Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Азия. Второй квартал 2025 года

19.09.2025

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. Региональный показатель в 5,5 раза превышает среднемировой и является самым высоким значением в мире.

В мировом рейтинге категорий угроз по доле компьютеров АСУ, на которых угроза была заблокирована, вредоносные программы для AutoCAD находятся на предпоследнем месте, а в региональном рейтинге – на шестом, с показателем, который в 7,9 раза превышает среднемировой и является самым высоким в мире.

Недостатки сегментации сети предприятий в регионе

Юго-Восточная Азия занимает второе место среди регионов по доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, с 0,11%. Это значение выше среднемирового в 2,1 раза.

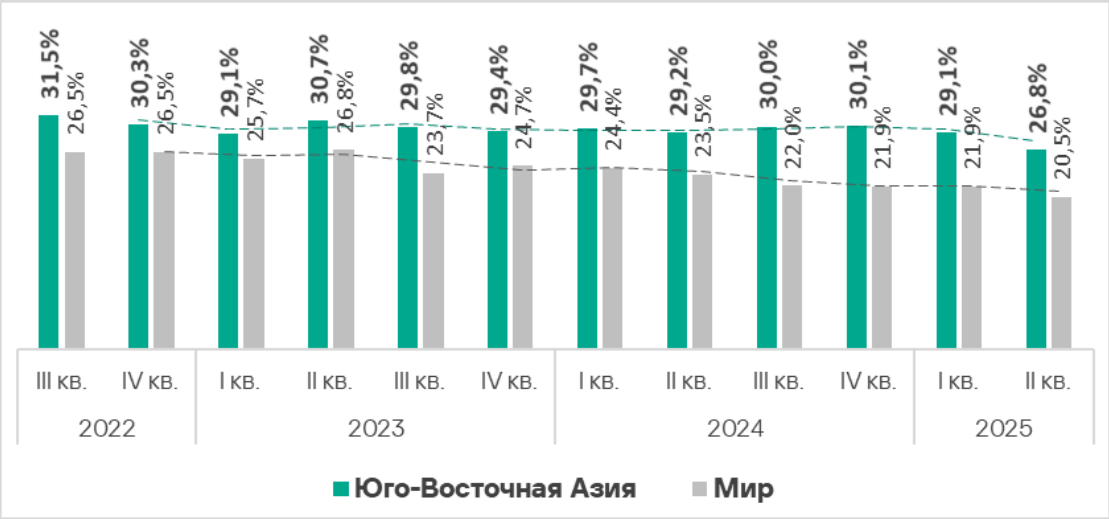
Преимущественно это результат ситуации во Вьетнаме, который с большим отрывом лидирует среди стран региона и по сетевым папкам, и по вирусам, и по вредоносному ПО для AutoCAD.

Статистика по всем угрозам

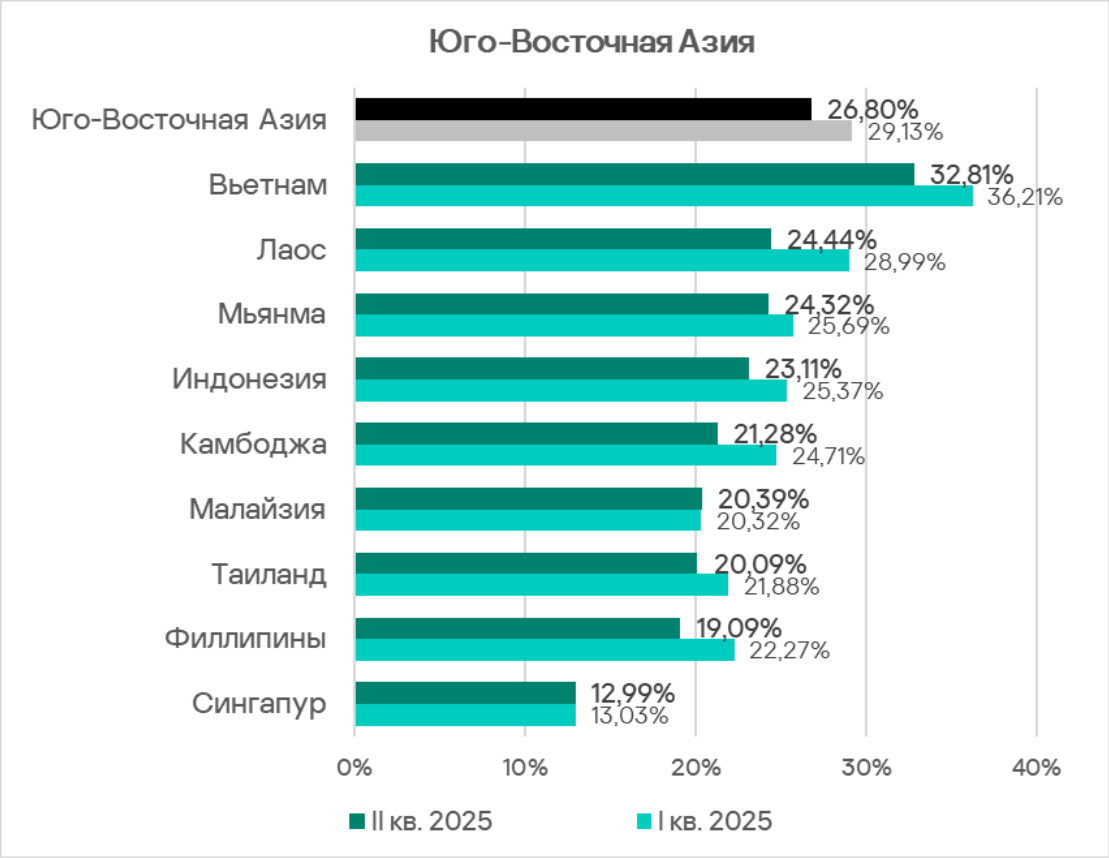
Юго-Восточная Азия занимает второе место в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с показателем 26,8%. Это значение больше среднемирового в 1,3 раза и в 2,4

раза оно больше минимального значения среди регионов, зафиксированного в Северной Европе.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, снизилась в Юго-Восточной Азии на заметные 2,3 п. п. Показатель региона уменьшается второй квартал подряд.



В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 12,99% в Сингапуре до 32,81% во Вьетнаме. Показатели остальных стран — в диапазоне от 19% до 25%.



Источники угроз

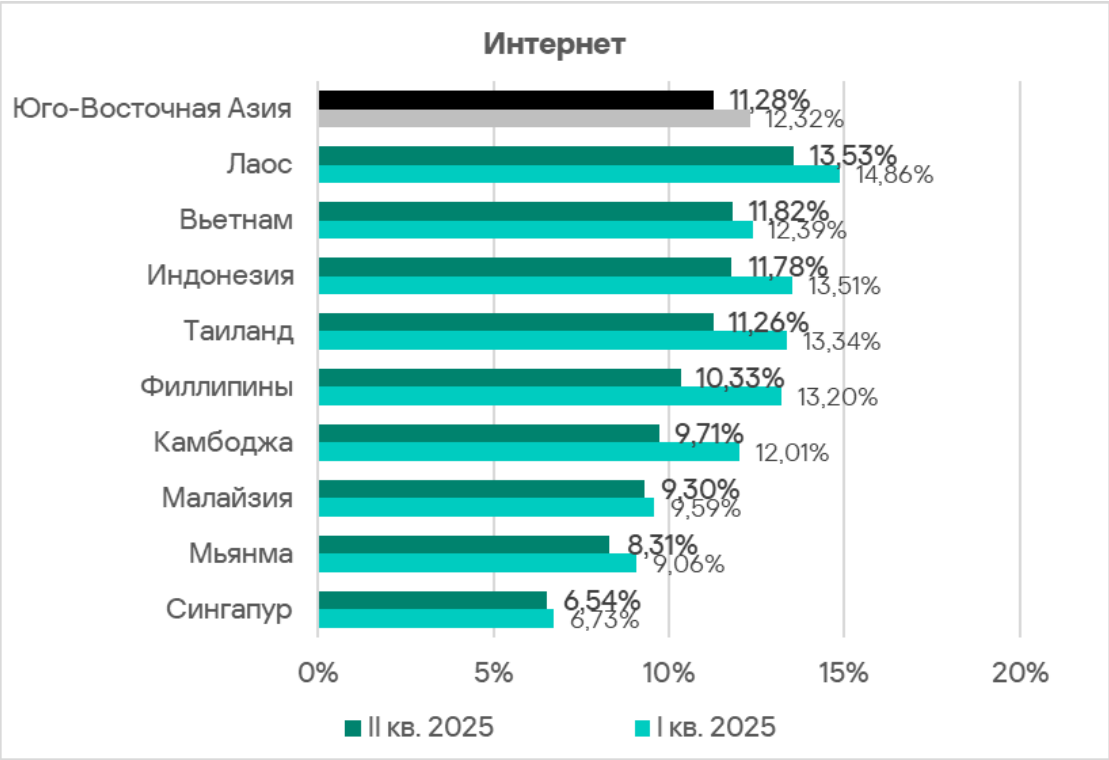
Доля компьютеров АСУ, на которых угрозы были заблокированы из разных источников, по всем источникам в регионе выше среднемировых показателей. По доле компьютеров АСУ, где источником угрозы стал интернет, — в 1,2 раза, почтовые клиенты — в 1,5 раза, съемные носители — в 1,4 раза, сетевые папки — в 2,2 раза.

Из всех источников угроз показатель растет только у почтовых клиентов.

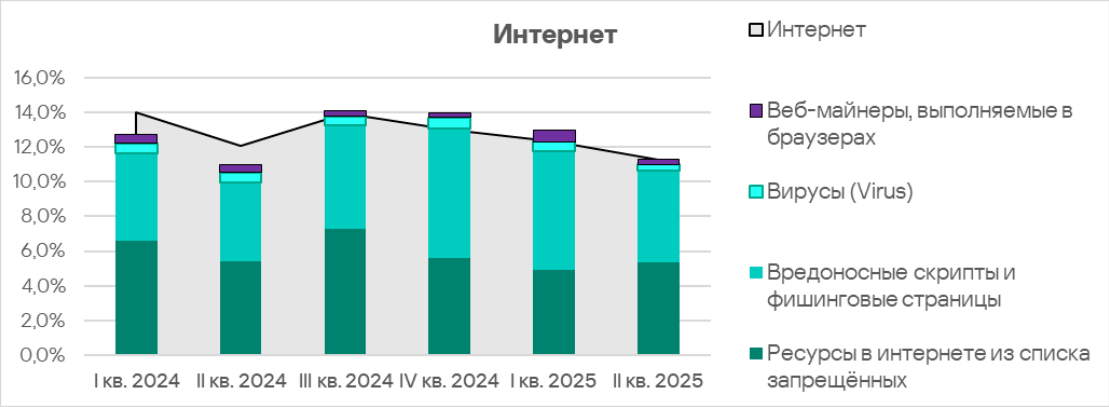
Интернет

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 Восточной Азии — в 1,8 раза.

Показатели стран региона варьируют от 6,54% в Сингапуре до 13,53% в Лаосе.



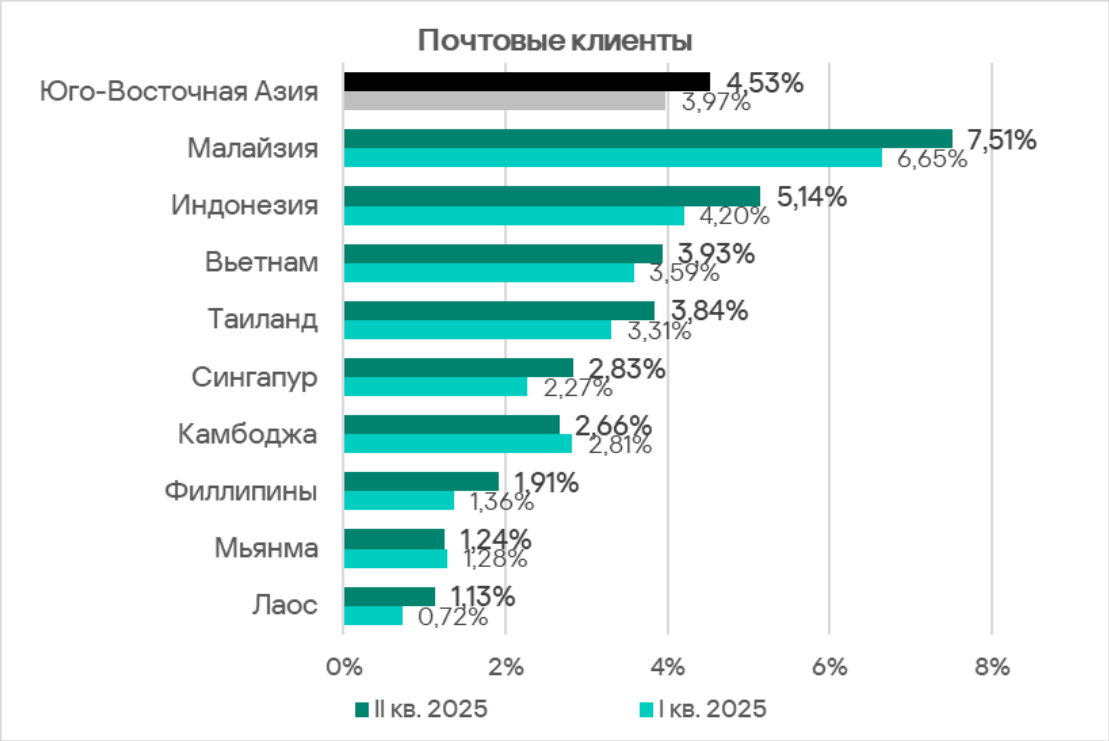
Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе, — это ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вирусы и веб-майнеры.



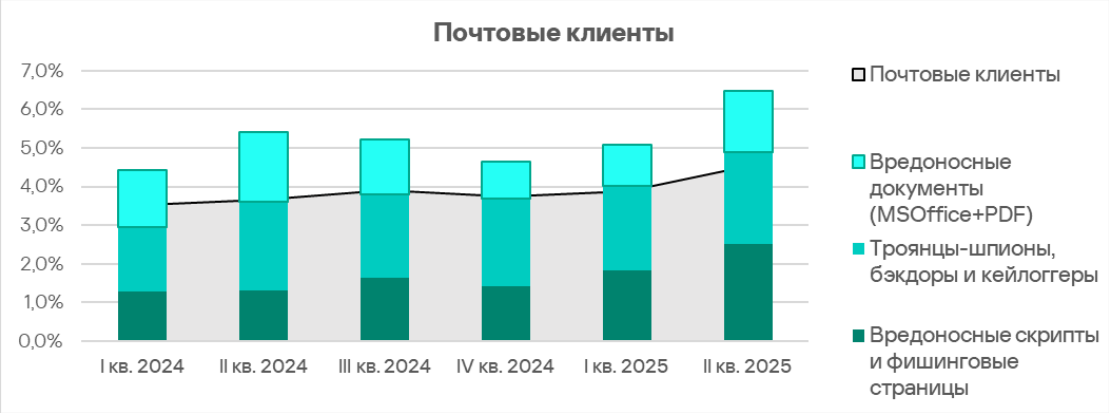
Почтовые клиенты

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

Среди стран региона по этому показателю с заметным отрывом лидирует Малайзия с 7,51%. Минимальная доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, в Лаосе — 1,13%.



Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ, — это вредоносные документы, вредоносные скрипты и фишинговые страницы, шпионское ПО. В рейтинге регионов по шпионским программам Юго-Восточная Азия занимает третье место.

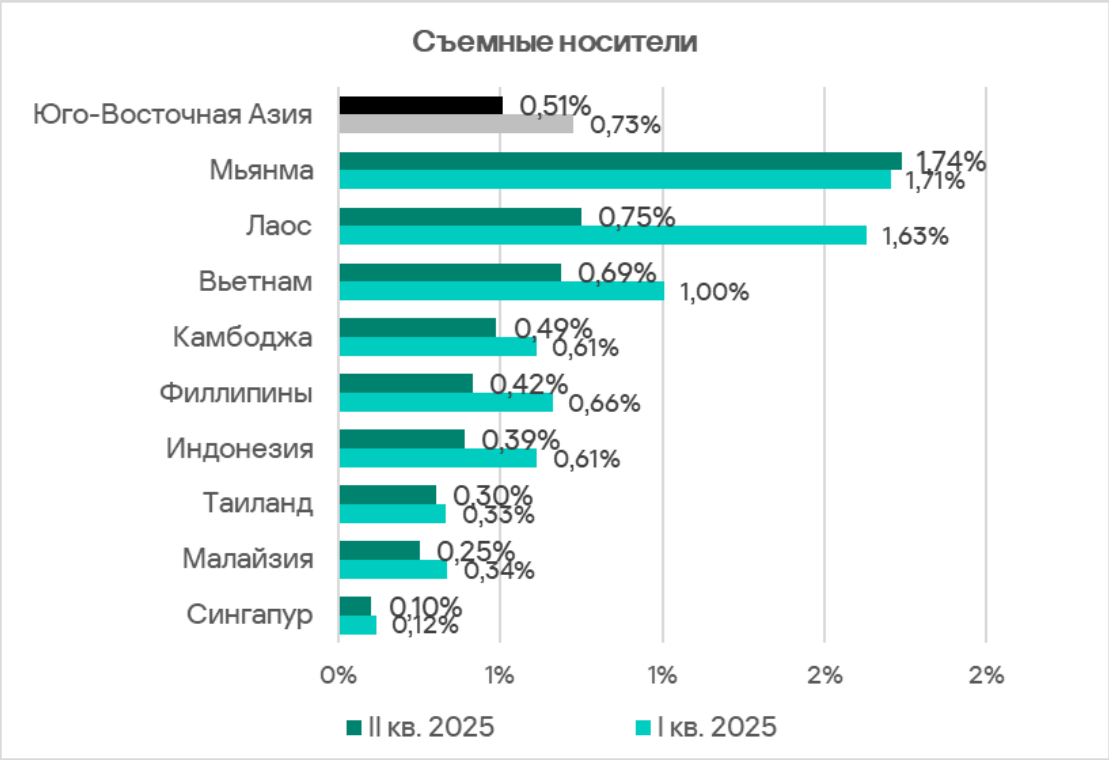


Съемные носители

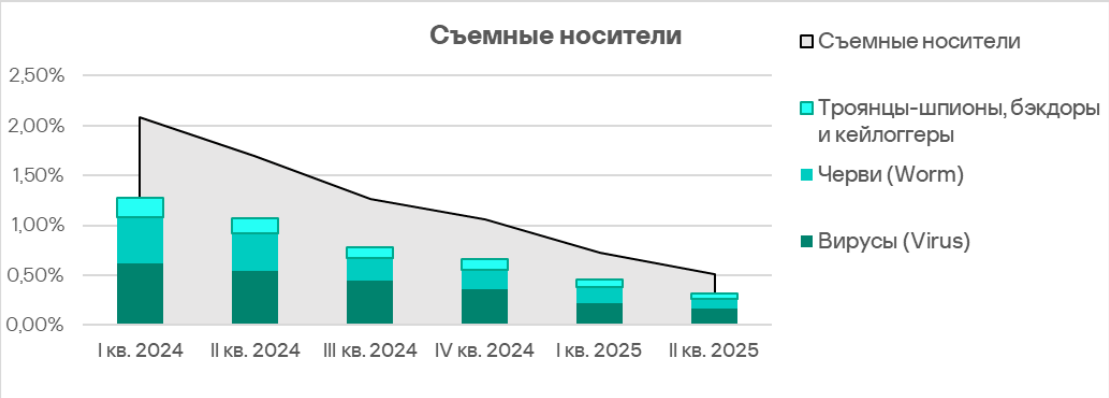
На первых шести позициях в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, — Африка и регионы Азии. Юго-Восточная Азия занимает шестое место с 0,51%.

Среди азиатских регионов у Юго-Восточной Азии показатель наименьший, однако он превышает значения следующего в рейтинге региона — Восточной Европы — в 2,2 раза. В Северной Америке (Канаде), которая занимает последнее место в рейтинге, показатель меньше в 18,9 раз.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует Мьянма с 1,74%. Отметим, что эта страна была предпоследней в рейтинге по почтовым клиентам. Показатели остальных стран варьируют от 0,10% в Сингапуре до 0,75% в Лаосе.



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



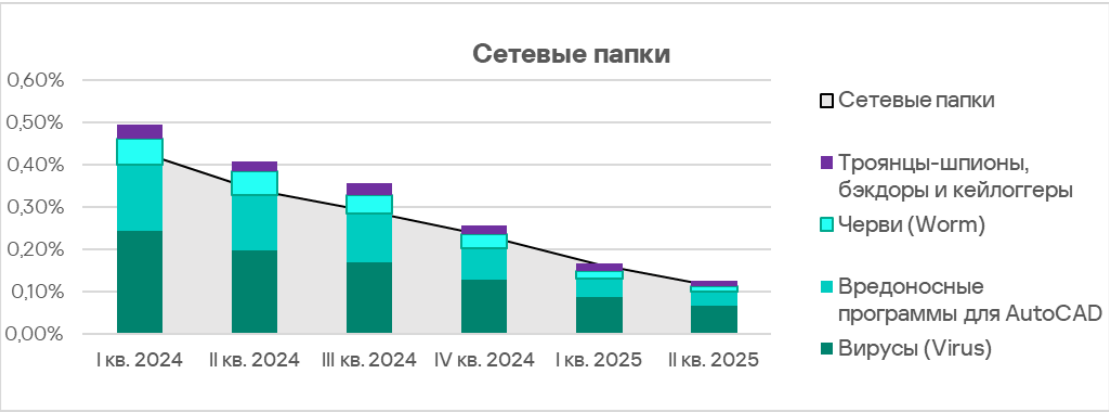
Сетевые папки

Юго-Восточная Азия занимает второе место среди регионов по доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, с 0,11%, уступая только Восточной Азии.

Показатели двух регионов-лидеров заметно превышают остальные. У Юго-Восточной Азии показатель превышает значение следующего в рейтинге региона — Южной Азии — в 1,7 раза. С Северной Европой, которая занимает последнее место в рейтинге, показатели отличаются в 11,7 раза.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, с заметным отрывом лидирует Вьетнам с 0,18%.

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



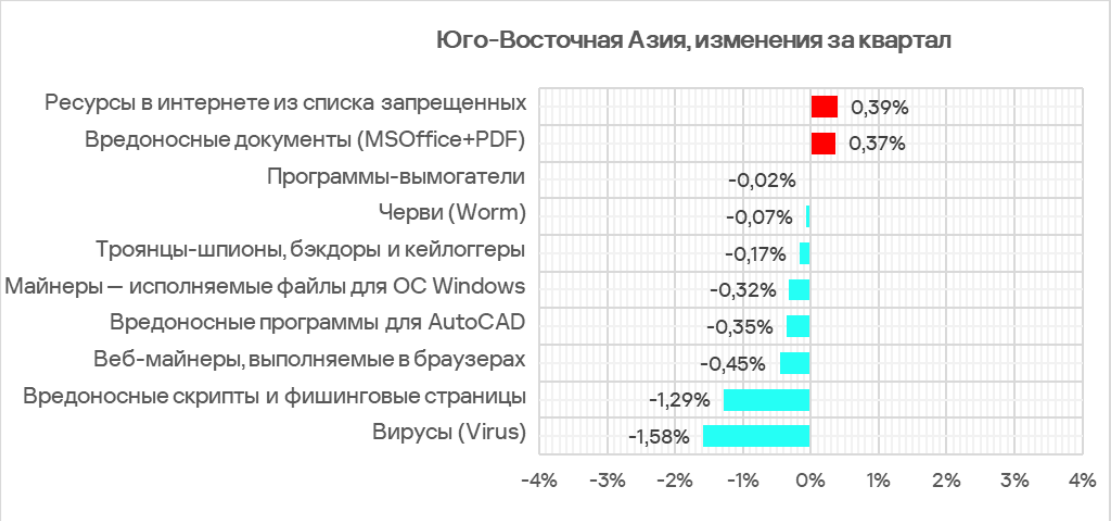
Категории угроз

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

Особенно значительно региональные показатели превышают среднемировые у категорий угроз:

- шпионские программы — в 1,5 раза;
- вирусы — в 5,5 раза;
- вредоносное ПО для AutoCAD — в 7,9 раза.

