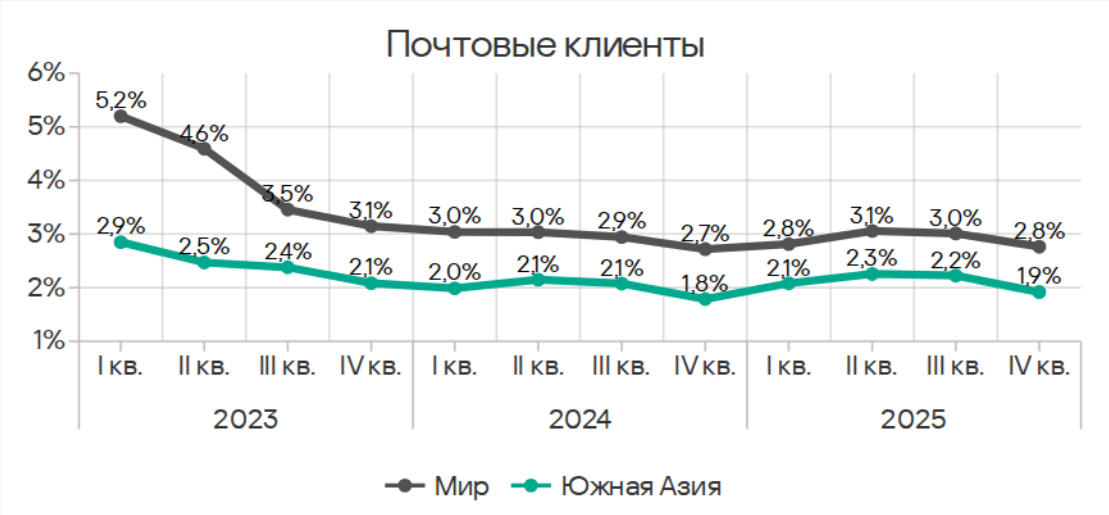
В четвертом квартале 2025 года в Южной Азии в 1,73 раза выросла доля компьютеров АСУ, на котоырх были заблокированы вредоносные скрипты и фишинговые страницы в интернете.

По доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, в регионе лидирует Афганистан.

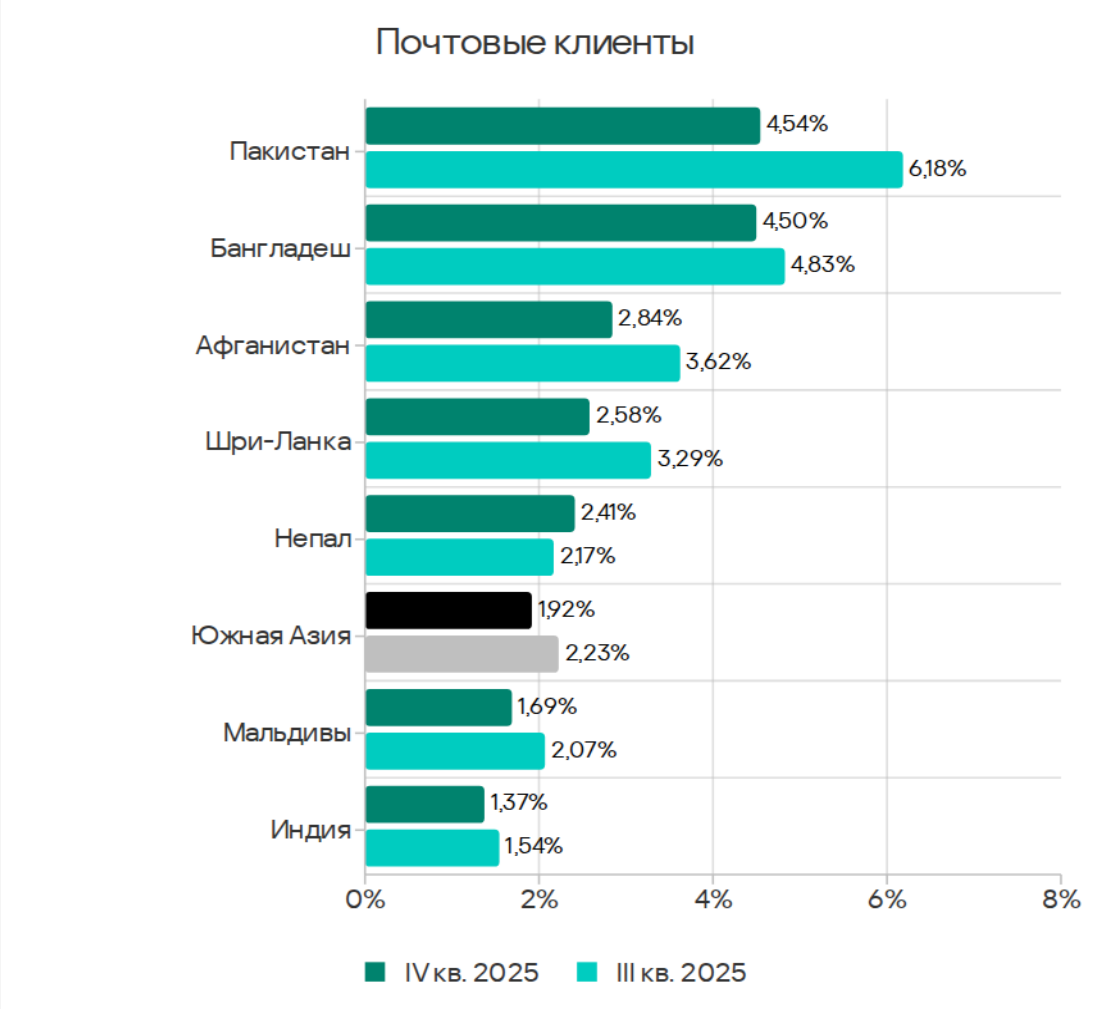
Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, Южная Азия среди регионов заняла восьмое место с 1,92%. Это в 3,0 раза больше, чем в Северной Европе, где показатель – наименьший.

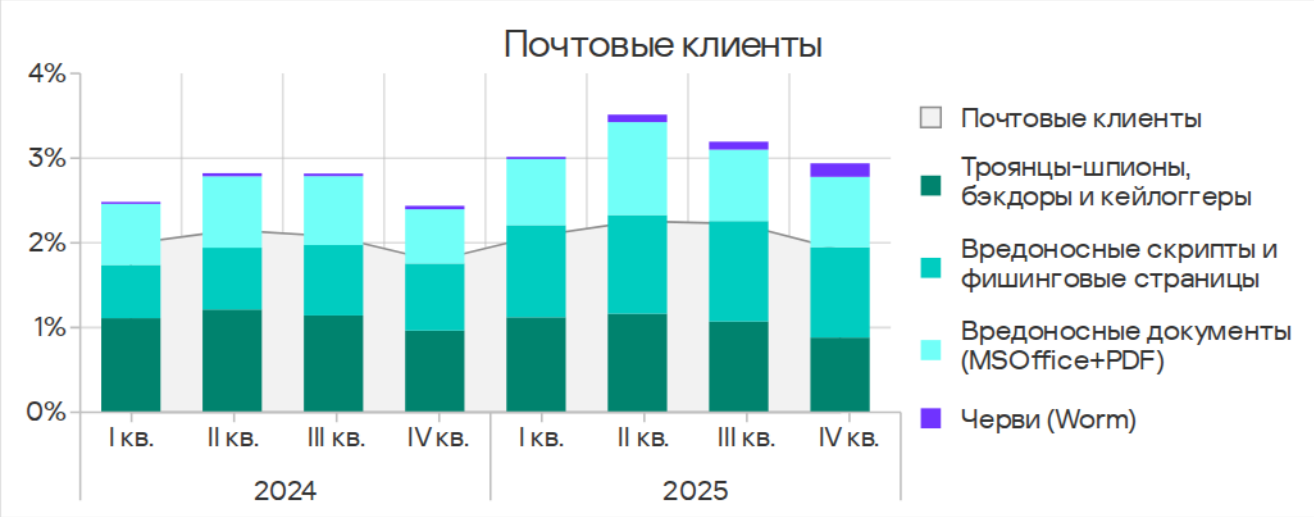
После роста в течение трех предыдущих кварталов значение этого показателя в регионе уменьшилось, но все же оказалось выше, чем в четвертом квартале 2024 года.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, лидирующие позиции заняли Пакистан с 4,54% и Бангладеш с 4,50%. Наименьший показатель – в Индии (1,37%).



Основные категории угроз из почтовых клиентов, заблокированные на компьютерах АСУ: вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы. Пакистан оказался на первом месте также по показателю вредоносных документов, а Бангладеш — по показателю шпионских программ.



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых были заблокированы черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, в ходе которых были атакованы организации во всех регионах мира. В Южной Азии пик атак пришелся на ноябрь.

Злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Под видом резюме (Curriculum Vitae) такие письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm). При запуске файла происходило заражение системы.

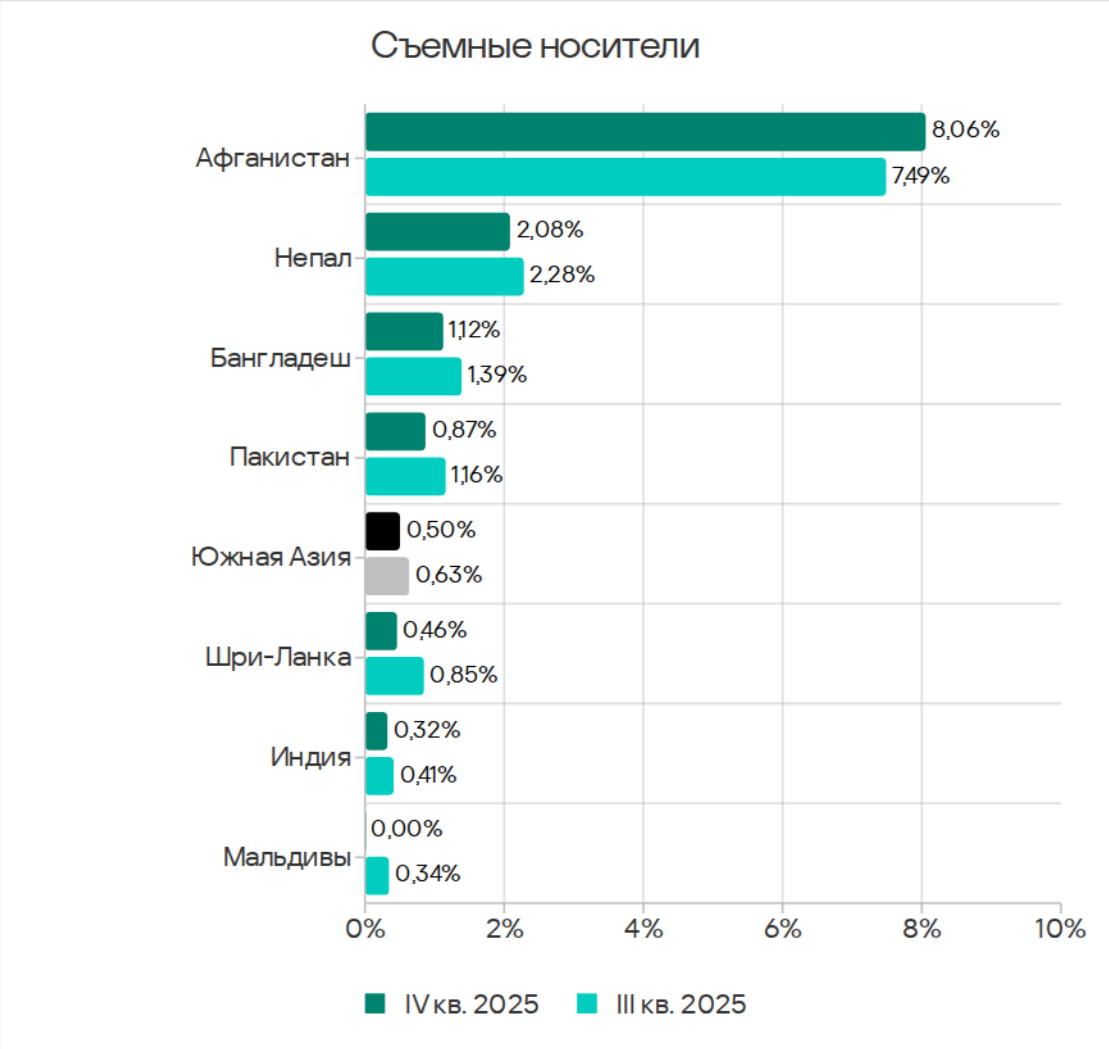
Как правило, такие кампании направлены на доставку вредоносного ПО для кражи данных, а также на доставку программ-шпионов или инструментов для удаленного управления (RAT).

Съемные носители

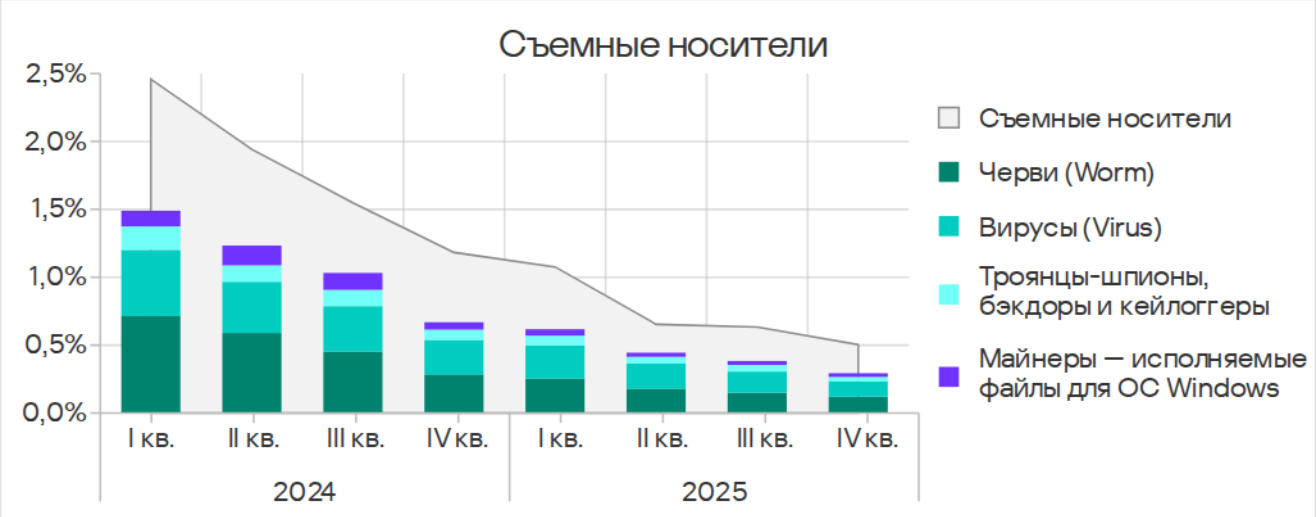
По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Южная Азия заняла четвертое место среди регионов с 0,50%. Это в 10,0 раза больше, чем показатель в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с большим

отрывом лидирует Афганистан с 8,06%. Показатели остальных стран варьируют от около нулевого значения на Мальдивах до 2,08% в Непале.



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

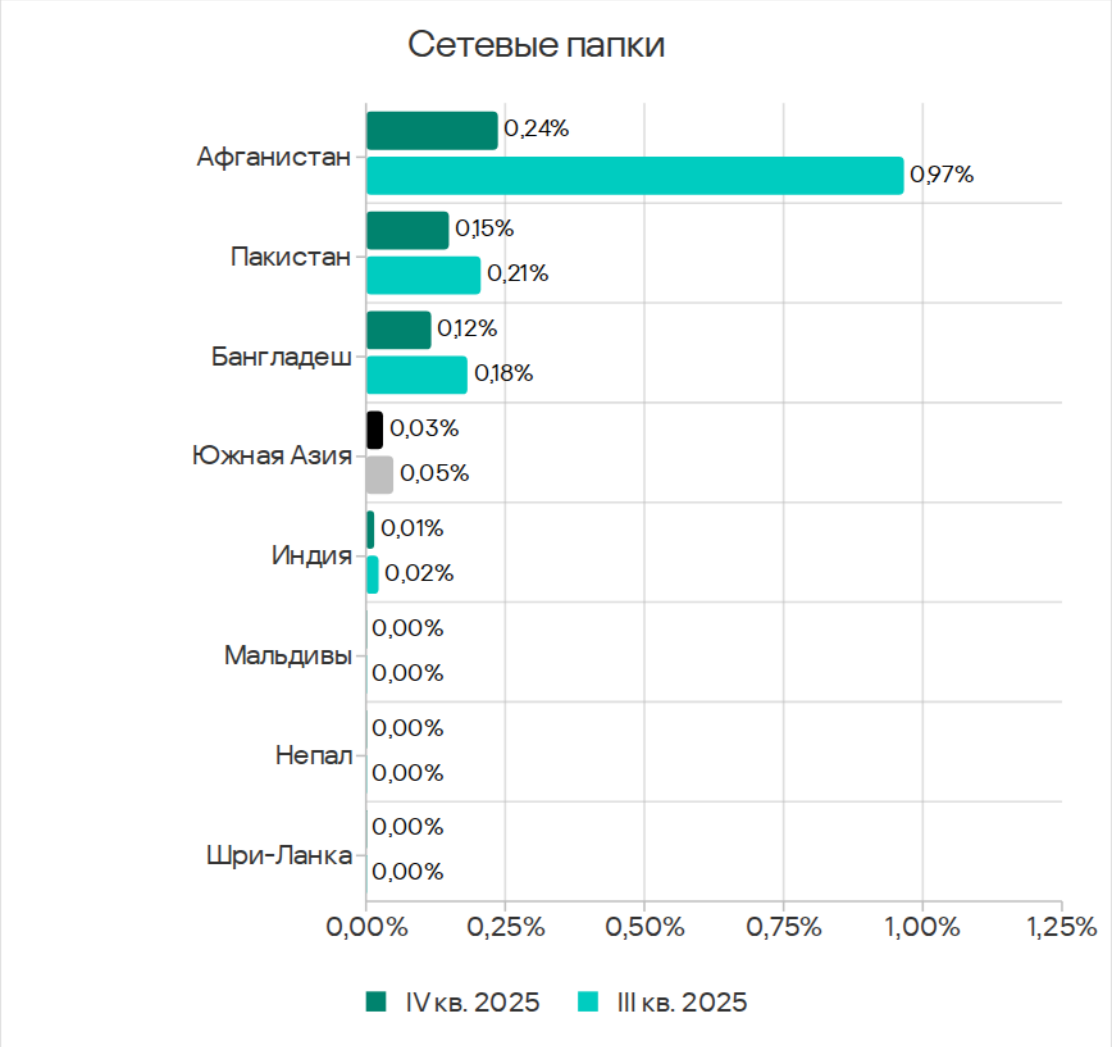


Афганистан также лидирует (и тоже с большим отрывом) по доле компьютеров АСУ, на которых были заблокированы вирусы и черви.

Сетевые папки

Южная Азия занимает пятое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, с 0,03%. В четвертом квартале 2025 года показатель Южной Азии в 4,4 раза превышает показатель Северной Европы, которая замыкает этот рейтинг.

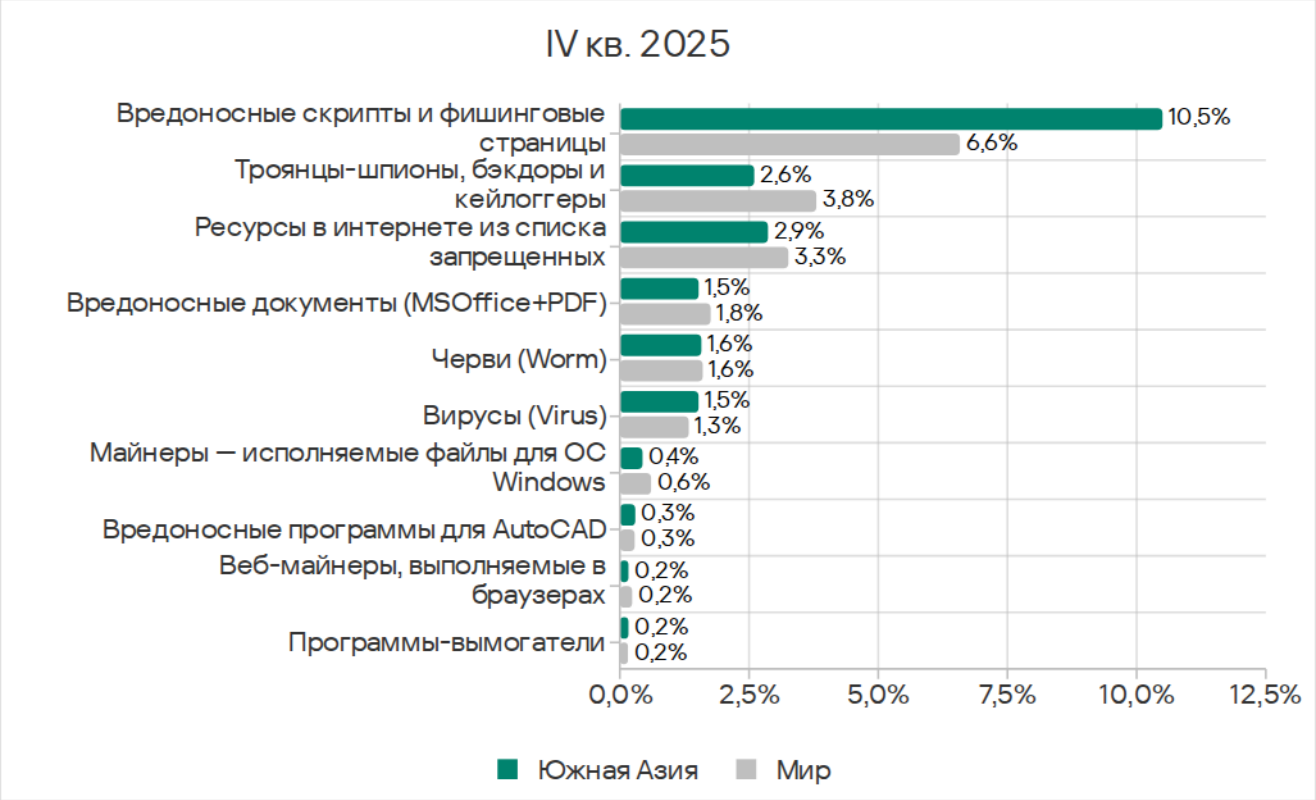
По доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, среди стран региона лидирует Афганистан с 0,24%. После резкого роста в предыдущем квартале показатель в стране вернулся к обычным значениям. Наименьший показатель наблюдается на Мальдивах, в Непале и Шри-Ланке.



Основные категории угроз, которые распространяются в регионе через сетевые папки: вирусы, вредоносные скрипты, черви и вредоносные программы для AutoCAD.

Категории угроз

В четвертом 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.



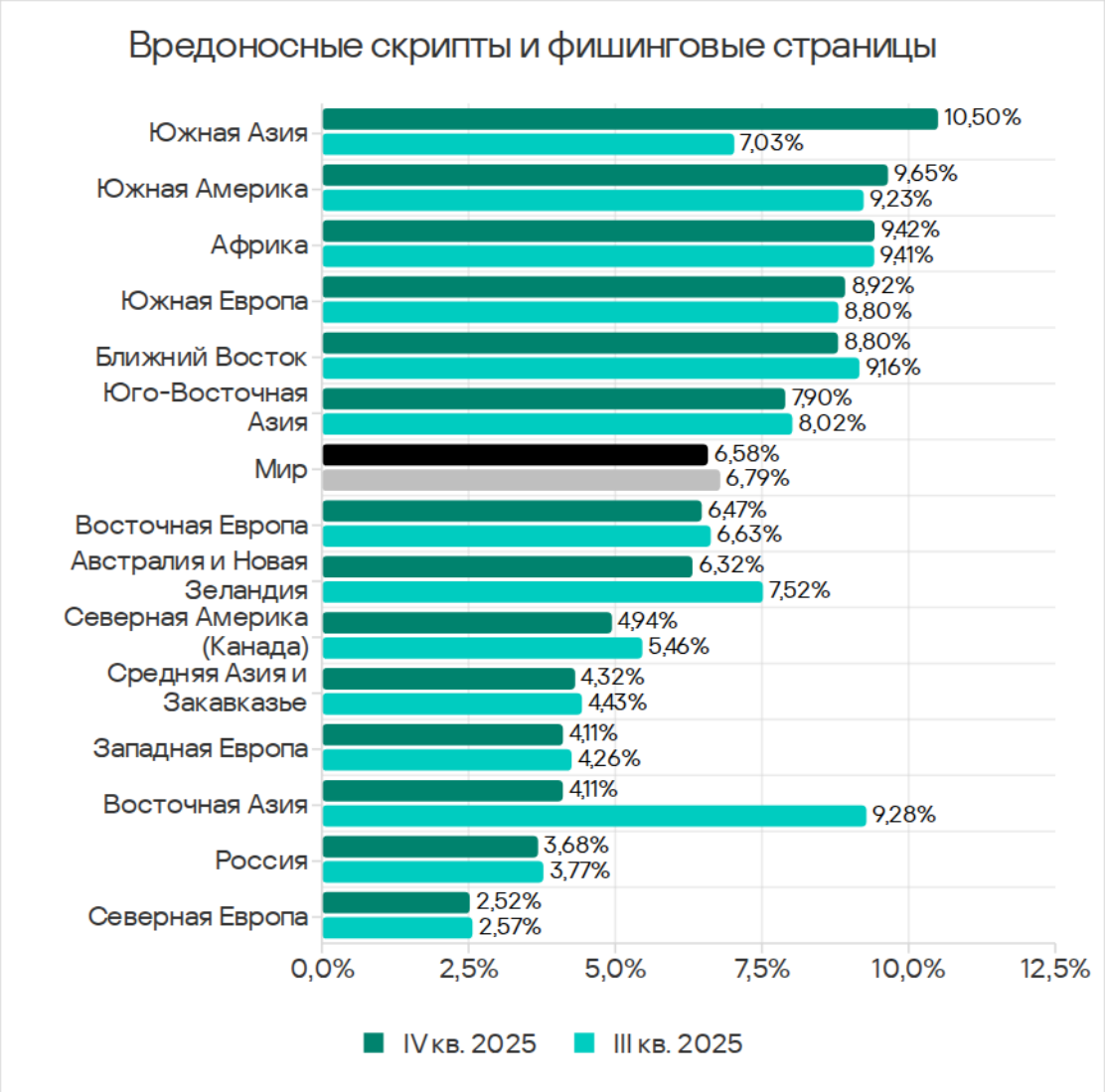
В четвертом квартале в регионе показатель категории вредоносные скрипты и фишинговые страницы вырос в 1,49 раза. В результате в рейтингах регионов Южная Азия заняла первое место и по росту показателя, и по доле компьютеров АСУ, на которых блокировалась эта угроза.

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

- вредоносные скрипты и фишинговые страницы — в 1,6 раза;
- вирусы — в 1,1 раза;
- программы-вымогатели — в 1,1 раза.

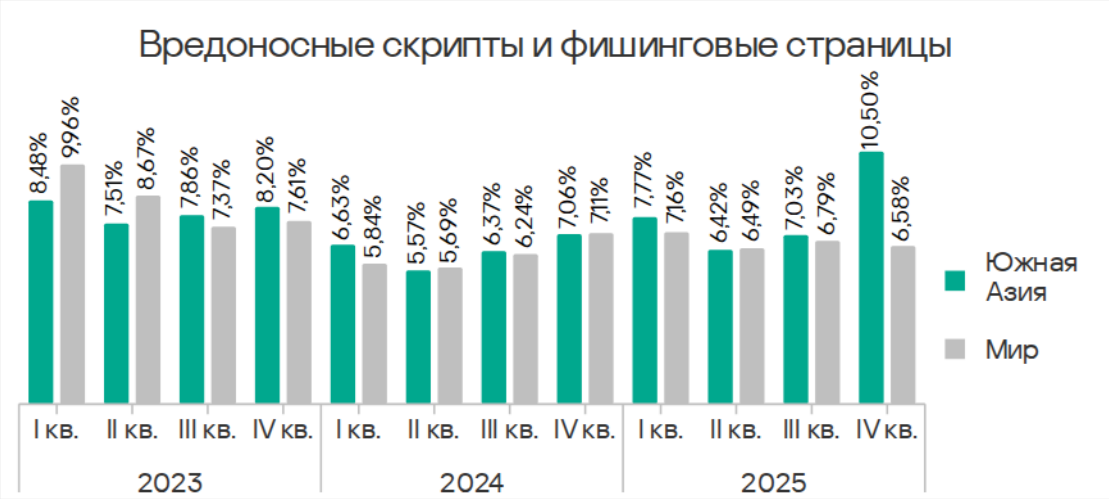
Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, в четвертом квартале 2025 года Южная Азия занимает первое место среди регионов, поднявшись с восьмой позиции в этом рейтинге.



За квартал показатель вырос в 1,49 раза и достиг 10,50%. Это в 4,2 раза больше, чем в Северной Европе, где он – наименьший. Распространялась эта угроза через все источники, но преимущественно – в интернете.

Рост показателя в регионе обеспечила Индия, где значение за квартал увеличилось в 1,87 раза. Напомним, что в этой стране в 1,34 раза вырос и показатель угроз из интернета.



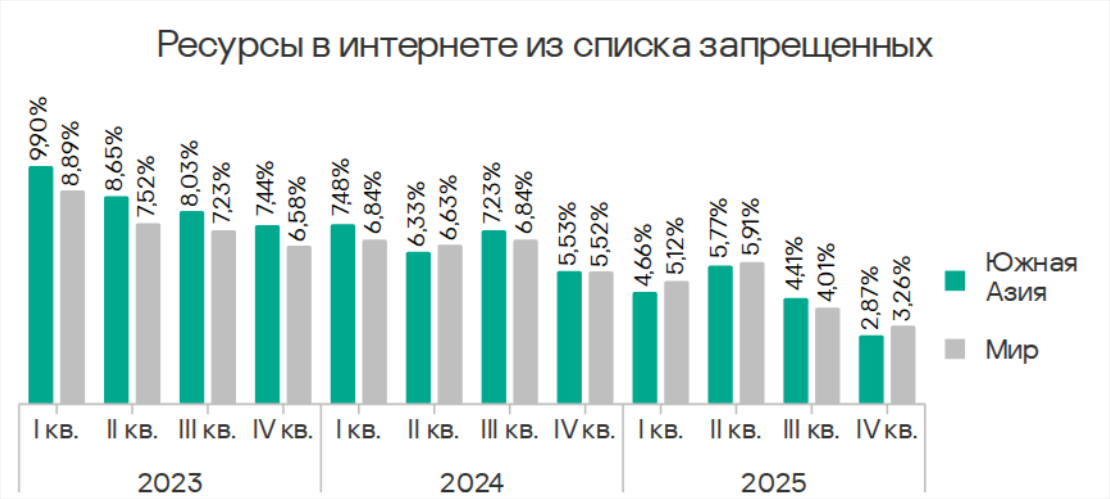
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Шри-Ланка с 12,26%. Наименьший показатель – на Мальдивах (5,07%). Как было сказано выше, показатель в Индии вырос в 1,87 раза, а на Мальдивах – в 1,62 раза.

В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, в Индии была самой высокой за три года.

