Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второй квартал 2026 года

25.08.2026

Версия 1.0

Итоги квартала

В этом разделе мы рассматриваем наиболее значимые изменения показателей за квартал, в том числе в регионах и в отраслях. Больше диаграмм представлено в соответствующих главах раздела «Основная статистика».

Цифры

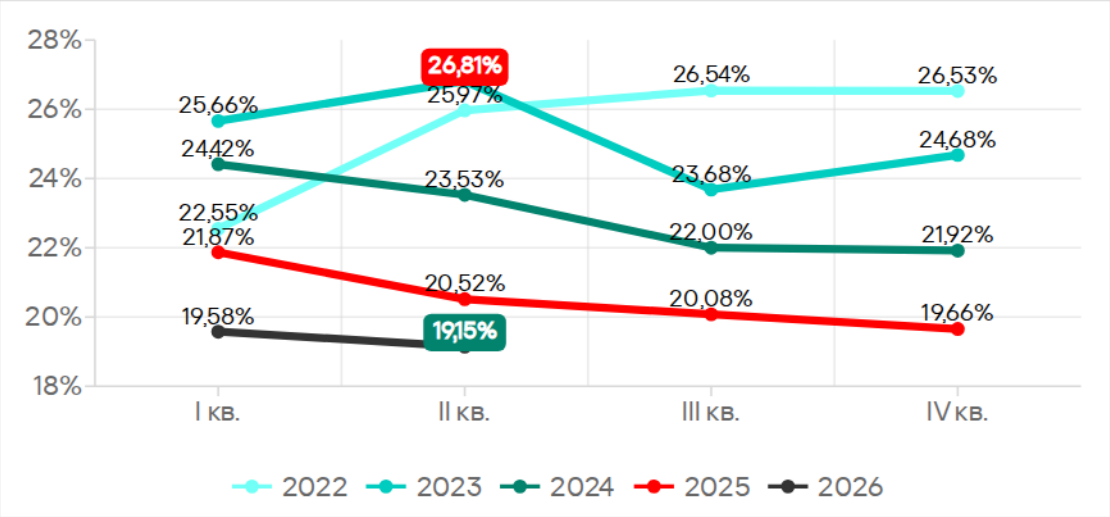
Показатель	I кв. 2026	II кв. 2026	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	19,6%	19,2%	▼0,4 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	6,56%	5,42%	▼1,14 п. п.
Ресурсы в интернете из списка запрещенных	3,54%	4,31%	▲0,77 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,73%	3,30%	▼0,43 п. п.
Вредоносные документы (MSOffice+PDF)	1,56%	1,77%	▲0,21 п. п.
Черви (Worm)	1,33%	1,43%	▲0,10 п. п.
Вирусы (Virus)	1,31%	1,29%	▼0,02 п. п.
Майнеры – исполняемые файлы для ОС Windows	0,59%	0,48%	▼0,11 п. п.
Вредоносные программы для AutoCAD	0,30%	0,31%	▲0,01 п. п.
Программы-вымогатели	0,14%	0,16%	▲0,02 п. п.
Веб-майнеры, выполняемые в браузерах	0,22%	0,14%	▼0,08 п. п.
Основные источники угроз			
Интернет	7,88%	7,61%	▼0,27 п. п.
Почтовые клиенты	2,59%	2,84%	▲0,25 п. п.

Съемные носители	0,26%	0,24%	▼0,02 п. п.
Сетевые папки	0,03%	0,02%	▼0,01 п. п.

Все угрозы

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, продолжила снижаться – во втором квартале 2026 года она составила 19,15%. Это наименьший показатель с 2022 года.

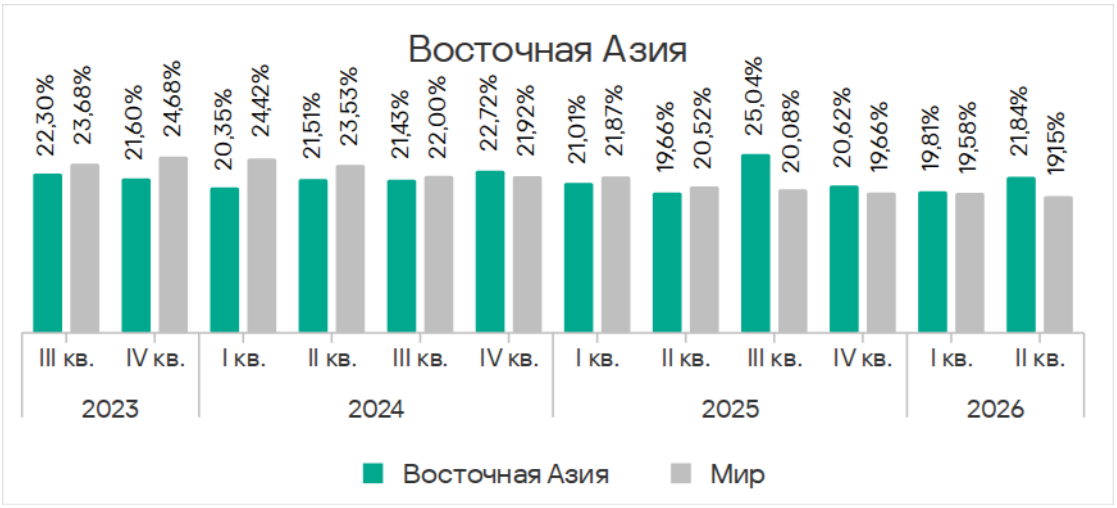
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2022 года – II квартал 2026 года



Показатели в регионах варьируют от 8,1% в Северной Европе до 27,9% в Африке. Разница максимального и минимального показателей в регионах довольно значительная: в Африке он в 3,4 раза больше, чем в Северной Европе.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал увеличилась в пяти регионах, больше всего – в Восточной Азии (на 2,03 п. п.) и в Африке (на 0,55 п. п.).

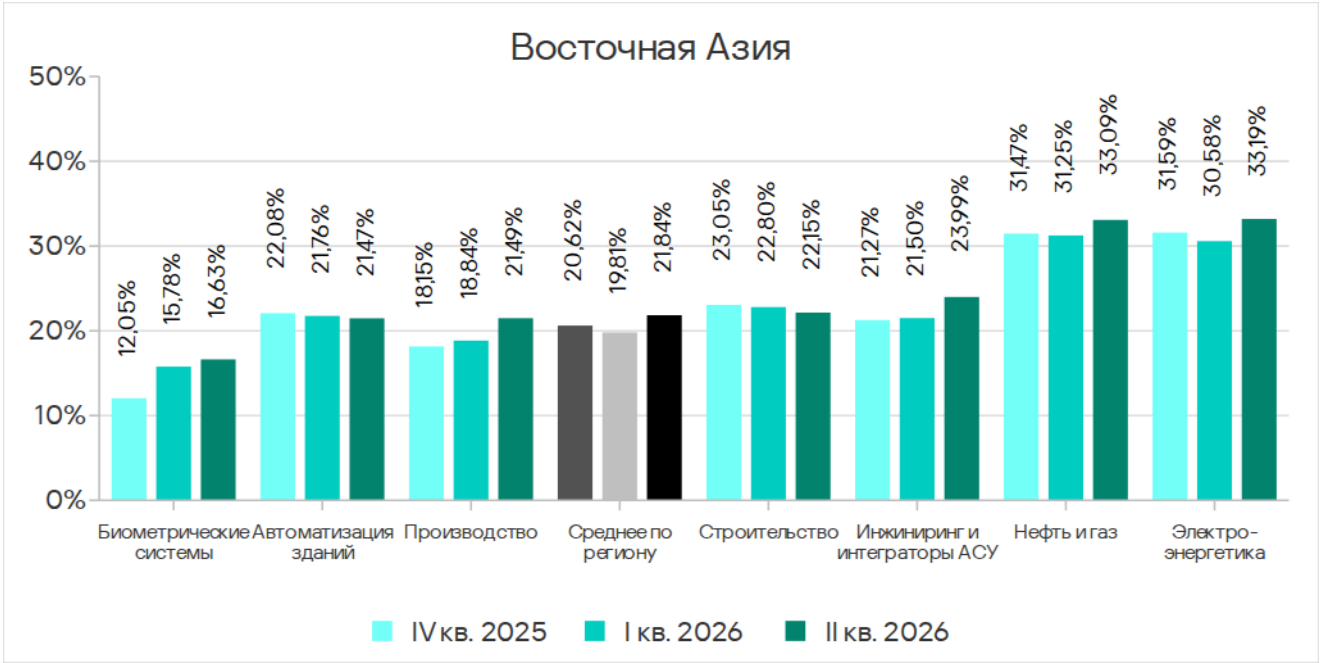
В **Восточной Азии** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором квартале 2026 года увеличилась до 21,84%, что превышает среднемировое значение.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Восточной Азии, III квартал 2023 года – II квартал 2026 года

Во втором квартале 2026 года в Восточной Азии увеличились показатели угроз всех категорий, кроме майнеров. Регион занял первое место по росту значений вредоносных скриптов и фишинговых страниц, шпионских программ и вирусов. Восточная Азия лидирует и по росту показателя угроз из интернета, в регионе также увеличилась доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов.

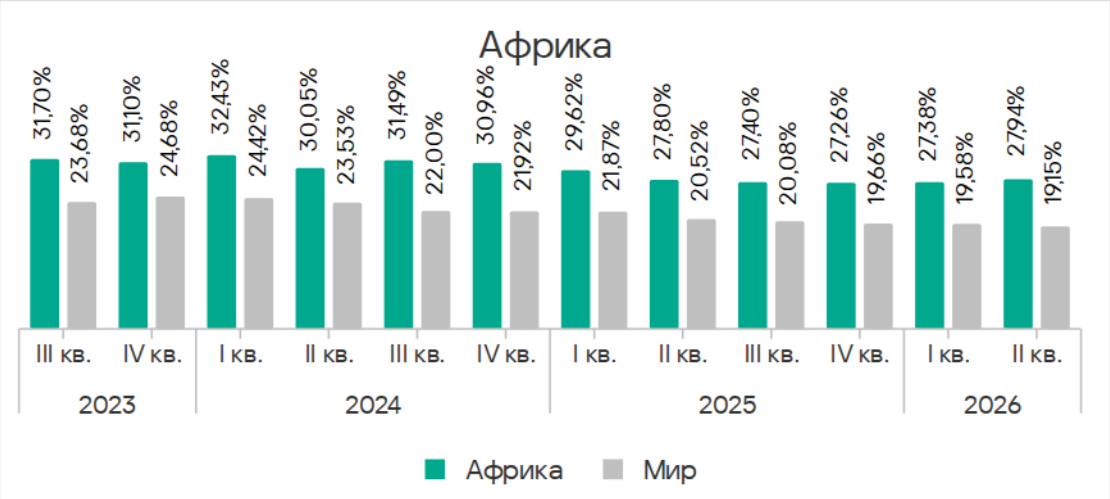
В регионе показатели выросли во всех исследуемых отраслях, кроме автоматизации зданий и строительства.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в различных отраслях в Восточной Азии

В Африке показатель колеблется, в отчетный период он оказался самым высоким со второго квартала 2025 года.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Африке, III квартал 2023 года – II квартал 2026 года



Среди угроз различных категорий в регионе больше всего вырос показатель ресурсов в интернете из списка запрещенных. Африка находится на первом месте среди регионов по росту значения программ-вымогателей и вредоносных программ для AutoCAD, на третьем месте – по увеличению показателей обеих категорий самораспространяющегося вредоносного ПО (червей и вирусов).

Африка на втором месте среди регионов по росту показателя угроз из почтовых клиентов.

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 26,44%.

Для этих систем характерны доступность интернета, активное использование электронной почты и, зачастую, минимальный контроль ИБ со стороны организации-потребителя.

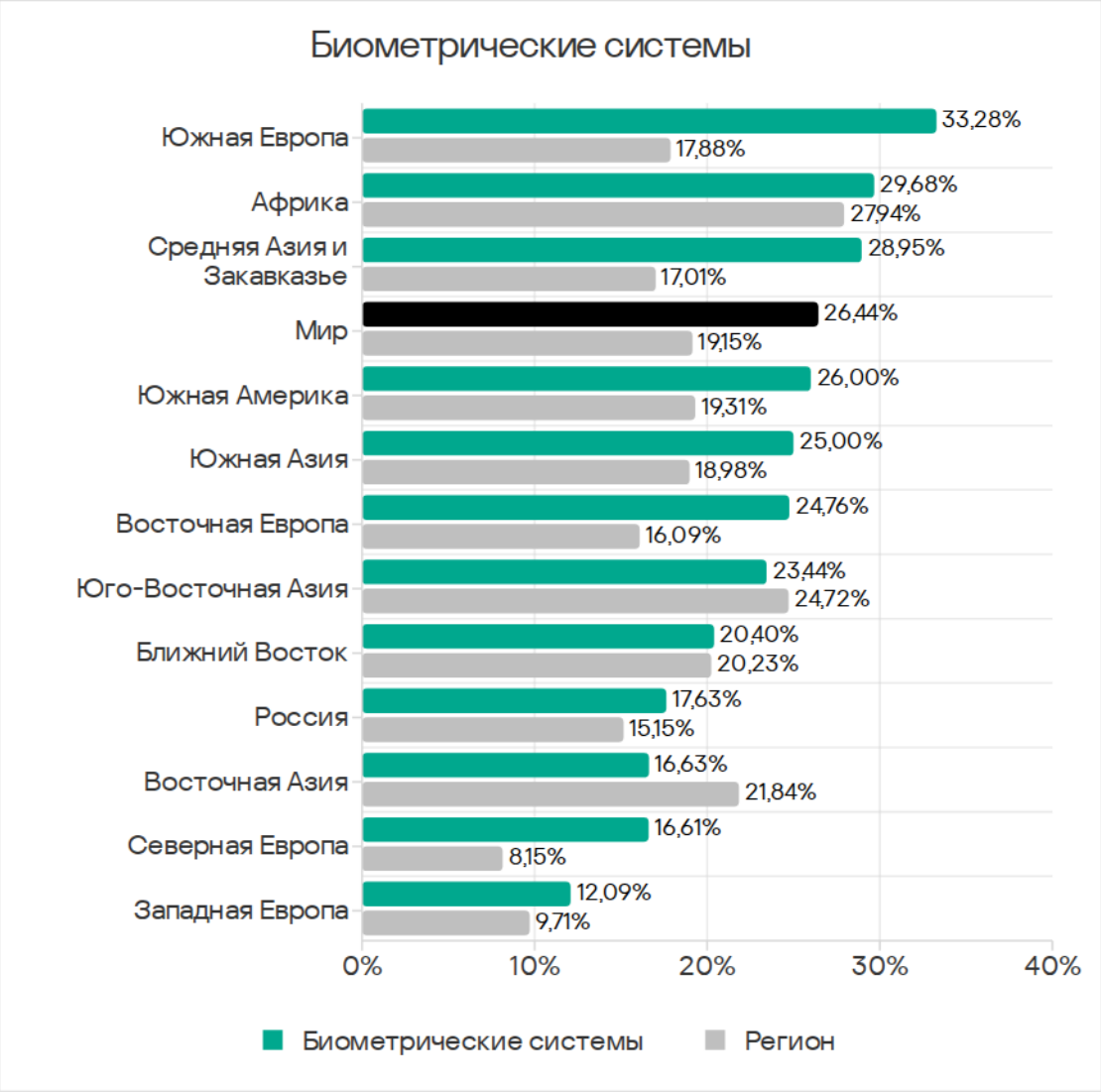
Биометрические системы лидируют в рейтингах исследуемых отраслей по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, программы-вымогатели, черви.

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

Во втором квартале 2026 года показатель биометрических систем немного вырос, значения у других исследуемых отраслей уменьшились.

Среди регионов по показателю биометрических систем лидирует Южная Европа с 33,28%. 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, II квартал 2026 года



Во всех исследуемых отраслях наблюдается тенденция к уменьшению среднемирового показателя.

Категории вредоносных объектов

Во втором квартале 2026 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 10 904 семейств, относящихся к различным категориям.

За квартал выросла доля компьютеров АСУ, на которых были заблокированы вредоносные объекты следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные документы, черви, программы-вымогатели и вредоносные программы для AutoCAD.

Вредоносные объекты, используемые для первичного заражения

Ресурсы в интернете из списка запрещенных

Ресурсы в интернете из списка запрещенных во втором квартале 2026 года в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, поднялись с третьего на второе место, потеснив шпионские программы.

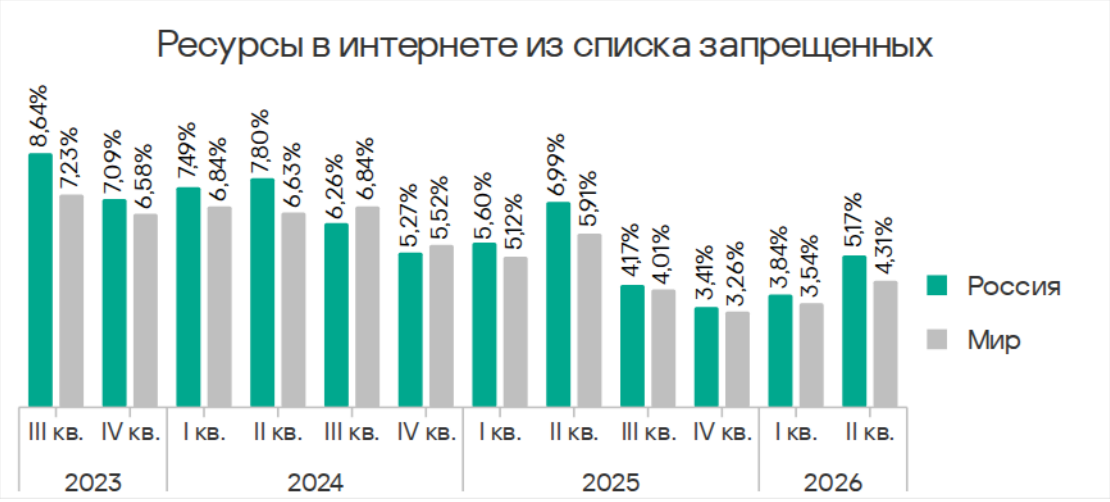
В мире доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, росла два квартала подряд и достигла 4,31%.

В регионах доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, варьирует от 2,32% в Северной Европе до 5,17% в России.

Показатель за квартал увеличился во всех регионах, наиболее заметно в России – на 1,33 п. п.

