Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первый квартал 2026 года

09.06.2026

Версия 1.0

Итоги квартала

Цифры

Показатель	IV кв. 2025	I кв. 2026	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	19,7%	19,6%	▼0,1 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	6,58%	6,56%	▼0,02 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,80%	3,73%	▼0,07 п. п.
Ресурсы в интернете из списка запрещенных	3,26%	3,54%	▲0,28 п. п.
Вредоносные документы (MSOffice+PDF)	1,76%	1,56%	▼0,20 п. п.
Черви (Worm)	1,60%	1,33%	▼0,27 п. п.
Вирусы (Virus)	1,33%	1,31%	▼0,02 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,60%	0,59%	▼0,01 п. п.
Вредоносные программы для AutoCAD	0,29%	0,30%	▲0,01 п. п.
Веб-майнеры, выполняемые в браузерах	0,24%	0,22%	▼0,02 п. п.
Программы-вымогатели	0,16%	0,14%	▼0,02 п. п.
Основные источники угроз			
Интернет	7,67%	7,88%	▲0,21 п. п.
Почтовые клиенты	2,76%	2,59%	▼0,17 п. п.
Съемные носители	0,31%	0,26%	▼0,05 п. п.
Сетевые папки	0,04%	0,03%	▼0,01 п. п.

Все угрозы

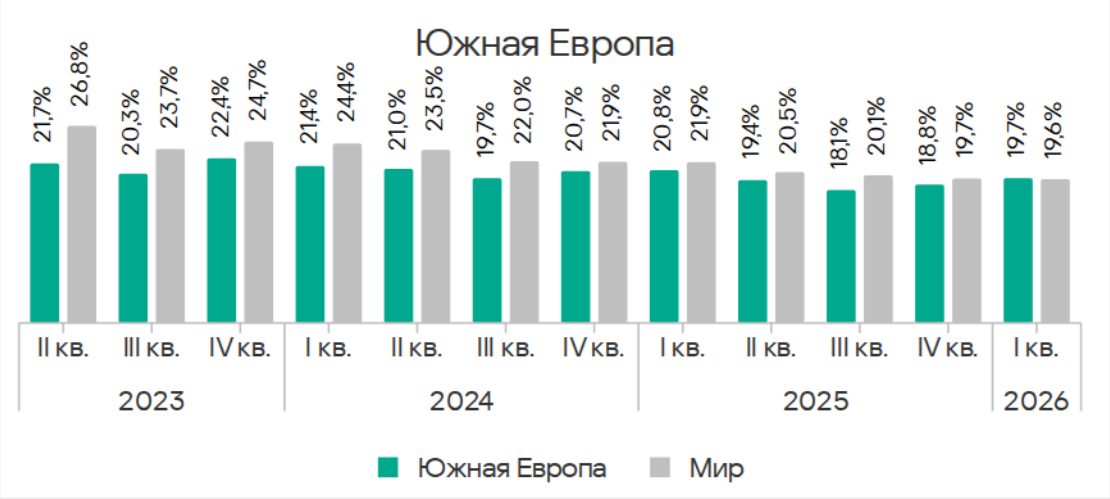
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, продолжила снижаться и в первом квартале 2026 года составила 19,6%. Это наименьший показатель за три года, и он в 1,4 раза меньше, чем во втором квартале 2023 года.

Показатели в регионах варьируют от 9,1% в Северной Европе до 27,4% в Африке. Разница максимального и минимального показателей в регионах довольно значительная: в Африке он в 3,0 раза больше, чем в Северной Европе (см. диаграмму в разделе «Основная статистика. Все угрозы»).

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал увеличилась в пяти регионах, больше всего — в Южной Европе, Северной Европе и России.

В **Южной Европе** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, росла два квартала подряд и впервые за период наблюдений оказалась чуть выше среднемирового значения.

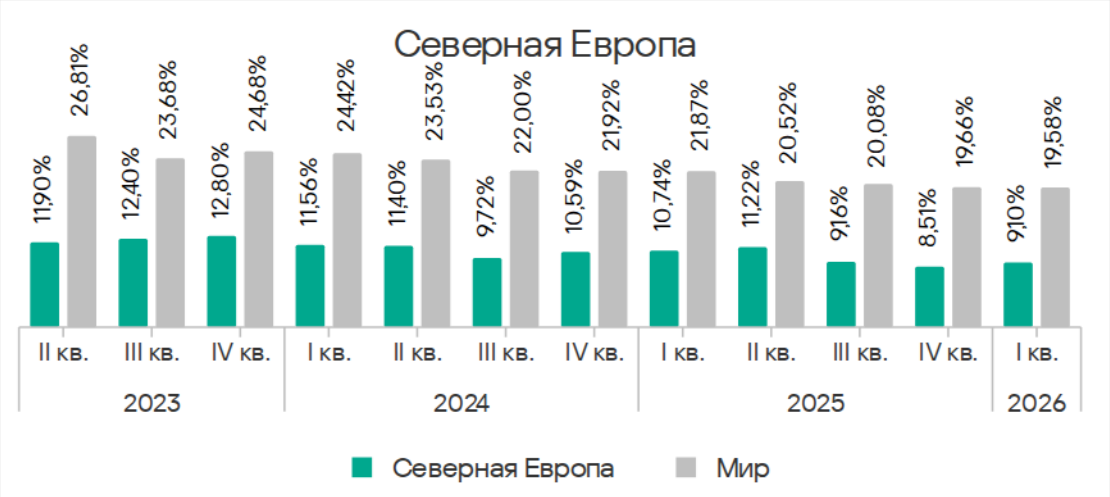
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Южной Европе, II квартал 2023 года — I квартал 2026 года



В первом квартале 2026 года Южная Европа заняла первое место по росту показателей угроз из интернета и почтовых клиентов. Регион находится на первом месте и по росту показателя шпионских программ, а также вредоносных скриптов и фишинговых страниц.

Для **Северной Европы,** которая традиционно замыкает рейтинг регионов, рост показателя на 0,6 п. п. означает, что количество атакованных компьютеров АСУ в регионе увеличилось на 7%.

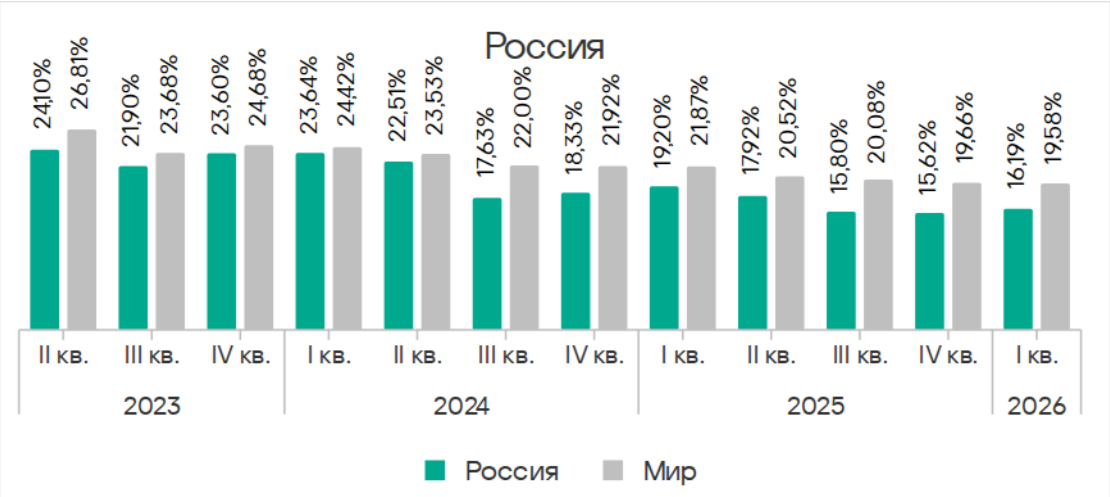
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Северной Европе, II квартал 2023 года — I квартал 2026 года



В Северной Европе увеличились показатели угроз из интернета и четырех категорий угроз: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы (второе место среди регионов по росту показателя), шпионские программы и программы-вымогатели (один из двух регионов, где значение выросло).

В **России** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превысила показатели предыдущих двух кварталов.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в России, II квартал 2023 года — I квартал 2026 года



В России вырос показатель угроз из интернета, и немного выросло значение у угроз из почтовых клиентов (Россия — один из трех регионов, где этот показатель не уменьшился).

Среди категорий угроз больше всего показатель вырос у ресурсов в интернете из списка запрещенных, а также у шпионских программ (распространяются в регионе через интеренет и почтовые клиенты).

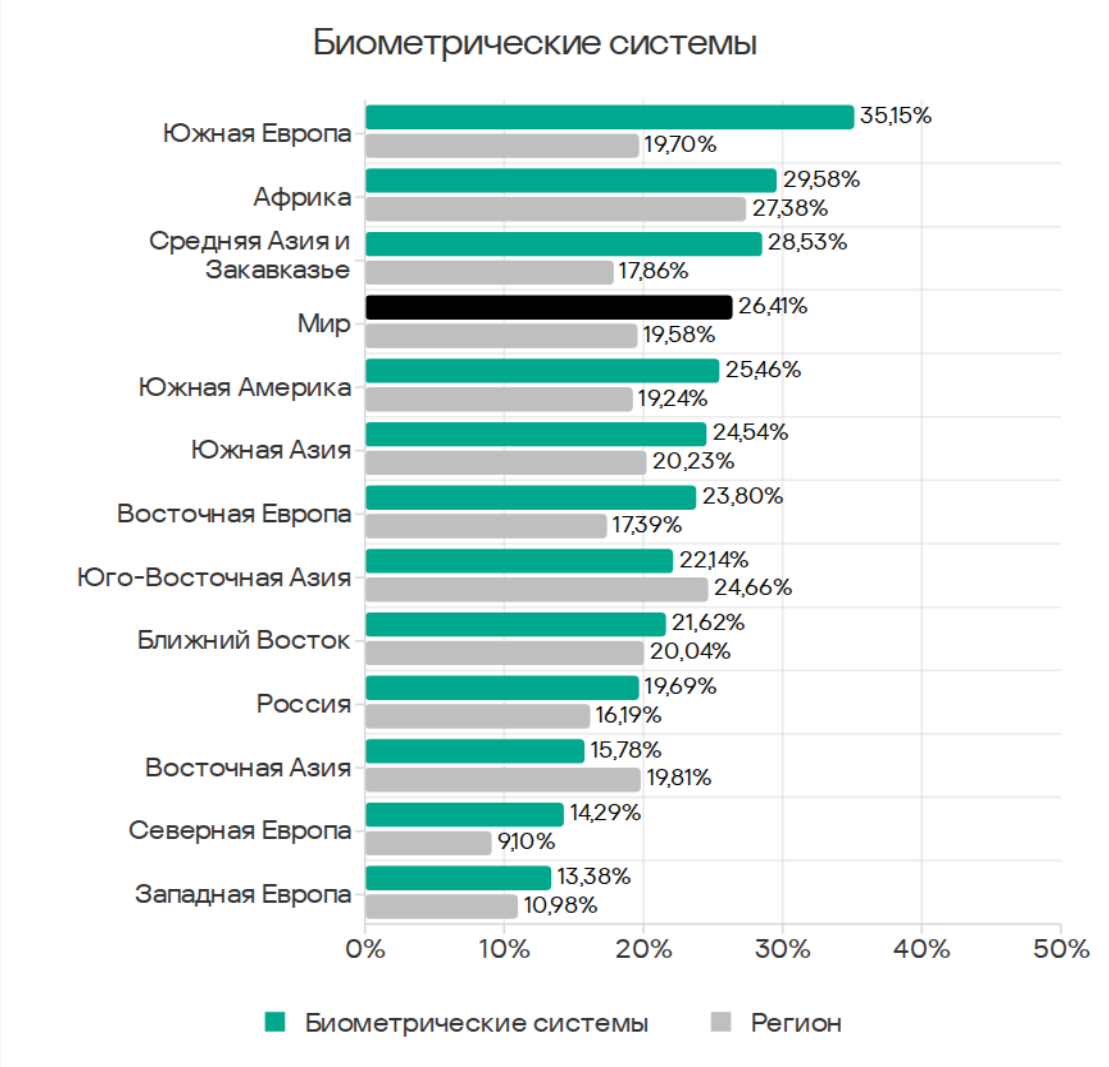
Исследуемые отрасли

Рейтинг исследуемых отраслей и типов OT-инфраструктур по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, традиционно возглавляют биометрические системы с показателем 26,4%. Для этих систем характерны доступность интернета, активное использование электронной почты и, зачастую, минимальный контроль ИБ со стороны организации-потребителя.

Биометрические системы находятся на первом месте среди отраслей по показателям угроз из почты. При этом, в отличие от остальных отраслей, у биометрических систем показатель почтовых клиентов превышает показатель угроз из интернета.

Среди регионов по показателю биометрических систем лидирует Южная Европа с 35,15%. Она же занимает первое место по показателю угроз из почтовых клиентов.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в биометрических системах, I квартал 2026 года



Во всех исследуемых отраслях наблюдается тенденция к уменьшению среднемирового показателя.

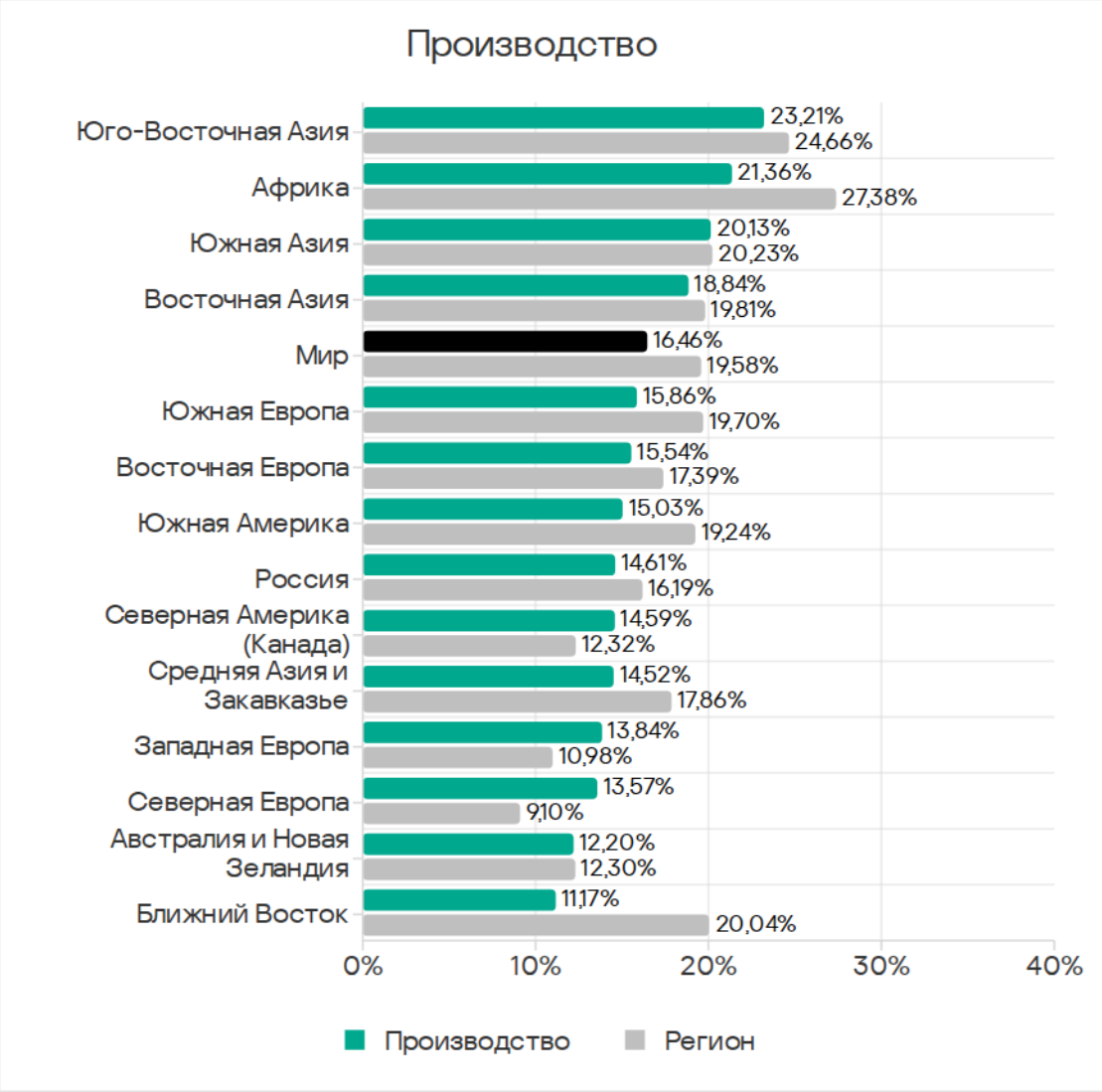
В первом квартале 2026 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась только в производственной отрасли — на 1 п. п.

Производственная отрасль в первом квартале 2026 года

Среди регионов по доле атакованных компьютеров АСУ в производственной отрасли первое место занимает Юго-Восточная Азия.

В Восточной Азии, Западной и Северной Европе, в регионе Средняя Азия и Закавказье значение в производственной отрасли превышает показатель региона в целом.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в производстве, I квартал 2026 года



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты в производстве, I квартал 2026 года

Показатель производственной отрасли увеличился в десяти регионах, больше всего — в Западной Европе, Северной Европе и России.

В этих трех регионах в производственной отрасли больше всего (в процентных пунктах) увеличилась доля компьютеров АСУ, на которых блокировались вредоносные скрипты и ресурсы в интернете из списка запрещенных.

Кроме того, в Западной Европе и России в производственной отрасли выросли показатели шпионских программ (в Западной Европе — в 1,36 раза, России — в 1,50 раза).

К тому же, в России в производственной отрасли увеличился показатель программ-вымогателей — 2,5 раза, а в Западной Европе — майнеров в формате исполняемых файлов — в 2,35 раза.

Категории вредоносных объектов

В первом квартале 2026 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 10 052 семейств, относящихся к различным категориям.

За квартал выросла доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных (предыдущие два квартала показатель снижался), и немного выросло значение у вредоносных программ для AutoCAD.

Вредоносные скрипты и фишинговые страницы (JS и HTML)

Вредоносные скрипты и фишинговые страницы сохранили за собой первое место в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. В первом квартале 2026 года среднемировой показатель составил 6,56%.

В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, варьирует от 2,73% в Северной Европе до 9,85% в Южной Европе.

За квартал показатель вырос в четырех регионах. Самое значительное изменение отмечено в **Южной Европе.** Показатель вредоносных скриптов там рос три квартала подряд.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты в Южной Европе, II квартал 2023 года — I квартал 2026 года

Среди исследуемых отраслей в Южной Европе наибольший показатель вредоносных скриптов — у биометрических систем и автоматизации зданий. За квартал значение увеличилось во всех исследуемых отраслях в регионе.

Среди исследуемых отраслей во всех регионах самые высокие показатели категории вредоносные скрипты и фишинговые страницы — в Южной Европе у биометрических систем (19,59%) и автоматизации зданий (15,43%). Эти же отрасли лидируют в аналогичных рейтингах по показателям вредоносных документов и шпионских программ.

Программы-шпионы

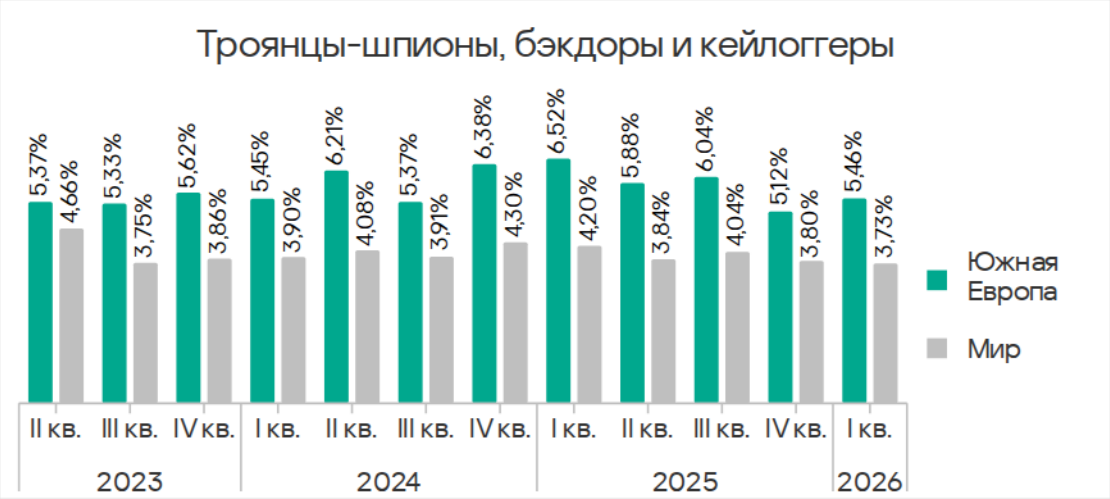
В мире доля компьютеров АСУ, на которых было заблокировано шпионское ПО, уменьшалась в течение двух кварталов подряд и достигла 3,73%. Несмотря на снижение показателя, шпионские программы уже три квартала занимают второе место в рейтинге категорий угроз по доле атакованных компьютеров.

В регионах доля компьютеров АСУ, на которых было заблокировано шпионское ПО, варьирует от 1,34% в Северной Европе до 5,94% в Африке. Южная Европа в соответствующем рейтинге потеснила со второго места Юго-Восточную Азию.

За квартал показатель вырос в пяти регионах, больше всего — в Южной Европе и России (см. раздел «Вредоносное ПО следующего этапа. Программы-шпионы»).

Южная Европа в рейтинге по показателю шпионских программ занимает второе место после Африки с 5,46%. На компьютеры АСУ шпионские программы в регионе попадают премущественно через почтовые клиенты.

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в Южной Европе, II квартал 2023 года — I квартал 2026 года



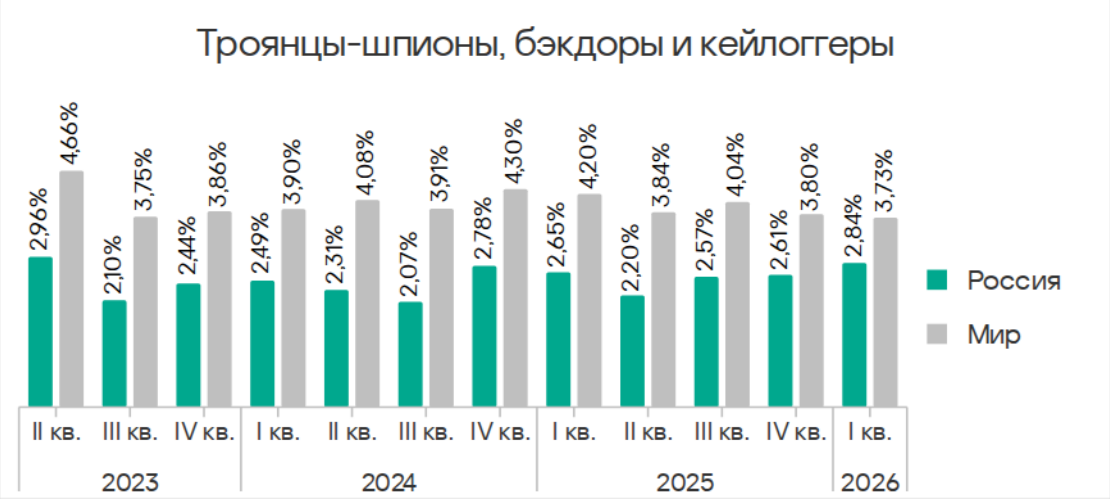
Напомним, что Южная Европа занимает первое место среди регионов и по показателю, и по росту показателя вредоносных скриптов, которые применяются в том числе для заражения компьютеров шпионскими программами.

В Южной Европе среди исследуемых отраслей доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла во всех отраслях, кроме производства. Больше всего показатель увеличился у биометрических систем.

В России доля компьютеров АСУ, на которых были заблокированы шпионские программы, росла в течение трех кварталов подряд, по сравнению со вторым кварталом 2025 года значение увеличилось в 1,3 раза — до 2,84%. За три года показатель был выше только во втором квартале 2023 года.

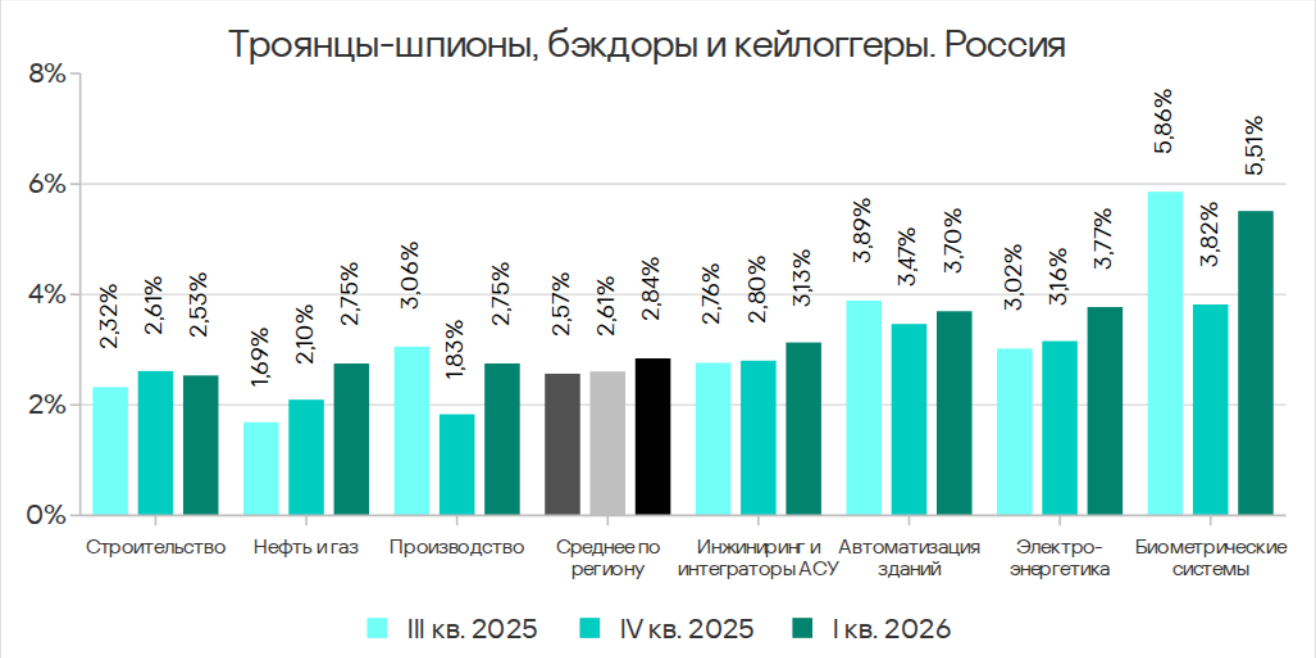
Шпионские программы распространяются в регионе через интернет и почту.

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в России, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей в России самый высокий показатель шпионских программ — у биометрических систем.

Доля компьютеров АСУ, на которых блокировались шпионские программы, в России выросла во всех отраслях, кроме строительства. Два квартала подряд показатель рос в нефтегазовой отрасли (за полгода он увеличился в 1,63 раза), три квартала — в отраслях инжиниринг и интеграторы АСУ и электроэергетика. В остальных секторах значения колеблются.



Доля компьютеров АСУ, на которых были заблокированы шпионские программы в различных отраслях в России, III квартал 2025 года — I квартал 2026 года

Шпионские программы зачастую используются в том числе для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели. Отметим, что в России показатель программ-вымогателей вырос во всех исследуемых отраслях, кроме нефтегазовой и автоматизации зданий.

Среди исследуемых отраслей во всех регионах самые высокие показатели шпионских программ также — в Южной Европе — у биометрических систем (17,48%) и автоматизации зданий (9,57%). Эти же отрасли лидируют в аналогичных рейтингах по показателям вредоносных скриптов и вредоносных документов.

Ресурсы в интернете из списка запрещенных

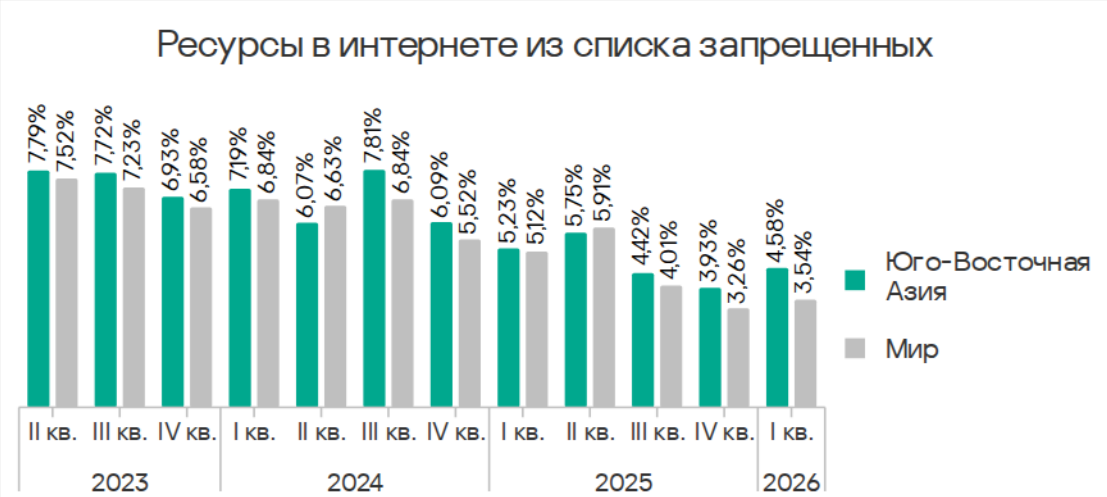
Ресурсы в интернете из списка запрещенных занимают третье место в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

В мире доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, выросла до 3,54%. Тем не менее, это значение меньше, чем остальные квартальные показатели за три года.

В регионах доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, варьирует от 2,06% в Северной Европе до 4,58% в Юго-Восточной Азии.

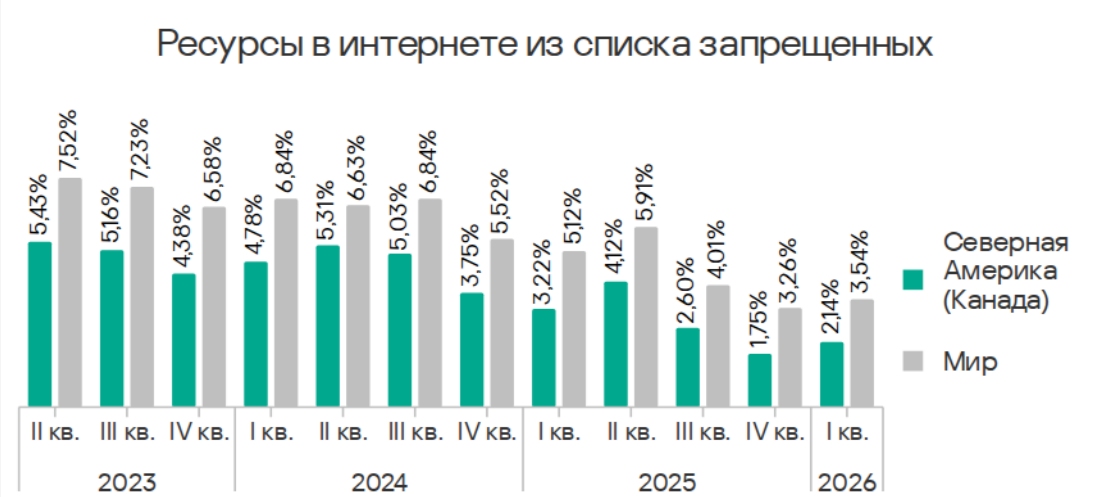
Больше всего показатель за квартал увеличился в **Юго-Восточной Азии.** Среди отраслей в регионе самые высокие показатели угроз этой категории — в электроэнергетике и строительстве. За квартал показатели больше всего выросли в электроэнергетической и производственной отраслях.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных в Юго-Восточной Азии, II квартал 2023 года — I квартал 2026 года



В **Северной Америке (Канада)** рост показателя ресурсов в интернете из списка запрещенных по темпу роста был наибольшим среди всех категорий: значение выросло в 1,22 раза.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных в Северной Америке (Канада), II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей во всех регионах самые высокие показатели категории ресурсы в интернете из списка запрещенных — в Юго-Восточной Азии в электроэнергетической (7,11%) и строительной (6,25%) отраслях.