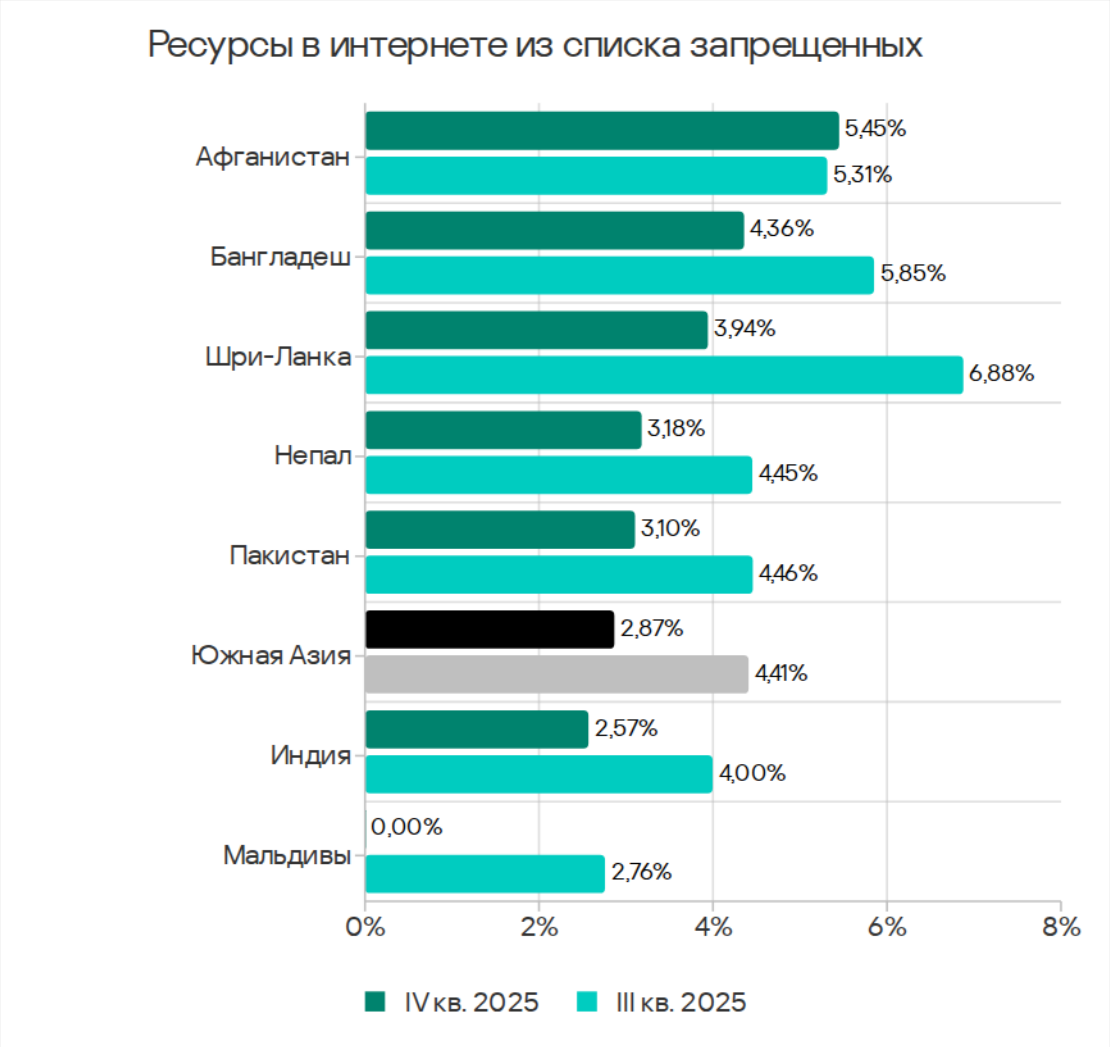
Ресурсы в интернете из списка запрещенных

Южная Азия занимает седьмое место среди регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, с 2,87%. Этот показатель в 1,6 раза больше, чем в Северной Европе, 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 Афганистан с 5,45%. Кроме Мальдив, где показатель в четвертом квартале 2025 года показывает околонулевое значение, следующий наименьший показатель – в Индии (2,57%).

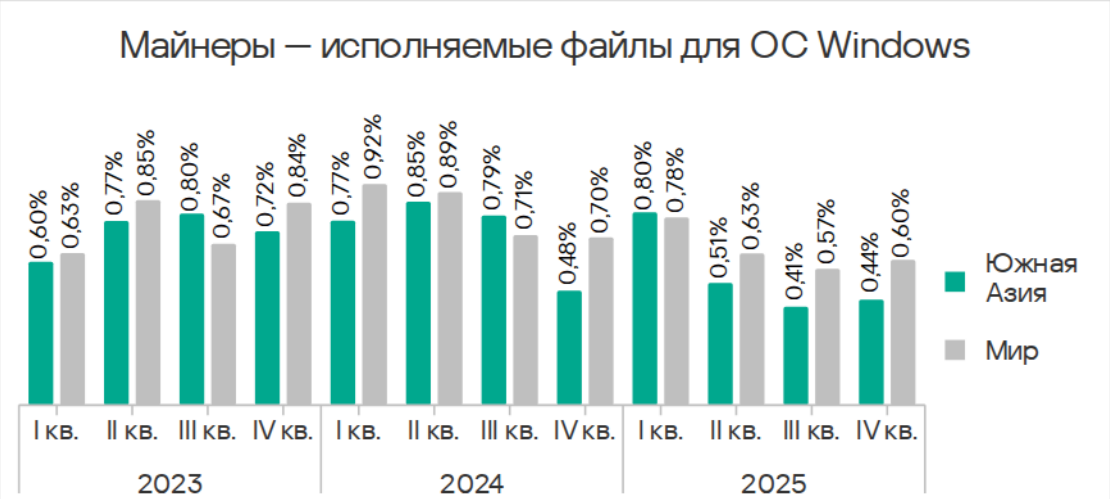


Единственный источник распространения этой категории угроз — интернет. По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, лидирует Шри-Ланка.

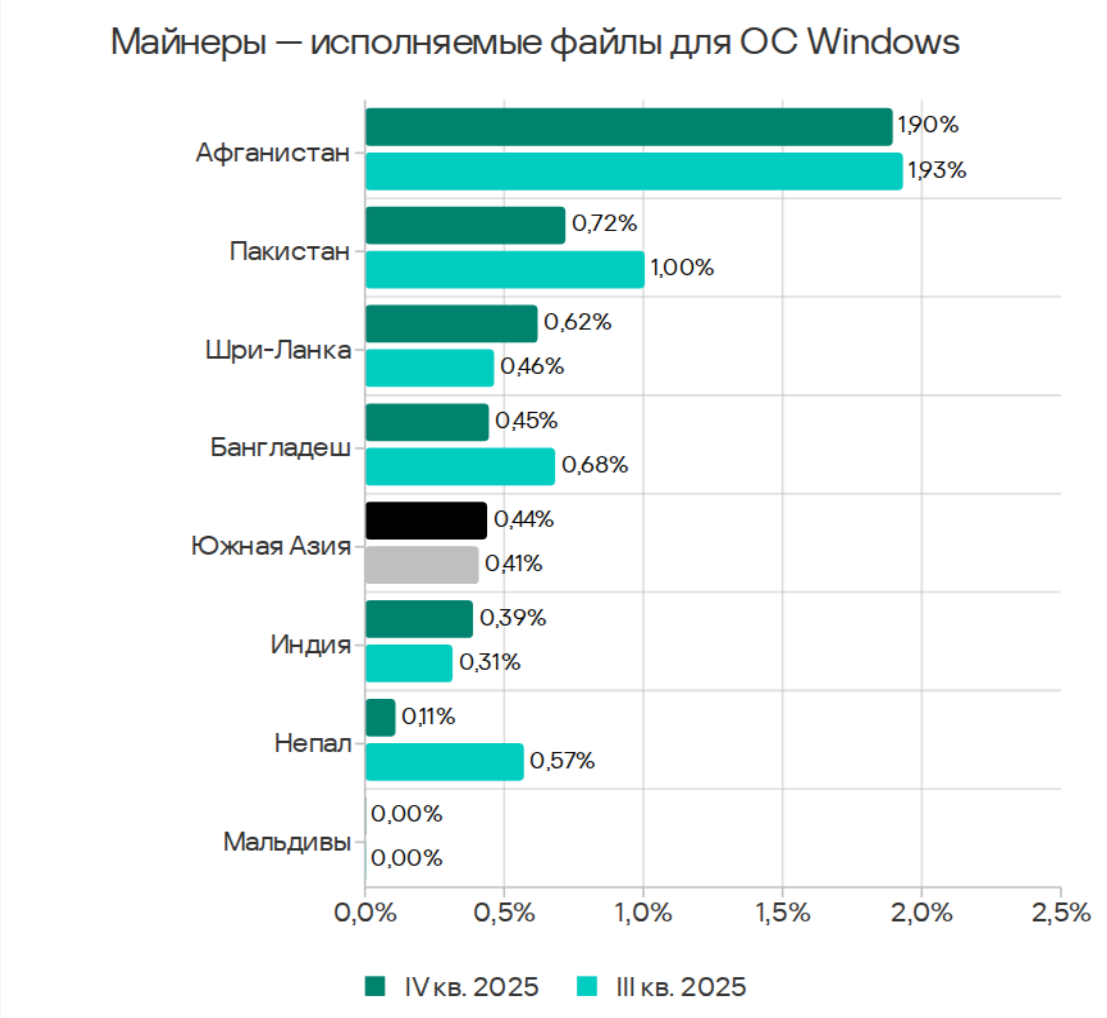
Майнеры – исполняемые файлы для ОС Windows

Южная Азия занимает пятое место среди регионов по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows, с 0,44%. Это в 3,1 раза больше, чем в Северной Америке (Канада), где показатель – наименьший.

Майнеры в формате исполняемых файлов — одна из четырех категорий угроз в регионе, у которых за квартал показатель увеличился.



Среди стран региона по этому показателю с большим отрывом лидирует Афганистан с 1,90%. За квартал значения выросли в Шри-Ланке и Индии.

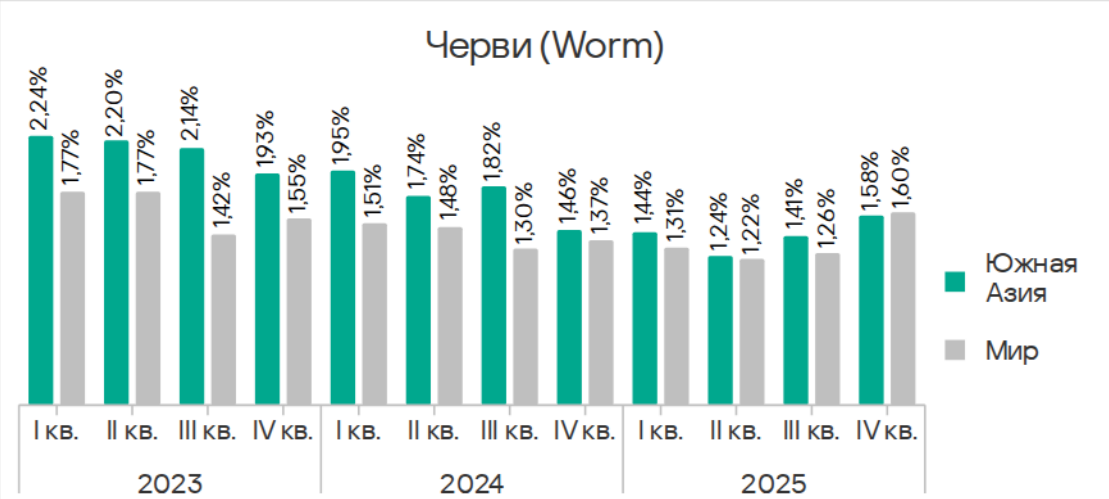


Распространяется эта угроза через интернет и на съемных носителях, но в разы чаще – через интернет.

Черви

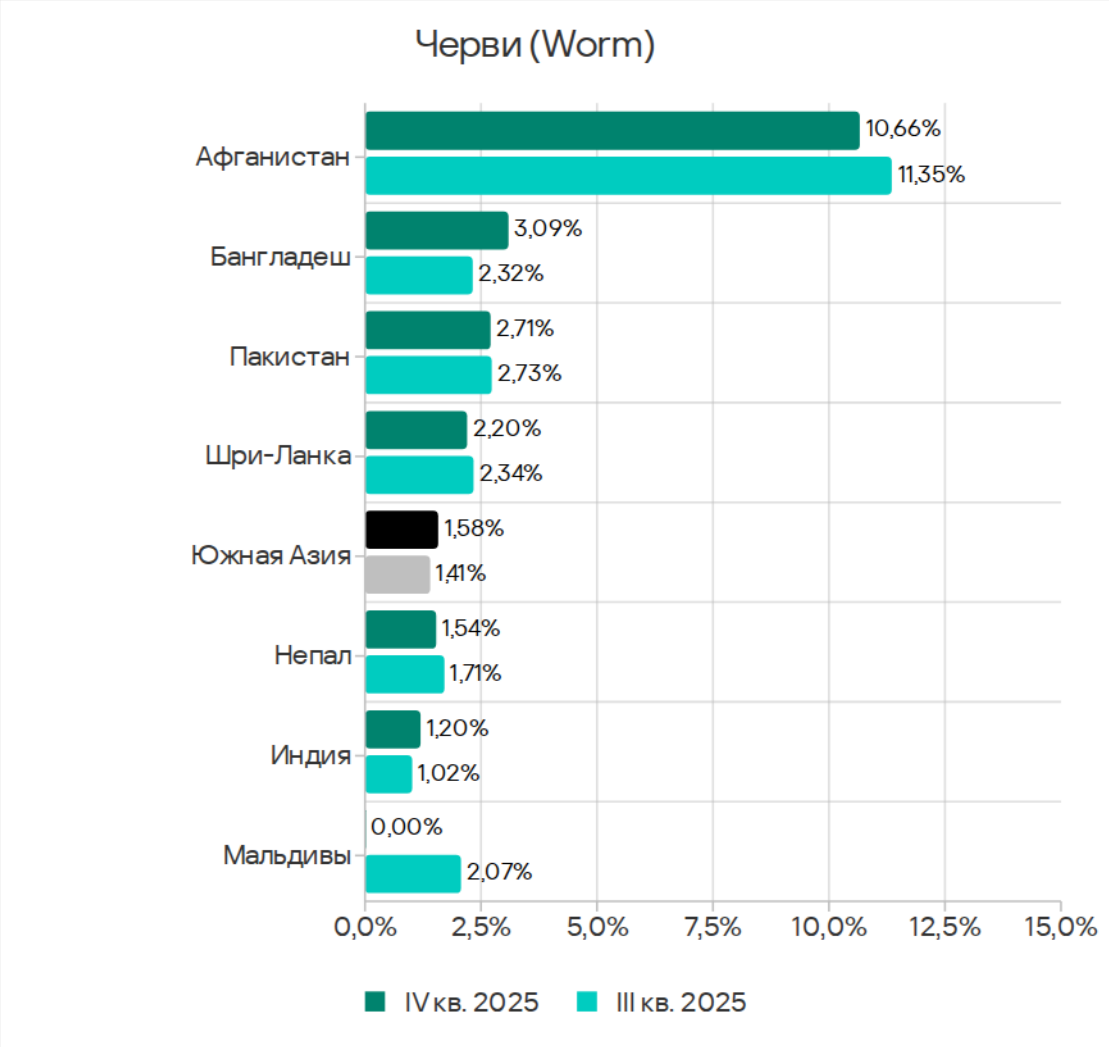
Южная Азия занимает восьмое место среди регионов по доле компьютеров АСУ, на которых были заблокированы черви.

В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие очередной волны фишинговых кампаний Curriculum-vitae-catalina, о которых мы рассказывали выше. В Южной Азии показатель вырос до 1,58% — это в 4,9 раза больше, чем в Северной Европе, где значение – наименьшее среди регионов.



В Южной Азии в рейтинге категорий угроз черви занимают четвертое место. На такой высокой позиции в региональном рейтинге черви, кроме Южной Азии, находятся еще в трех регионах — в России, Средней Азии и Закавказье, а также в Африке.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы черви, лидирует Афганистан с огромным для этой категории угроз показателем 10,66%. Значения за квартал выросли только в Бангладеш и Индии.



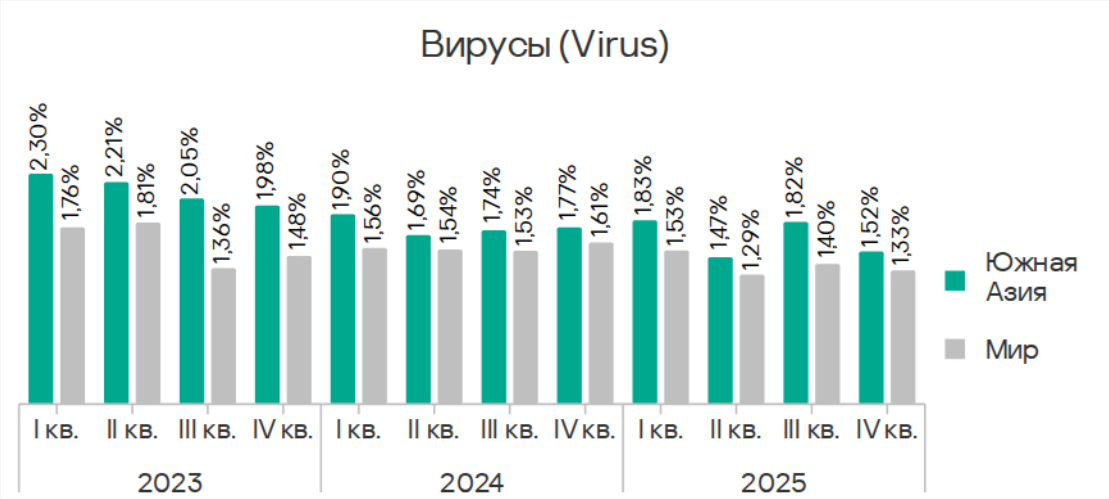
Черви в регионе распространяются через все источники угроз, чаще всего их блокируют при подключении съемных носителей. По показателю этого источника угроз в регионе также лидирует Афганистан, и тоже с большим отрывом от остальных стран.

Вирусы и вредоносные программы для AutoCAD

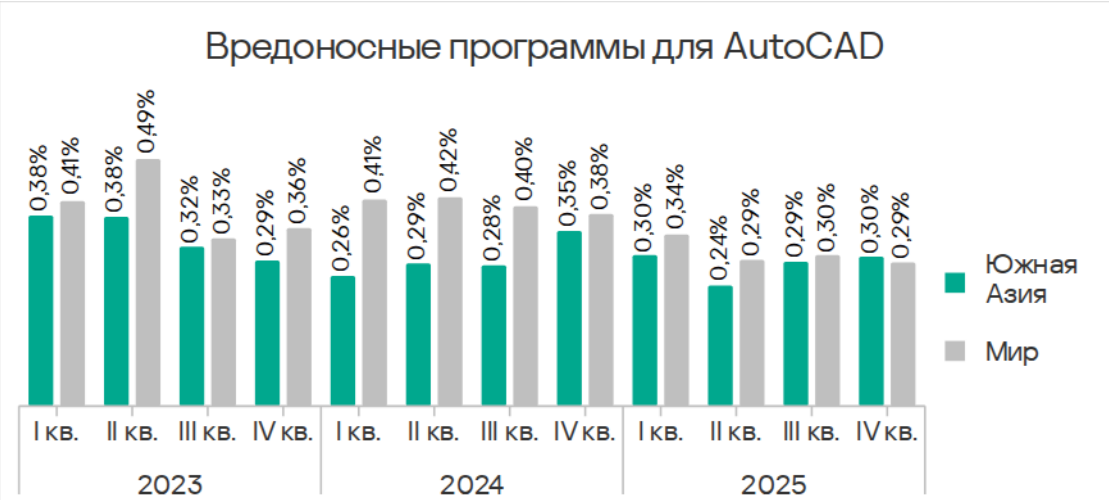
Южная Азия занимает пятое место среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, и четвертое место – по показателям вредоносных программ для AutoCAD.

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 показатель для этой категории вредоносного ПО.

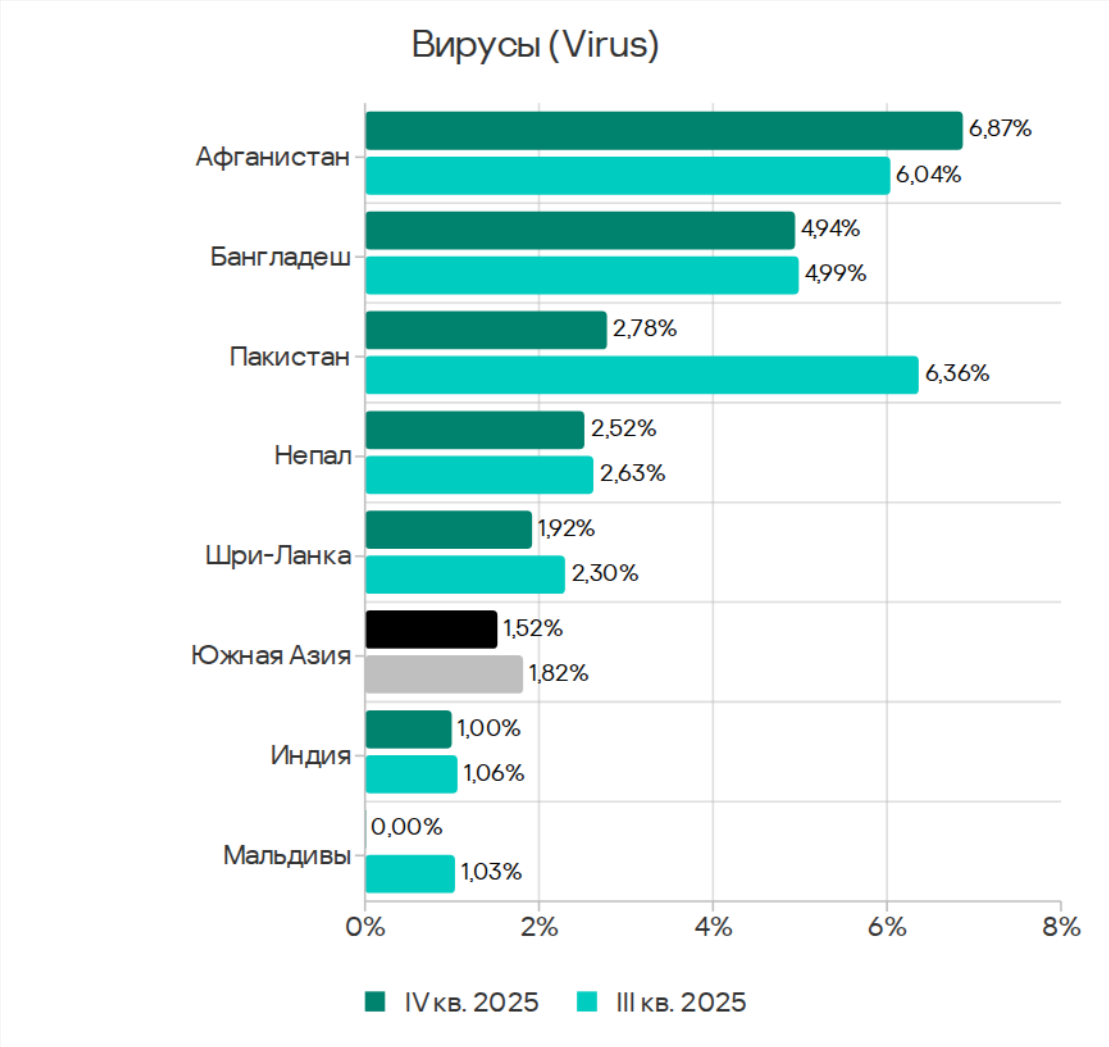
Показатель вирусов в Южной Азии колеблется с тенденцией к снижению. В четвертом квартале 2025 года он уменьшился до 1,52% — это в 10,1 раза больше, чем в Западной Европе, где значение наименьшее среди регионов.



Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, в Южной Азии еще немного выросла — до 0,30%. Это в 30,0 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.

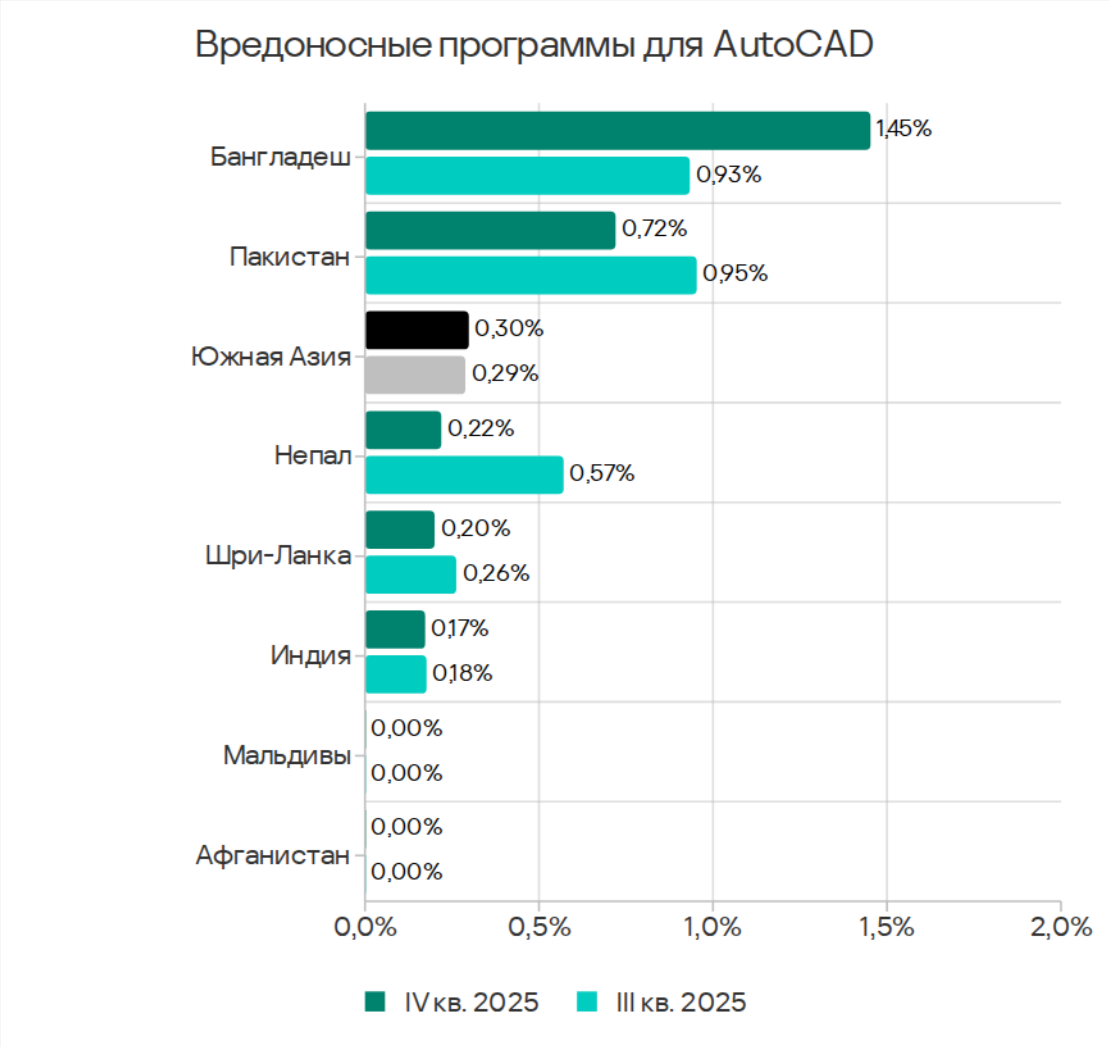


Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вирусы, лидирует Афганистан с 6,87%. Показатель Пакистана, который в прошлом квартале вырос почти вдвое, вернулся к более привычному значению.



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

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, на первом месте Бангладеш с 1,45%. В прошлом квартале показатель этой страны увеличился почти вдвое, в четвертом квартале рост продолжился.

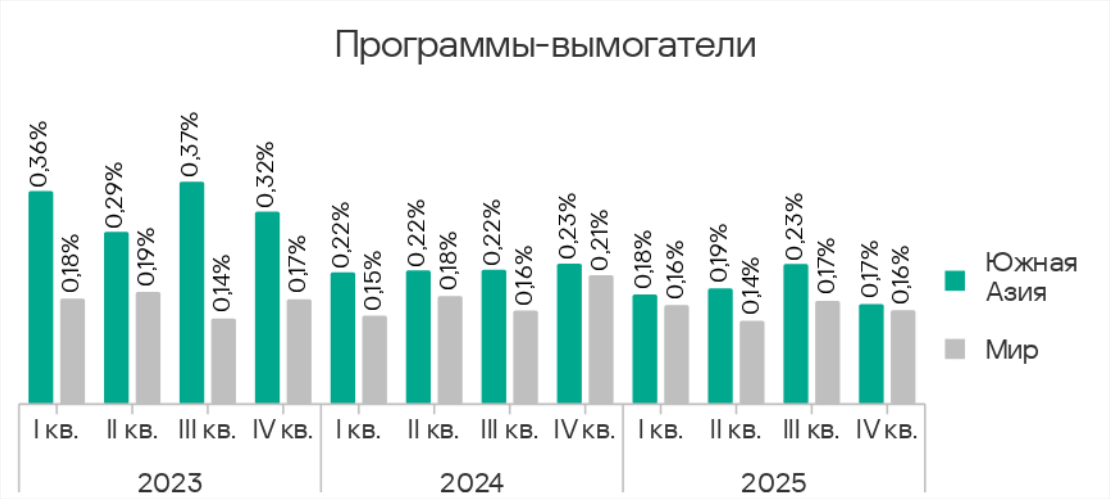


Вредоносные программы для AutoCAD в регионе чаще всего распространялись через сетевые папки.

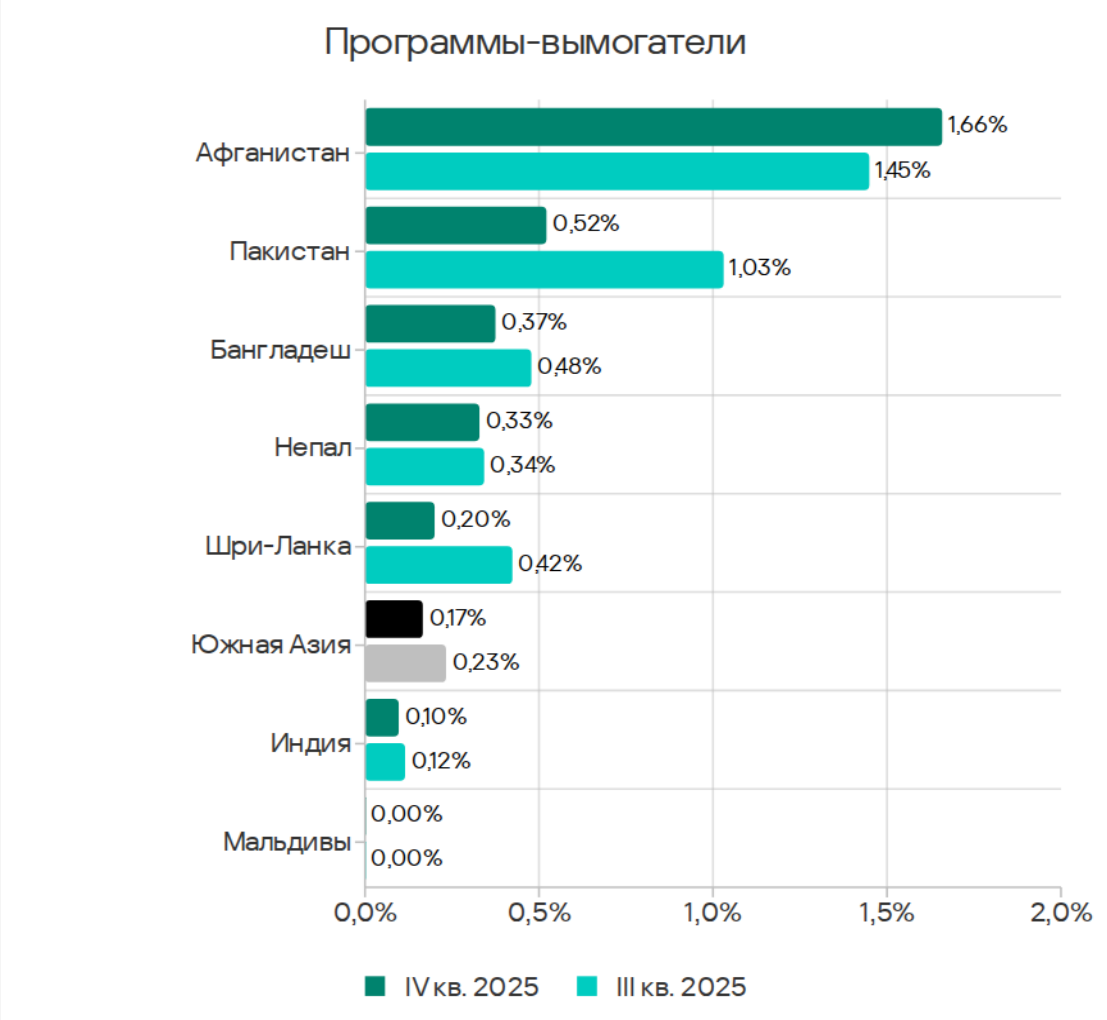
Программы-вымогатели

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Южная Азия находится на пятом месте среди регионов – с 0,17%. Это в 3,4 раза больше, чем в Северной Европе, где показатель наименьший.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, в регионе колеблется.