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

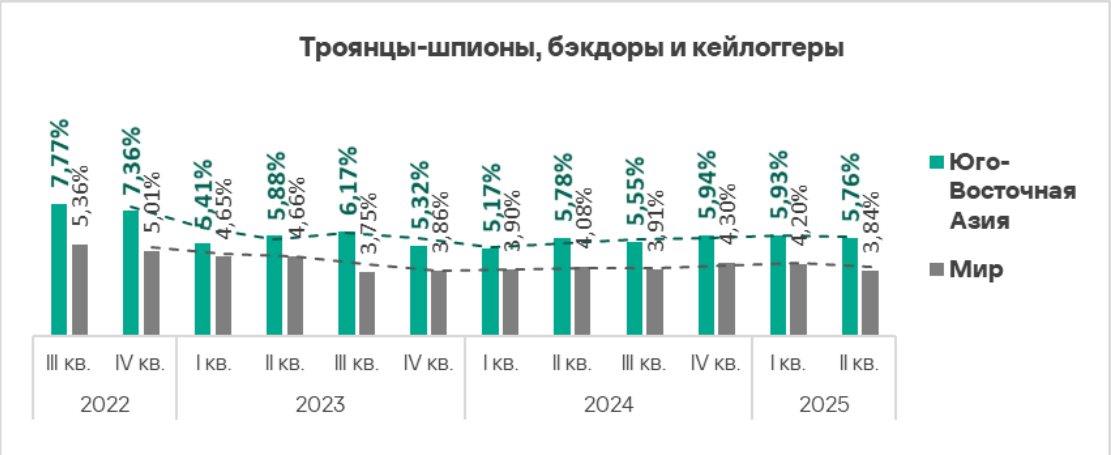


Из всех категорий угроз за квартал показатель вырос только у двух: ресурсы в интернете из списка запрещенных и вредоносные документы.

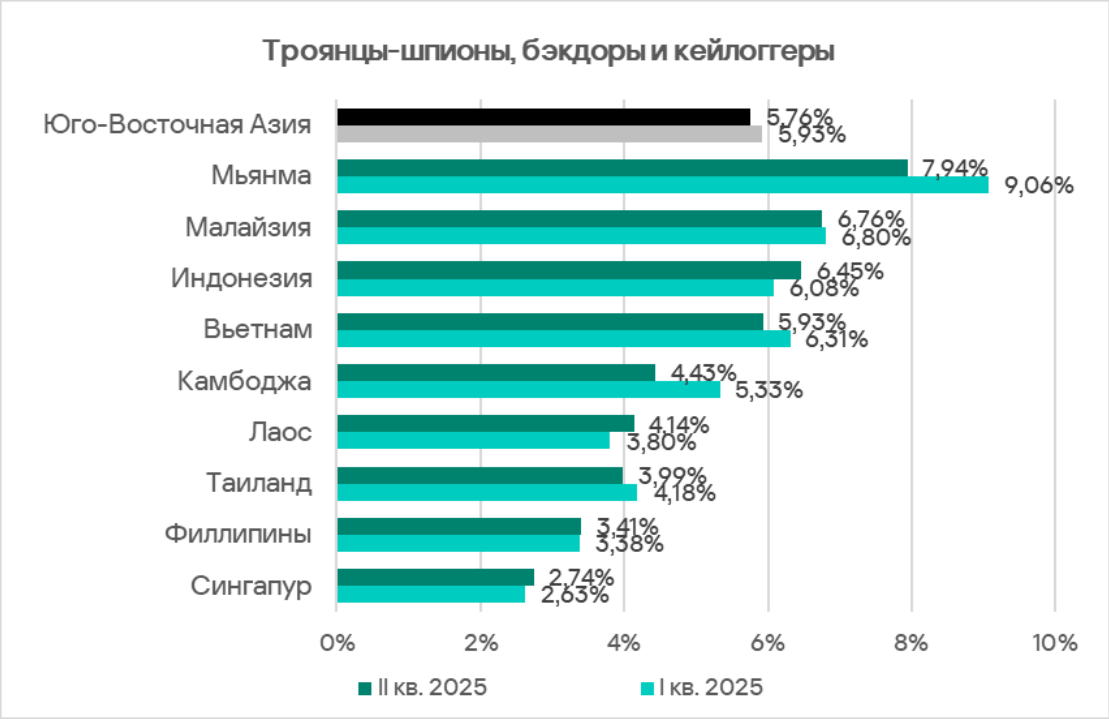
Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, в соответствующем рейтинге регионов Юго-Восточная Азия находится на третьем месте с 5,76%.

Этот показатель в регионе довольно стабилен и с первого квартала 2023 года колеблется в диапазоне от 5,17% до 6,17%.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы программы-шпионы, лидирует Мьянма с 7,94%. В Сингапуре показатель наименьший — 2,74%.



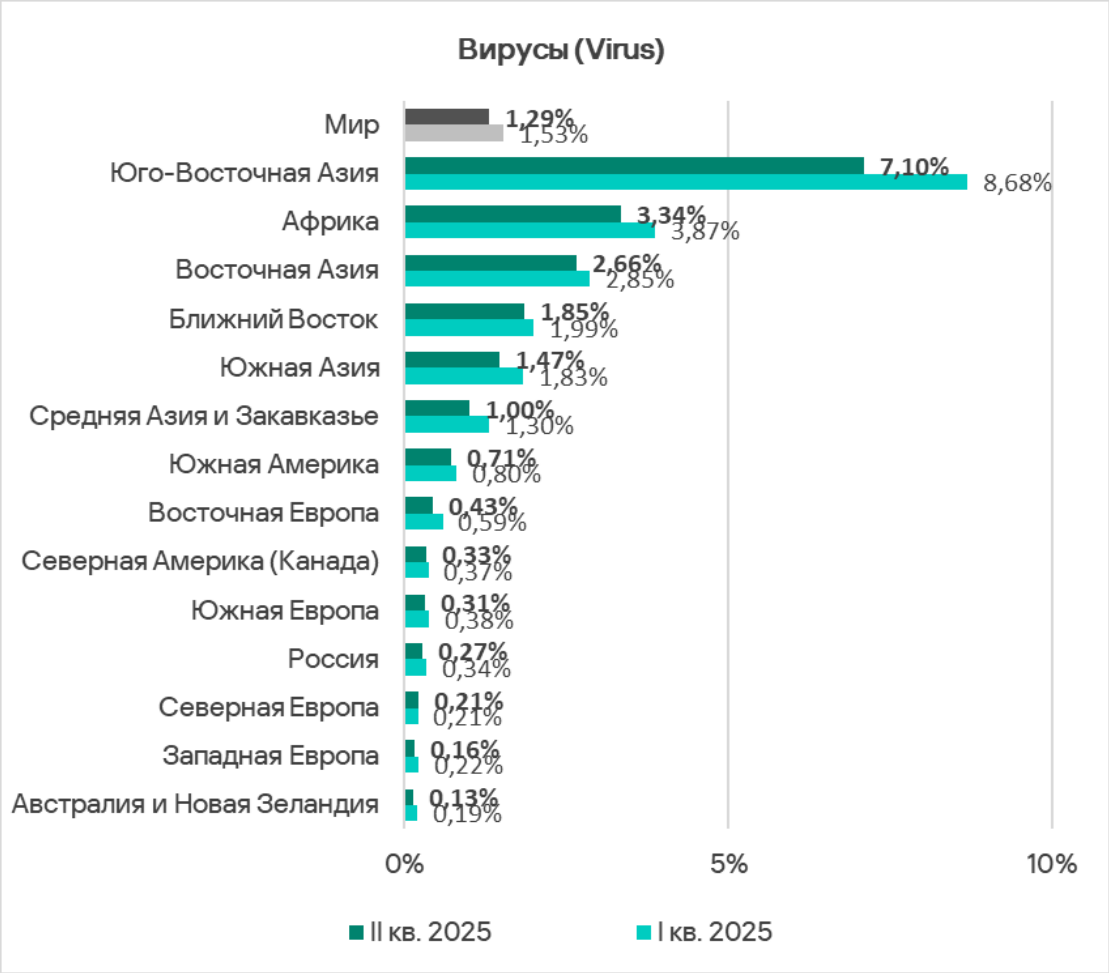
Шпионские программы в регионе блокируются во всех источниках угроз, но основной канал их распространения — электронная почта. Малайзия, Индонезия и Вьетнам, которые следуют за Мьянмой в рейтинге по шпионским программам, оказались в тройке стран региона, лидирующих и по угрозам из почтовых клиентов. А вот в Мьянме, судя по всему, ситуация иная: страна лидирует 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.

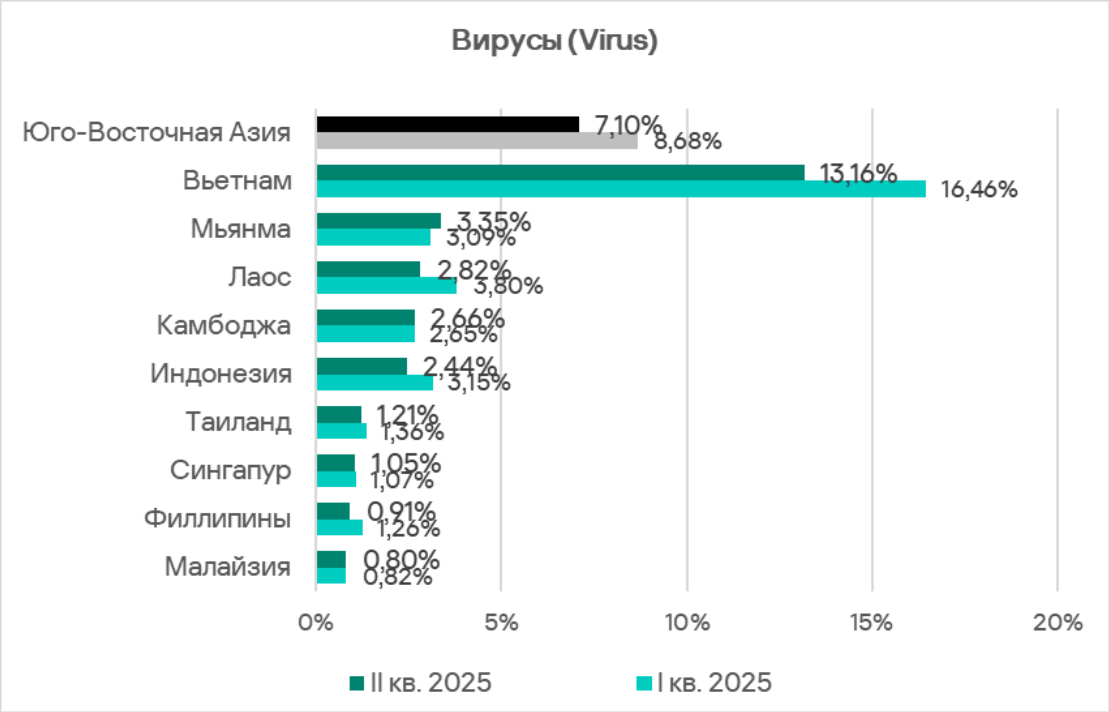
Вирусы

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



В Юго-Восточной Азии показатель больше, чем в Африке (следующий в рейтинге регион), в 2,1 раза, а по сравнению с регионом Австралия и Новая Зеландия, который замыкает рейтинг, — в 55 раз.

Столь яркое лидерство Юго-Восточной Азии обеспечивает Вьетнам. В этой стране показатель выше, чем у следующей в рейтинге Мьянмы, в 3,9 раза.



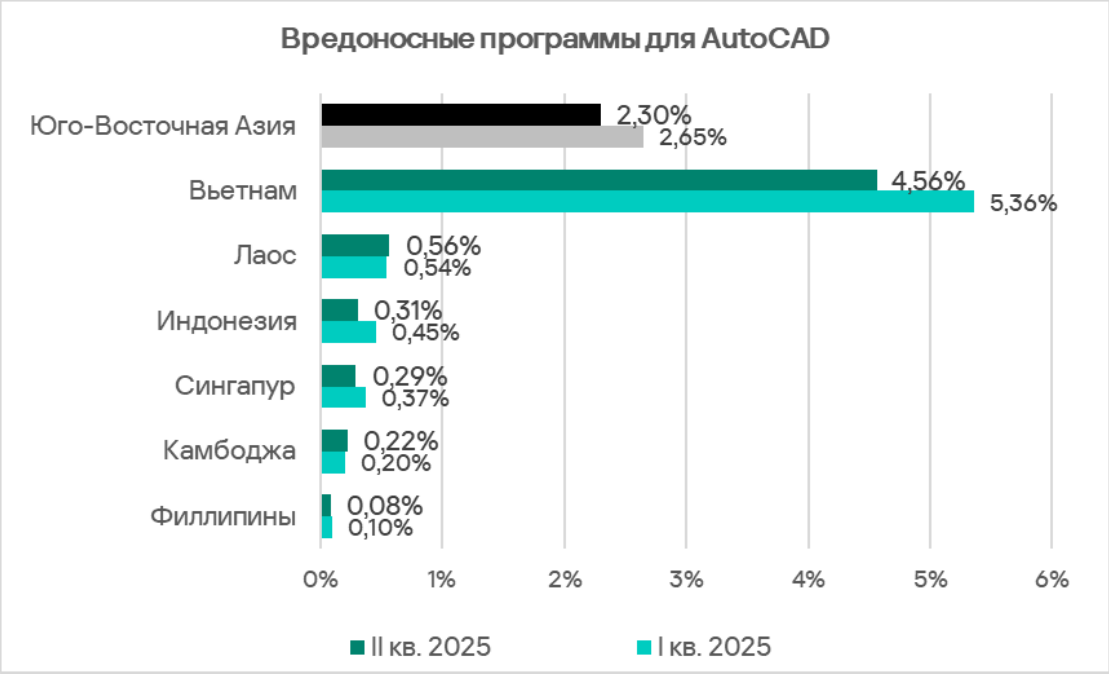
Вирусы в регионе блокируются во всех источниках угроз. Отметим, что Вьетнам на третьей позиции по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, почтовых клиентов и съемных носителей. И первый в рейтинге по сетевым папкам.

Вредоносное ПО для AutoCAD

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

В Юго-Восточной Азии показатель больше, чем в следующем в рейтинге регионе — в Восточной Азии, в 2,1 раза. В свою очередь Восточная Азия тоже заметно отличается от других регионов: ее показатель больше, чем значение следующего в рейтинге региона — Африки, в 2,5 раза.

Лидерство региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, также обеспечивает Вьетнам.

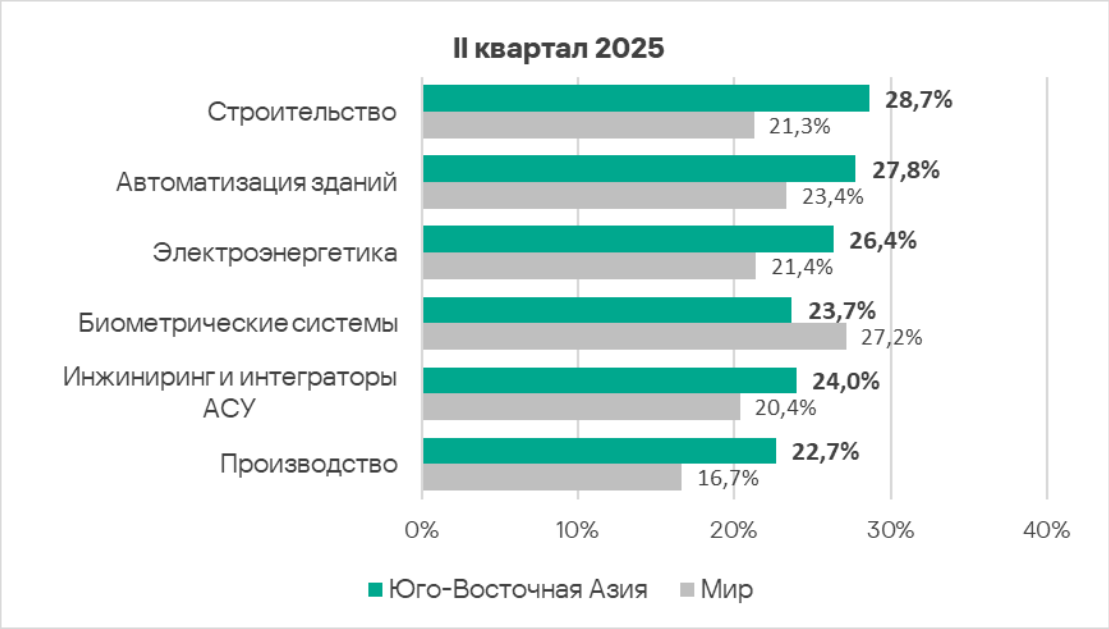


Отрасли

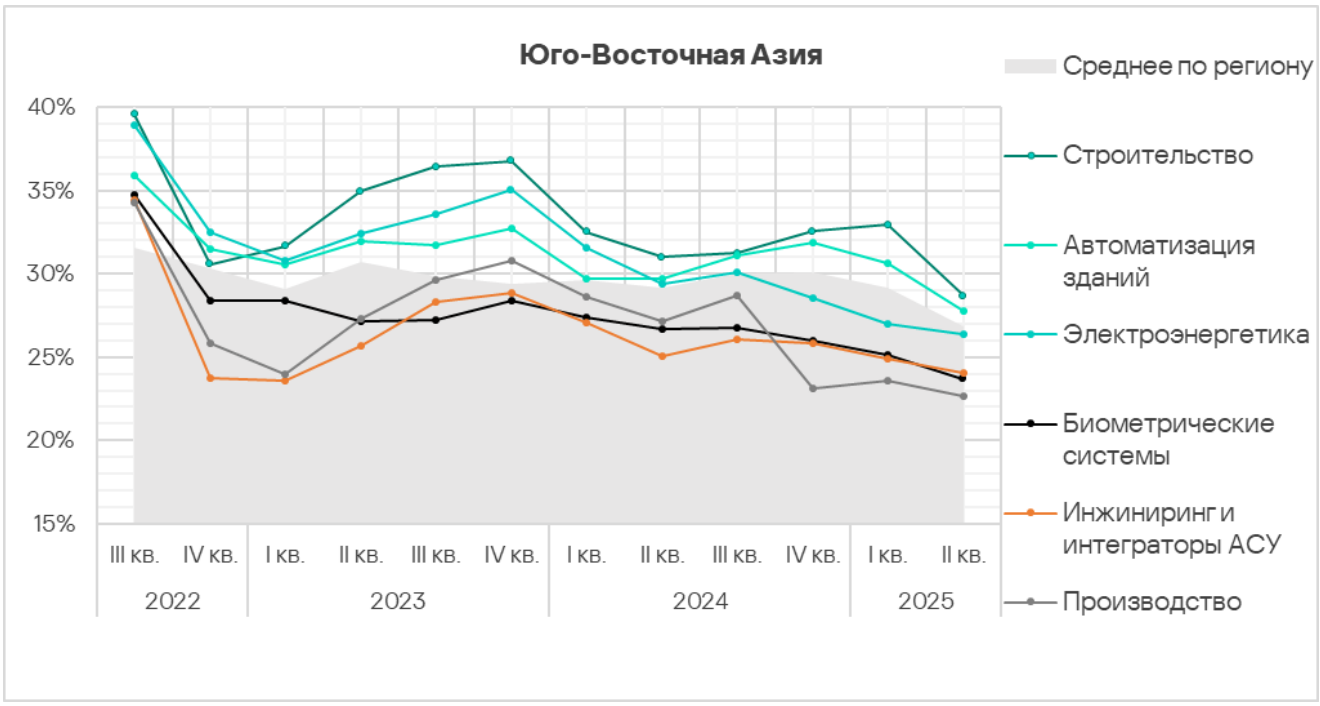
В Юго-Восточной Азии наиболее часто встречающейся с угрозами отраслью среди рассмотренных в отчете по-прежнему остается строительство.

Показатели всех отраслей превышают аналогичные среднемировые. Больше всего разница у отрасли производство — в 1,4 раза.

По доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий, регион лидирует.



Показатели всех отраслей за квартал уменьшились. 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 мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение для источника или типа угроз среди всех регионов и индустрий. В Юго-Восточной Азии максимальное значение наблюдается в категории вредоносных программ для AutoCAD, заблокированных на компьютерах в сфере строительства.

На тепловых картах хорошо видны «горячие точки» отраслей — позиции источников и категорий вредоносного ПО, показатель по которым выше ожидаемого в соответствии с местом отрасли и местом угрозы или источника угрозы в соответствующих региональных рейтингах.

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	9,90%	11,46%	13,25%	12,19%	10,12%	14,17%	10,41%	11,28%
Почтовые клиенты	8,49%	6,43%	2,56%	4,04%	3,47%	3,46%	5,18%	4,53%
Съемные носители	0,53%	0,48%	0,60%	0,47%	0,42%	0,38%	0,47%	0,51%
Сетевые папки	0,08%	0,09%	0,00%	0,04%	0,00%	0,13%	0,00%	0,11%
Показатель отрасли в регионе	23,70%	27,79%	26,35%	24,01%	17,48%	28,67%	22,69%	

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

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	5,26%	5,47%	7,33%	6,47%	5,13%	7,07%	5,70%	5,62%
Вредоносные скрипты и фишинговые страницы	9,90%	9,63%	7,72%	7,86%	5,96%	9,13%	7,97%	8,05%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,29%	7,40%	4,98%	5,22%	4,02%	5,04%	6,40%	5,76%
Черви (Worm)	1,92%	1,35%	1,90%	1,27%	0,55%	1,12%	1,69%	1,49%
Майнеры - исполняемые файлы для ОС Windows	0,78%	0,47%	0,70%	0,50%	0,55%	0,74%	0,41%	0,42%
Вредоносные документы (MSOffice + PDF)	4,67%	3,24%	1,96%	1,94%	0,97%	2,75%	2,68%	2,35%
Вирусы (Virus)	2,68%	6,72%	5,82%	3,55%	2,36%	7,53%	3,90%	7,10%
Программы-вымогатели	0,40%	0,14%	0,08%	0,06%	0,14%	0,13%	0,17%	0,10%
Веб-майнеры, выполняемые в браузерах	0,71%	0,41%	0,76%	0,51%	0,55%	0,79%	0,47%	0,35%
Вредоносные программы для AutoCAD	0,33%	0,88%	1,85%	1,17%	1,25%	4,94%	0,70%	2,30%
Показатель отрасли в регионе	23,70%	27,79%	26,35%	24,01%	17,48%	28,67%	22,69%	

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

«Горячие точки» отраслей

Строительство

- Лидер среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и в сетевых папках.
- Лидер среди отраслей в регионе по показателям следующих категорий: вредоносные программы для AutoCAD, веб-майнеры.
- Первое место среди всех индустрий во всех регионах по доле заблокированных вирусов и ресурсов в интернете из списка запрещенных.
- Второе место среди отраслей в регионе по показателям следующих категорий: ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows.
- Третье место по показателям следующих категорий: вредоносные документы, вредоносные скрипты и фишинговые страницы в регионе.

Автоматизация зданий

- Второе место среди отраслей в регионе по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов и в сетевых папках.
- Второе место в регионе среди отраслей по показателям категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы.
- Третье место в регионе среди отраслей по показателю вирусов и программ-вымогателей.

Электроэнергетика

- Лидер среди отраслей региона по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей. На втором месте по показателям угроз из интернета.
- Лидер среди отраслей региона по показателям ресурсов в интернете из списка запрещенных.
- Второе место среди отраслей региона по показателям категорий угроз: черви и веб-майнеры.
- Третье место в регионе среди отраслей по показателям категорий угроз: вредоносные программы для AutoCAD и майнеры – исполняемые файлы для ОС Windows.