Отметим, что электроэнергетика и строительство в Юго-Восточной Азии, в Центральной Азии и Закавказье, в Африке, электроэнергетика в России и строительство в Восточной Европе занимают восемь первых мест в рейтинге отраслей во всех регионах по доле компьютеров АСУ, на которых

блокируются ресурсы в интернете из списка запрещенных в различных отраслях.

Вредоносные документы (MSOffice+PDF)

Вредоносные документы находятся на четвертом месте в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

Показатель этой категории снижался два квартала подряд и в первом квартале 2026 года оказался наименьшим за исследуемый период — 1,56%.

В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные документы, варьирует от 0,43% в Северной Европе до 3,14% в Южной Европе. Ближний Восток в этом рейтинге поднялся с четвертого на второе место.

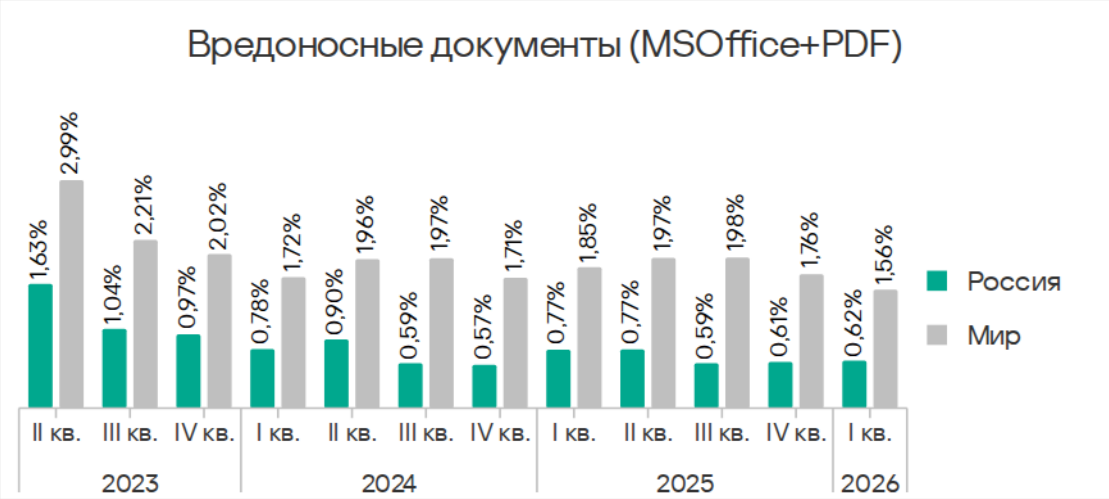
Показатель за квартал увеличился только в двух регионах — в Австралии и Новой Зеландии и в России, да и то незначительно.

В **Австралии и Новой Зеландии** значение за первый квартал 2026 года — одно из наименьших за три года.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в Австралии и Новой Зеландии, II квартал 2023 года — I квартал 2026 года

В **России** значение росло второй квартал подряд.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в России, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей во всех регионах самые высокие показатели вредоносных документов — в Южной Европе у биометрических систем (9,02%) и автоматизации зданий (6,97%). Эти же отрасли лидируют в аналогичных рейтингах по показателям вредоносных скриптов и шпионских программ.

Программы-вымогатели

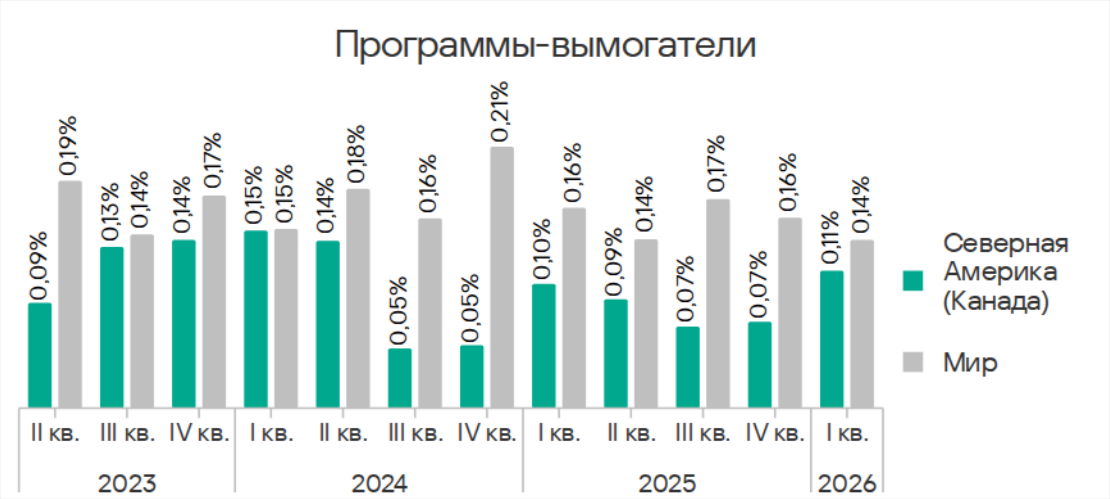
В мире в первом квартале 2026 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, уменьшалась два квартала подряд и достигла 0,14%. Это наименьшее значение из показателей всех категорий.

В регионах доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, варьирует от 0,06% в Австралии и Новой Зеландии до 0,26% на Ближнем Востоке.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, выросла в двух регионах: в Северной Америке (Канада) и немного в Северной Европе (на 0,01 п. п.).

Северная Америка (Канада) поднялась в соответствующем рейтинге регионов с предпоследнего на седьмое место с 0,11%. В регионе программы-вымогатели распространяются преимущественно через почтовые клиенты.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в Северной Америке (Канада), II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей в Северной Америке (Канада) программы-вымогатели были заблокированы в отраслях автоматизация зданий (0,16%) и строительство (0,09%).

В **Северной Европе** показатели программ-вымогателей увеличились во всех иследуемых отраслях.

Отметим, что в **России** доля компьютеров АСУ, на которых блокировались программы-вымогатели, выросла во всех исследуемых отраслях, кроме нефтегазовой отрасли и автоматизации зданий. Больше всего значение увеличилось в производственной отрасли — в 2,3 раза.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в различных отраслях в России, III квартал 2025 года — I квартал 2026 года

Среди исследуемых отраслей во всех регионах самые высокие показатели программ-вымогателей были в Средней Азии и Закавказье в нефтегазовой и производственной отраслях (0,92% и 0,65% соответственно) и в России у биометрических систем (0,89%).

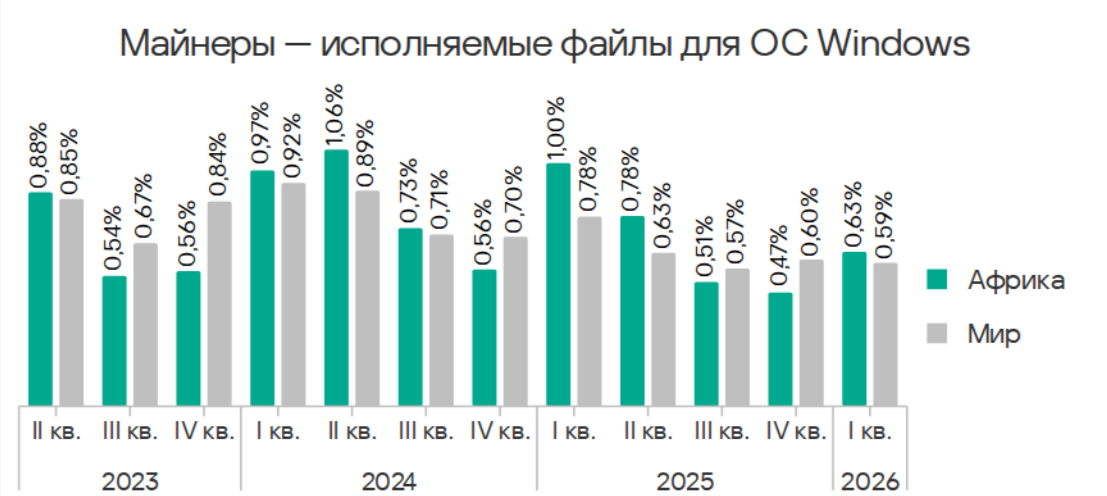
Майнеры — исполняемые файлы для ОС Windows

В мире в первом квартале 2026 года доля компьютеров АСУ, на которых были заблокированы майнеры в формате исполняемых файлов для Windows, уменьшилась до 0,59%.

В регионах показатель варьирует от 0,14% в Австралии и Новой Зеландии до 1,12% в Средней Азии и Закавказье. В тройке лидеров Африка потеснила с третьего места Восточную Европу. Россия с 0,82% по-прежнему занимает второе место.

Показатель увеличился в семи регионах (см. раздел «Вредоносное ПО следующего этапа. Майнеры — исполняемые файлы для ОС Windows»). Больше всего — в **Африке.** В исследуемых отраслях в регионе больше всего значение увеличилось в производственной и нефтегазовой отраслях.

Доля компьютеров АСУ, на которых были заблокированы майнеры в формате исполняемых файлов в Африке, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей во всех регионах самые высокие показатели майнеров в формате исполняемых файлов — в Средней Азии и Закавказье. В топ-10 отраслей по этому показателю попали все исследуемые отрасли в регионе, кроме сектора инжиниринг и интеграторы АСУ. На верхних строчках — строительство (1,99%), биометрические системы (1,98%) и нефтегазовая отрасль (1,97%).

Веб-майнеры

В мире доля компьютеров АСУ, на которых были заблокированы веб-майнеры, уменьшается уже год и в первом квартале 2026 года она

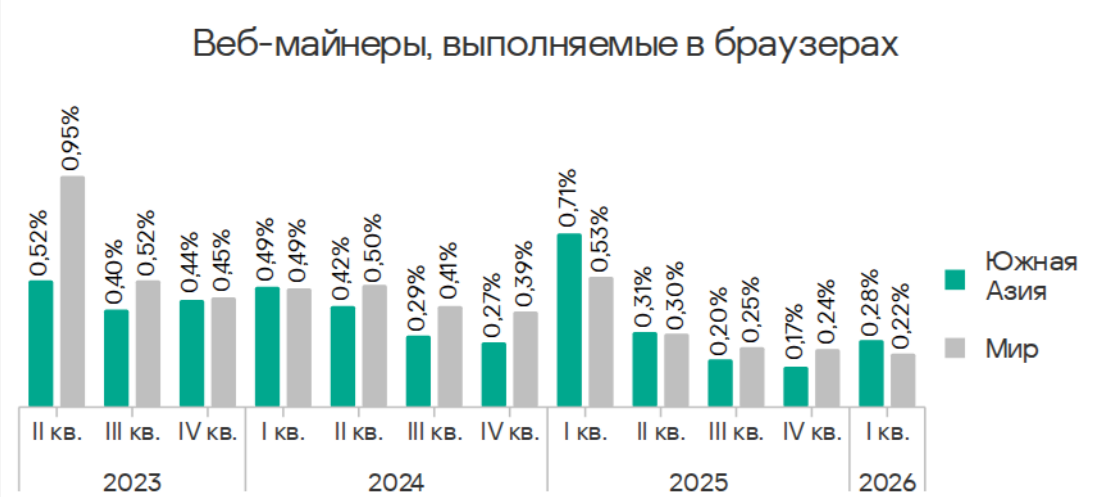
опустилась до минимального значения за рассматриваемый период — 0,22%.

В регионах показатель варьирует от 0,06% в Восточной Азии до 0,34% в Африке.

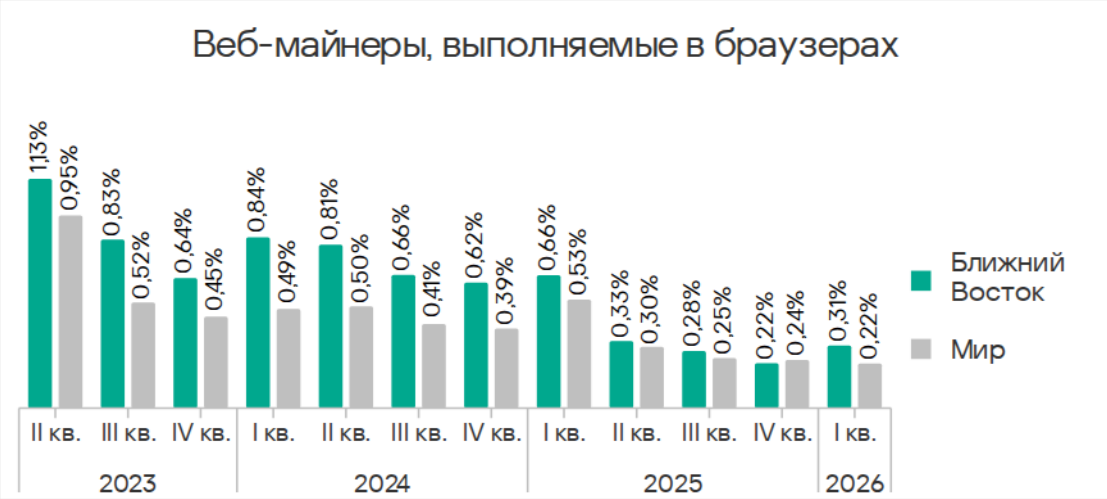
Африка в первом квартале 2026 года поднялась в соответствующем рейтинге регионов с третьего на первое место, Ближний Восток — с шестого на второе место.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, больше всего увеличилась в **Южной Азии** (в 1,6 раза), на **Ближнем Востоке** (в 1,4 раза) и в **Африке** (в 1,3 раза). Несмотря на рост, в этих регионах показатели за первый квартал 2026 года не превысили значений, которые наблюдались в 2023—2024 годах и в первом квартале 2025 года.

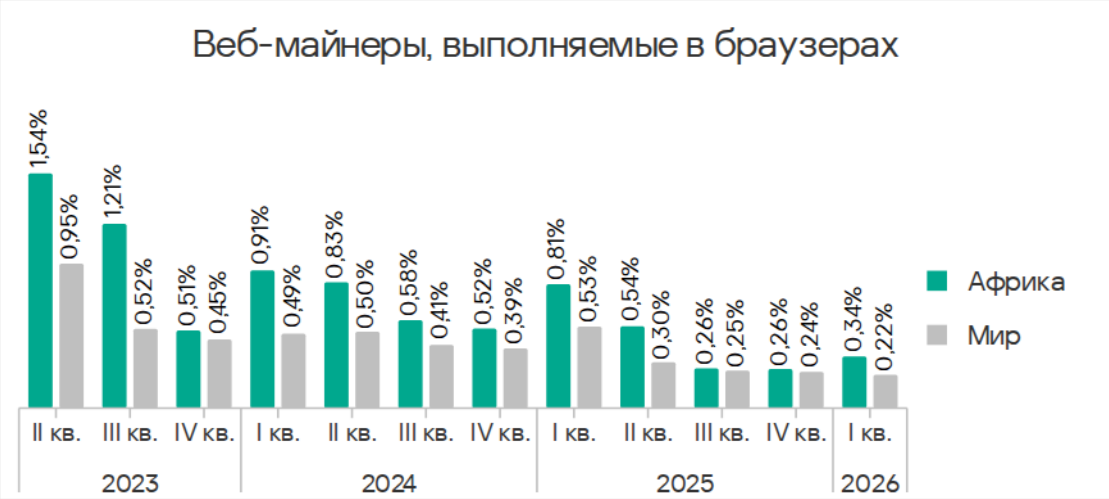
Доля компьютеров АСУ, на которых были заблокированы веб-майнеры в Южной Азии, II квартал 2023 года — I квартал 2026 года



Доля компьютеров АСУ, на которых были заблокированы веб-майнеры на Ближнем Востоке, II квартал 2023 года — I квартал 2026 года



Доля компьютеров АСУ, на которых были заблокированы веб-майнеры в Африке, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей во всех регионах самые высокие показатели веб-майнеров оказались в России у биометрических систем (0,97%). На втором месте — биометрические системы в Южной Азии (0,79%), на третьем — электроэнергетика в Юго-Восточной Азии (0,76%).

Черви

В мире доля компьютеров АСУ, на которых были заблокированы черви, в первом квартале 2026 года уменьшилась до 1,33%.

После роста показателя в предыдущем квартале (из-за очередной волны фишинговых атак, в ходе которых во всех регионах мира распространялся червь-бэкдор Backdoor.MSIL.XWorm) значение уменьшилось во всех регионах.

Показатель в регионах варьирует от 0,21% в Австралии и Новой Зеландии до 3,26% в Африке.

Среди исследуемых отраслей в регионах самые высокие показатели червей — в Центральной Азии и Закавказье у биометрических систем (4,80%). Второе и третье места по этому показателю занимают отрасли в Африке — биометрические системы (4,04%) и электроэнергетика (3,53%).

Вирусы

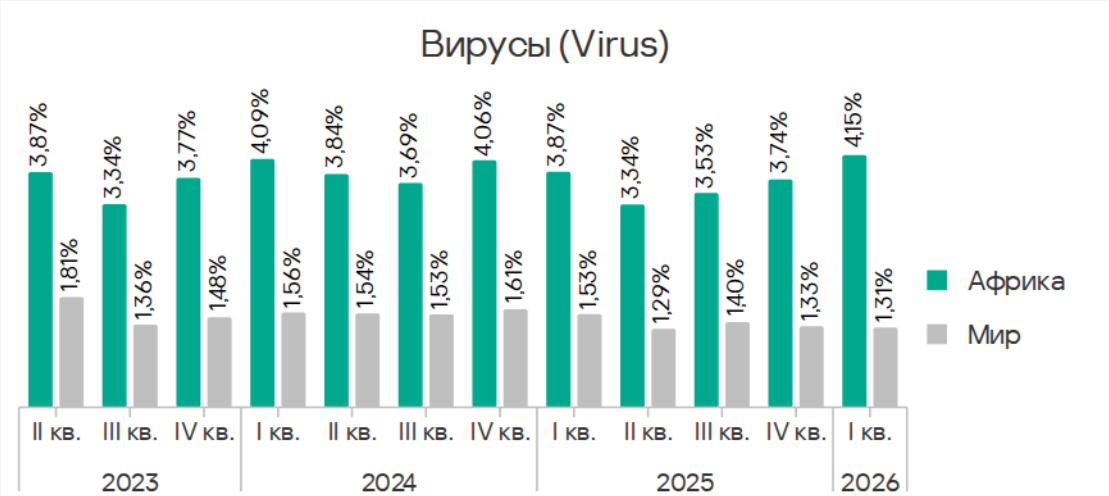
В мире доля компьютеров АСУ, на которых были заблокированы вирусы, в первом квартале 2026 года уменьшилась до 1,31%.

В регионах показатель варьирует от 0,13% в Австралии и Новой Зеландии до 6,11% в Юго-Восточной Азии. Топ-3 регионов по этому показателю не изменился: Юго-Восточная Азия (с большим отрывом от остальных), Африка и Восточная Азия. Эти же регионы входят в список лидеров и в случае вредоносных программ для AutoCAD.

Больше всего показатель увеличился в Африке.

Доля компьютеров АСУ, на которых были заблокированы вирусы в **Африке,** росла в течение трех кварталов подряд и достигла максимального значения за исследуемый период — 4,15%.

Доля компьютеров АСУ, на которых были заблокированы вирусы в Африке II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей в Африке самый высокий показатель вирусов — в строительной отрасли (5,35%).

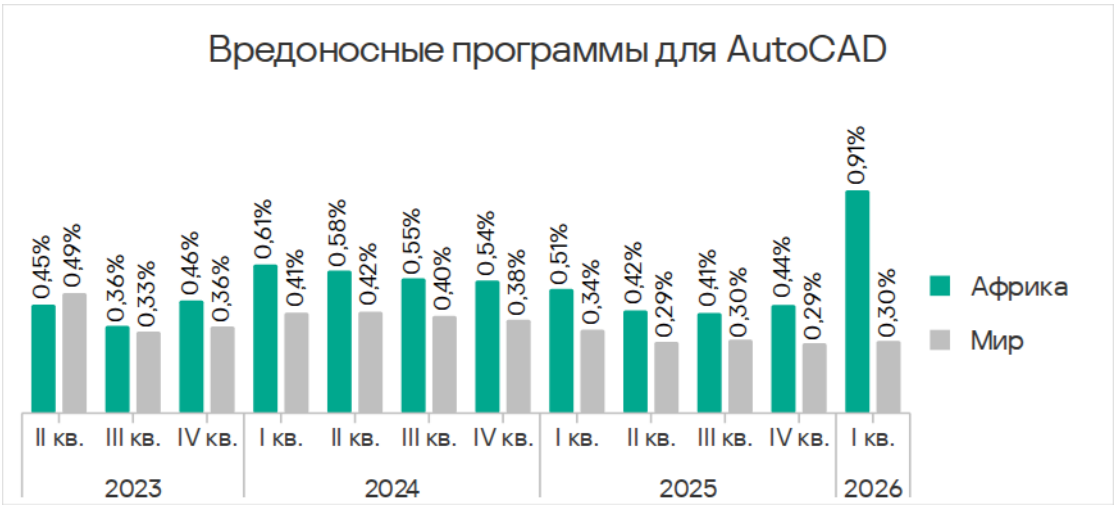
Среди исследуемых отраслей во всех регионах самые высокие показатели вирусов — в Юго-Восточной Азии у строительной отрасли (6,35%) и у автоматизации зданий (5,50%).

Вредоносные программы для AutoCAD

Доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, увеличилась до 0,30%.

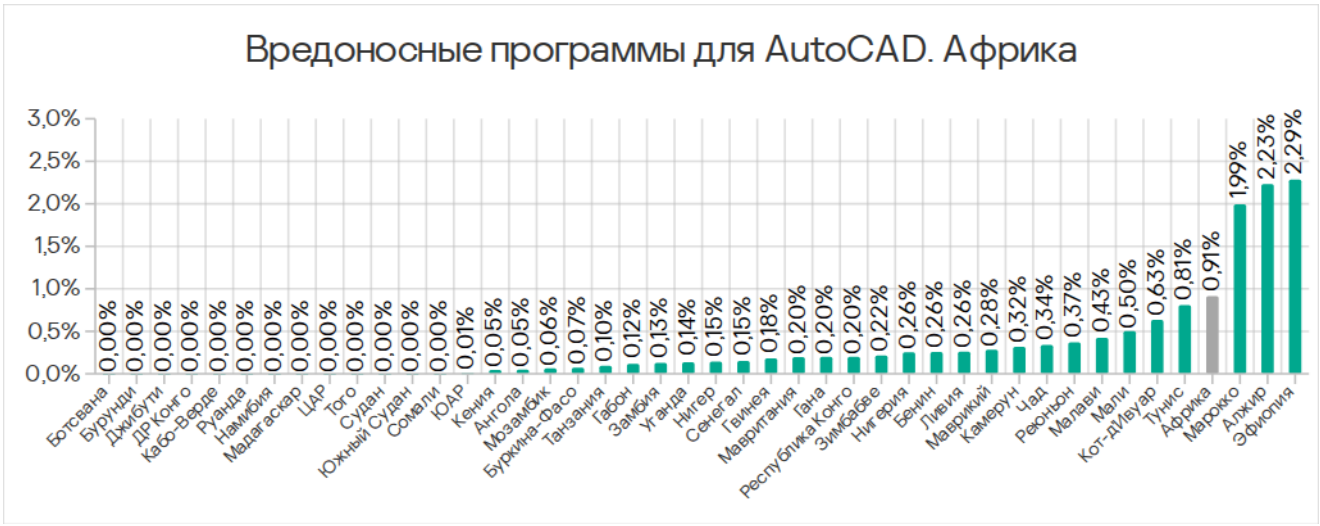
В регионах показатель варьирует от 0,00% в Северной Европе до 1,87% в Юго-Восточной Азии. Лидируют по этому показателю те же регионы, что и в рейтинге по вирусам: Юго-Восточная и Восточная Азия (оба региона с отрывом от остальных), а также Африка.

Больше всего показатель за квартал увеличился в **Африке** — практически вдвое, на весьма значительные для этой категории 0,47 п. п.



Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD в Африке II квартал 2023 года — I квартал 2026 года

Среди стран Африки по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD, лидируют Эфиопия, Алжир и Марокко, показатели в которых необычно высоки для этой категории угроз (около 2%). Больше всего доля компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD, выросла в Алжире и Марокко — на 0,96 п. п. и 1,40 п. п. соответственно.



Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD в странах Африки, II квартал 2023 года — I квартал 2026 года

Среди исследуемых отраслей в регионе самые высокие показатели вредоносных программ для AutoCAD, как и у вирусов, — в строительной отрасли (1,95%).

Среди исследуемых отраслей во всех регионах самые высокие показатели вредоносных программ для AutoCAD — в строительной отрасли в Восточной Азии (5,58%) и в Юго-Восточной Азии (3,87%).

Основные источники угроз

В первом квартале 2026 года показатели всех источников угроз, кроме угроз из интернета, в среднем по миру уменьшились.

Интернет

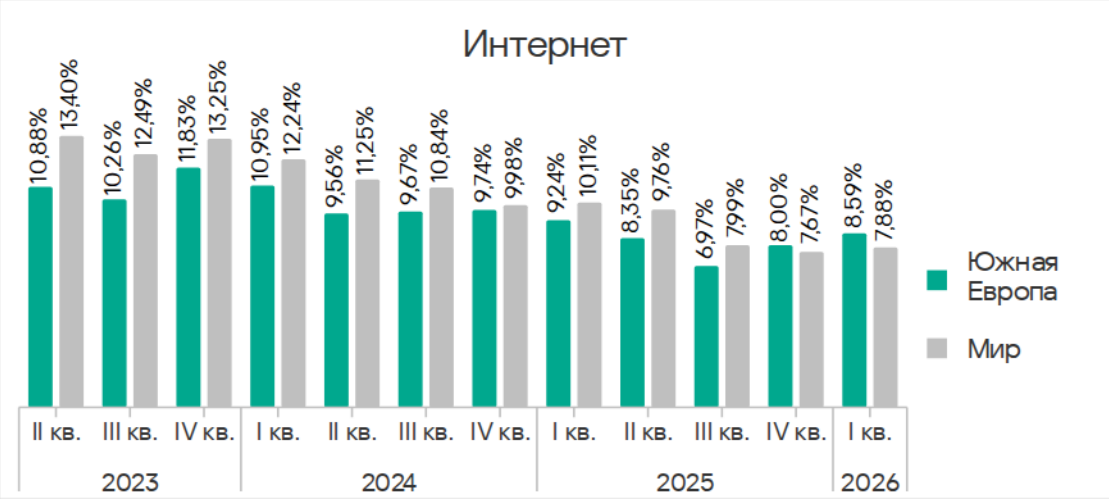
В мире в первом квартале 2026 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, выросла до 7,88%. Однако три последних года показатель угроз из интернета демонстрирует тренд к снижению.

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, варьирует от 4,48% в Северной Европе до 10,16% в Юго-Восточной Азии.

Больше всего показатель увеличился в Южной Европе, Юго-Восточной Азии и Северной Европе.

В **Южной Европе** доля компьютеров АСУ, на которых блокируются угрозы из интернета, растет второй квартал подряд и в прошлом квартале впервые превысила среднемировое значение.

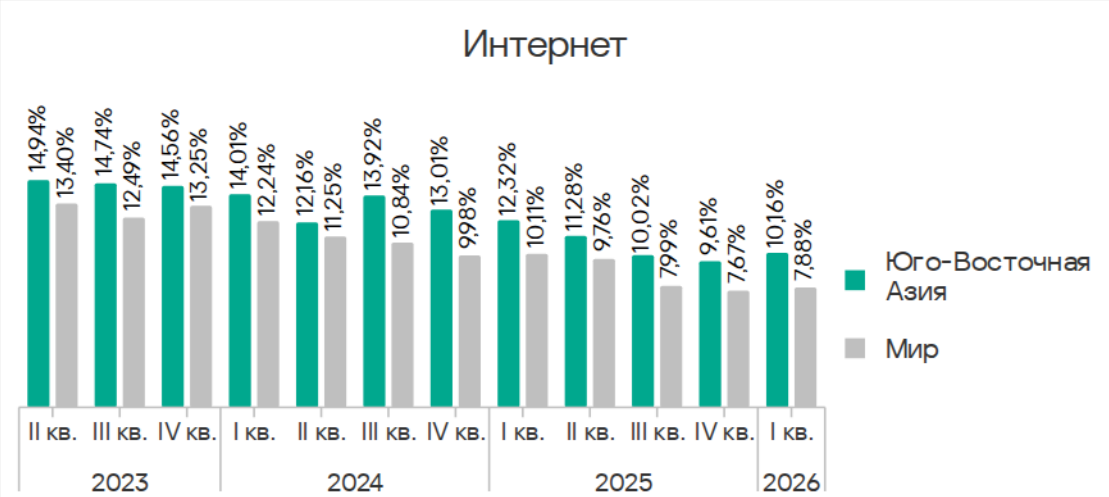
Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета в Южной Европе, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей в регионе больше всего в первом квартале 2026 года значения увеличились в производственной и строительной отраслях.

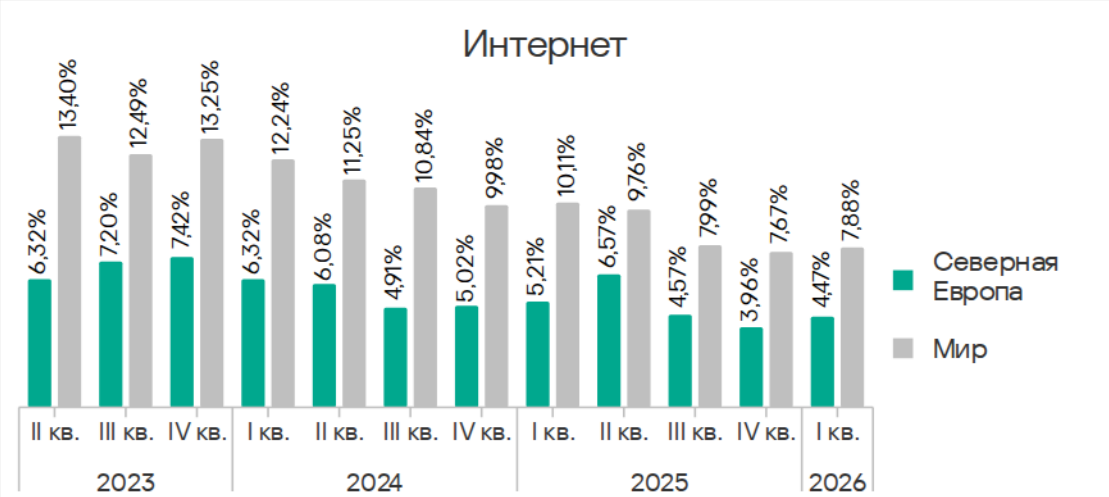
В **Юго-Восточной Азии** показатель увеличился впервые с третьего квартала 2024 года. Среди исследуемых отраслей в регионе самые высокие показатели угроз из интернета в электроэнергетике и строительстве, больше всего за квартал значение выросло в электроэнергетике.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета в Юго-Восточной Азии, II квартал 2023 года — I квартал 2026 года



Динамика показателя в **Северной Европе** близка к среднемировому тренду. Среди исследуемых отраслей в регионе самый высокий показатель угроз из интернета — у биометрических систем и в электроэнергетике, в этих же отраслях обльше всего выросло значение за квартал.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета в Северной Европе, II квартал 2023 года — I квартал 2026 года



Среди исследуемых отраслей во всех регионах самые высокие показатели угроз из интернета — в Юго-Восточной Азии в электроэнергетике (13,16%) и строительстве (12,55%), а также в Южной Азии в секторе инжиниринг и интеграторы АСУ (12,33%).

Почтовые клиенты

В мире доля компьютеров АСУ, на которых были заблокированы почтовые клиенты, уменьшилась до 2,59%. Это наименьшее значение за три года.

В регионах показатель варьирует от 0,58% в Северной Европе до 6,54% в Южной Европе.

В первом квартале 2026 показатель угроз из почтовых клиентов увеличился в трех регионах — в Южной Европе, Восточной Азии и немного в России.

Больше всего значение увеличилось в **Южной Европе.** Среди исследуемых отраслей безусловный лидер по показателю угроз из почтовых клиентов и по росту этого показателя за квартал — биометрические системы.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов в Южной Европе, II квартал 2023 года — I квартал 2026 года

Среди исследуемых отраслей во всех регионах самые высокие показатели угроз из почтовых клиентов — в Южной Европе у биометрических систем (19,78%) и автоматизации зданий (12,34%). В этих двух отраслях доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, выше показателя угроз из интернета. Аналогичная ситуация отмечена еще в двух случаях, оба раза — в биометрических системах (в Южной Америке и Юго-Восточной Азии).