Среди стран региона по доле компьютеров АСУ, на которых блокируются программы-вымогатели, лидирует Афганистан с 1,66%. Как и в случае вирусов, в прошлом квартале показатель в Афганистане увеличился почти вдвое. В четвертом квартале он продолжил расти.



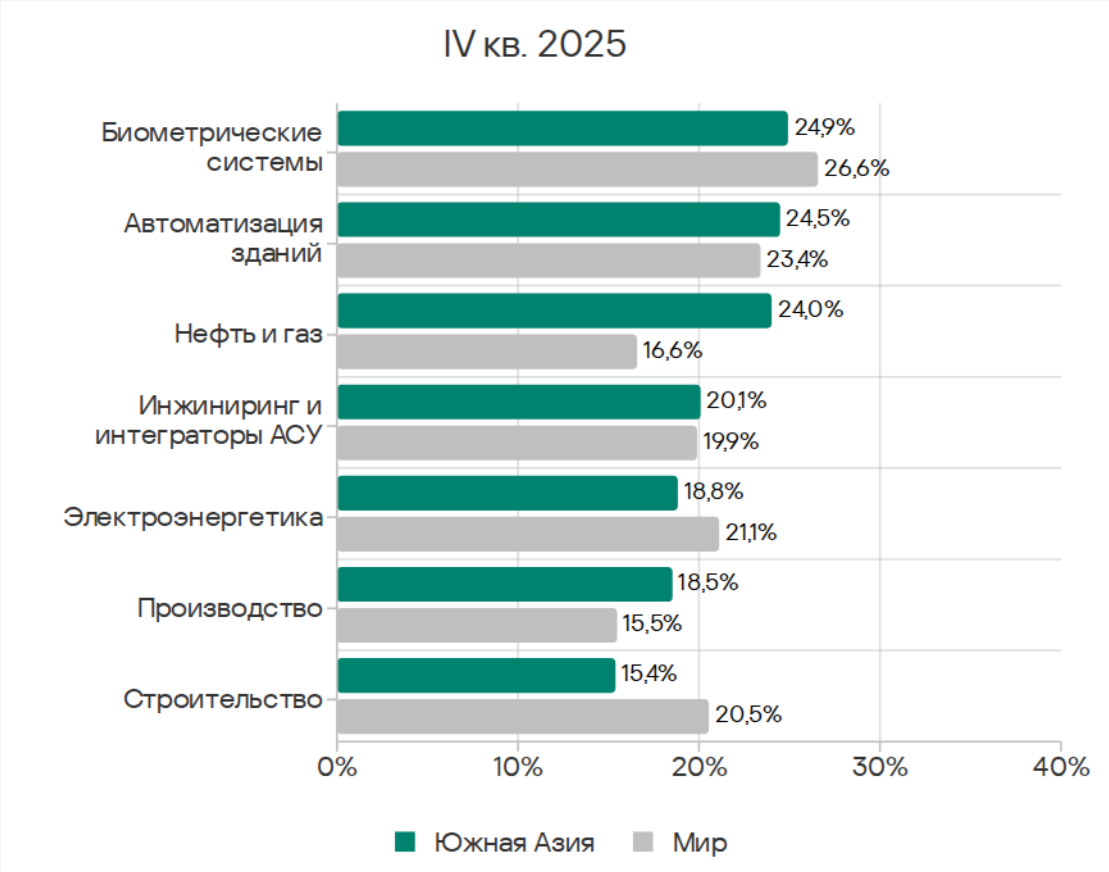
В Южной Азии программы-вымогатели чаще всего распространяются на съемных носителях. Среди стран региона по показателю этого источника угроз также лидирует Афганистан.

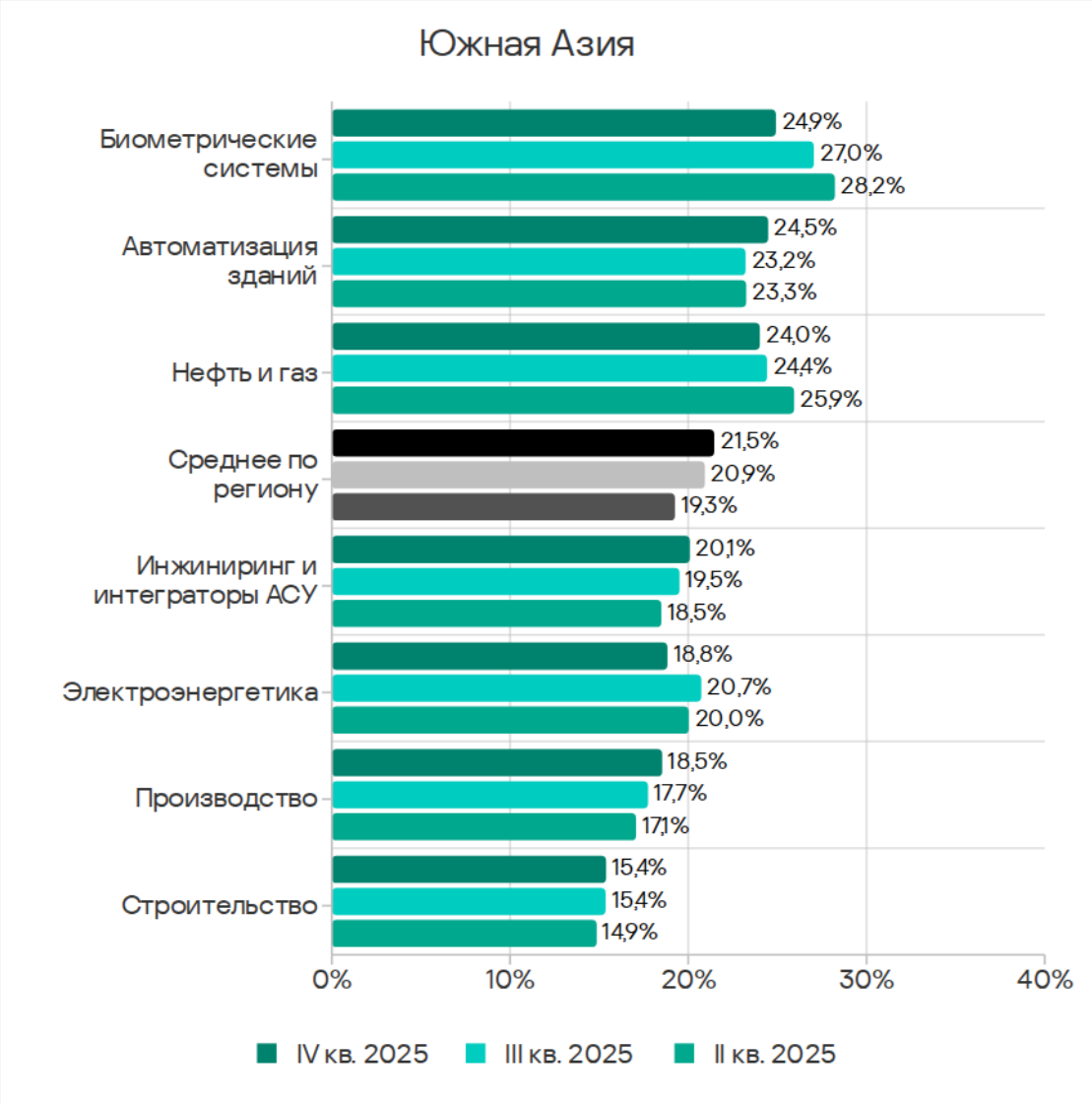
Отрасли

Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является инфраструктура биометрических систем.

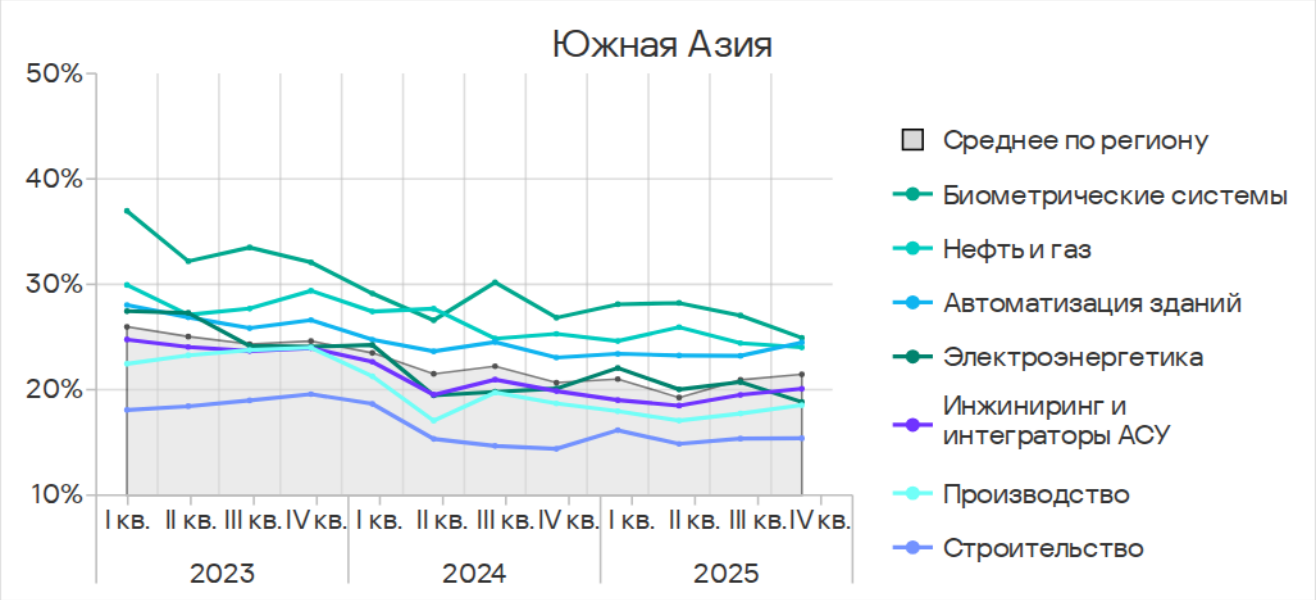
По сравнению с соответствующими среднемировыми значениями показатели выше в отраслях автоматизация зданий, инжиниринг и интеграторы АСУ, производство. В этих же отраслях выросли показатели за квартал.

Самая большая разница со среднемировым показателем – у отрасли производство — он в 1,2 раза превышает среднемировой.





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, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	11,12%	12,08%	12,08%	8,61%	10,63%	8,80%	10,12%	11,33%
Почтовые клиенты	4,43%	2,95%	0,76%	2,34%	4,72%	1,01%	1,37%	1,92%
Съемные носители	1,42%	0,67%	0,29%	0,44%	—	0,20%	0,39%	0,50%
Сетевые папки	—	0,05%	0,02%	—	0,79%	0,05%	—	0,03%
Показатель отрасли в регионе	24,92%	24,48%	20,09%	18,83%	24,02%	15,39%	18,54%	

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

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	3,18%	3,00%	2,98%	2,53%	6,69%	2,11%	2,87%	2,87%
Вредоносные скрипты и фишинговые страницы	11,20%	11,80%	10,38%	8,66%	9,84%	7,72%	9,14%	10,50%
Вредоносные документы (MSOffice+PDF)	3,43%	2,22%	0,80%	1,56%	1,57%	0,52%	0,98%	1,52%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,43%	3,59%	1,63%	2,77%	3,94%	1,25%	2,15%	2,60%
Программы-вымогатели	0,67%	0,20%	0,11%	—	0,39%	0,05%	0,07%	0,17%
Майнеры — исполняемые файлы для ОС Windows	0,67%	0,49%	0,38%	0,19%	0,79%	0,17%	0,59%	0,44%
Веб-майнеры, выполняемые в браузерах	0,42%	0,16%	0,18%	0,05%	0,39%	0,07%	0,13%	0,17%
Вредоносные программы для AutoCAD	0,17%	0,18%	0,38%	0,19%	0,79%	1,06%	0,33%	0,30%
Черви (Worm)	3,18%	2,27%	0,96%	1,36%	0,39%	0,88%	1,37%	1,58%
Вирусы (Virus)	3,34%	1,84%	1,02%	2,53%	0,39%	1,43%	1,89%	1,52%
Показатель отрасли в регионе	24,92%	24,48%	20,09%	18,83%	24,02%	15,39%	18,54%	

Особенности региона

У отраслей в регионе – высокий показатель угроз из интернета. По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, регион находится на первом месте по показателям во всех отраслях, кроме строительства и электроэнергетической отрасли.

В регионе показатели угроз из интернета увеличились во всех отраслях, кроме инфраструктуры биометрических систем. По росту этого показателя лидируют производство и инжиниринг и интеграторы АСУ.

Показатель категории вредоносные скрипты и фишинговые страницы вырос во всех отраслях, кроме инфраструктуры биометрических систем. По росту доли компьютеров АСУ, на которых была заблокирована эта угроза, в регионе также лидируют отрасли инжиниринг и интеграторы АСУ, производство.

По доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, Южная Азия занимает первое место среди регионов в отраслях электроэнергетика, инжиниринг и интеграторы АСУ, производство и второе место – в автоматизации зданий.

В рейтингах регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отраслях производство и инжиниринг и интеграторы АСУ, Южная Азия поднялась с шестого на третье место.

Биометрические системы

Южная Азия находится на пятом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

Среди регионов по показателям в отрасли Южная Азия занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- второе место по показателю угроз на съемных носителях;
- второе место по доле компьютеров АСУ, на которых были заблокированы вирусы;
- третье место по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы, майнеры в формате исполняемых файлов и программы-вымогатели.

Среди отраслей в регионе биометрические системы занимают:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и на съемных носителях;
- третье место по показателю угроз из интернета;
- первое место по показателям всех категорий угроз, кроме категорий вредоносные скрипты и фишинговые страницы и вредоносные программы для AutoCAD;
- второе место по показателю категории вредоносные скрипты и фишинговые страницы.

Автоматизация зданий

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

Среди регионов по показателям в отрасли Южная Азия занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- третье место по показателю съемных носителей;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе автоматизация зданий занимает:

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

Электроэнергетика

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

Среди регионов по показателям в отрасли Южная Азия занимает первое место по показателю категории вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе электроэнергетика занимает:

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

Инжиниринг и интеграторы АСУ

Южная Азия находится на четвертом 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:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- первое место по показателю категории вредоносные скрипты и фишинговые страницы;
- третье место по показателю вредоносных программ для AutoCAD.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- первое место по показателю угроз из интернета;
- третье место по показателю угроз в сетевых папках;
- второе место по показателю угроз следующих категорий: веб-майнеры и вредоносные программы для AutoCAD;
- третье место по показателю угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, программы-вымогатели.

Производство

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

Среди регионов по показателям в отрасли Южная Азия занимает:

- первое место по показателю угроз из интернета;
- первое место по показателю категории вредоносные скрипты и фишинговые страницы;
- третье место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных и вредоносные программы для AutoCAD.

Среди отраслей в регионе производство занимает:

- второе место по показателю майнеров в формате исполняемых файлов;
- третье место по показателю угроз следующих категорий: черви, вирусы, вредоносные программы для AutoCAD.

Строительство

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

Среди отраслей в регионе строительство занимает:

- второе место по показателю угроз в сетевых папках;
- первое место по показателю вредоносных программ 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 четвертом квартале 2025 года эта категория занимала первое место в рейтинге категорий вредоносного ПО доле компьютеров АСУ в регионе, на которых оно было заблокировано. Восточная Азия — единственный регион, где в этом рейтинге на первом месте находятся шпионские программы.

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 показателю вредоносного ПО для AutoCAD во всех индустриях во всех регионах 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 глобальном рейтинге всех индустрий во всех регионах по показателю угроз, заблокированных при обращении к сетевым папкам.

Восточная Азия лидирует среди регионов по показателю вредоносного ПО для AutoCAD во всех отраслях, кроме инфраструктуры биометрических систем, где регион занимает второе место.

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.

По доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, Восточная Азия занимает не ниже третьего места по показателям во всех отраслях, кроме OT-инфраструктуры биометрические системы.

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 четвертом квартале 2025 года лидирует среди регионов по показателю электроэнергетики с 31,59%. По показателю

отрасли инжиниринг и интеграторы АСУ 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 OT-систем сектора для киберугроз. Ведь при вводе в эксплуатацию новых объектов адекватные меры киберзащиты обычно применяются с существенным запозданием.

Различия в странах региона

Ситуация с кибербезопасностью в разных странах и на территориях региона существенно отличается.

Показатели региона в целом во многом определяет ситуация в континентальном Китае.

Именно континентальный Китай лидирует по угрозам на съемных носителях и в сетевых папках и категориям угроз, которые распространяются через эти источники. Это обуславливает высокие позиции региона по показателям вирусов и вредоносных программ для AutoCAD.

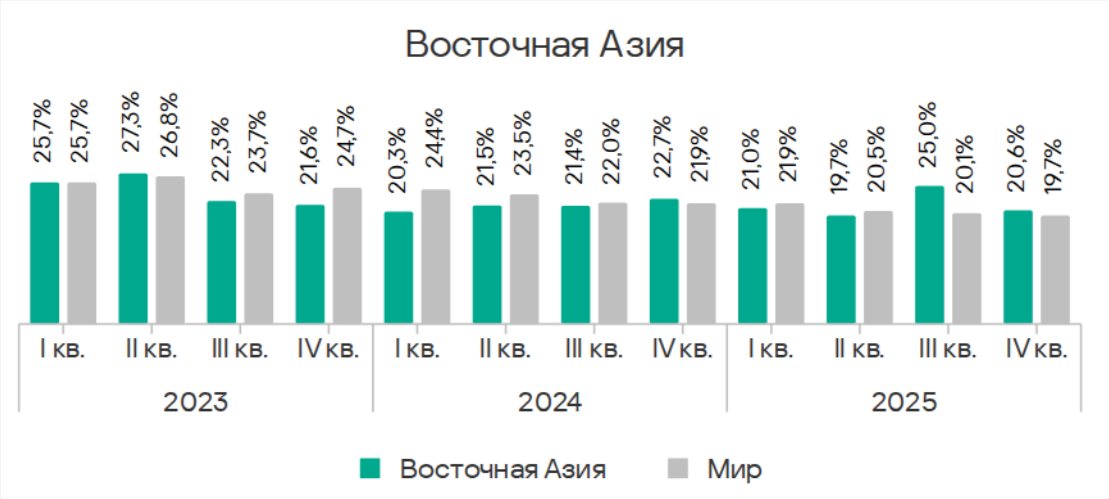
Китай также с большим отрывом лидирует по показателю шпионских программ, в результате эта категория угроз оказалась на первом месте в региональном рейтинге, а регион по показателю шпионских программ — на пятом.

Континентальный Китай лидирует в рейтингах по показателям шести из десяти категорий угроз. Япония занимает последние места в большинстве рейтингов.

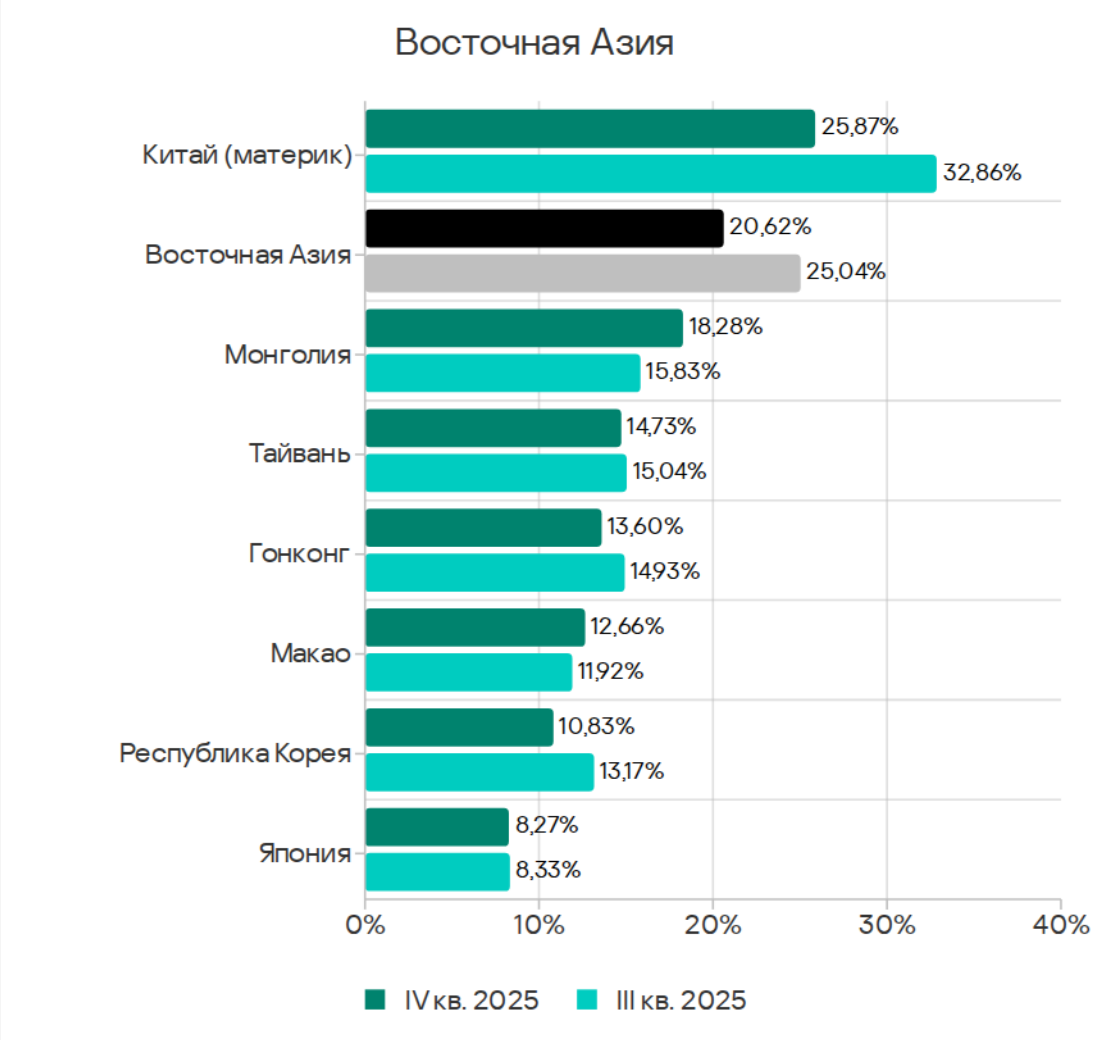
Статистика по всем угрозам

В четвертом квартале 2025 года Восточная Азия в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, опустилась с третьего на пятое место. В предыдущем квартале показатель региона вырос в 1,3 раза из-за всплеска блокировок вредоносных скриптов на компьютерах в сфере инжиниринга и интеграторов АСУ в континентальном Китае. В четвертом квартале показатель вернулся к обычному уровню.

Значение в Восточной Азии превышает минимальное — в Северной Европе — в 2,4 раза.



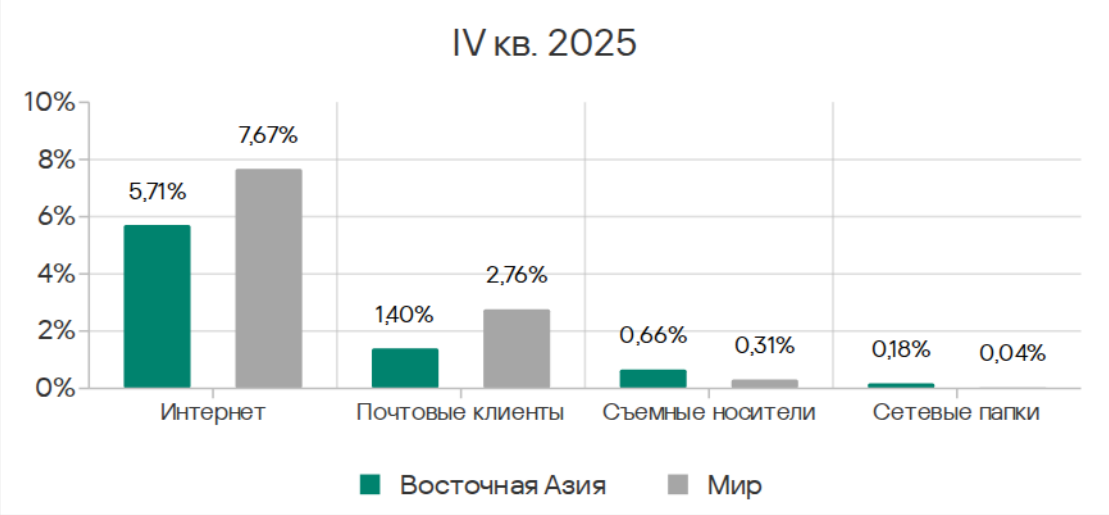
В странах и на территориях региона показатель варьирует от 8,27% в Японии до 25,87% в континентальном Китае.



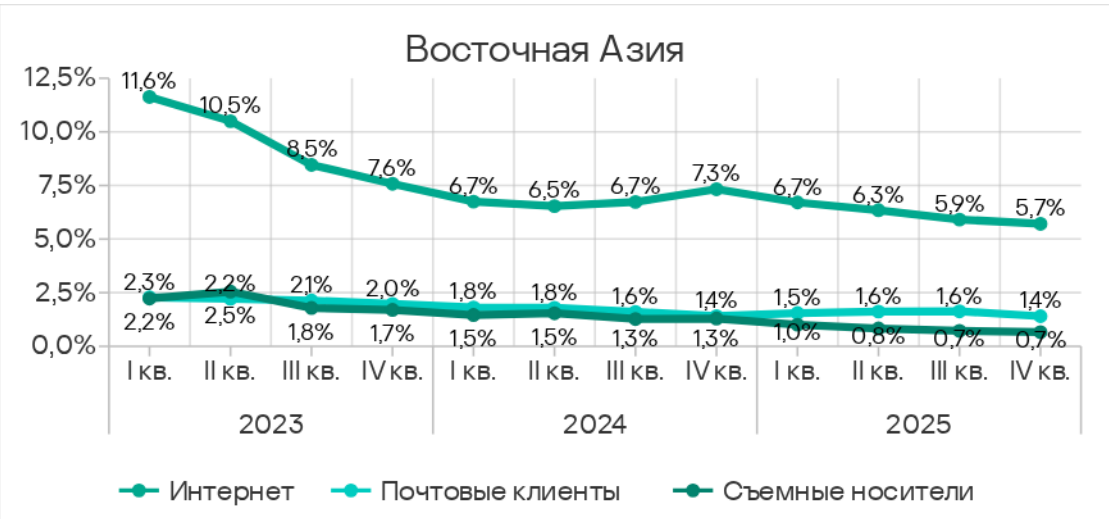
Источники угроз

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

- съемные носители — в 2,1 раза, второе место среди регионов;
- сетевые папки — в 4,5 раза, первое 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.

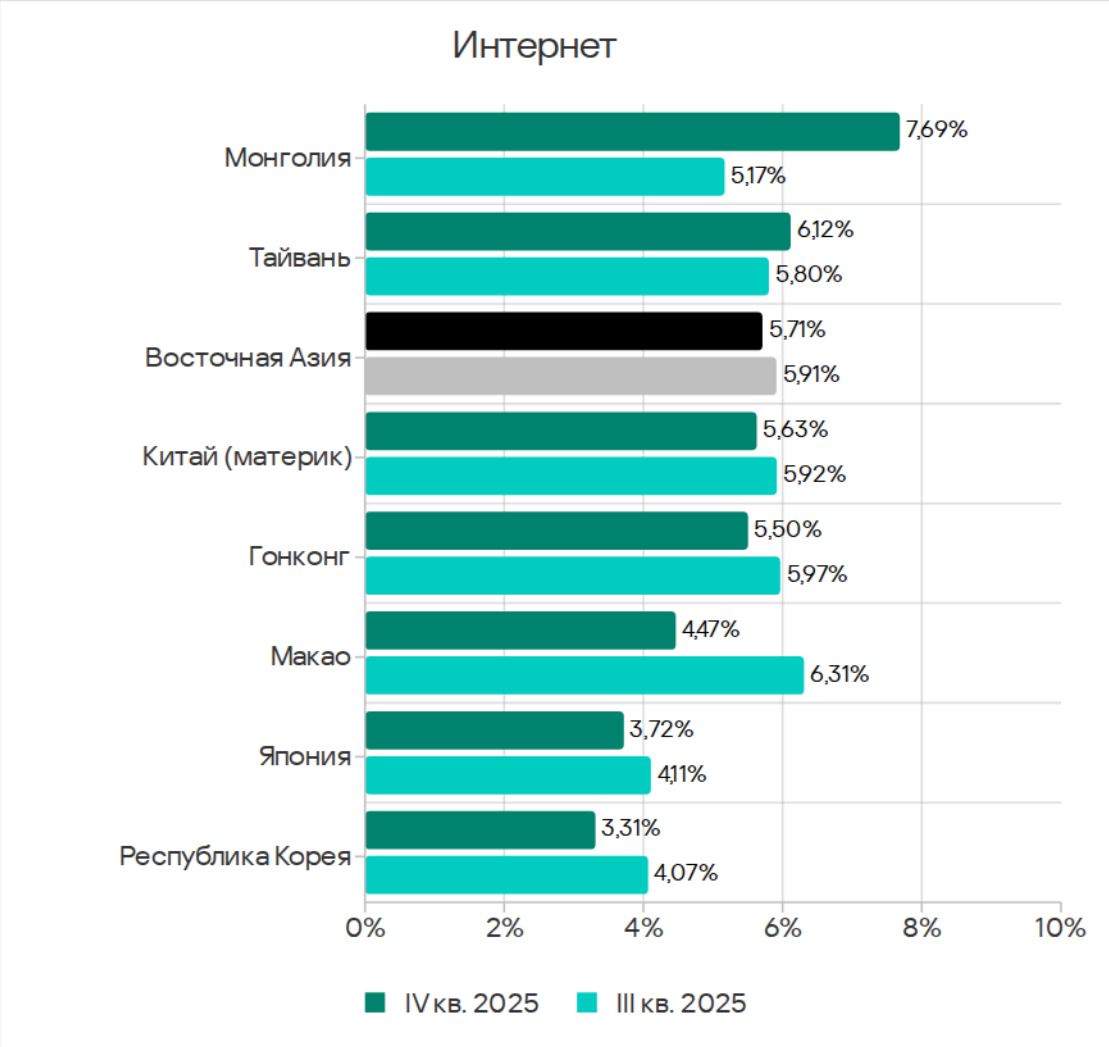


Интернет

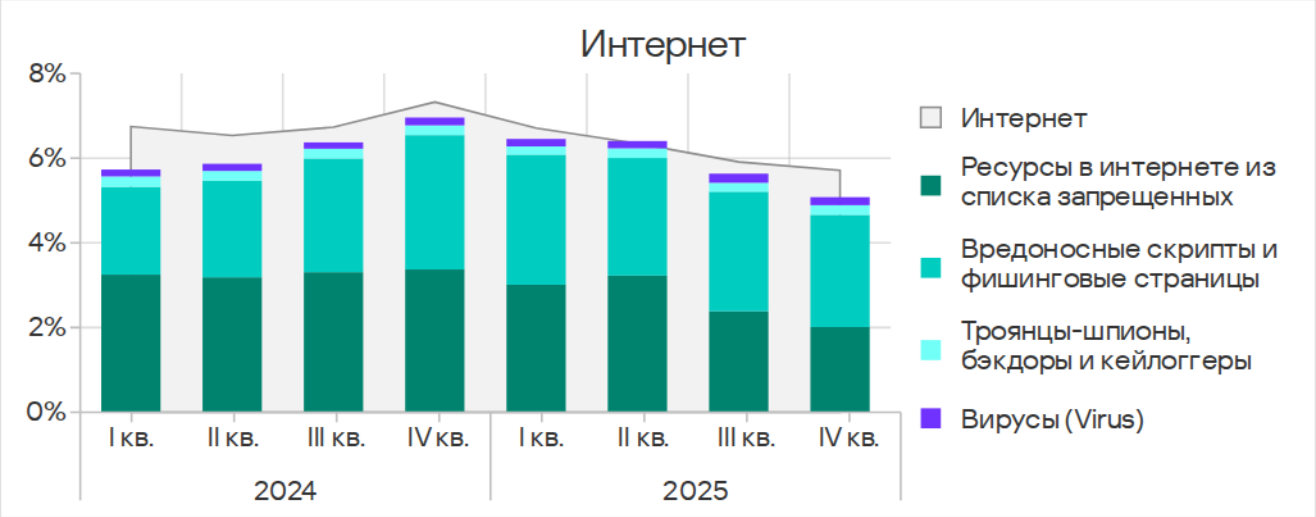
По доле компьютеров АСУ, на которых блокируются угрозы из интернета, Восточная Азия заняла 13-е место в соответствующем рейтинге регионов.