Россия во втором квартале 2026 года оказалась на первом месте среди регионов по показателю ресурсов в интернете из списка запрещенных. С 2022 года регион занимал первые места в этом рейтинге еще дважды, и оба раза во втором квартале – 2022 и 2024 годов.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных в России, III квартал 2023 года – II квартал 2026 года



Среди отраслей в регионе самые высокие значения угроз этой категории – в электроэнергетике (6,61%) и в отрасли инжиниринг и интеграторы АСУ (5,62%). В этих же отраслях больше всего выросли показатели за квартал.

В среднем по миру среди исследуемых отраслей первое место по показателю категории ресурсы в интернете из списка запрещенных занимает электроэнергетика (4,72%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Биометрические системы в Центральной Азии и Закавказье – 6,73%;
2. Электроэнергетика в России – 6,61%;
3. Электроэнергетика в Юго-Восточной Азии – 6,45%;
4. Строительство в Юго-Восточной Азии – 6,42%;
5. Электроэнергетика в Центральной Азии и Закавказье – 6,37%.

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. Во втором квартале 2026 года среднемировой показатель уменьшился и составил 5,42%.

Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и через почтовые клиенты.

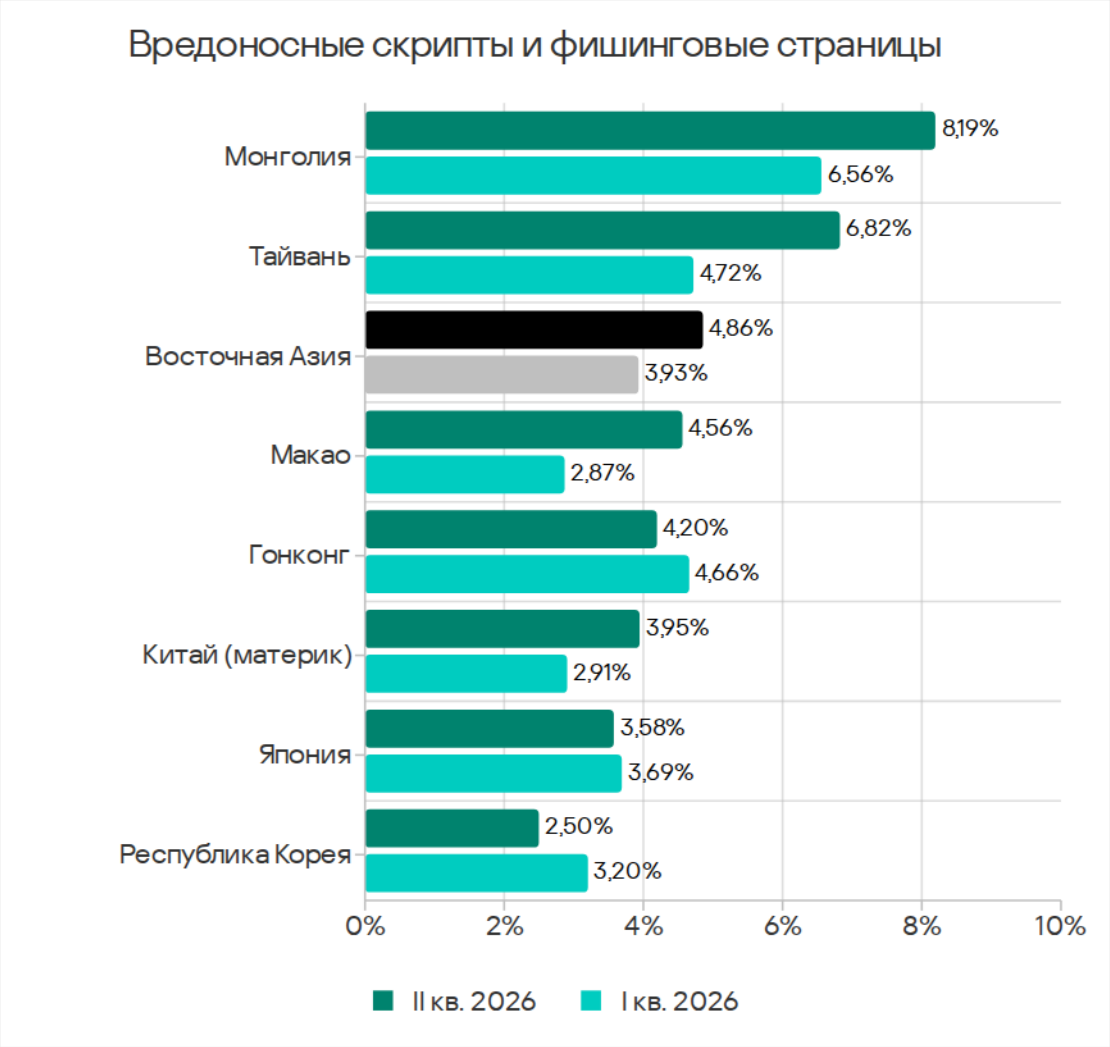
В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, варьирует от 1,67% в Северной Европе до 8,76% в Южной Европе.

За квартал показатель вырос только в **Восточной Азии** — на 0,93 п. п. – и достиг 4,86%. В регионе это второе по величине значение за последние три года.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы в Восточной Азии, III квартал 2023 года – II квартал 2026 года

Среди стран региона самый высокий показатель вредоносных скриптов и фишинговых страниц — в Монголии (8,19%).

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы в странах Восточной Азии



В регионе показатель вредоносных скриптов и фишинговых страниц увеличился во всех исследуемых отраслях, кроме строительства. Самые высокие значения отмечены у биометрических систем (9,01%) и автоматизации зданий (6,49%).

В среднем по миру среди исследуемых отраслей первое место по показателю категории вредоносные скрипты и фишинговые страницы занимают биометрические системы (13,20%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Биометрические системы в Южной Европе – 20,72%;
2. Автоматизация зданий в Южной Европе – 14,91%;
3. Биометрические системы в Южной Америке – 13,45%;
4. Автоматизация зданий в Африке – 11,78%;
5. Биометрические системы в Африке – 11,60%.

Отметим, что в аналогичном рейтинге по показателям вредоносных документов первые три позиции занимают те же отрасли в тех же регионах.

Вредоносные документы (MSOffice+PDF)

Вредоносные документы находятся на четвертом месте в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. За предыдущие три квартала показатель уменьшился до минимального за три года значения, а во втором квартале 2026 года увеличился до 1,77%.

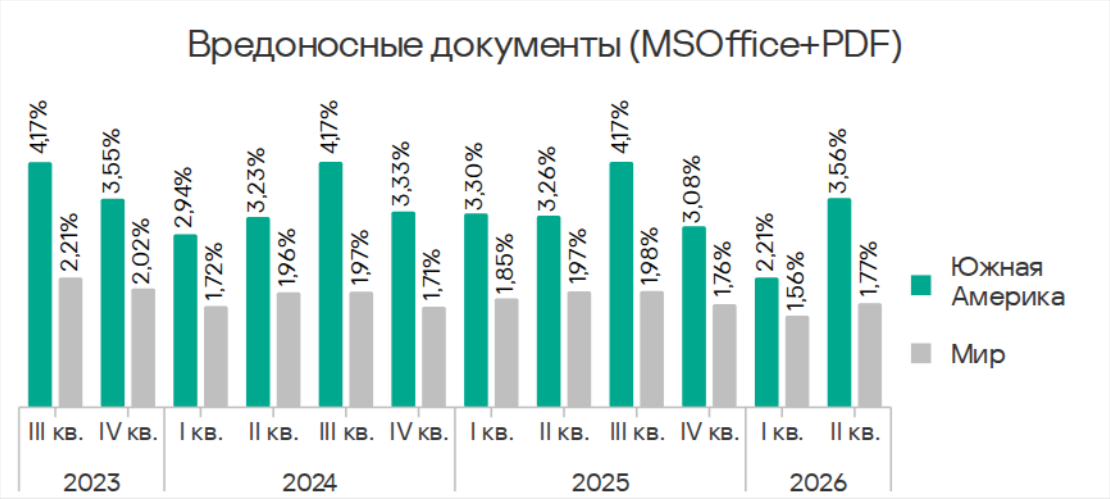
Распространяются вредоносные документы через все источники угроз, преимущественно через почтовые клиенты.

В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные документы, варьирует от 0,37% в Северной Европе до 3,63% в Южной Европе.

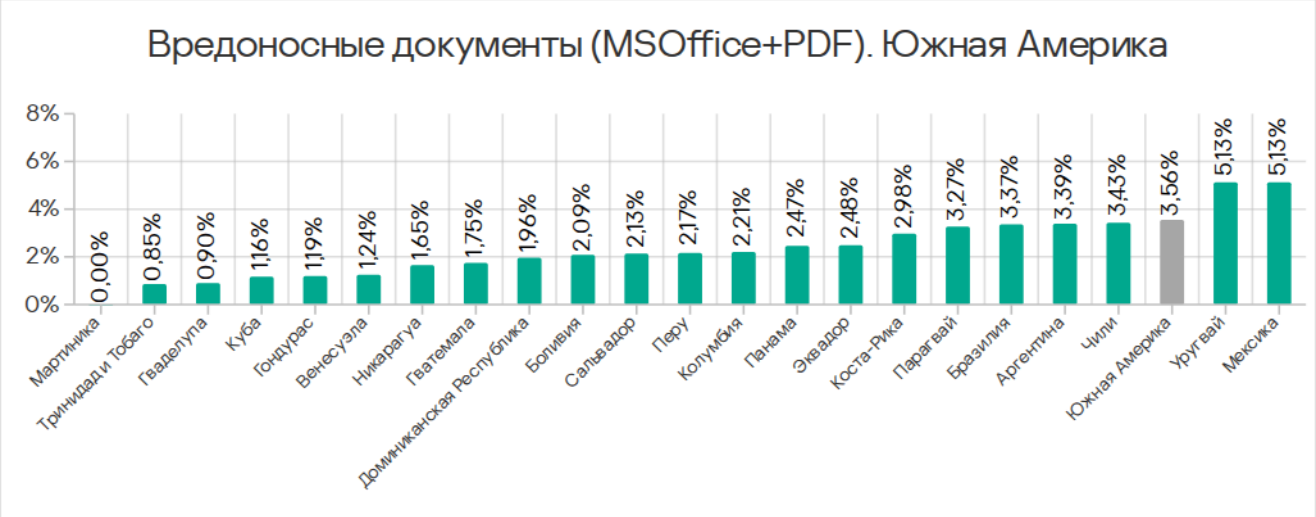
Показатель за квартал увеличился в семи регионах, больше всего – в Южной Америке (на 1,35 п. п.) и в Южной Европе (на 0,48 п. п.). Эти два региона входят в топ-3 по показателям вредоносных документов, вредоносных скриптов и фишинговых страниц, а также угроз из почты.

Южная Америка находится на втором месте в рейтинге регионов по показателю вредоносных документов. Во втором квартале 2026 года значение в регионе – 3,56% – четвертое по величине за три года.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в Южной Америке, III квартал 2023 года – II квартал 2026 года



Среди стран региона по показателю вредоносных документов с отрывом от остальных лидируют Мексика и Уругвай (5,13% каждая).

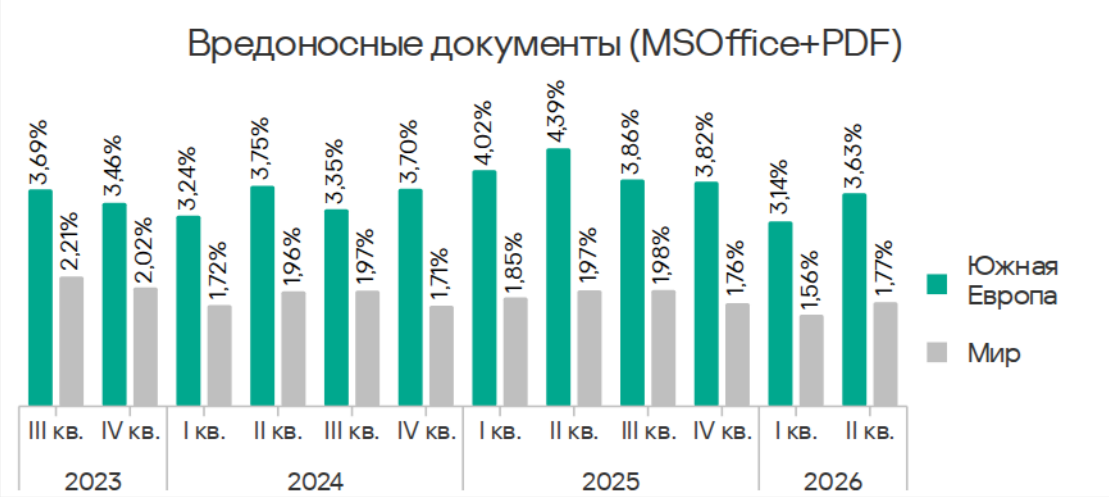


Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в странах Южной Америки

Среди исследуемых отраслей в Южной Америке самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные документы, – у биометричечких систем (6,67%).

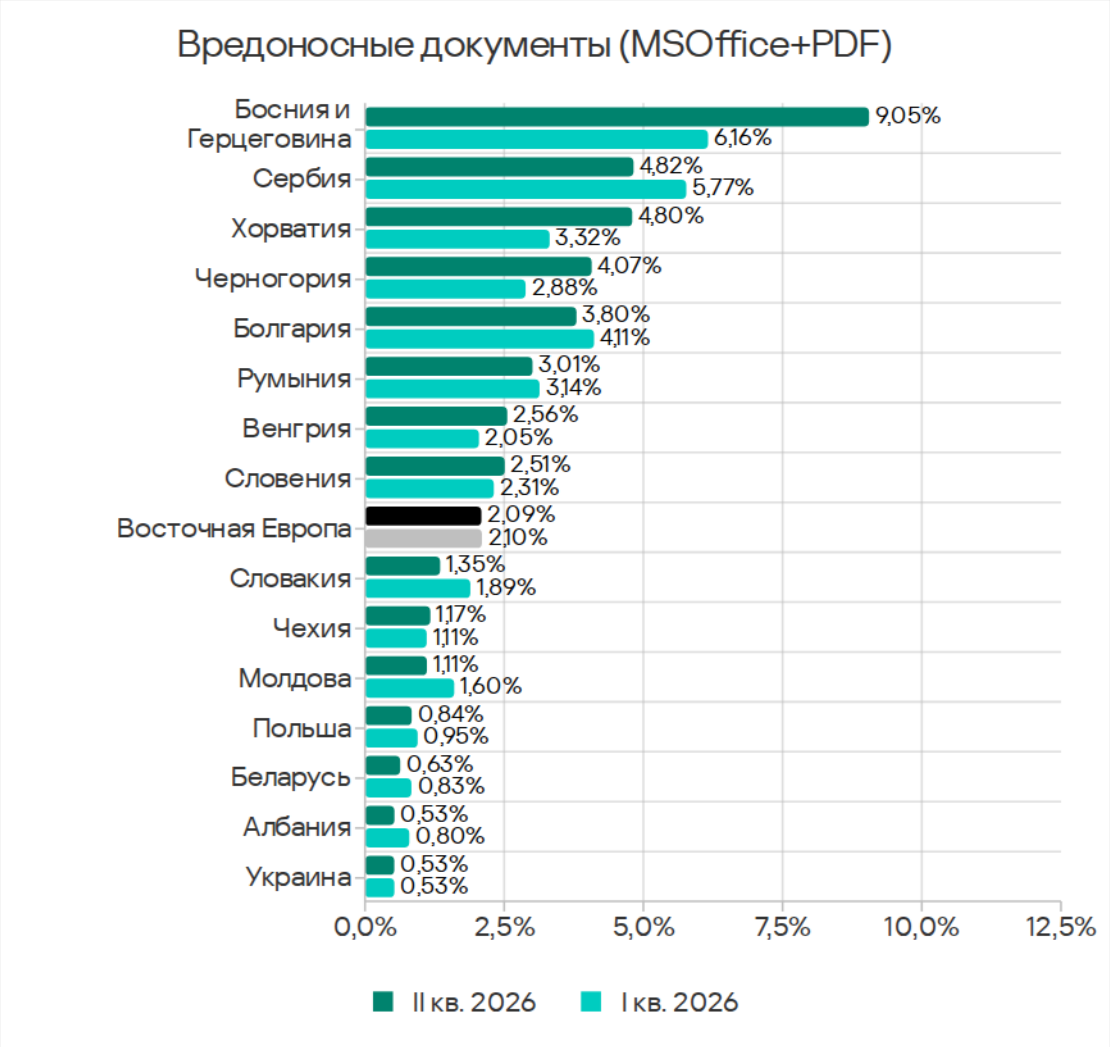
Южная Европа занимает первое место в рейтинге регионов по показателю вредоносных документов. В предыдущем квартале значение в регионе было наименьшим за три года, во втором квартале показатель вырос до 3,63%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в Южной Европе, III квартал 2023 года – II квартал 2026 года



Среди стран региона показатель вредоносных документов во втором квартале 2026 года заметно вырос в Боснии и Герцеговине, которая занимает первое место в соответствующем рейтинге.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы в странах Южной Европы



Среди исследуемых отраслей в Южной Европе самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные документы, – у биометричечких систем (11,48%).

В среднем по миру среди исследуемых отраслей первое место по показателю вредоносных документов занимают биометрические системы (6,03%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Биометрические системы в Южной Европе – 11,48%;
2. Автоматизация зданий в Южной Европе – 7,21%;
3. Биометрические системы в Южной Америке – 6,67%;
4. Автоматизация зданий в Восточной Европе – 5,14%;
5. Автоматизация зданий в Южной Америке – 4,94%.

Отметим, что в аналогичном рейтинге по показателям вредоносных скриптов и фишинговых страниц первые три позиции занимают те же отрасли в тех же регионах.

В топ-5 попали по две отрасли из Южной Европы и Южной Америки. Напомним, что эти регионы входят в тройку регионов с самыми высокими показателями угроз из почтовых клиентов, а электронная почта – основной источник вредоносных документов.

Вредоносное ПО следующего этапа

Программы-шпионы

В рейтинге категорий угроз по доле компьютеров АСУ, на которых было заблокировано шпионское ПО, шпионские программы находятся на третьем месте с показателем 3,30%. Это наименьшее значение с 2022 года.