Съемные носители

В мире доля компьютеров АСУ, на которых угрозы были обнаружены при подключении съемных носителей, продолжила снижаться и достигла минимального значения за исследуемый период — 0,26%.

Показатель за квартал не увеличился ни в одном регионе. В регионах показатель варьирует от 0,04% в Австралии и Новой Зеландии до 1,23% в Африке.

Африка — многолетний лидер этого рейтинга. Хотя показатель в регионе уменьшается, отрыв от остальных регионов все еще весьма значительный. По сравнению с регионом Австралия и Новая Зеландия, который замыкает этот рейтинг, значение в Африке больше в 29,3 раза.

Среди исследуемых отраслей в Африке самые высокие показатели угроз на съемных носителях в электроэнергетике (1,16%) и у биометрических систем (1,15%).

Среди исследуемых отраслей во всех регионах самые высокие показатели угроз, которые блокируются на компьютерах АСУ при подключении съемных носителей, — в электроэнергетической отрасли в Центральной Азии и Закавказье (1,45%), Восточной Азии (1,34%) и Африке (1,16%).

Сетевые папки

Доля компьютеров АСУ, на которых угрозы блокируются в сетевых папках, неуклонно снижается. В первом квартале 2026 года она была наименьшей за исследуемый период — 0,029%.

В регионах показатель варьирует от 0,005% в Северной Европе до 0,135% в Восточной Азии.

Восточная Азия традиционно лидирует по этому показателю с большим отрывом от остальных регионов. Значение в Восточной Азии больше минимального среди регионов (в Северной Европе) в 27 раз.

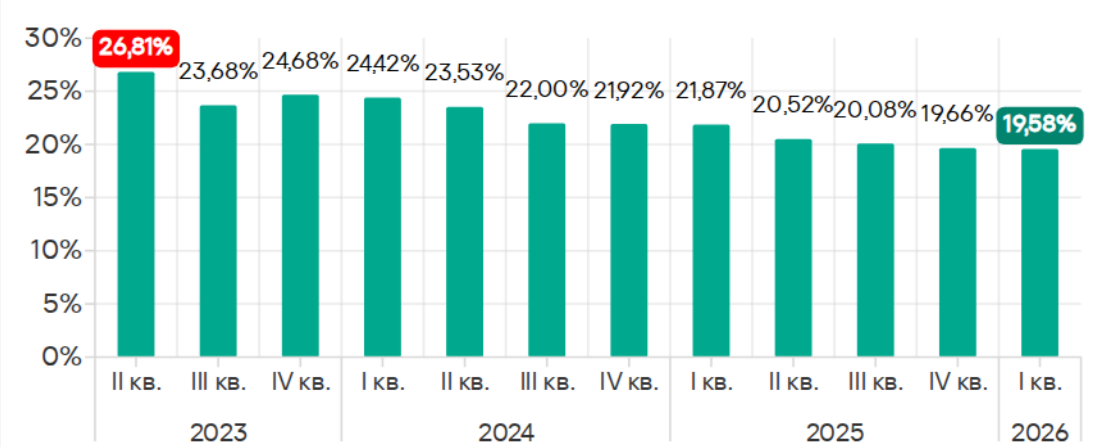
Показатель угроз в сетевых папках больше всего вырос в Африке и Южной Америке.

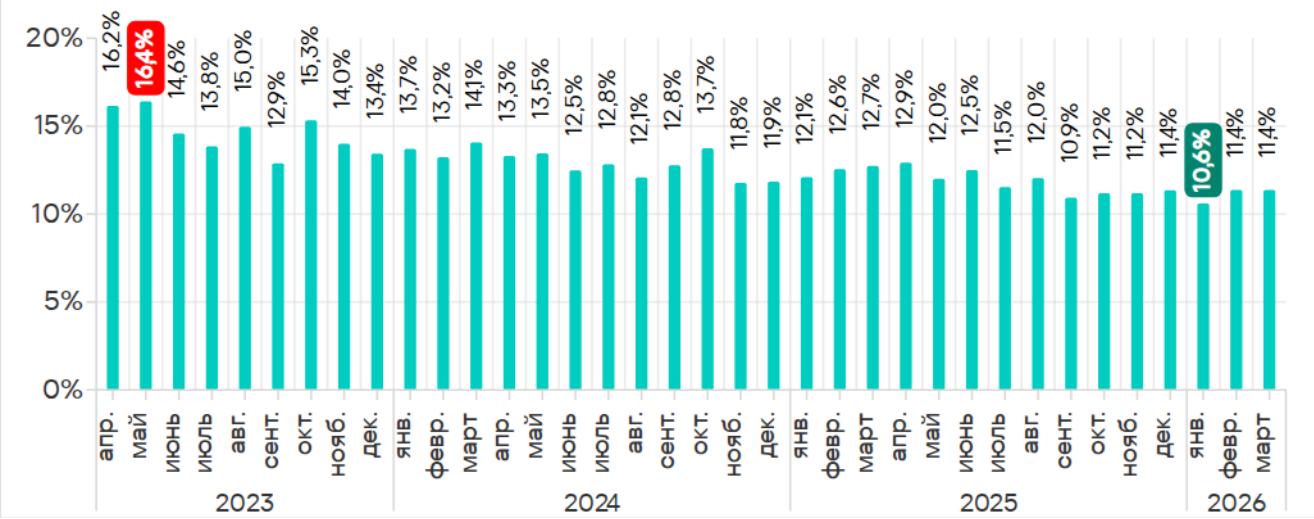
Среди исследуемых отраслей во всех регионах верхние строчки в рейтинге по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, заняли отрасли в Восточной Азии (что ожидаемо, учитывая показатель по сетевым папкам региона в целом). Наибольшее значение — в строительной отрасли (0,36%).

Основная статистика

Все угрозы

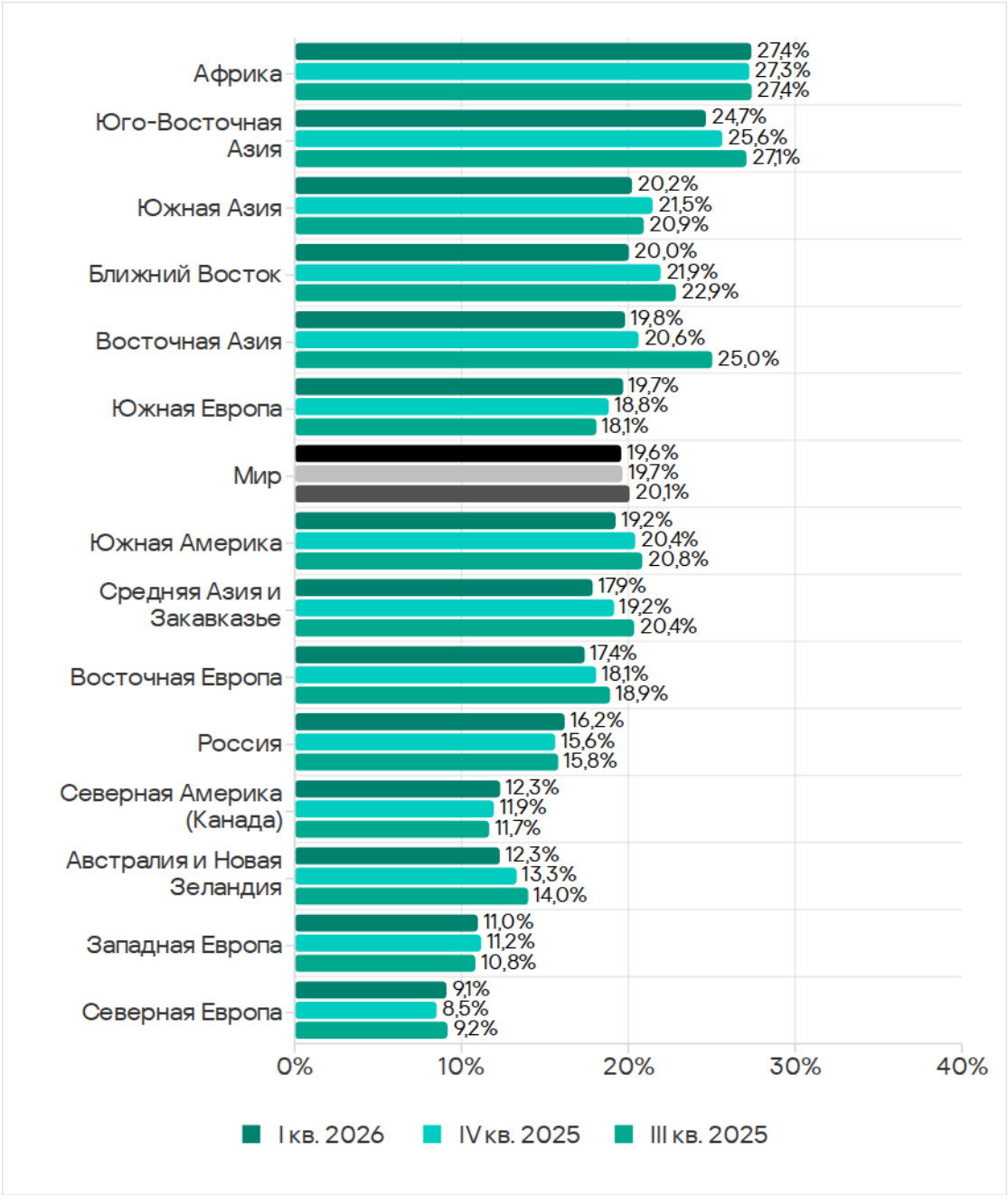
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, II квартал 2023 года — I квартал 2026 года



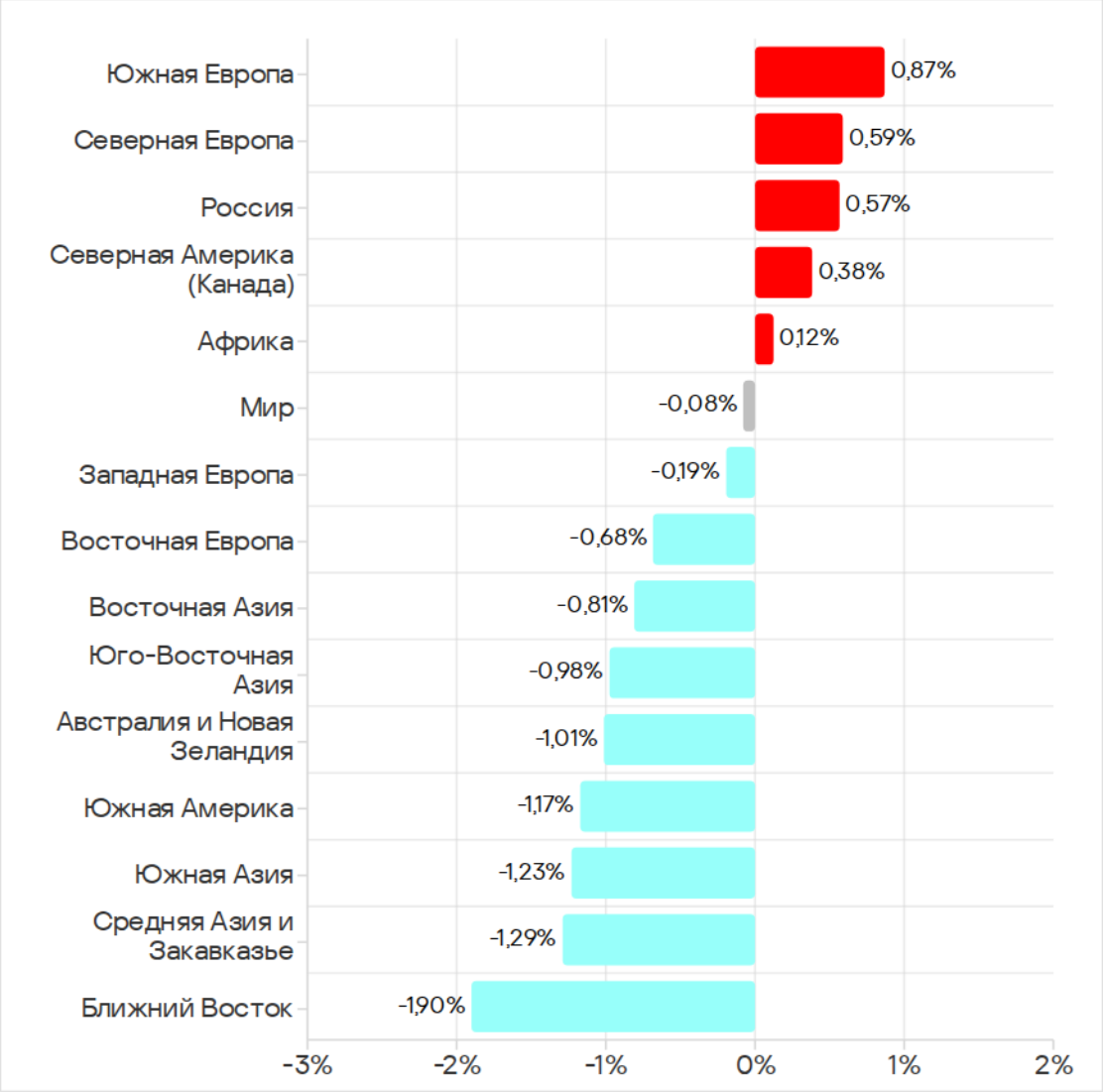


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, апрель 2023 года — март 2026 года

Рейтинг регионов по доле атакованных компьютеров АСУ

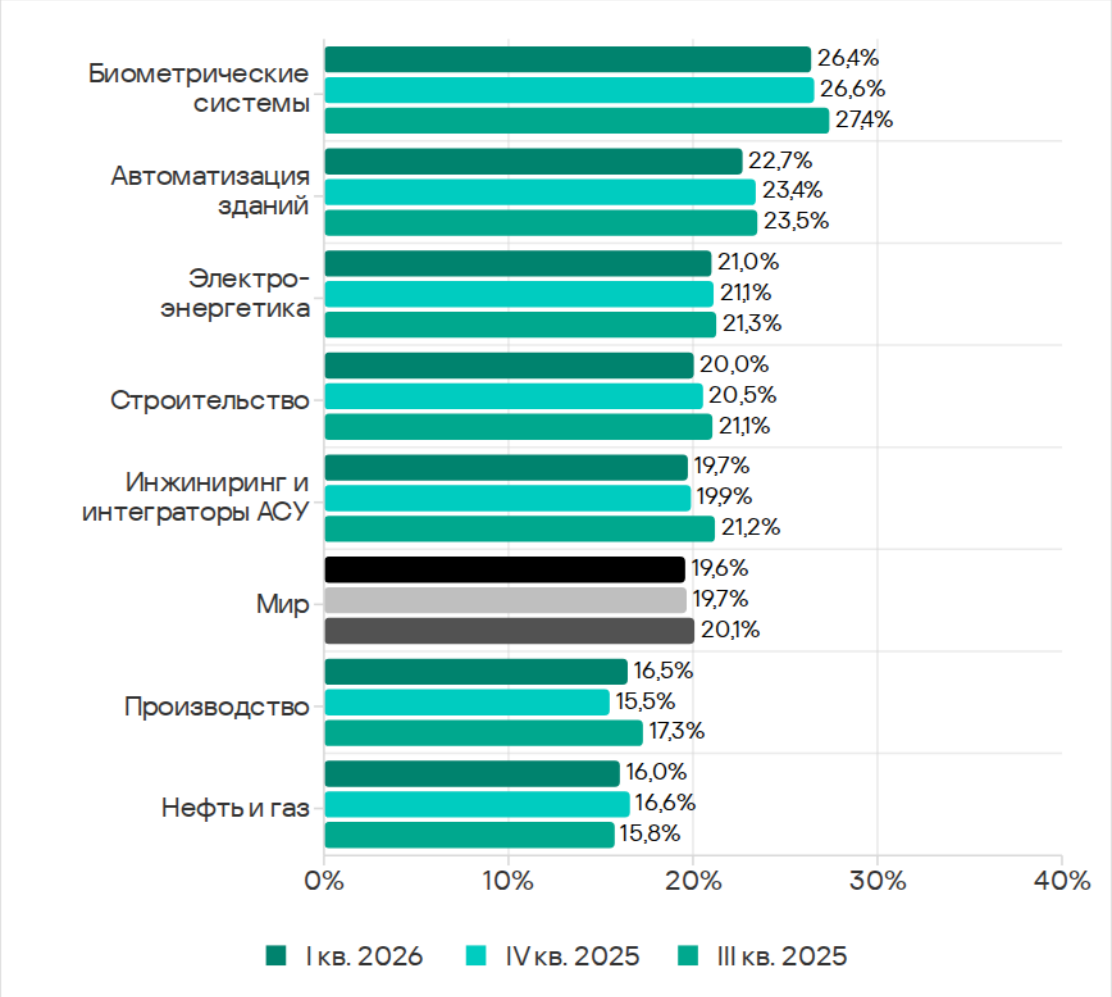


Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2026 года

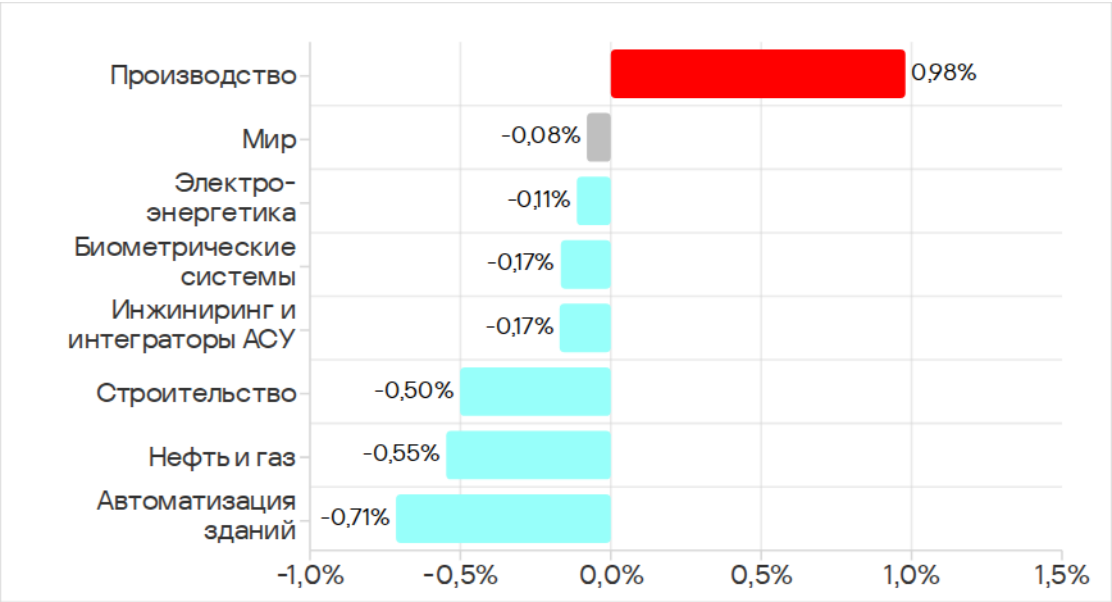


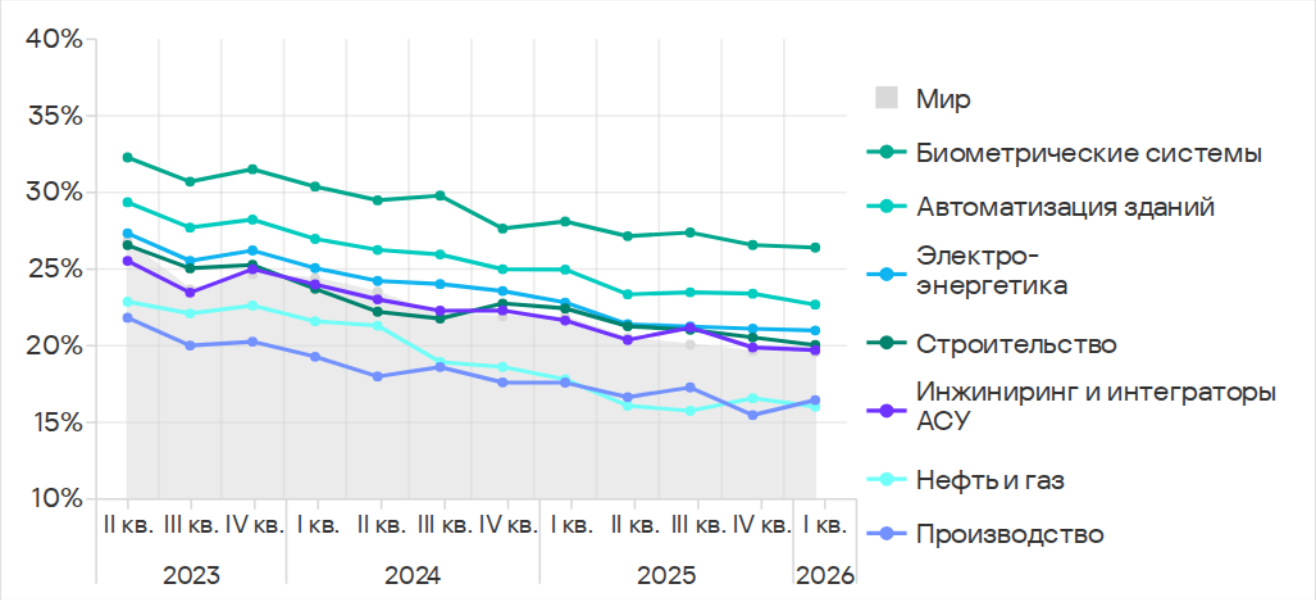
Исследуемые отрасли

Рейтинг исследуемых отраслей по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты в отраслях, I квартал 2026 года





Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в исследуемых отраслях

Источники угроз и категории вредоносного ПО в отраслях

При оценке проблем отраслей мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей по категориям или источникам угроз. Красный цвет указывает на то, что значение близко к максимальному. Желтым подсвечены максимальные среди отраслей показатели определенной категории или источника угрозы.

Показатели источников угроз в отраслях (мир), I квартал 2026 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Строительство	Инжиниринг и интеграторы АСУ	Производство	Нефть и газ	Показатель категории в мире
Интернет	8,49%	8,63%	9,46%	9,50%	8,78%	7,40%	6,22%	7,88%
Почтовые клиенты	9,53%	5,32%	2,31%	2,55%	2,14%	2,06%	1,48%	2,59%
Съемные носители	0,27%	0,30%	0,47%	0,23%	0,26%	0,25%	0,41%	0,26%
Сетевые папки	0,03%	0,04%	0,03%	0,04%	0,04%	0,02%	0,02%	0,03%
Показатель отрасли в мире	26,41%	22,69%	21,00%	20,05%	19,72%	16,46%	16,04%	

Показатели категорий угроз в отраслях (мир), I квартал 2026 года

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Строительство	Инжиниринг и интеграторы АСУ	Производство	Нефть и газ	Показатель категории в мире
Вредоносные скрипты и фишинговые страницы	13,38%	9,69%	7,09%	7,55%	6,66%	6,18%	4,77%	6,56%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,11%	5,44%	3,82%	3,30%	3,45%	2,62%	3,05%	3,73%
Ресурсы в интернете из списка запрещенных	2,81%	3,42%	4,40%	3,74%	3,69%	2,95%	3,60%	3,54%
Вредоносные документы (MSOffice+PDF)	4,44%	3,10%	1,81%	1,46%	1,40%	1,20%	1,27%	1,56%
Черви (Worm)	2,12%	1,81%	1,81%	1,11%	1,15%	1,21%	1,31%	1,33%
Вирусы (Virus)	1,69%	1,71%	1,87%	1,96%	1,29%	1,09%	1,07%	1,31%
Майнеры — исполняемые файлы для ОС Windows	0,45%	0,59%	0,71%	0,69%	0,61%	0,44%	0,82%	0,59%
Вредоносные программы для AutoCAD	0,09%	0,15%	0,33%	1,12%	0,31%	0,18%	0,29%	0,30%
Веб-майнеры, выполняемые в браузерах	0,27%	0,28%	0,40%	0,44%	0,29%	0,27%	0,45%	0,22%
Программы-вымогатели	0,27%	0,25%	0,20%	0,16%	0,13%	0,13%	0,21%	0,14%
Показатель отрасли в мире	26,41%	22,69%	21,00%	20,05%	19,72%	16,46%	16,04%	

Биометрические системы находятся на первом месте по показателям угроз из почты. При этом, в отличие от остальных отраслей, показатель почтовых клиентов у биометрических систем превышает показатель угроз из интернета.

Почта — источник вредоносных скриптов и вредоносных документов. Переход по вредоносной ссылке в письме или открытие вложения из фишингового письма могут приводить к заражению компьютера шпионским ПО. Шпионские программы, в свою очередь, могут

использоваться (в том числе) для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели.

По показателям всех этих категорий вредоносного ПО — вредоносных скриптов, вредоносных документов, шпионских программ, программ-вымогателей — биометрические системы занимают первое место. Лидируют они и по показателю червей.

Электроэнергетика находится на первом месте по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, и на втором месте по показателю червей (распространяются преимущественно на съемных носителях).

Для отрасли также актуальны угрозы из интернета, значение в электроэнергетике по этому источнику угроз мало отличается от максимального среди отраслей показателя. А по показателю ресурсов в интернете из списка запрещенных электроэнергетика находится на первом месте.

Строительная отрасль занимает первое место по показателю угроз из интернета и второе — по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных.

Отрасль также находится на первом месте по угрозам из сетевых папок. Сетевые папки — основной канал распространения вирусов и вредоносных программ для AutoCAD, По показателям этих категорий угроз строительство также находится на первом месте.

Нефтегазовая отрасль, которая замыкает рейтинг исследуемых отраслей по доле атакованных компьютеров АСУ, занимает первое место по показателям и веб-майнеров, и майнеров в формате исполняемых файлов.

Категории вредоносных объектов

Типовые атаки, блокируемые в сети АСУ, представляют собой многошаговые последовательности вредоносных действий, где каждый последующий шаг злоумышленников направлен на сбор дополнительной информации, повышение привилегий и/или получение доступа к другим системам путем эксплуатации проблем безопасности промышленных предприятий, в том числе технологических инфраструктур.

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, по способу распространения и назначению можно условно разделить на три группы.

1. Вредоносные объекты, используемые для первичного заражения. Чаще всего, это ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вредоносные документы.
2. Вредоносное ПО следующего этапа.
   Как правило, это программы-шпионы, программы-вымогатели, майнеры — исполняемые файлы для ОС Windows и веб-майнеры.
3. Самораспространяющееся вредоносное ПО.
   Эта категория включает в себя вирусы и черви.

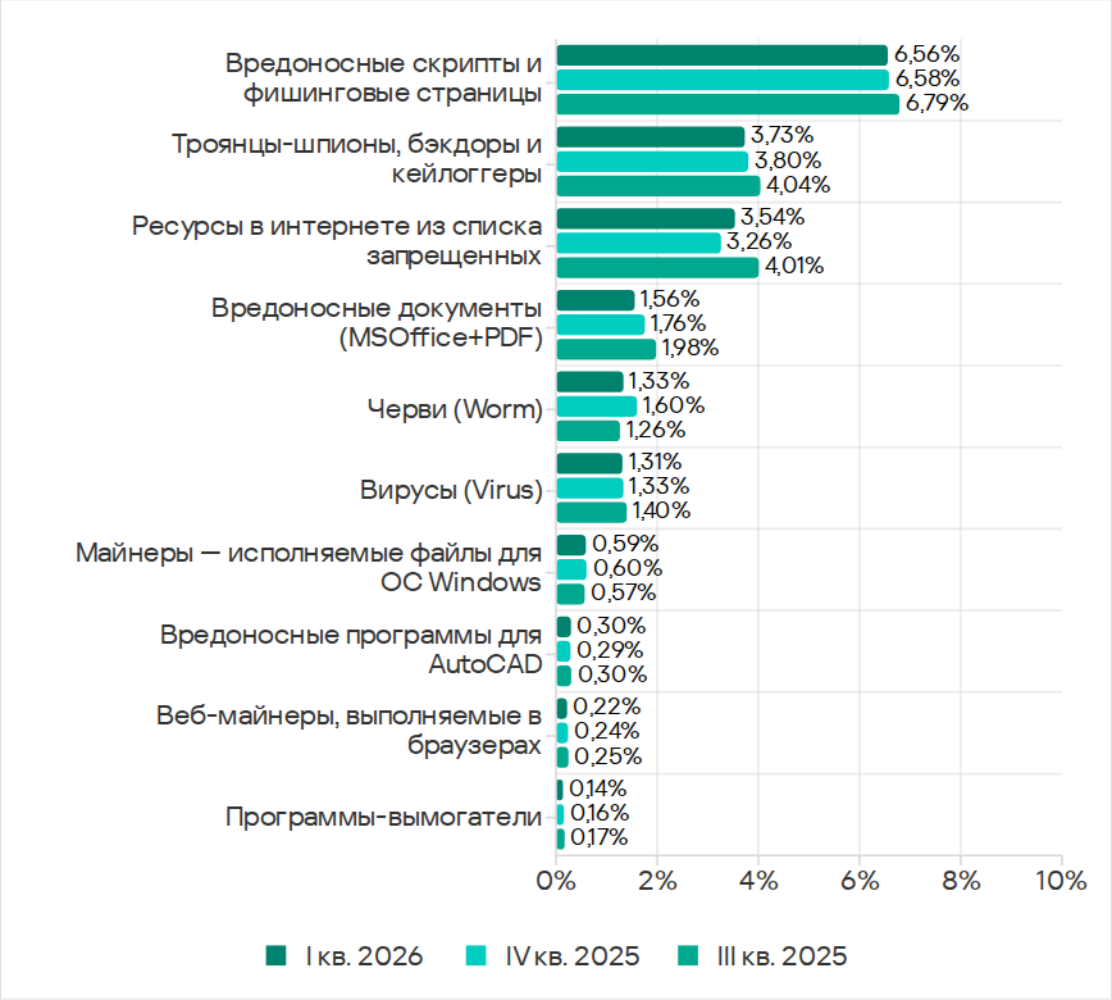
Вредоносные программы для AutoCAD распространяются разными способами, поэтому мы не относим их к конкретной группе по типу распространения.

Вредоносные объекты для первичного заражения компьютеров АСУ активно используются злоумышленниками, в результате они чаще остальных блокируются защитными решениями. Это отражается и в нашей статистике: в мире и почти во всех регионах вредоносные скрипты и фишинговые страницы, а также интернет-ресурсы из списка запрещенных занимают первые места в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

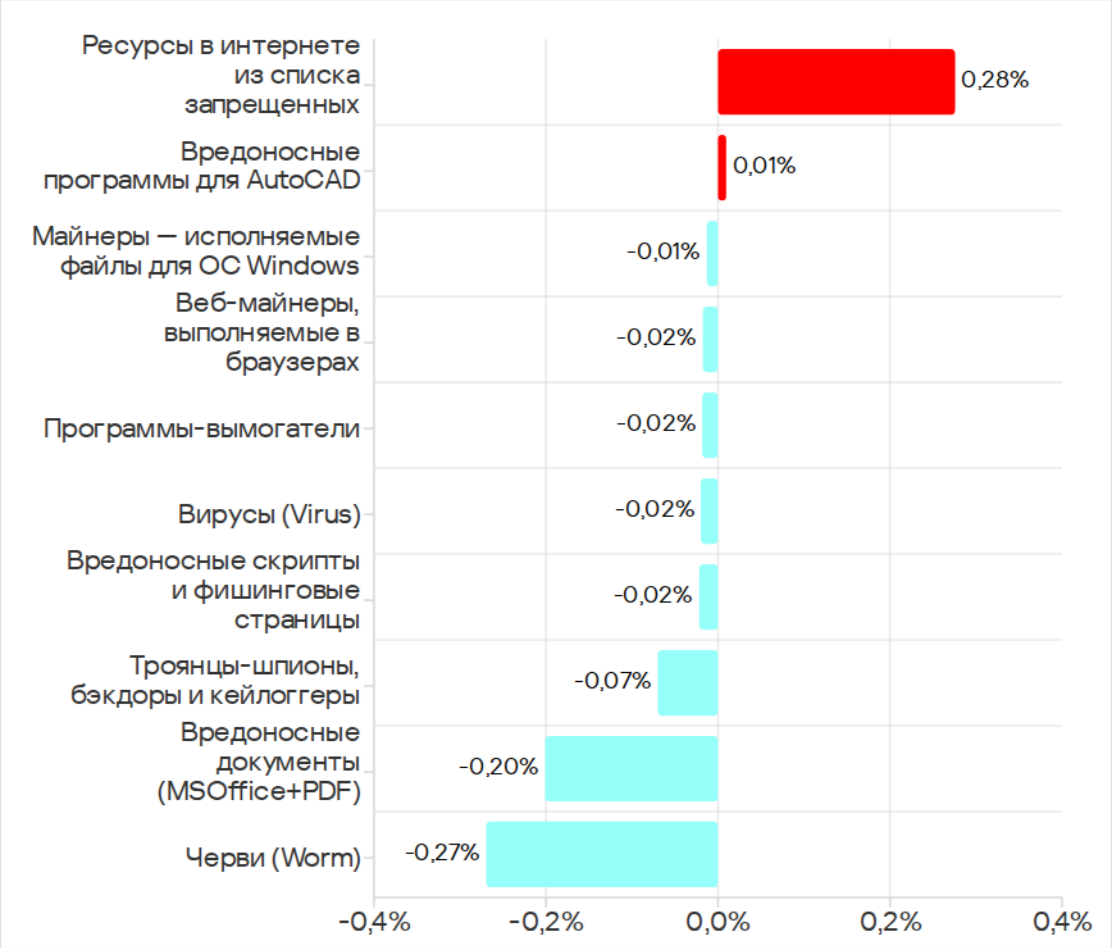
Следует заметить, что в небольшом проценте случаев категории угроз, которые мы относим к объектам первичного заражения, скажем, вредоносные ссылки, также используются на последующих этапах атаки. Так, например, иногда ссылка на вредоносный ресурс может быть обнаружена при сканировании реестра компьютера, где она появились, очевидно, в результате работы другого вредоносного ПО — до того момента, как оно было идентифицировано и заблокировано. Более строгое деление атакованных компьютеров АСУ по категориям заблокированного на них вредоносного ПО и по источникам его попадания на компьютер описано в нашей статье «Динамика внешних и внутренних угроз АСУ», открывающей новый цикл публикаций результатов более глубокого исследования ландшафта угроз АСУ ТП по данным статистики срабатывания защитных компонентов наших продуктов.