Показатель по угрозам из интернета снижается в регионе четвертый квартал подряд и достиг наименьшего значения за три последних года — 5,71%. Это больше, чем минимальное среди регионов значение — в Северной Европе — в 1,4 раза.

Доля компьютеров АСУ, на которых блокируются угрозы из интернета, в странах и на территориях региона варьирует от 3,31% в Корее до 7,69% в Монголии. В предыдущем квартале показатель в Монголии снизился почти вдвое, в четвертом квартале он вернулся к более характерным для страны значениям.



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

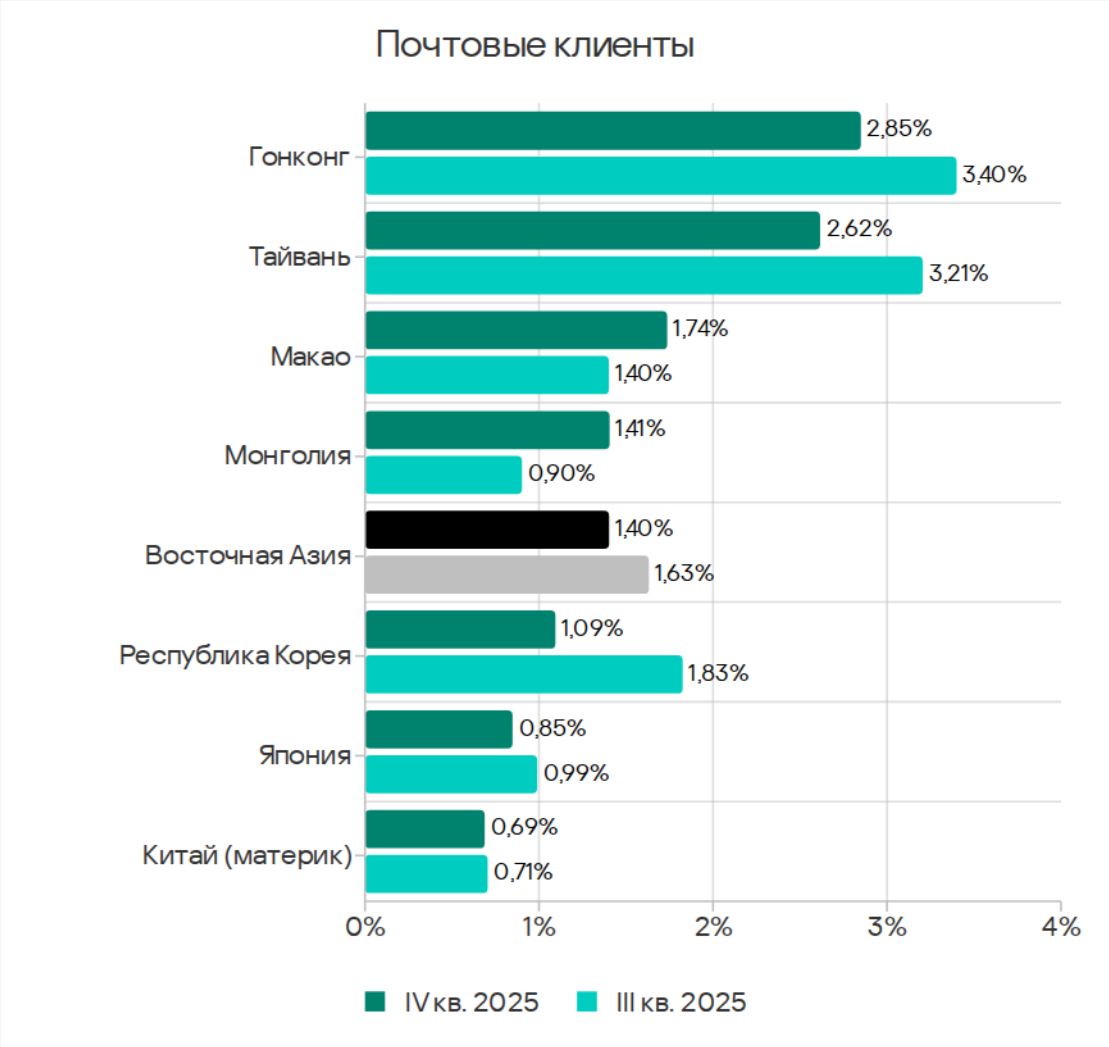


По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в регионе лидирует континентальный Китай, по показателю вредоносных скриптов — Монголия.

Почтовые клиенты

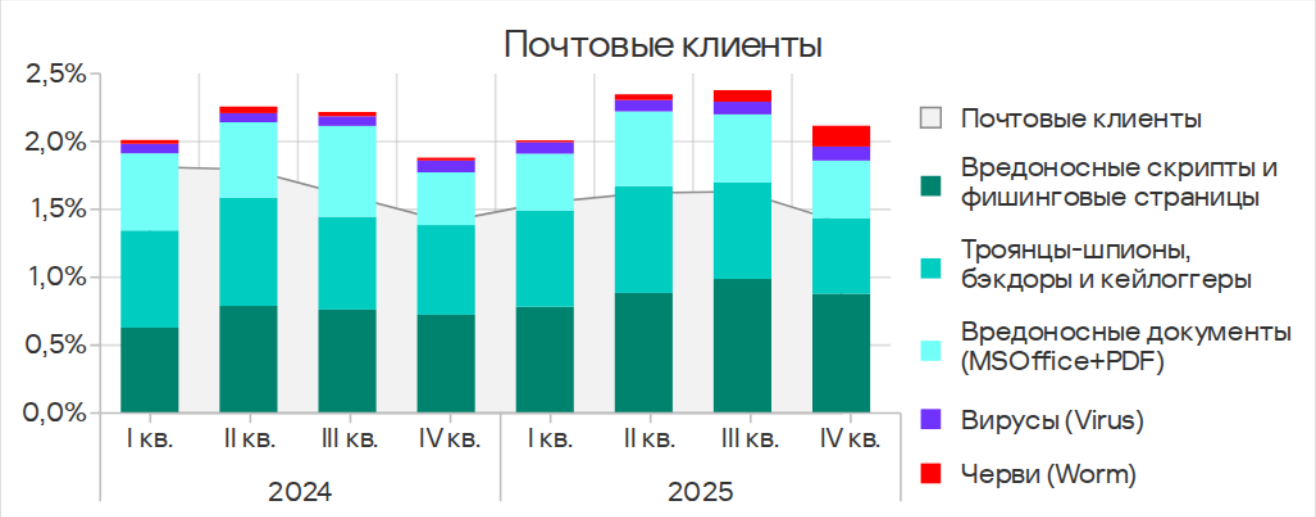
По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, Восточная Азия среди регионов занимает 11-е место с 1,40%. Это в 2,2 раза больше, чем в Северной Европе, где показатель наименьший.

Среди стран и территорий региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидируют Гонконг с 2,85% и Тайвань с 2,62%. Минимальный показатель — в континентальном Китае (0,69%).



Гонконг лидирует и по показателю угрозы, которая распространяется преимущественно через почту, — вредоносные документы.

Основные категории угроз из почтовых клиентов, которые были заблокированы на компьютерах АСУ, — это вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы.



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний Curriculum-vitae-catalina, в ходе которых были атакованы организации во всех регионах мира. В Восточной Азии пик атаки пришелся на ноябрь.

Злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Под видом резюме (Curriculum Vitae) такие письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm). При запуске файла происходило заражение системы.

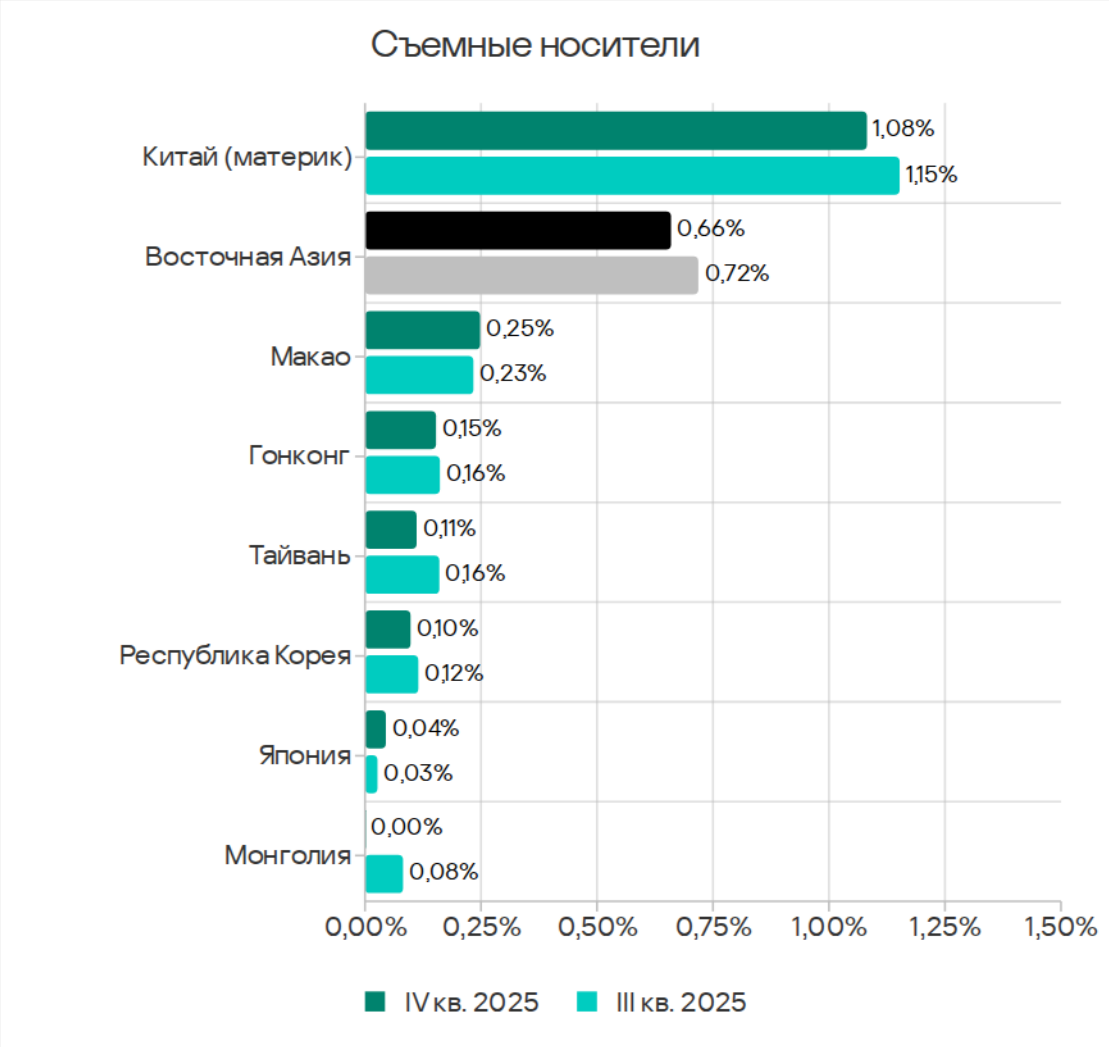
Как правило, такие кампании направлены на доставку вредоносного ПО для кражи данных, а также на доставку программ-шпионов или инструментов для удаленного управления (RAT).

Съемные носители

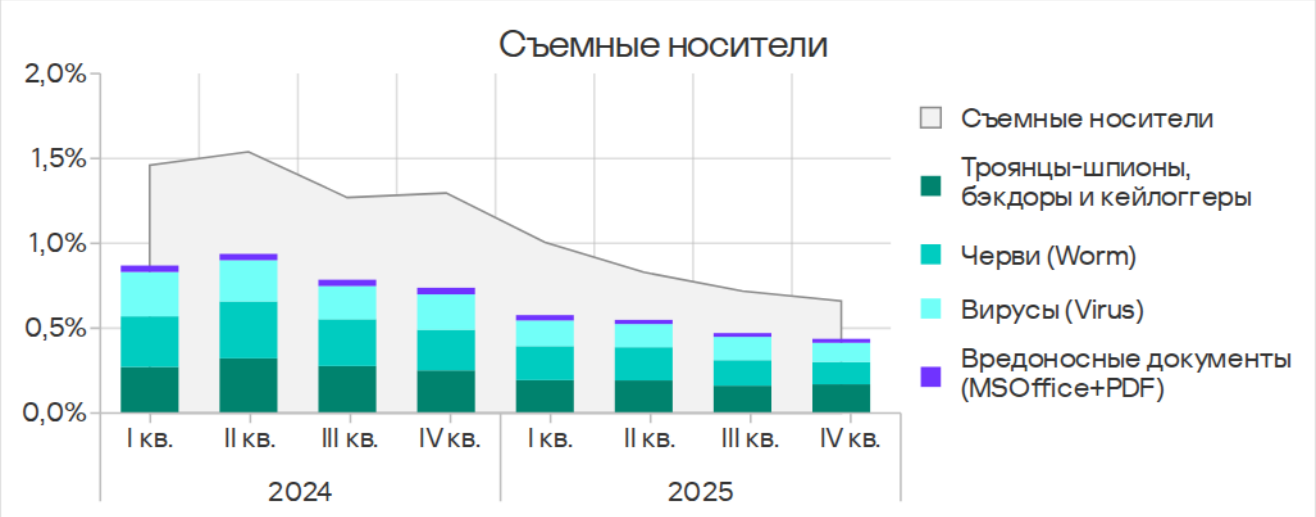
По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Восточная Азия занимает второе место среди регионов, уступая только Африке.

Показатель в регионе – 0,66%. Это в 14,0 раза больше, чем в регионе Австралия и Новая Зеландия, где значение — наименьшее среди регионов.

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 1,08%. Показатели остальных стран и территорий варьируют от 0,04% в Японии до 0,25% в Макао. В Монголии доля компьютеров АСУ, на которых блокировались угрозы при подключении съемных носителей, был незначительным.

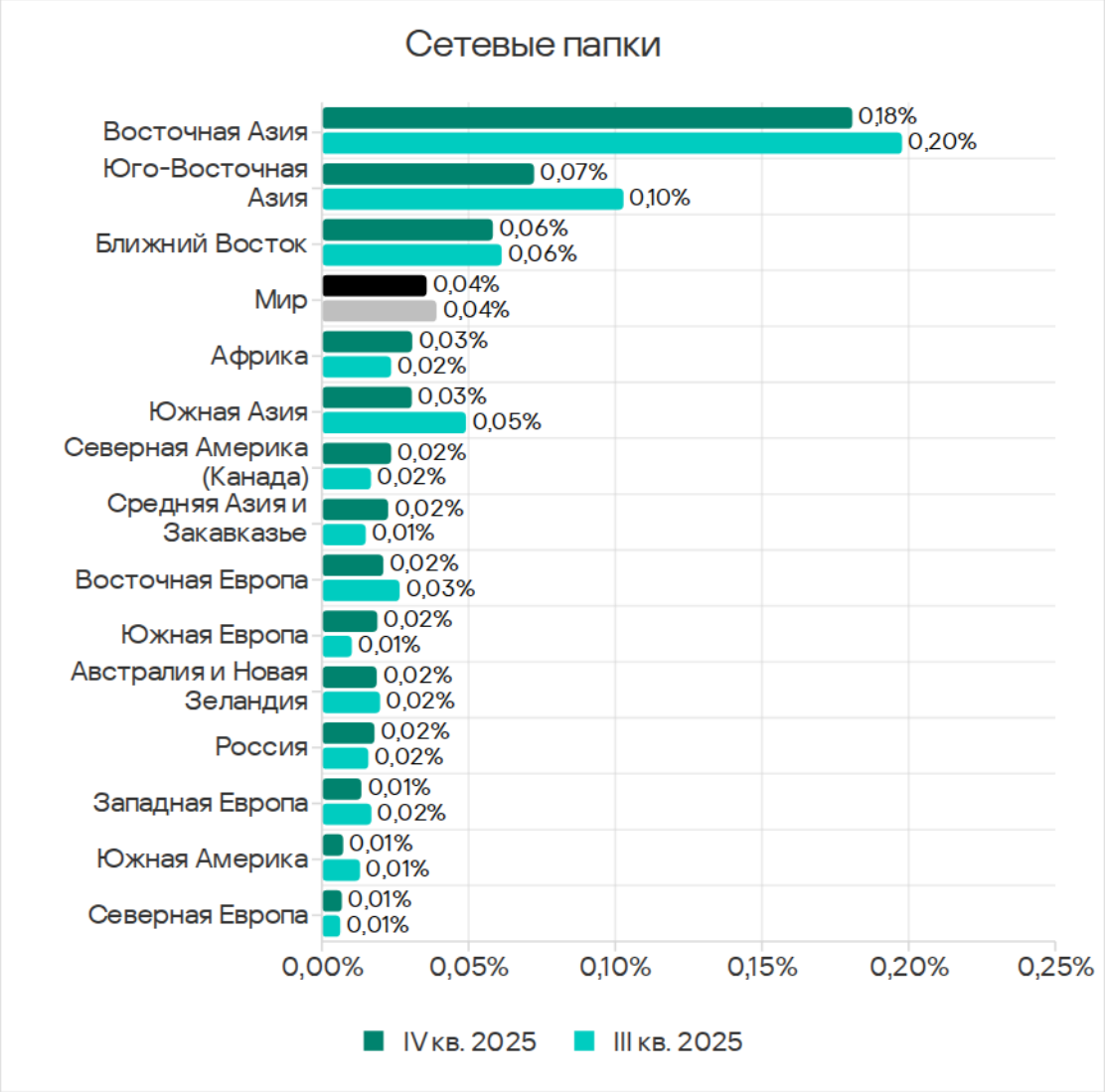


Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ: шпионское ПО, черви и вирусы. Отметим, что континентальный Китай лидирует по показателям всех этих категорий угроз.

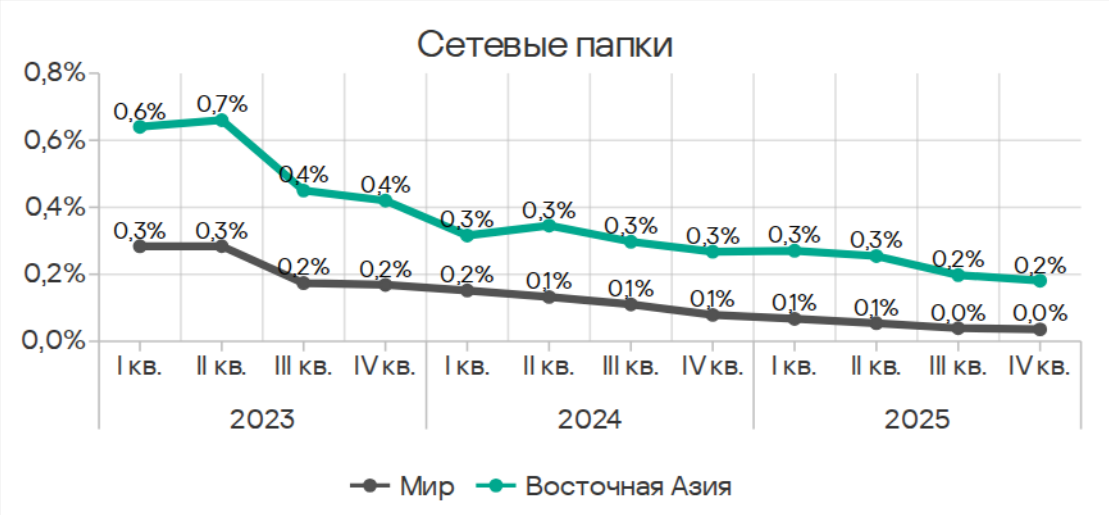


Сетевые папки

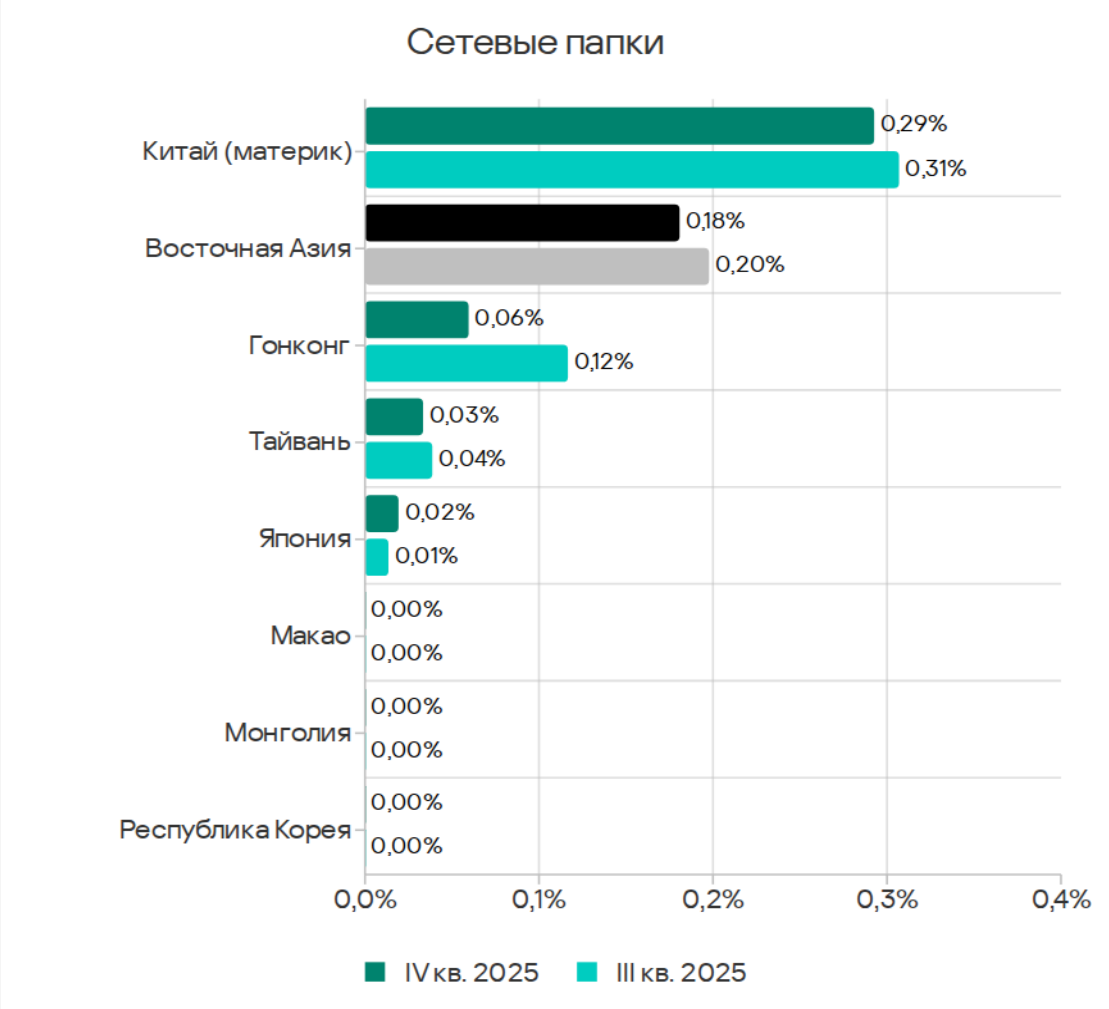
Восточная Азия по-прежнему занимает первое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. В четвертом квартале 2025 года показатель региона составил 0,18%. Это в 25,9 раза больше, чем в Северной Европе, где показатель наименьший среди регионов. Показатель Юго-Восточной Азии, которая находится на втором месте в этом рейтинге, меньше, чем в Восточной Азии в 2,5 раза.



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

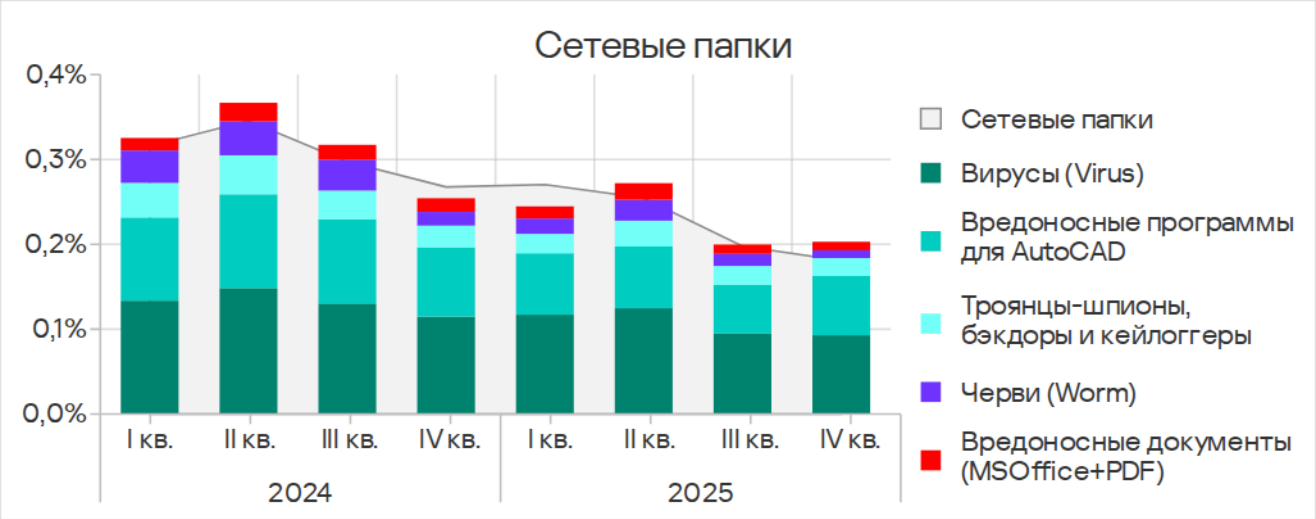


Первое место Восточной Азии по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, обеспечивает континентальный Китай, который с большим отрывом лидирует по этому показателю среди стран и территорий региона — с 0,29%.



Отметим, что угрозы в сетевых папках были обнаружены не во всех странах и территориях 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. А показатель сетевых папок как источника этой угрозы лишь в 1,1 раза меньше показателей почтовых клиентов и съемных носителей.

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, Восточная Азия находится на втором месте среди регионов.

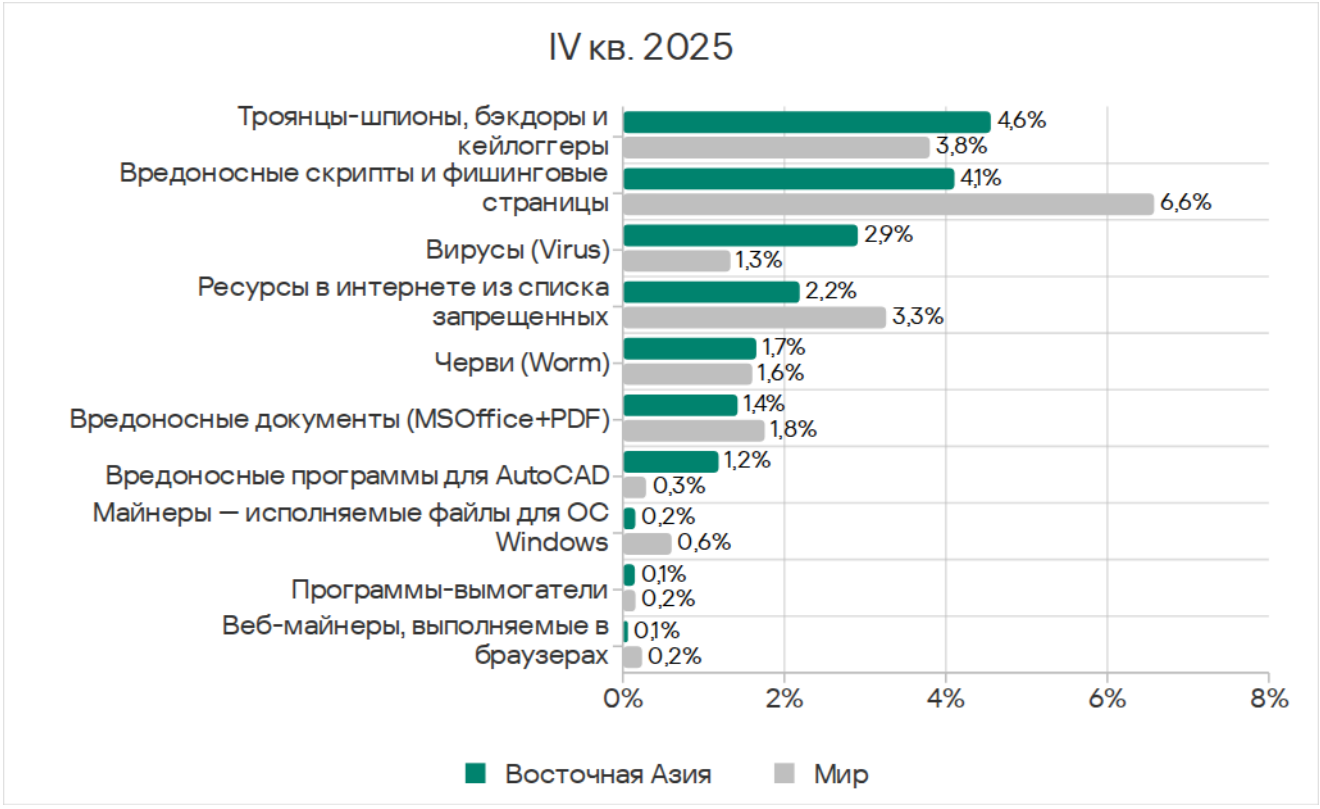
И по вирусам, и по вредоносному ПО для AutoCAD, в регионе лидирует континентальный Китай.