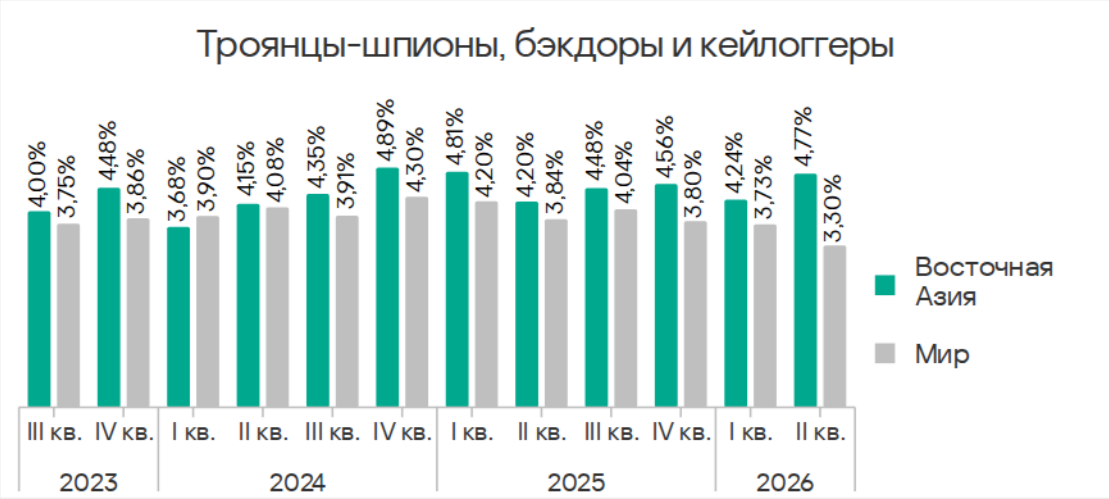
Шпионские программы распространяются через все источники угроз, преимущественно через электронную почту.

В регионах доля компьютеров АСУ, на которых было заблокировано шпионское ПО, варьирует от 0,98% в Северной Европе до 5,77% в Африке.

За квартал показатель вырос в трех регионах, больше всего – в Восточной Азии (на 0,53 п. п.) и Юго-Восточной Азии (на 0,42 п. п.).

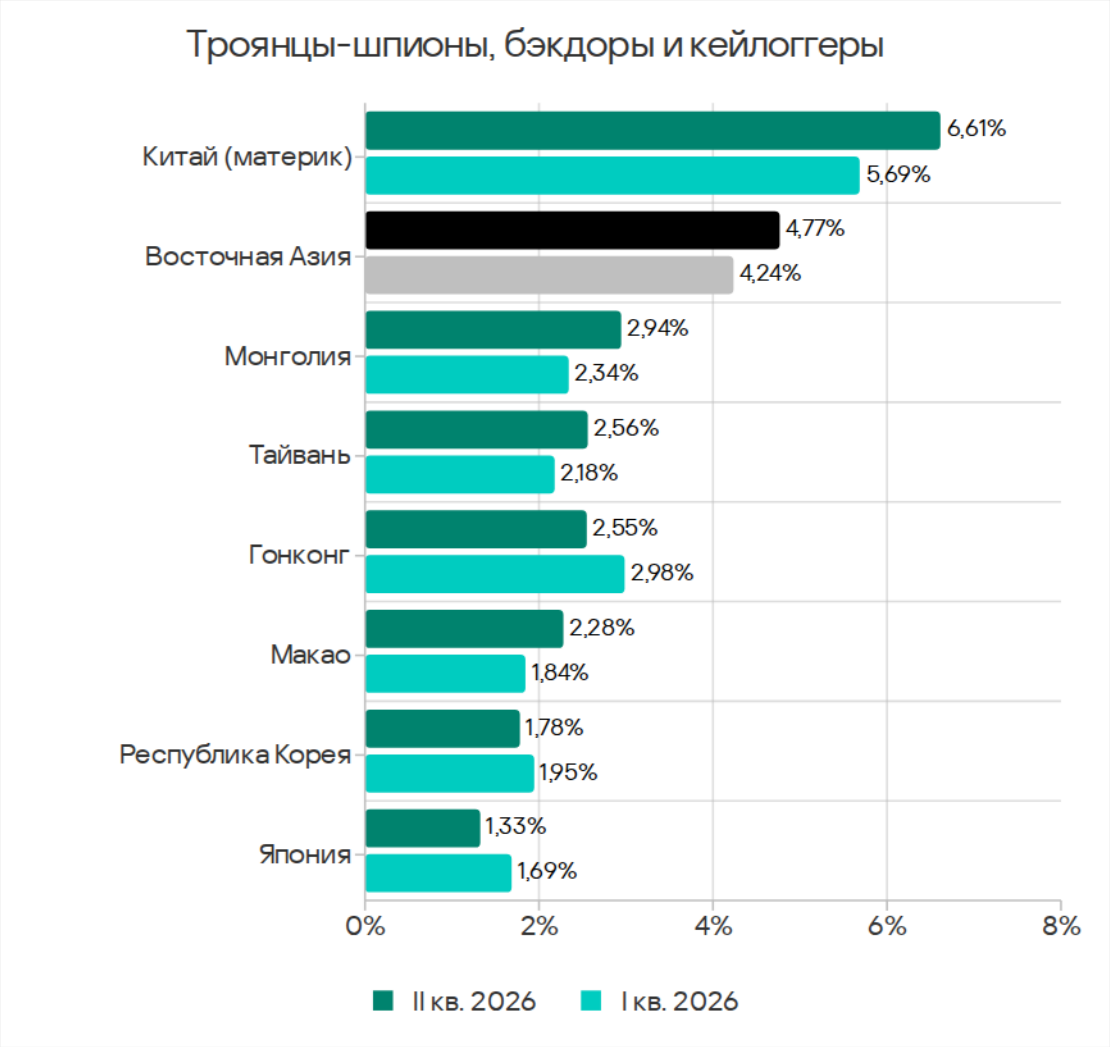
Восточная Азия в рейтинге по показателю шпионских программ (4,77%) занимает третье место после Африки и Юго-Восточной Азии. В регионе это самый высокий показатель со второго квартала 2025 года.

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в Восточной Азии, III квартал 2023 года – II квартал 2026 года



Среди стран региона самый высокий показатель шпионских программ – в материковом Китае (6,61%).

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в странах и территориях Восточной Азии

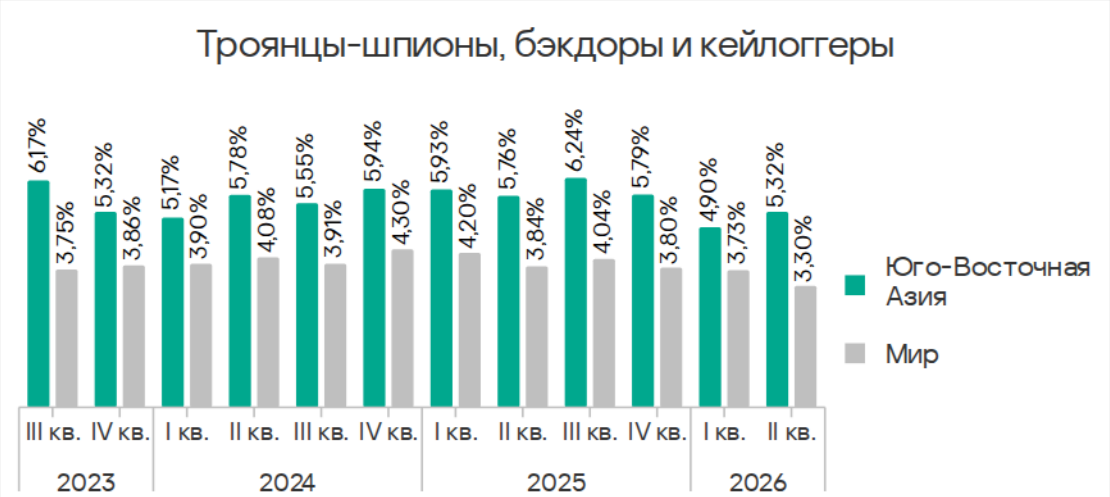


Среди исследуемых отраслей в Восточной Азии самая высокая доля компьютеров АСУ, на которых были заблокированы шпионские программы, – в электроэнергетике (11,75%) и производстве (5,87%). Во всех исследуемых отраслях показатель выше, чем в среднем по региону.

Напомним, что Восточная Азия – единственный регион, где вырос показатель угрозы категории вредоносные скрипты и фишинговые страницы. Распространение злоумышленниками вредоносных скриптов и фишинговых страниц зачастую предшествует целевым атакам и заражению компьютеров шпионскими программами.

Юго-Восточная Азия в рейтинге регионов по показателю шпионских программ занимает второе после Африки место с показателем 5,32%.

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в Юго-Восточной Азии, III квартал 2023 года – II квартал 2026 года



Среди стран региона по доле компьютеров АСУ, на которых были блокированы шпионские программы, лидируют Индонезия (6,96%) и Мьянма (6,92%).

Доля компьютеров АСУ, на которых были заблокированы шпионские программы в странах Юго-Восточной Азии

Среди исследуемых отраслей в регионе самый высокий показатель шпионских программ – у биометрических систем (8,93%) и в производственном секторе (7,32%). Значения за квартал выросли во всех отраслях.

В среднем по миру среди исследуемых отраслей первое место по показателю шпионских программ занимают биометрические системы с 7,29%.

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Электроэнергетика в Восточной Азии – 11,75%;
2. Биометрические системы в Южной Европе – 11,36%;
3. Биометрические системы в Юго-Восточной Азии – 8,93%;
4. Биометрические системы в Африке – 7,71%;
5. Автоматизация зданий в Южной Европе – 7,38%.

Отметим, что две позиции в первой пятерке занимают отрасли из Южной Европы, которая лидирует среди регионов по показателям вредоносных документов, вредоносных скриптов и фишинговых страниц, а также по угрозам из почтовых клиентов. Напомним, что вредоносные скрипты рассылаются в том числе в почтовых вложениях и используются для загрузки на компьютеры шпионских программ.

Программы-вымогатели

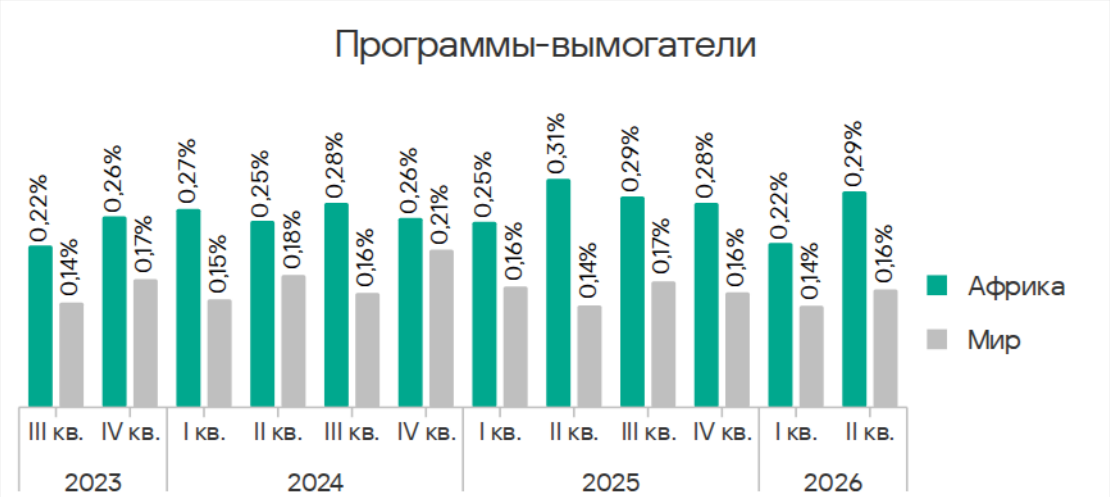
В мире доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, снижалась предыдущие три квартала, а во втором квартале 2026 года увеличилась до 0,16%.

В регионах доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, варьирует от 0,06% в Западной Европе до 0,29% в Африке.

Показатель за квартал вырос во всех регионах, кроме Западной и Южной Европы, а также Северной Америки (Канады). Рейтинг по росту показателя возглавляет Африка.

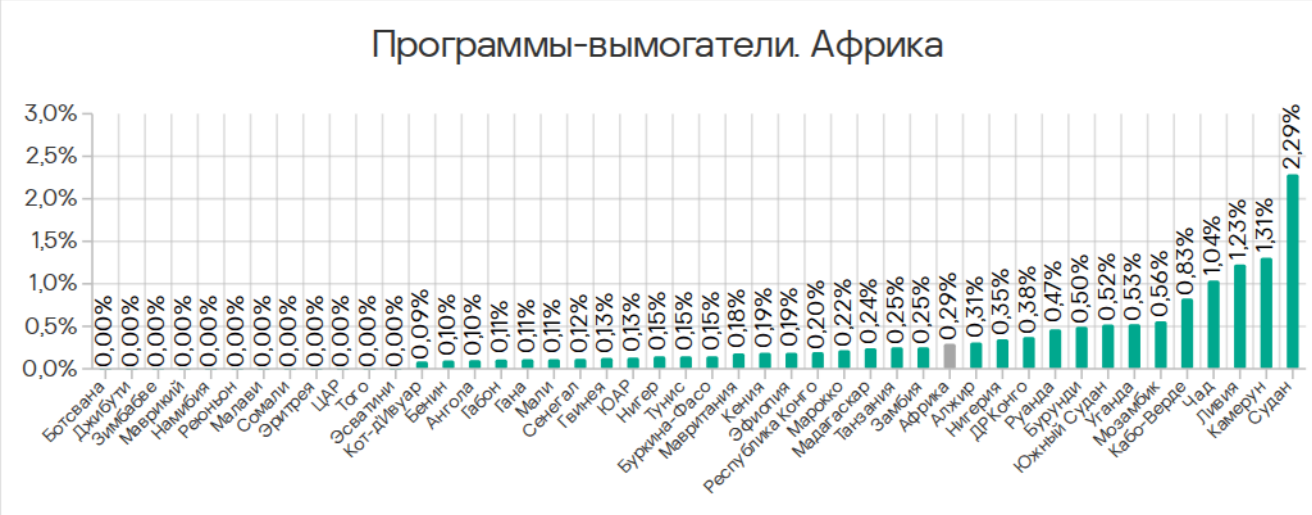
Африка во втором квартале 2026 года заняла первое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются программы-вымогатели, с 0,29%. За три последних года выше показатель был только во втором квартале 2025 года (0,31%).

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в Африке, III квартал 2023 года – II квартал 2026 года



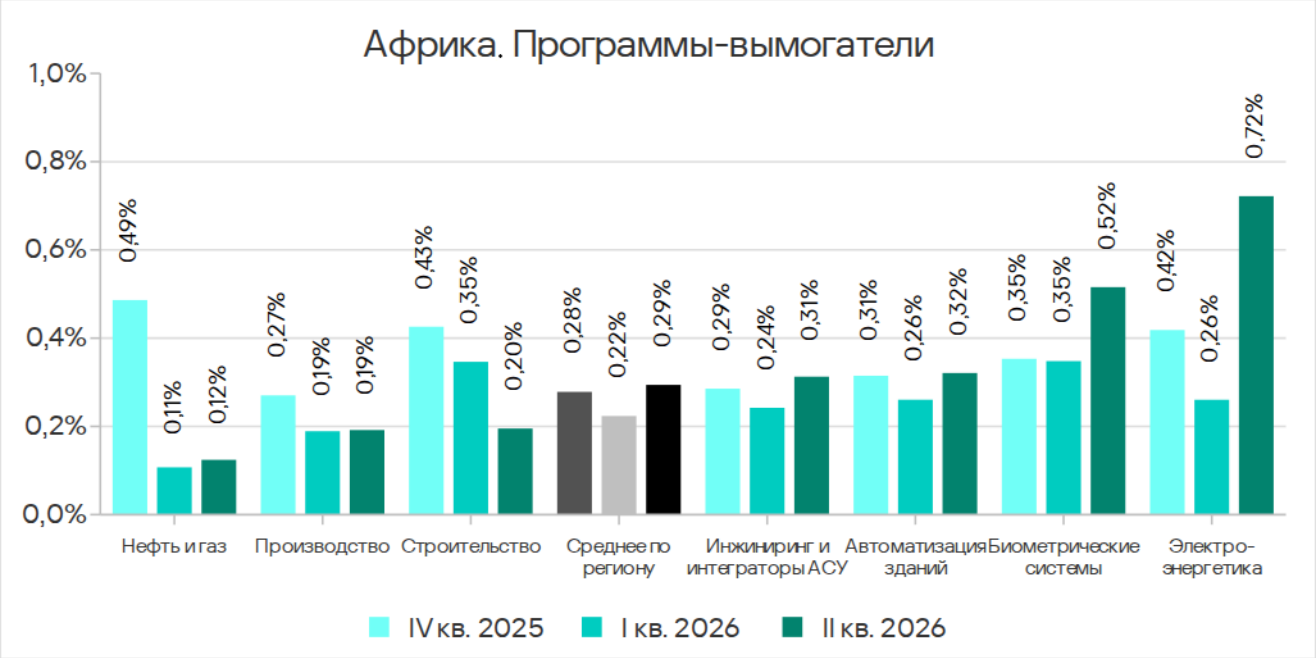
В регионе программы-вымогатели распространяются преимущественно через интернет, встречаются они и на съемных носителях.

Среди стран региона по доле компьютеров АСУ, на которых блокируются программы-вымогатели, с большим отрывом от остальных лидирует Судан (2,29%).