Инжиниринг и интеграторы АСУ

- Третье место среди отраслей в регионе по показателю угроз из интернета.
- Третье место среди отраслей региона по показателю категории угроз: ресурсы в интернете из списка запрещенных.
- Четвертое место в регионе среди отраслей по показателю вредоносных программ для AutoCAD и майнеров обеих категорий.

Биометрические системы

- Лидер среди отраслей в регионе по доле компьютеров АСУ, на которых блокировались угрозы в почтовых клиентах. На втором месте по показателю съемных носителей, на третьем — по показателю угроз в сетевых папках.
- Лидер в регионе среди отраслей по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, программы-вымогатели, черви, майнеры в формате исполняемых файлов.
- Третье место среди отраслей региона по показателю червей.

Производство

- Третье место среди отраслей в регионе по показателю угроз из почтовых клиентов.
- Второе место в регионе среди отраслей по показателю программ-вымогателей.
- Третье место в регионе среди отраслей по доле компьютеров АСУ, на которых были заблокированы шпионские программы и черви.

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. Во втором квартале 2025 года соответствующий показатель в регионе был в 1,6 раза выше, чем в среднем по миру.

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

По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы, Средняя Азия и Закавказье лидирует среди всех регионов, по показателю червей она находится на втором месте после Африки. Показатели обеих категорий выше среднемировых в 1,9 раза.

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 незащищенной части инфраструктуры предприятия, которая является источником самораспространяющегося ПО;
- об общей низкой культуре информационной безопасности.

Отсутствие контроля за установкой пользователями ПО на компьютеры АСУ

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

Сравнение майнеров — исполняемых файлов в Средней Азии и Закавказье по индустриям показывает, что чаще такое вредоносное ПО встречается на компьютерах, используемых в системах биометрии (наибольшая доля среди всех регионов и индустрий), а также в сферах электроэнергетики, производства и строительства.

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 и токенов, имперсонацию пользователей, эксплуатацию локальных и сетевых уязвимостей. Поэтому их присутствие в технологической сети нельзя считать незначительной угрозой.

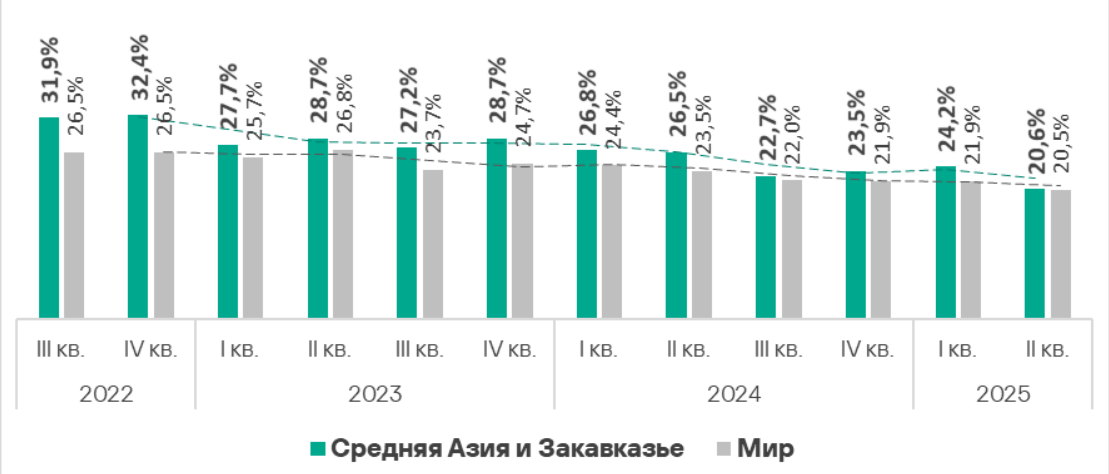
Стабильно высокий уровень показателя программ-вымогателей

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье занимает третье место с показателем, который в 1,4 раза выше среднемирового. Эта категория угроз в регионе распространяется как в интернете, так и на съемных носителях.

Статистика по всем угрозам

Средняя Азия и Закавказье занимает четвертое место в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с 20,6%.

Во втором квартале 2025 года региональный показатель уменьшился на 3,6 п. п. Тем не менее, по сравнению с минимальной долей атакованных компьютеров АСУ среди всех регионов (11,2% в Северной Европе), показатель Средней Азии и Закавказья во втором квартале 2025 года больше в 1,8 раза.



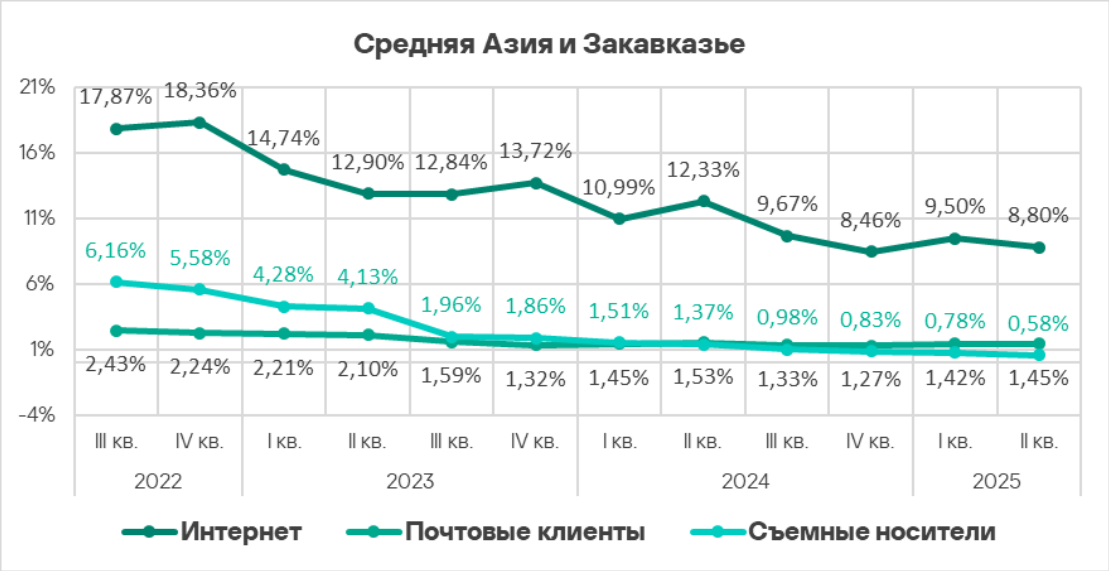
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 15,96% в Армении до 38,50% в Туркмении. Высокий показатель также у Таджикистана, который занимает

второе место (33,74%). Показатели остальных стран — в диапазоне от 16% до 27%.

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 1,6 раза.

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



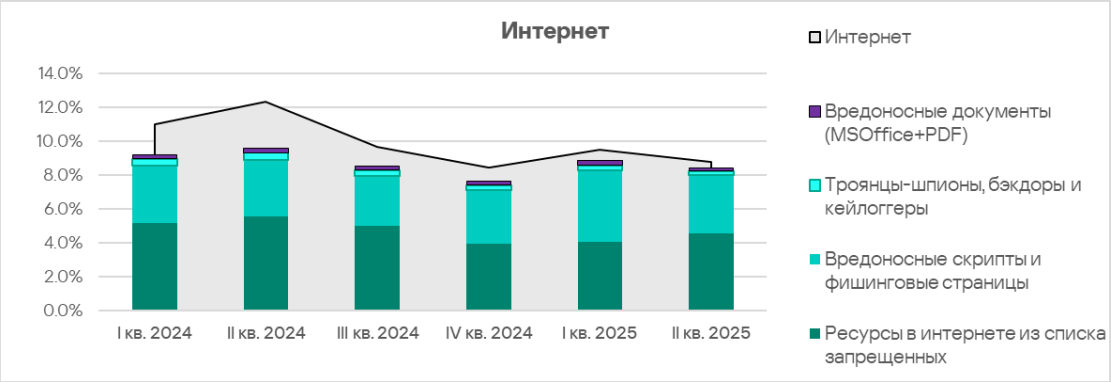
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Средняя Азия и Закавказье занимает восьмое место в рейтинге регионов с показателем 8,80%, который превышает минимальный — у Восточной Азии (6,35%) — в 1,4 раза.

Показатели стран региона варьируют от 3,88% в Туркмении до 15,48% в Таджикистане.

Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе, — это ресурсы в интернете из списка запрещенных, вредоносные

скрипты и фишинговые страницы, шпионские программы и вредоносные документы.

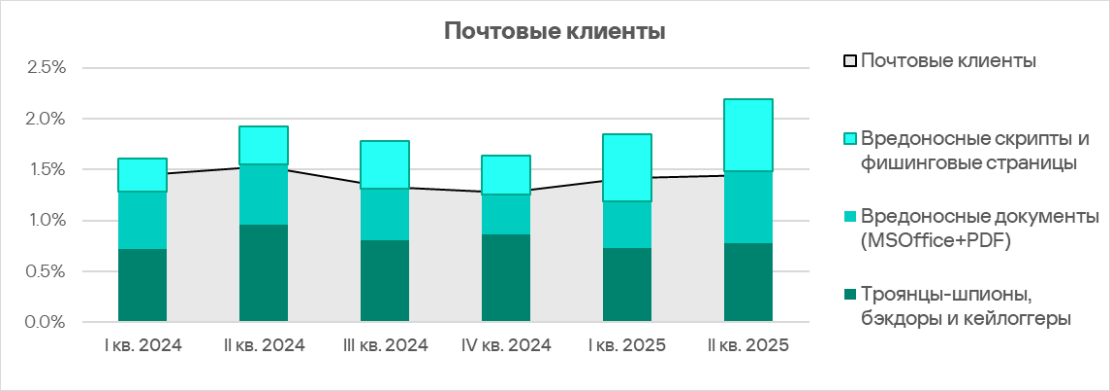


Почтовые клиенты

По сравнению с другими регионами доля компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, в Средней Азии и Закавказье относительно невысокая — с 1,45% регион занимает 12-е место в соответствующем рейтинге. Тем не менее, этот показатель в 1,8 раза выше, чем в России, которая этот рейтинг замыкает.

Среди стран региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидирует Азербайджан с 3,34%. Минимальный показатель в Туркмении — 0,26%.

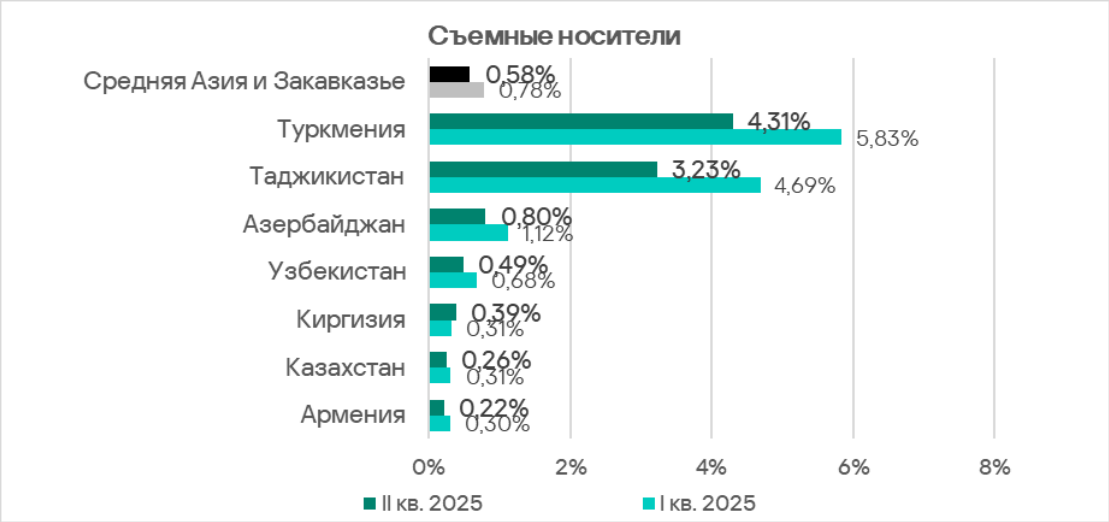
Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ, — это шпионское ПО, вредоносные документы, вредоносные скрипты и фишинговые страницы.



Съемные носители

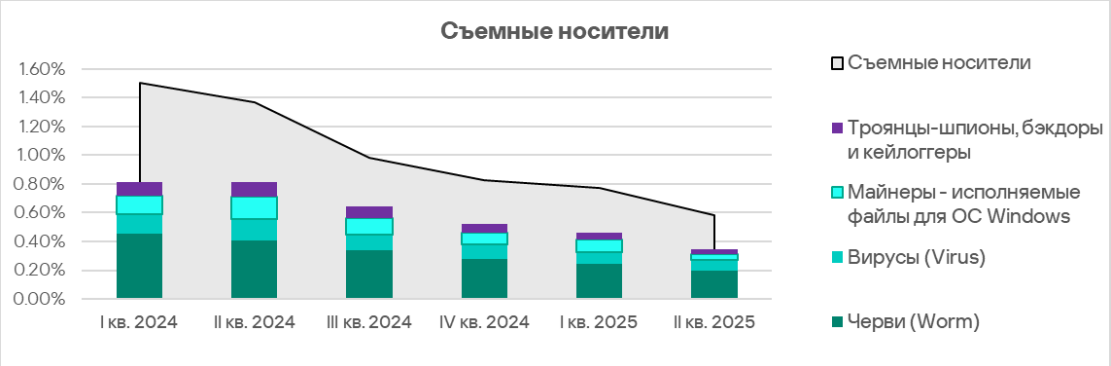
На первых шести позициях в рейтинге регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, — Африка и регионы Азии. Средняя Азия и Закавказье — на пятом месте с 0,58%. Это в 21,7 раза больше, чем в Северной Америке (Канаде) (0,03%), которая замыкает этот рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидируют Туркмения с 4,31% и Таджикистан с 3,23%. Отметим, что эти страны были последними в рейтинге по почтовым клиентам. Показатели остальных стран варьируют от 0,22% в Армении до 0,80% в Азербайджане.

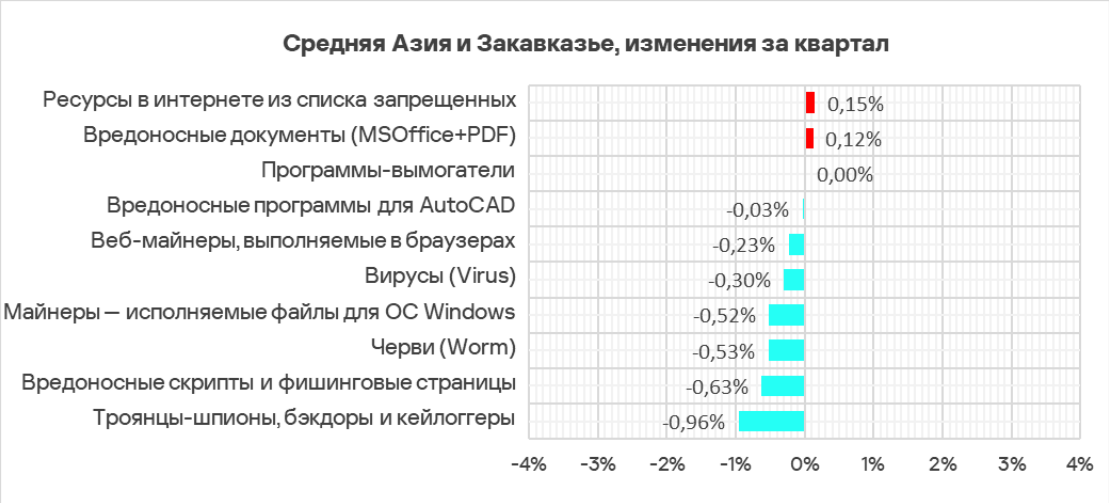


Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ, — черви, вирусы, майнеры — исполняемые файлы для ОС Windows и шпионское ПО.

По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы, Средняя Азия и Закавказье лидирует среди остальных регионов. По показателю червей — на втором месте после Африки.



Категории угроз



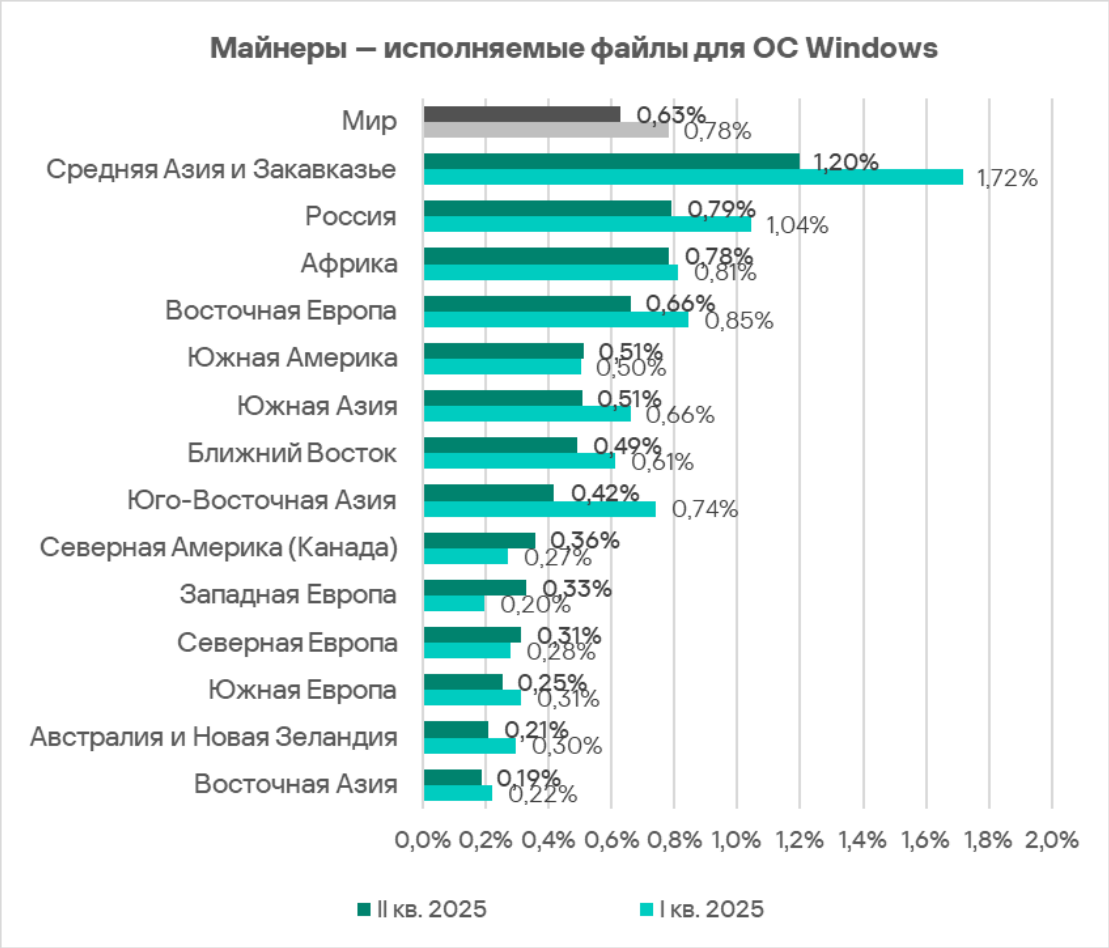
По сравнению со среднемировыми показателями в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории угроз:

- майнеры — исполняемые файлы для ОС Windows — в 1,9 раза; Средняя Азия и Закавказье лидирует среди регионов по этому показателю;
- черви — в 1,9 раза; регион находится на втором месте в соответствующем рейтинге;
- программы-вымогатели — в 1,4 раза; третье место в рейтинге регионов по этому показателю.

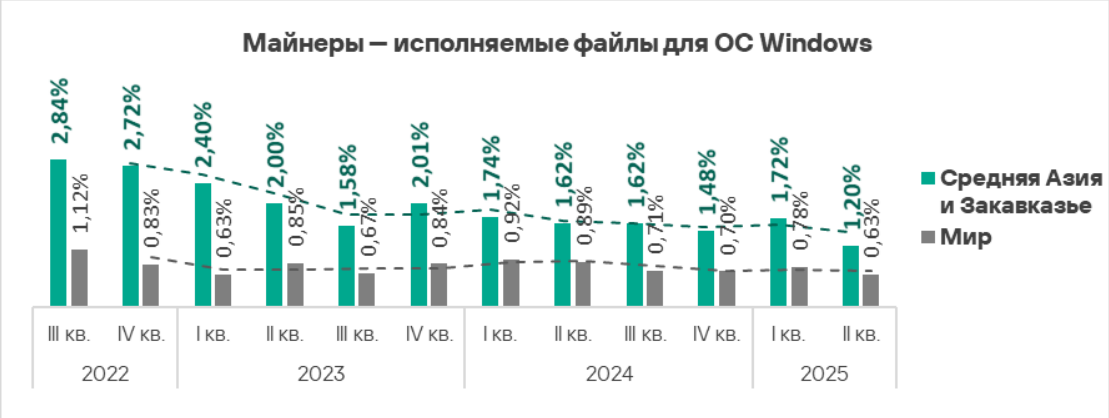
Из всех категорий угроз за квартал показатель вырос только у двух: ресурсы в интернете из списка запрещенных и вредоносные документы.

Майнеры — исполняемые файлы для ОС Windows

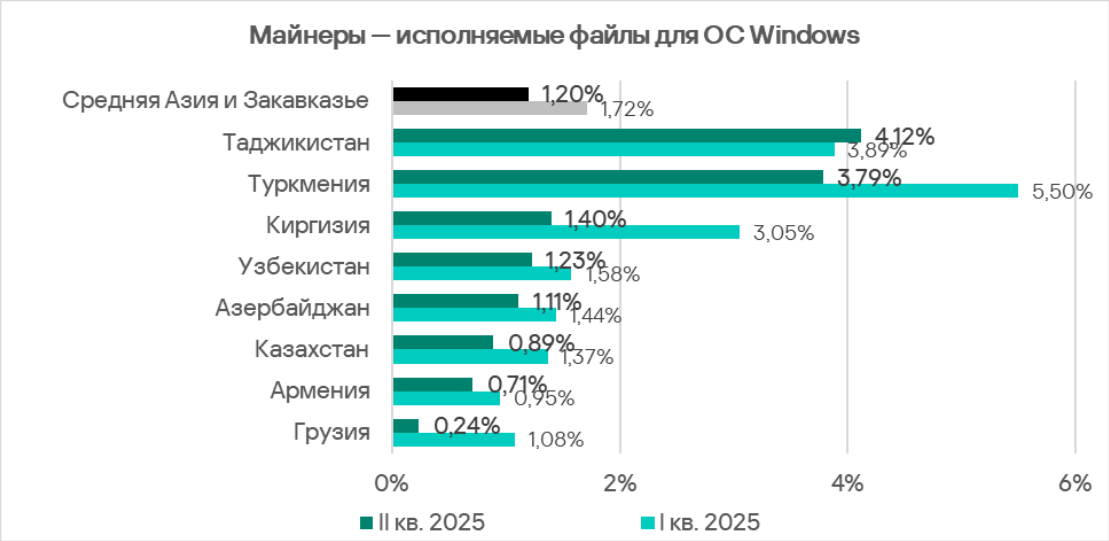
По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, Средняя Азия и Закавказье лидирует среди регионов с 1,20%. Этот показатель в 6,3 раза больше, чем в Восточной Азии, где он наименьший из всех среди регионов.



После роста в предыдущем квартале доля компьютеров АСУ, на которых блокировались майнеры — исполняемые файлы для ОС Windows, упала до минимального значения за период с III квартала 2022 года.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы майнеры в формате исполняемых файлов, лидируют Таджикистан с 4,12% и Туркмения с 3,79%. В Грузии показатель наименьший — 0,24%.