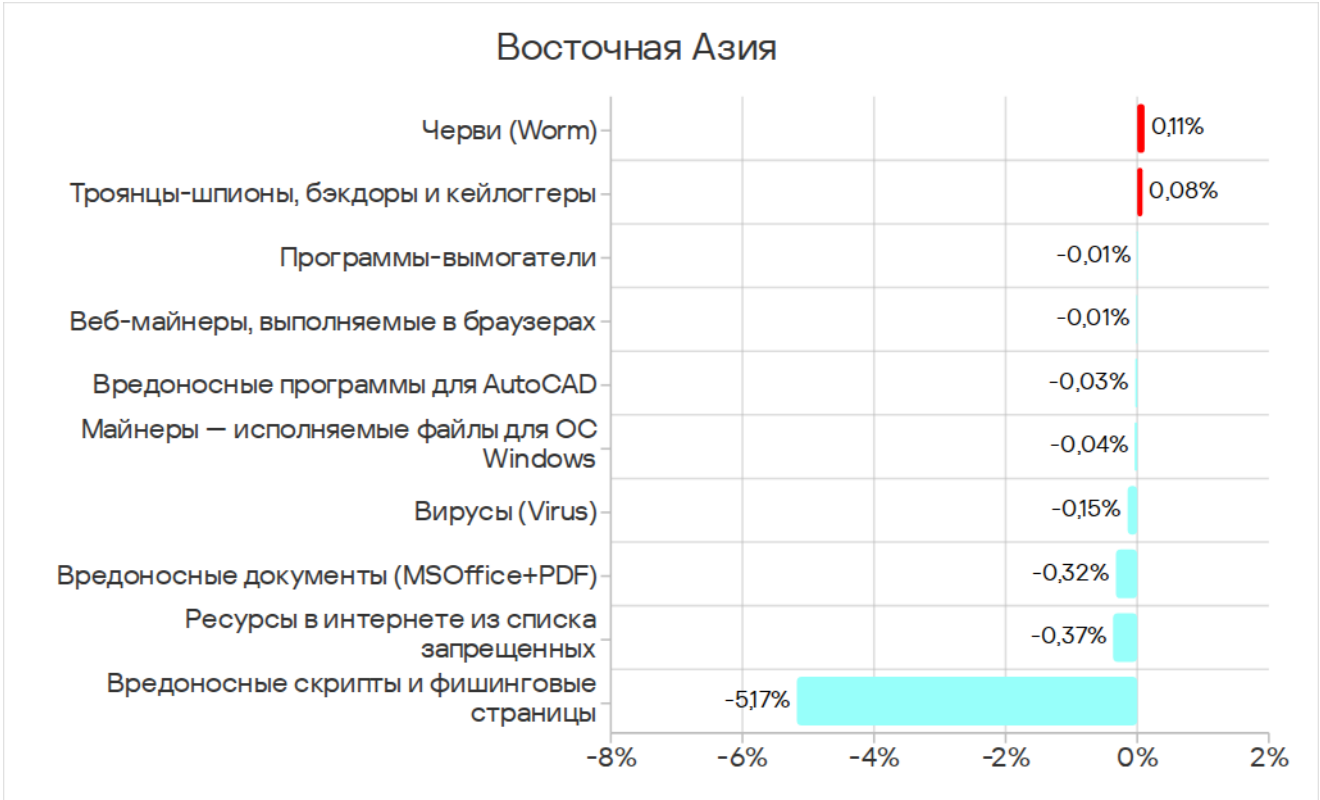
Категории угроз

В четвертом квартале 2025 года в Восточной Азии в рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы определенной категории, лидируют шпионские программы. Восточная Азия единственный регион, где в этом рейтинге лидирует шпионское ПО.

Показатель категории вредоносные скрипты и фишинговые страницы в предыдущем квартале резко вырос из-за того, что в континентальном Китае на компьютерах в сфере инжиниринга и интеграторов АСУ распространялись вредоносные скрипты-шпионы. Эта категория занимала первое место в рейтинге. В четвертом квартале показатель вернулся к

характерному для региона уровню, а вредоносные скрипты — на вторую позицию в рейтинге.





За квартал показатели выросли у шпионских программ и червей.

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

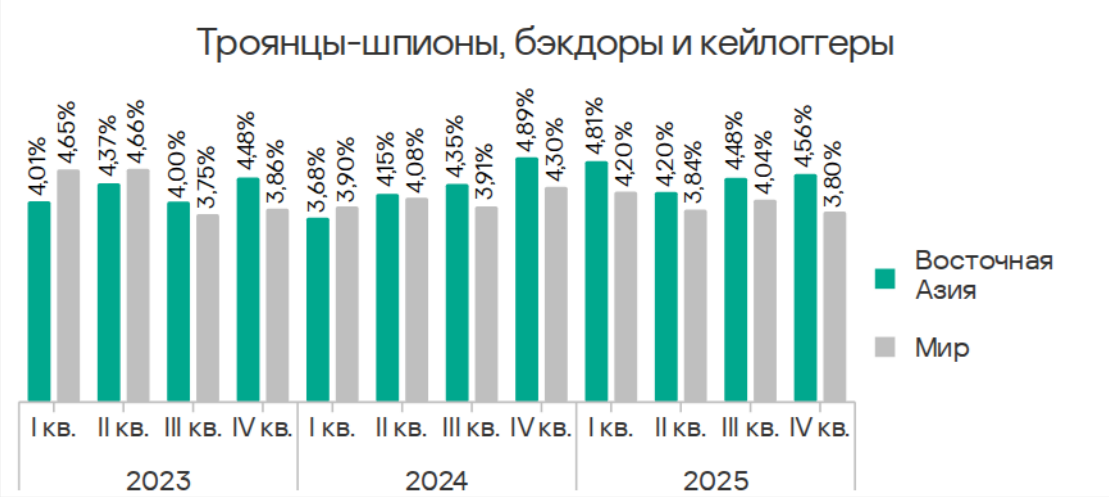
- черви;
- шпионские программы — в 1,2 раза;
- вирусы — в 2,2 раза, третье место среди регионов;
- вредоносное ПО для AutoCAD — в 4,1 раза, второе место среди регионов.

Шпионские программы

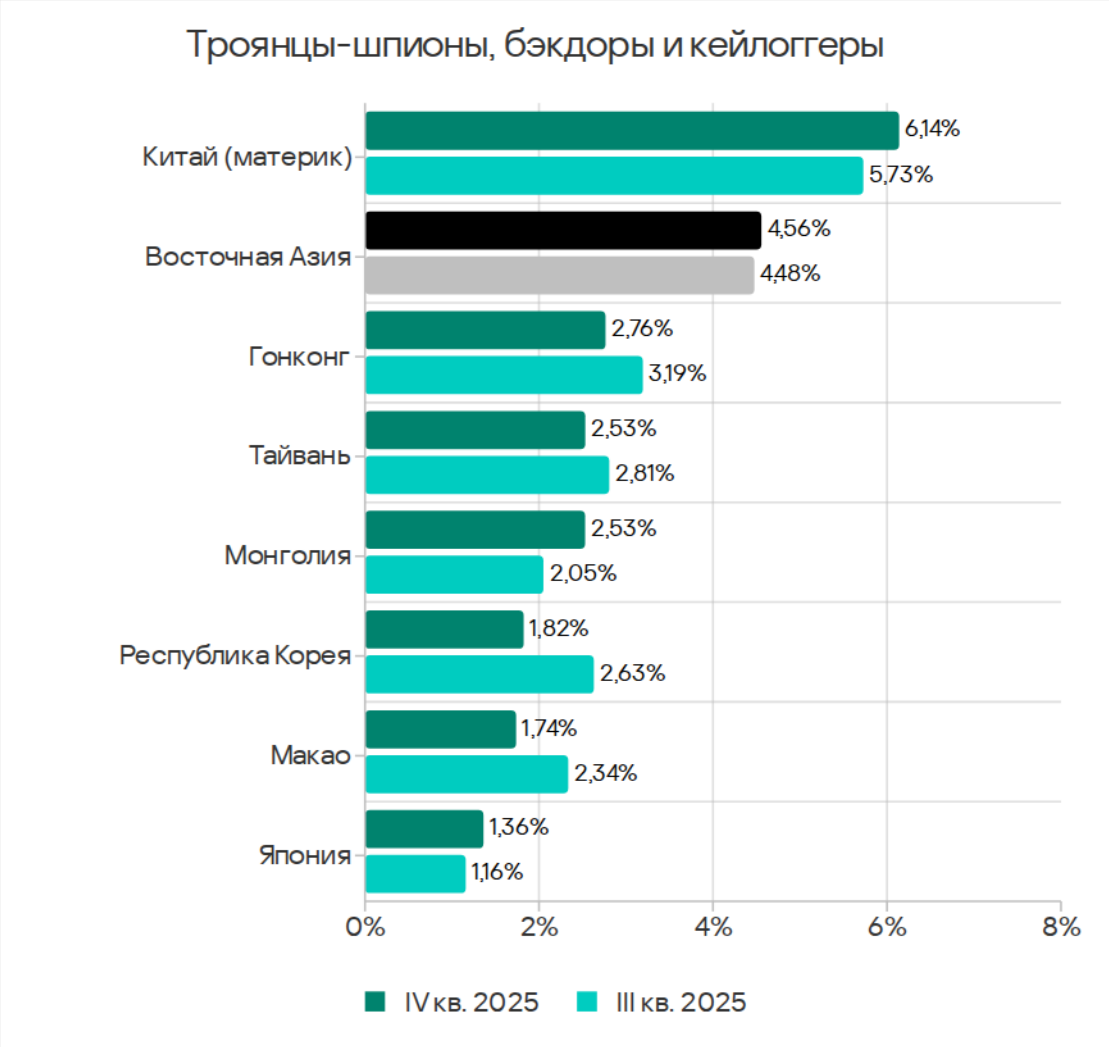
Среди регионов по доле компьютеров АСУ, на которых блокируются шпионские программы, Восточная Азия занимает пятое место. Это единственный регион, где шпионские программы лидируют в рейтинге категорий по доле компьютеров АСУ, на которых блокировались соответствующие угрозы.

Доля компьютеров АСУ, на которых блокируется шпионское ПО, в регионе довольно стабильна и относительно высока.

Показатель в регионе растет второй квартал подряд и достиг 4,56%. Это в 3,6 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 6,14%. В Японии показатель — наименьший (1,36%).



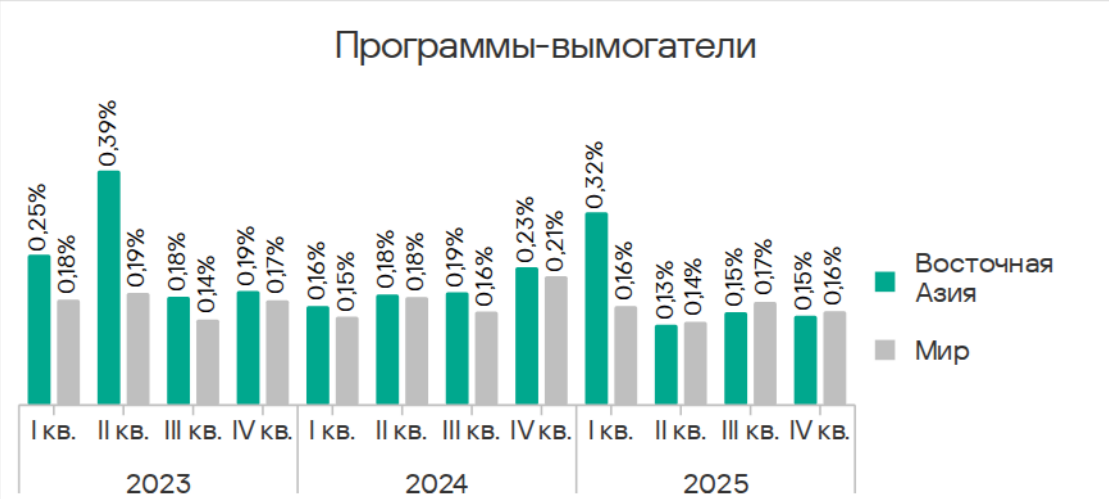
В регионе шпионские программы распространяются через все источники, в четвертом квартале 2025 года чаще всего — через почтовые клиенты.

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

Программы-вымогатели

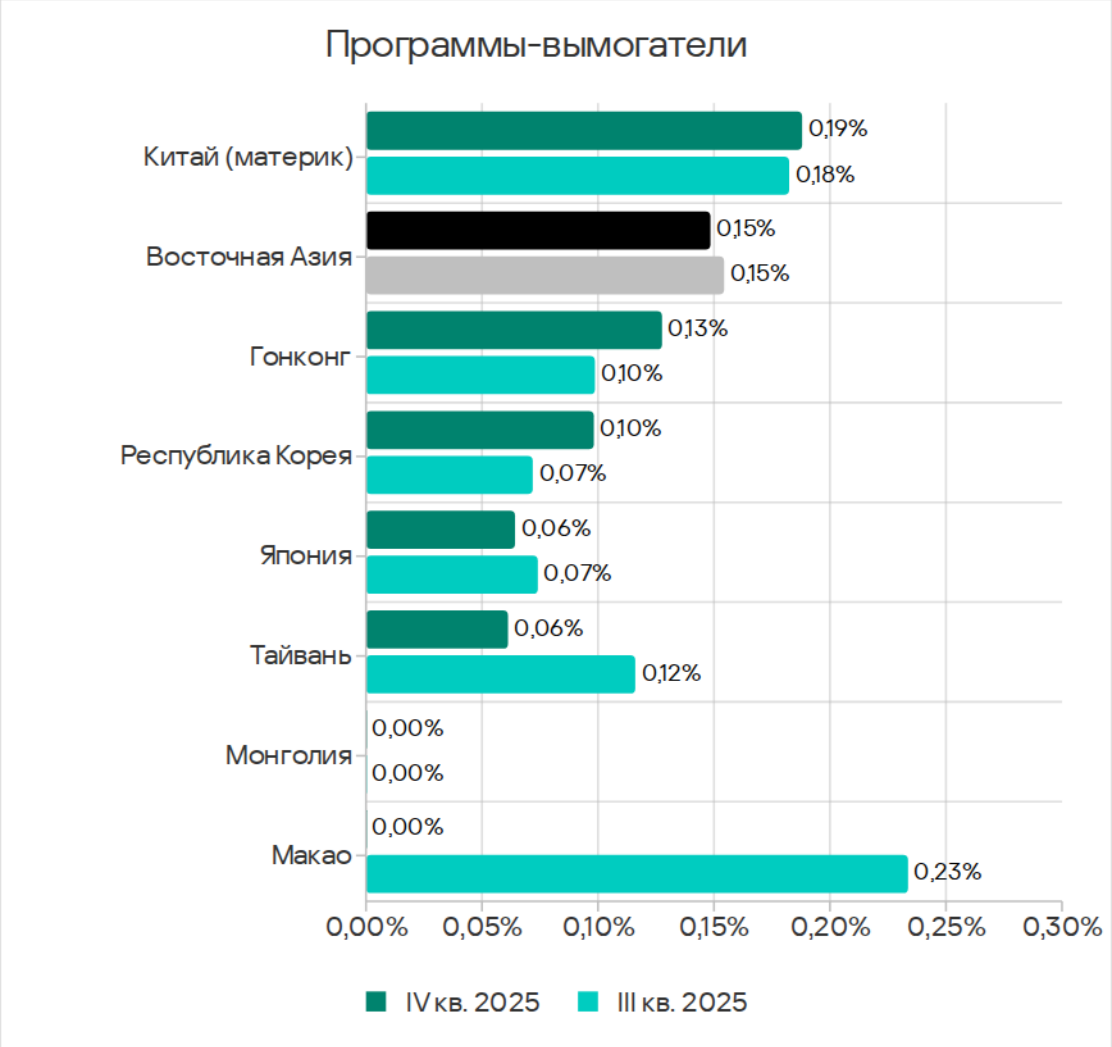
Восточная Азия находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, с 0,15%. Это в 3,0 раза больше, чем в Северной Европе, где показатель — наименьший.

В отличие от большинства других категорий угроз в регионе, у программ-вымогателей показатель за квартал не уменьшился.



Среди стран и территорий региона по этому показателю лидирует континентальный Китай с 0,19%. Отметим, что программы-вымогатели были обнаружены в значимых значениях не во всех странах.

Показатель вырос в континентальном Китае, Гонконге и Корее.



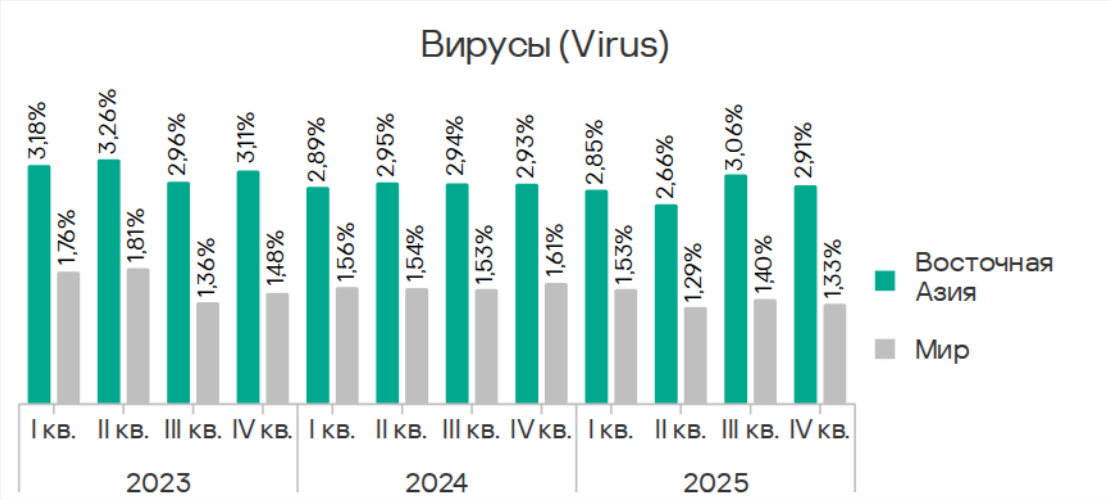
Вирусы и вредоносные программы для AutoCAD

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.

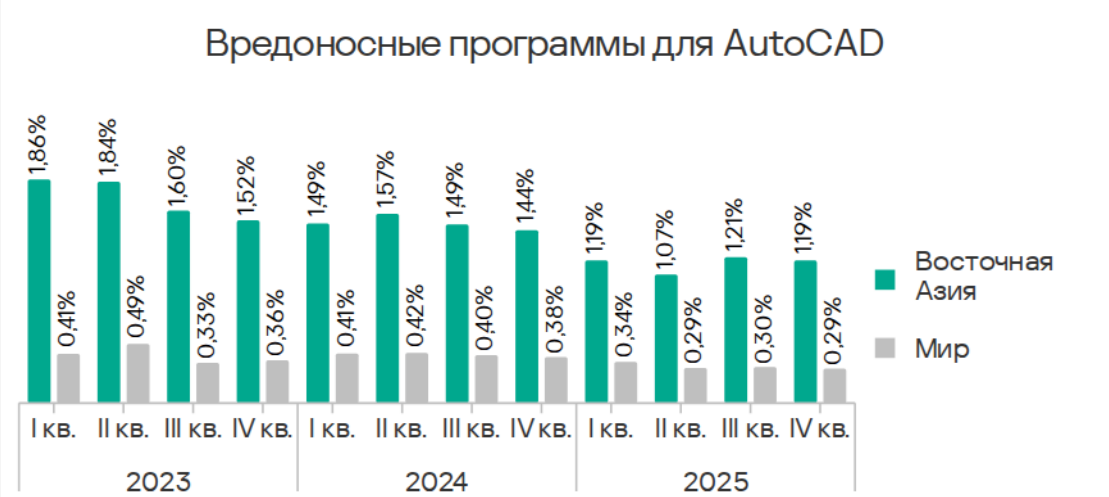
В Восточной и Юго-Восточной Азии ситуация с вредоносным ПО для AutoCAD схожая: в большинстве случаев оно распространяется так же, как вирусы. Эта особенность объясняет столь высокий показатель для этой категории вредоносного ПО.

Показатели обеих категорий за квартал уменьшились.

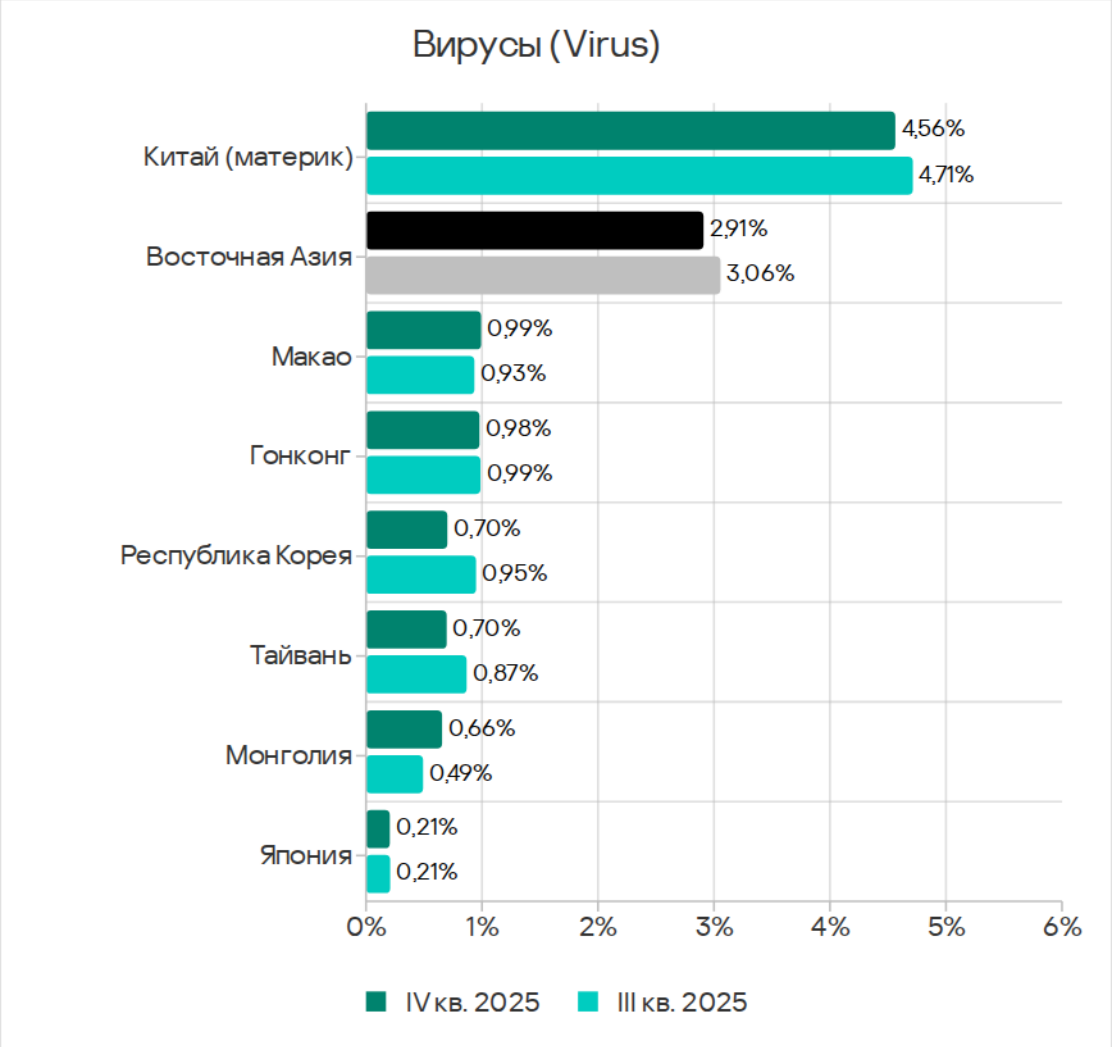
Доля компьютеров АСУ, на которых были заблокированы вирусы, в Восточной Азии составляет 2,91%. Это в 19,4 раза больше показателя в Западной Европе, где он — наименьший.

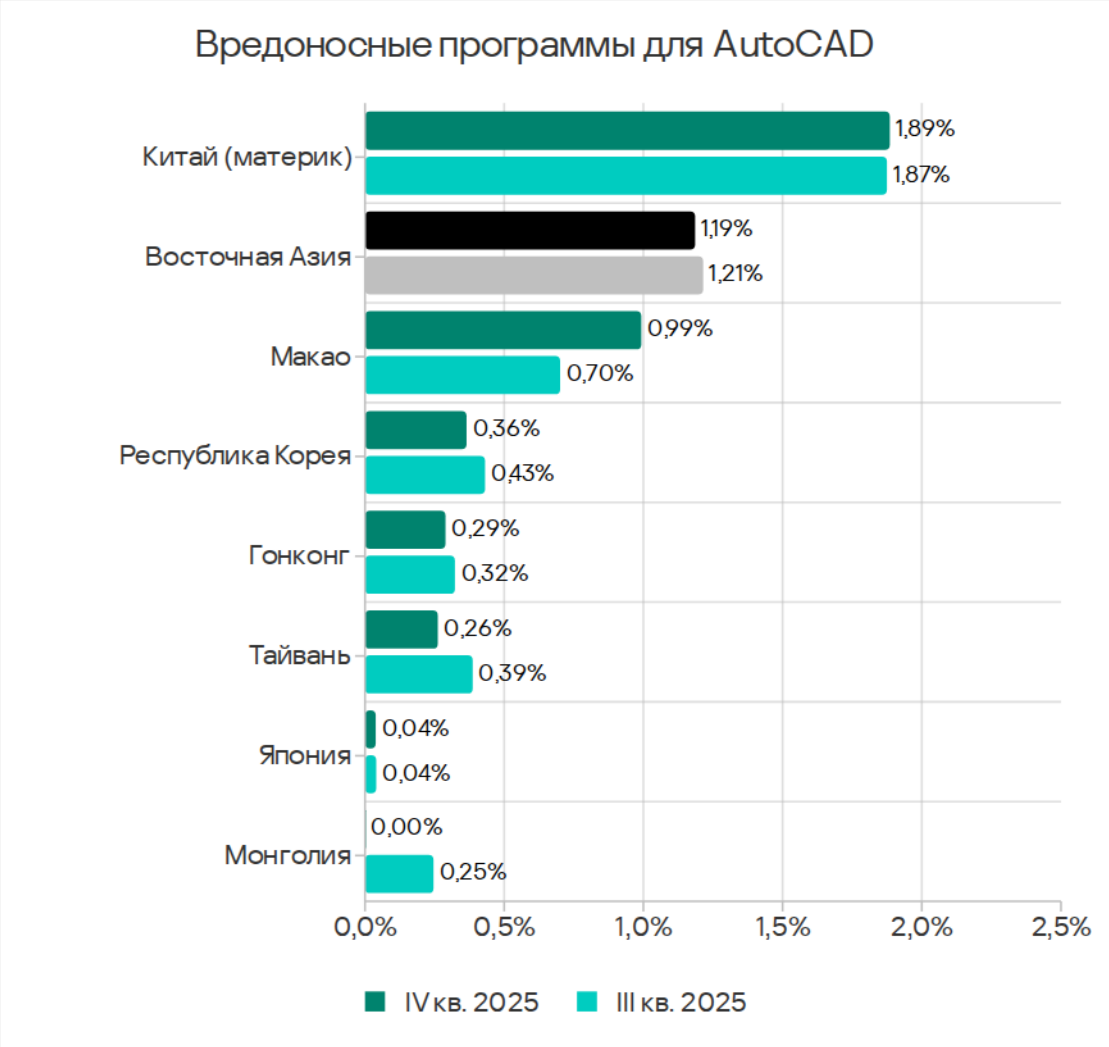


Показатель вредоносных программ для AutoCAD в Восточной Азии — 1,19% — в 119 (!) раз больше, чем в Северной Европе, где он — наименьший из регионов.



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, а показатель сетевых папок для этой угрозы всего в 1,1 раза меньше показателей почтовых клиентов и съемных носителей.

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

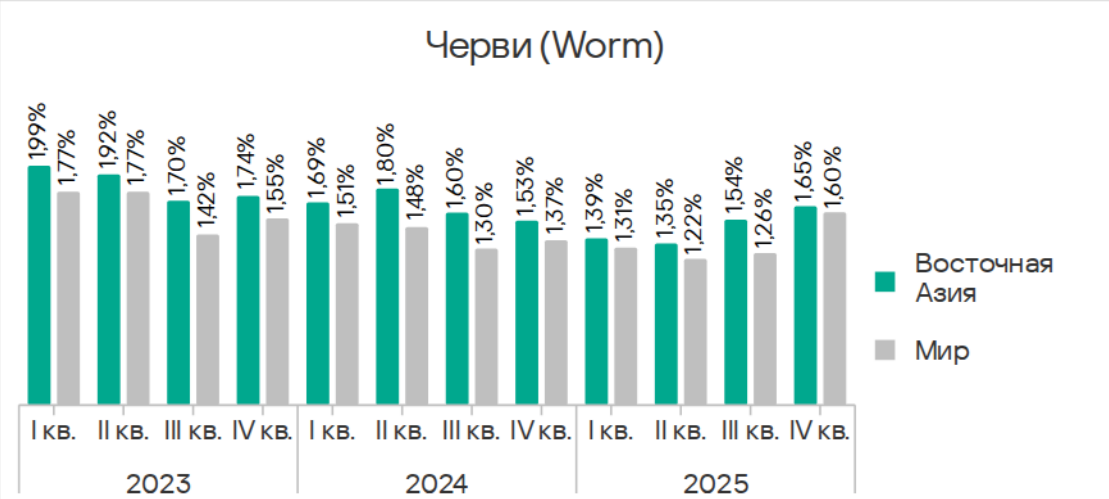
Черви

По доле компьютеров АСУ, на которых блокируются черви, Восточная Азия занимает среди регионов седьмое место.

В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие очередной волны фишинговых кампаний Curriculum-vitae-catalina, о которых мы рассказывали выше. Отметим, что Восточная

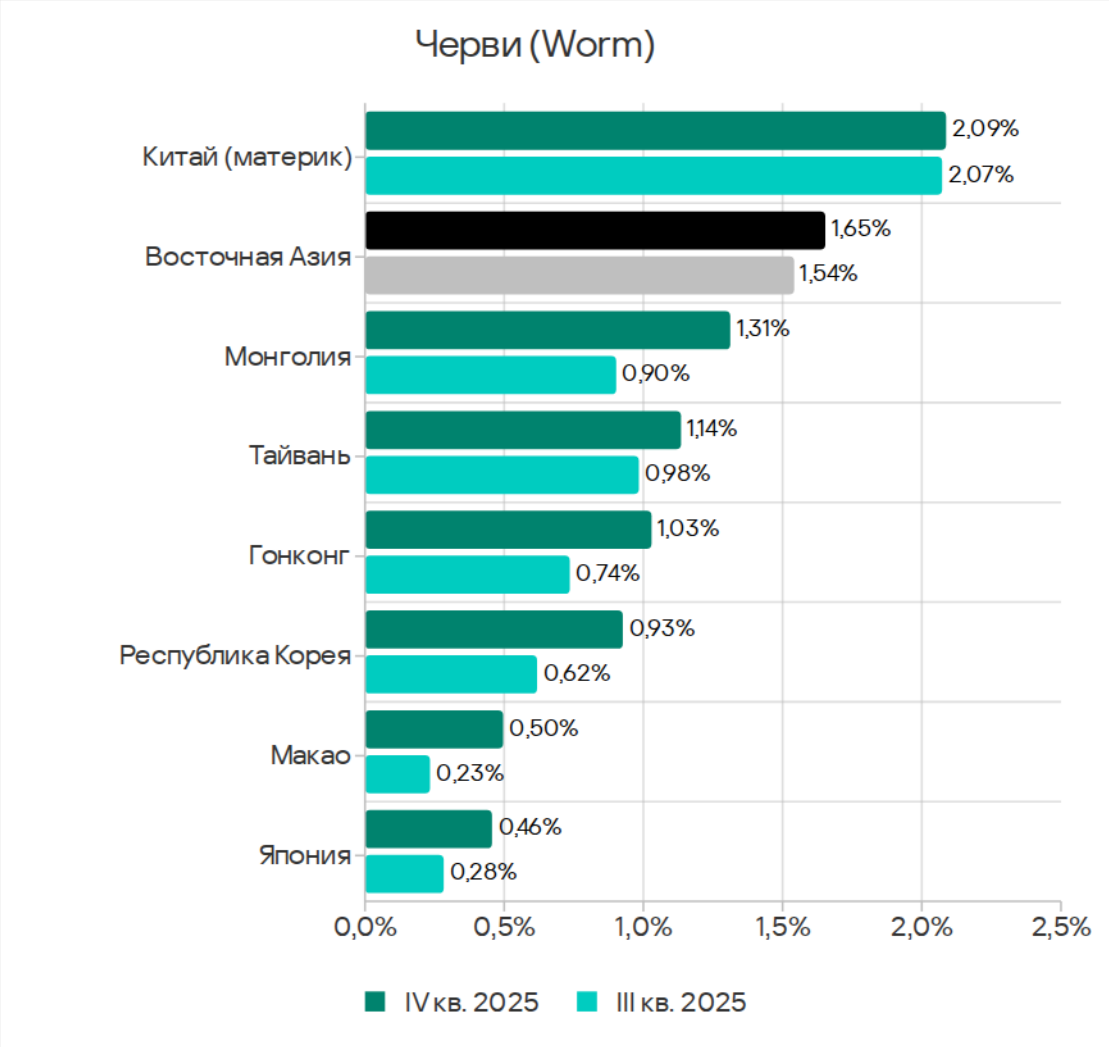
Азия входит в пятерку регионов, где изменения этого показателя — наименьшие.