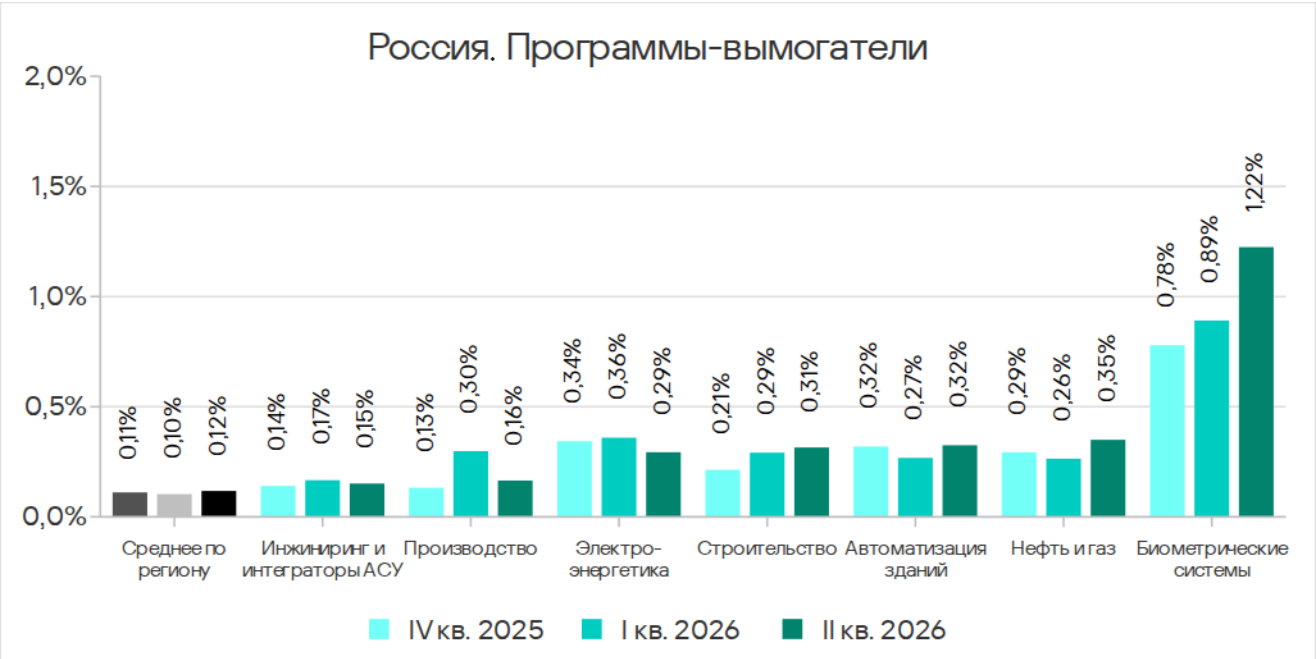
Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в странах Африки

Среди исследуемых отраслей в Африке самые высокие показатели программ-вымогателей – в электроэнергетической отрасли (0,72%) и у биометрических систем (0,52%). За квартал значения увеличились во всех отраслях, кроме производства и строительства, самое значительное изменение показателя отмечено в электроэнергетической отрасли.



Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в различных отраслях в Африке

В **России** доля компьютеров АСУ, на которых блокировались программы-вымогатели в биометрических системах, увеличивалась в течение трех кварталов подряд и достигла 1,22%. Это самый высокий показатель программ-вымогателей во всех отраслях во всех регионах.



Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели в различных отраслях в России

В среднем по миру среди исследуемых отраслей первое место в рейтинге по показателю программ-вымогателей занимают биометрические системы (0,31%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Биометрические системы в России – 1,22%;
2. Электроэнергетика в Африке – 0,72%;
3. Биометрические системы в Западной Европе – 0,59%;
4. Биометрические системы на Ближнем Востоке – 0,57%;
5. Электроэнергетика в Восточной Азии – 0,56%.

Майнеры

В мире во втором квартале 2026 года доля компьютеров АСУ, на которых были заблокированы майнеры, оказалась наименьшей с 2021 года для майнеров обеих категорий – и в формате исполняемых файлов для ОС Windows (0,48%), и веб-майнеров, выполняемых в браузерах (0,14%).

Значения обеих категорий уменьшились во всех регионах, за исключением показателя майнеров – исполняемых файлов для ОС Windows в Африке, где он незначительно увеличился.

Майнеры – исполняемые файлы для ОС Windows

В регионах показатель майнеров – исполняемых файлов для ОС Windows варьирует от 0,12% в Австралии и Новой Зеландии до 0,83% в Средней Азии и Закавказье. Россия (0,67%) по-прежнему занимает второе место.

Эта категория угроз распространяется через все источники угроз, чаще всего – через интернет.

В среднем по миру среди исследуемых отраслей первое место по показателю майнеров – исполняемых файлов для ОС Windows занимает нефтегазовая отрасль (0,66%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю попали четыре отрасли в Средней Азии и Закавказье: биометрические системы (2,05%), производство (1,66%), строительство (1,36%) и электроэнергетика (1,27%). На третьем месте в этом списке оказались биометрические системы в России (1,47%).

Веб-майнеры

Показатели веб-майнеров в регионах находятся в диапазоне от 0,04% (в Восточной Азии) до 0,25% (в Южной Америке).

В среднем по миру среди исследуемых отраслей первое место по показателю веб-майнеров занимает нефтегазовая отрасль (0,34%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Биометрические системы в России – 0,90%;
2. Производство в Средней Азии и Закавказье – 0,66%;
3. Электроэнергетика в Австралии и Новой Зеландии – 0,62%;
4. Производство в Северной Европе – 0,54%;
5. Строительство в Южной Америке – 0,45%.

Самораспространяющееся вредоносное ПО

Черви

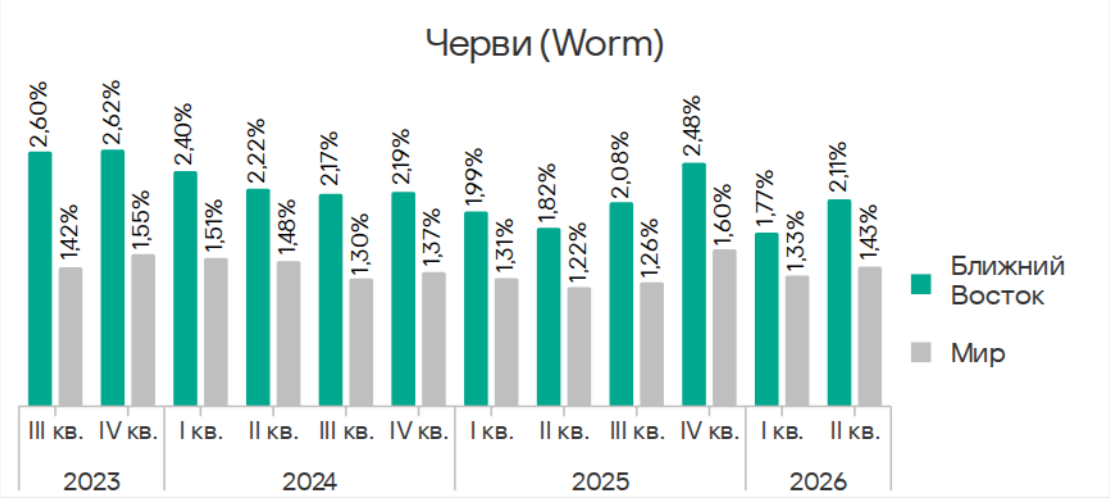
В мире доля компьютеров АСУ, на которых были заблокированы черви, во втором квартале 2026 года увеличилась до 1,43%.

Распространяется эта угроза через все источники, активно используется электронная почта.

Показатель в регионах варьирует от 0,27% в Северной Америке (Канаде) до 3,41% в Африке. За квартал значение больше всего выросло на Ближнем Востоке (на 0,34 п. п.) и в Австралии и Новой Зеландии (на 0,20 п. п.).

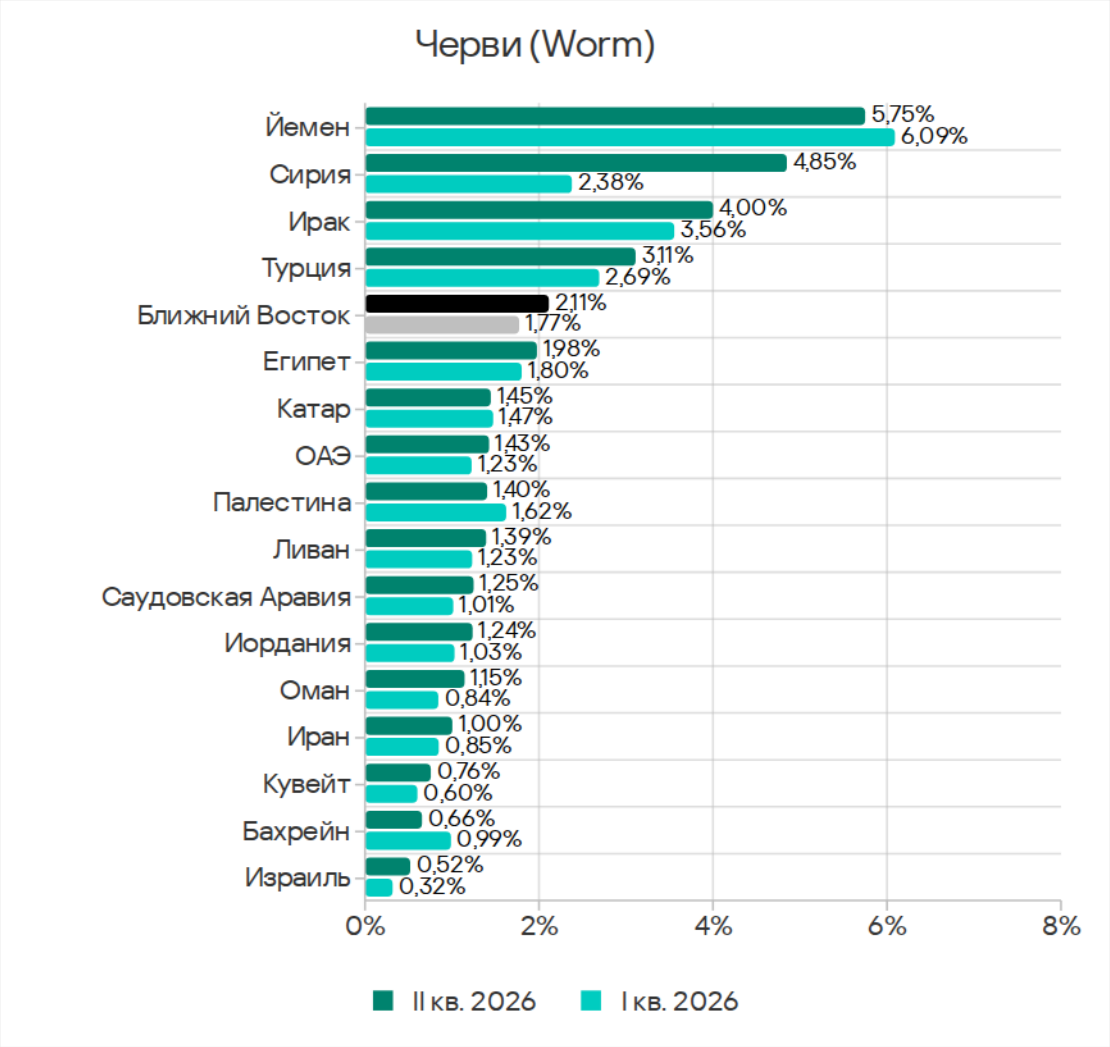
Во втором квартале 2026 года в рейтинге регионов по показателю червей **Ближний Восток** (2,11%) занял второе место (после Африки), сместив Центральную Азию и Закавказье.

Доля компьютеров АСУ, на которых были заблокированы черви на Ближнем Востоке, III квартал 2023 года – II квартал 2026 года

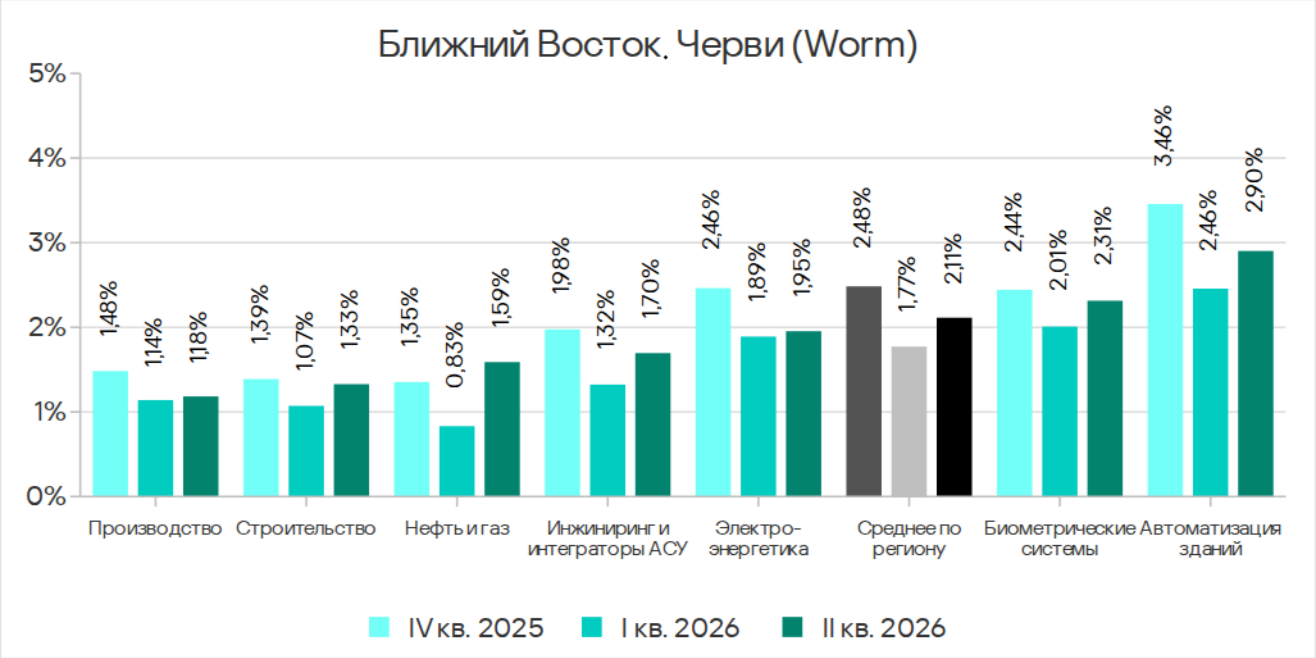


Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются черви, лидирует Йемен (5,75%).

Доля компьютеров АСУ, на которых были заблокированы черви в странах Ближнего Востока



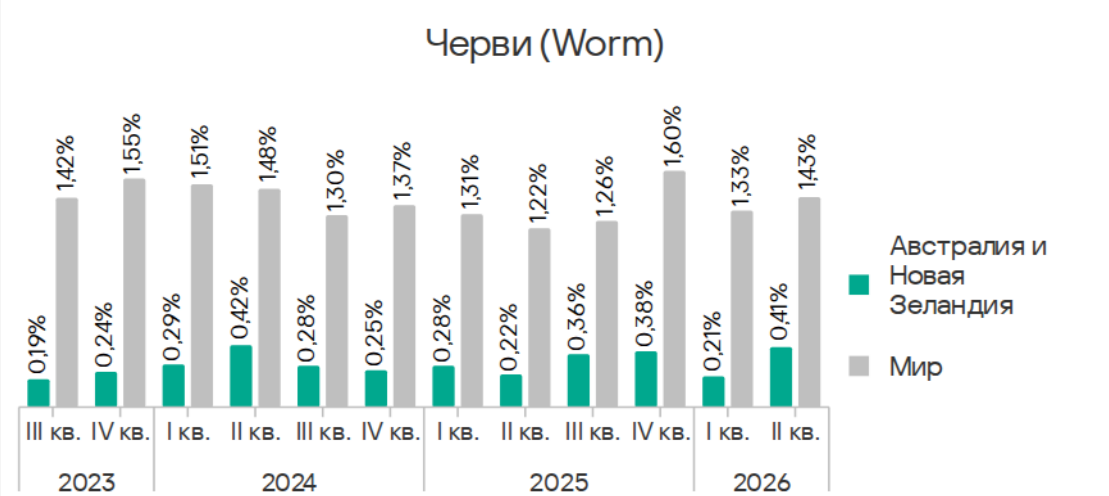
Среди исследуемых отраслей в регионе самые высокие показатели червей – у автоматизации зданий (2,90%). За квартал значения увеличились во всех отраслях.



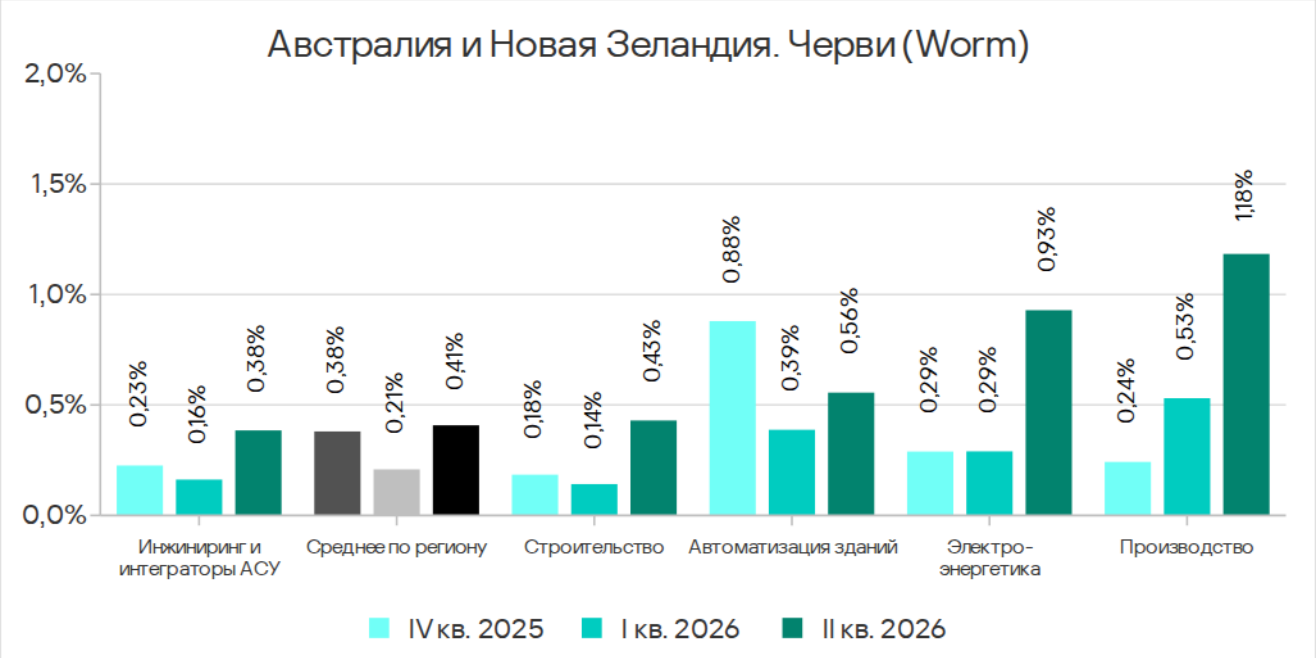
Доля компьютеров АСУ, на которых были заблокированы черви в различных отраслях на Ближнем Востоке

Австралия и Новая Зеландия занимает 12-е место в рейтинге регионов по показателю червей (0,41%). За три года показатель в регионе был выше только во втором квартале 2024 года (0,42%).

Доля компьютеров АСУ, на которых были заблокированы черви в Австралии и Новой Зеландии, III квартал 2023 года – II квартал 2026 года



В регионе показатель червей вырос во всех исследуемых отраслях, больше всего – в производстве и электроэнергетике. В результате их значения превысили среднее по региону в 2,9 и 2,3 раза соответственно.