Отметим, что техники размещения вредоносного ПО в интернете разнообразны, обширны и доступны любому злоумышленнику. Любой веб-сервис (даже самый защищенный) может быть использован как веб-хранилище, если он позволяет сохранять и запрашивать информацию. На практике это означает, что для защиты сети АСУ (как и любой другой) необходимо полагаться на весь стек технологий защиты, а не только на защиту периметра сети.

Доля компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, I квартал 2026 года



Вредоносные объекты, используемые для первичного заражения

Ресурсы в интернете из списка запрещенных

Список запрещенных интернет-ресурсов используется для предотвращения попыток первичного заражения. С помощью этого списка на компьютерах АСУ блокируются преимущественно:

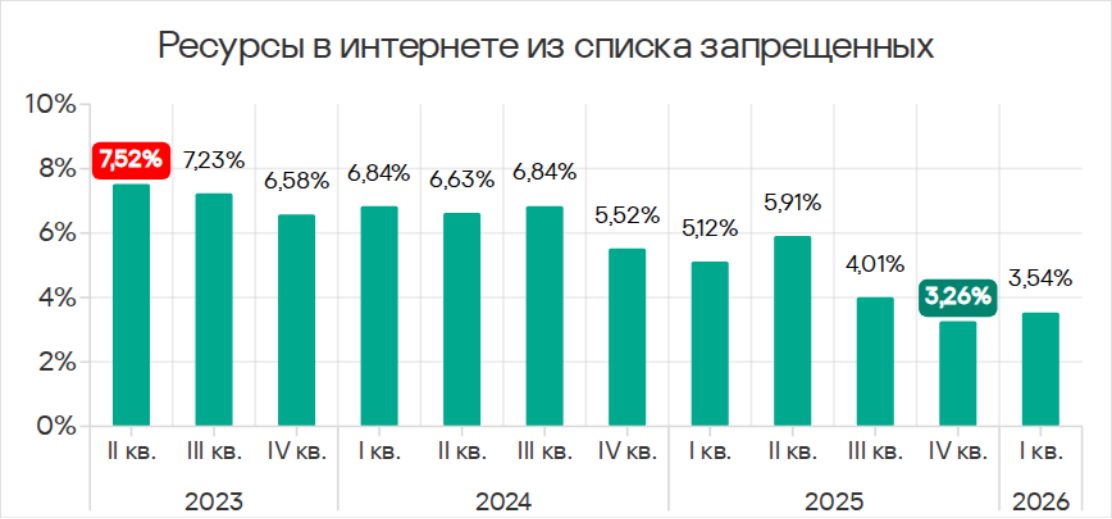
- Известные вредоносные URL-адреса и IP-адреса, используемые злоумышленниками для размещения вредоносных нагрузок и конфигураций.
- Подозрительные (небезопасные) веб-ресурсы с развлекательным и игровым контентом, часто используемые для доставки нежелательного программного обеспечения, криптомайнеров и вредоносных скриптов.
- Узлы CDN, используемые злоумышленниками для распространения вредоносных скриптов на популярных веб-сайтах.

- Сервисы обмена файлами и данными, включая репозитории, часто используемые злоумышленниками для размещения конфигураций и вредоносного ПО следующего этапа.

Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

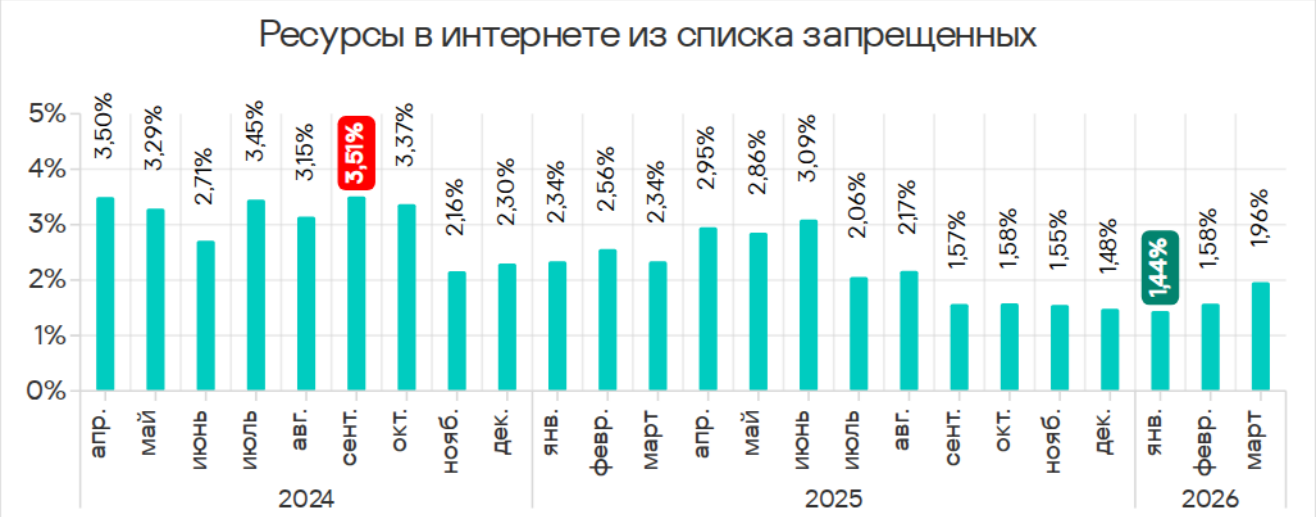
Обнаруженный опасный интернет-ресурс не всегда может быть легко добавлен в список запрещенных, поскольку злоумышленники все чаще используют легитимные интернет-ресурсы и сервисы, например платформы доставки контента (CDN), мессенджеры, репозитории и облачные хранилища. Подобные сервисы позволяют распространять вредоносный код по уникальным ссылкам на уникальный контент, затрудняя таким образом тактики блокировки по репутации. Настоятельно рекомендуем промышленным организациям предусмотреть блокировку подобных сервисов политикой, как минимум, для технологических сетей, где необходимость в таких сервисах крайне редко бывает обусловлена объективными причинами.

Высокие значения параметра, как правило, свидетельствуют о слабом контроле выполнения политик ИБ (компьютеры АСУ имеют так или иначе доступ к интернету, и этим доступом часто пользуются), недостатках защиты от фишинга (многие вредоносные ссылки доставляются в фишинговых сообщениях) и недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным веб-ресурсам и ссылкам из подозрительных писем и сообщений мессенджеров).



Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, II квартал 2023 года — I квартал 2026 года

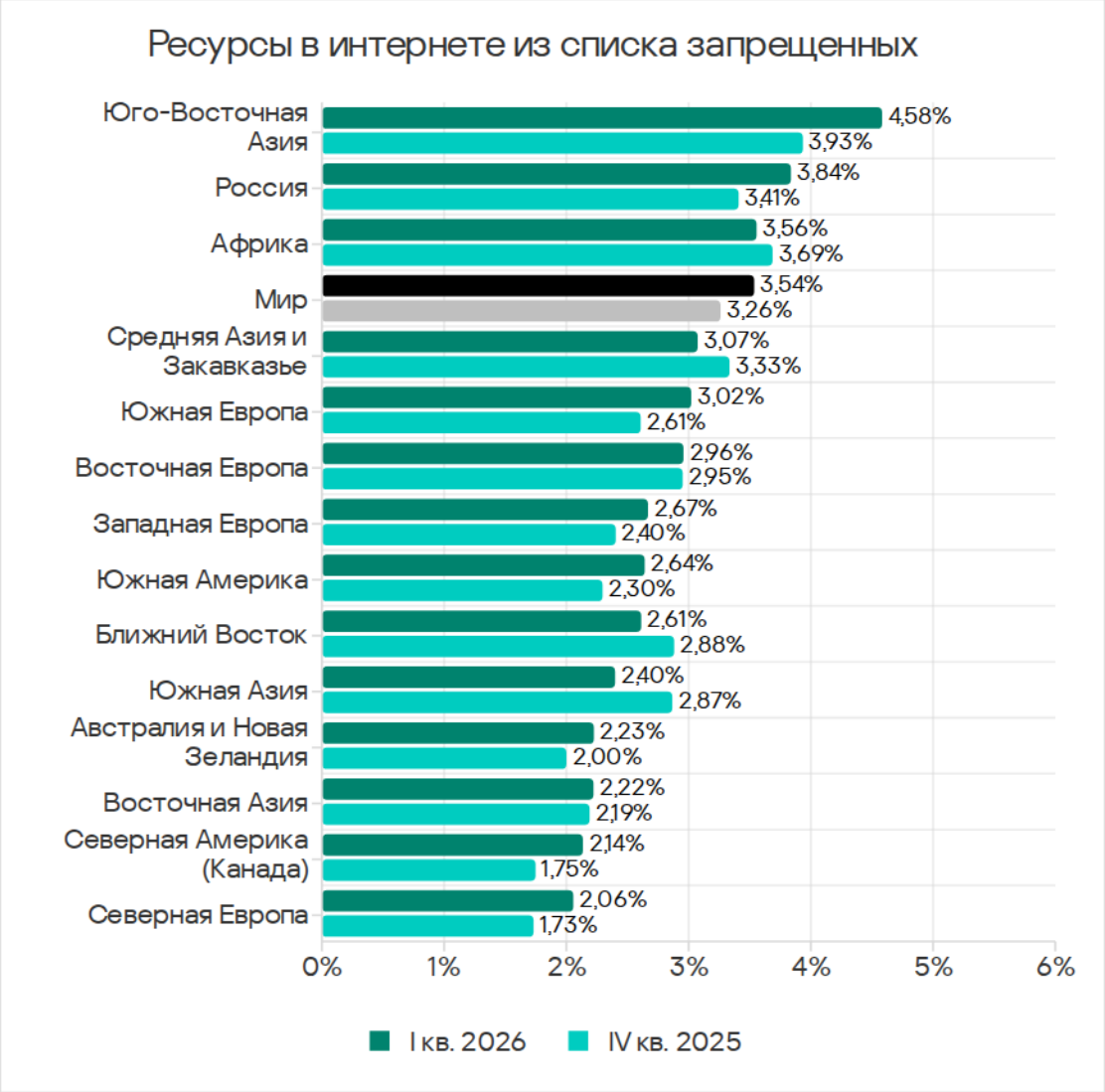
В январе 2026 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, была наименьшей за два года.



Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, апрель 2024 года — март 2026 года

В рейтинге категорий вредоносных объектов по доле атакованных компьютеров ресурсы в интернете из списка запрещенных долгое время занимали первое или второе место. В третьем квартале 2025 эта категория впервые опустилась на третье место, где и остается уже три квартала.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных



Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, I квартал 2026 года

Вредоносные скрипты и фишинговые страницы (JS и HTML)

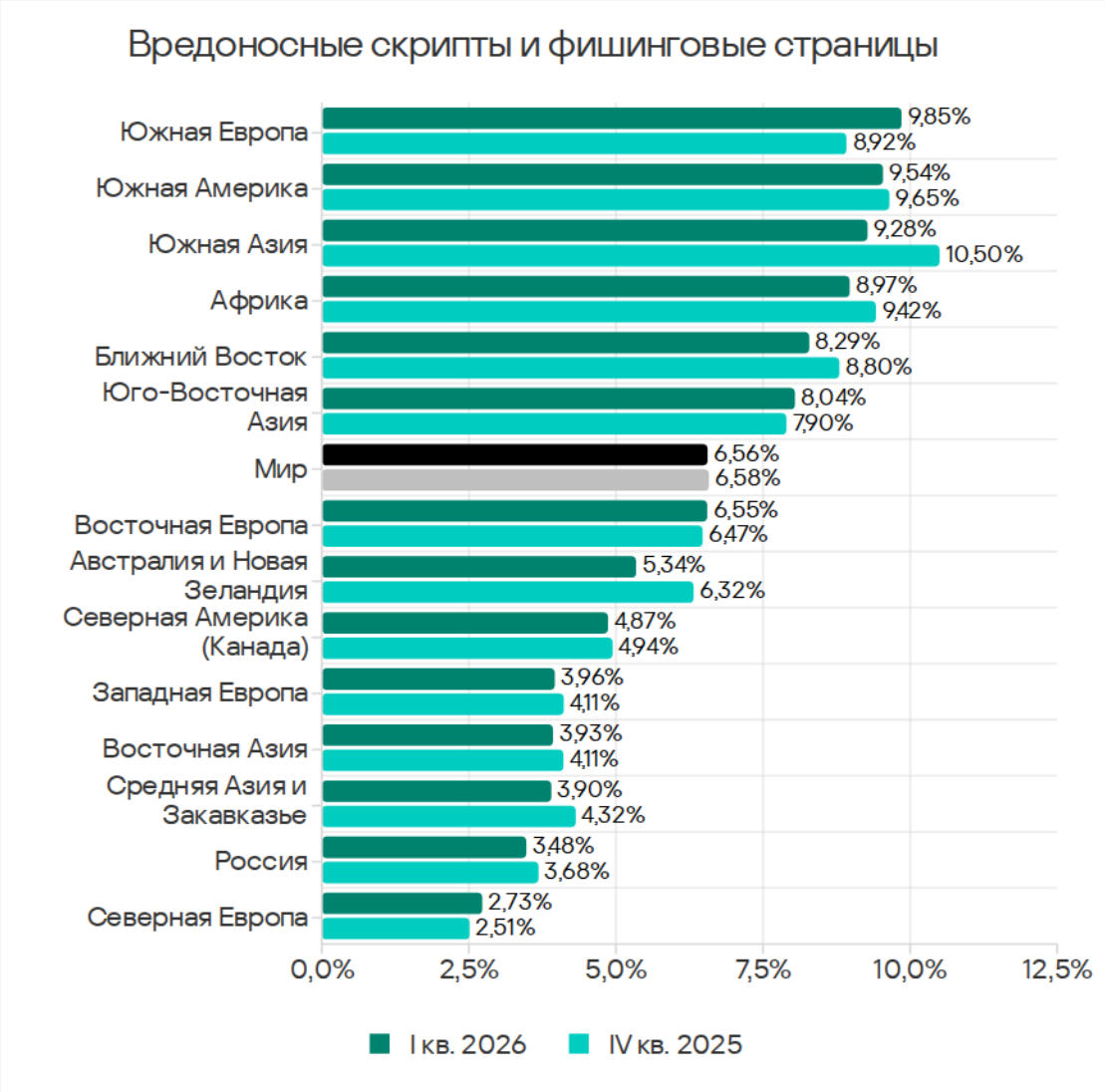
Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, II квартал 2023 года — I квартал 2026 года

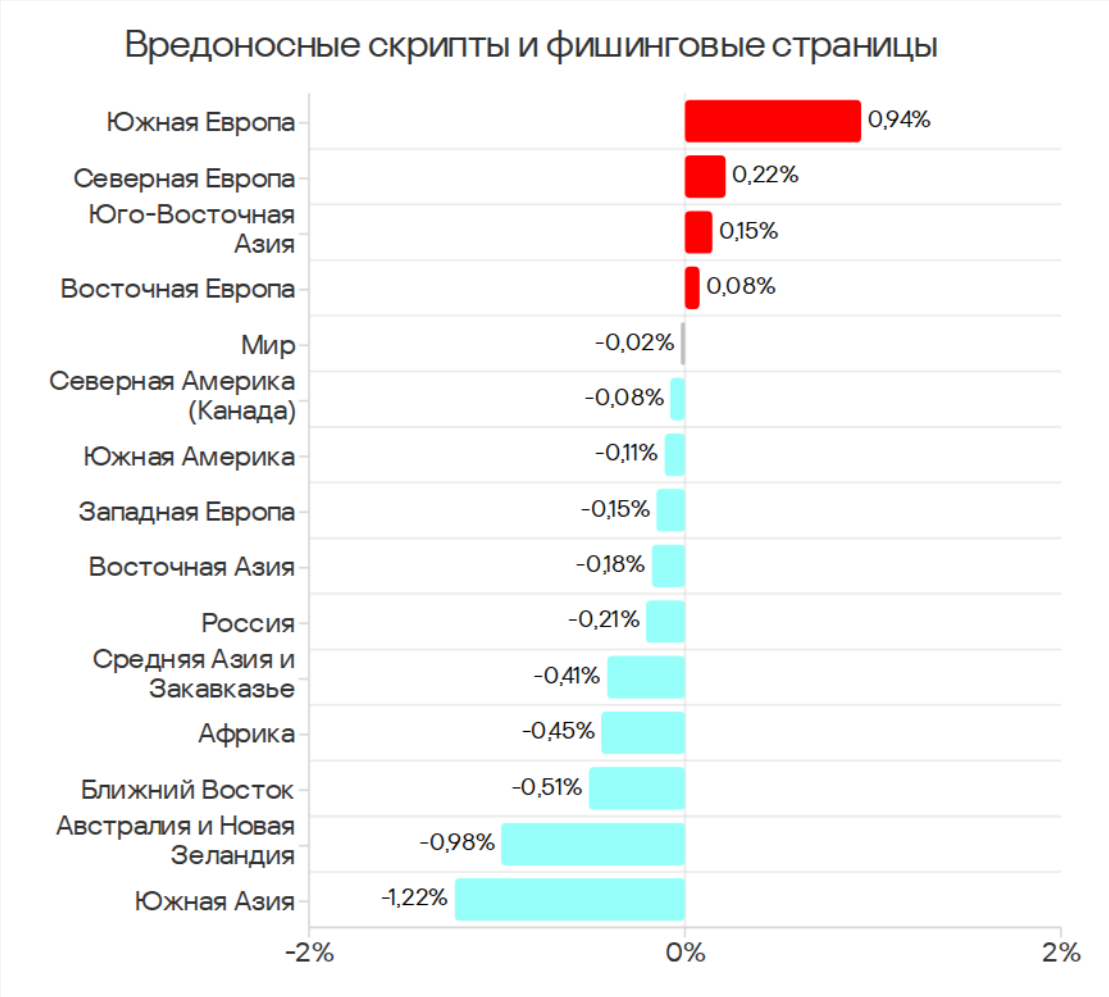
В первом квартале 2026 года самым высоким месячный показатель был в феврале. Значение превысило показатели предыдущих пяти месяцев.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, I квартал 2026 года

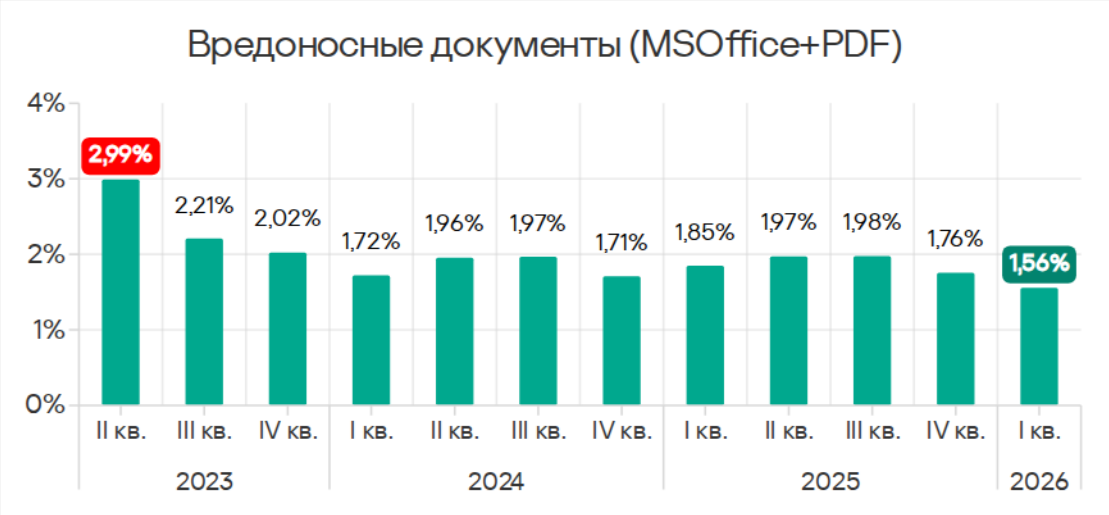


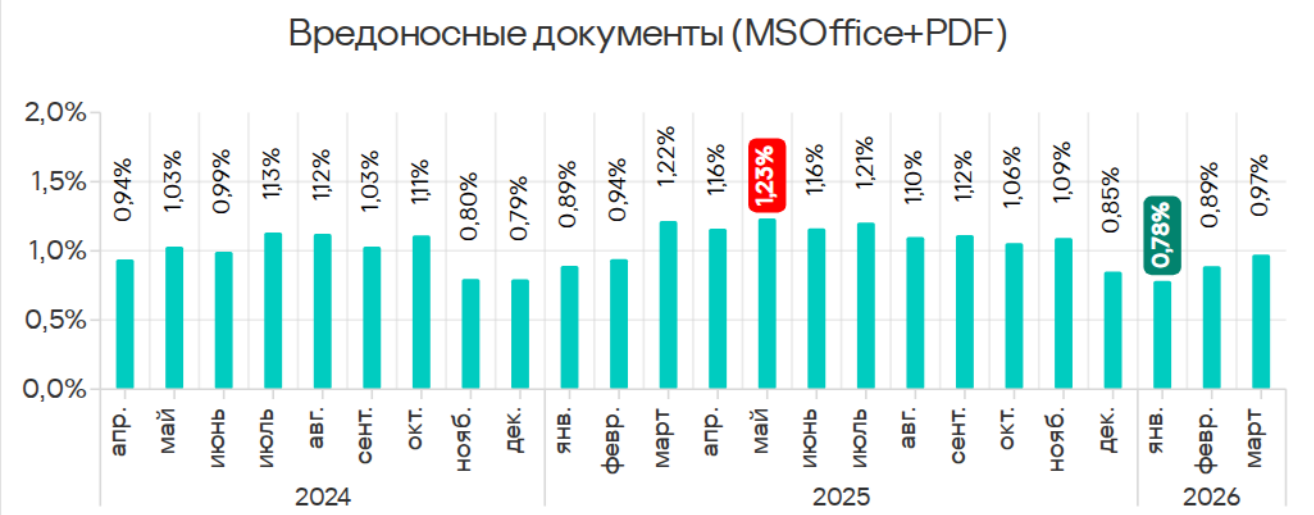
Вредоносные документы (MSOffice+PDF)

Вредоносные документы злоумышленники преимущественно рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

Вредоносные документы остаются популярным вектором для целевых атак, особенно с использованием эксплойтов нулевого дня. В 2025 году CISA выпустила более 450 предупреждений безопасности, многие из которых касаются обработки файлов, включая популярные форматы документов.

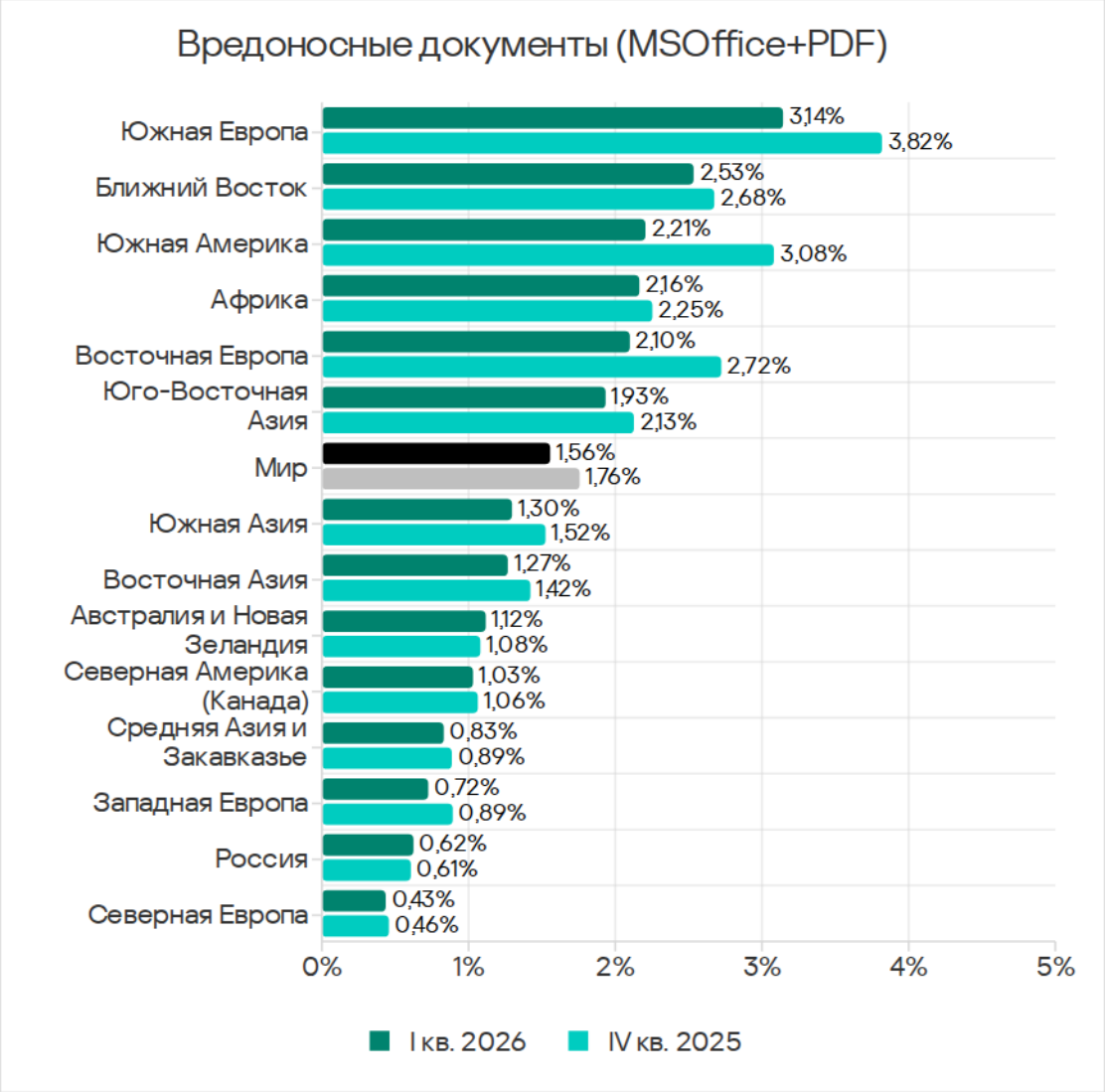
Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, II квартал 2023 года — I квартал 2026 года



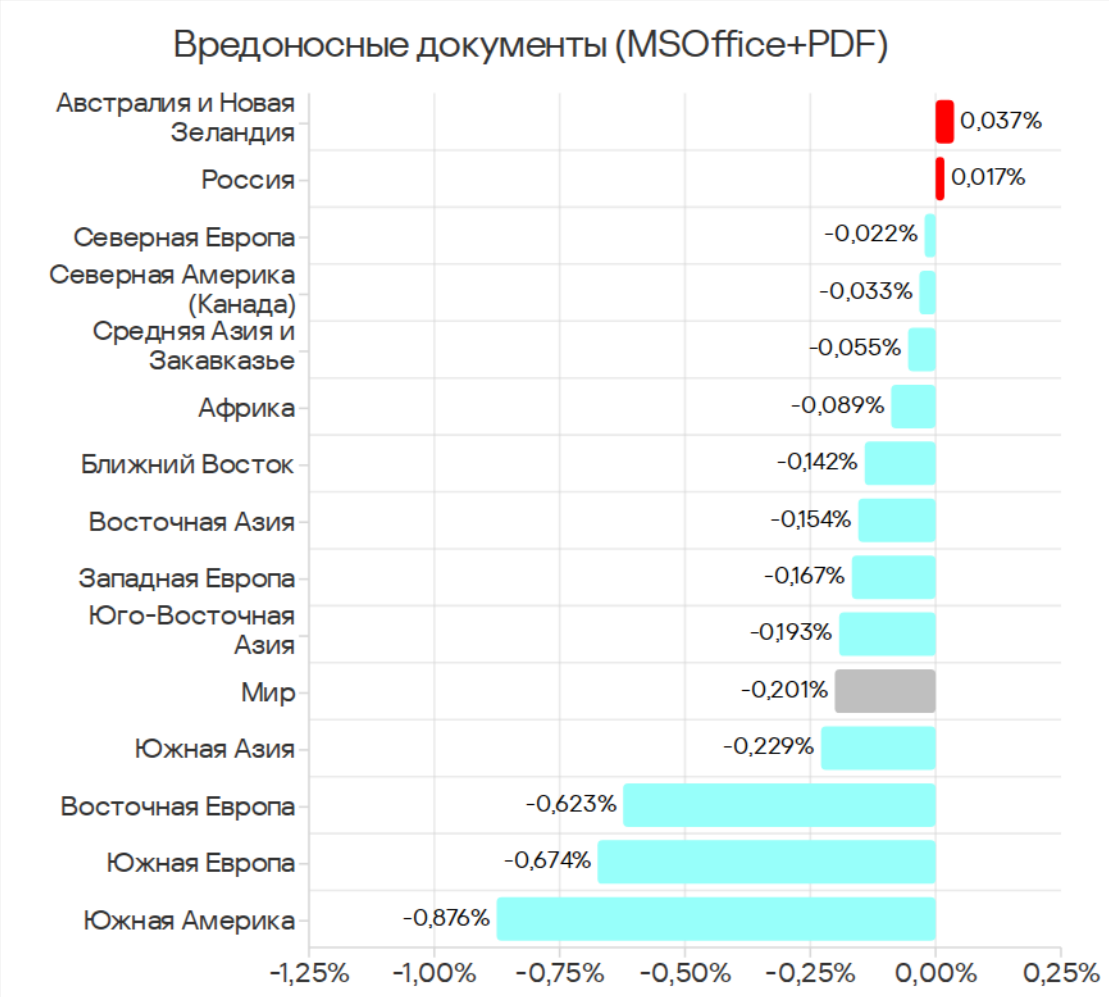


Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные документы, I квартал 2026 года



Вредоносное ПО следующего этапа

Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа. Как правило, это шпионское ПО, программы-вымогатели и майнеры. Обычно, чем выше доля компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, тем выше этот показатель и для вредоносного ПО следующего этапа.