В Восточной Азии доля компьютеров АСУ, на которых блокируются черви, выросла до 1,65%. Это в 5,2 раза больше, чем в Северной Европе, где показатель — наименьший среди всех регионов.



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются черви, лидирует континентальный Китай с 2,09%. В Японии показатель — наименьший (0,46%).

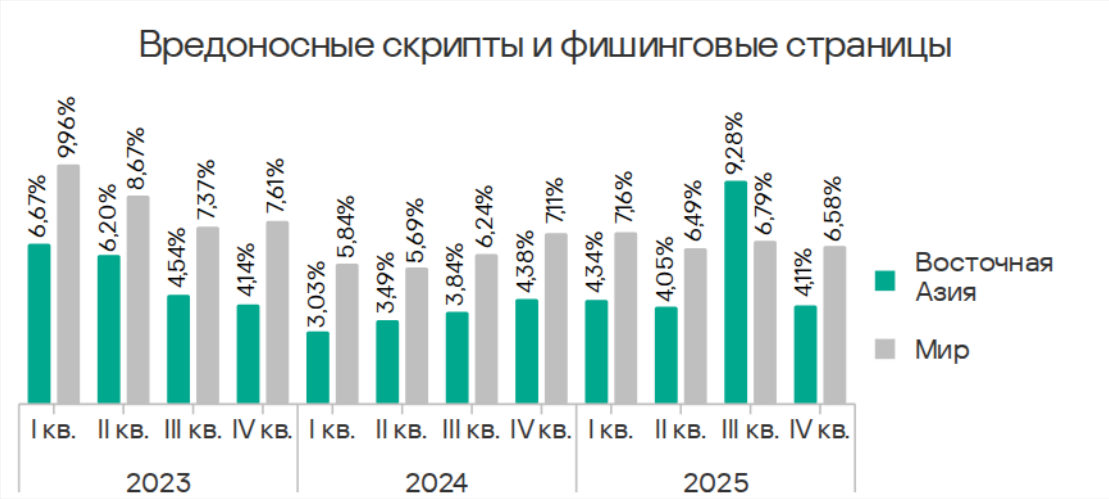
Значения выросли во всех странах и на всех территориях.



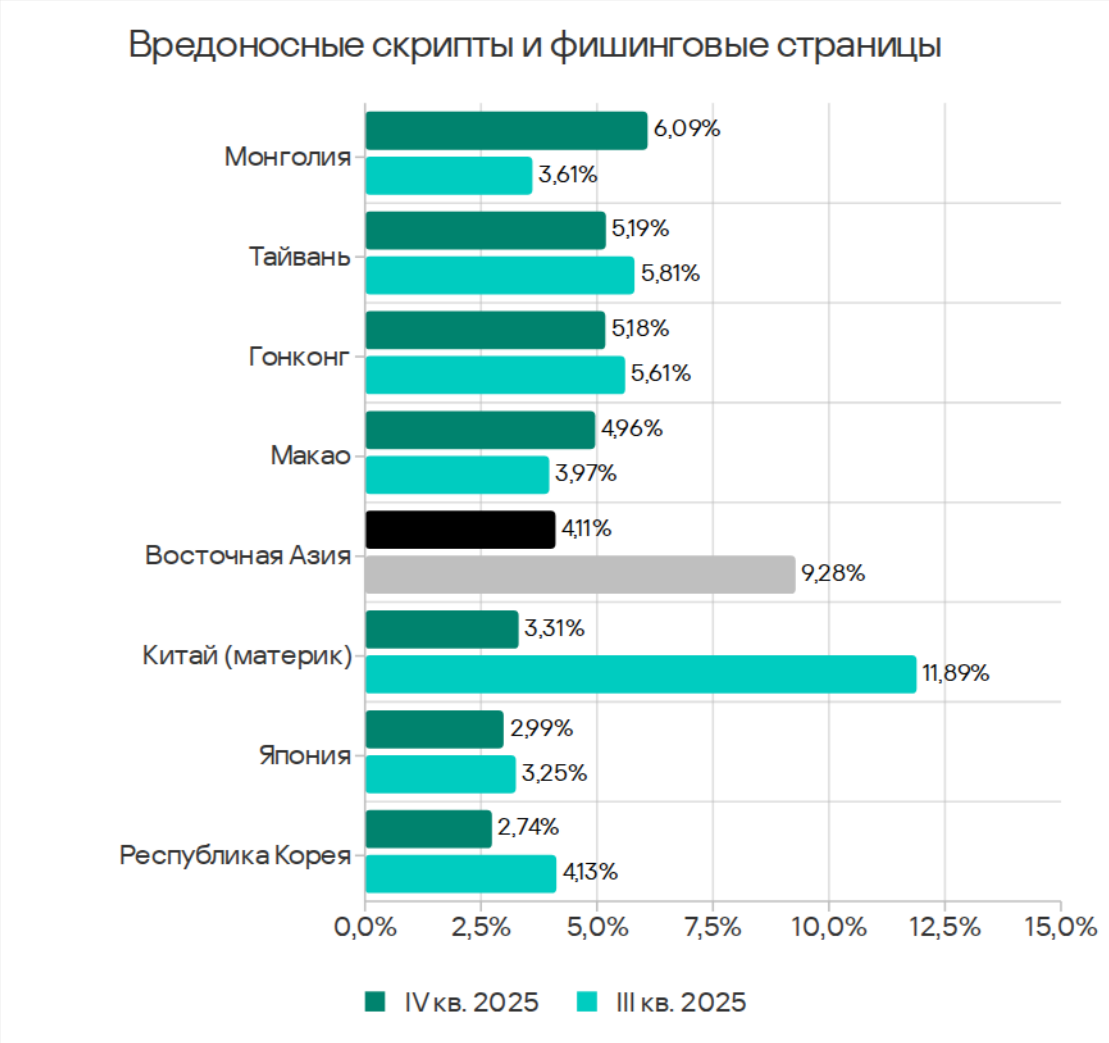
Распространяются черви через все источники угроз, преимущественно на съемных носителях. Континентальный Китай, который лидирует в рейтинге по червям, занимает первое место также по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Восточная Азия в соответствующем рейтинге регионов заняла 12-е место. Показатель в регионе, после роста в предыдущем квартале на 5,23 п. п., уменьшился на 5,17 п. п. — до 4,11%. Это в 1,6 раза больше, чем в Северной Европе, где значение — наименьшее.

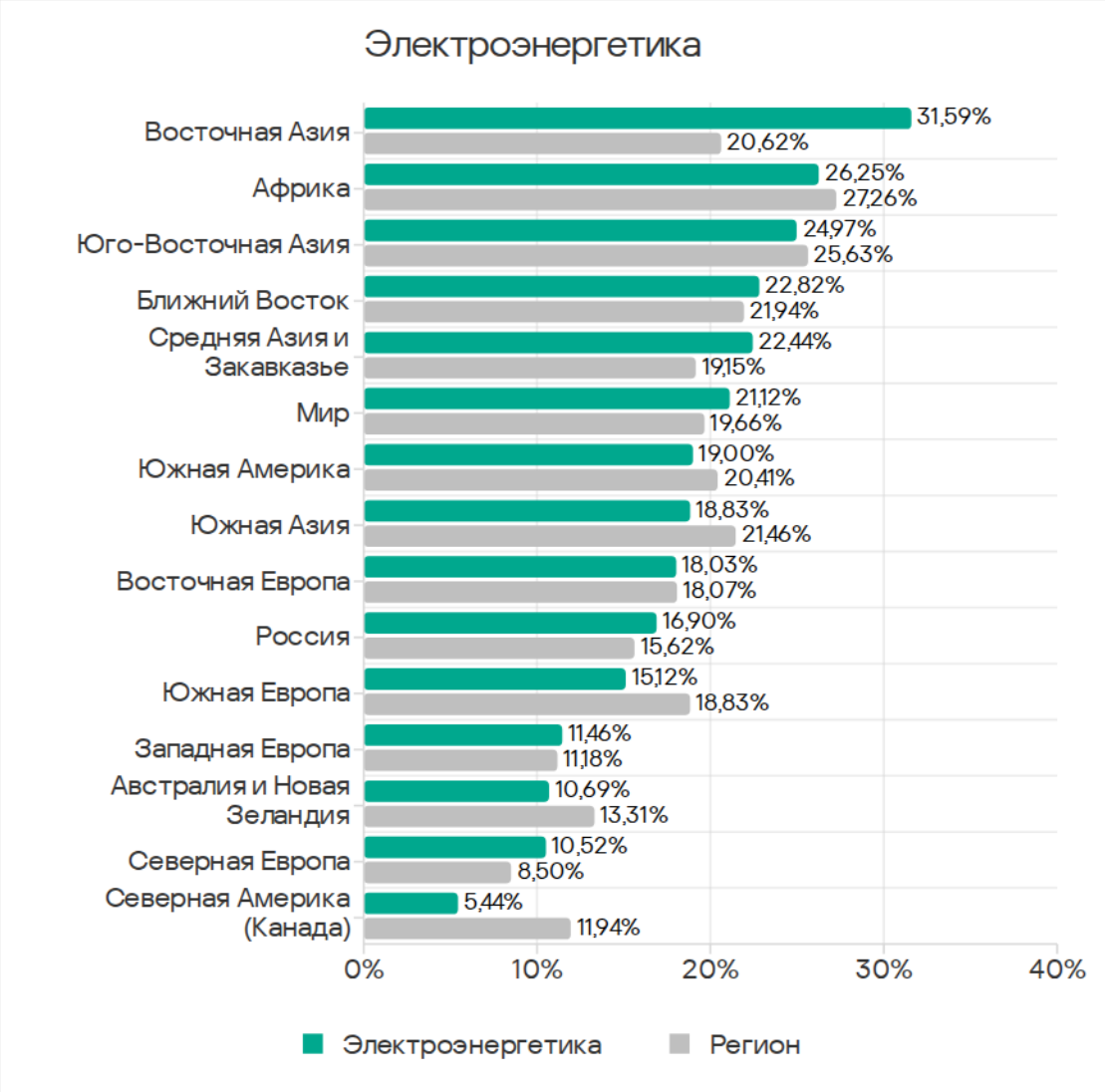


Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты, лидирует Монголия с 6,09%. В континентальном Китае показатель вернулся к норме, и в этом рейтинге он опустился с первого на пятое место.



Отрасли

В четвертом квартале 2025 года Восточная Азия лидирует среди регионов по показателю электроэнергетической отрасли — с 31,59%. Это в 5,8 раза больше, чем в регионе Северная Америка (Канада), где он — наименьший.

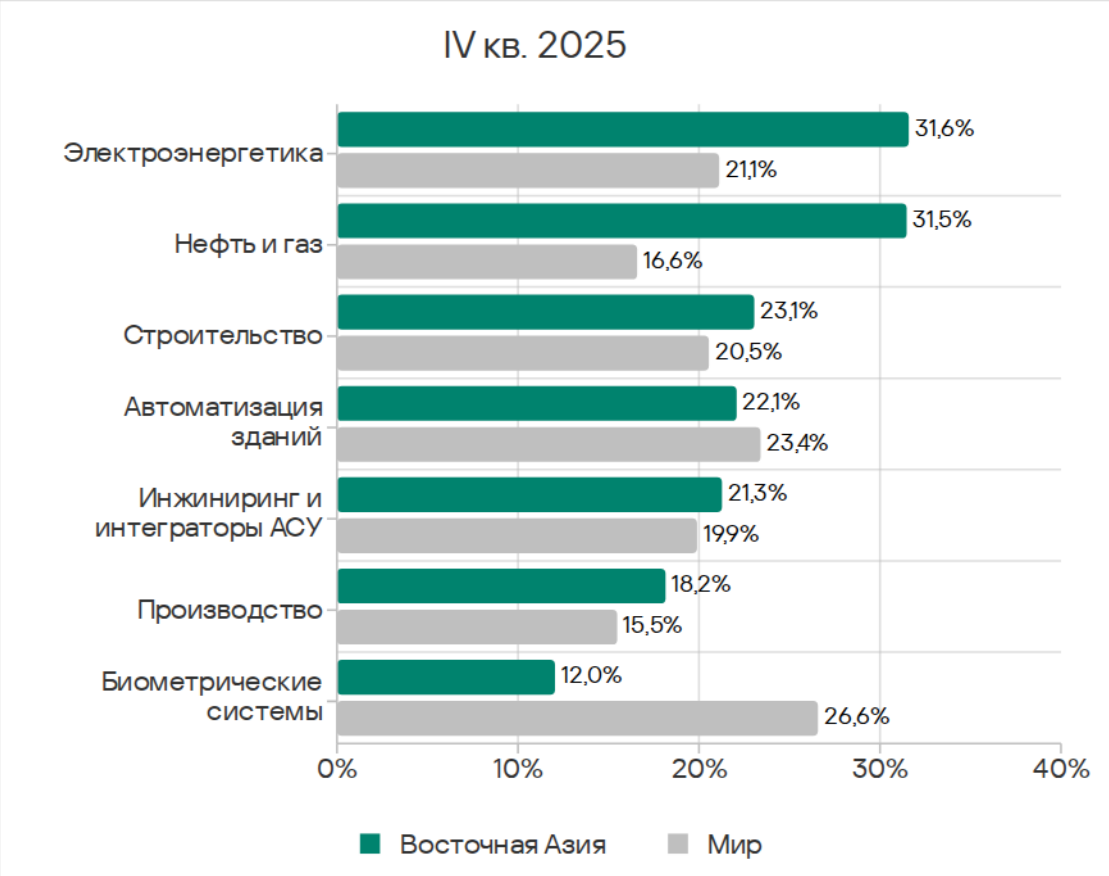


По показателю отрасли инжиниринг и интеграторы АСУ Восточная Азия занимает третье место среди регионов.

Восточная Азия — единственный регион, где электроэнергетика находится на первом месте среди отраслей по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Еще одна особенность региона — позиция инфраструктуры биометрических систем в рейтинге отраслей. В большинстве регионов она

находится в верхней части рейтинга, и только в Восточной и Юго-Восточной Азии замыкает его.

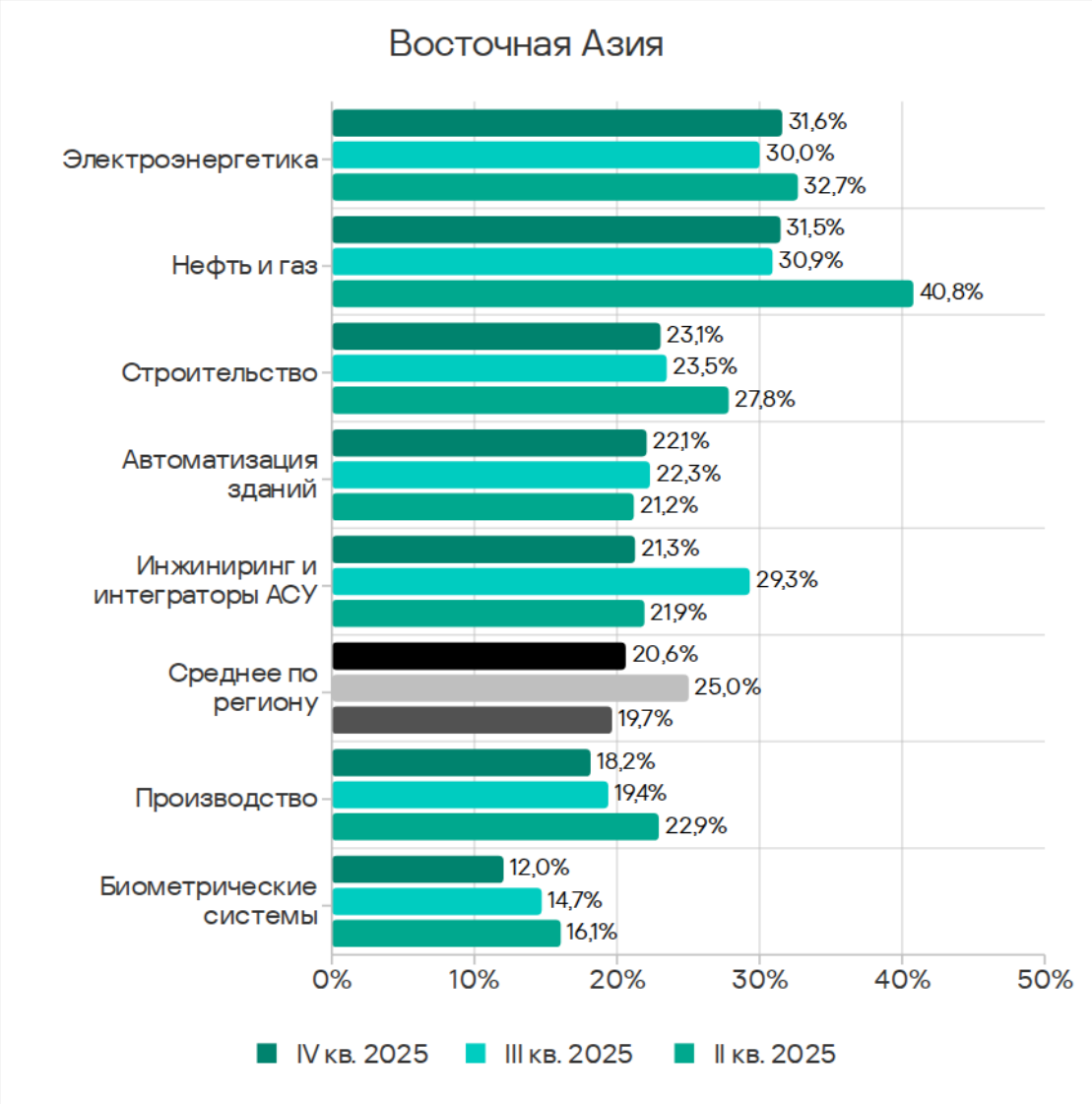


По сравнению с соответствующими среднемировыми значениями более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:

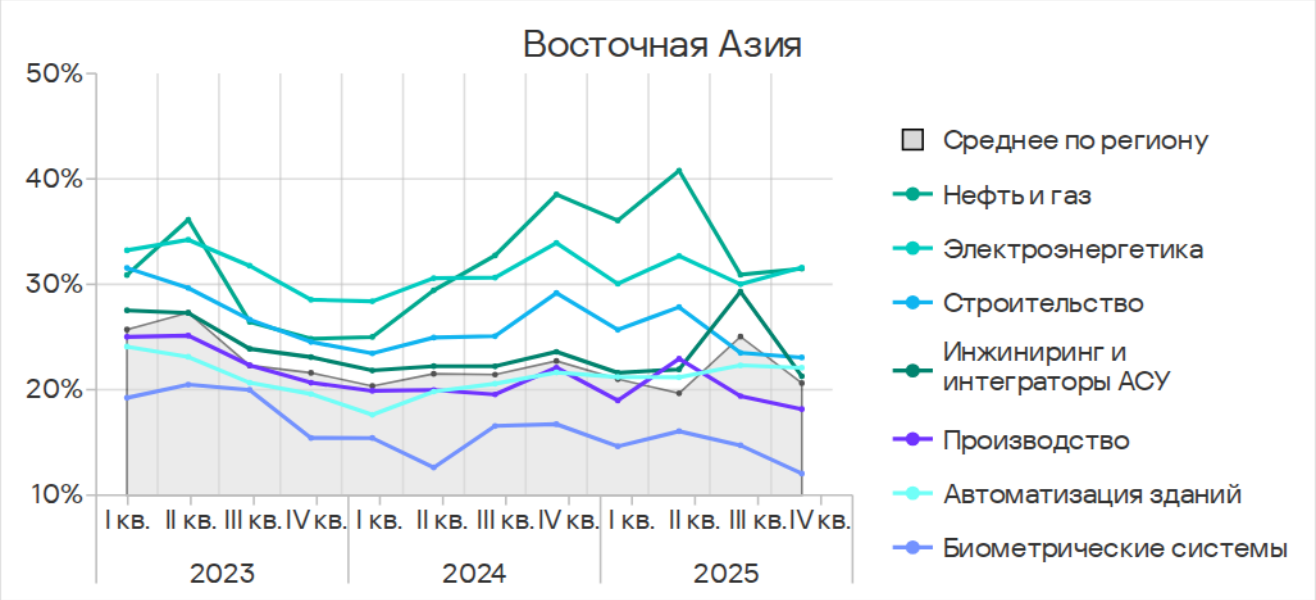
- электроэнергетика — в 1,5 раза;
- строительство — в 1,1 раза;
- инжиниринг и интеграторы АСУ — в 1,1 раза;
- производство — в 1,2 раза.

В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась только в электроэнергетической отрасли.

Показатель отрасли инжиниринг и интеграторы АСУ, который в предыдущем квартале резко увеличился, вернулся к уровню, характерному для этой отрасли.



Самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, сохраняется в электроэнергетике на протяжении всего рассматриваемого периода. При этом значение показателя в отрасли 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.



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, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	4,55%	6,15%	5,76%	9,18%	11,55%	8,47%	5,74%	5,71%
Почтовые клиенты	4,77%	2,90%	1,35%	0,82%	—	1,89%	1,01%	1,40%
Съемные носители	0,23%	0,83%	0,64%	1,86%	1,20%	0,46%	1,10%	0,66%
Сетевые папки	—	0,20%	0,22%	0,28%	—	0,29%	0,46%	0,18%
Показатель отрасли в регионе	12,05%	22,08%	21,27%	31,59%	31,47%	23,05%	18,15%	

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

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	1,36%	2,33%	2,25%	4,41%	5,98%	2,80%	2,11%	2,19%
Вредоносные скрипты и фишинговые страницы	7,50%	5,51%	3,97%	5,40%	8,76%	6,29%	4,09%	4,11%
Вредоносные документы (MSOffice+PDF)	3,18%	2,46%	1,42%	2,63%	2,39%	2,46%	1,84%	1,42%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,64%	6,19%	4,53%	9,52%	7,57%	4,86%	4,27%	4,56%
Программы-вымогатели	0,23%	0,31%	0,14%	0,31%	0,40%	0,29%	0,14%	0,15%
Майнеры — исполняемые файлы для ОС Windows	—	0,21%	0,17%	0,17%	—	0,23%	0,09%	0,15%
Веб-майнеры, выполняемые в браузерах	—	0,10%	0,06%	0,06%	—	0,11%	0,09%	0,06%
Вредоносные программы для AutoCAD	0,23%	1,07%	1,41%	2,57%	4,38%	5,89%	1,47%	1,19%
Черви (Worm)	1,82%	2,90%	1,49%	3,48%	3,19%	2,12%	2,62%	1,65%
Вирусы (Virus)	1,14%	2,58%	3,49%	5,88%	5,58%	5,72%	3,35%	2,91%
Показатель отрасли в регионе	12,05%	22,08%	21,27%	31,59%	31,47%	23,05%	18,15%	

Особенности региона

Высокая доля компьютеров АСУ, на которых блокируются шпионские программы. По этой угрозе Восточная Азия занимает не ниже третьего места по показателям во всех отраслях, кроме автоматизации зданий и инфраструктуры биометрических систем.

Высокий уровень угроз на съемных носителях. По доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, Восточная Азия занимает не ниже третьего места по

показателям во всех отраслях, кроме инфраструктуры биометрических систем.

Высокий уровень угроз в сетевых папках. По доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, Восточная Азия лидирует по показателям во всех отраслях, кроме инфраструктуры биометрических систем.

Высокая доля компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD. По этому показателю Восточная Азия лидирует среди регионов во всех отраслях, кроме инфраструктуры биометрических систем, где регион занимает второе место. Эта угроза распространяется преимущественно в сетевых папках.

Электроэнергетика

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

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, шпионские программы, вредоносные программы для AutoCAD;
- второе место по показателям вирусов и червей.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы 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, шпионские программы, черви, вирусы и программы-вымогатели;
- второе место по показателям угроз категорий вредоносные документы и вредоносные программы для AutoCAD;
- третье место по показателю майнеров в формате исполняемых файлов.

Инжиниринг и интеграторы АСУ

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 Восточная Азия занимает:

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

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- третье место по показателю вирусов.

Строительство

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

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, третье – 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;
- третье место по показателям червей, вирусов и программ-вымогателей.

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: майнеры обеих категорий, вредоносные программы для AutoCAD;
- второе место по показателю угроз категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вирусы;

- третье место по показателям угроз следующих категорий: вредоносные документы, шпионские программы, программы-вымогатели.

Автоматизация зданий

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

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 были заблокированы вредоносные программы для AutoCAD;
- третье место по показателю вирусов.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по угрозам из почты и третье – по угрозам из интернета и на съемных носителях;
- второе место по показателям следующих категорий угроз: шпионские программы, программы-вымогатели, черви и майнеры обеих категорий;
- третье место по показателям категорий вредоносные документы, вредоносные скрипты и фишинговые страницы.

Производство

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

Среди регионов по показателям в отрасли Восточная Азия занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках и на съемных носителях;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD;
- второе место по показателям шпионских программ, червей и вирусов;

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, второе – по показателю съемных носителей;
- третье место по показателю угроз следующих категорий: черви, веб-майнеры, вредоносные программы для AutoCAD.

Биометрические системы

Восточная Азия находится на 11-м месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

Среди регионов по показателям в отрасли Восточная Азия занимает второе место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

- первое место по угрозам в почтовых клиентах;
- первое место по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы и вредоносные документы.

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 четвертом квартале 2025 года соответствующий показатель в регионе был в 1,4 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 в формате исполняемых файлов, регион Средняя Азия и Закавказье лидирует среди регионов, по показателю червей она находится на третьем месте. Показатели этих категорий выше среднемировых в 2,0 и 1,5 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 занимают первое место. Основной канал распространения такого вредоносного ПО — интернет.

В четвертом 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. Среди всех индустрий во всех регионах строительная отрасль в Средней Азии и Закавказье занимает первое место по доле майнеров – исполняемых файлов, заблокированных на компьютерах АСУ.

Во всех рассмотренных в отчете отраслях, кроме отрасли инжиниринг и интеграторы АСУ, Средняя Азия и Закавказье лидируют среди регионов по

показателю майнеров — исполняемых файлов для ОС Windows. По показателям в отрасли инжиниринг и интеграторы АСУ регион находится на втором месте.

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

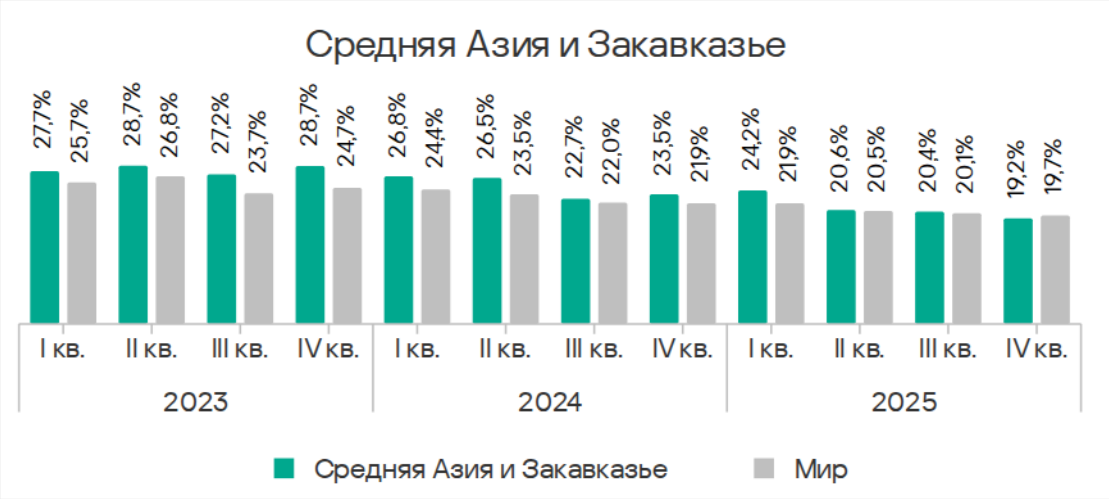
По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье занимают четвертое место с показателем, который в 1,1 раза выше среднемирового. Эта категория угроз в регионе в четвертом квартале 2025 года распространялась как в интернете, так и в электронной почте, и на съемных носителях.

По показателю программ-вымогателей регион Средняя Азия и Закавказье занимает не ниже третьего места в рейтингах регионов во всех отраслях. По показателям в инфраструктуре биометрических систем, а также строительной, электроэнергетической и производственной отраслях Средняя Азия и Закавказье занимают первое место среди регионов.

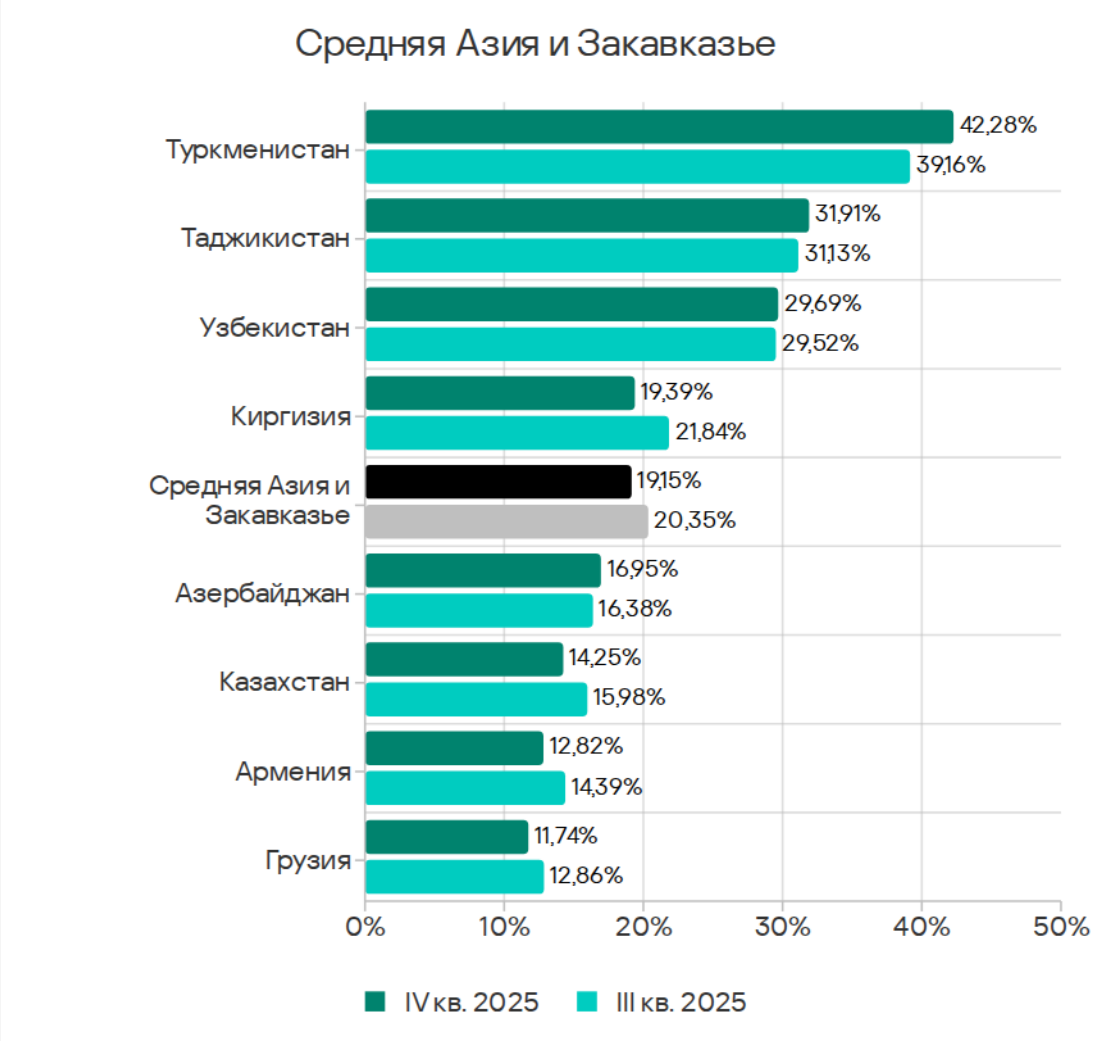
Статистика по всем угрозам

В четвертом квартале 2025 года Средняя Азия и Закавказье занимают седьмое место в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с 19.2%. Это в 2,3 раза больше, чем в Северной Европе, где показатель наименьший среди регионов.