Доля компьютеров АСУ, на которых были заблокированы черви в различных отраслях в Австралии и Новой Зеландии

В среднем по миру среди исследуемых отраслей первое место по показателю червей занимают биометрические системы (2,29%).

Среди исследуемых отраслей во всех регионах четыре отрасли в Африке входят в топ-5 по этому показателю:

1. Электроэнергетика в Африке – 4,09%;
2. Биометрические системы в Африке – 3,81%;
3. Биометрические системы в Центральной Азии и Закавказье – 3,51%;
4. Инжиниринг и интеграторы АСУ в Африке – 3,26%;
5. Строительство в Африке – 3,19%.

Напомним, что Африка – многолетний и неизменный лидер среди регионов по доле компьютеров АСУ, на которых блокируются черви, а также по показателю угроз на съемных носителях.

Вирусы

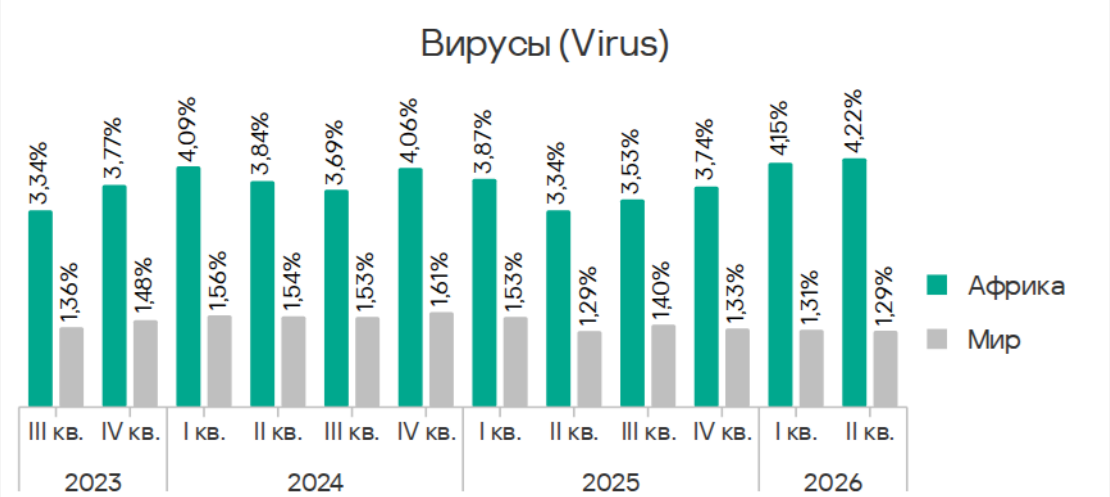
В мире доля компьютеров АСУ, на которых были заблокированы вирусы, во втором квартале 2026 года уменьшилась до 1,29%.

В регионах показатель варьирует от 0,12% в Западной Европе до 6,03% в Юго-Восточной Азии. Топ-3 регионов по этому показателю неизменен: Юго-Восточная Азия (с большим отрывом от остальных регионов), Африка и Восточная Азия. Эти же регионы входят в список лидеров и в случае вредоносных программ для AutoCAD.

Показатель увеличился в трех регионах: в Восточной Азии, Австралии и Новой Зеландии, а также в Африке.

Африка занимает второе место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вирусы. Показатель в регионе растет четвертый квартал подряд и достиг максимального с 2022 года значения – 4,22%.

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

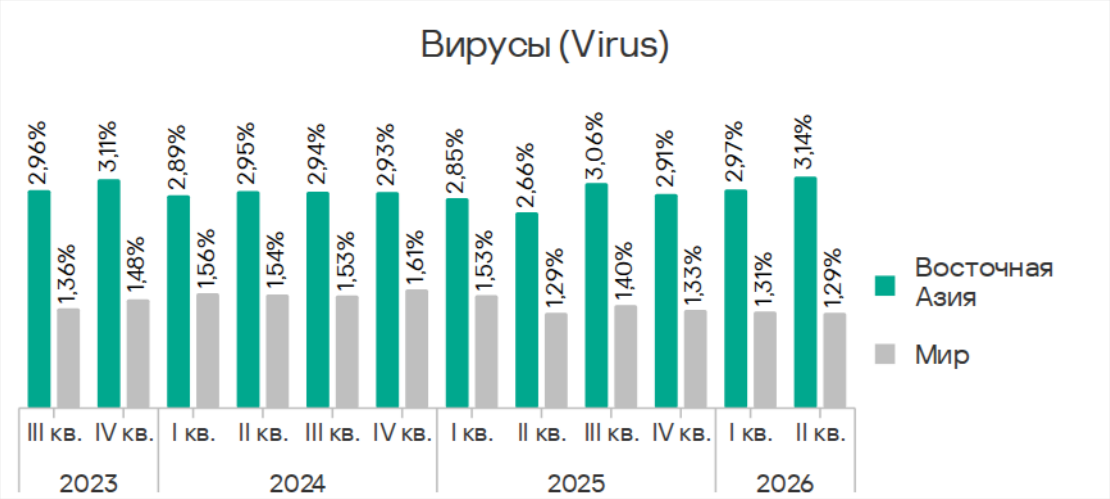


Среди стран региона по показателю вирусов лидируют Камерун (9,46%) и Алжир (7,12%).

Среди исследуемых отраслей в Африке самый высокий показатель вирусов – в строительной отрасли (5,47%).

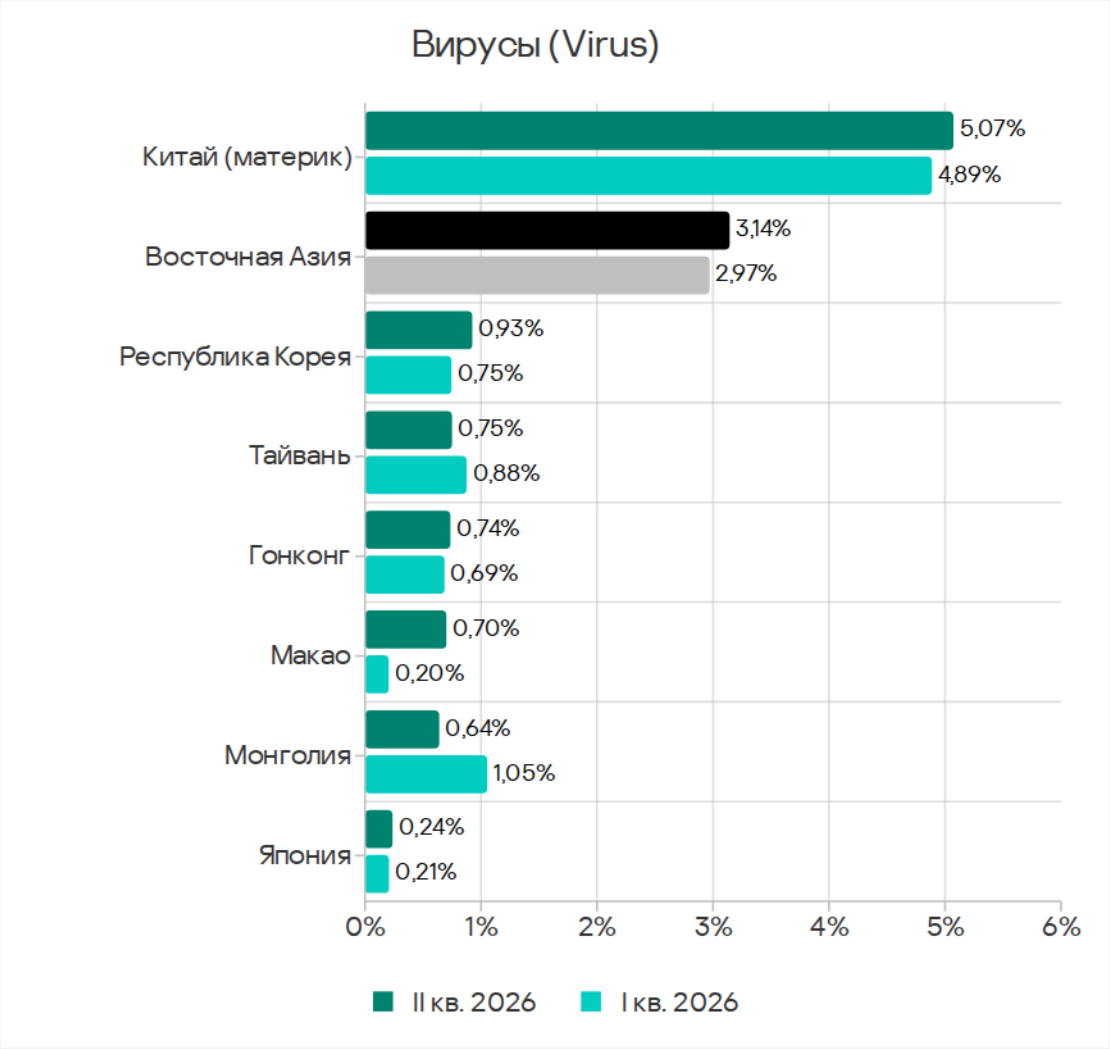
Восточная Азия находится на третьем месте среди регионов по показателю вирусов (3,14%). Это максимальное значение в регионе за последние три года.

Доля компьютеров АСУ, на которых были заблокированы вирусы в Восточной Азии, III квартал 2023 года – II квартал 2026 года



Среди стран и территорий региона очевидный лидер по показателю вирусов – материковый Китай (5,07%). Отметим, что он же занимает первое место по показателю вредоносных программ для AutoCAD.

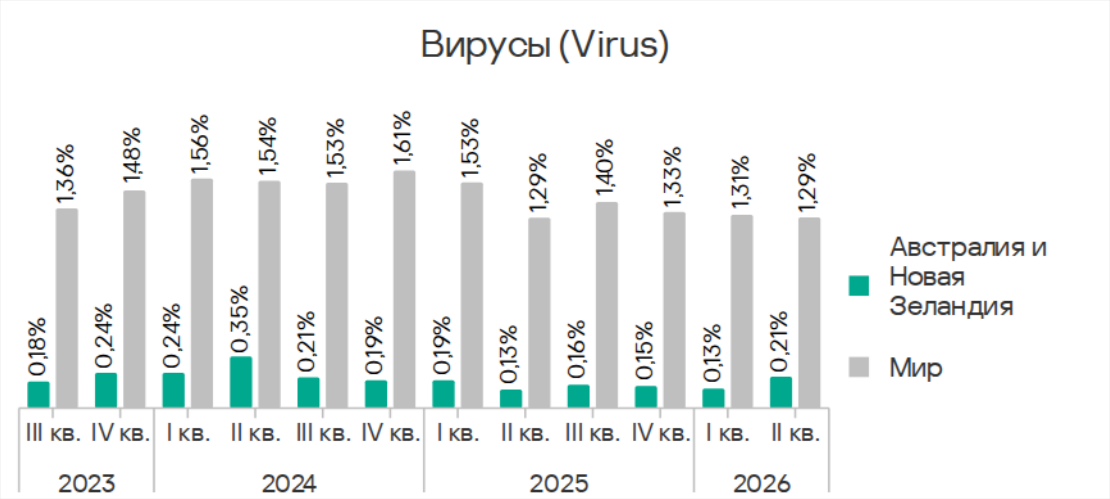
Доля компьютеров АСУ, на которых были заблокированы вирусы в странах Восточной Азии

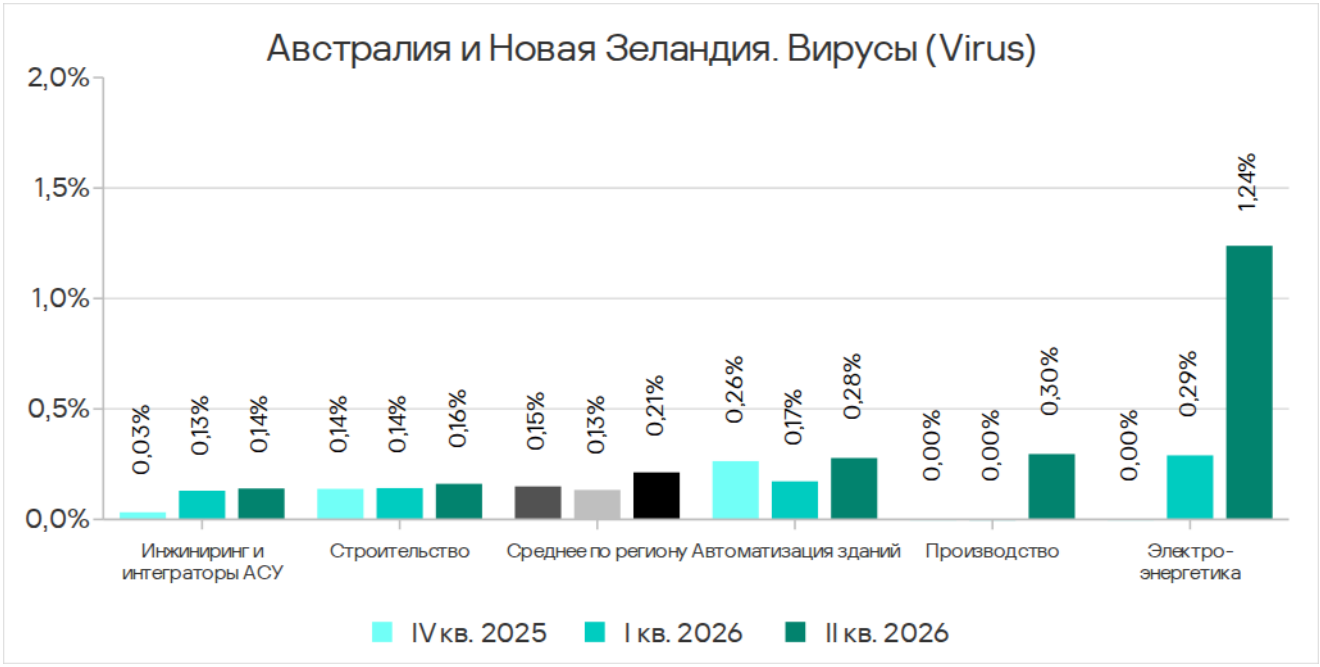


Среди исследуемых отраслей в Восточной Азии самый высокий показатель вирусов – в строительной отрасли (5,93%).

В **Австралии и Новой Зеландии** рост доли компьютеров АСУ, на которых блокируются вирусы, обусловлен прежде всего увеличением в 4,3 раза показателя в электроэнергетической отрасли – с 0,29% до 1,24%. Для региона, в котором показатель атакованных компьютеров АСУ по всем угрозам составляет 0,12%, это очень высокое значение.

Доля компьютеров АСУ, на которых были заблокированы вирусы в Австралии и Новой Зеландии, III квартал 2023 года – II квартал 2026 года





Доля компьютеров АСУ, на которых были заблокированы вирусы в различных отраслях в Австралии и Новой Зеландии

В среднем по миру среди исследуемых отраслей первое место по показателю вирусов занимает строительство (2,03%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю первые три места занимает строительство в разных регионах, на трех позициях в этом списке – отрасли в Юго-Восточной Азии:

1. Строительство в Юго-Восточной Азии – 6,77%;
2. Строительство в Восточной Азии – 5,93%;
3. Строительство в Африке – 5,47%;
4. Автоматизация зданий в Юго-Восточной Азии – 5,35%;
5. Электроэнергетика в Юго-Восточной Азии – 5,07%.

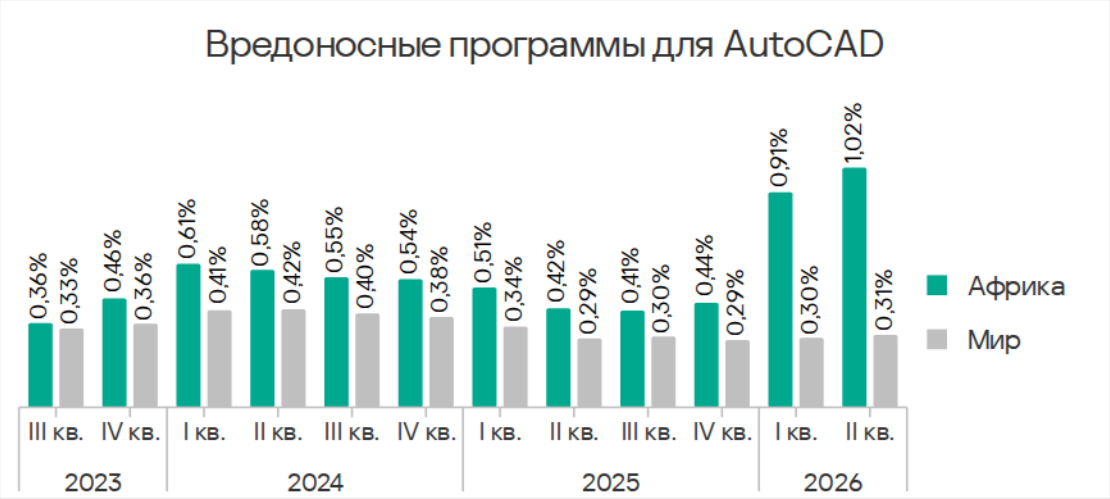
Вредоносные программы для AutoCAD

В мире доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, увеличилась до 0,31%.

В регионах показатель варьирует от практически 0% в Северной Европе до 1,93% в Юго-Восточной Азии, которая неизменно лидирует по этому показателю с большим отрывом от остальных регионов. На втором и третьем местах в этом рейтинге – те же регионы, что и в рейтинге по вирусам: Африка и Восточная Азия.