Программы-шпионы

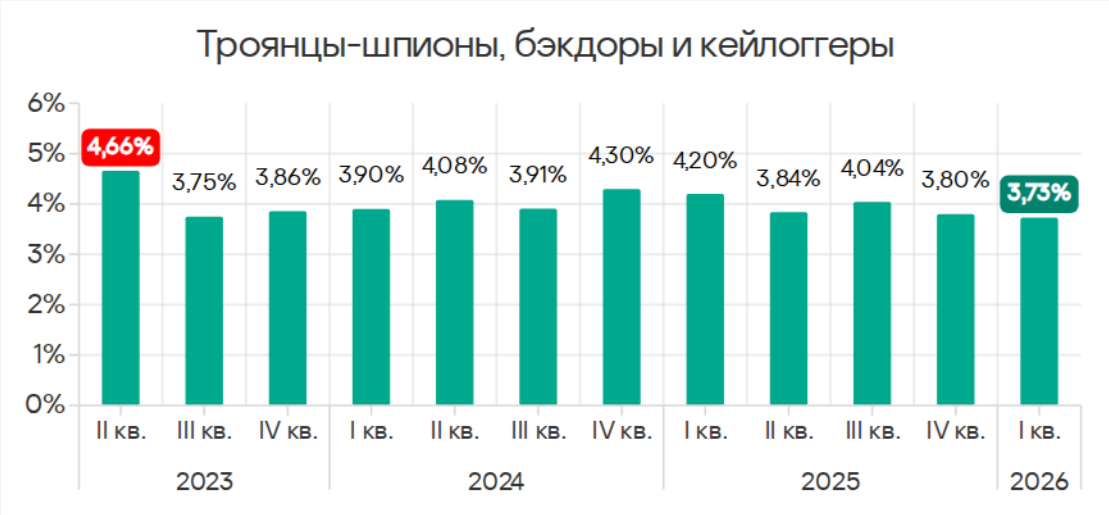
Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО (троянцы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструментарий промежуточных этапов кибератаки (например, разведки и

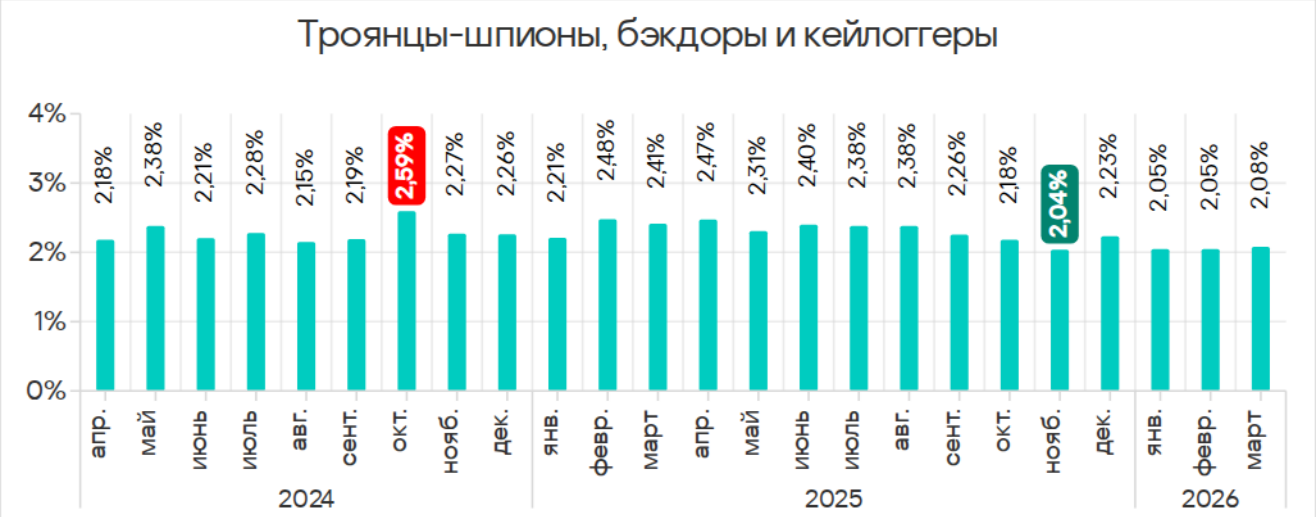
распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных. В большинстве случаев конечная цель атак с применением такого ПО — кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

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).

Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, II квартал 2023 года — I квартал 2026 года

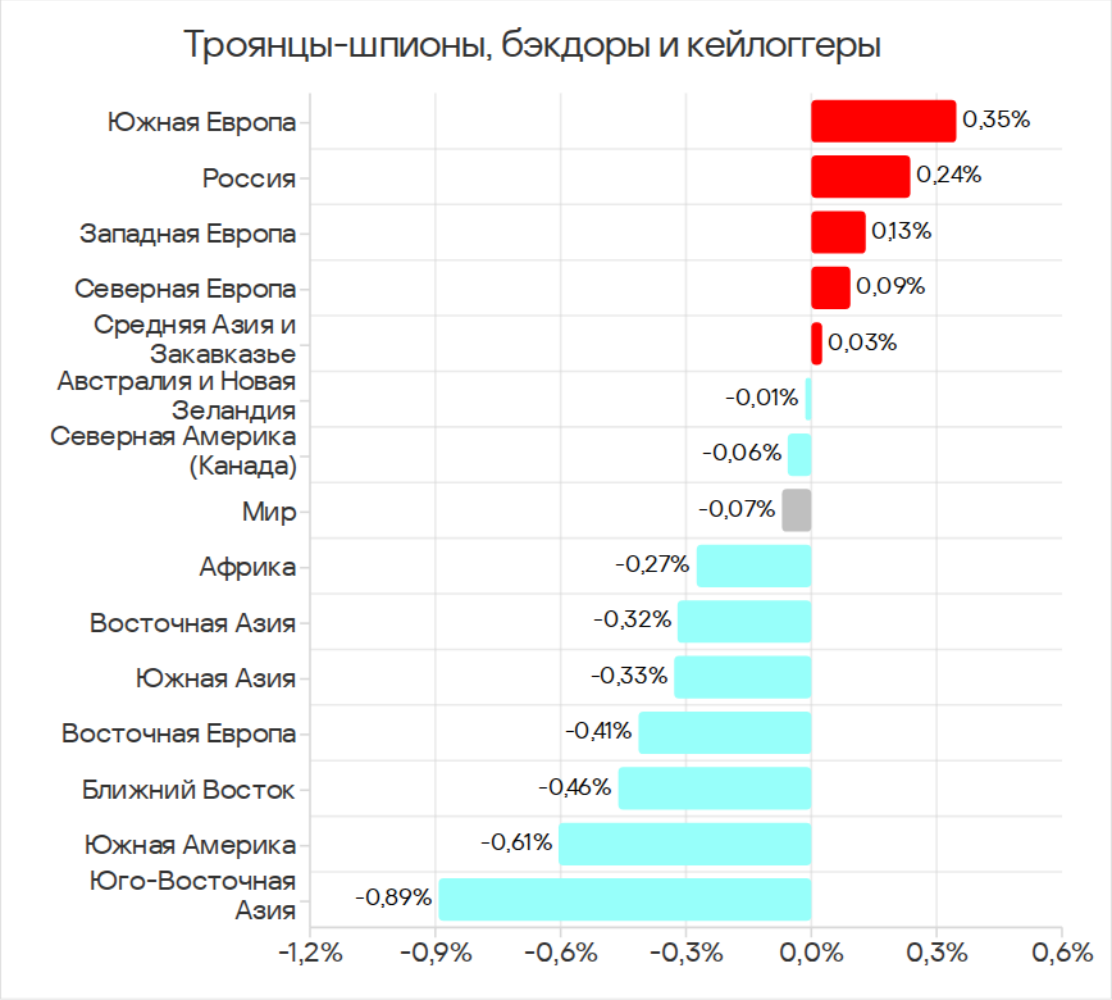




Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, апрель 2024 года — март 2026 года

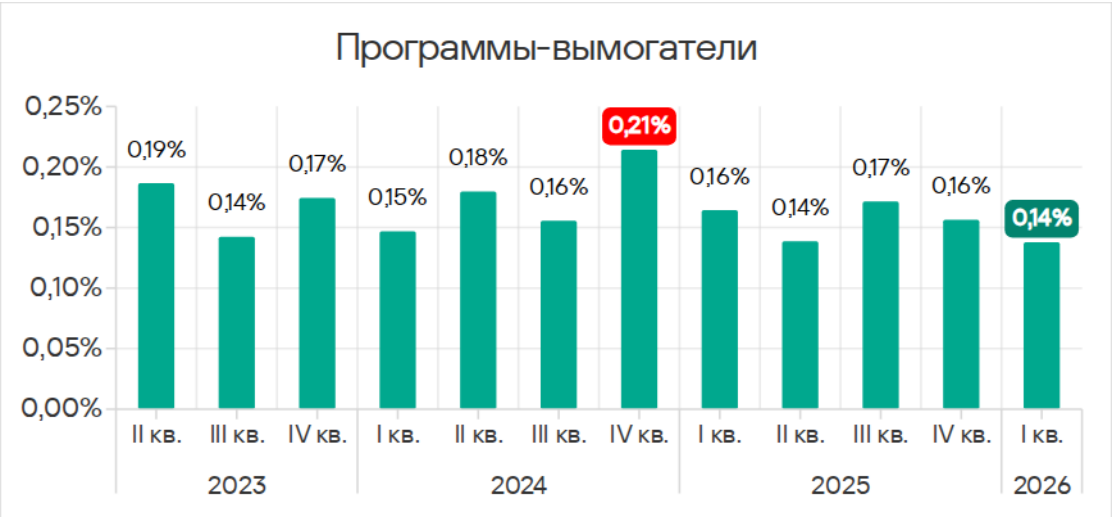
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы

Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, I квартал 2026 года



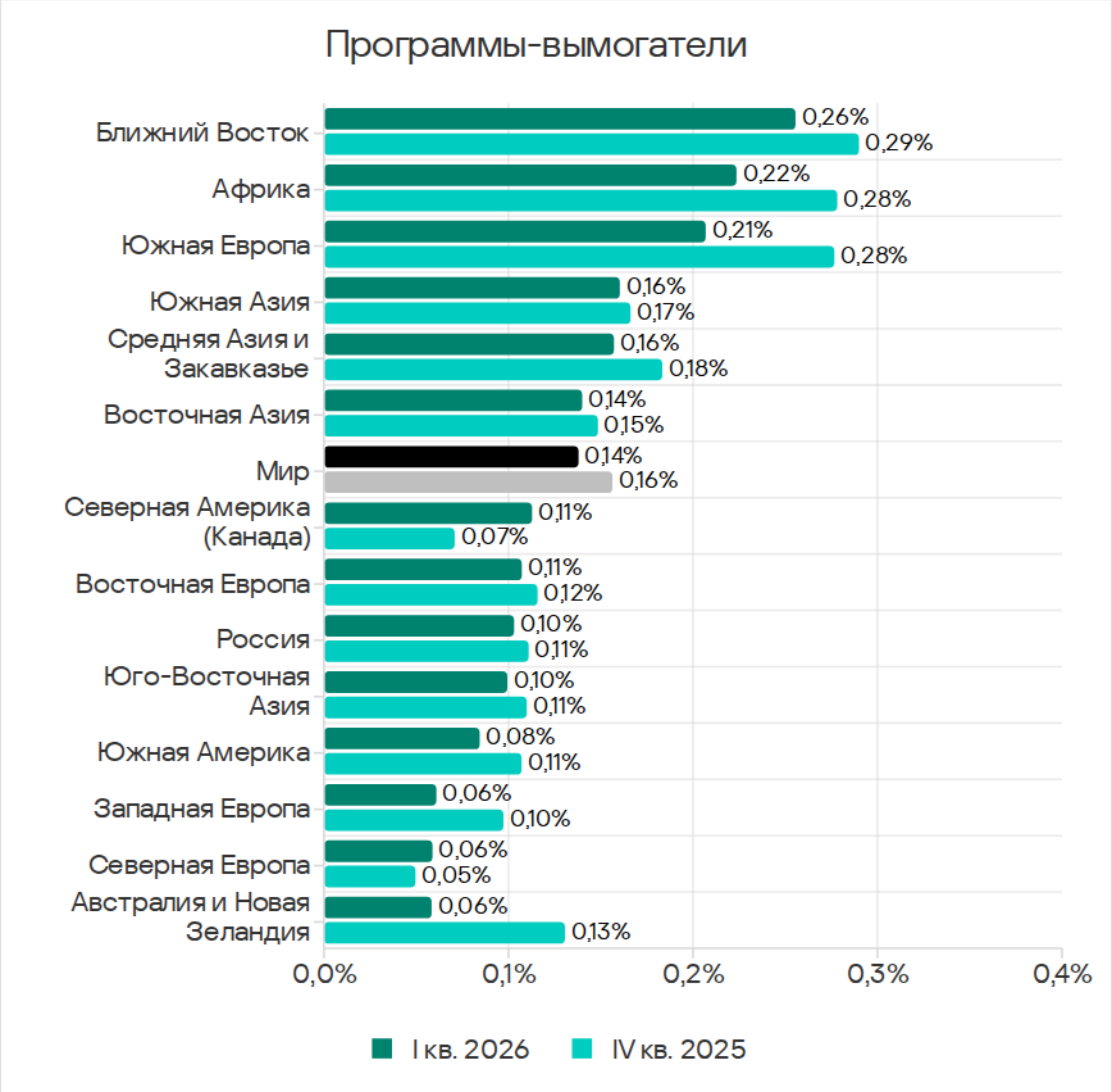
Программы-вымогатели

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, II квартал 2023 года — I квартал 2026 года

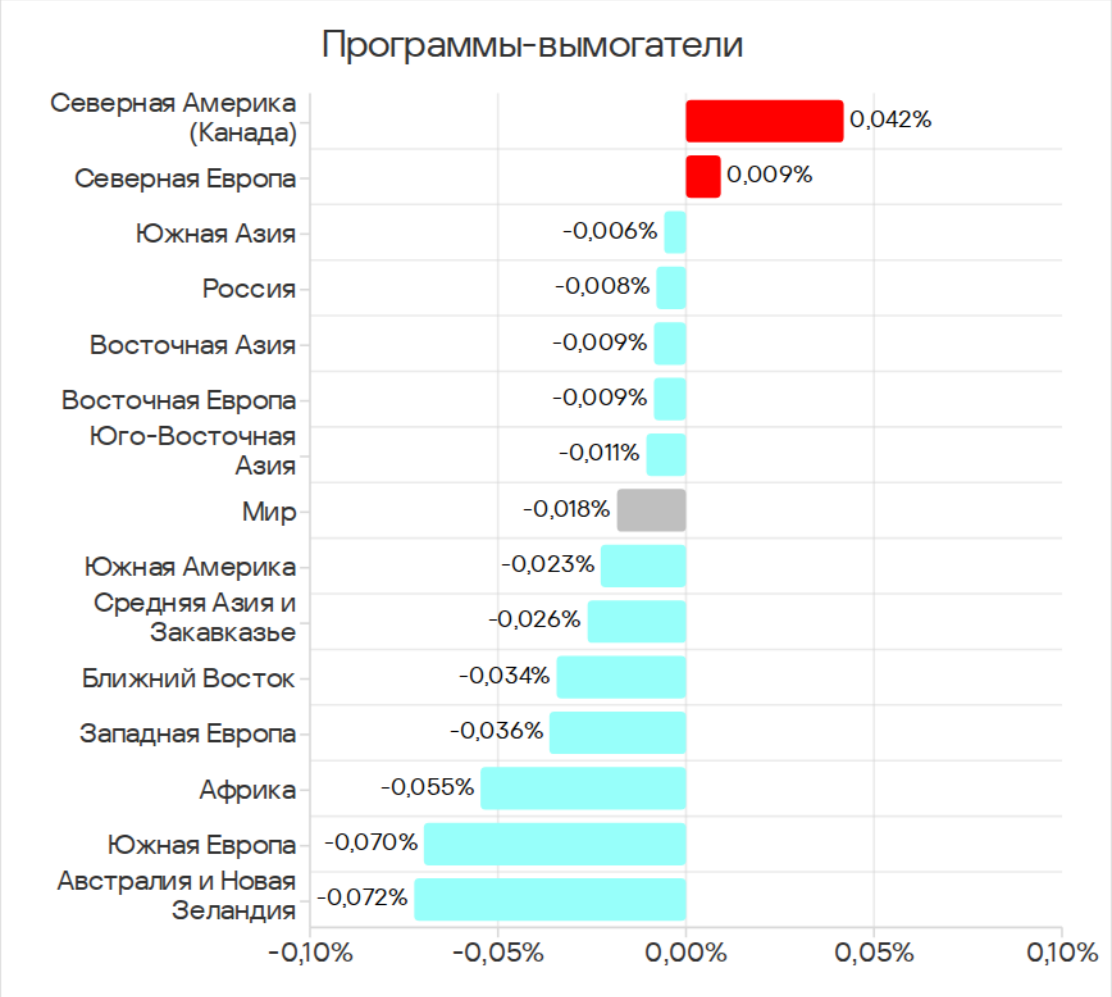


Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели



Изменение доли компьютеров АСУ, на которых были заблокированы программы-вымогатели, I квартал 2026 года



Майнеры — исполняемые файлы для ОС Windows

Наряду с «классическими» майнерами — приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют, — появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры криптовалют на компьютеры АСУ.

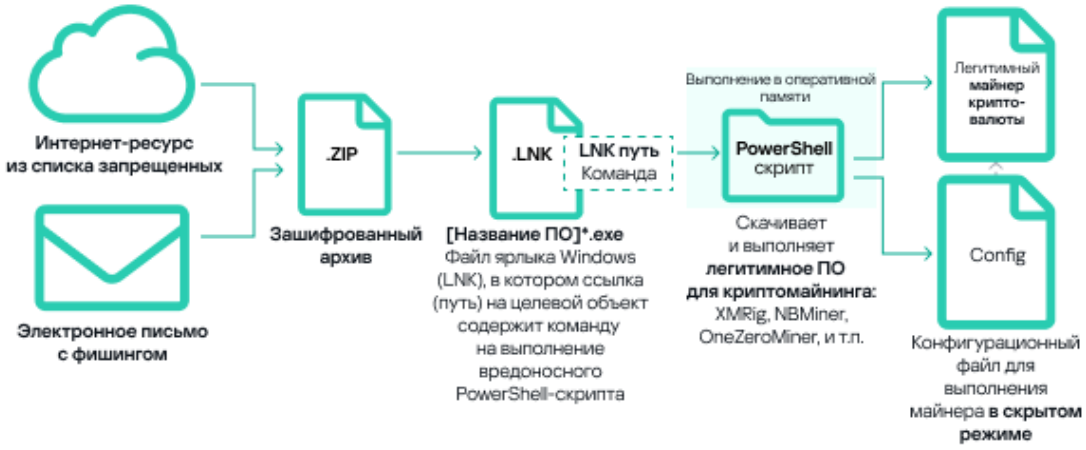
Значительная часть майнеров для ОС Windows, обнаруженных на компьютерах АСУ, представляет собой архивы, названия которых имитировали легальное программное обеспечение. Эти архивы не содержат реального программного обеспечения, но включают в себя файл формата Windows LNK, более известный как ярлык. Однако целевой объект (или путь), на который указывает LNK-файл, не является обычным приложением, а представляет собой команду, которая может выполнить вредоносный код, например, скрипт PowerShell. Злоумышленники все чаще выбирают PowerShell, с помощью которого код вредоносного ПО (в том

числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом. Бесфайловое выполнение майнера делает проблематичным его обнаружение средствами защиты.

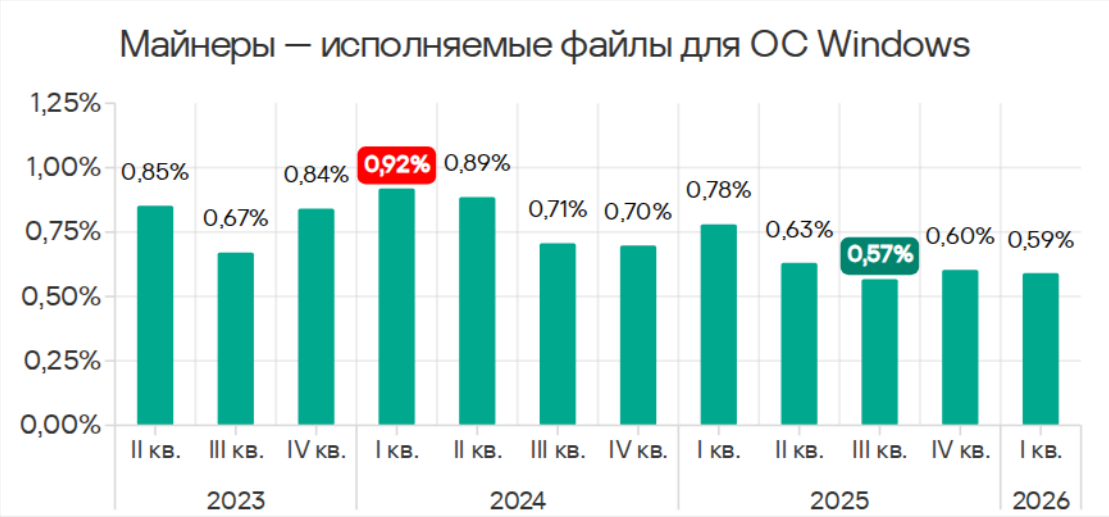
Цепочка атаки: пример бесфайлового исполнения в майнинговых атаках

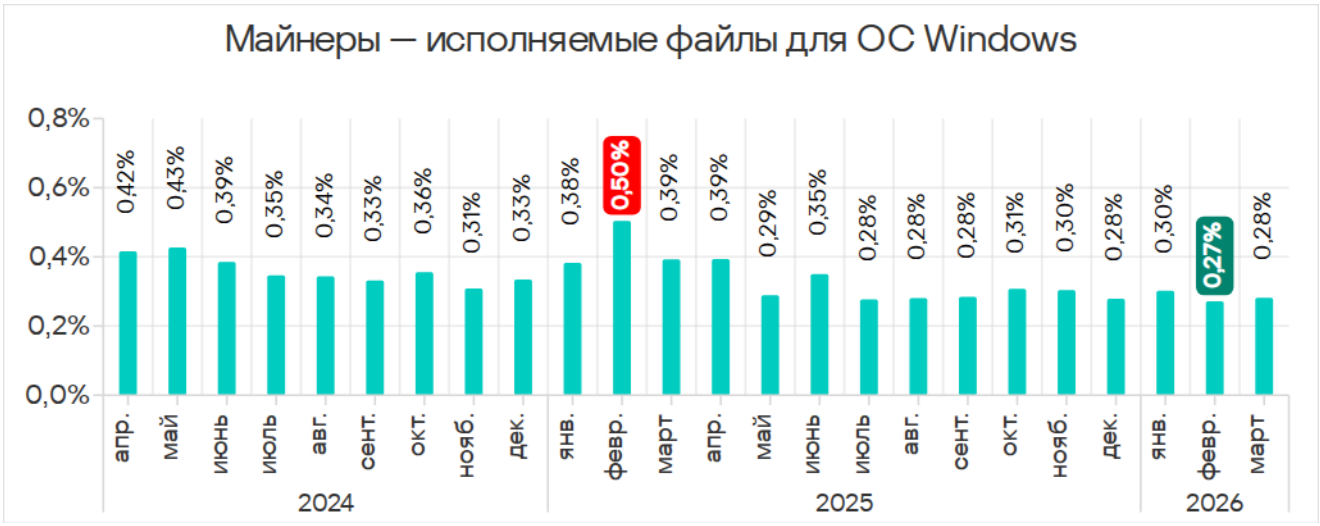
Еще одним популярным методом внедрения майнеров в технологическую инфраструктуру является использование легитимных криптомайнеров, таких как XMRig, NBMiner, OneZeroMiner и т. д. Сами по себе эти майнеры не являются вредоносными, однако защитные системы классифицируют их как RiskTools. Злоумышленники используют такие майнеры со специфическими файлами конфигурации, позволяющими скрыть активность майнера от пользователя.

Цепочка атаки: пример с использованием легитимных крипто-майнеров



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, II квартал 2023 года — I квартал 2026 года

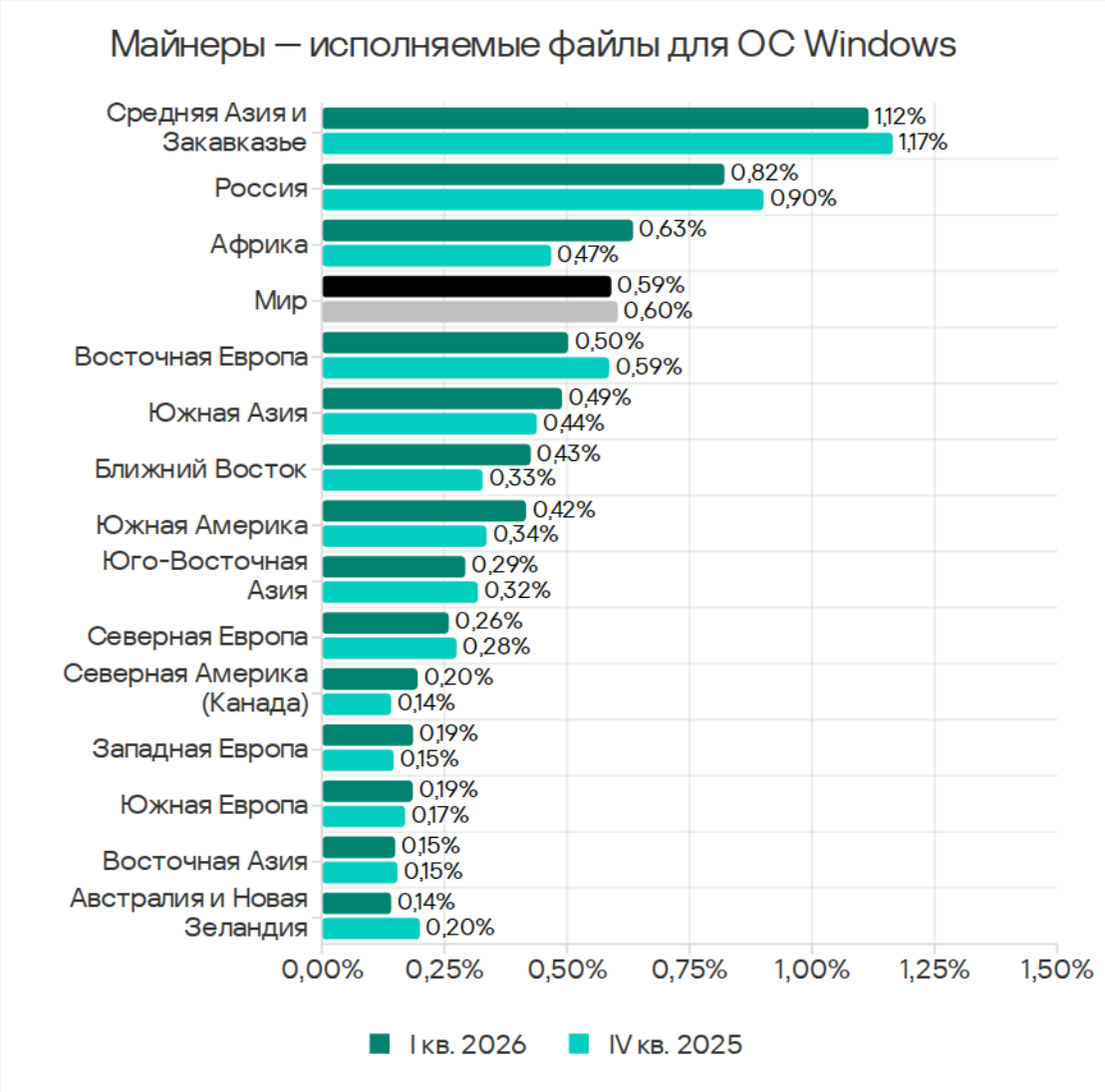




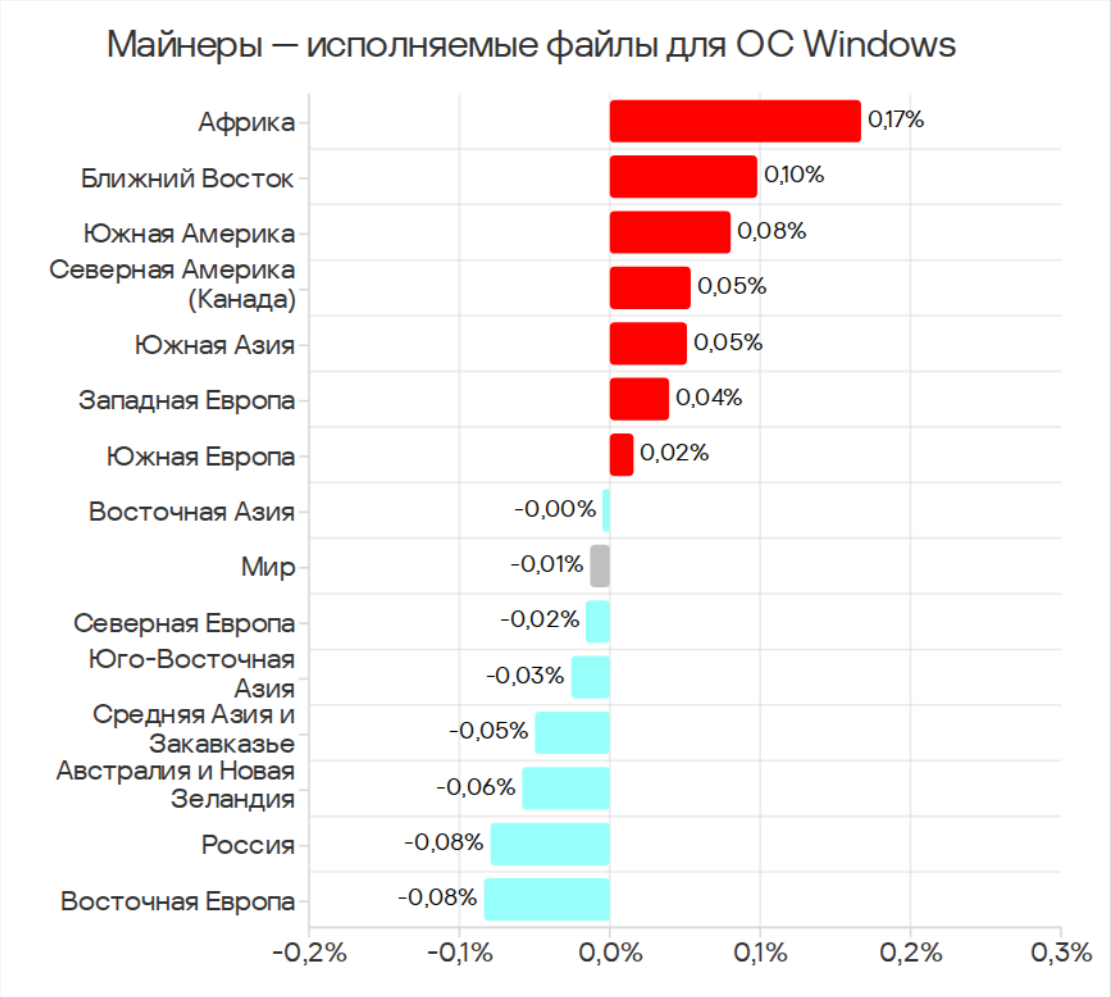
Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, апрель 2024 года — март 2026 года

В феврале 2026 года месячный показатель был наименьшим за рассматриваемый период.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows

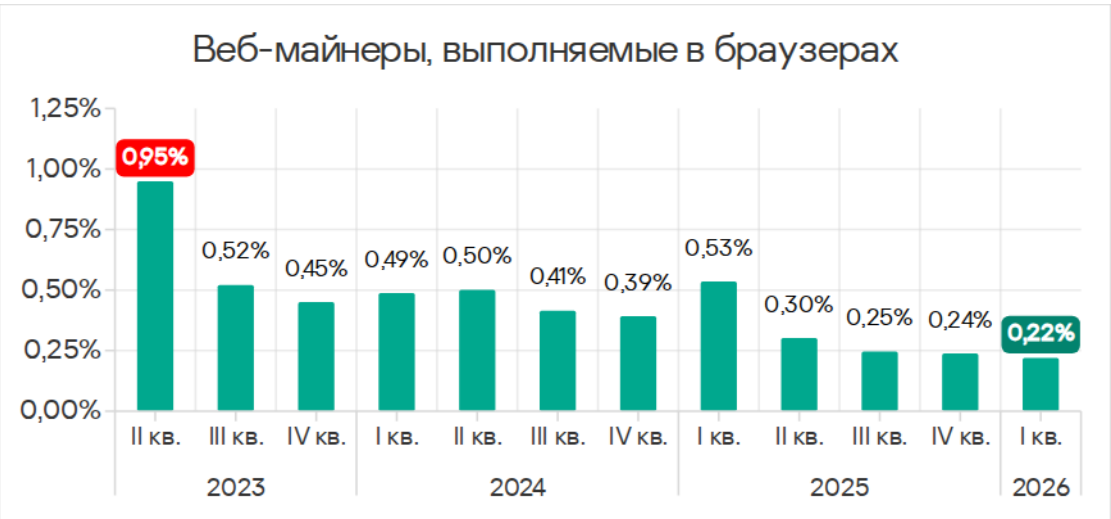


Изменение доли компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2026 года