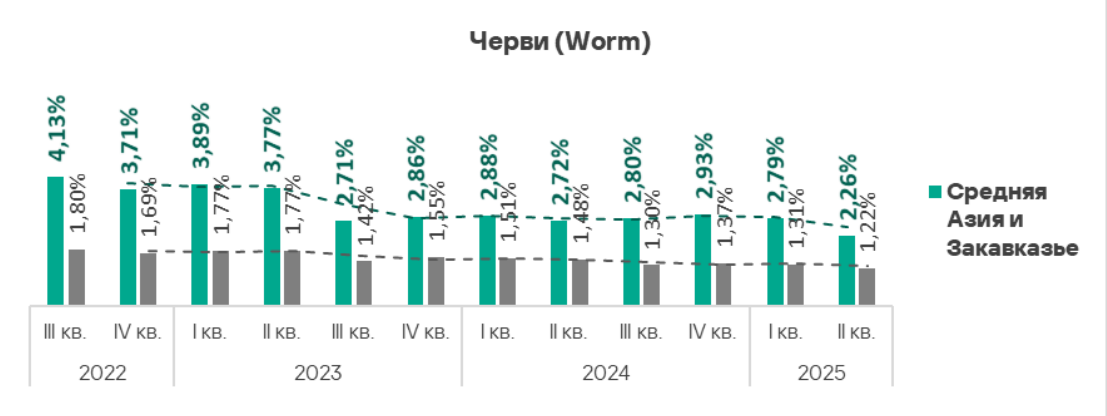


Распространяются такие угрозы через интернет и на съемных носителях. Таджикистан и Туркмения, лидирующие в этом рейтинге, лидируют также по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Черви

По доле компьютеров АСУ, на которых блокируются черви, Средняя Азия и Закавказье занимает среди регионов второе место, уступая только Африке. Показатель в регионе — 2,26%, это в 10,2 раза больше, чем в Австралии и Новой Зеландии, где он наименьший среди всех регионов.

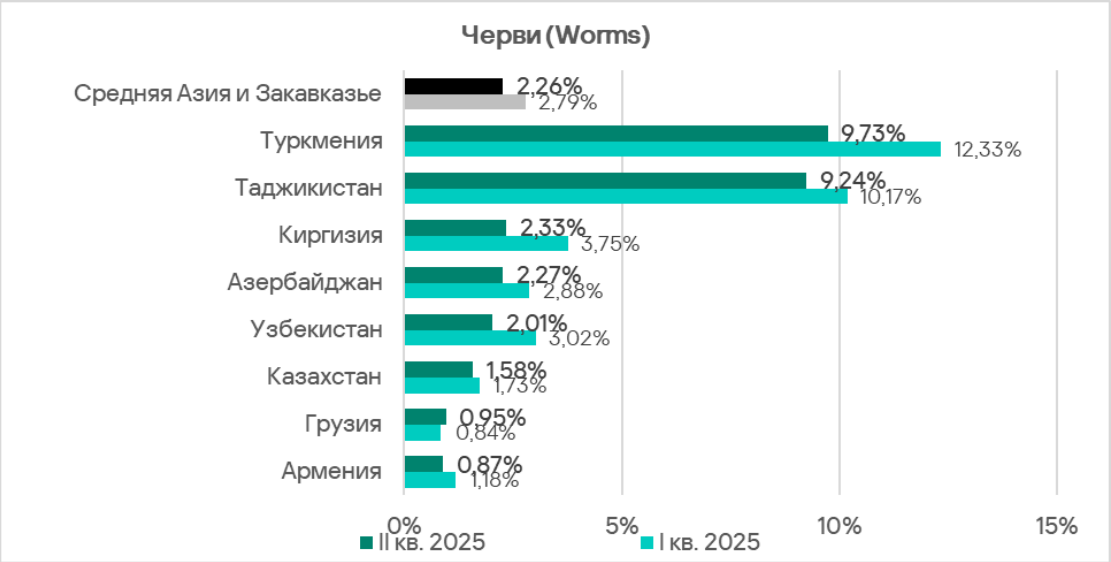
Показатель червей снижается в Средней Азии и Закавказье второй квартал подряд. Во втором квартале 2025 года он оказался минимальным за период с третьего квартала 2022 года.



Во втором квартале 2025 года, как и в предыдущем, в Средней Азии и Закавказье в рейтинге категорий угроз черви занимают четвертое место. На

такой высокой позиции в региональном рейтинге черви, кроме Средней Азии и Закавказья, находятся только в России.

Среди стран региона по доле компьютеров АСУ, на которых заблокированы черви, лидируют Таджикистан с 9,73% и Туркмения с 9,24%. В Армении показатель наименьший — 0,87%.



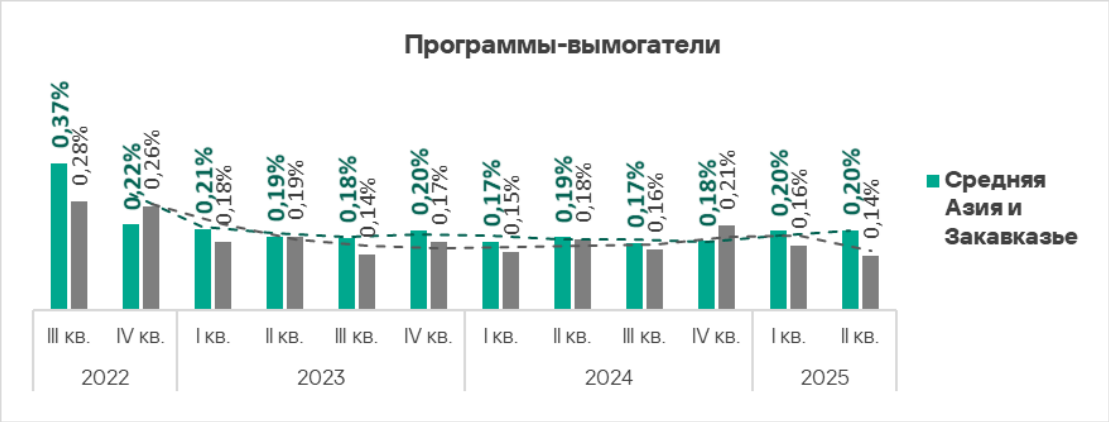
Распространяются такие угрозы преимущественно на съемных носителях. Таджикистан и Туркмения, лидирующие в этом рейтинге, лидируют также по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

Отметим также, что эти же страны лидируют в рейтинге по майнерам — исполняемым файлам для ОС Windows.

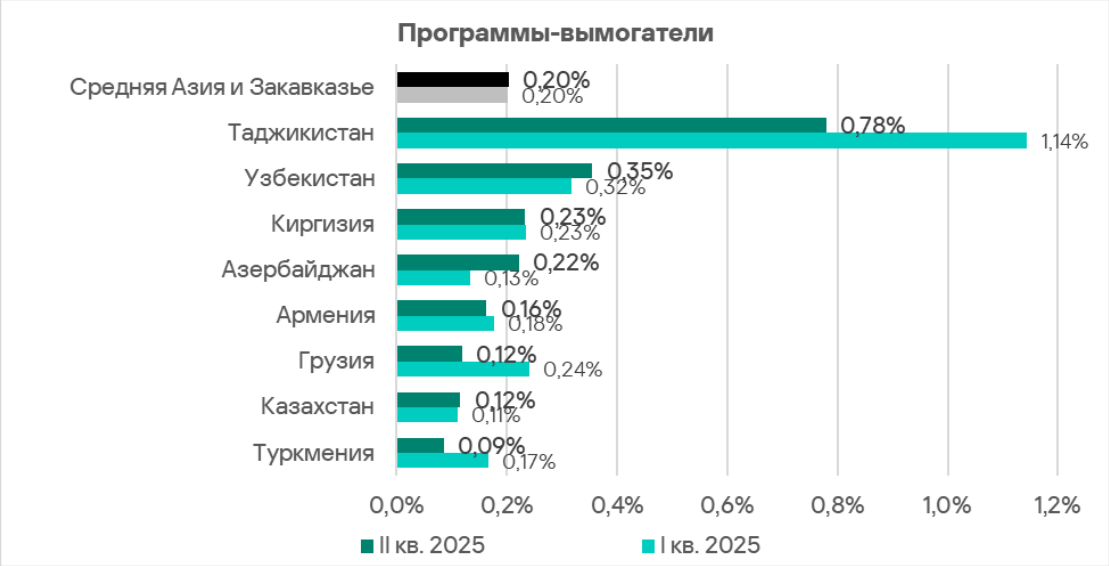
Программы-вымогатели

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Средняя Азия и Закавказье среди регионов занимает третье место. В этом регионе показатель больше, чем в Западной Европе, которая замыкает рейтинг, в 3,1 раза.

Показатель программ-вымогателей в Средней Азии и Закавказье довольно стабилен и, в отличие от большинства других категорий угроз, не изменился за квартал.



Лидерство региона по доле компьютеров АСУ, на которых были заблокированы вредоносные программы-вымогатели, обеспечивает прежде всего Таджикистан с 0,78%.

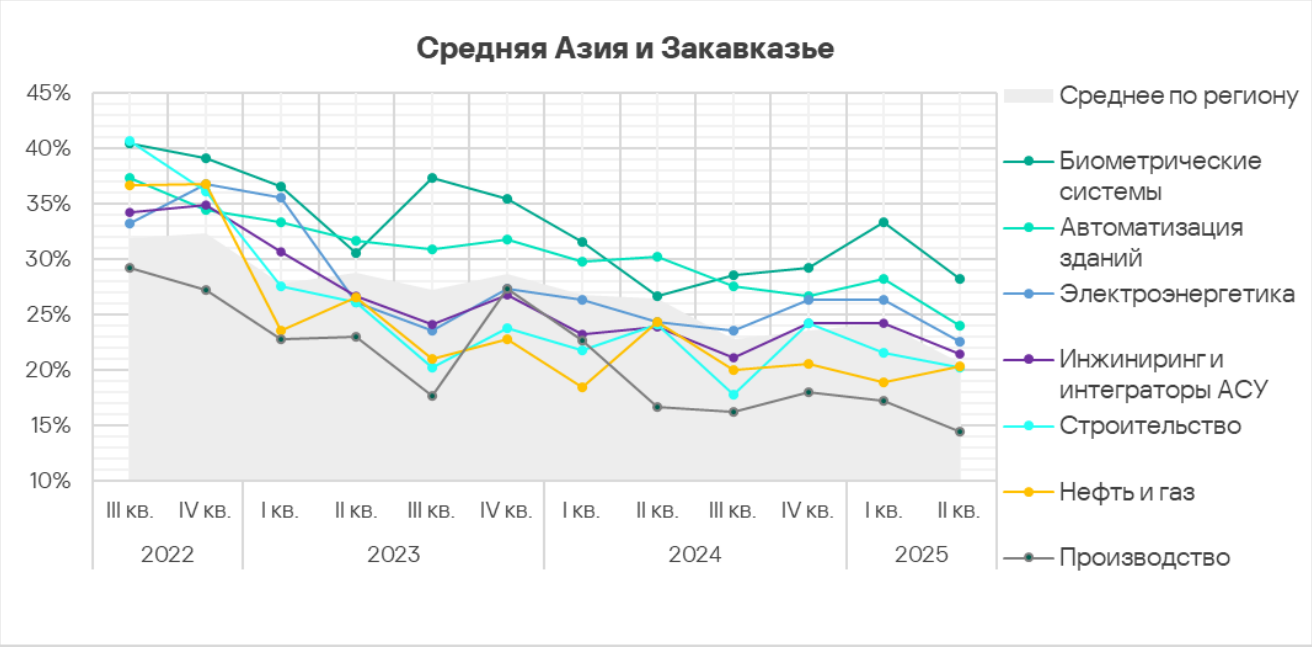


Отрасли

Из отраслей региона, рассмотренных в отчете, чаще встречаются с угрозами OT-инфраструктура биометрические системы и автоматизация зданий.

У всех отраслей, кроме строительства и производства, показатели выше среднемировых. Больше всего региональный показатель превышает среднемировое значение у нефтегазовой отрасли — в 1,26 раза. Это единственная отрасль, где показатель за квартал вырос, причем на заметные 4,2 п. п. В прошлом квартале он уменьшился, и даже после роста до 20,3% не достиг значений четвертого квартала 2024 года (20,5%).

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 проблемы отраслей мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение для источника или типа угроз среди всех регионов и индустрий. В Средней Азии и Закавказье максимальное значение наблюдается для майнеров — исполняемых файлов, заблокированных на компьютерах в системах сбора, обработки и хранения биометрических данных.

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	10,67%	9,29%	10,84%	11,09%	7,71%	9,35%	5,56%	8,80%
Почтовые клиенты	4,80%	2,41%	1,61%	1,06%	2,81%	0,81%	0,74%	1,45%
Съемные носители	0,80%	0,71%	1,07%	0,53%	0,14%	0,58%	0,37%	0,58%
Сетевые папки	0,00%	0,05%	0,00%	0,00%	0,00%	0,00%	0,00%	0,03%
Показатель отрасли в регионе	28,27%	23,95%	22,49%	21,46%	20,34%	20,21%	14,44%	

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

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	8,27%	5,93%	8,17%	7,31%	4,49%	6,81%	4,07%	5,65%
Вредоносные скрипты и фишинговые страницы	6,67%	5,73%	6,16%	5,56%	7,15%	5,08%	2,96%	4,77%
Троянцы-шпионы, бэкдоры и кейлоггеры	6,13%	5,62%	3,88%	3,61%	1,54%	3,00%	3,70%	3,74%
Черви (Worm)	4,53%	3,08%	2,01%	1,89%	1,12%	1,96%	2,22%	2,26%
Майнеры - исполняемые файлы для ОС Windows	2,67%	1,37%	2,14%	1,36%	0,98%	1,73%	1,85%	1,20%
Вредоносные документы (MSOffice + PDF)	3,73%	1,80%	0,80%	1,20%	0,98%	0,81%	1,11%	1,17%
Вирусы (Virus)	1,33%	1,35%	1,74%	1,03%	0,70%	1,39%	1,48%	1,00%
Программы-вымогатели	0,27%	0,35%	0,40%	0,33%	0,28%	0,35%	0,37%	0,20%
Веб-майнеры, выполняемые в браузерах	0,53%	0,20%	0,40%	0,28%	0,14%	0,23%	0,37%	0,18%
Вредоносные программы для AutoCAD	0,00%	0,02%	0,40%	0,17%	0,00%	0,35%	0,00%	0,06%
Показатель отрасли в регионе	28,27%	23,95%	22,49%	21,46%	20,34%	20,21%	14,44%	

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

«Горячие точки» отраслей

Биометрические системы

- Самый высокий из всех отраслей показатель почтовых клиентов. Второе место по съемным носителям.
- Лидер по показателям большинства категорий угроз.

Автоматизация зданий

- Единственная отрасль, где были заблокированы угрозы в сетевых папках.
- Второе место по вредоносным документам, шпионским программам, червям.

Электроэнергетика

- Лидер среди отраслей региона по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.

- Лидирует по показателям вирусов, программ-вымогателей и вредоносных программ для AutoCAD. Второе место по майнерам обеих категорий.

Инжиниринг и интеграторы АСУ

- Лидер по показателю угроз из интернета.
- Третье место по ресурсам в интернете из списка запрещенных и вредоносным документам.

Нефть и газ

- Второе место по почтовым клиентам.
- Лидер по вредоносным скриптам и фишинговым страницам.

Строительство

- Четвертое место по съемным клиентам.
- Второе место по вредоносным программам для AutoCAD, третье место по вирусам и программам вымогателям (вместе с автоматизацией зданий).

Производство

- Угрозы из почтовых клиентов.
- Второе место по вирусам и показателю программ-вымогателей, третье — по доле компьютеров АСУ, на которых были заблокированы черви и майнеры обеих категорий.

Восточная Азия

Основные проблемы кибербезопасности в регионе

Отсутствие или неэффективность мер защиты периметра технологической сети

Восточная Азия — единственный регион, где шпионские программы занимают первое место в рейтинге категорий вредоносного ПО по доле компьютеров АСУ, на которых они были заблокированы.

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 рейтинге по всем индустриям во всех регионах сфера строительства в Восточной Азии занимает первое место по показателю вредоносного ПО для AutoCAD.

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.

Электроэнергетика в Восточной Азии лидирует среди всех индустрий во всех регионах по доле компьютеров, на которых угрозы блокировались на съемных и сетевых дисках.

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, помимо червей, чаще всего блокируется шпионское ПО.

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 электроэнергетике, Восточная Азия во втором квартале 2025 года лидирует среди регионов с 30,33%. По показателям отраслей строительство и производство регион находится на третьем месте в соответствующих рейтингах.

Восточная Азия — крупнейший мировой потребитель электроэнергии. Потребление и, соответственно, генерация в регионе растут практически непрерывно. Соответственно, неудивительны высокие значения показателя доступности OT-систем сектора для киберугроз. Ведь при вводе в эксплуатацию новых объектов адекватные меры киберзащиты обычно применяются с заметным запозданием.

Яркие различия в странах региона

Ситуация с кибербезопасностью в разных странах региона существенно отличается. Это хорошо заметно, в частности, по рейтингам стран по показателям компьютеров АСУ, где вредоносные объекты были заблокированы из разных источников:

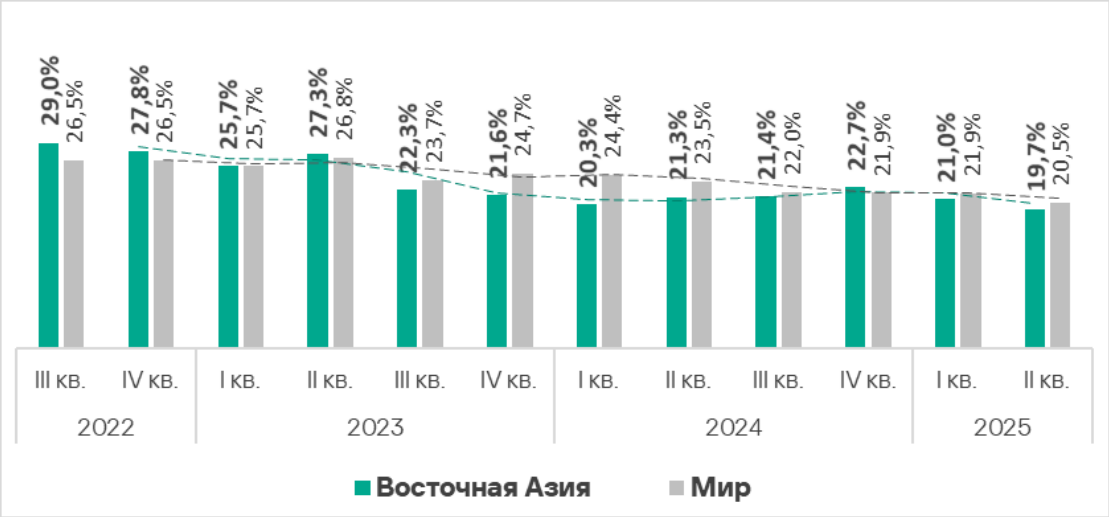
- Монголия лидирует по угрозам из интернета;
- Тайвань и Гонконг — по угрозам из почты;
- континентальный Китай лидирует по угрозам на съемных носителях и в сетевых папках, что обуславливает высокие позиции региона по показателям вирусов и вредоносных программам для AutoCAD.

Япония занимает последние места в большинстве рейтингов.

Статистика по всем угрозам

Восточная Азия занимает седьмое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с 19,7%.

Показатель в регионе снижается второй квартал подряд. Несмотря на это, значение показателя во втором квартале 2025 года превышает минимальное — в Северной Европе — в 1,8 раза.

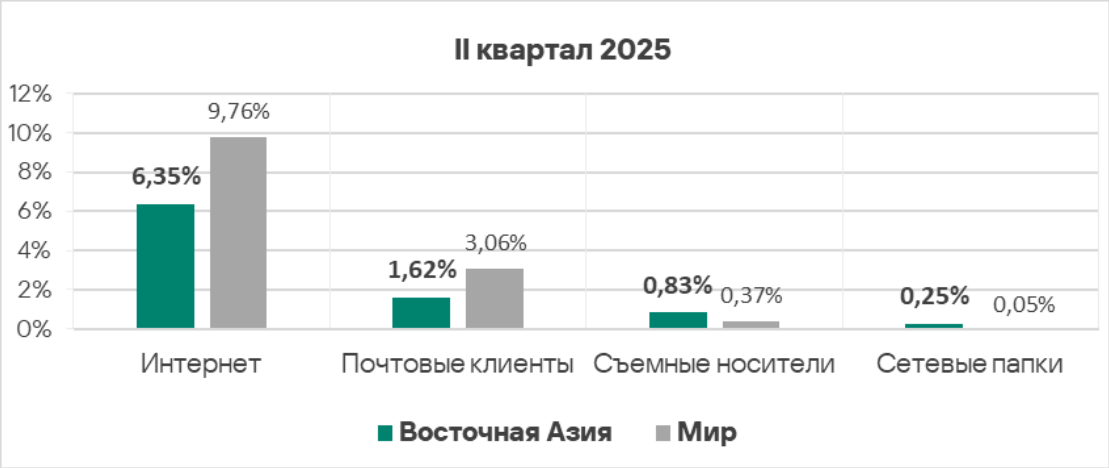


В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 9,65% в Японии до 23,15% в континентальном Китае. Высокий показатель также у Монголии, которая занимает второе место с 22,94%. Показатели остальных стран — в диапазоне от 13% до 16%.

Источники угроз

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

- съемные носители — в 2,2 раза, второе место среди регионов;
- сетевые папки — в 4,7 раза, первое место среди регионов.



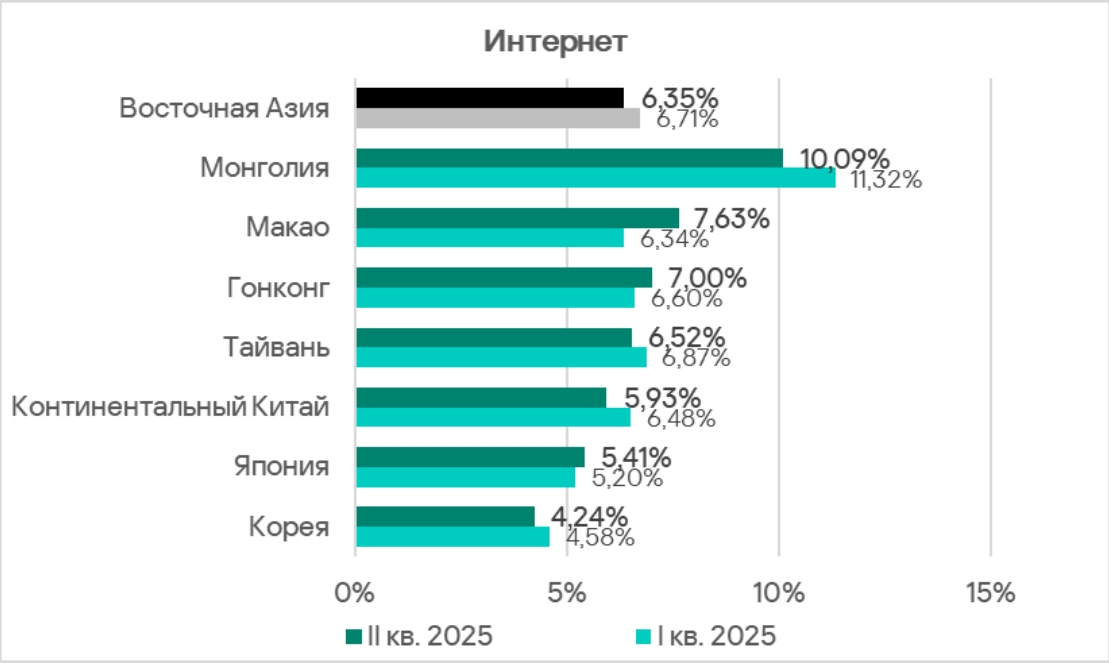
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз, кроме почтовых клиентов, показатель которых вернулся к значениям второго квартала 2024 года.