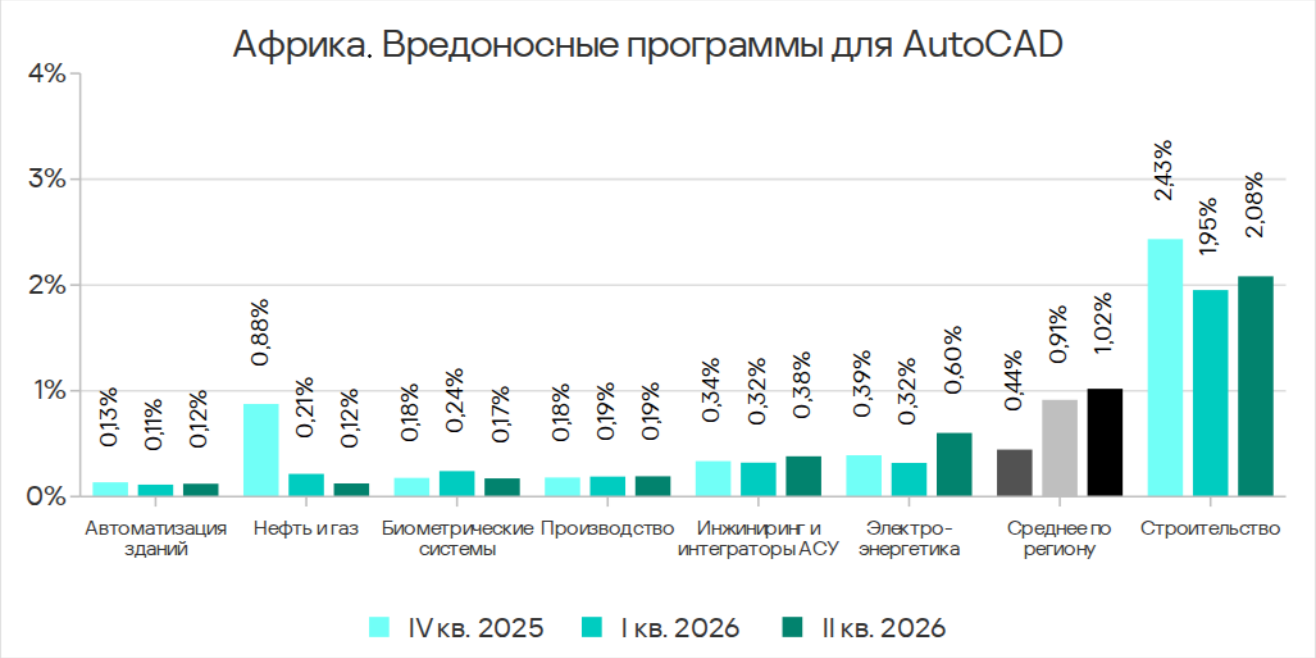
Больше всего показатель за квартал вырос в **Африке.** После увеличения в предыдущем квартале более чем вдвое, значение в регионе продолжило расти (хотя и не столь драматично) и достигло 1,02%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD в Африке III квартал 2023 года – II 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 превышают 2%, что необычно много для этой категории угроз.

Среди исследуемых отраслей в регионе самый высокий показатель вредоносных программ для AutoCAD, как и у вирусов, – в строительной отрасли (2,08%).



Доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD в различных отраслях в Африке

В среднем по миру среди исследуемых отраслей первое место по показателю вредоносных программ для AutoCAD занимает строительство (1,17%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят:

1. Строительство в Восточной Азии – 6,38% (!);
2. Строительство в Юго-Восточной Азии – 4,05%;
3. Строительство в Африке – 2,08%;
4. Электроэнергетика в Восточной Азии – 1,84%;
5. Инжиниринг и интеграторы АСУ в Восточной Азии – 1,33%.

Основные источники угроз

Во втором квартале 2026 года из всех источников угроз показатель вырос только у почтовых клиентов.

Интернет

В мире во втором квартале 2026 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, уменьшилась до 7,61%. Это наименьший показатель с 2021 года.

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, варьирует от 3,82% в Северной Европе до 10,35% в

Южной Азии, которая поднялась со второго на первое место в соответствующем рейтинге. На втором месте – Юго-Восточная Азия (9,65%).

За квартал показатель увеличился в трех регионах – в Восточной Азии, Южной Азии и России.

Отметим, что в Южной Азии резко вырос соответствующий показатель в Бангладеш (с 10,52% до 17,76%).

В среднем по миру среди исследуемых отраслей первое место по показателю угроз из интернета занимает строительство (8,99%).

Среди исследуемых отраслей во всех регионах в топ-5 по этому показателю входят отрасли из Южной и Юго-Восточной Азии:

1. Биометрические системы в Южной Азии – 13,03%;
2. Инжиниринг и интеграторы АСУ в Южной Азии – 12,16%;
3. Строительство в Юго-Восточной Азии – 11,69%;
4. Электроэнергетика в Юго-Восточной Азии – 11,24%;
5. Производство в Южной Азии – 10,94%.

Почтовые клиенты

В мире доля компьютеров АСУ, на которых были заблокированы почтовые клиенты, увеличилась до 2,84%.

В регионах показатель варьирует от 0,52% в Северной Европе до 6,45% в Южной Европе.

Во втором квартале 2026 года показатель угроз из почтовых клиентов больше всего увеличился в Южной Америке (на 0,95 п. п.) и Африке (на 0,77 п. п.).

Южная Америка находится на втором месте в рейтинге регионов по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов (5,2%). Среди стран региона самые высокие значения – в Мексике (8,35%) и Уругвае (7,41%). Среди исследуемых отраслей в регионе самый высокий показатель – у биометрических систем (11,52%), у этой же отрасли показатель вырос больше всего.

Африка находится на пятом месте в рейтинге регионов по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов (4,3%). При этом в Намибии показатель составил 12,35%. Среди исследуемых отраслей в регионе самый высокий показатель – у автоматизации зданий (8,06%), больше всего значение увеличилось у биометрических систем.

В среднем по миру среди исследуемых отраслей на первом месте по показателю угроз из почтовых клиентов находятся биометрические системы (10,65%). В этом секторе значение у почтовых клиентов превышает показатель угроз из интернета.

Среди исследуемых отраслей во всех регионах в топ-5 по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, входят:

1. Биометрические системы в Южной Европе – 19,14%;
2. Автоматизация зданий в Южной Европе – 12,49%;
3. Биометрические системы в Южной Америке – 11,52%;
4. Автоматизация зданий в Восточной Европе – 8,42%;
5. Автоматизация зданий в Африке – 8,06%.

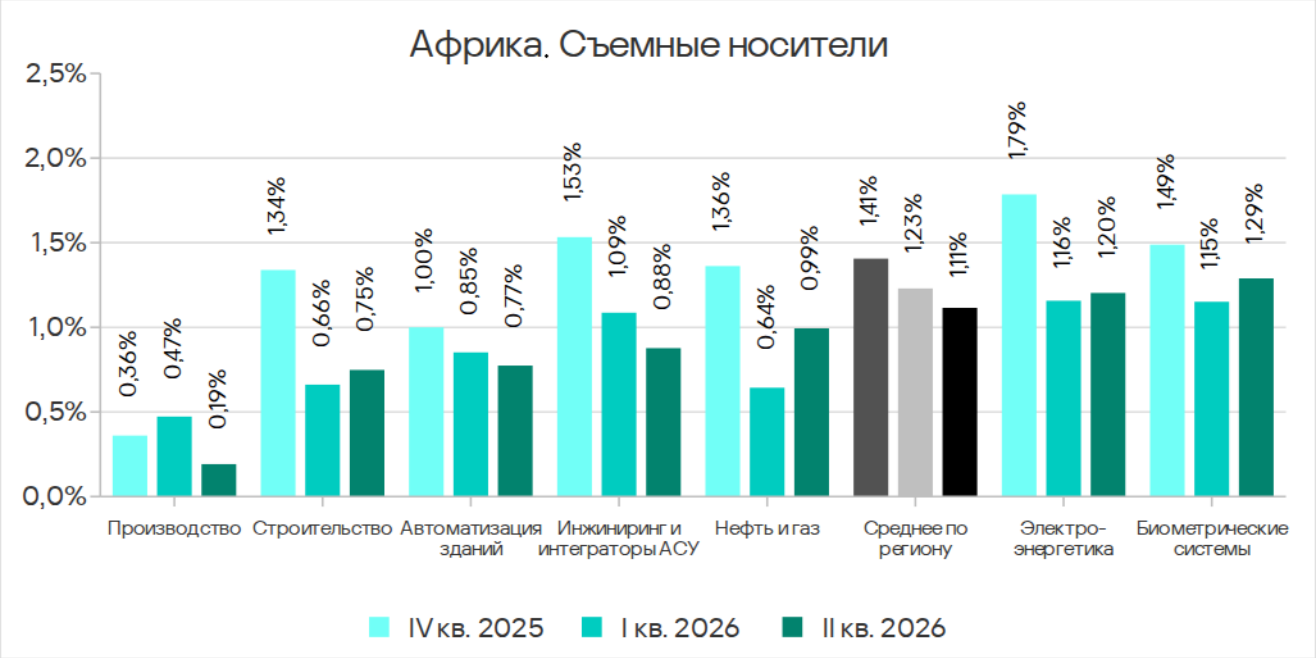
Съемные носители

В мире доля компьютеров АСУ, на которых угрозы были обнаружены при подключении съемных носителей, продолжила снижаться и достигла минимального значения за исследуемый период – 0,24%.

В регионах показатель варьирует от 0,04% в Австралии и Новой Зеландии до 1,11% в Африке. За квартал он уменьшился во всех регионах, кроме Юго-Восточной Азии и Австралии и Новой Зеландии, где значения практически не изменились.

Африка – многолетний лидер этого рейтинга. Хотя доля компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, в Африке неуклонно уменьшается, отрыв от остальных регионов все еще весьма значительный.

Среди исследуемых отраслей в Африке самые высокие показатели угроз, которые блокируются при подключении съемных носителей, в электроэнергетике (1,20%) и у биометрических систем (1,29%).



Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях в различных отраслях в Африке

В среднем по миру среди исследуемых отраслей на первом месте по показателю угроз на съемных носителях находится электроэнергетика (0,43%).

Среди исследуемых отраслей во всех регионах в топ-5 по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, входят:

1. Электроэнергетика в Восточной Азии – 1,34%;
2. Биометрические системы в Африке – 1,29%;
3. Электроэнергетика в Африке – 1,20%;
4. Биометрические системы в Южной Азии – 1,06%;
5. Нефтегазовая отрасль в Африке – 0,99%.

Сетевые папки

Доля компьютеров АСУ, на которых угрозы блокируются в сетевых папках, постепенно снижается. Во втором квартале 2026 года она была наименьшей за исследуемый период – 0,023%.

В регионах показатель варьирует от 0,00% в Австралии и Новой Зеландии до 0,11% в Восточной Азии.

Восточная Азия традиционно лидирует по этому показателю с большим отрывом от остальных регионов. Как и в случае вирусов и вредоносных

программ для AutoCAD, среди стран региона безусловный лидер по показателю угроз в сетевых папках – материковый Китай (0,11%).

Показатель угроз в сетевых папках за квартал увеличился только **в Африке** – в основном за счет роста значения в автоматизации зданий до 0,05%.

В среднем по миру среди исследуемых отраслей на первом месте по показателю угроз в сетевых папках находится нефтегазовая отрасль (0,04%).

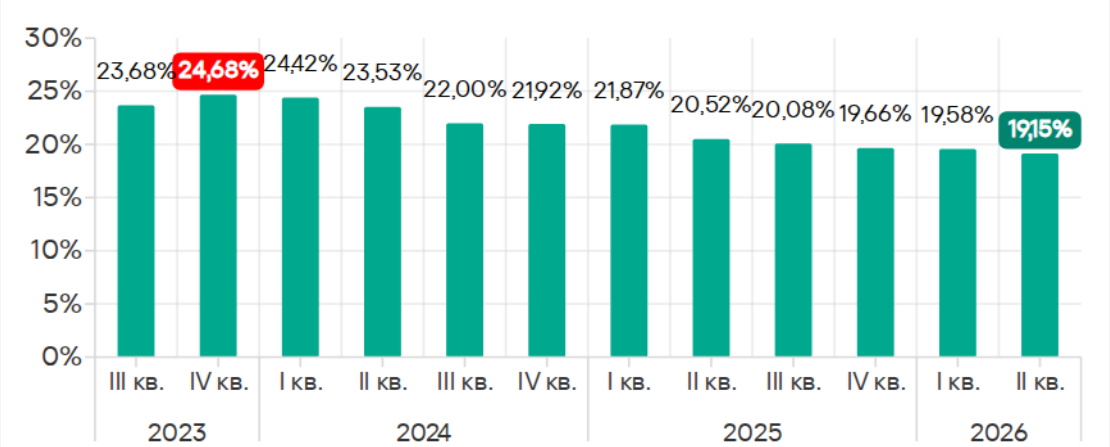
Среди исследуемых отраслей во всех регионах в топ-5 по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, входят четыре отрасли в Восточной Азии:

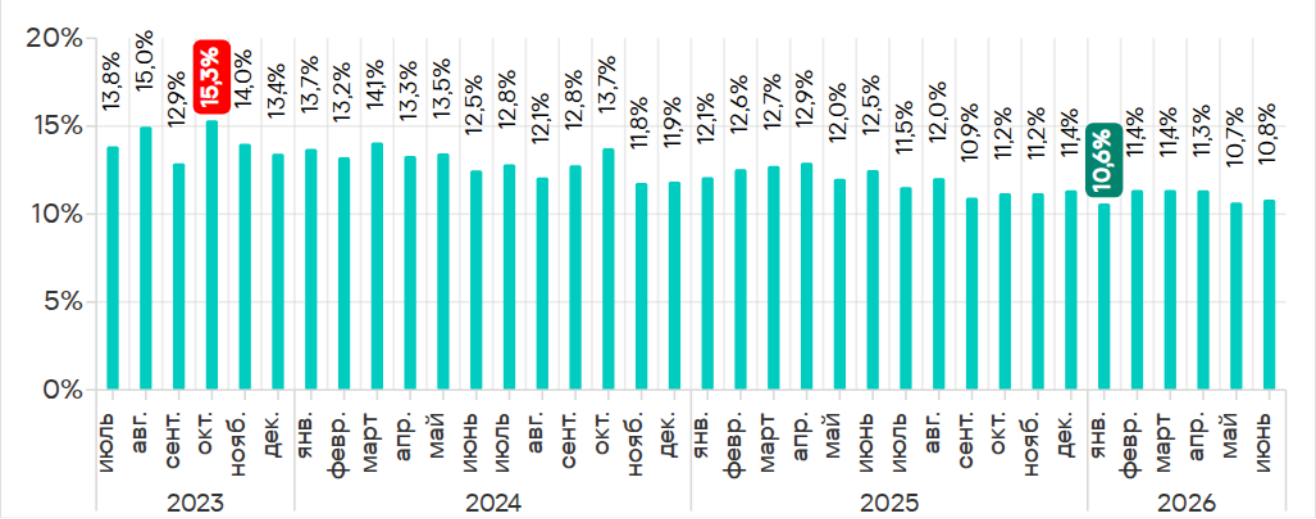
1. Биометрические системы в Восточной Азии – 0,23%;
2. Автоматизация зданий в Восточной Азии – 0,17%;
3. Инжиниринг и интеграторы АСУ в Восточной Азии – 0,13%;
4. Биометрические системы в Юго-Восточной Азии – 0,11%;
5. Строительство в Восточной Азии – 0,11%.

Основная статистика

Все угрозы

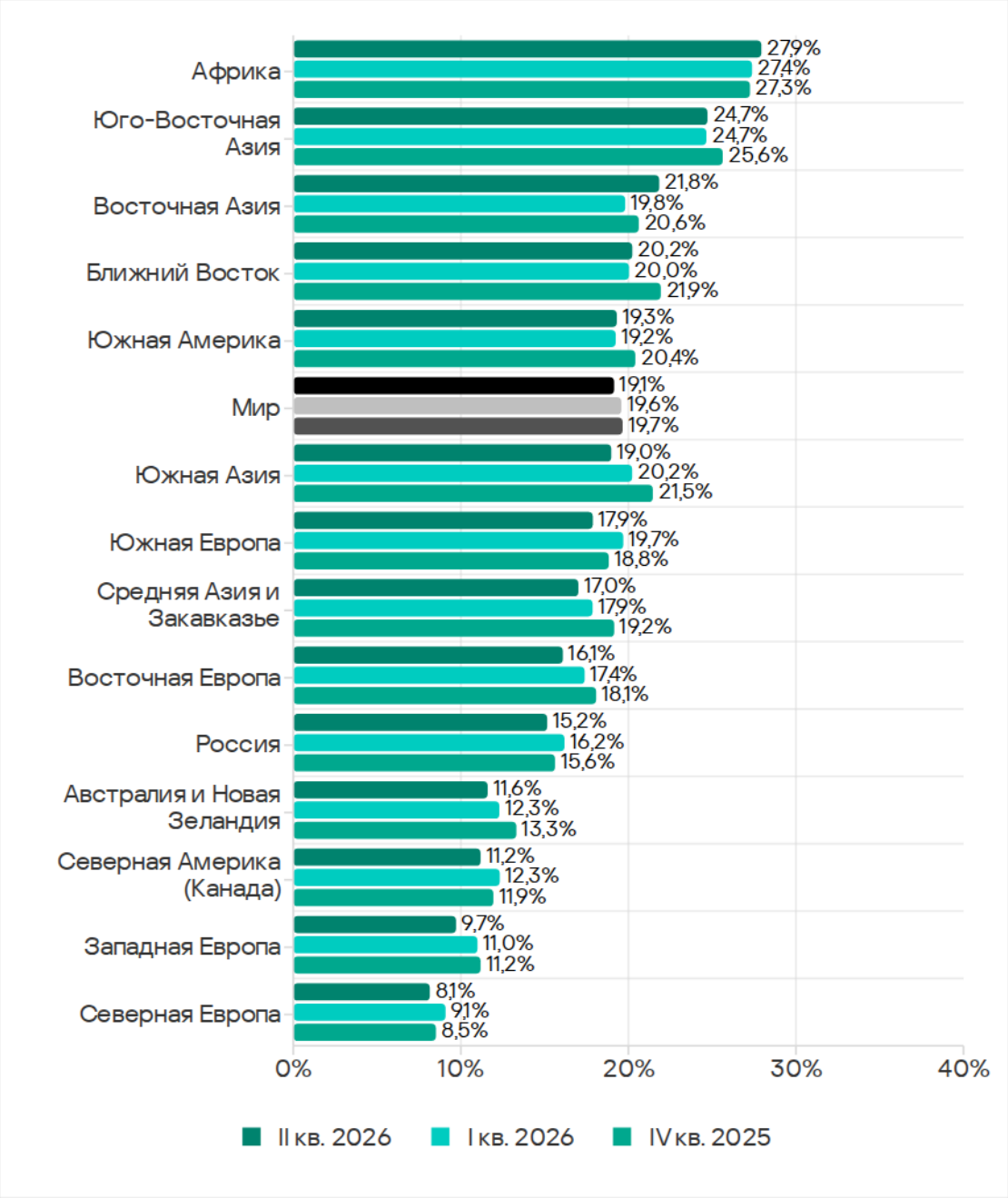
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, III квартал 2023 года – II квартал 2026 года