Веб-майнеры

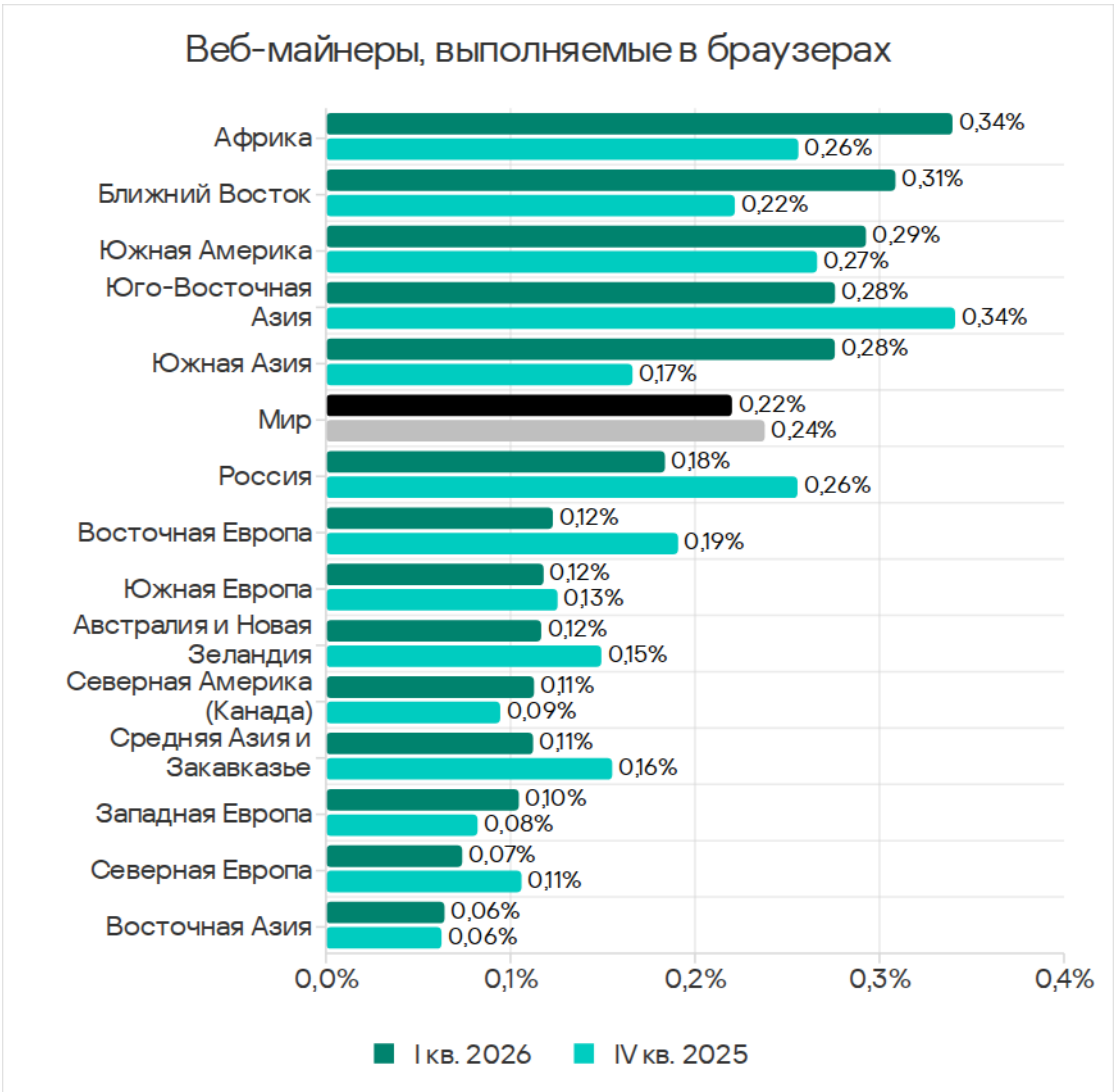
Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, II квартал 2023 года — I квартал 2026 года



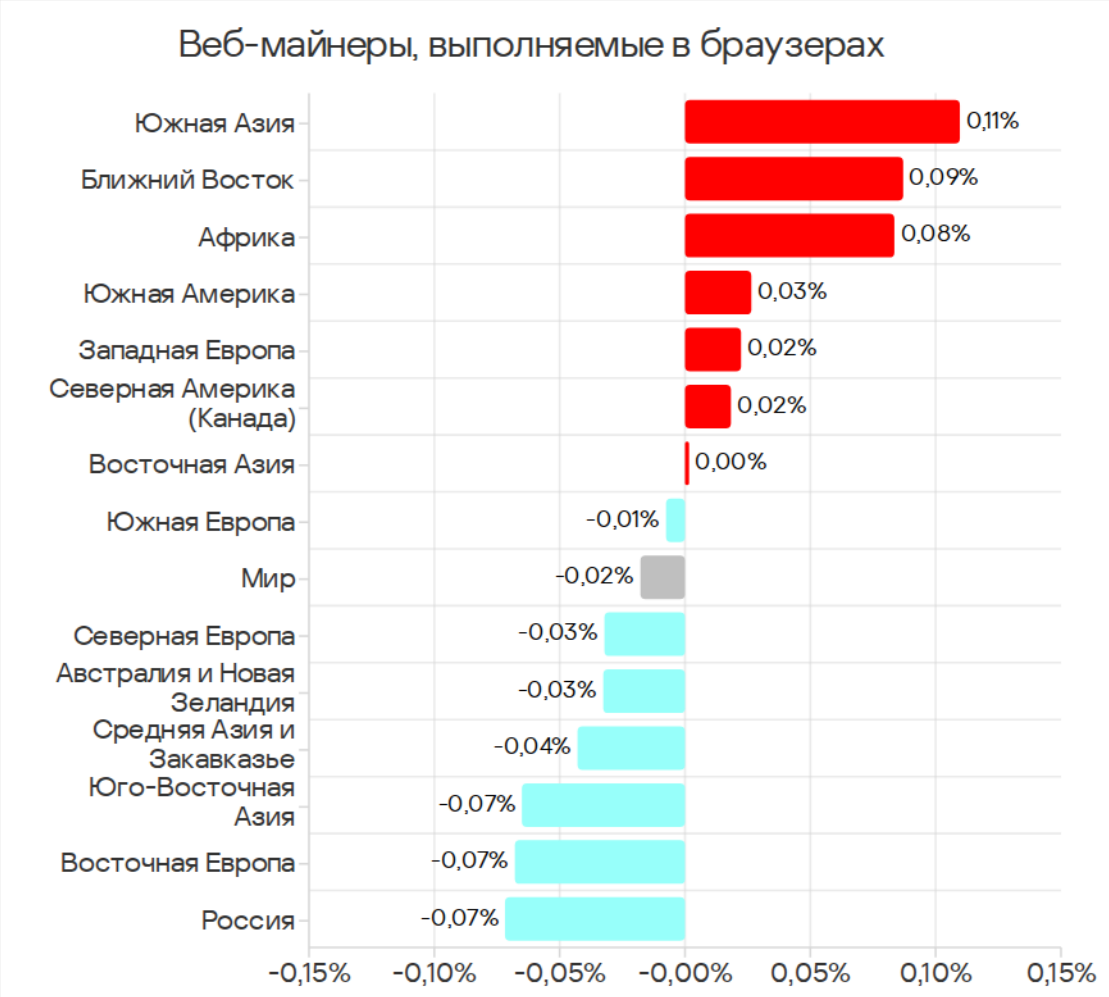
В феврале 2026 года месячный показатель также был наименьшим за рассматриваемый период.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах



Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, I квартал 2026 года



Самораспространяющееся вредоносное ПО. Черви и вирусы

Самораспространяющееся вредоносное ПО — черви и вирусы — относится к отдельной категории. Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнетов, приобрели черты угроз следующего этапа.

Вирусы и черви в основном распространяются в сетях АСУ через съемные носители и сетевые папки в форме зараженных файлов — архивов с бэкапами, офисными документами, пиратскими играми и взломанными приложениями. В более редких и опасных случаях зараженными оказываются веб-страницы с настройками сетевого оборудования, а также файлы, хранящиеся во внутренних системах документооборота, управления жизненным циклом продукта (PLM), управления ресурсами (ERP) и других интранет-сервисах.

Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры.

Следует иметь в виду, что распространение может происходить и в активной форме — с использованием техник перебора пароля, кражи и использования данных аутентификации пользователя (включая токены доступа), а также сетевых атак на уязвимое ПО — все это давно входит в модульный инструментарий любого современного майнера-червя.

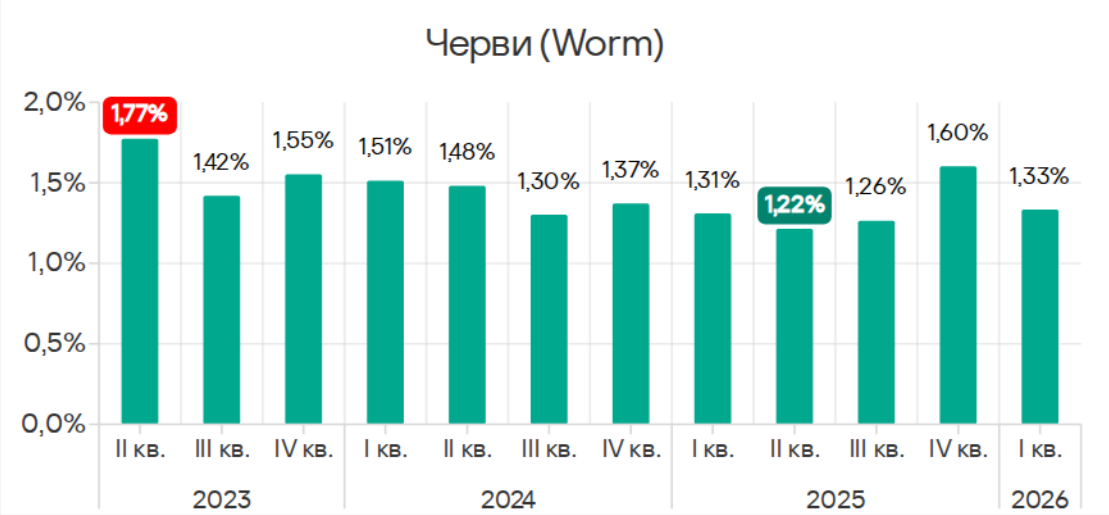
Современные версии червей встречаются в сетях АСУ не часто, но наносимый в случае заражения ущерб всегда значительный — даже простое обслуживание сети, зараженной майнерами-червями, становится кратно дороже из-за большего времени простоя (downtime) и дополнительных человеко-часов, необходимых для восстановления работоспособности. А в случае загрузки через червя на компьютер в технологической сети программы-вымогателя после предварительного профилирования — дороже на порядок.

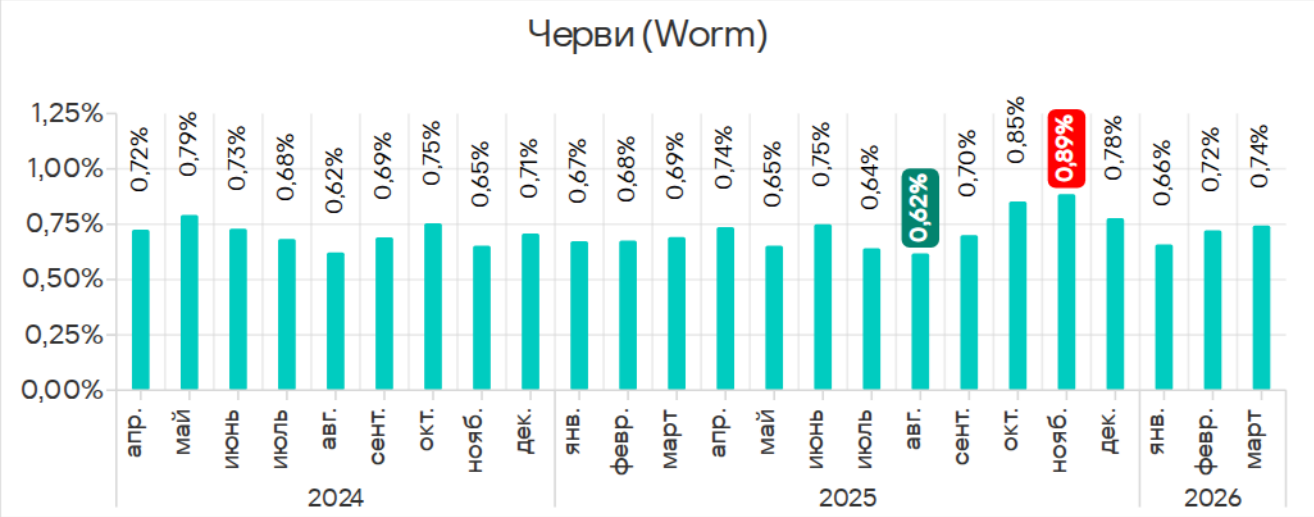
Вместе с тем, среди распространяющихся вирусов и червей довольно много старых модификаций, их командные серверы уже отключены. Тем не менее, они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, но также могут приводить к сбоям в работе ПО, отказам в обслуживании и т. п.

Высокие показатели обнаружения самораспространяющегося вредоносного ПО и ПО, которое распространяется через сетевые папки, на уровне отрасли, страны или региона, как правило, указывают на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных устройств. Эти незащищенные компьютеры становятся источниками распространения вредоносного ПО. Ситуацию может ухудшать и слабая сегментация сети предприятия, и отсутствие контроля использования съемных носителей информации.

Черви

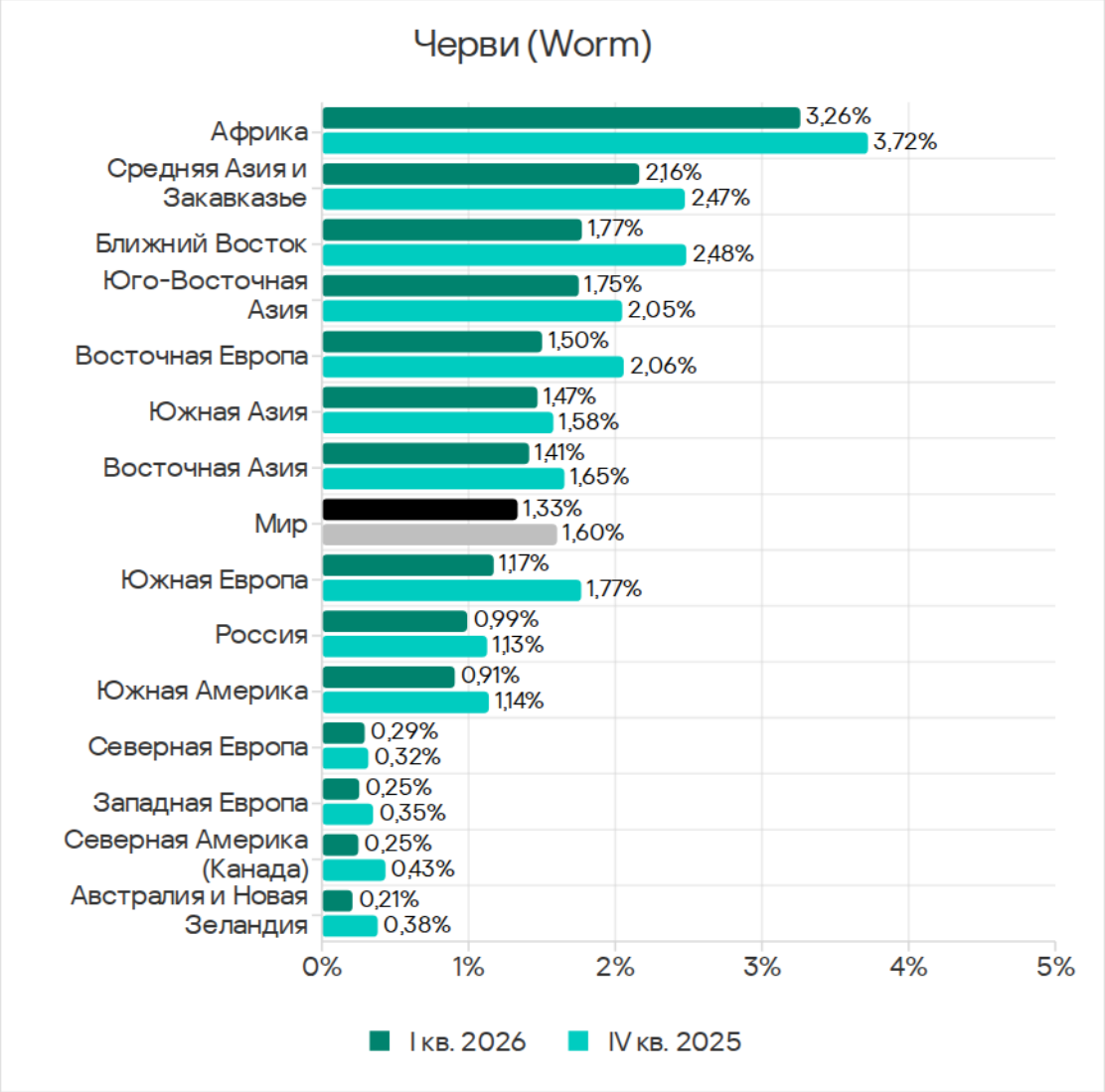
Доля компьютеров АСУ, на которых были заблокированы черви, II квартал 2023 года — I квартал 2026 года



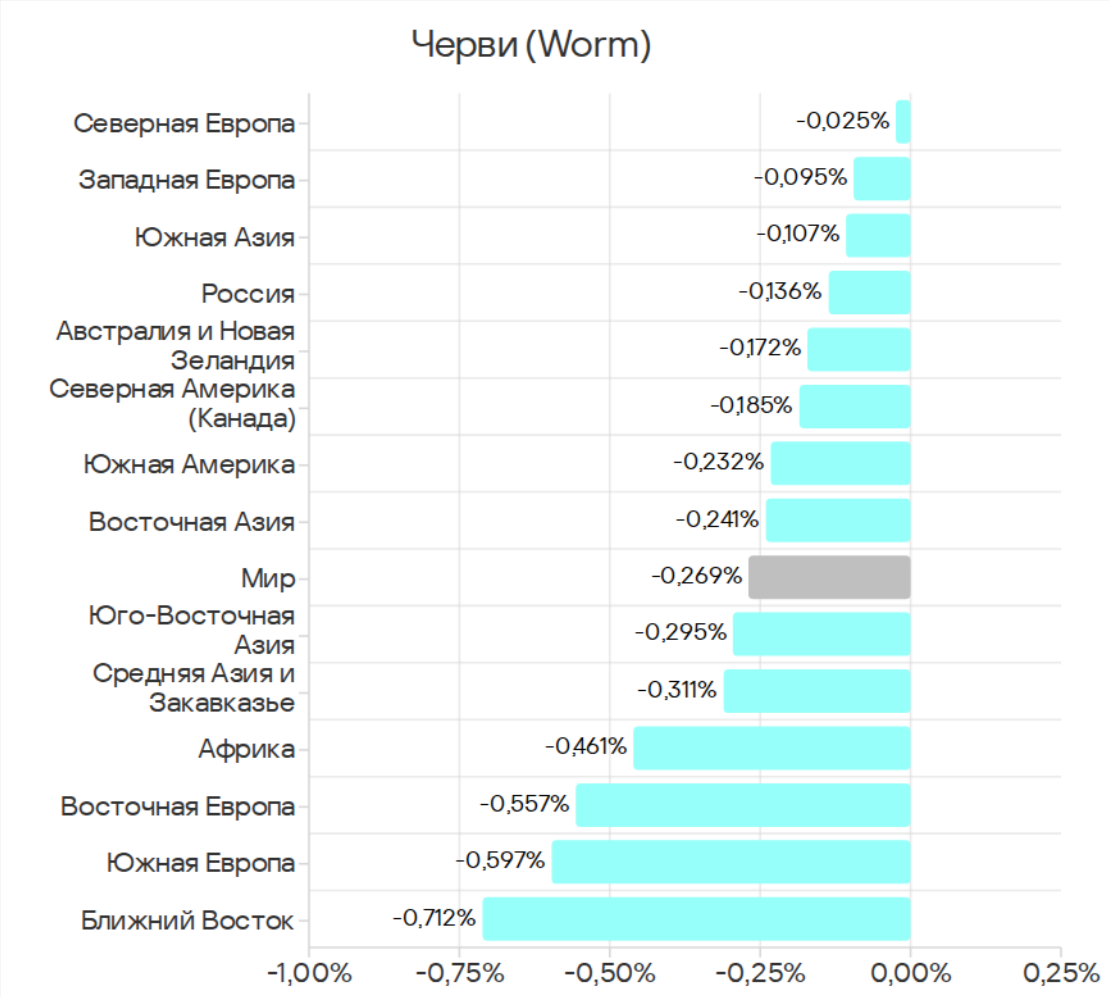


Доля компьютеров АСУ, на которых были заблокированы черви, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы черви

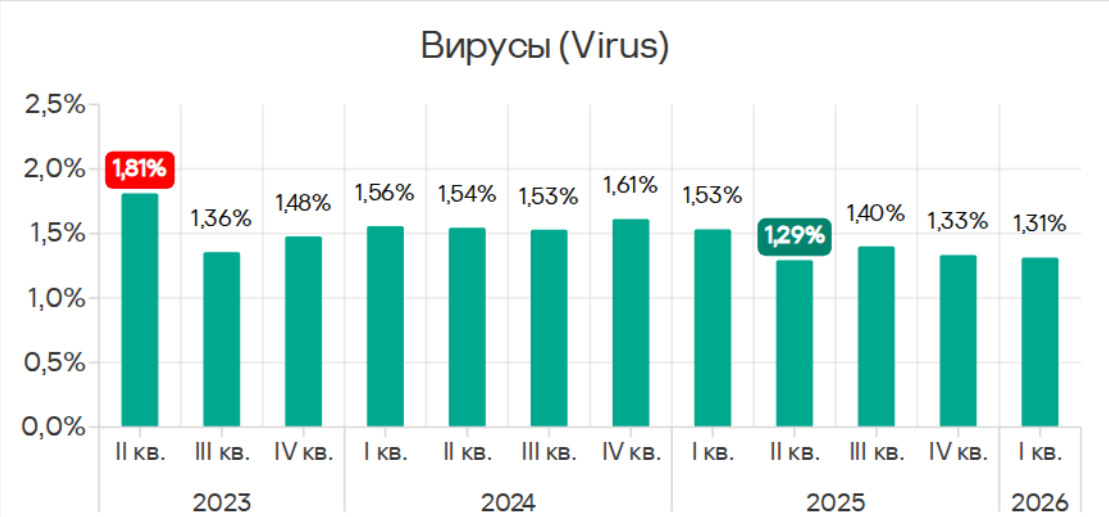


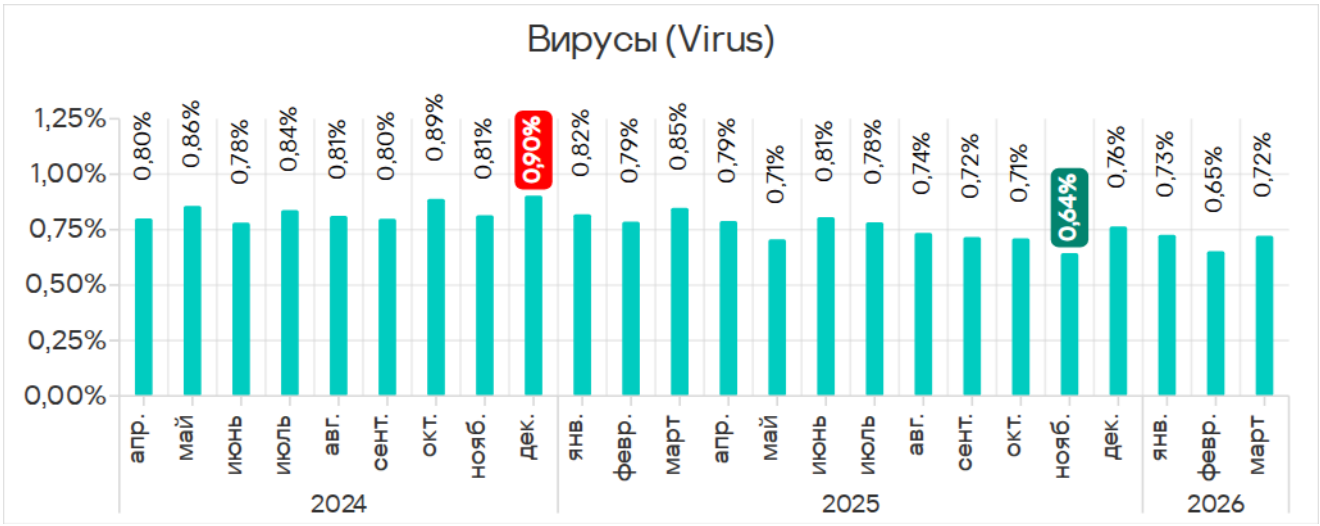
Изменение доли компьютеров АСУ, на которых были заблокированы черви, I квартал 2026 года



Вирусы

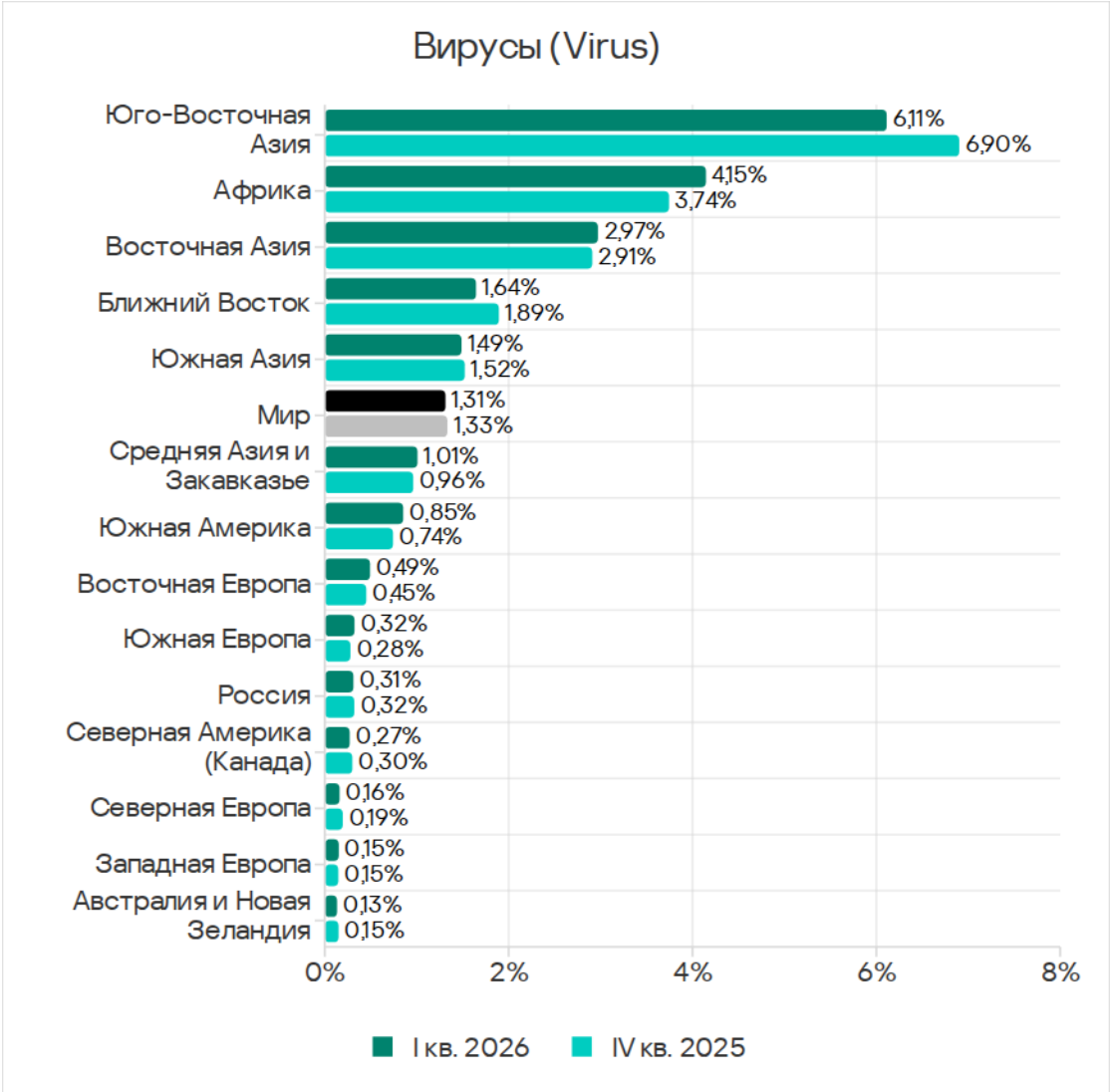
Доля компьютеров АСУ, на которых были заблокированы вирусы, II квартал 2023 года — I квартал 2026 года



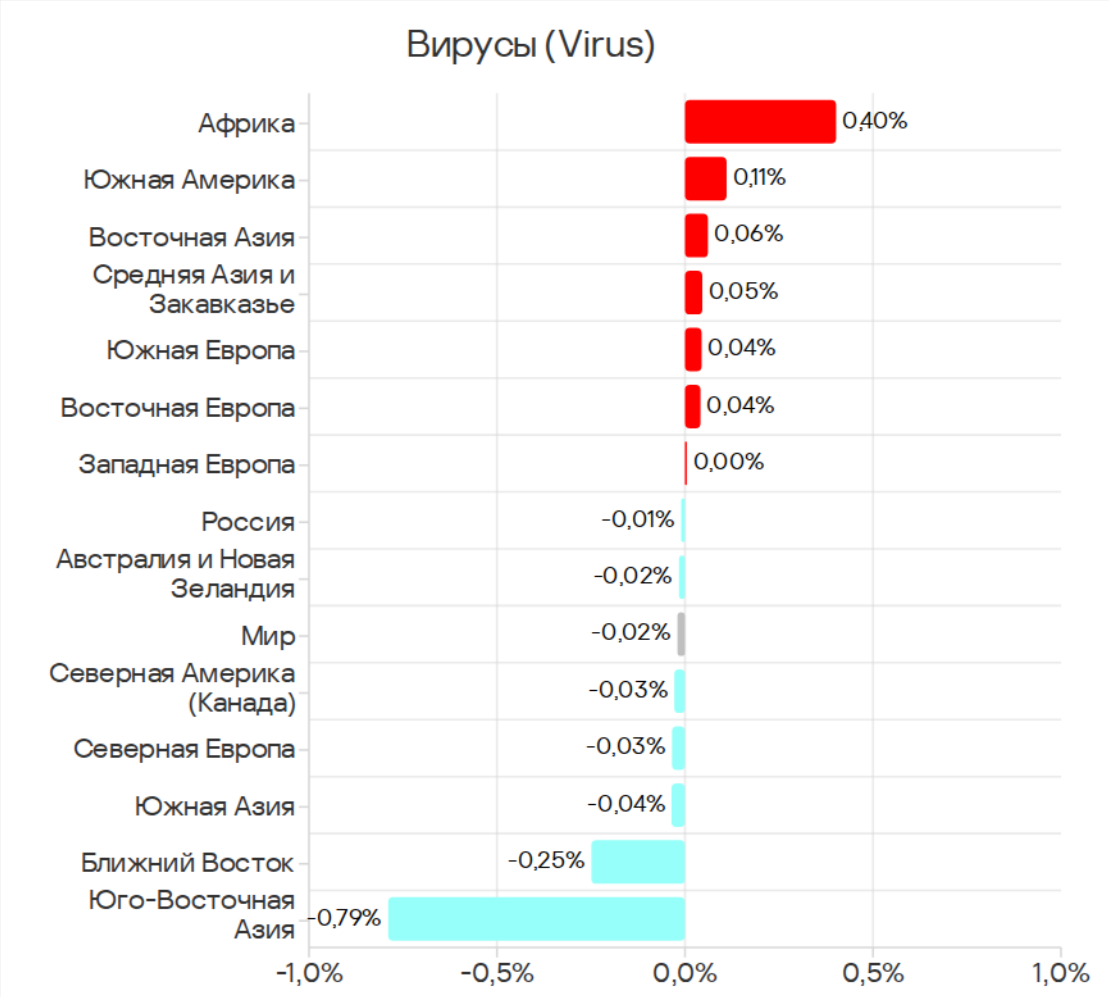


Доля компьютеров АСУ, на которых были заблокированы вирусы, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вирусы



Изменение доли компьютеров АСУ, на которых были заблокированы вирусы, I квартал 2026 года

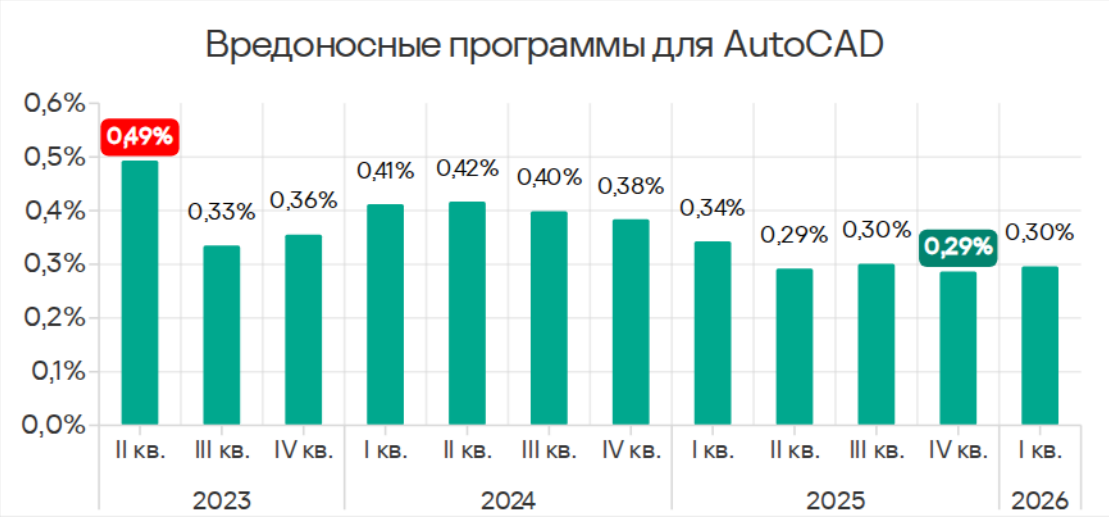


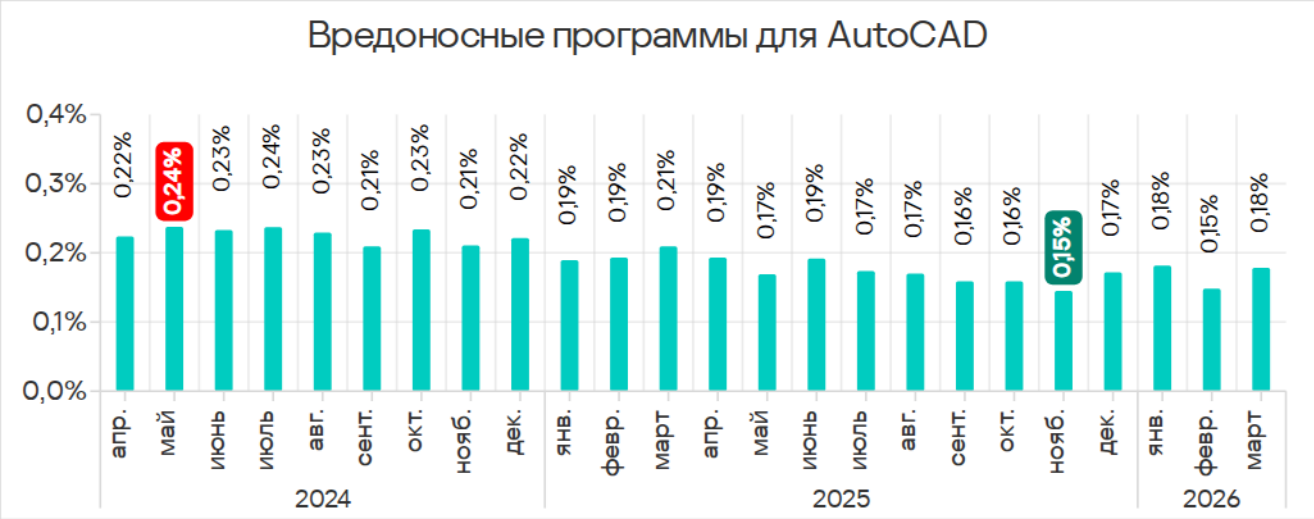
Вредоносные программы для AutoCAD

Эта категория вредоносного ПО может распространяться по-разному, поэтому не относится к конкретной группе.