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

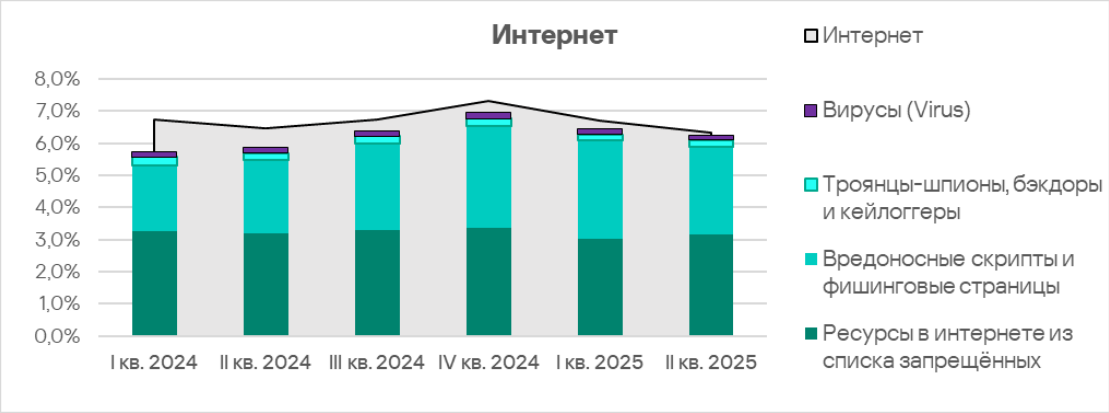
Интернет

Во втором квартале 2025 года у Восточной Азии оказался наименьший из всех регионов показатель по угрозам из интернета — 6,35%. Это также наименьший показатель в регионе за период с третьего квартала 2022 года.

Показатели стран региона варьируют от 4,24% в Корее до 10,09% в Монголии.



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

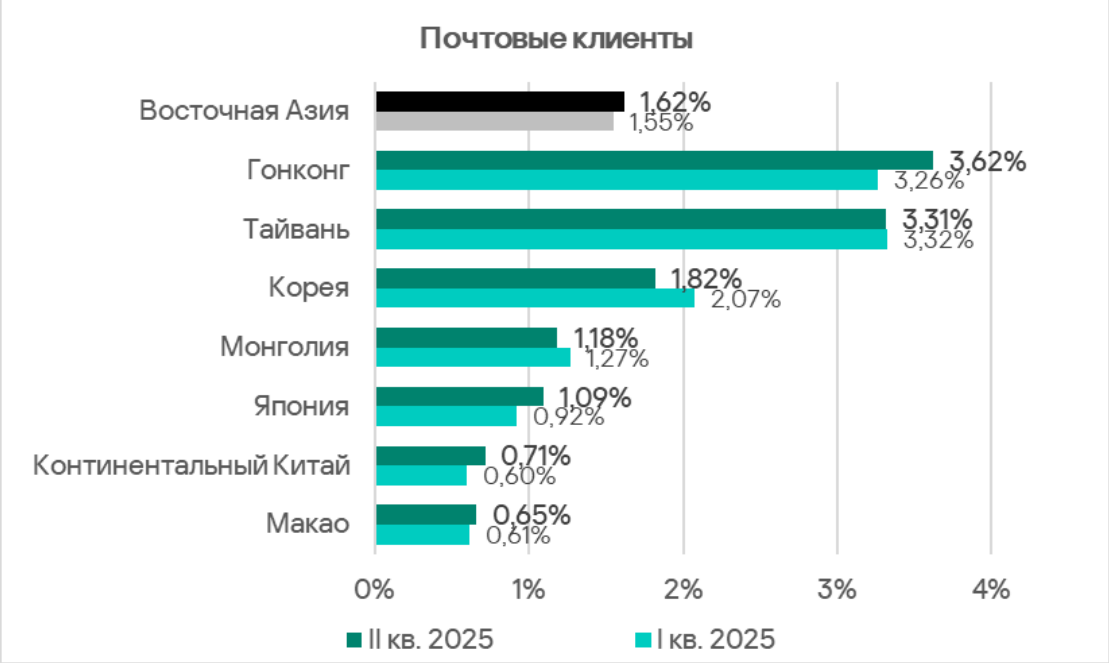


По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в регионе также лидирует Монголия.

Почтовые клиенты

По доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, Восточная Азия среди регионов занимает 11-е место с 1,62%. Это вдвое больше, чем в России, где показатель наименьший.

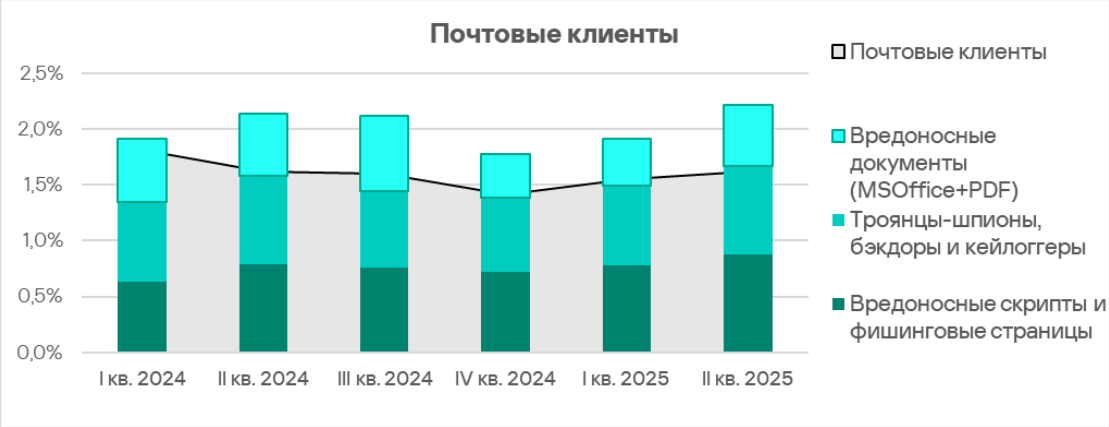
Среди стран и территорий региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидируют Гонконг с 3,62% и Тайвань с 3,31%. Минимальный показатель в Макао — 0,65%.



Гонконг и Тайвань находятся в числе лидеров и по показателям угроз, распространяемых преимущественно через почту, — вредоносные документы (Тайвань — на первом месте, Гонконг — на третьем) и

вредоносные скрипты и фишинговые страницы (первое и второе места соответственно).

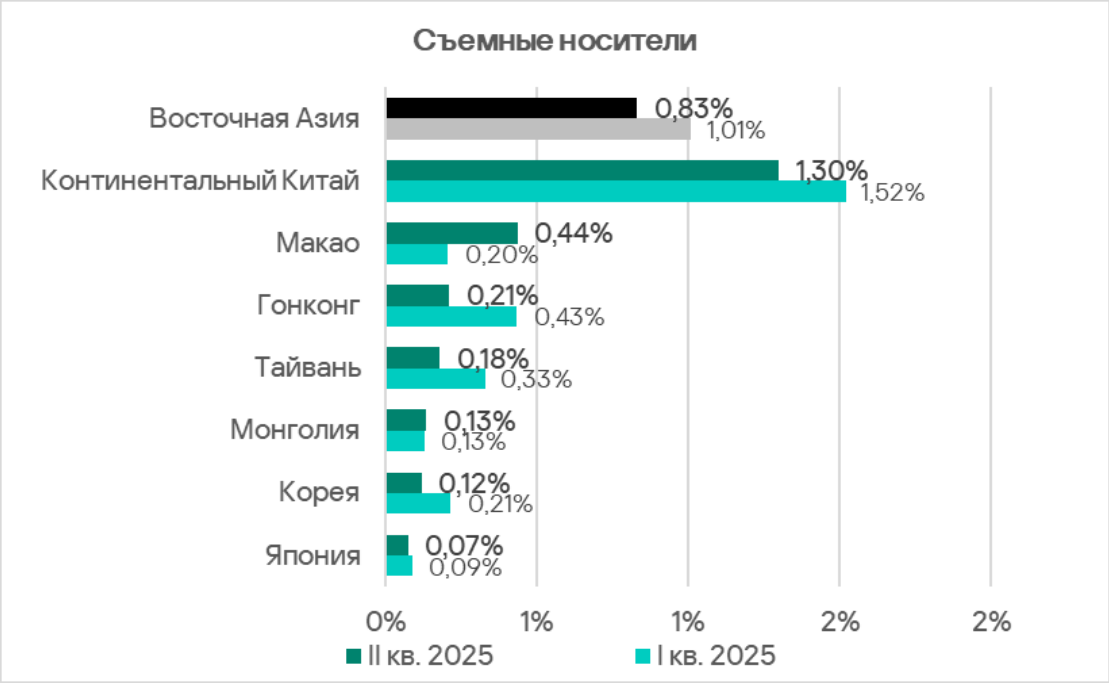
Основные категории угроз из почтовых клиентов, заблокированные на компьютерах АСУ, — это вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы. Шпионские программы, которые занимают первое место в региональном рейтинге по доле атакованных компьютеров АСУ, распространяются во всех источниках угроз, но почта — основной.



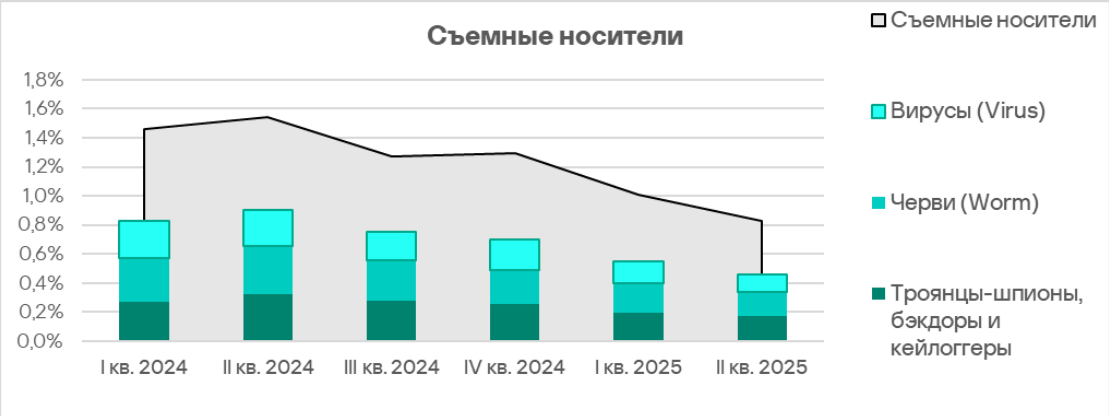
Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Восточная Азия занимает второе место среди регионов, уступая только Африке. Показатель региона (0,83%) в 30,9 раза больше, чем в Северной Америке (Канаде), которая замыкает этот рейтинг.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует континентальный Китай с 1,30%. Показатели остальных стран и территорий варьируют от 0,07% в Японии до 0,44% в Макао.

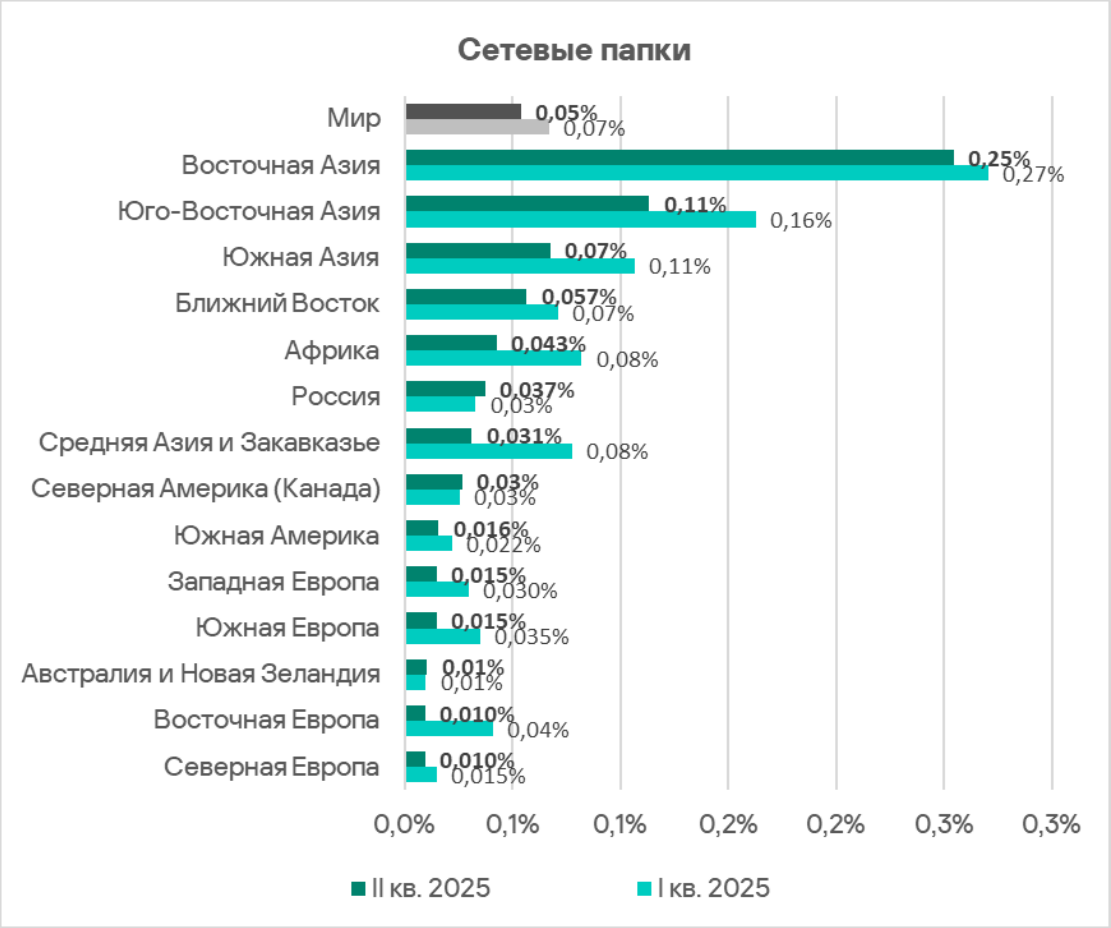


Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ, — шпионское ПО, черви и вирусы. Для червей это основной канал распространения. Отметим, что континентальный Китай лидирует также и по доле компьютеров АСУ, на которых были заблокированы черви.

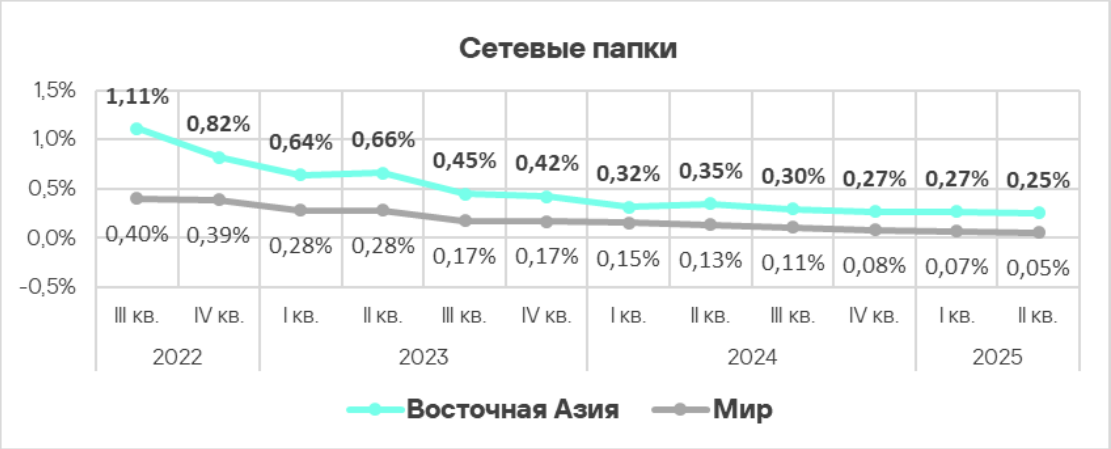


Сетевые папки

Восточная Азия по-прежнему занимает первое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. Во втором квартале 2025 года показатель региона (0,25%) превышает среднемировой в 4,7 раза и в 26,3 раза показатель Северной Европы, где он наименьший среди регионов.

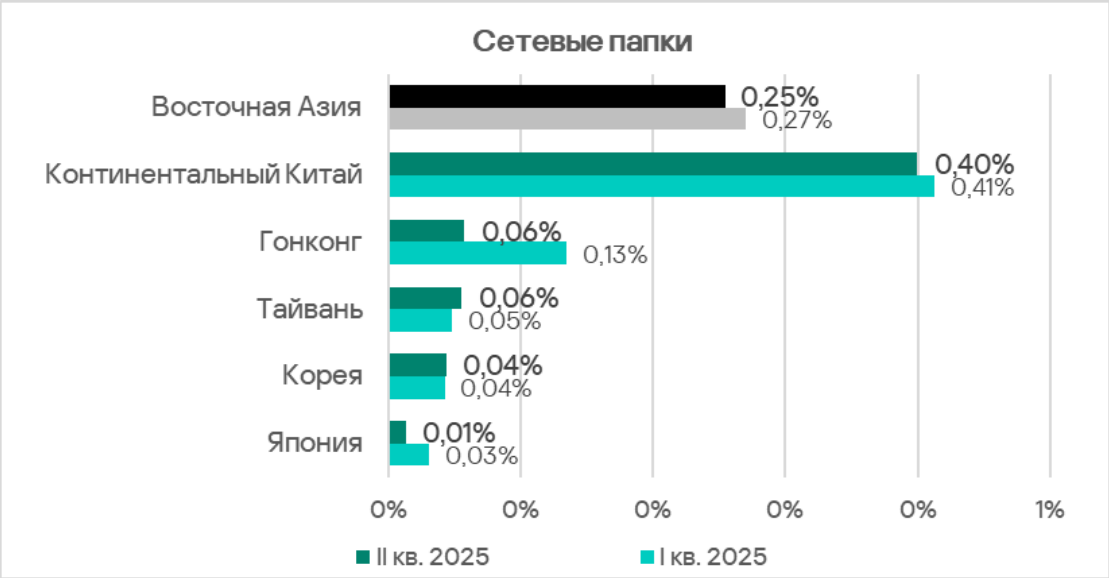


Доля компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, в Восточной Азии демонстрирует нисходящий тренд. Показатель во втором квартале 2025 года был минимальным за период с третьего квартала 2022 года.



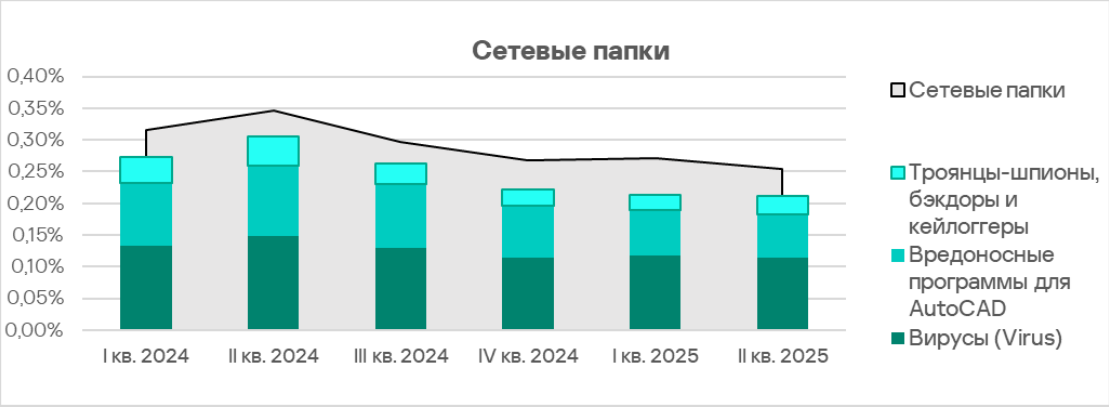
Лидерство Восточной Азии по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, обеспечивает континентальный

Китай, с огромным отрывом лидирующий среди стран и территорий региона с 0,40%.



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

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

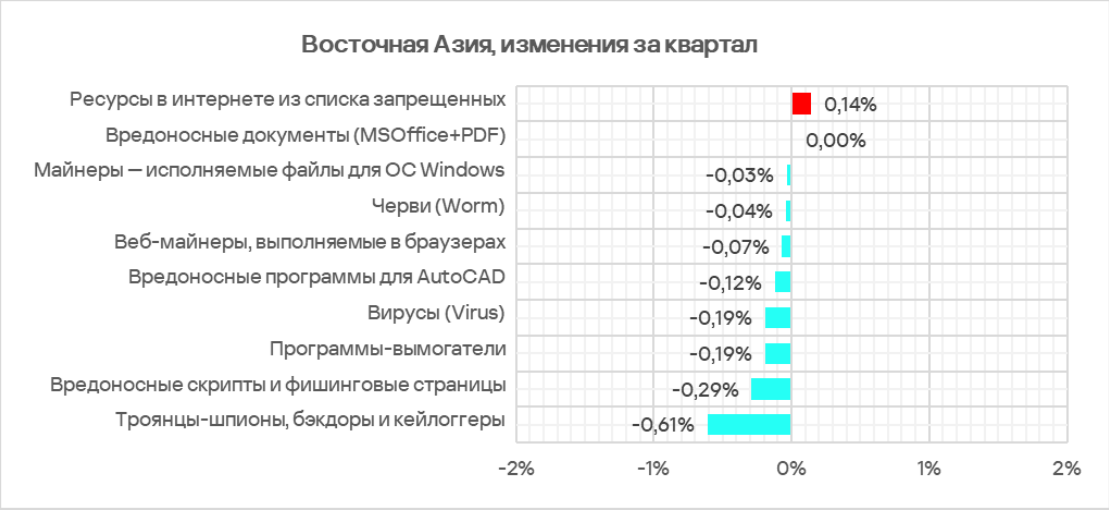


Вирусы в регионе распространяются через все источники угроз, однако показатель сетевых папок для этой угрозы высок и сопоставим с показателем съемных носителей.

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

Категории угроз

Восточная Азия — единственный регион, где шпионские программы занимают первое место в рейтинге категорий угроз.



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

- шпионские программы — в 1,1 раза;
- вирусы — в 2,1 раза, на третьем месте среди регионов;
- черви — в 1,1 раза;

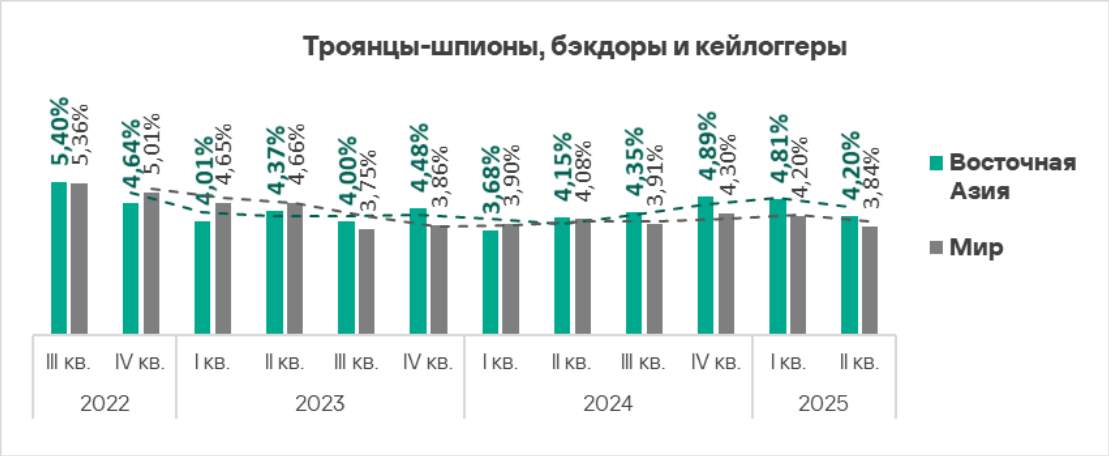
- вредоносное ПО для AutoCAD — в 3,7 раза, на втором месте среди регионов.