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

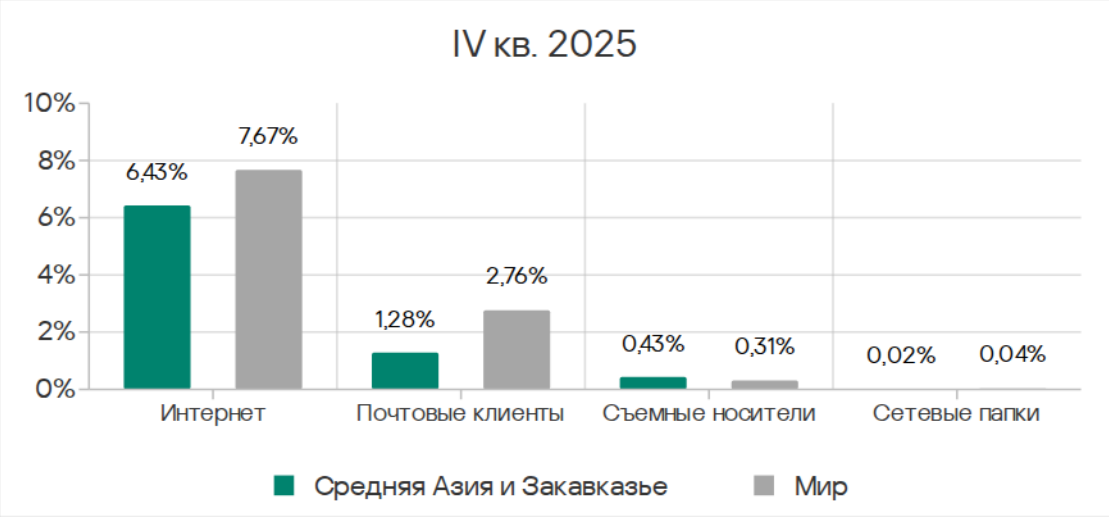


В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 11,74% в Грузии до 42,28% в Туркмении.

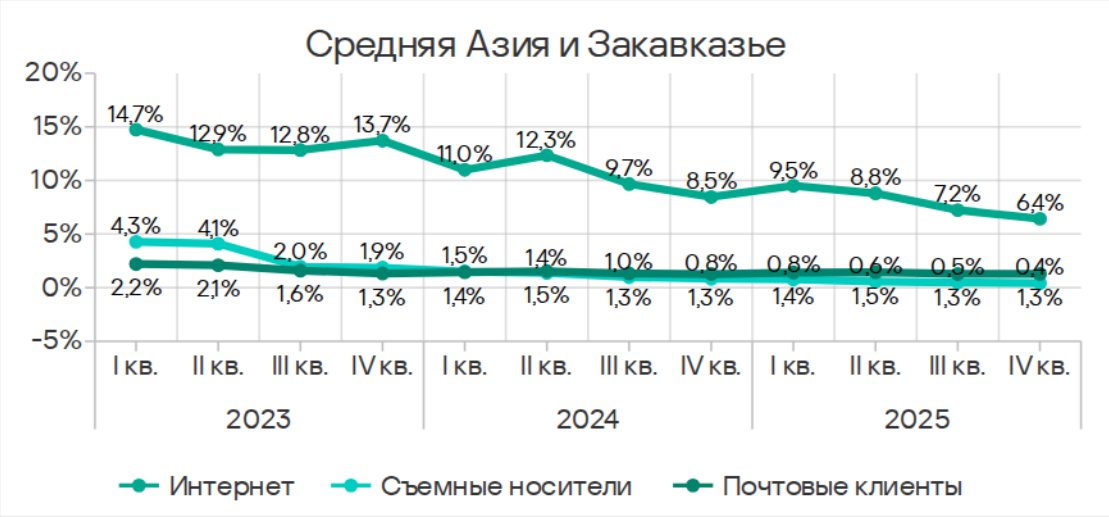


Источники угроз

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 1,4 раза.



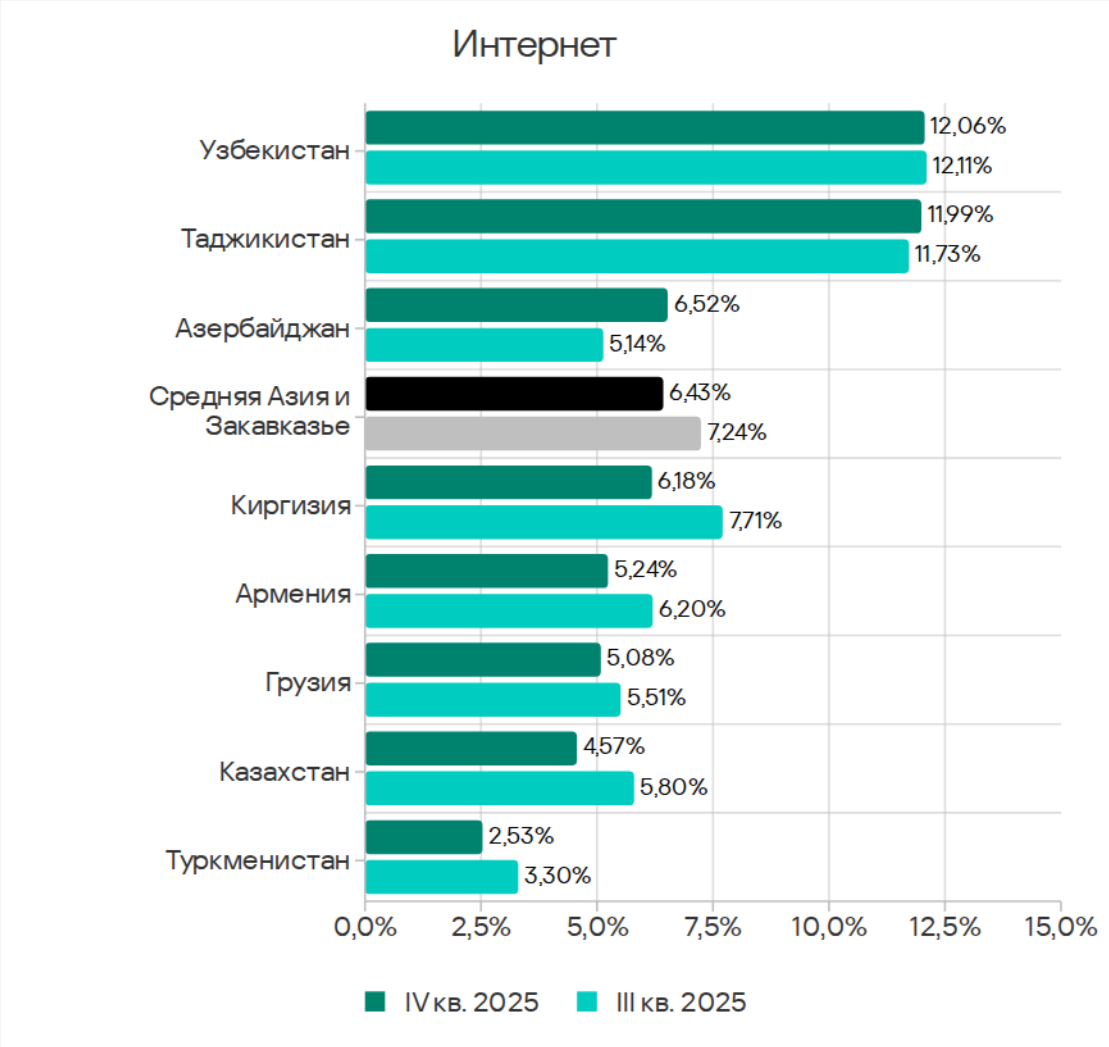
В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз, кроме почтовых клиентов.



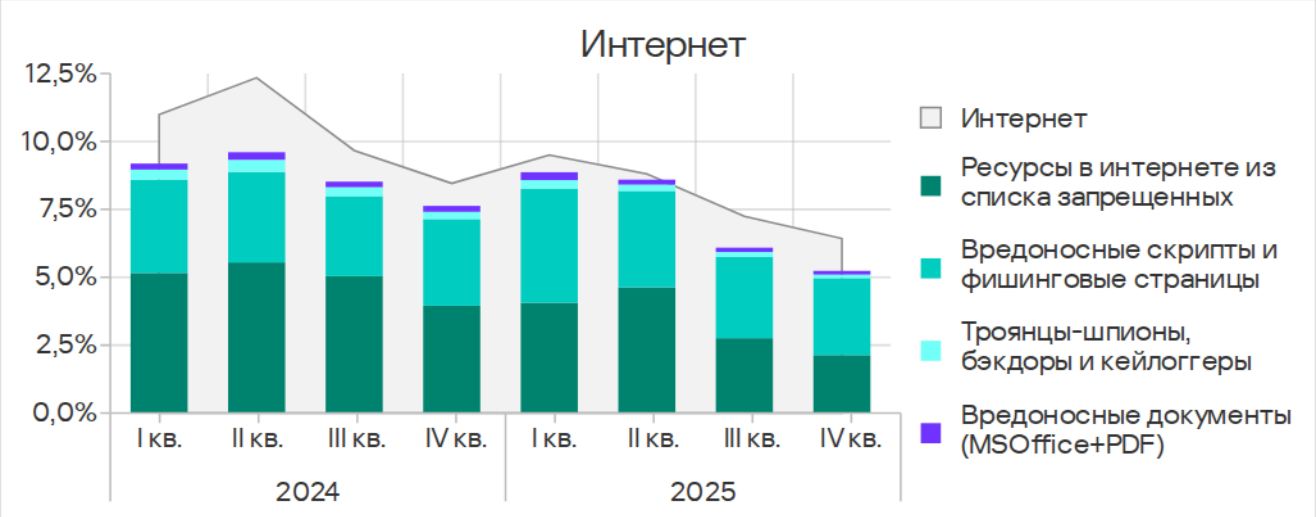
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Средняя Азия и Закавказье занимают 10-е место в рейтинге регионов с показателем 6,43%, который превышает минимальный — у Северной Европы — в 1,6 раза.

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, лидируют Узбекистан с 12,06% и Таджикистан с 11,99%. Наименьший показатель в Туркмении — 2,53%.



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

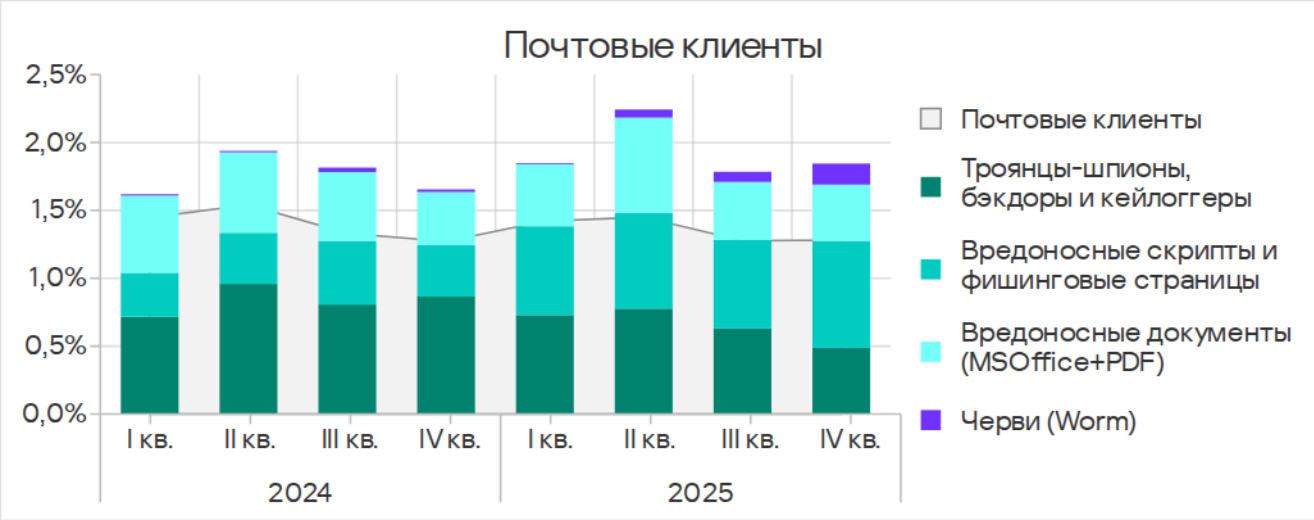


Почтовые клиенты

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 2,0 раза выше, чем в Северной Европе, которая этот рейтинг замыкает.

Среди стран региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидирует Азербайджан с 2,36%. Минимальный показатель — в Туркмении (0,48%). Показатель за квартал вырос во всех странах, кроме Казахстана и Таджикистана.

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



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это вызвано очередной волной фишинговых кампаний Curriculum-vitae-catalina, в ходе которых атакам подверглись организации во всех регионах мира. В Средней Азии и Закавказье пик атак пришелся на ноябрь.

Злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Под видом резюме (Curriculum Vitae) такие письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm). При запуске файла происходило заражение системы.

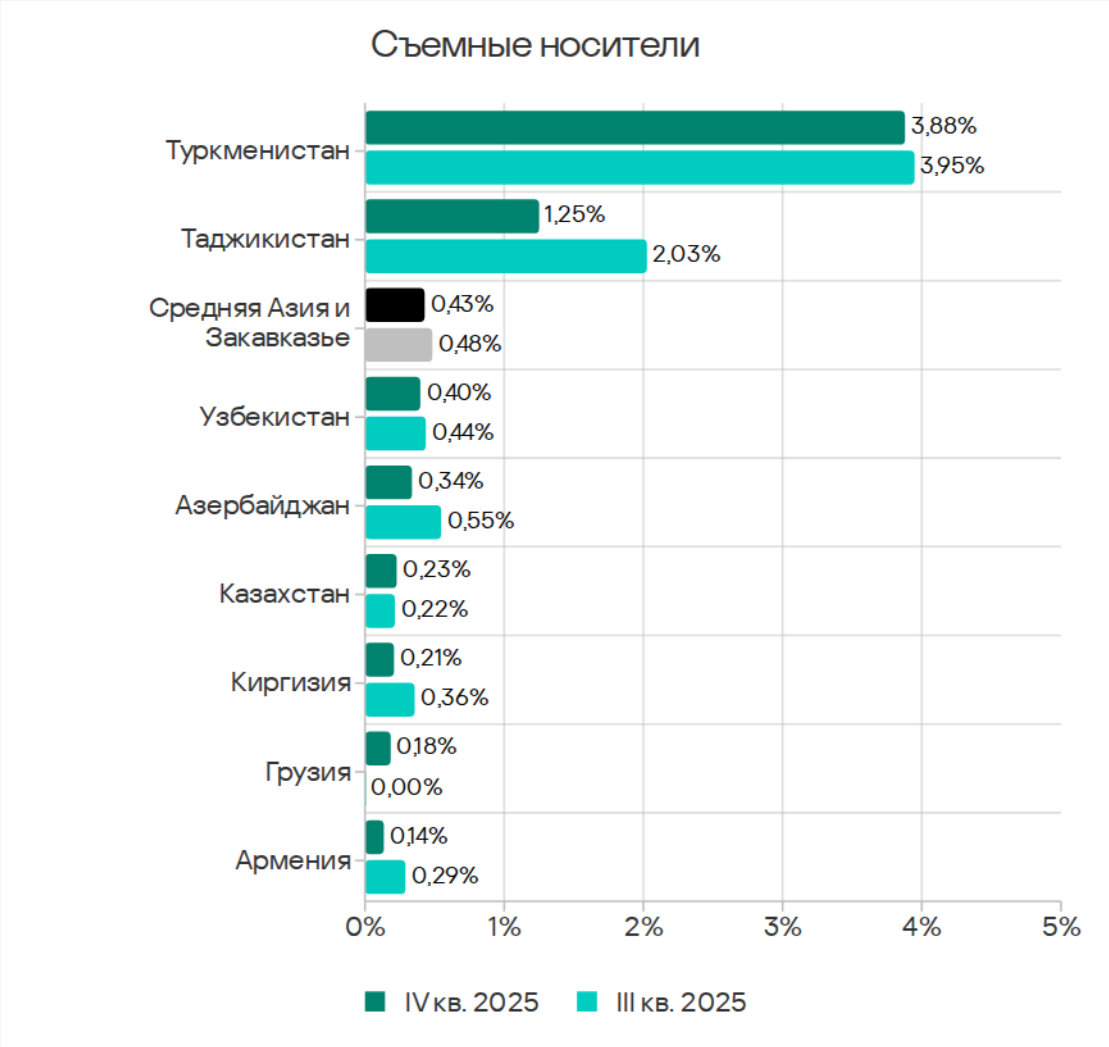
Как правило, такие кампании направлены на доставку вредоносного ПО для кражи данных, а также на доставку программ-шпионов или инструментов для удаленного управления (RAT).

Съемные носители

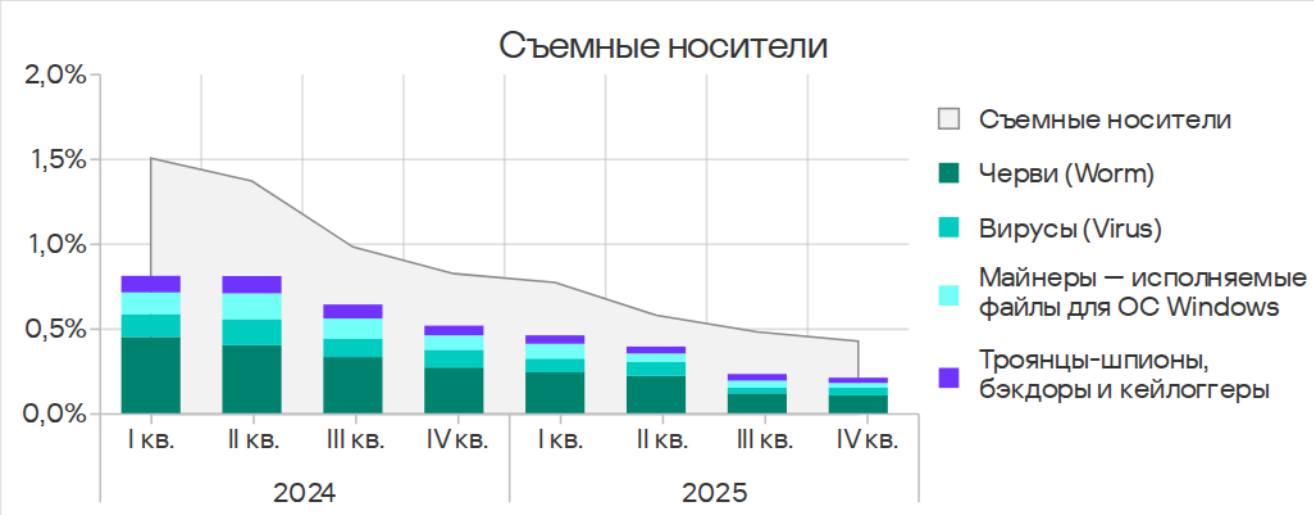
На первых шести позициях в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей – Африка, Ближний Восток и регионы Азии. Показатели этих регионов превышают показатели остальных не менее, чем в 2,2 раза.

Средняя Азия и Закавказье занимают пятое место с 0,43%. Это в 8,6 раза больше, чем в регионе Австралия и Новая Зеландия, где значение – наименьшее.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует Туркмения с 3,88%. Отметим, что эта страна была последней в рейтинге по угрозам из почтовых клиентов и интернета.

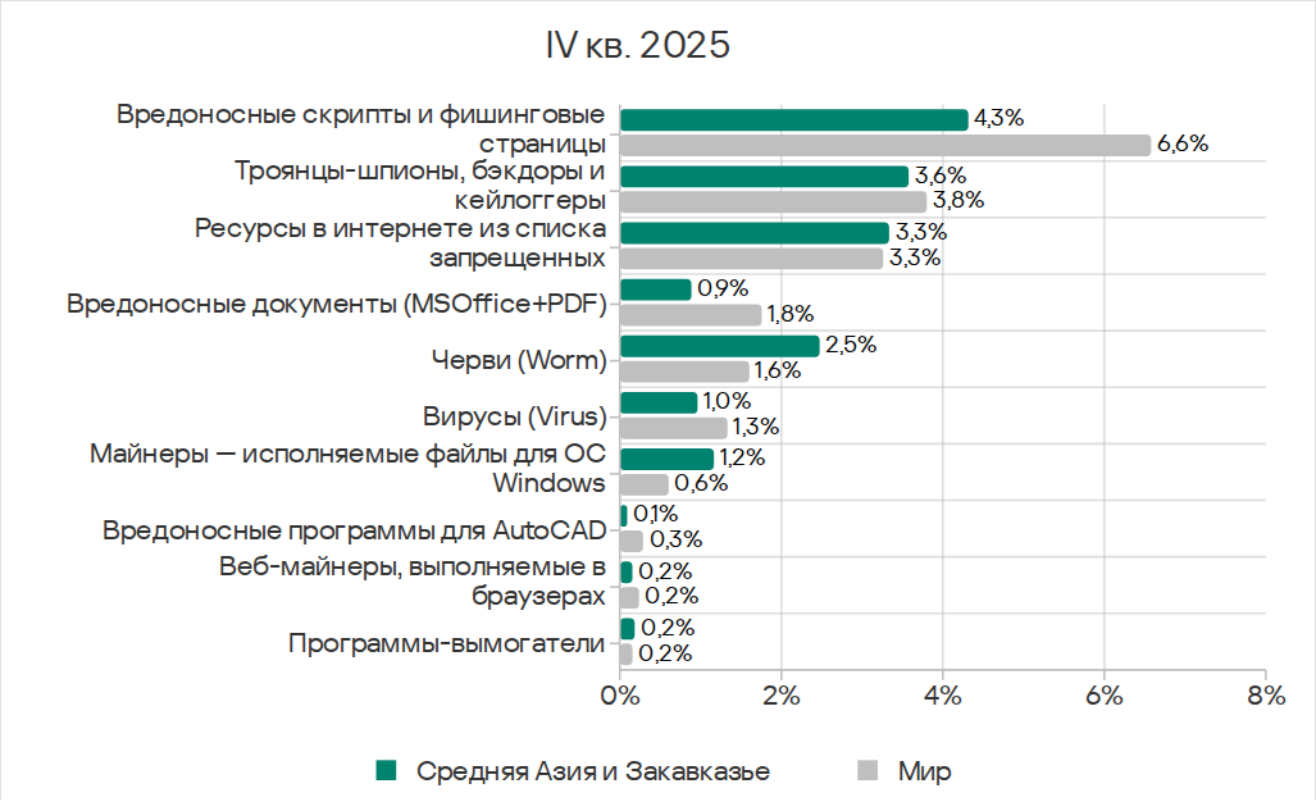


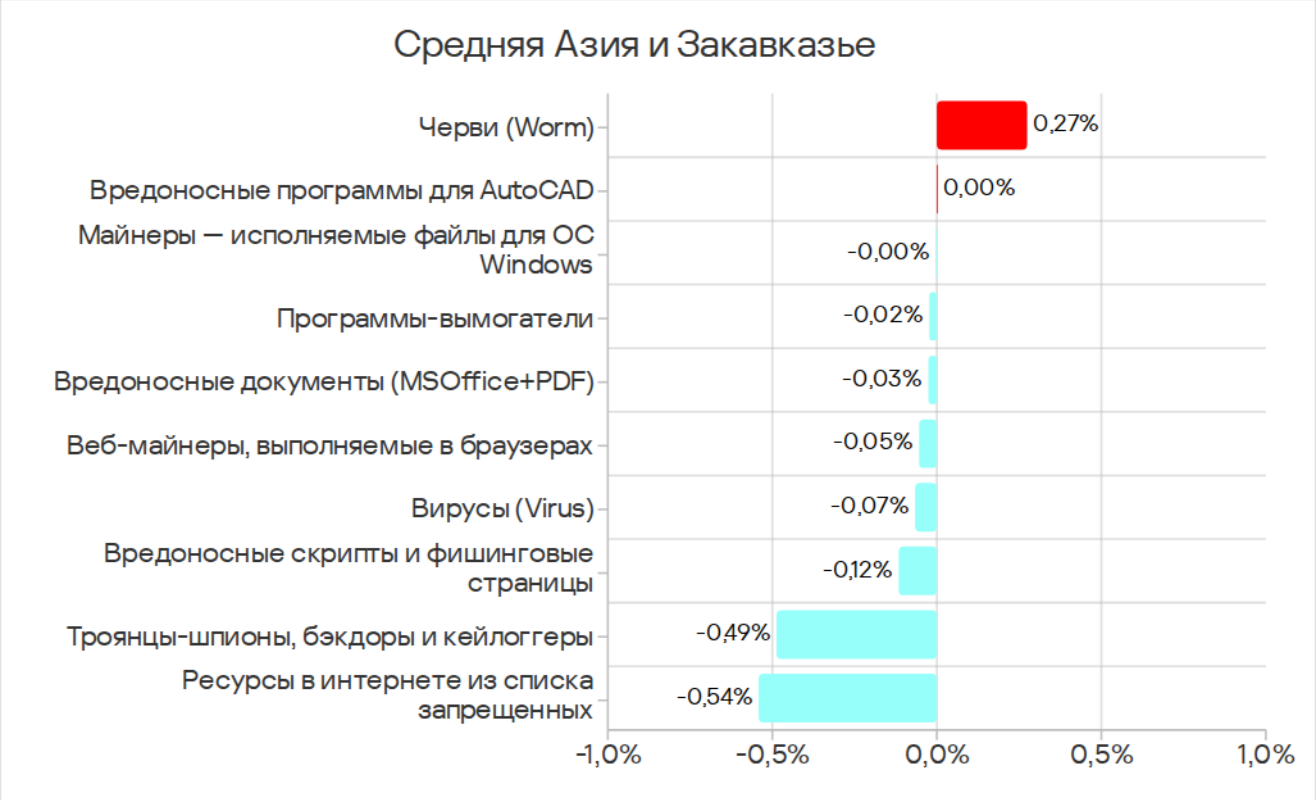
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы, шпионское ПО и майнеры — исполняемые файлы для ОС Windows.



По доле компьютеров АСУ, на которых блокируются майнеры в формате исполняемых файлов, Средняя Азия и Закавказье лидируют среди остальных регионов. По показателю червей регион находится на третьем месте.

Категории угроз





Из всех категорий угроз за квартал показатель вырос только у червей.

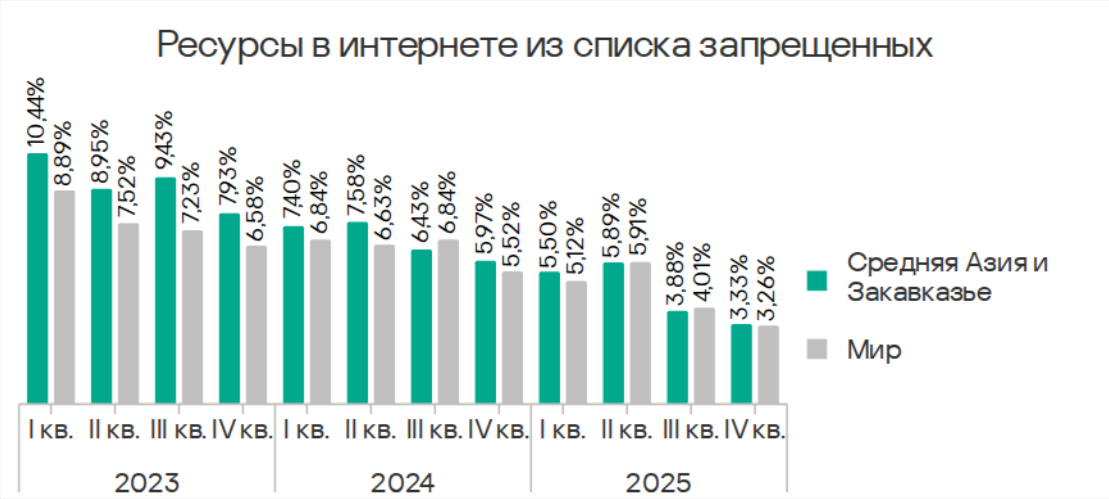
По сравнению со среднемировыми показателями в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории угроз:

- майнеры — исполняемые файлы для ОС Windows — в 2,0 раза; Средняя Азия и Закавказье лидируют среди регионов по этому показателю;
- черви — в 1,5 раза; регион находится на третьем месте в соответствующем рейтинге;
- программы-вымогатели — в 1,1 раза; четвертое место в рейтинге регионов по этому показателю;
- ресурсы в интернете из списка запрещенных.

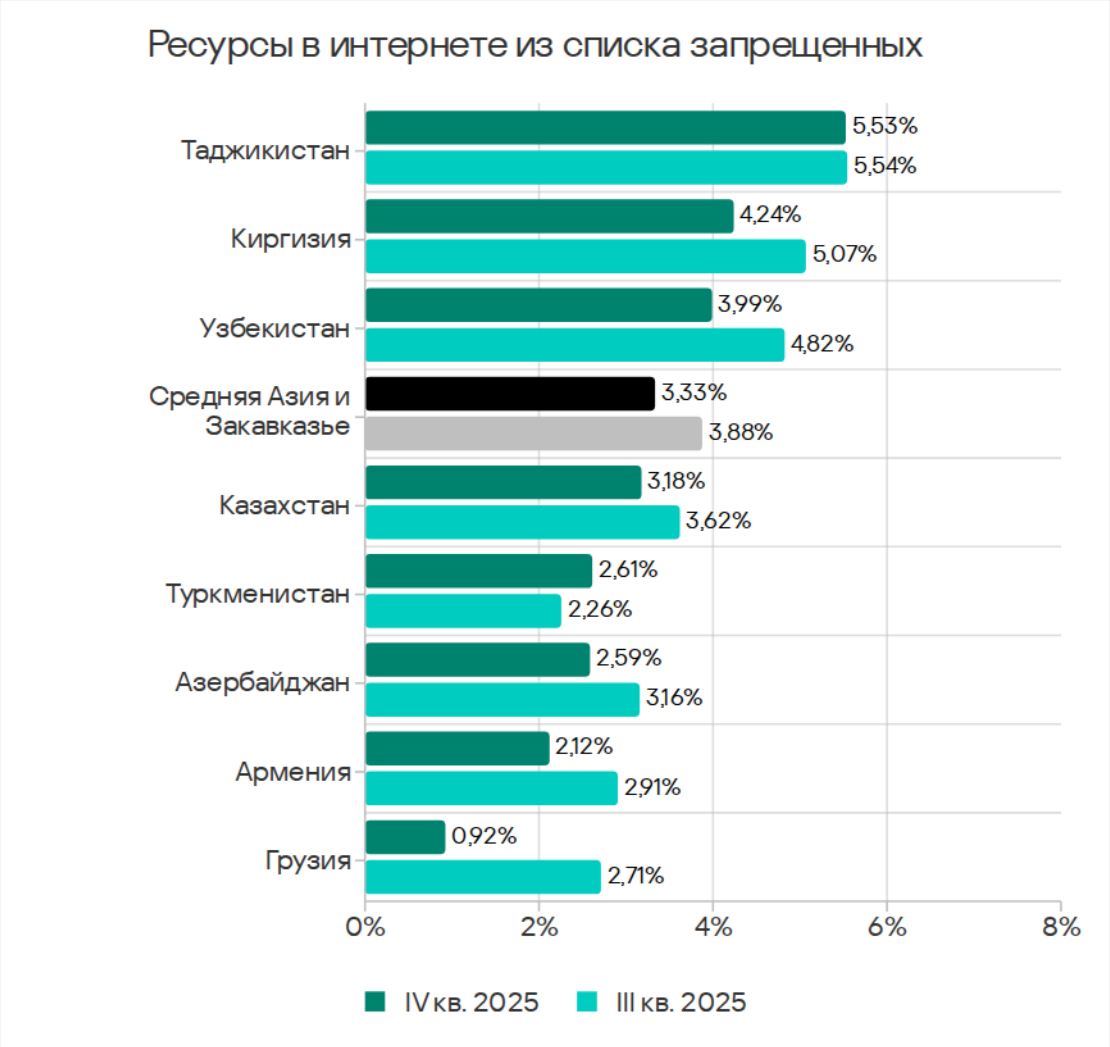
Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Средняя Азия и Закавказье занимают четвертое место среди регионов с 3,33%. Этот показатель в 1,9 раза больше, чем в Северной Европе, где он наименьший среди регионов.