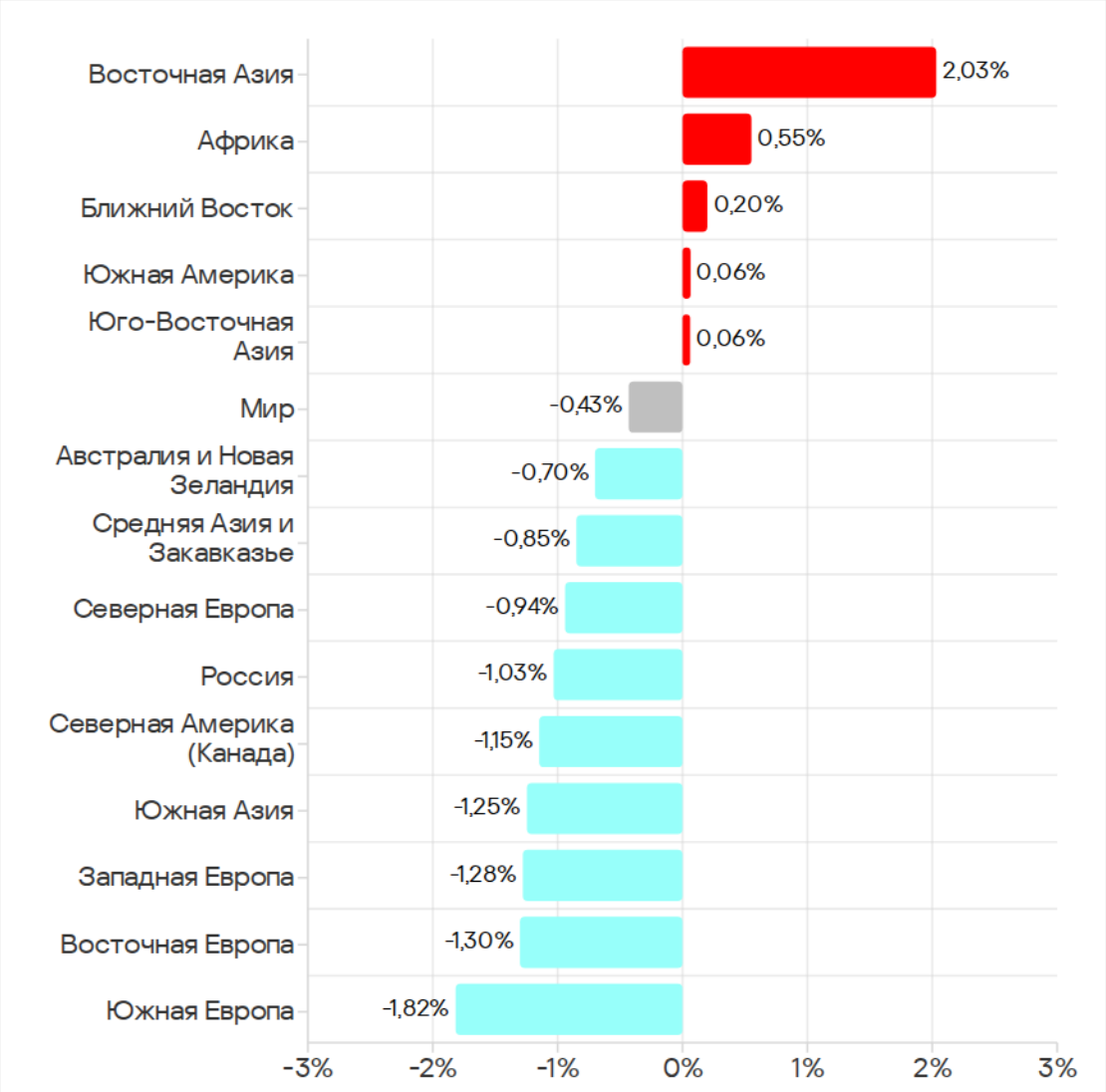


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, июль 2023 года – июнь 2026 года

Рейтинг регионов по доле атакованных компьютеров АСУ

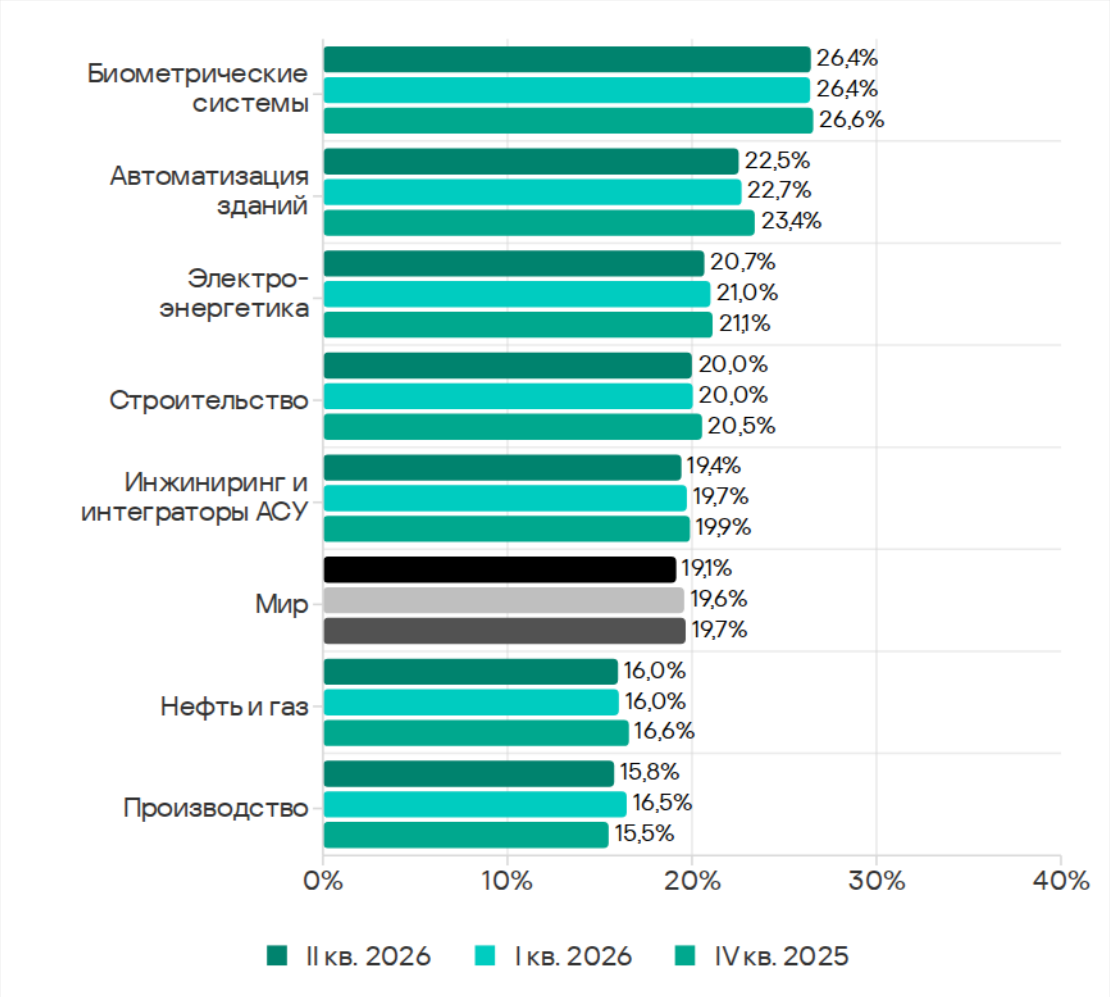


Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, II квартал 2026 года

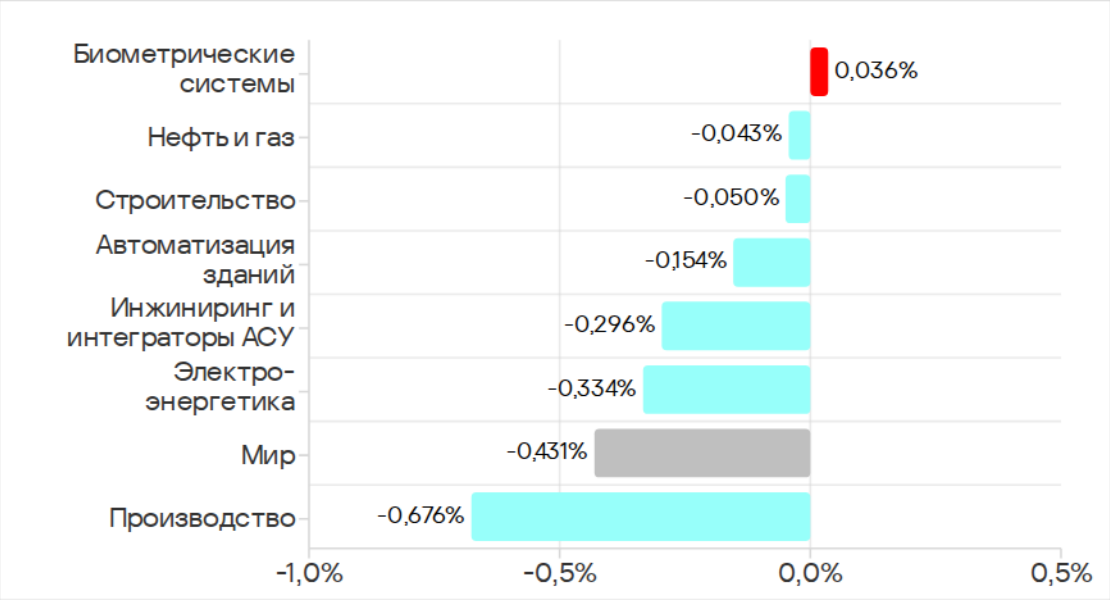


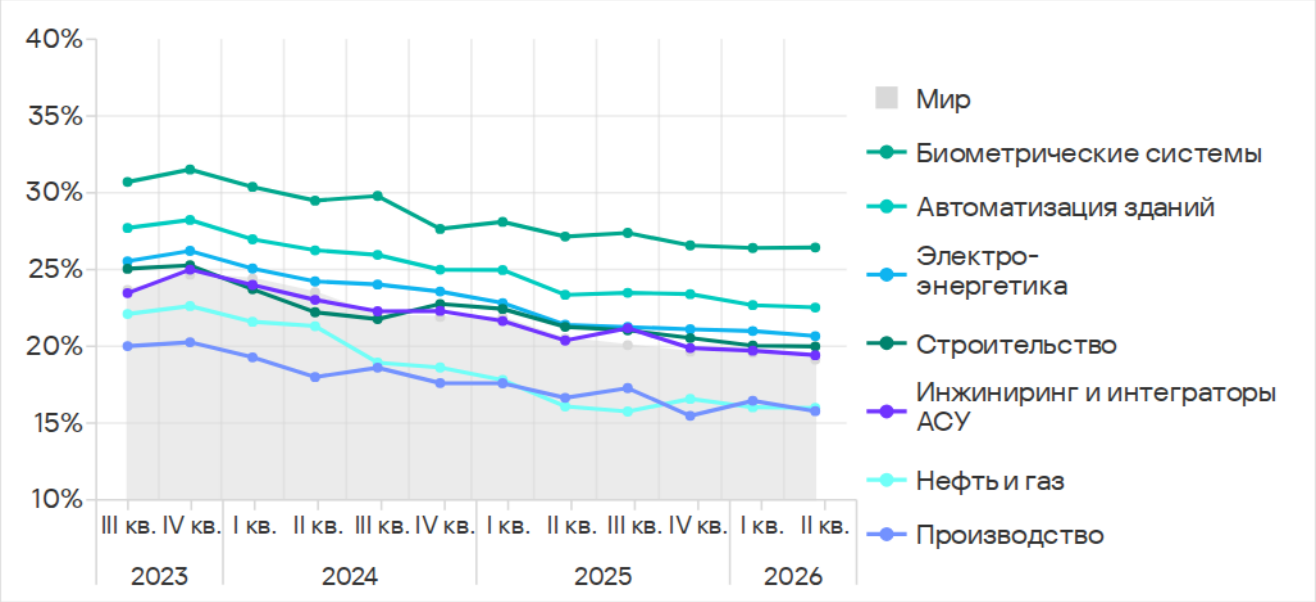
Исследуемые отрасли

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, II квартал 2026 года





Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в исследуемых отраслях, III квартал 2023 года – II квартал 2026 года

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. Желтым подсвечены максимальные среди отраслей показатели определенной категории или источника угрозы. Красный цвет указывает на то, что значение близко к максимальному.

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Строительство	Инжиниринг и интеграторы АСУ	Нефть и газ	Производство	Показатель категории в мире
Интернет	8,14%	8,37%	8,65%	8,99%	8,17%	5,96%	6,53%	7,61%
Почтовые клиенты	10,65%	5,85%	2,45%	2,72%	2,43%	1,67%	2,19%	2,84%
Съемные носители	0,30%	0,27%	0,43%	0,22%	0,24%	0,41%	0,22%	0,24%
Сетевые папки	0,03%	0,03%	0,02%	0,02%	0,03%	0,04%	0,01%	0,02%
Показатель отрасли в мире	26,44%	22,53%	20,67%	20,00%	19,43%	15,99%	15,79%	

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

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Строительство	Инжиниринг и интеграторы АСУ	Нефть и газ	Производство	Показатель категории в мире
Вредоносные скрипты и фишинговые страницы	13,20%	8,96%	5,77%	6,42%	5,50%	3,62%	4,92%	5,42%
Ресурсы в интернете из списка запрещенных	3,33%	4,01%	4,72%	4,13%	4,25%	4,01%	3,33%	4,31%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,29%	5,17%	4,10%	3,07%	3,26%	2,82%	2,64%	3,30%
Вредоносные документы (MSOffice+PDF)	6,03%	3,50%	1,97%	1,61%	1,59%	1,34%	1,46%	1,77%
Черви (Worm)	2,29%	1,86%	1,81%	1,13%	1,25%	1,56%	1,14%	1,43%
Вирусы (Virus)	1,42%	1,62%	1,92%	2,03%	1,32%	1,25%	1,12%	1,29%
Майнеры — исполняемые файлы для ОС Windows	0,46%	0,50%	0,55%	0,57%	0,48%	0,66%	0,29%	0,48%
Вредоносные программы для AutoCAD	0,10%	0,16%	0,37%	1,17%	0,32%	0,38%	0,20%	0,31%
Программы-вымогатели	0,31%	0,29%	0,28%	0,14%	0,14%	0,27%	0,15%	0,16%
Веб-майнеры, выполняемые в браузерах	0,21%	0,19%	0,24%	0,28%	0,17%	0,34%	0,17%	0,14%
Показатель отрасли в мире	26,44%	22,53%	20,67%	20,00%	19,43%	15,99%	15,79%	

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.

Автоматизация зданий занимает второе место по тому же набору угроз: угрозы из почтовых клиентов, вредоносные скрипты, вредоносные документы, шпионские программы, программы-вымогатели.

Строительная отрасль занимает первое место по показателю угроз из интернета и третье – по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных. Кроме того, отрасль лидирует по показателям вирусов и вредоносных программ для AutoCAD.

Электроэнергетика находится на первом месте по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, и на третьем месте по показателю червей (распространяются преимущественно на съемных носителях). Для отрасли также актуальны угрозы из интернета, значение в электроэнергетике по этому источнику – на втором месте среди отраслей. А по показателю ресурсов в интернете из списка запрещенных электроэнергетика находится на первом месте.

Нефтегазовая отрасль во втором квартале 2026 года находится на первом месте по угрозам из сетевых папок и по доле майнеров, которые блокируются на компьютерах АСУ в отрасли.

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.

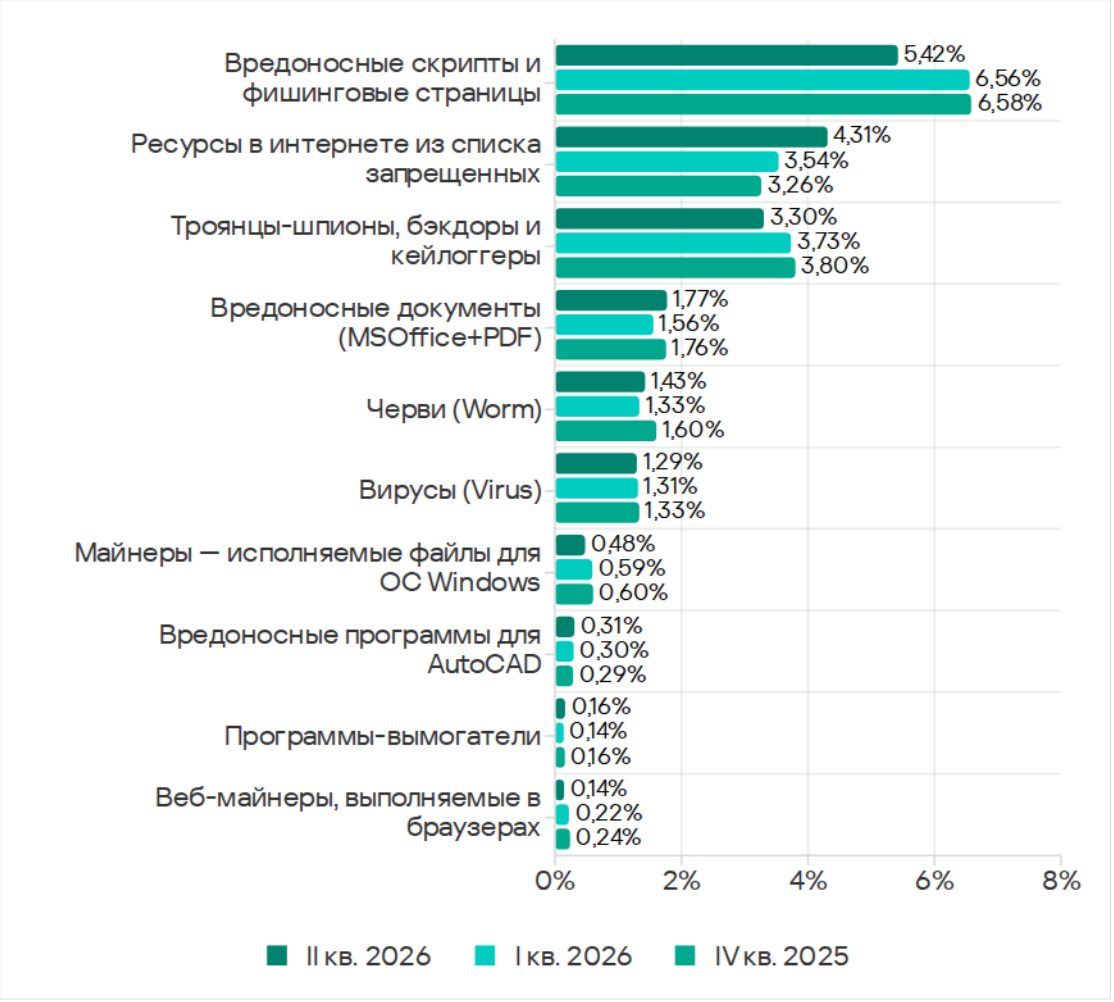
Вредоносные программы для AutoCAD распространяются разными способами, поэтому мы не относим их к конкретной группе по типу распространения.