Шпионские программы

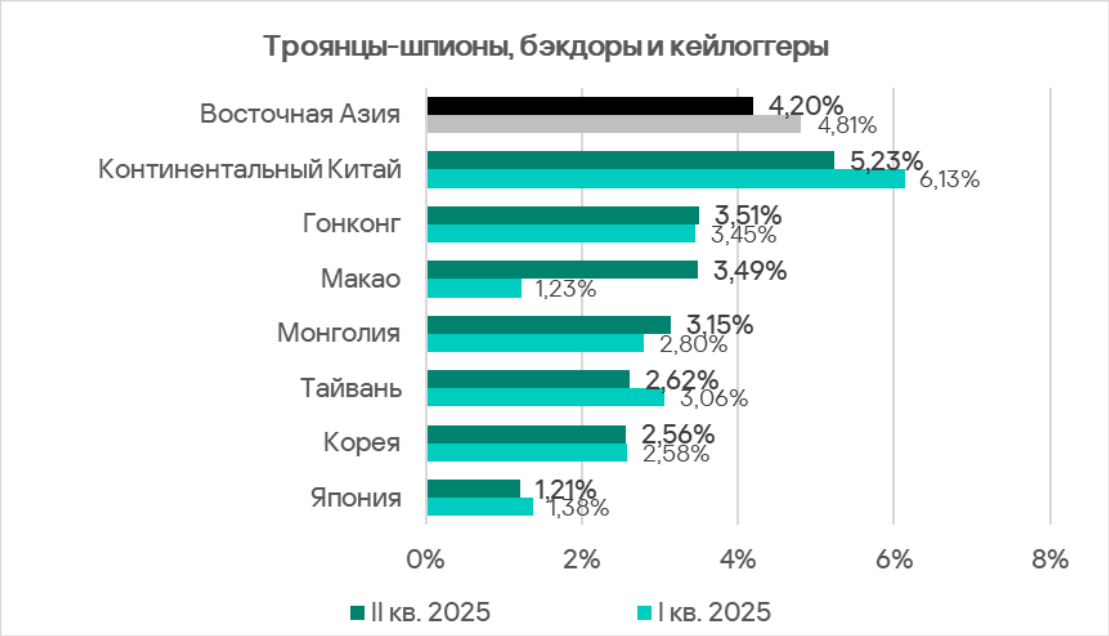
Как уже было сказано выше, только в Восточной Азии в региональном рейтинге по показателям категорий угроз лидируют программы-шпионы.

Среди регионов по доле компьютеров АСУ, на которых блокируются шпионские программы, Восточная Азия занимает седьмое место с 4,20%. Этот показатель в 3 раза больше, чем в Западной Европе, где он наименьший среди регионов.

Доля компьютеров АСУ, на которых блокируется шпионское ПО, в регионе довольно стабильна и с конца 2022 года колеблется в диапазоне от 3,68% до 4,89%. Последние два квартала показатель снижается.



Среди стран и территорий региона по доле компьютеров АСУ, на которых заблокированы шпионские программы, лидирует континентальный Китай с 5,23%. В Японии показатель наименьший — 1,21%.



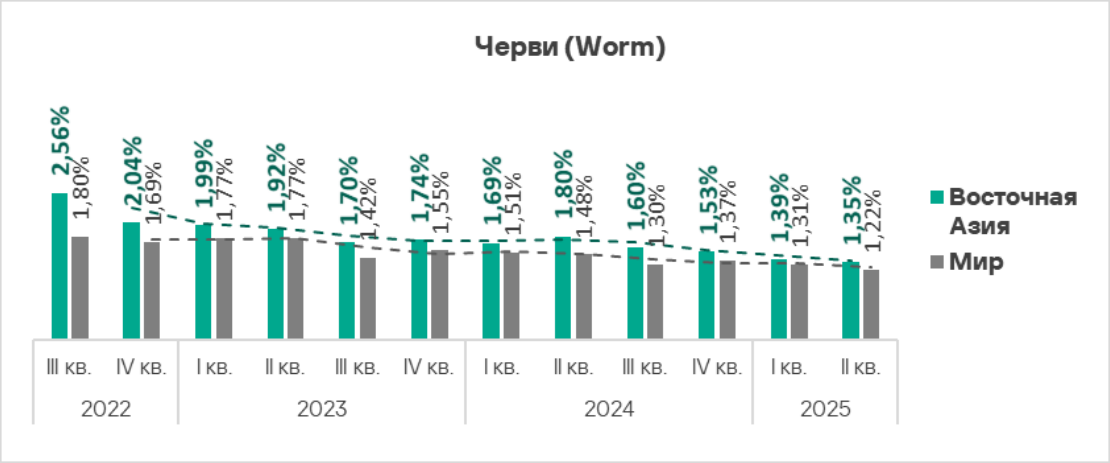
В регионе такие угрозы распространяются через все источники, но в первую очередь на съемных носителях.

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

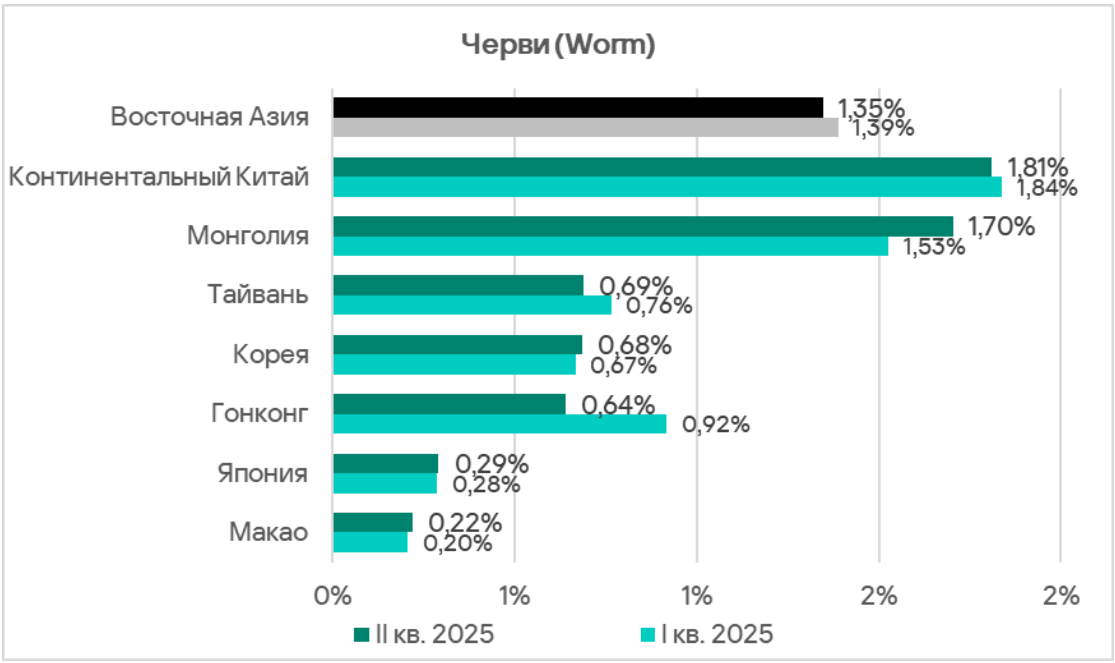
Черви

По доле компьютеров АСУ, на которых блокируются черви, Восточная Азия занимает среди регионов шестое место с 1,35%. Это в 6,1 раза больше, чем в Австралии и Новой Зеландии, где показатель наименьший среди всех регионов.

Доля компьютеров АСУ, на которых блокируются черви, в Восточной Азии снижается третий квартал подряд. Во втором квартале 2025 года она оказалась минимальной за период с третьего квартала 2022 года.



Среди стран и территорий региона по доле компьютеров АСУ, на которых заблокированы черви, лидируют континентальный Китай с 1,81% и Монголия с 1,70%.



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

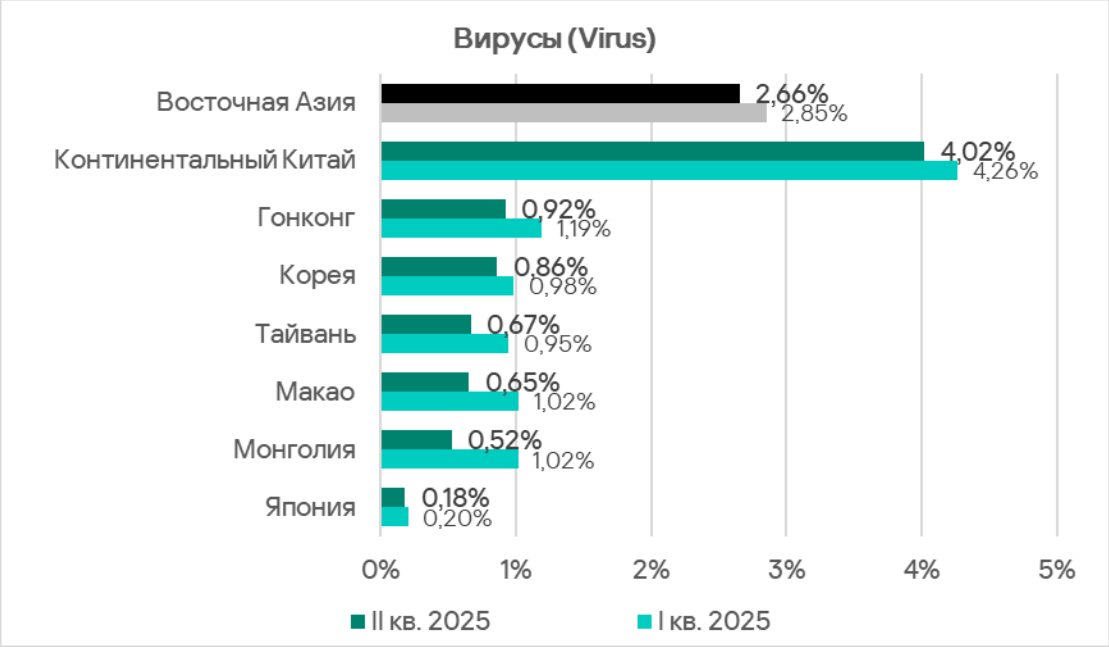
Вирусы и вредоносные программы для AutoCAD

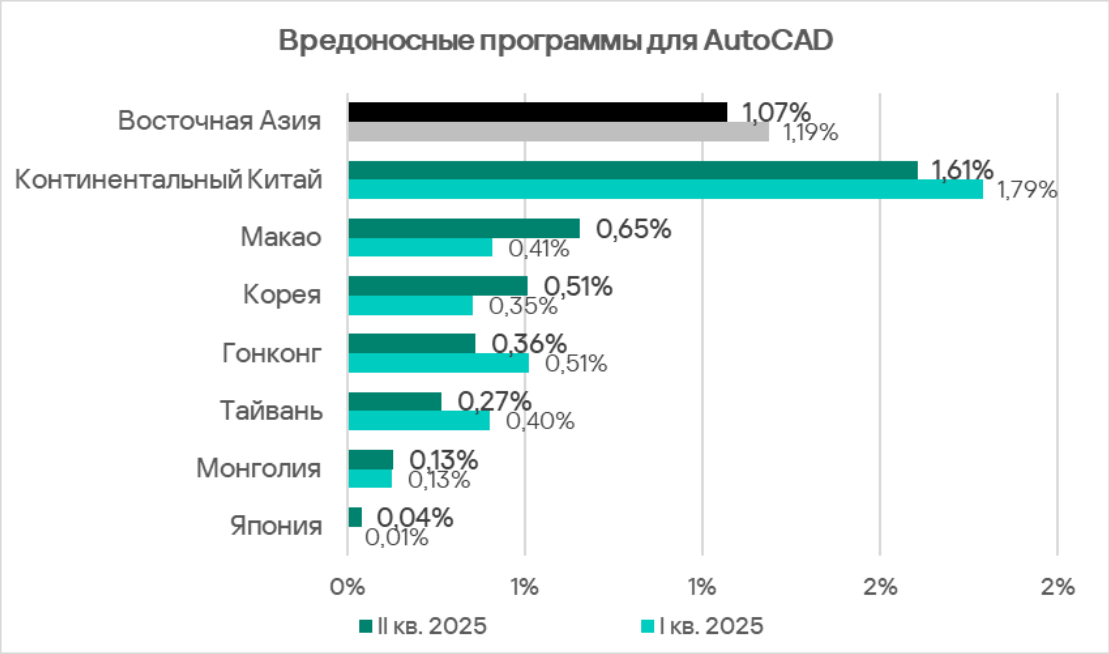
Восточная Азия занимает третье место среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, и второе место

по показателям вредоносных программ для AutoCAD, уступая в этом рейтинге только Юго-Восточной Азии.

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

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





Вирусы в регионе распространяются через все источники угроз, при этом показатель сетевых папок для этой угрозы сопоставим с показателем съемных носителей.

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

Отрасли

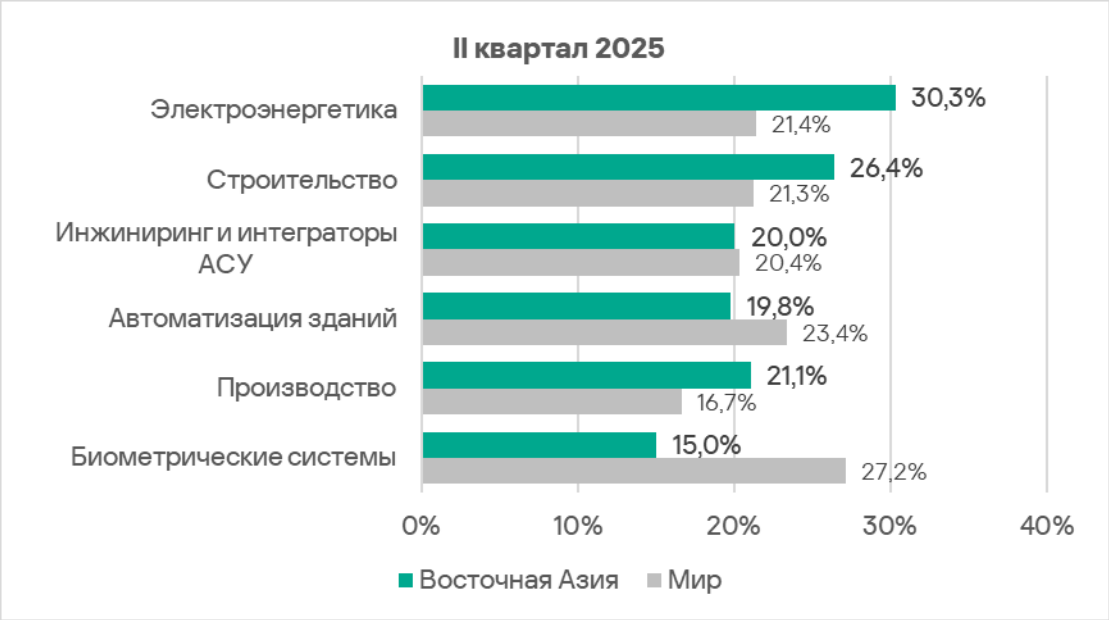
Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является электроэнергетика.

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

- электроэнергетика — в 1,4 раза;
- производство — в 1,3 раза;
- строительство — в 1,2 раза.

По показателю электроэнергетики Восточная Азия во втором квартале 2025 года лидирует среди регионов с 30,33%.

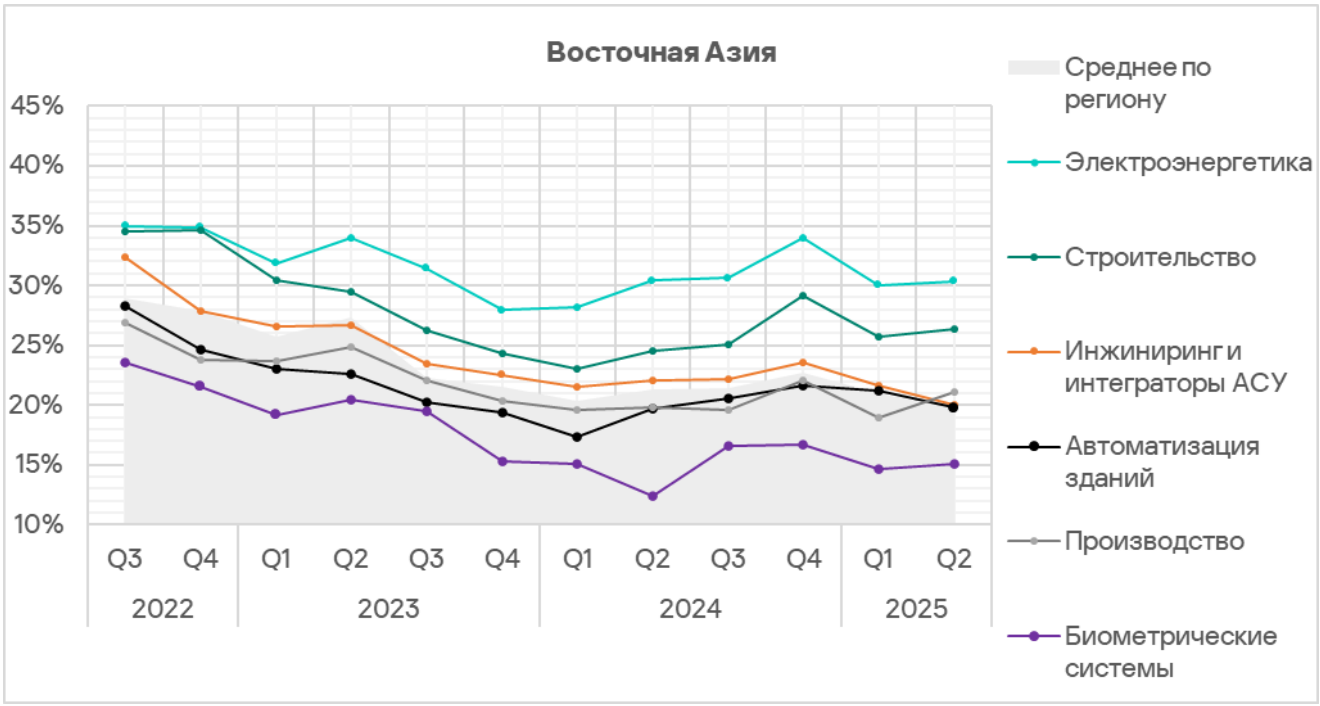
По показателю отраслей производство и строительство Восточная Азия среди регионов занимает третье место в соответствующих рейтингах.



Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась только в двух отраслях: автоматизация зданий, а также инжиниринг и интеграторы АСУ.

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

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



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

При оценке проблем отраслей мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение для источника или типа угроз среди всех регионов и индустрий. В Восточной Азии максимальное значение наблюдается в категории вредоносных программ для AutoCAD, заблокированных на компьютерах в сфере строительства.

На тепловых картах хорошо видны «горячие точки» отраслей — позиции источников и категорий вредоносного ПО, показатель по которым выше ожидаемого в соответствии с местом отрасли и местом угрозы или источника угрозы в соответствующих региональных и глобальных рейтингах.

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	4,88%	6,44%	10,64%	6,23%	10,61%	7,26%	6,35%
Почтовые клиенты	5,89%	3,00%	1,19%	1,54%	2,05%	1,73%	1,62%
Съемные носители	0,00%	1,02%	2,16%	0,77%	0,51%	1,35%	0,83%
Сетевые папки	0,00%	0,33%	0,73%	0,30%	0,57%	0,72%	0,25%
Показатель отрасли в регионе	15,04%	19,78%	30,33%	20,05%	26,41%	21,06%	

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

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	2,03%	3,16%	5,74%	3,14%	5,08%	4,13%	3,28%
Вредоносные скрипты и фишинговые страницы	5,49%	5,19%	5,48%	3,90%	7,02%	4,81%	4,05%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,28%	5,49%	8,57%	4,13%	6,45%	5,00%	4,20%
Черви (Worm)	0,81%	1,71%	3,18%	1,32%	1,88%	3,17%	1,35%
Майнеры - исполняемые файлы для ОС Windows	0,81%	0,37%	0,32%	0,16%	0,34%	0,34%	0,19%
Вредоносные документы (MSOffice + PDF)	3,05%	2,22%	2,71%	1,54%	2,45%	2,64%	1,46%
Вирусы (Virus)	0,61%	2,04%	5,33%	3,28%	5,42%	3,85%	2,66%
Программы-вымогатели	0,00%	0,23%	0,26%	0,12%	0,23%	0,29%	0,13%
Веб-майнеры, выполняемые в браузерах	0,61%	0,20%	0,17%	0,08%	0,46%	0,19%	0,11%
Вредоносные программы для AutoCAD	0,20%	0,92%	2,51%	1,23%	6,33%	1,92%	1,07%
Показатель отрасли в регионе	15,04%	19,78%	30,33%	20,05%	26,41%	21,06%	

У всех отраслей высокий показатель шпионских программ и категории вредоносные скрипты и фишинговые страницы.

«Горячие точки» отраслей

Электроэнергетика

- Лидер среди отраслей в регионе по показателям угроз из интернета.

- Лидер среди всех отраслей во всех регионах по показателям угроз на съемных носителях и в сетевых папках.
- Первое место по показателям следующих категорий угроз в регионе: шпионские программы, ресурсы в интернете из списка запрещенных, черви.
- Второе место по доле компьютеров АСУ в электроэнергетике, на которых блокировались угрозы, среди всех регионов.
- Второе место по показателям следующих категорий в регионе: вредоносные документы, вирусы, вредоносные программы для AutoCAD, программы-вымогатели.
- Третье место в регионе по показателю вредоносных скриптов и фишинговых страниц.

Строительство

- Первое место среди всех отраслей во всех регионах по показателю вредоносного ПО для AutoCAD.
- Второе место в регионе среди отраслей по угрозам из интернета. Третье — по показателю угроз из почтовых клиентов и в сетевых папках.
- Второе место в регионе по показателям следующих категорий: шпионские программы, ресурсы в интернете из списка запрещенных и веб-майнеры.

Производство

- Второе место среди всех отраслей во всех регионах по угрозам в сетевых папках.
- Второе место среди отраслей в регионе по угрозам на съемных носителях и в сетевых папках. Третье место по угрозам из интернета.
- Второе место в регионе по показателю червей.
- Третье место по показателям внутри региона: ресурсы в интернете из списка запрещенных, вредоносные документы, вирусы и вредоносные программы для AutoCAD.

Инжиниринг и интеграторы АСУ

- Четвертое место среди отраслей в регионе по угрозам на съемных носителях.
- Четвертое место в регионе по показателям вирусов и вредоносных программ для AutoCAD.

Автоматизация зданий

- Второе место по угрозам из почты среди отраслей в регионе. Третье место по угрозам на съемных носителях. Четвертое место по угрозам из интернета и в сетевых папках.
- Второе место в регионе по майнерам — исполняемым файлам для ОС Windows.
- Третье место в регионе по следующим категориям угроз: шпионские программы, программы-вымогатели и веб-майнеры.
- Четвертое место в регионе по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, черви.

Биометрические системы

- Лидер по угрозам в почтовых клиентах среди отраслей в регионе.
- Лидер в регионе среди отраслей по категориям угроз: вредоносные документы и майнеры обеих категорий.
- Второе место в регионе по показателю категории вредоносные скрипты и фишинговые страницы.
- Четвертое место по показателю шпионских программ в регионе.

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 1,7 раза.

Южная Азия находится на третьем месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. Показатель по этому источнику угроз превышает среднемировое значение в 1,2 раза.