Как правило, вредоносные программы для AutoCAD — минорная угроза, которая в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых она была заблокирована, занимает последние места.

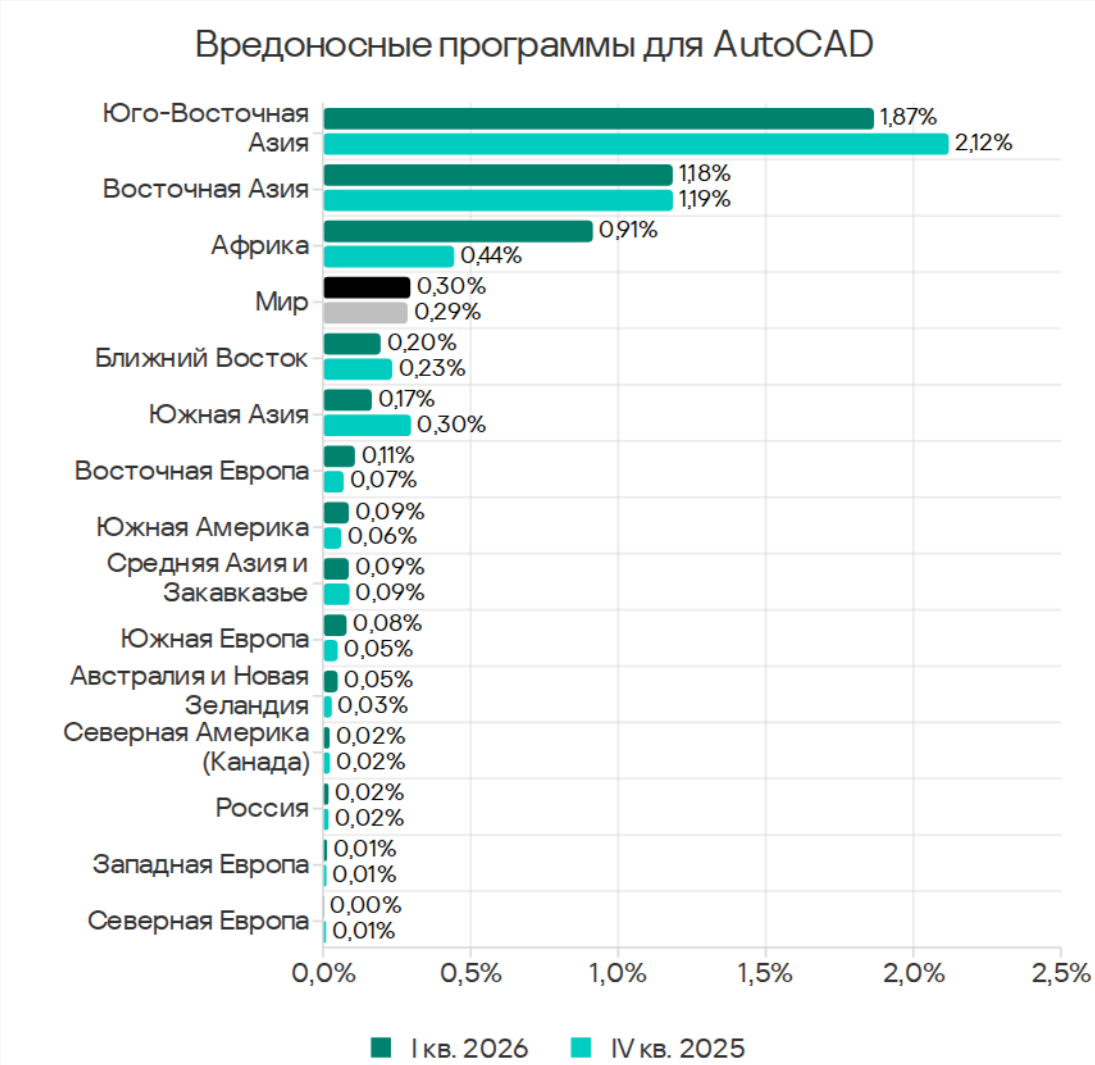
Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, II квартал 2023 года — I квартал 2026 года



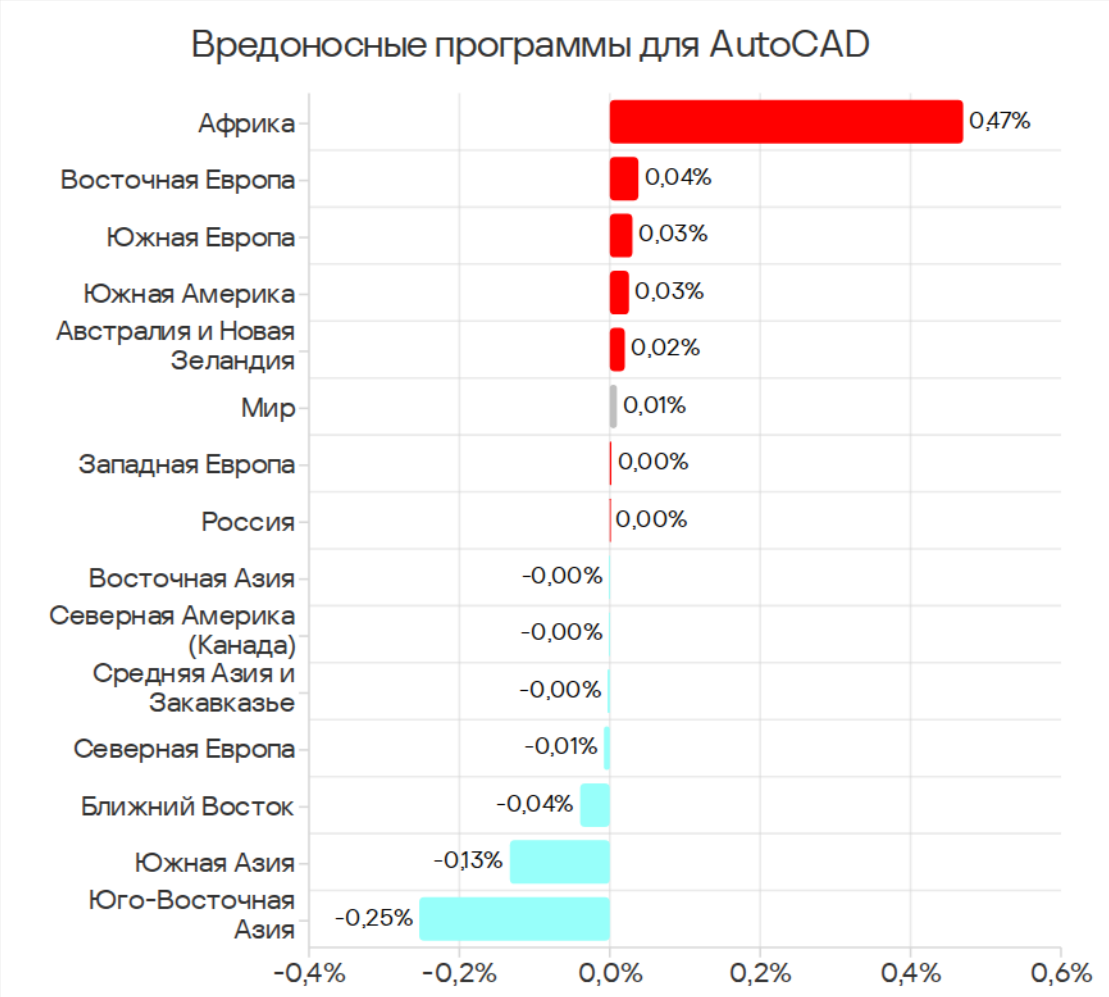


Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, апрель 2024 года — март 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, I квартал 2026 года

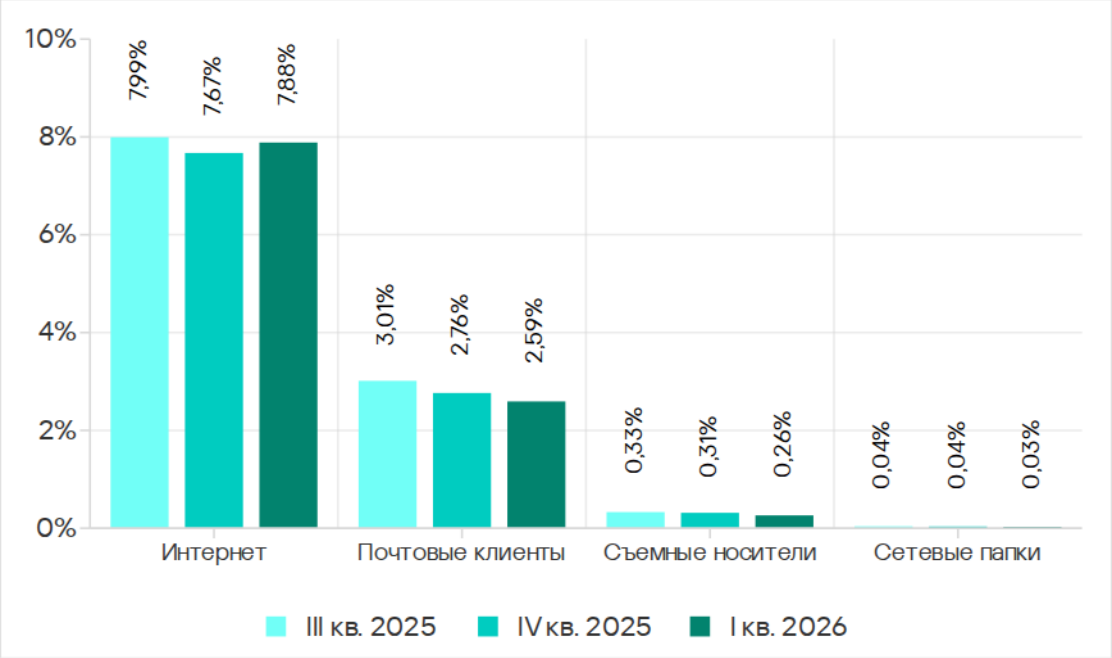


Основные источники угроз

В зависимости от сценария обнаружения и блокирования угрозы не всегда возможно надежно определить ее источник. Косвенным признаком того или иного источника может быть вид (категория) заблокированной угрозы.

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет (обращения к вредоносным или скомпрометированным интернет-ресурсам; вредоносный контент, распространяемый через мессенджеры; облачные сервисы хранения и обработки данных и CDN), почтовые клиенты (фишинговые рассылки) и съемные носители.

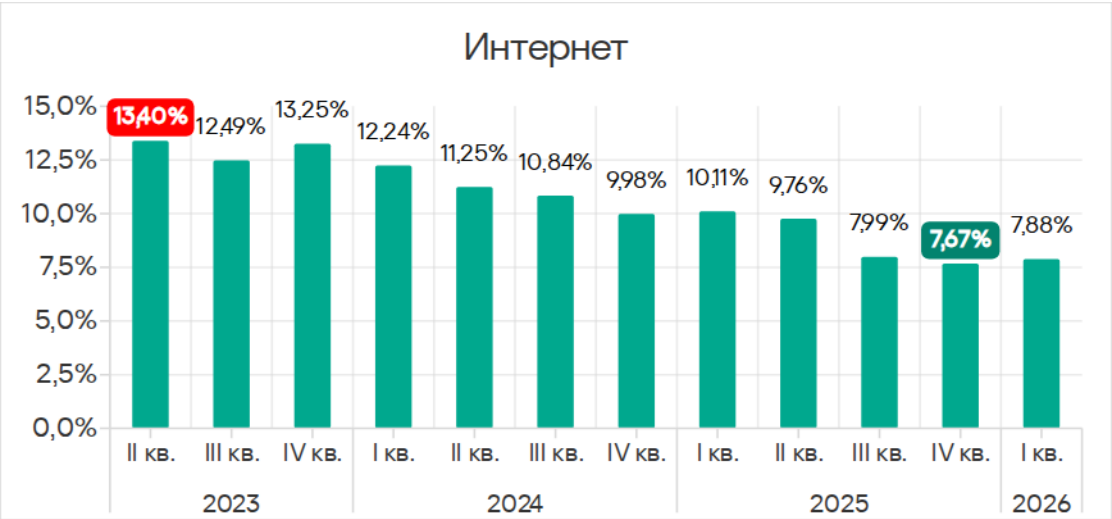
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников



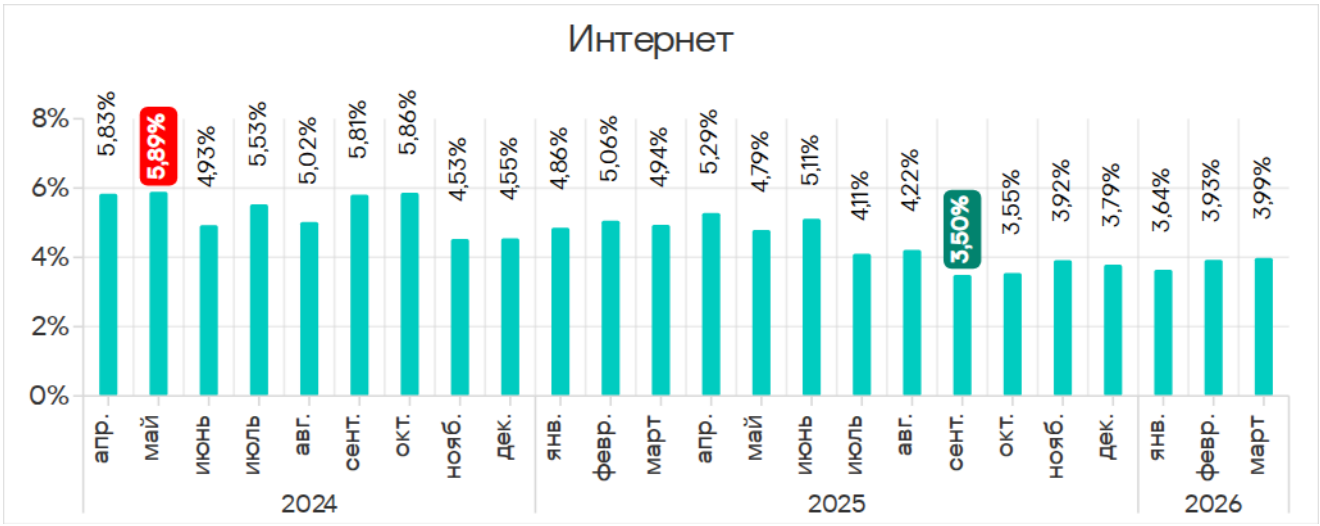
Интернет

Обнаружение и блокирование угроз из интернета на компьютерах АСУ, защищенных решением «Лаборатории Касперского», означает, что на момент обнаружения на них был разрешен доступ к внешним сервисам.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, II квартал 2023 года — I квартал 2026 года

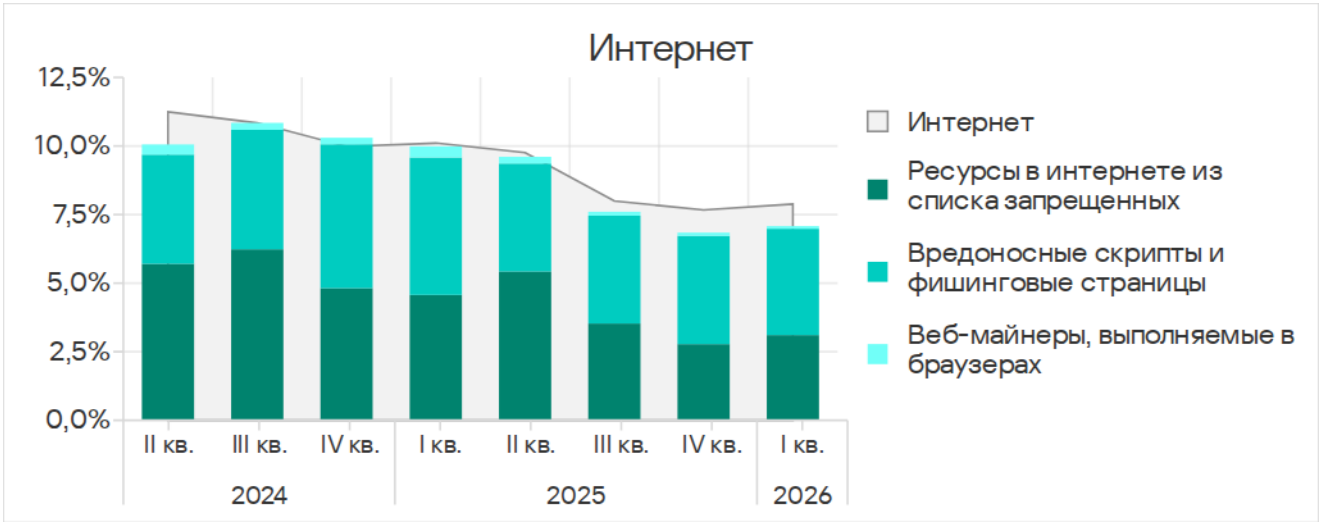


Месячный показатель в первом квартале 2026 года рос два месяца подряд.



Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, апрель 2024 года — март 2026 года

Основные категории угроз из интернета*, которые были заблокированы на компьютерах АСУ в первом квартале 2026 года, — это вредоносные скрипты и фишинговые страницы, а также ресурсы в интернете из списка запрещенных.

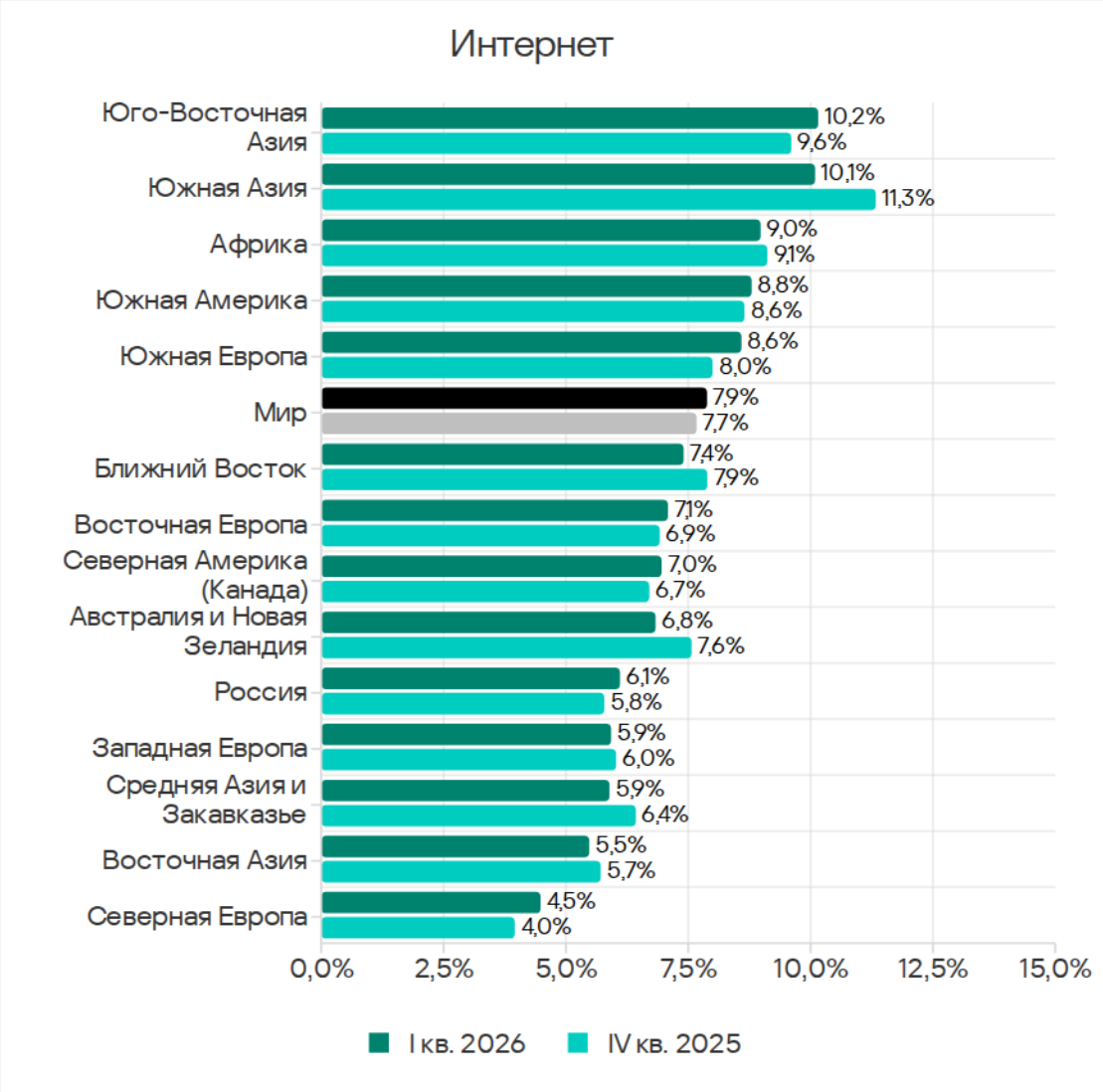


Угрозы из интернета и основные категории угроз из интернета, II квартал 2024 года — I квартал 2026 года

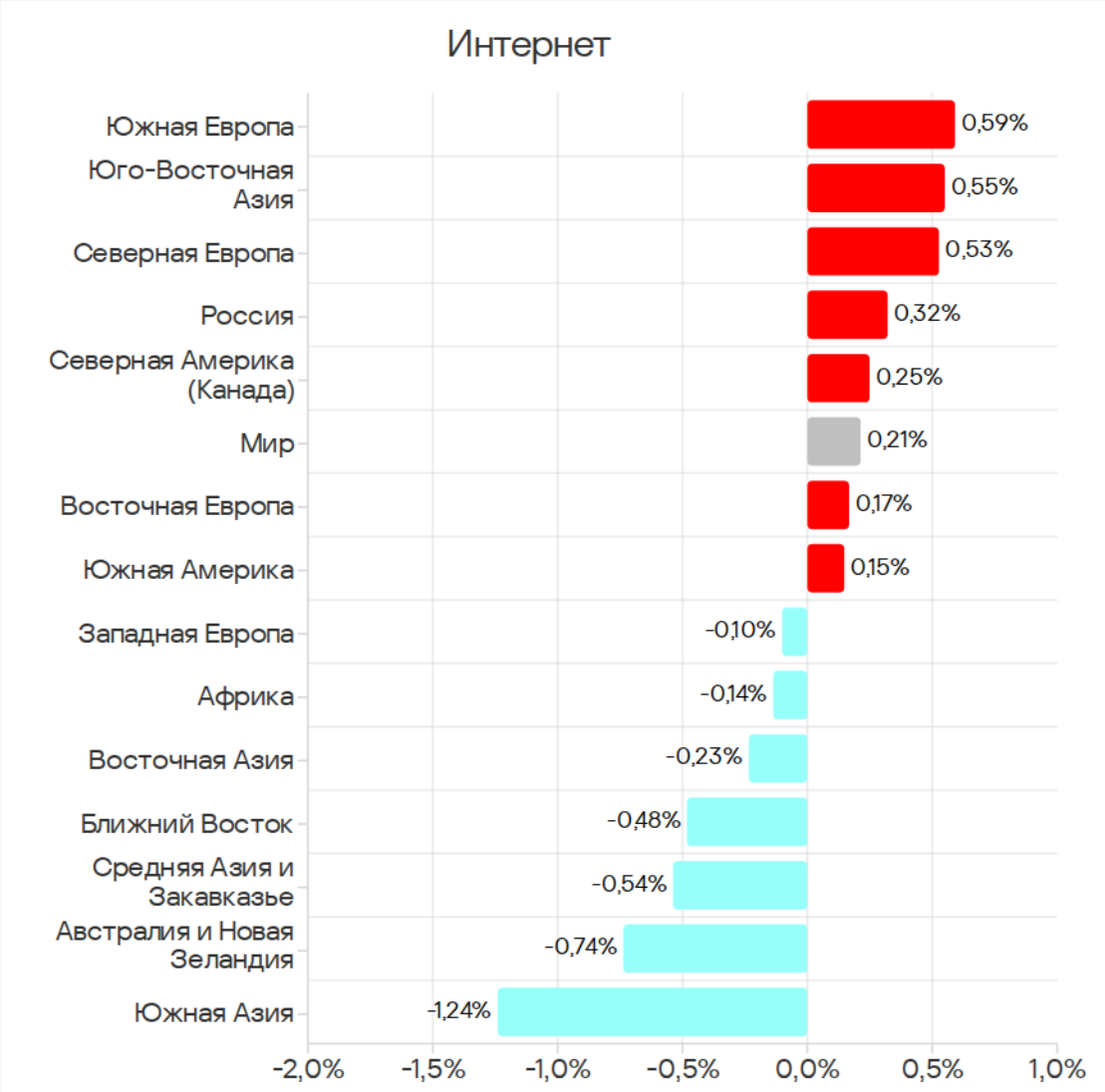
*Напомним, что один и тот же компьютер в течение квартала может быть атакован несколькими категориями вредоносного ПО, которое распространяется из одного источника. Такой компьютер будет учтен при подсчете процента атакованных компьютеров для каждой категории угроз, но для источника угрозы будет учитываться лишь один раз (мы считаем уникальные атакованные компьютеры). К тому же, однозначно определить источник первоначальной попытки заражения не всегда представляется возможным. Поэтому суммарная доля компьютеров АСУ, на которых были заблокированы

различные категории угроз из определенного источника, может превышать долю угроз из самого источника.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета



Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, I квартал 2026 года



Почтовые клиенты

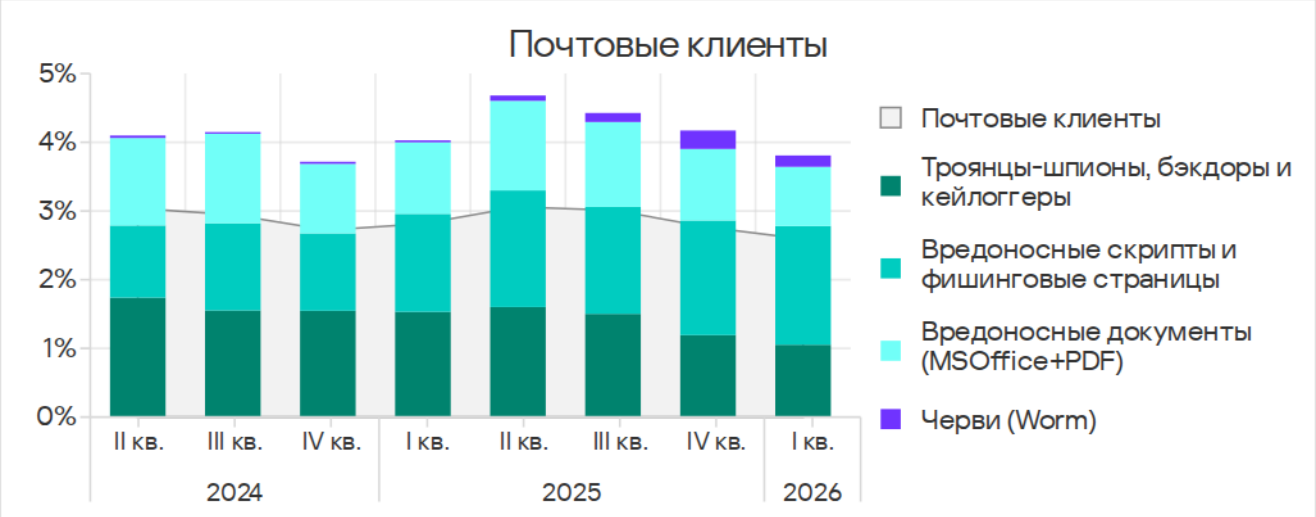
Некоторые из обнаруженных и заблокированных угроз были доставлены на защищенные компьютеры системой доставки почты и/или пытались получить доступ через клиентское приложение электронной почты.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, II квартал 2023 года — I квартал 2026 года

В январе месячный показатель был наименьшим за два года.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, апрель 2024 года — март 2026 года

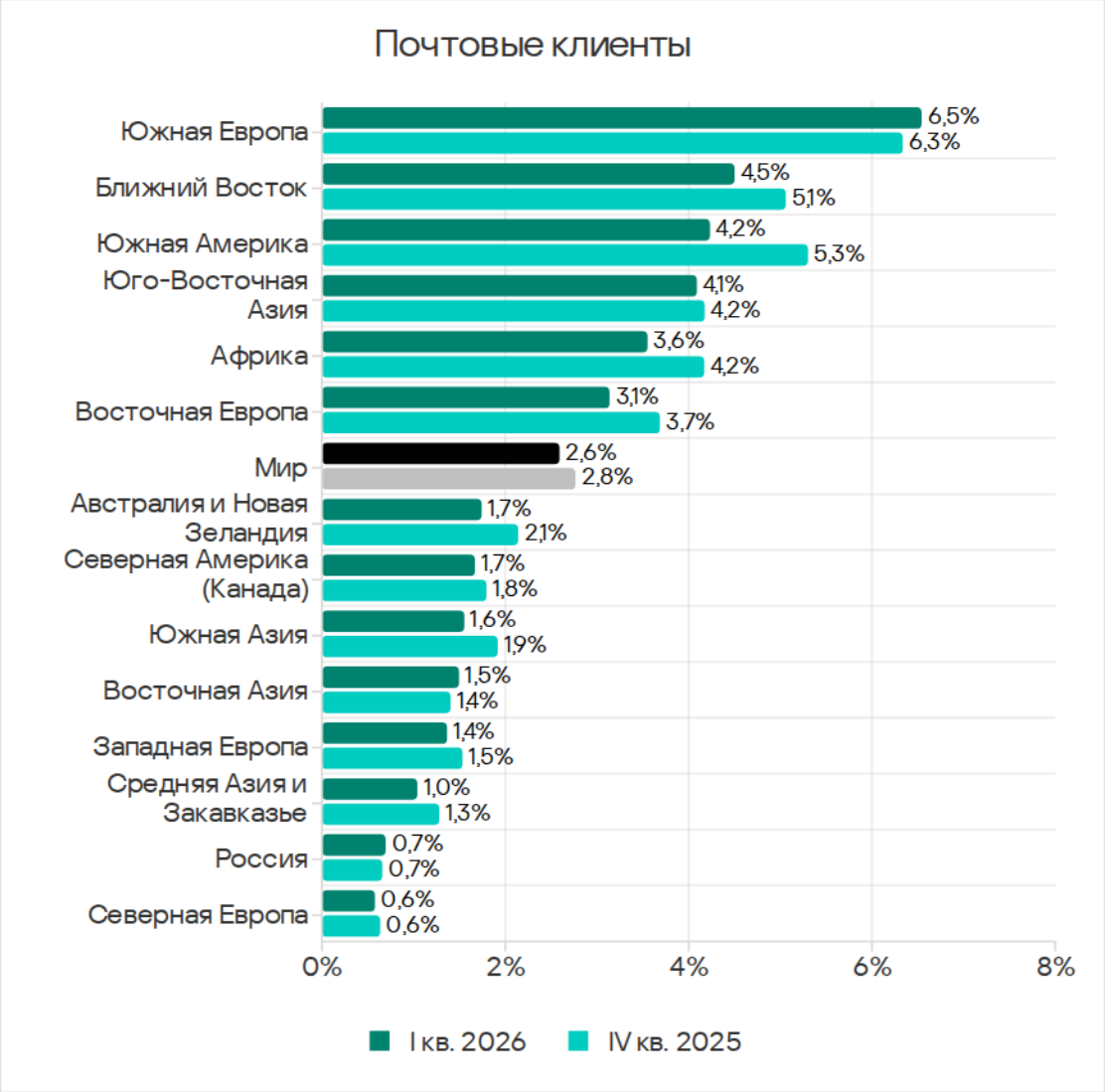
Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ в первом квартале 2026 года: вредоносные скрипты и фишинговые страницы, шпионское ПО, а также вредоносные документы. Доля компьютеров, на которых были заблокированы черви из почтовых клиентов, уменьшилась, но все еще заметна.