Показатель постепенно снижается во всех регионах мира, в Средней Азии и Закавказье в четвертом квартале 2025 года он был наименьшим за три года.



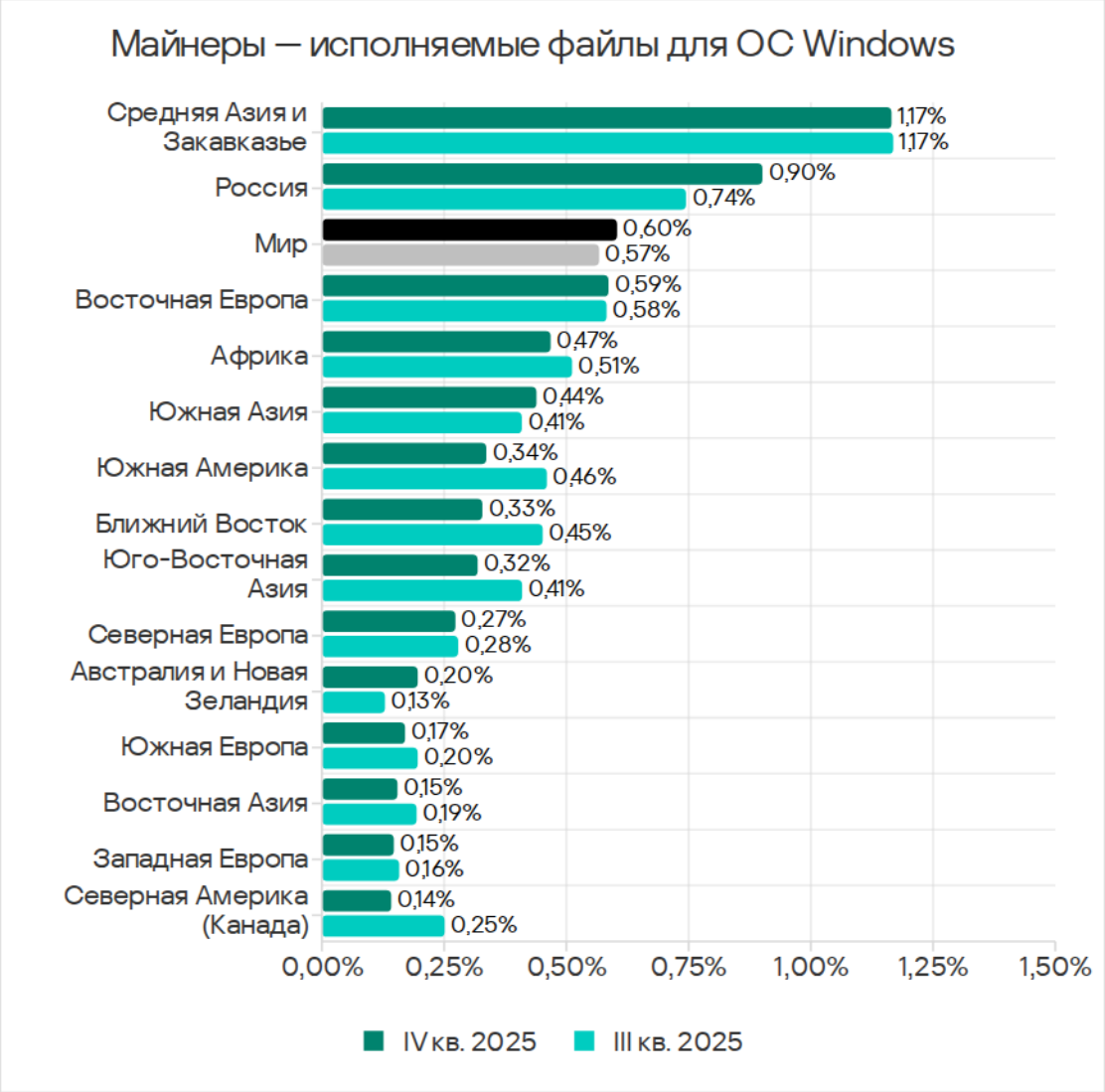
Среди стран региона по доле компьютеров АСУ, на которых заблокированы ресурсы в интернете из списка запрещенных, лидирует Таджикистан с 5,53%. Наименьший показатель – в Грузии (0,92%).



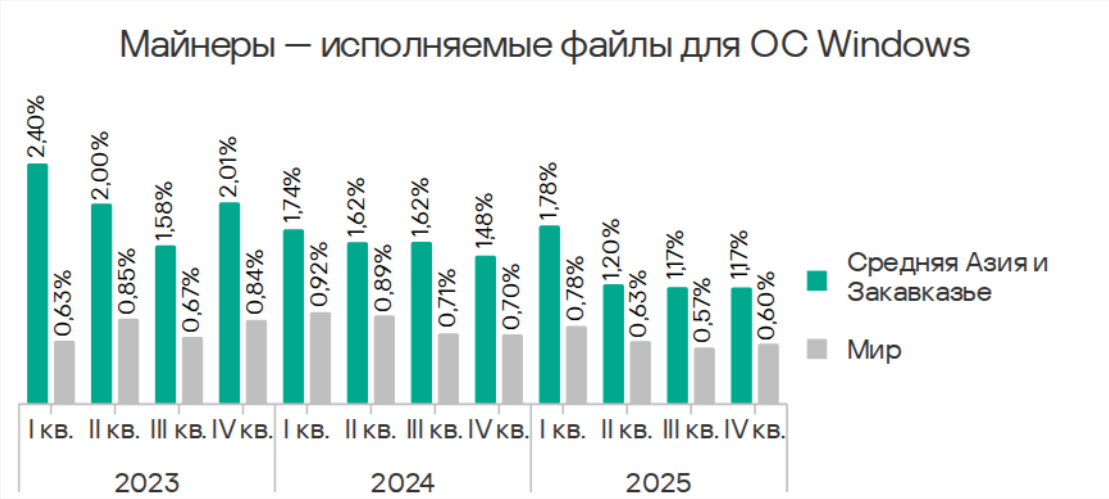
Единственный источник этой категории угроз — интернет. Таджикистан — одна из двух стран-лидеров по показателю угроз из интернета.

Майнеры — исполняемые файлы для ОС Windows

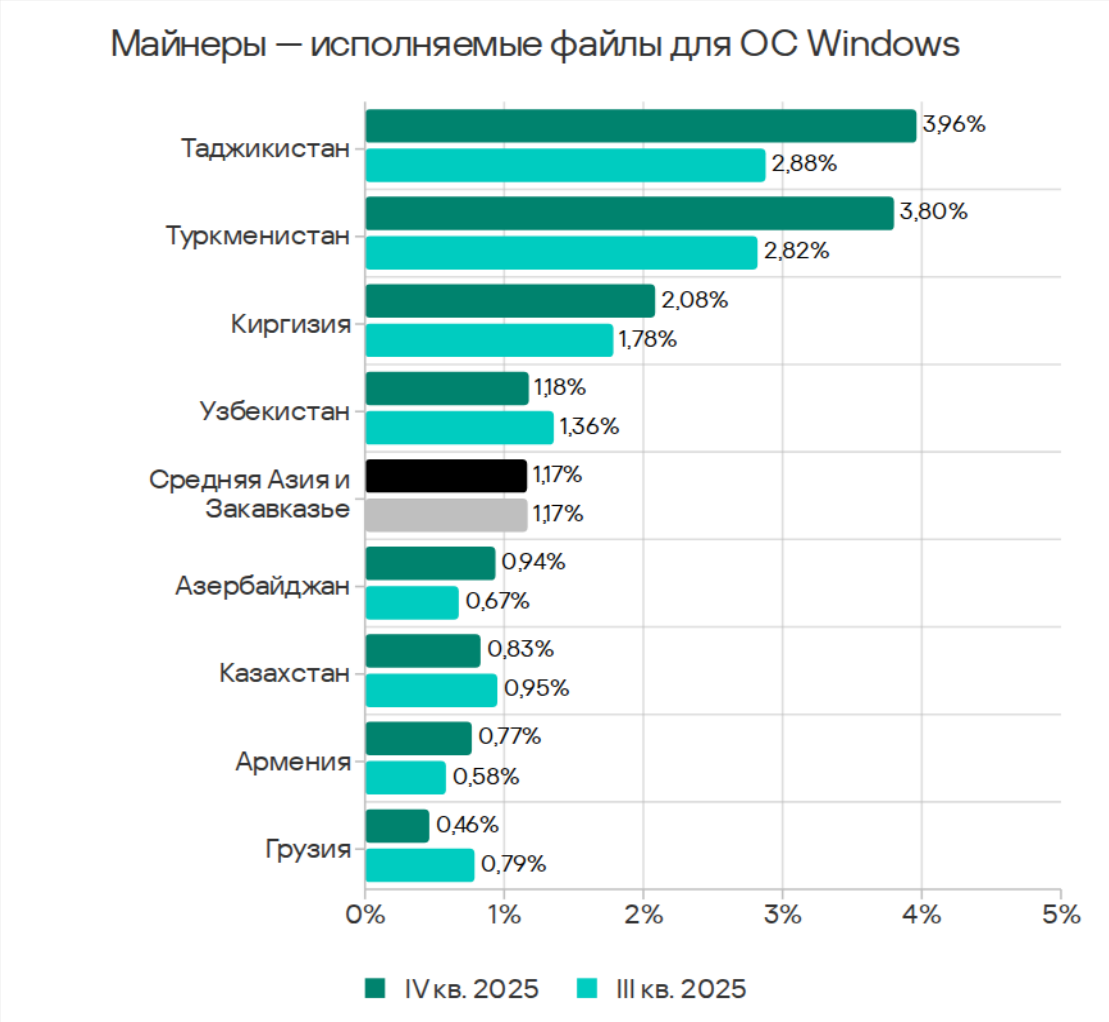
По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, Средняя Азия и Закавказье лидируют среди регионов с 1,17%. Этот показатель в 8,4 раза больше, чем в регионе Австралия и Новая Зеландия, где он – наименьший среди регионов.



Доля компьютеров АСУ, на которых блокировались майнеры — исполняемые файлы для ОС Windows, в регионе демонстрирует тенденцию к уменьшению. Показатель за квартал не изменился и по-прежнему наименьший за три года.



Среди стран региона по доле компьютеров АСУ, на которых блокируются майнеры в формате исполняемых файлов, лидируют Таджикистан с 3,96% и Туркмения с 3,80%. В обеих странах-лидерах показатели после падения в прошлом квартале вернулись почти что к прежним значениям.



Майнеры – исполняемые файлы для ОС Windows распространяются преимущественно через интернет и съемные носители.

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.

Важно отметить, что майнеры – исполняемые файлы для ОС Windows распространяются, используя функциональность червей. Поэтому динамика показателей у майнеров — исполняемых файлов и червей в Средней Азии и Закавказье во многом схожа.

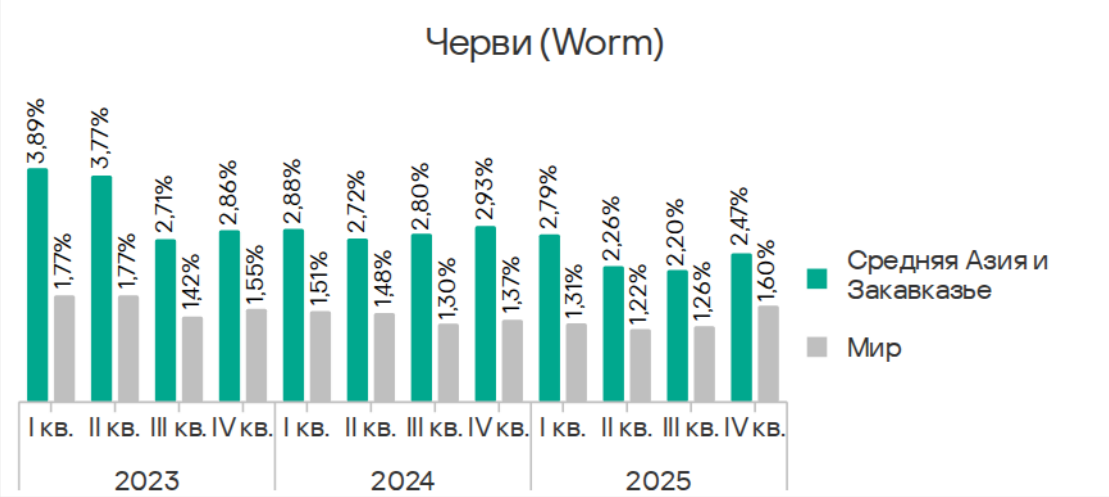
Черви

По доле компьютеров АСУ, на которых блокируются черви, Средняя Азия и Закавказье занимают третье место среди регионов.

В Средней Азии и Закавказье в рейтинге категорий угроз черви занимают четвертое место. На такой высокой позиции в региональных рейтингах черви находятся еще в трех регионах — в России, Южной Азии и Африке.

В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие очередной волны фишинговых кампаний Curriculum-vitae-catalina, о которой мы рассказывали выше.

В Средней Азии и Закавказье показатель подрос до 2,47%. Это в 7,7 раза больше, чем в Северной Европе, где показатель – наименьший среди всех регионов.

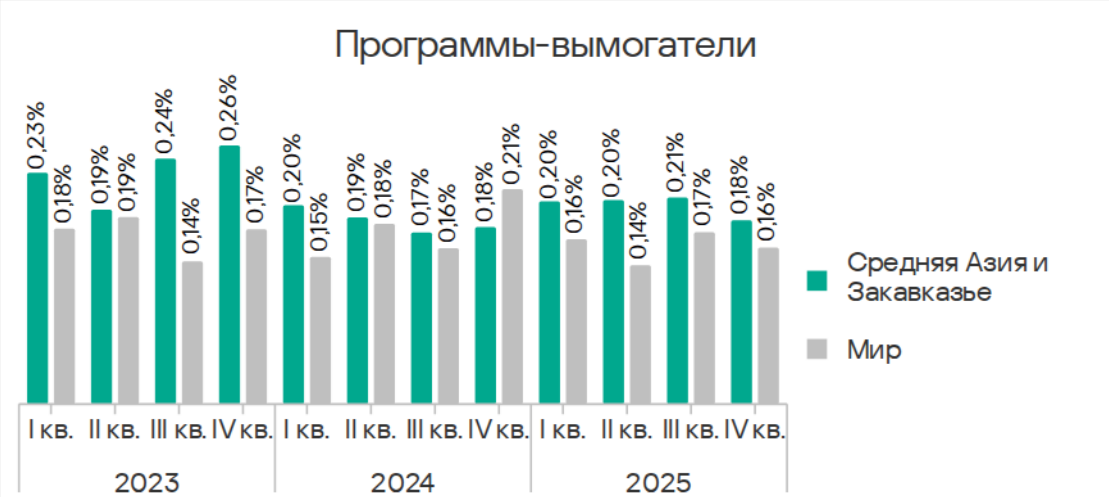


Среди стран региона по доле компьютеров АСУ, на которых были заблокированы черви, лидирует Туркмения с 11,64%. Показатель за квартал увеличился во всех странах региона, кроме Армении.

Программы-вымогатели

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье среди регионов занимают четвертое место с 0,18%. Этот показатель больше, чем в Северной Европе, которая замыкает соответствующий рейтинг, в 3,6 раза.

Показатель программ-вымогателей в Средней Азии и Закавказье довольно стабилен, за квартал он немного уменьшился.



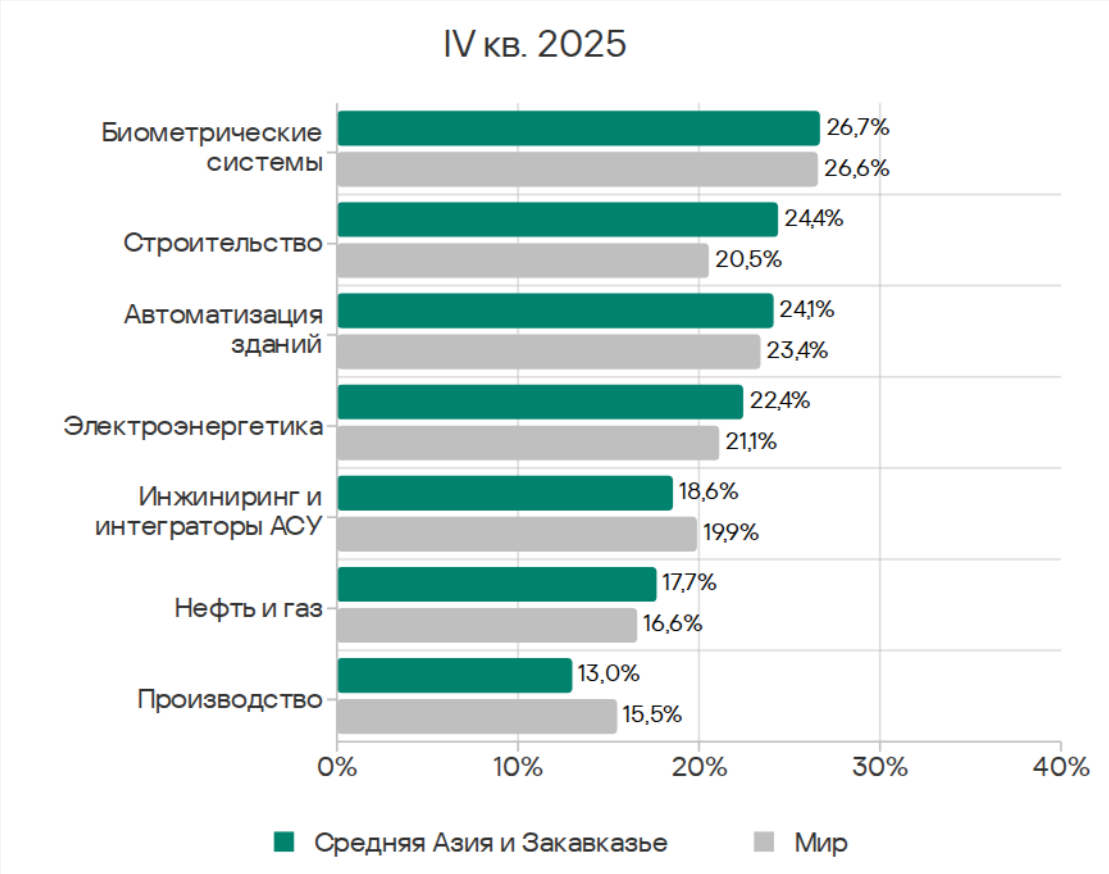
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы-вымогатели, с большим отрывом от остальных лидирует Таджикистан с 0,83%.

Отрасли

В рейтингах регионов по доле компьютеров АСУ, на которых блокируются угрозы в различных отраслях, самые высокие позиции Средней Азии и Закавказья по показателям в следующих отраслях:

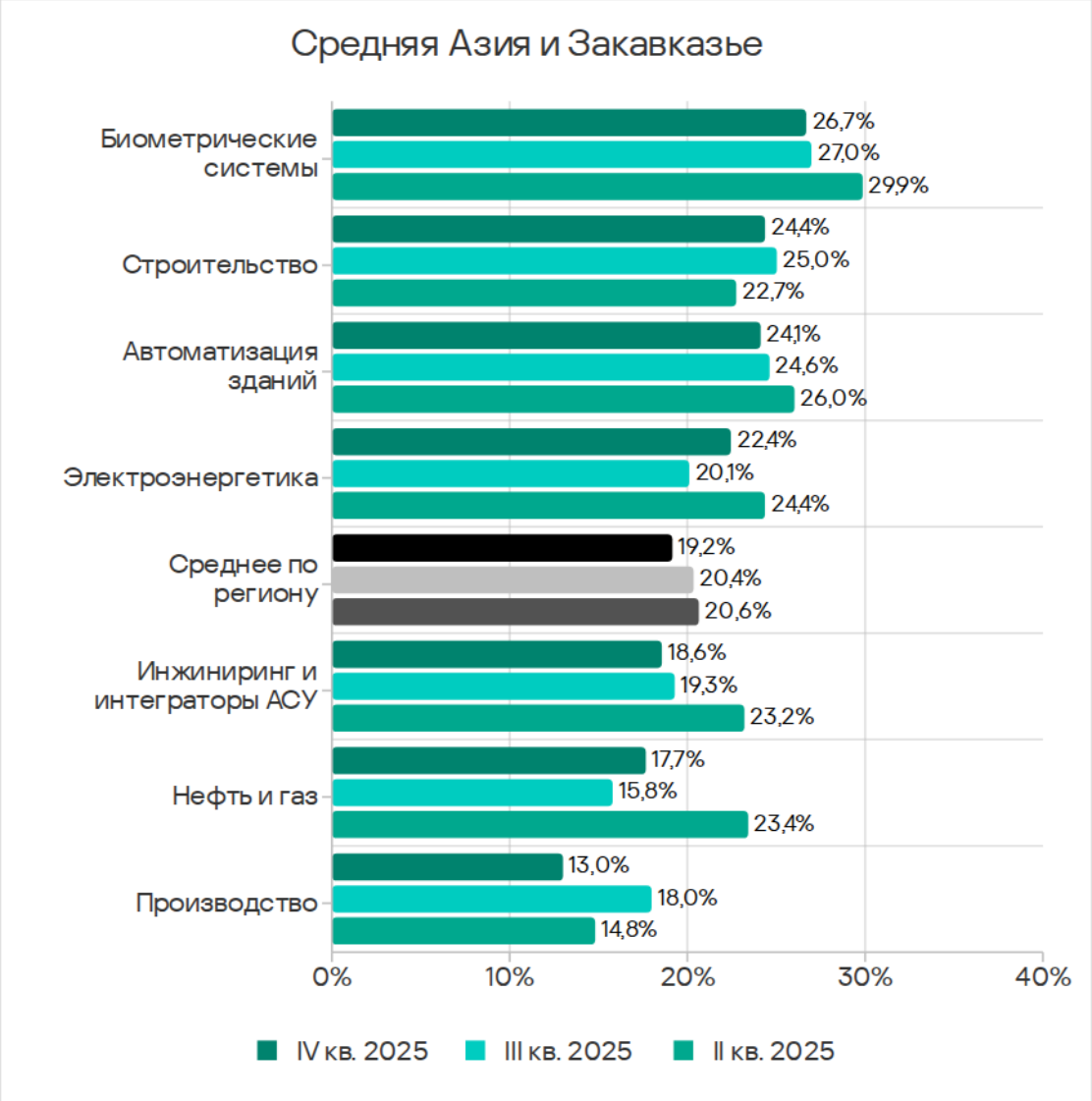
- строительство — третье место;
- биометрические системы — четвертое место;
- нефтегазовая отрасль — четвертое место.

Из отраслей региона, рассмотренных в отчете, чаще встречается с угрозами инфраструктура биометрических систем.

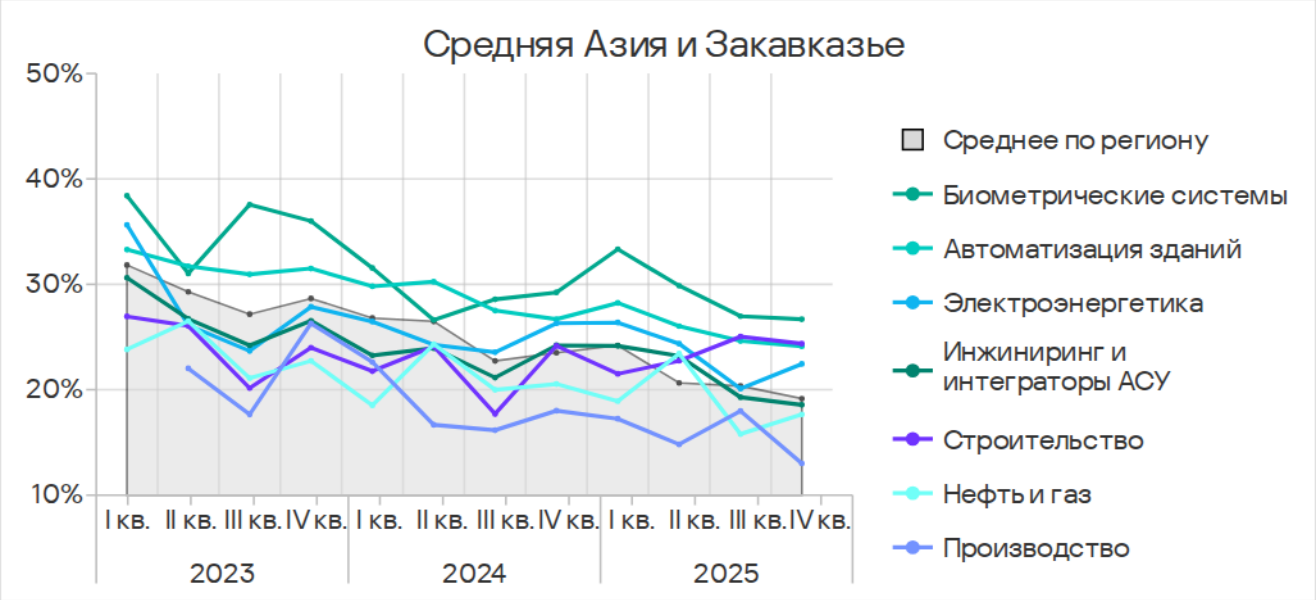


У всех рассмотренных отраслей, кроме производства и отрасли инжиниринг и интеграторы АСУ, показатель выше среднемирового. Больше всего положительная разница у строительной отрасли — в 1,2 раза.

Доля компьютеров АСУ, на которых блокируются вредоносные объекты, за квартал выросла в двух отраслях: нефтегазовой и электроэнергетической.



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, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	5,93%	7,81%	7,25%	8,23%	6,51%	10,07%	4,64%	6,43%
Почтовые клиенты	3,77%	2,17%	1,16%	2,12%	1,06%	1,32%	0,31%	1,28%
Съемные носители	—	0,54%	0,25%	0,62%	0,40%	0,93%	0,62%	0,43%
Сетевые папки	—	0,03%	0,02%	0,12%	—	—	0,31%	0,02%
Показатель отрасли в регионе	26,68%	24,12%	18,57%	22,44%	17,66%	24,37%	13,00%	

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

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	5,39%	3,84%	3,82%	5,74%	4,52%	4,37%	1,86%	3,33%
Вредоносные скрипты и фишинговые страницы	6,47%	5,50%	4,76%	7,11%	4,38%	5,96%	3,10%	4,32%
Вредоносные документы (MSOffice+PDF)	2,43%	1,41%	0,84%	1,25%	0,80%	0,53%	0,62%	0,89%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,01%	5,84%	3,40%	4,74%	2,79%	3,84%	2,48%	3,58%
Программы-вымогатели	0,81%	0,33%	0,27%	0,62%	0,40%	0,53%	0,31%	0,18%
Майнеры — исполняемые файлы для ОС Windows	1,62%	1,51%	0,96%	1,75%	0,93%	1,99%	1,24%	1,17%
Веб-майнеры, выполняемые в браузерах	0,81%	0,19%	0,17%	0,62%	0,27%	0,26%	0,62%	0,16%
Вредоносные программы для AutoCAD	—	0,04%	0,17%	0,37%	0,13%	0,53%	—	0,09%
Черви (Worm)	3,77%	3,66%	1,53%	2,99%	1,86%	2,38%	0,62%	2,47%
Вирусы (Virus)	1,08%	1,44%	0,84%	2,37%	0,80%	1,46%	1,24%	0,96%
Показатель отрасли в регионе	26,68%	24,12%	18,57%	22,44%	17,66%	24,37%	13,00%	

Особенности региона

Высокий показатель интернета как источника угроз. Как следствие, актуальны такие категории угроз как интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы.

Высокий показатель угрозы категории майнеры — исполняемые файлы для ОС Windows. 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, ее основной источник — интернет.

Во всех рассмотренных в отчете отраслях Средняя Азия и Закавказье лидируют по этому показателю среди регионов. Исключение составляет инжиниринг и интеграторы АСУ – в этой отрасли регион находится на втором месте.

Еще одна актуальная угроза — черви. По показателю червей во всех отраслях, кроме производственной отрасли, Средняя Азия и Закавказье занимают второе или третье места в соответствующих рейтингах регионов.

Высок в отраслях региона и показатель программ-вымогателей – по нему Средняя Азия и Закавказье занимают не ниже третьего места среди регионов в рейтингах отраслей:

- первое место среди регионов — в инфраструктуре биометрических систем, строительной, электроэнергетической и производственной отраслях;
- второе место — в нефтегазовой отрасли и отрасли инжиниринг и интеграторы АСУ;
- третье место — в автоматизации зданий.

Биометрические системы

Средняя Азия и Закавказье находятся на четвертом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

Среди регионов по показателям в инфраструктуре биометрических систем регион занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, майнеры обеих категорий и программы-вымогатели;
- третье место по показателям червей.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

- первое место по показателю угроз из почтовых клиентов;
- первое место по показателям угроз следующих категорий: вредоносные документы, шпионские программы, программы-вымогатели, черви, веб-майнеры;

- второе место по показателям категорий ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы;
- третье место по показателю майнеров в формате исполняемых файлов.

Строительство

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

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

- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows.

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

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях;
- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows и программы-вымогатели;
- второе место по показателю червей;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионах строительство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в интернете;
- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры в формате исполняемых файлов для ОС Windows и вредоносные программы для AutoCAD;
- второе место по показателям вирусов;
- третье место по показателю категорий вредоносные скрипты и фишинговые страницы, а также программы-вымогатели.

Автоматизация зданий

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

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

- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows;
- второе место по показателю категорий ресурсы в интернете из списка запрещенных и черви;
- третье место по показателю программ-вымогателей.

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

- второе место по угрозам в почтовых клиентах;
- третье место по угрозам из интернета, на съемных носителях и в сетевых папках;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, шпионские программы и черви;
- третье место по показателю вирусов.

Электроэнергетика

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

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

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках;
- третье место по угрозам на съемных носителях;
- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: ресурсы в интернете из списка запрещенных, майнеры обеих категорий и программы-вымогатели;
- третье место по показателю червей.

Среди отраслей в регионе электроэнергетика занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы в интернете и сетевых папках;
- третье место по угрозам в почтовых клиентах;
- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: ресурсы в интернете

из списка запрещенных, вредоносные скрипты и фишинговые страницы, вирусы;
- второе место по показателям майнеров обеих категорий, программ-вымогателей и вредоносных программ для AutoCAD;
- третье место по показателям вредоносных документов, шпионских программ и червей.

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:

- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках;
- второе место по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows и программы-вымогатели;
- третье место по показателю ресурсов в интернете из списка запрещенных и червей.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей;
- третье место по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD.

Производство

Средняя Азия и Закавказье находятся на девятом 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:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows и программы-вымогатели;

- второе место по показателю веб-майнеров.

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках;
- третье место по доле компьютеров АСУ, на которых были заблокированы веб-майнеры.

Нефть и газ

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

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

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях;
- третье место по показателю угроз из почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных и майнеры – исполняемые файлы для ОС Windows;
- второе место по показателям угроз следующих категорий: шпионские программы, программы-вымогатели и черви;
- третье место по показателям вирусов и вредоносных программ для AutoCAD.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях;
- третье место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных.

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 APT[1].

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 вовне 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.

Атакованными 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