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

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

Высокий уровень угроз из интернета

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

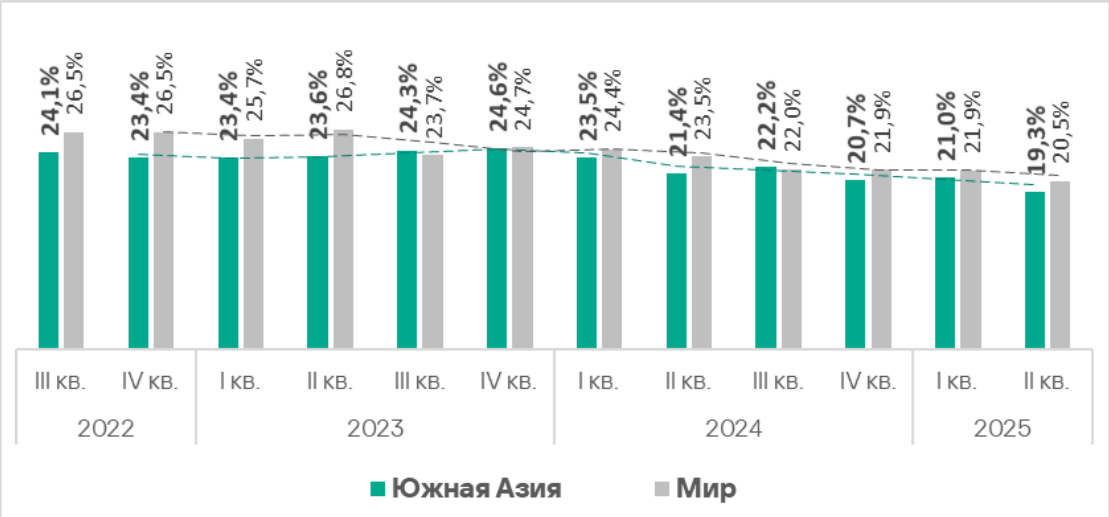
Различия в странах региона

- На все показатели региона большое влияние оказывает Индия. Эта страна находится в конце большинства рейтингов по источникам и по категориям угроз с долей атакованных компьютеров АСУ, которая заметно ниже, чем в большинстве других стран региона, и меньше среднего по региону.
- Ситуация с кибербезопасностью в Афганистане заметно отличается от других стран региона в отношении контроля подключения съемных носителей. Это заметно по показателям съемных носителей и самораспространяющегося ПО в разных странах — в Афганистане они заметно выше, чем в других странах региона.

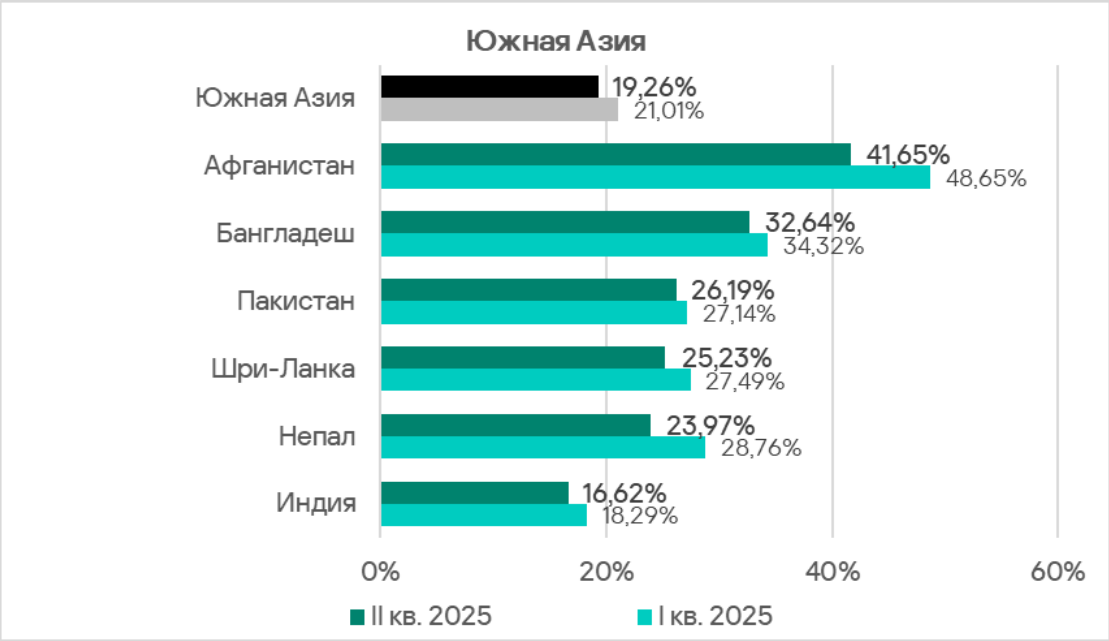
Статистика по всем угрозам

Во втором квартале 2025 года Южная Азия занимает девятое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Показатель в регионе за квартал уменьшился на 1,7 п. п. до 19,3%. Это в 1,7 раза больше, чем в Северной Европе, которая замыкает этот рейтинг.

Регион демонстрирует плавный нисходящий тренд с некоторыми колебаниями.



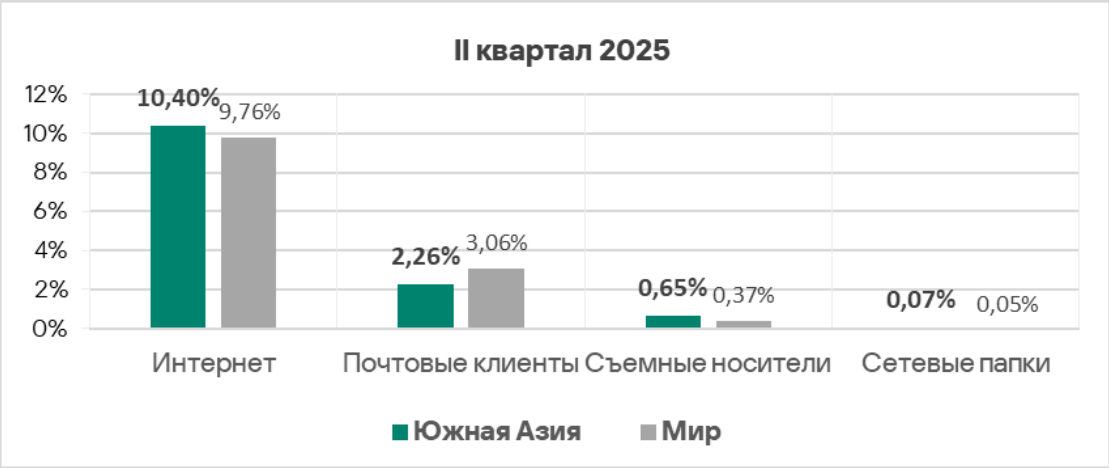
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 16,62% в Индии до 41,65% в Афганистане.



Источники угроз

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

- интернет — в 1,1 раза, третье место среди регионов;
- съемные носители — в 1,7 раза, четвертое место среди регионов;
- сетевые папки — в 1,2 раза, третье место среди регионов.



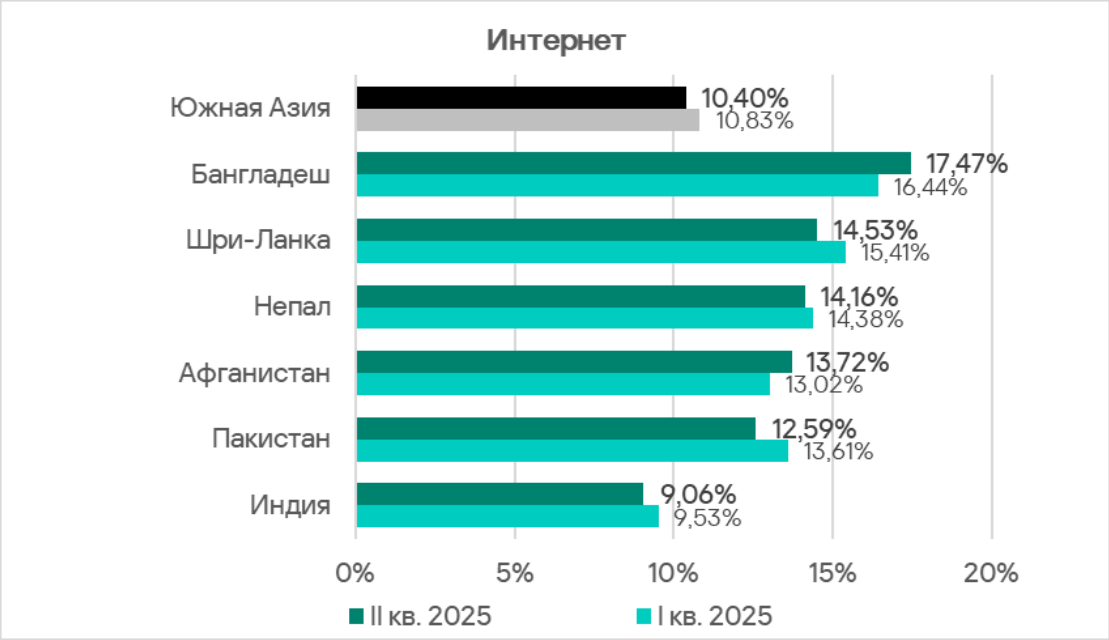
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз, кроме почтовых клиентов, где показатель вырос до 2,26%.

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

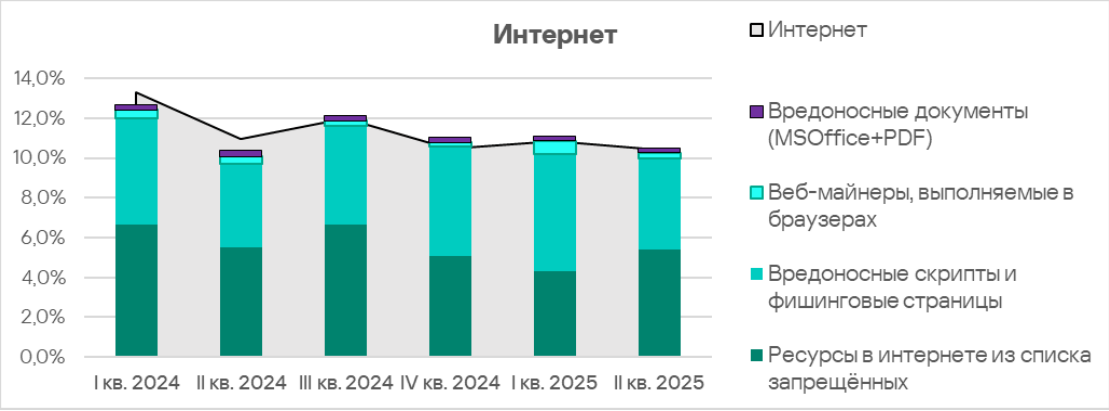
Интернет

Во втором квартале 2025 года Южная Азия по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, заняла третье место среди регионов с 10,40%. Этот показатель в 1,6 раза больше, чем в Восточной Азии, которая замыкает соответствующий рейтинг регионов. Это также наименьший показатель в регионе с третьего квартала 2022 года.

Показатели стран региона варьируют от 9,06% в Индии до 17,47% в Бангладеш.



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

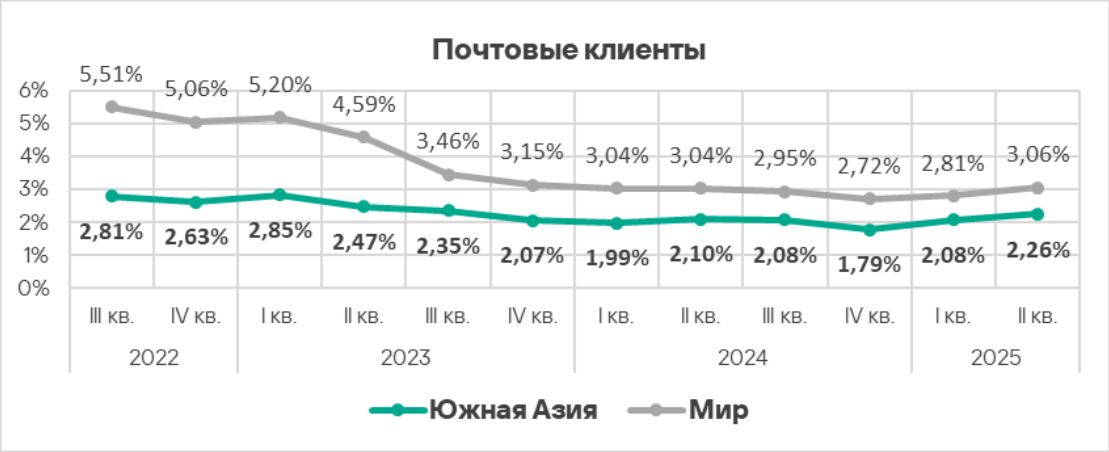


По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в регионе также лидирует Бангладеш.

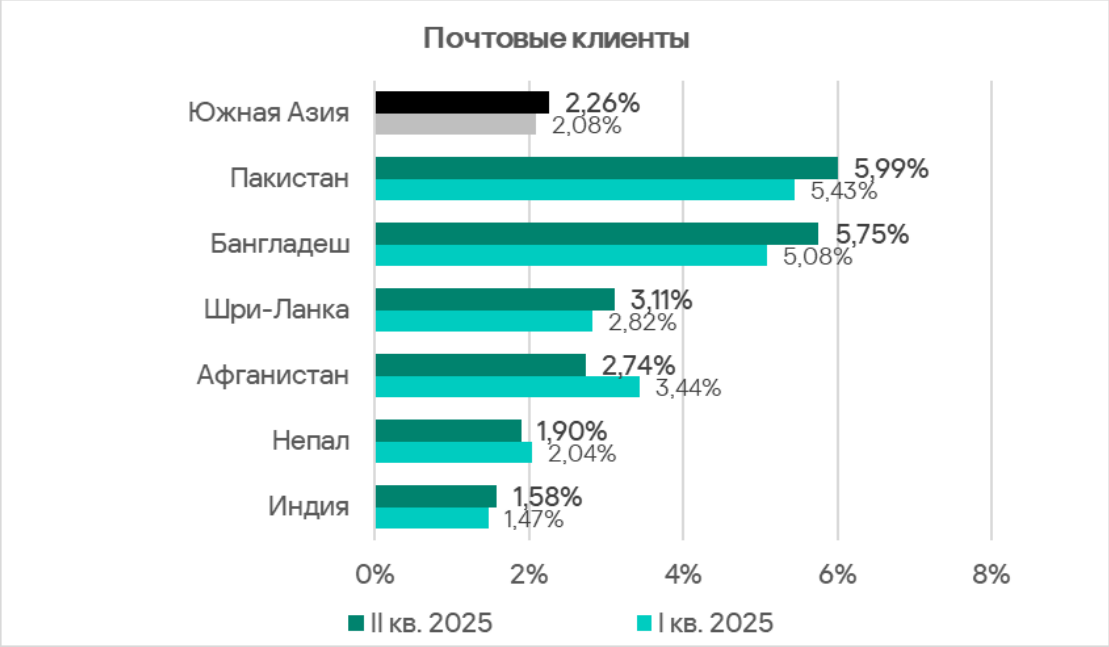
Почтовые клиенты

По доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, Южная Азия среди регионов занимает девятое место с 2,26%. Это в 2,8 раза больше, чем в России, где показатель наименьший.

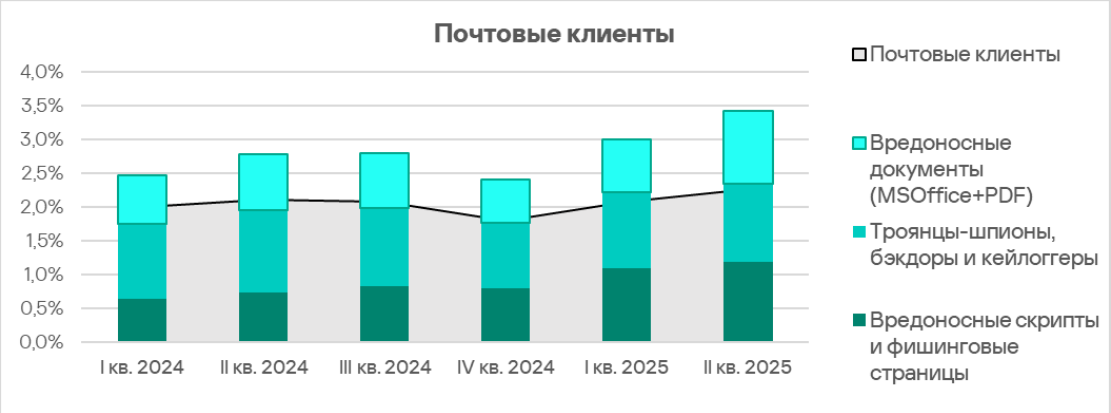
Показатель почтовых клиентов растет в регионе второй квартал подряд.



Среди стран региона по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах, лидируют Пакистан с 5,99% и Бангладеш с 5,75%. Минимальный показатель в Индии — 1,58%.



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

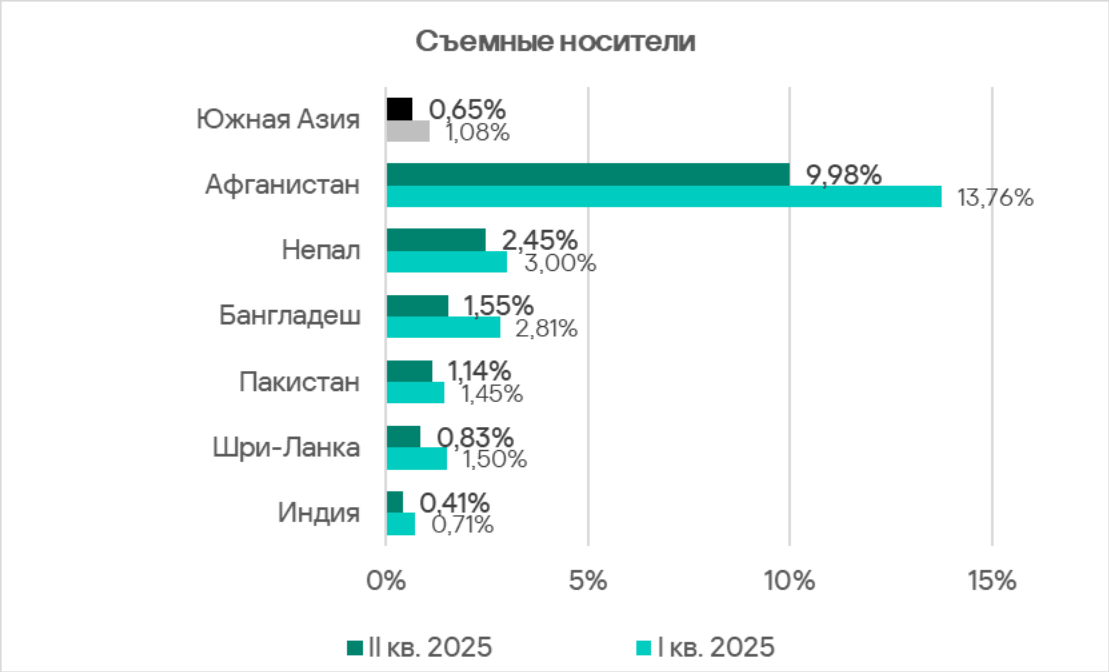


Пакистан и Бангладеш находятся среди лидеров и по показателям угроз, распространяемых преимущественно через почту, — это вредоносные документы, вредоносные скрипты и фишинговые страницы. Бангладеш лидирует еще и по шпионским программам.

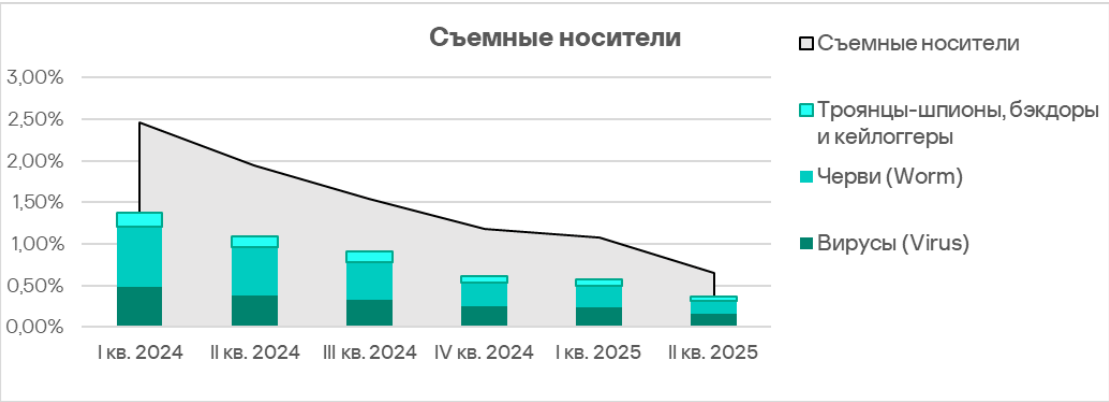
Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, Южная Азия занимает четвертое место среди регионов с 0,65%. Это в 24,4 раза больше, чем показатель в Северной Америке (Канаде), которая замыкает соответствующий рейтинг.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с большим отрывом лидирует Афганистан с 9,98%. Показатели остальных стран варьируют от 0,41% в индии до 2,45% в Непале.



Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ, — вирусы, черви и шпионское ПО. Афганистан также лидирует (и тоже с большим отрывом) по доле компьютеров АСУ, на которых были заблокированы черви.

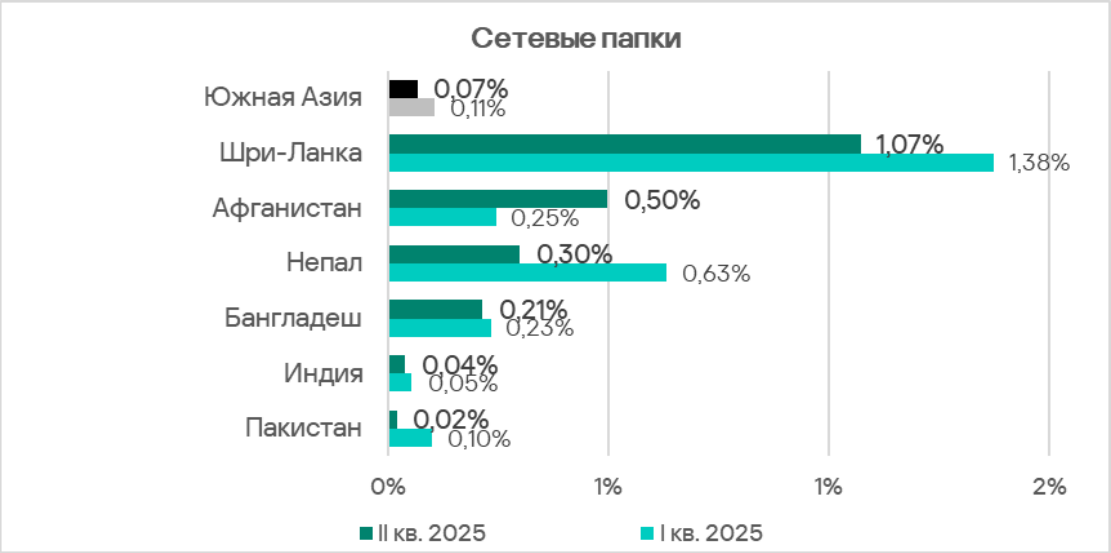


Сетевые папки

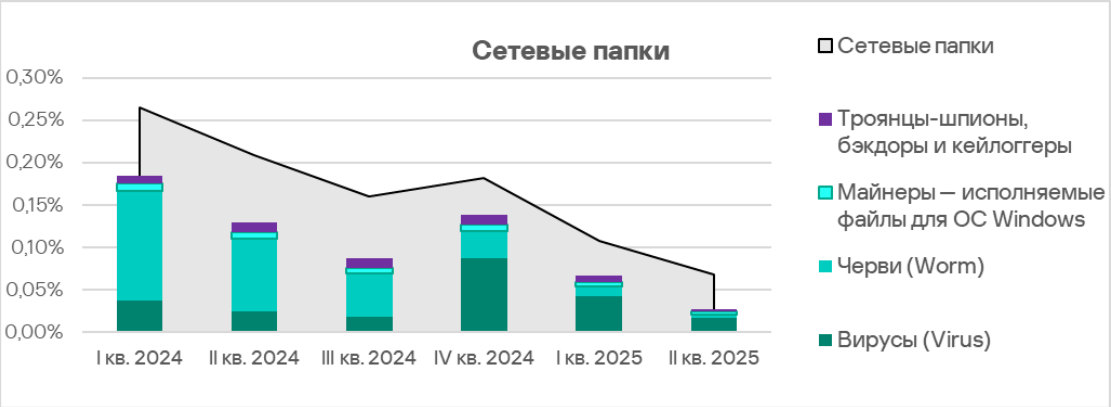
Южная Азия занимает третье место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. Во втором квартале 2025 года показатель региона (0,07%) превышает в 7 раз показатель Северной Европы, которая замыкает соответствующий рейтинг.