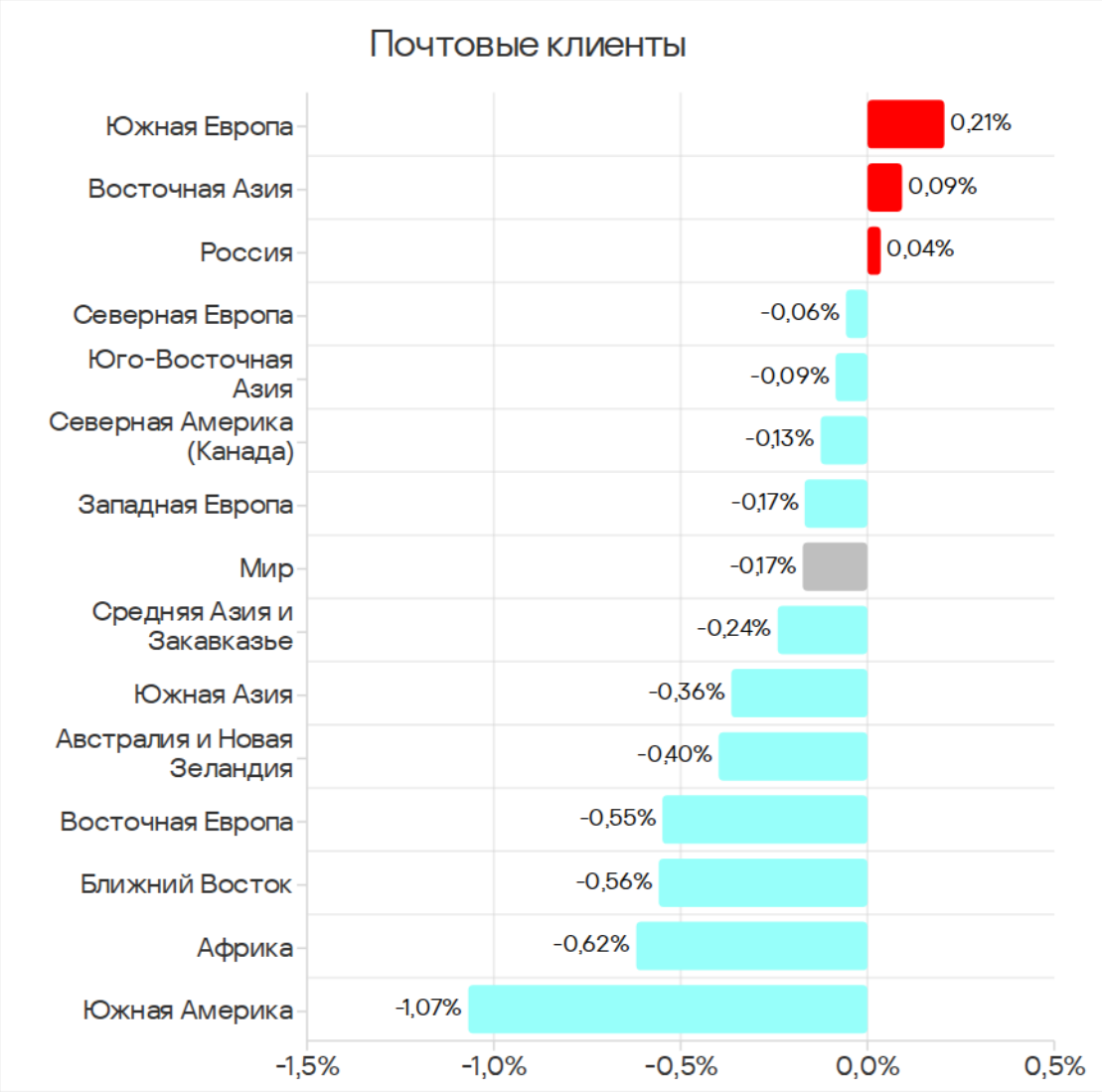
Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов, I квартал 2024 года — I квартал 2026 года

Большинство шпионских программ, обнаруженных в фишинговых письмах, доставлялись в форме архива с паролем или многослойного скрипта, встроенного в файлы офисных документов.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов

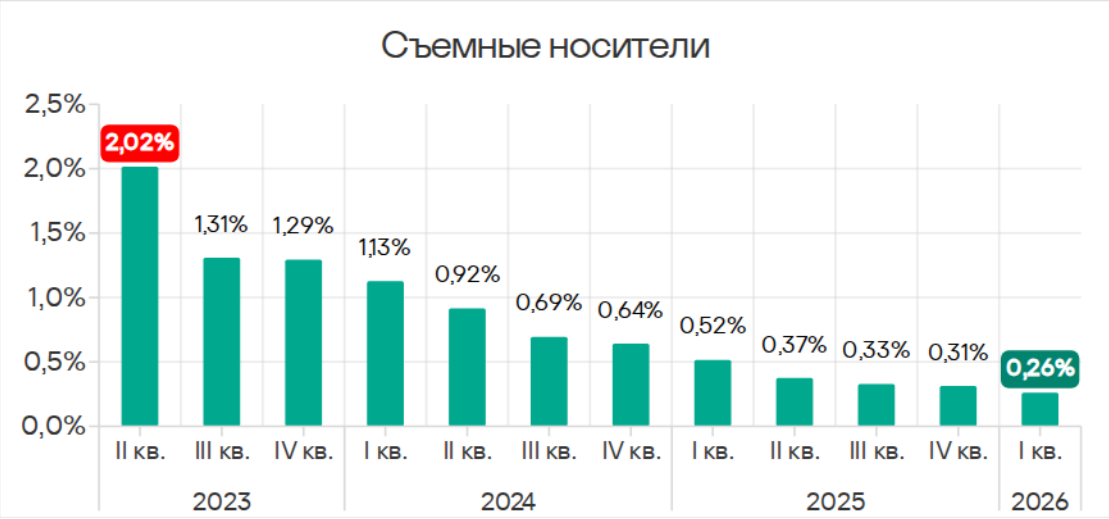


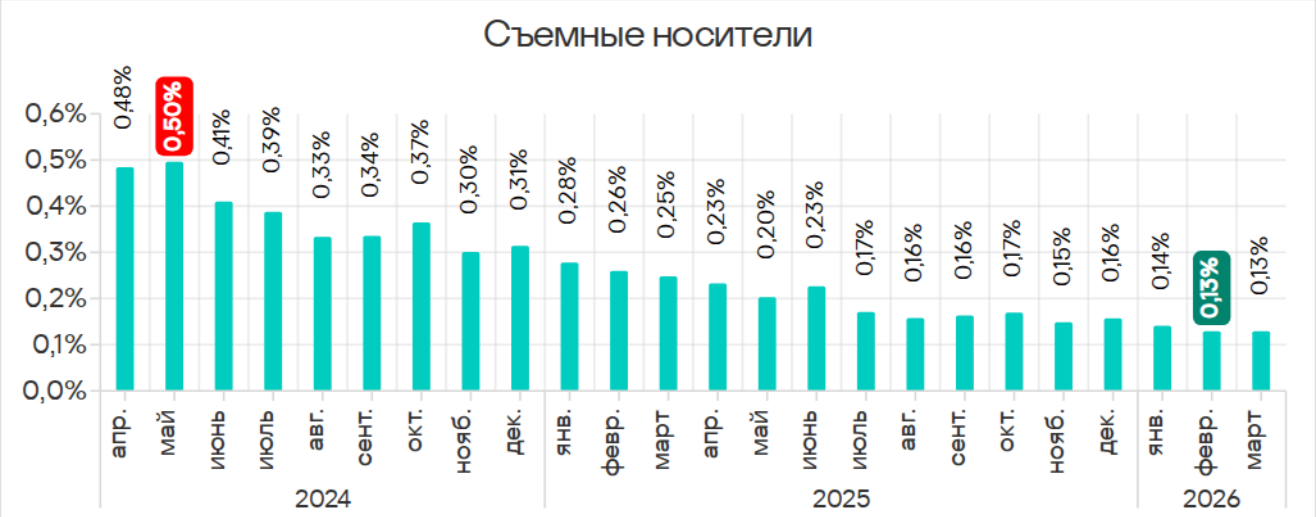
Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, I квартал 2026 года



Съемные носители

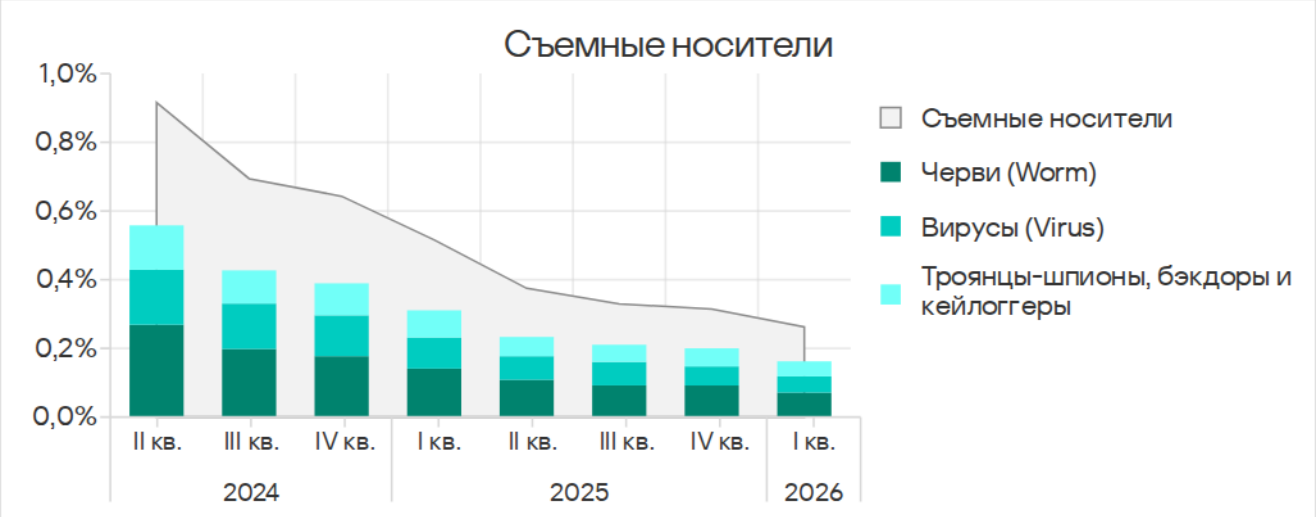
Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, II квартал 2023 года — I квартал 2026 года





Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, апрель 2024 года — март 2026 года

Основные категории угроз, которые в первом квартале 2026 года были заблокированы при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионское ПО.



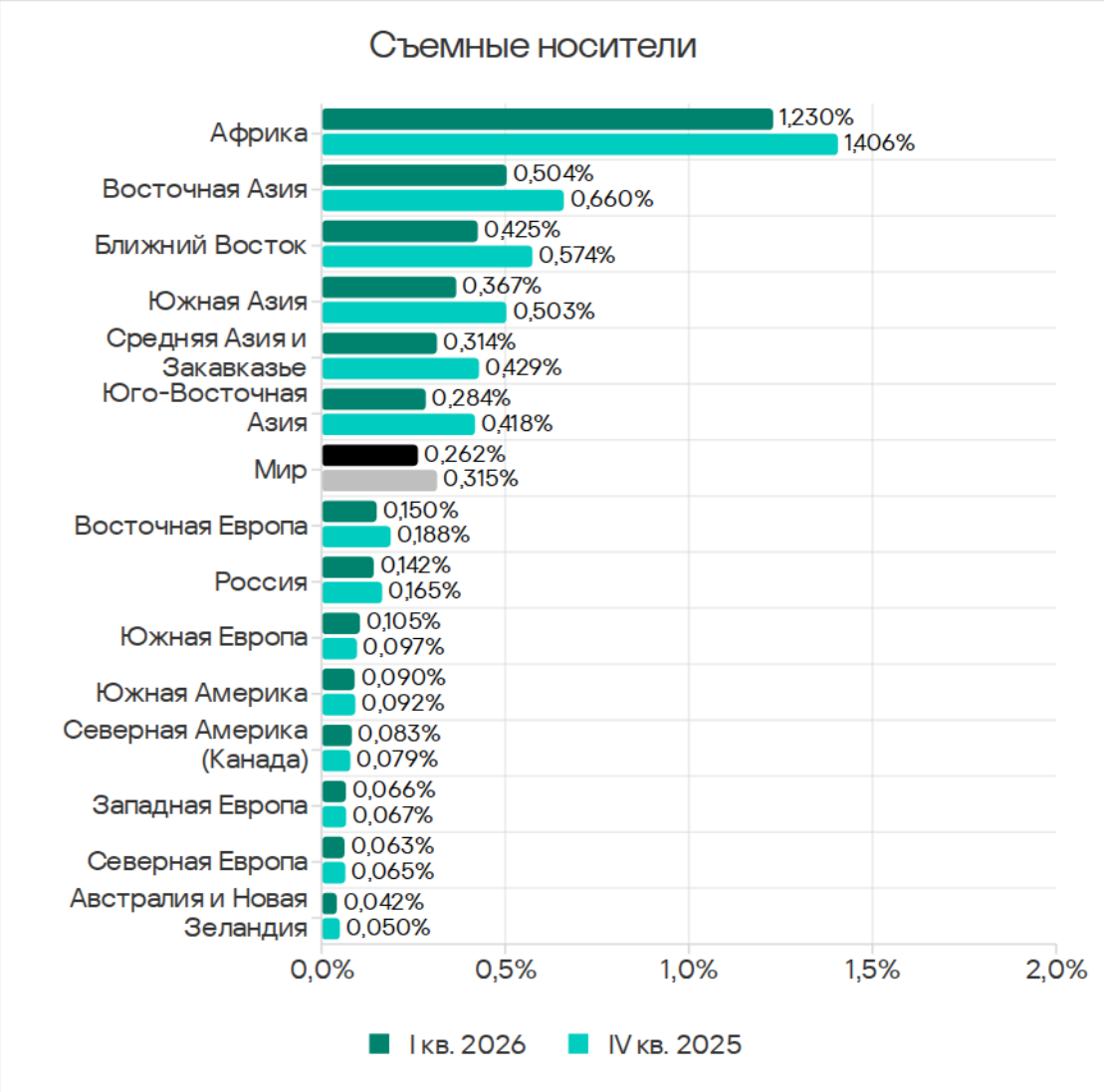
Угрозы на съемных носителях и основные категории угроз на съемных носителях, II квартал 2024 года — I квартал 2026 года

Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры. Эти современные криптомайнеры способны распространяться по локальным сетям, используя кражу учетных данных с зараженных хостов, эксплуатируя уязвимости (известные, но еще не

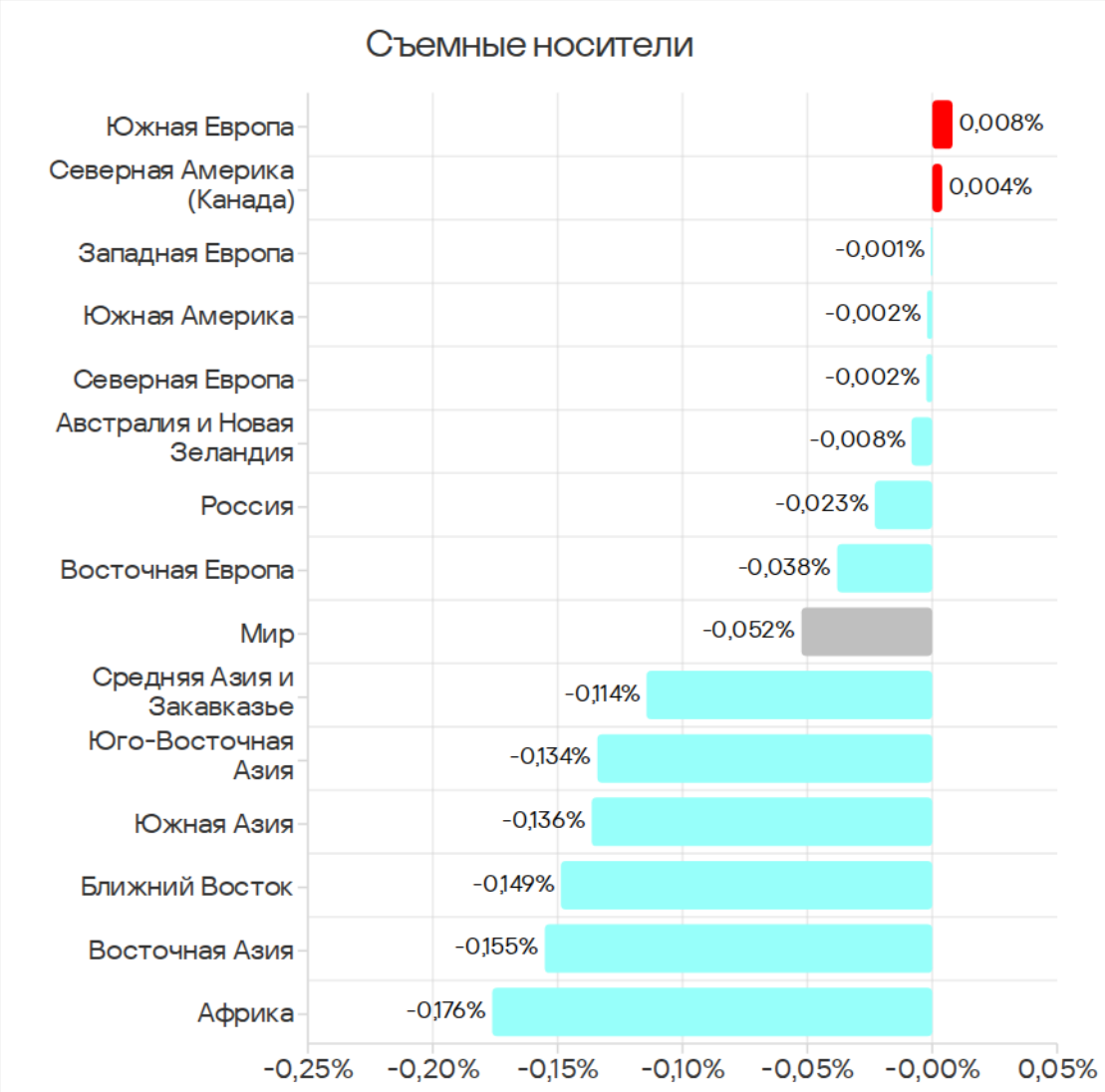
закрытые) и выполняя атаки на сетевые службы методом перебора (брутфорс).

Большинство шпионских программ, обнаруженных на съемных носителях, состояли из универсальных компонентов как современных, так и устаревших червей, таких как стилеры, загрузчики, AV-киллеры.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях



Изменение доли компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, I квартал 2026 года

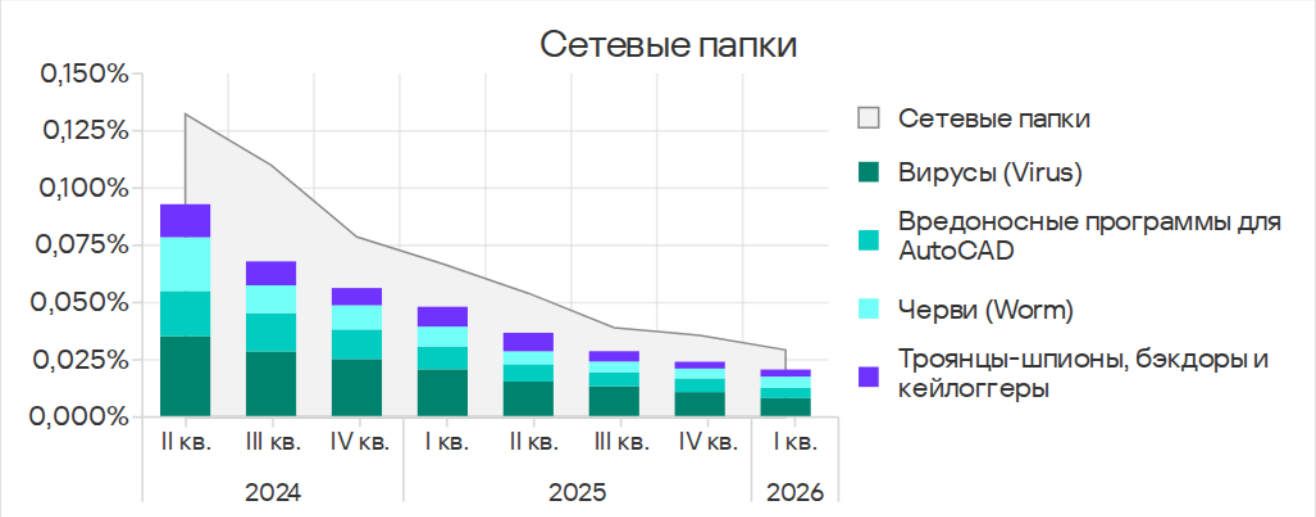


Сетевые папки

Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, I квартал 2023 года — I квартал 2026 года

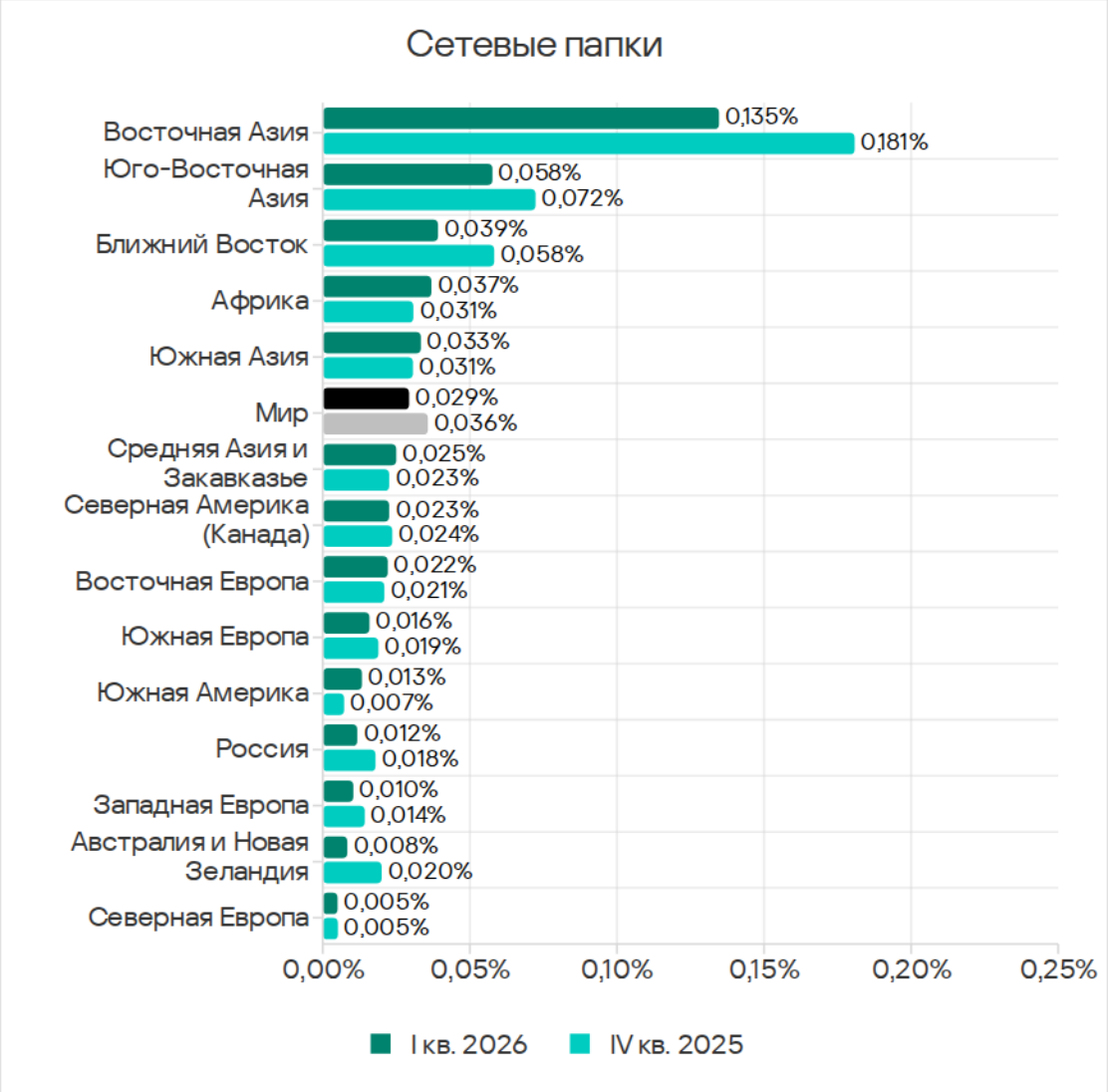
Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, апрель 2024 года — март 2026 года

Основными категориями угроз, которые распространялись через сетевые папки в первом квартале 2026 года, были вирусы, вредоносное ПО для AutoCAD, черви и шпионское ПО.

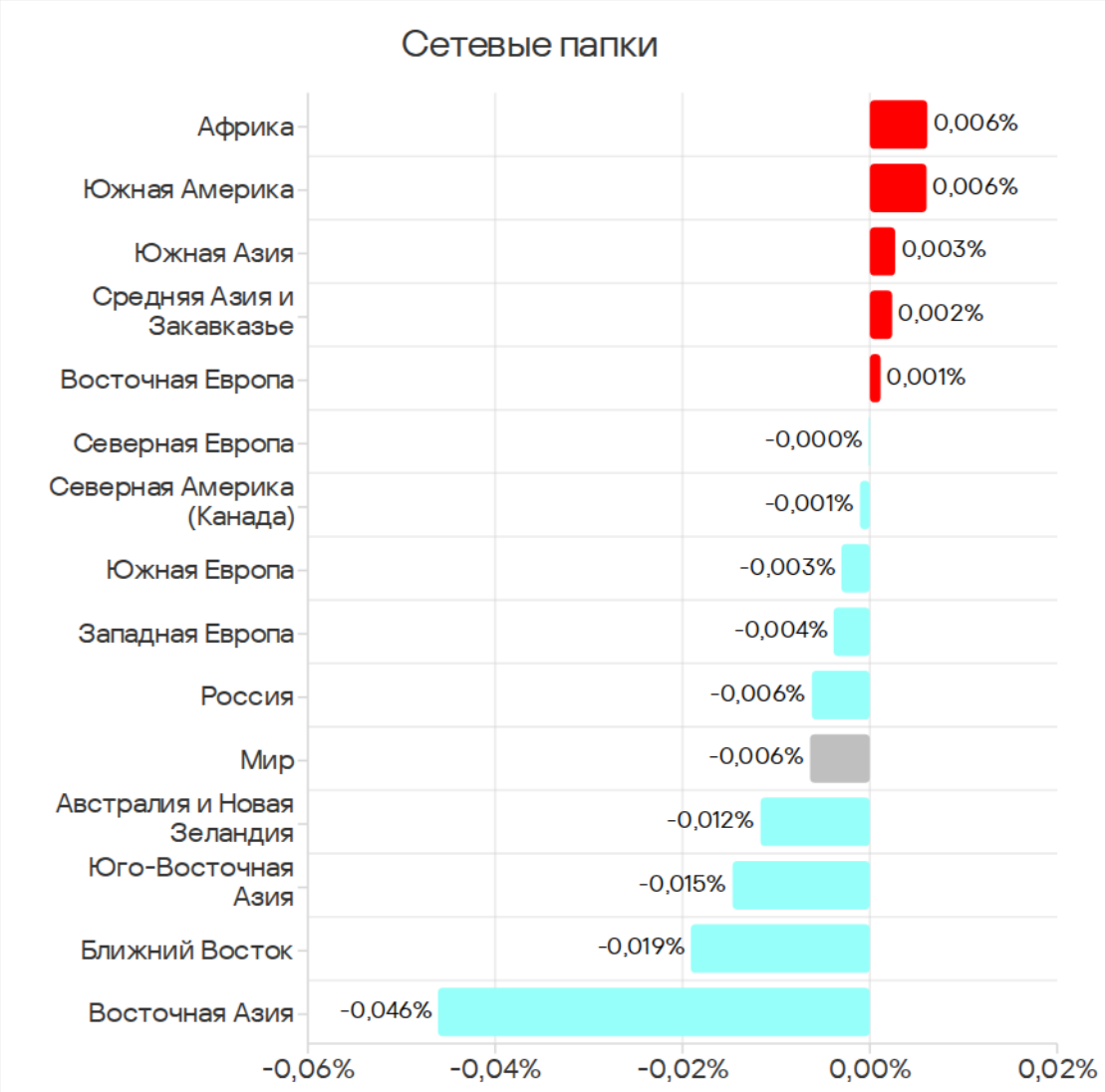


Угрозы в сетевых папках и основные категории угроз в сетевых папках, II квартал 2024 года — I квартал 2026 года

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках



Изменение доли компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, I квартал 2026 года



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