Высокую позицию Южной Азии в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках,

обеспечивает Шри-Ланка, которая с большим отрывом лидирует по этому показателю с 1,07%.

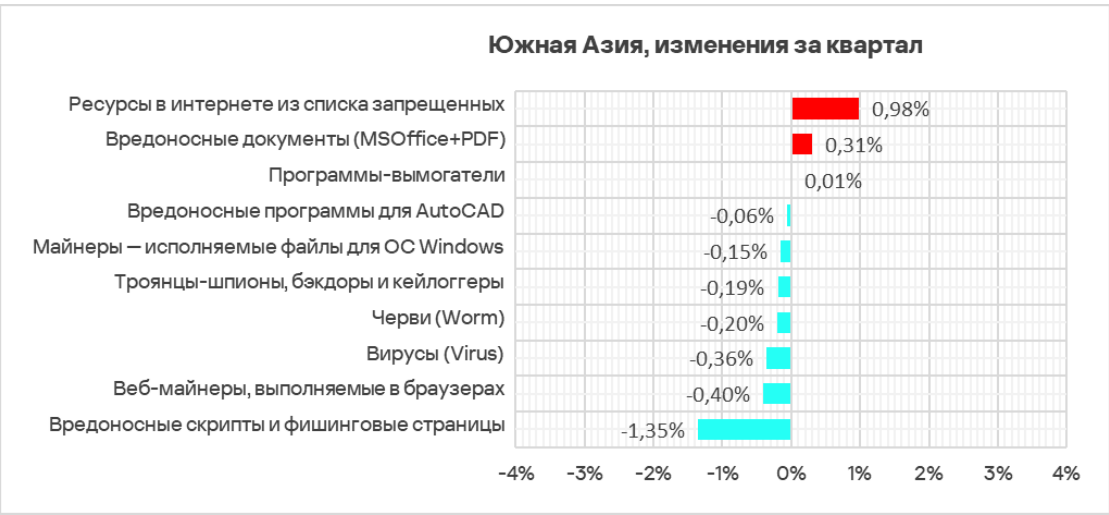


Основными категориями угроз, которые распространяются через сетевые папки, являются вирусы, черви, майнеры — исполняемые файлы для ОС Windows и шпионские программы.



Категории угроз

В Южной Азии порядок категорий в рейтинге категорий угроз соответствует среднемировому рейтингу.



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

- вирусы — в 1,1 раза;
- программы-вымогатели — в 1,4 раза, четвертое место среди регионов.

Южная Азия находится также на четвертом месте среди регионов по показателю вредоносных программ для AutoCAD.

Вирусы и вредоносные программы для AutoCAD

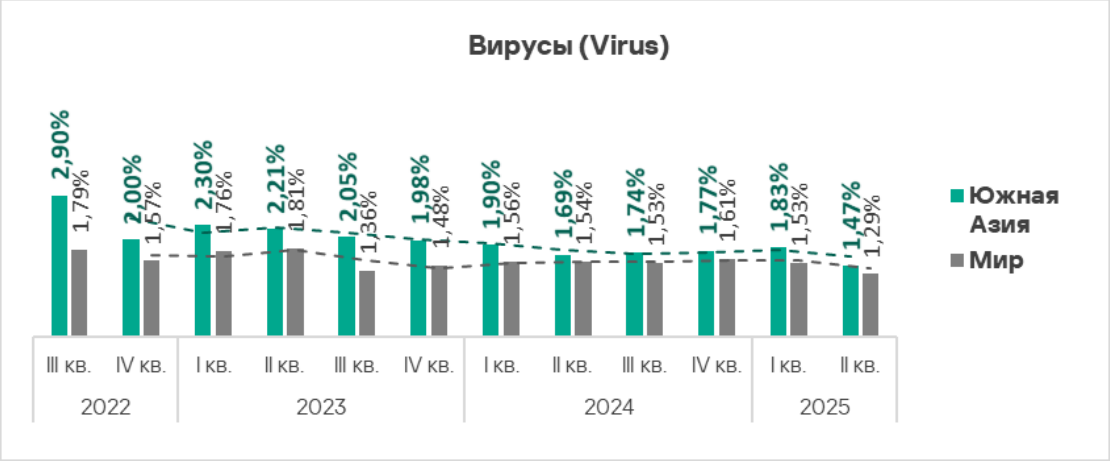
Южная Азия занимает пятое место среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, и четвертое место по показателям вредоносных программ для AutoCAD.

Во втором квартале 2025 года показатель вирусов в регионе (1,47%) в 11,6 раза больше, чем в Австралии и Новой Зеландии, где он наименьший среди регионов.

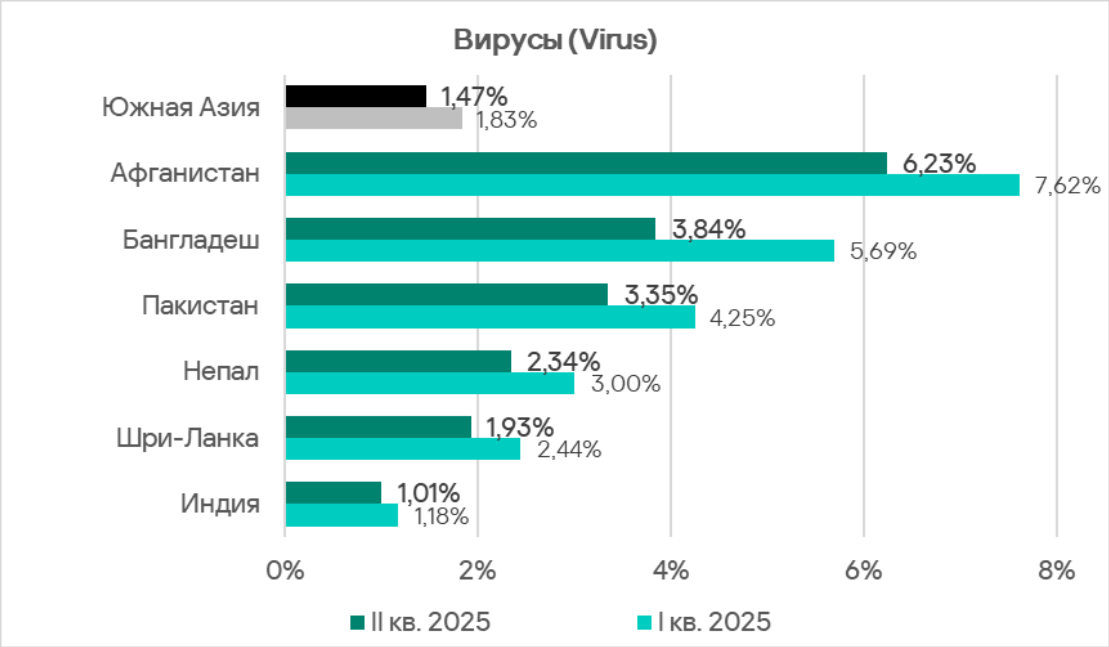
Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, в Южной Азии (0,24%) в 20 раз больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.

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

Показатель вирусов в Южной Азии колеблется с тенденцией к снижению. Во втором квартале 2025 года он был наименьшим за период с третьего квартала 2022 года.

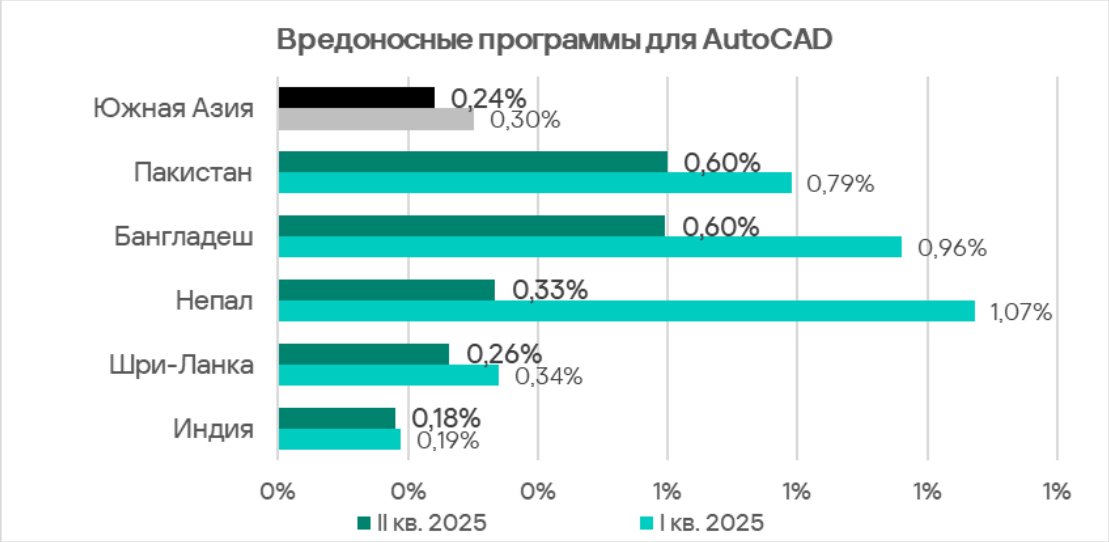


Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вирусы, лидирует Афганистан с 6,23%.



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

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, первенство держат две страны — Пакистан и Бангладеш, обе с 0,6%.

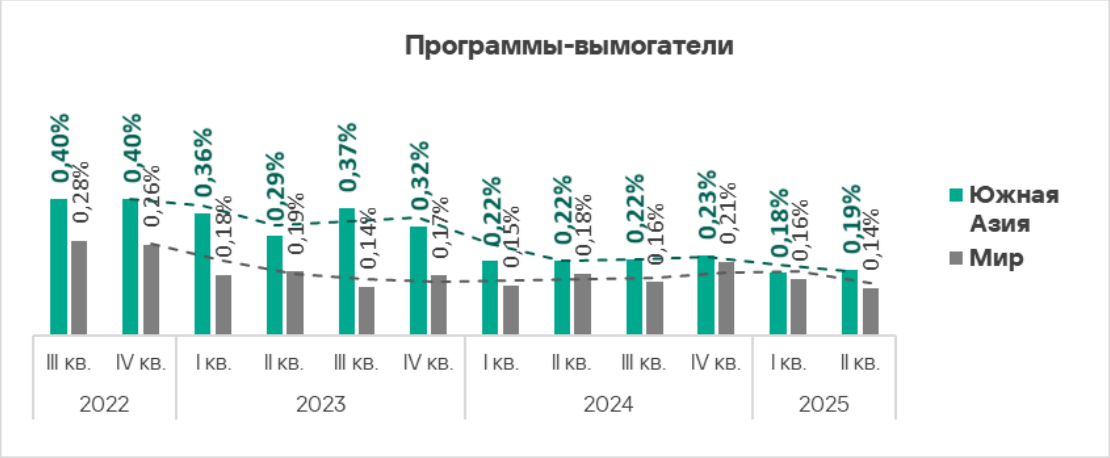


Как и вирусы, вредоносные программы для AutoCAD в регионе распространяются через все источники угроз, но преимущественно на съемных носителях.

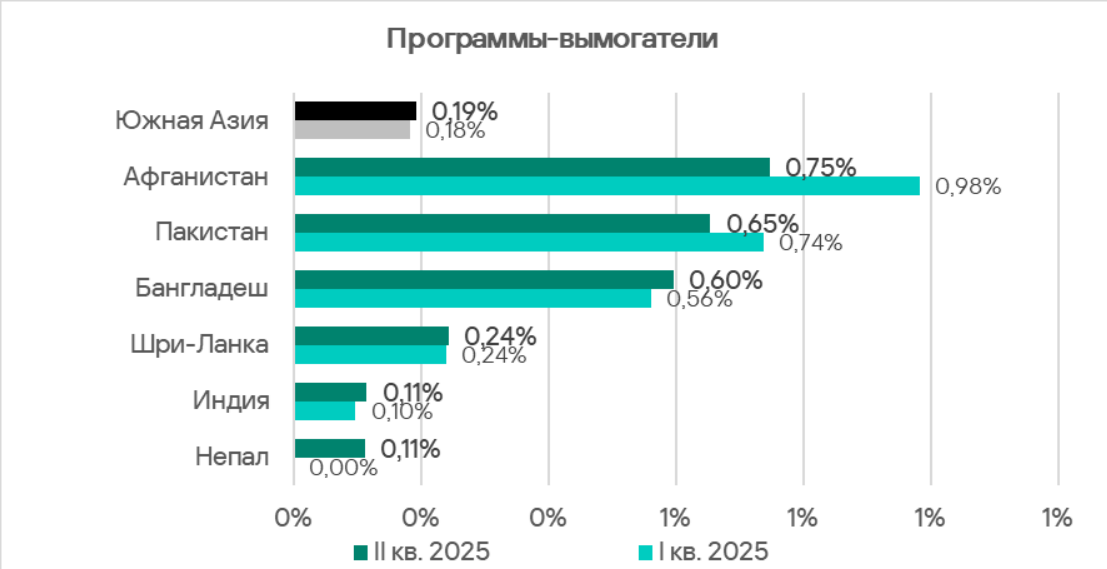
Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Южная Азия находится на четвертом месте среди регионов. Показатель в регионе (0,19%) в 3 раза выше, чем в Западной Европе, где он наименьший.

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в регионе с начала 2024 года колеблется в диапазоне от 0,18% до 0,23%. Последние два квартала показатели наименьшие за период с третьего квартала 2022 года.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы программы-вымогатели, лидирует Афганистан с 0,75%. Высокие показатели также у следующих в рейтинге Пакистана и Бангладеш (0,65% и 0,60% соответственно).

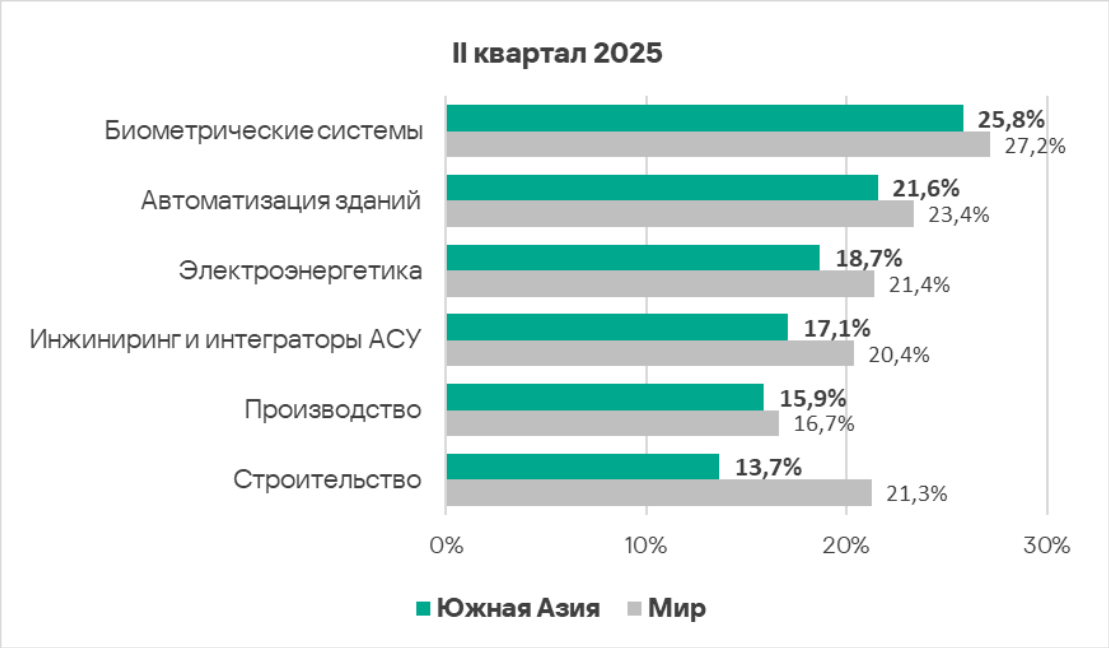


В Южной Азии программы-вымогатели распространяются через почту и — чаще всего — на съемных носителях.

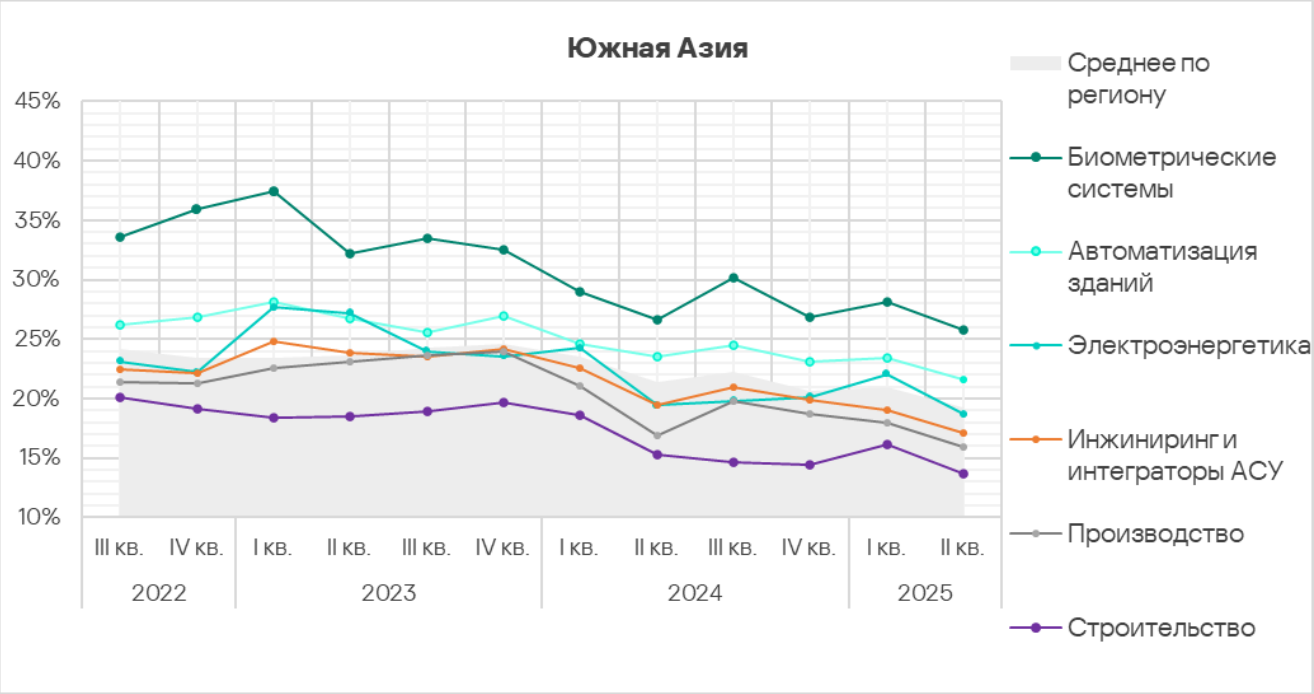
Отрасли

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

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



Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех отраслях.



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

При оценке проблем отраслей, мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение для источника или типа угроз среди всех регионов и индустрий. В Южной Азии во втором квартале 2025 года близкие к максимальным значения наблюдались для интернета и съемных носителей в биометрических системах.

На тепловых картах хорошо видны «горячие точки» отраслей — позиции источников и категорий вредоносного ПО, показатель по которым выше ожидаемого в соответствии с местом отрасли и местом угрозы или источника угрозы в соответствующих региональных рейтингах.

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	12,83%	11,14%	8,19%	10,33%	7,62%	7,70%	10,40%
Почтовые клиенты	4,68%	3,30%	2,43%	1,02%	1,62%	1,67%	2,26%
Съемные носители	1,89%	0,81%	0,25%	0,38%	0,23%	0,56%	0,65%
Сетевые папки	0,08%	0,13%	0,05%	0,02%	0,08%	0,00%	0,07%
Показатель отрасли в регионе	25,81%	21,56%	18,66%	17,10%	13,66%	15,89%	

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

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	7,32%	5,88%	4,81%	5,85%	3,67%	4,72%	5,64%
Вредоносные скрипты и фишинговые страницы	9,89%	7,80%	5,21%	5,16%	3,93%	4,65%	6,42%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,66%	3,70%	3,09%	1,59%	1,41%	2,64%	2,71%
Черви (Worm)	1,66%	1,51%	1,47%	0,71%	0,62%	1,25%	1,24%
Майнеры — исполняемые файлы для ОС Windows	0,45%	0,51%	0,25%	0,39%	0,26%	0,49%	0,51%
Вредоносные документы (MSOffice+PDF)	3,40%	2,36%	1,72%	0,88%	0,85%	0,83%	1,64%
Вирусы (Virus)	3,17%	1,77%	1,47%	0,95%	1,10%	1,46%	1,47%
Программы-вымогатели	0,53%	0,26%	0,10%	0,11%	0,00%	0,14%	0,19%
Веб-майнеры, выполняемые в браузерах	0,23%	0,32%	0,30%	0,26%	0,28%	0,21%	0,31%
Вредоносные программы для AutoCAD	0,15%	0,12%	0,15%	0,32%	0,80%	0,49%	0,24%
Показатель отрасли в регионе	25,81%	21,56%	18,66%	17,10%	13,66%	15,89%	

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

«Горячие точки» отраслей

Биометрические системы

- Лидер среди отраслей в регионе по всем источникам угроз, кроме сетевых папок (по этому источнику — третье место).

- Лидер среди отраслей в регионе по всем категориям угроз, кроме категорий: майнеры — исполняемые файлы для ОС Windows (третье место), веб-майнеры и вредоносные программы для AutoCAD.

Автоматизация зданий

- Лидер среди отраслей региона по угрозам в сетевых папках. По остальным источникам угроз — на втором месте в рейтингах.
- Лидер среди отраслей региона по показателям майнеров обеих категорий. По всем остальным категориям, кроме вредоносных программ для AutoCAD, — на втором месте.

Электроэнергетика

- Третье место в регионе среди отраслей по показателю угроз в почтовых клиентах. Четвертое место по угрозам из интернета и угрозам в сетевых папках.
- Второе место в регионе среди отраслей по показателю веб-майнеров.
- Третье место среди отраслей региона по показателям в следующих категориях: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, вирусы, черви.
- Четвертое место в регионе по показателю вредоносных программ для AutoCAD.

Инжиниринг и интеграторы АСУ

- Третье место в регионе среди отраслей по показателю угроз из интернета, четвертое место по съемным носителям.
- Третье место в регионе среди отраслей по показателю в следующих категориях: ресурсы в интернете из списка запрещенных, вредоносные программы для AutoCAD.
- Четвертое место в регионе по показателю в следующих категориях: вредоносные скрипты и фишинговые страницы, вредоносные документы, майнеры обеих категорий и вредоносные программы для AutoCAD.

Производство

- Третье место среди отраслей региона по угрозам на съемных носителях, четвертое место по показателю угроз из почтовых клиентов.
- Второе место среди отраслей региона по показателю в следующих категориях: майнеры — исполняемые файлы для ОС Windows, вредоносные программы для AutoCAD.
- Третье место в регионе по показателю программ-вымогателей.

- Четвертое в регионе по показателю шпионских программ, вирусов и червей.

Строительство

- Второе место среди отраслей в регионе по показателю угроз в сетевых папках.
- Лидер среди отраслей в регионе по показателю вредоносных программ для AutoCAD.
- Третье место в регионе по показателю веб-майнеров.

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