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.

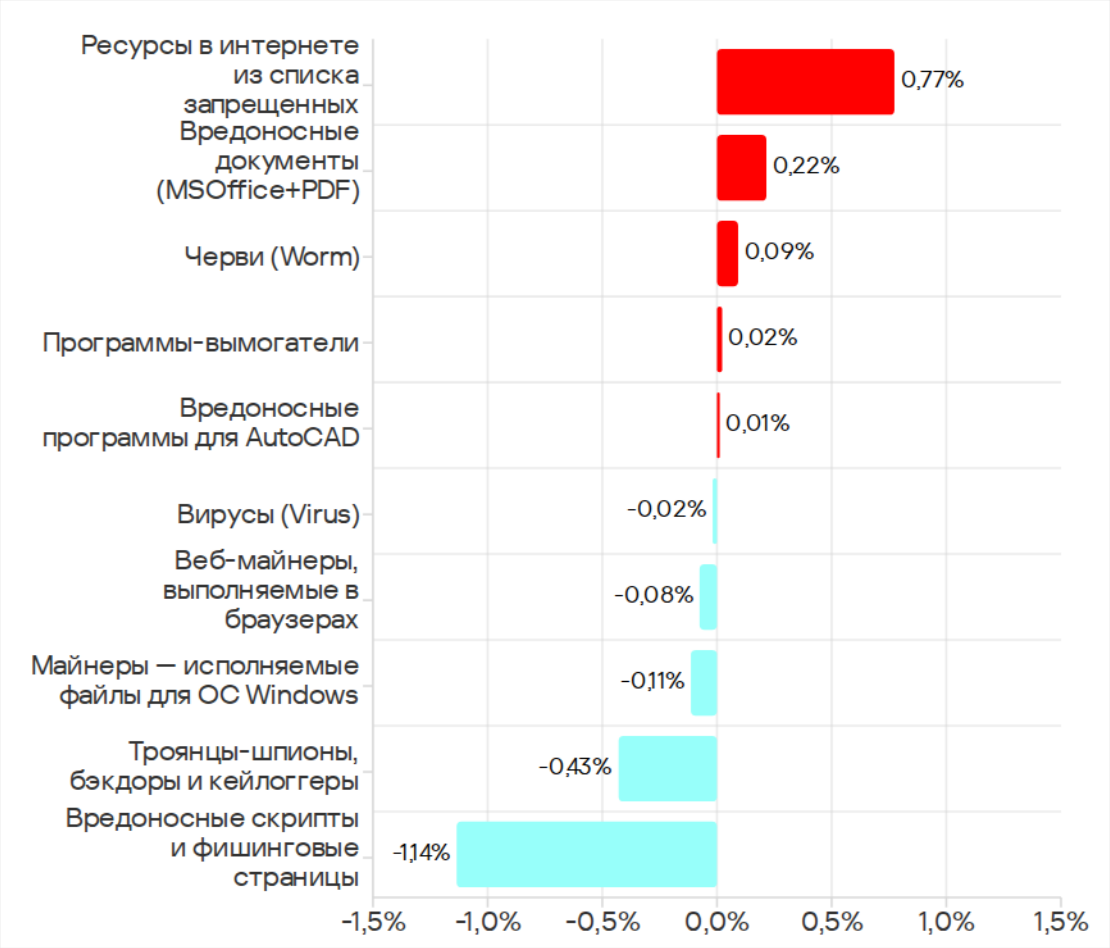
Следует заметить, что в небольшом проценте случаев категории угроз, которые мы относим к объектам первичного заражения, скажем, вредоносные ссылки, также используются на последующих этапах атаки. Так, например, иногда ссылка на вредоносный ресурс может быть обнаружена при сканировании реестра компьютера, 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, II 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.

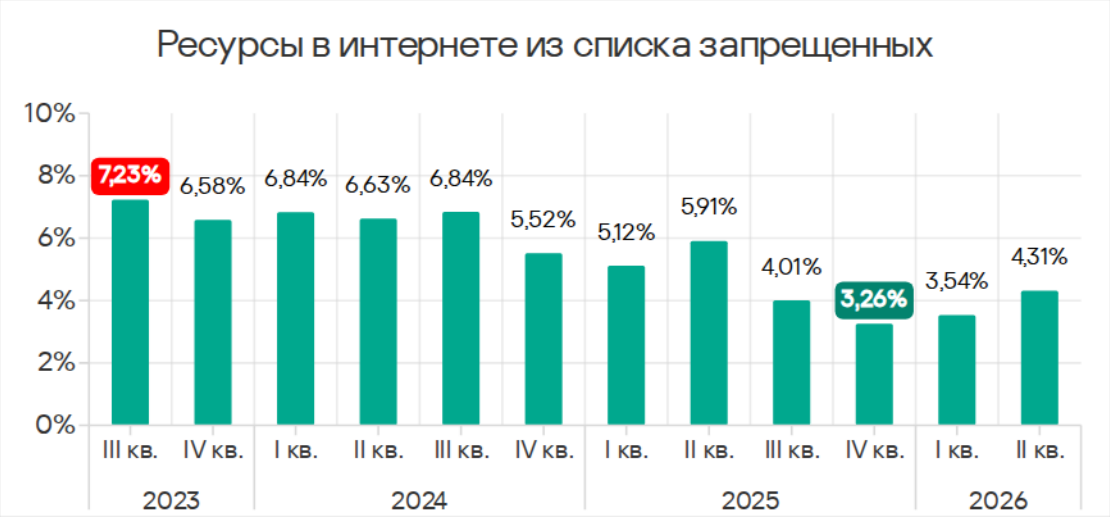
Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

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.

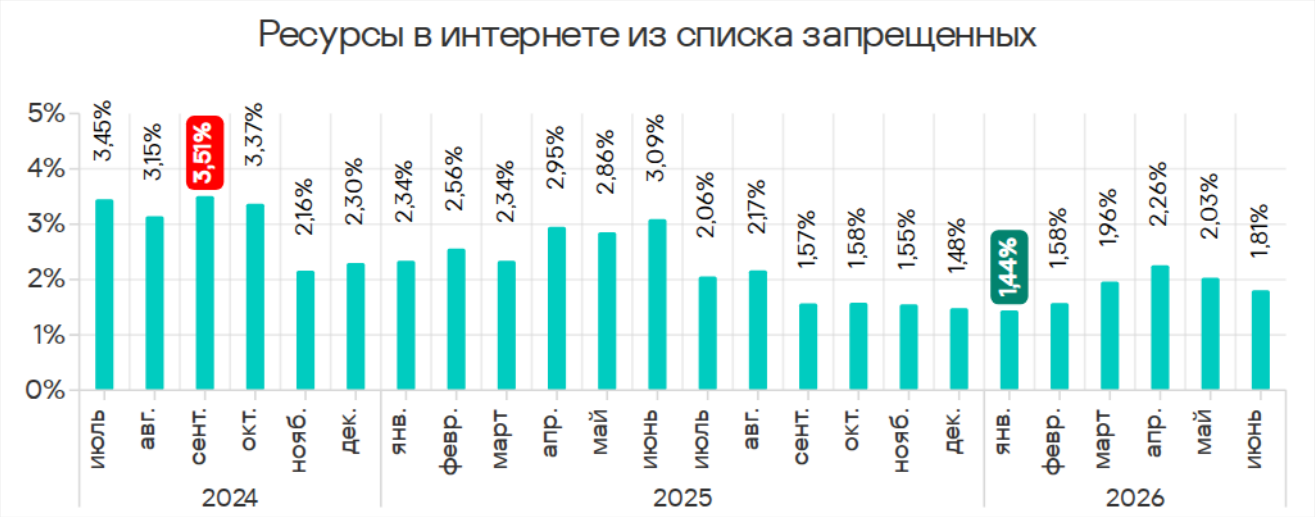
Высокие значения параметра, как правило, свидетельствуют о слабом контроле выполнения политик ИБ (компьютеры АСУ имеют так или иначе доступ к интернету, и этим доступом часто пользуются), недостатках защиты от фишинга (многие вредоносные ссылки доставляются в фишинговых сообщениях) и недостатках культуры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

В рейтинге категорий вредоносных объектов по доле атакованных компьютеров ресурсы в интернете из списка запрещенных во втором квартале 2026 года вернулась на второе место.

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



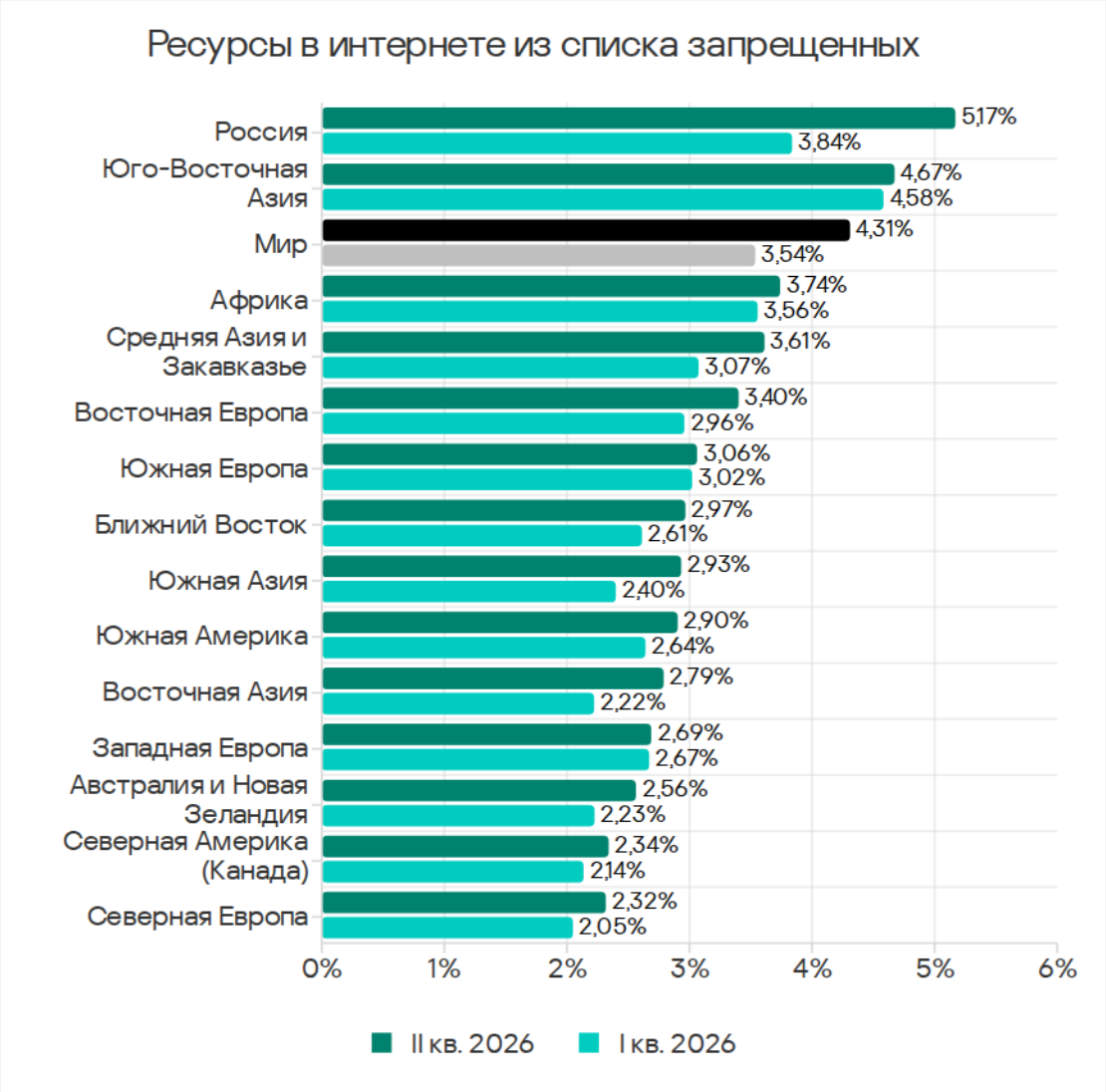
В апреле 2026 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, была максимальной за последний год.



Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, июль 2024 года – июнь 2026 года

Во втором квартале 2026 года в рейтинге регионов по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, впервые за два года на первом месте оказалась Россия.

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

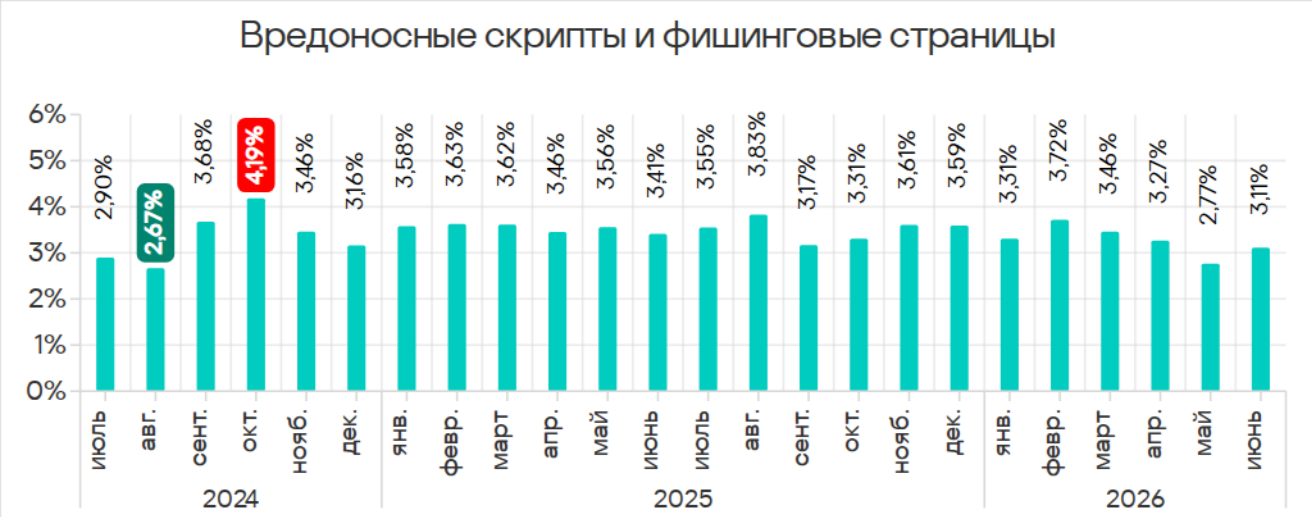


Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, II квартал 2026 года

Вредоносные скрипты и фишинговые страницы (JS и HTML)

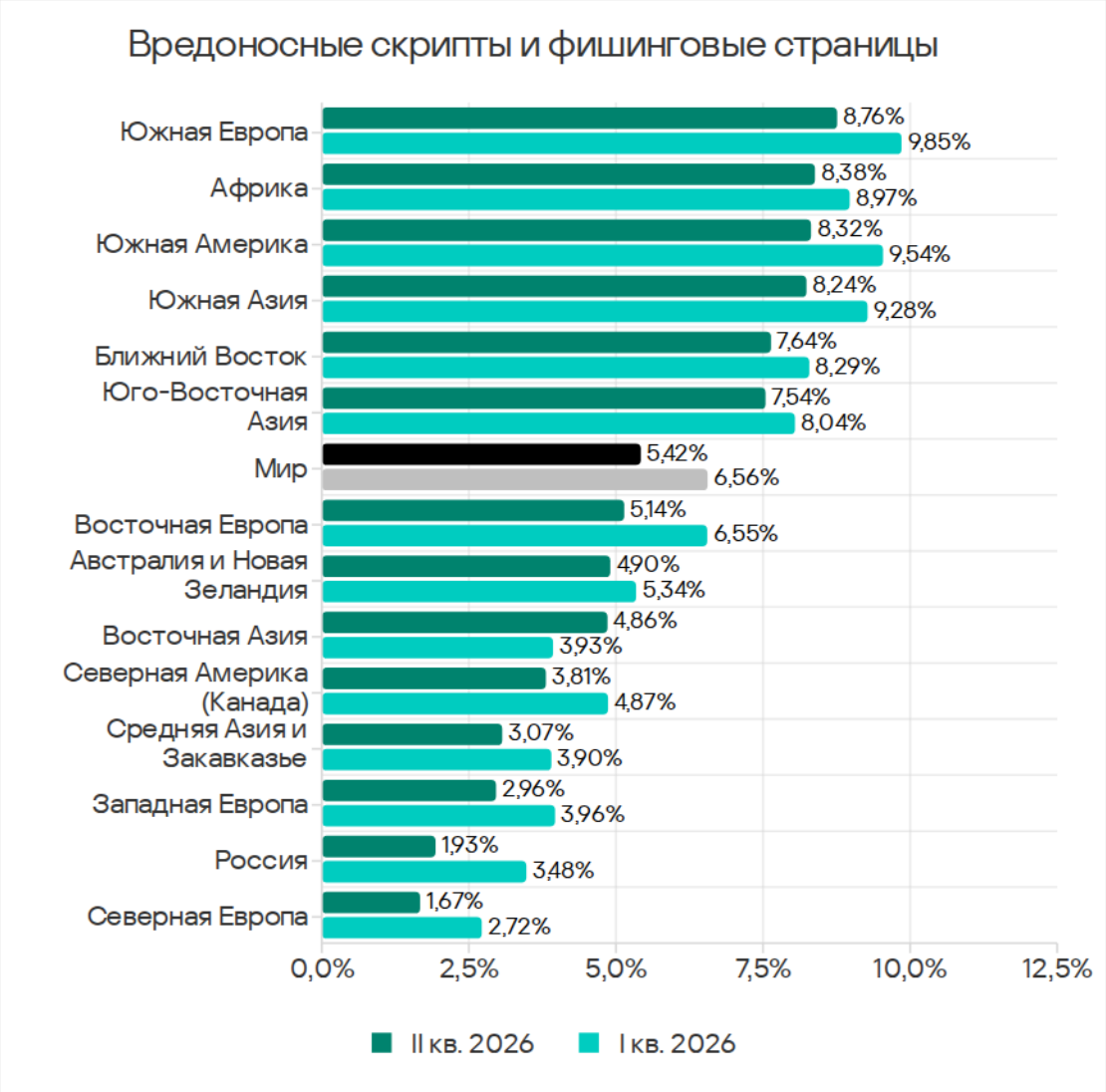
Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач – от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для 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, III квартал 2023 года – II квартал 2026 года



Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, июль 2024 года – июнь 2026 года

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



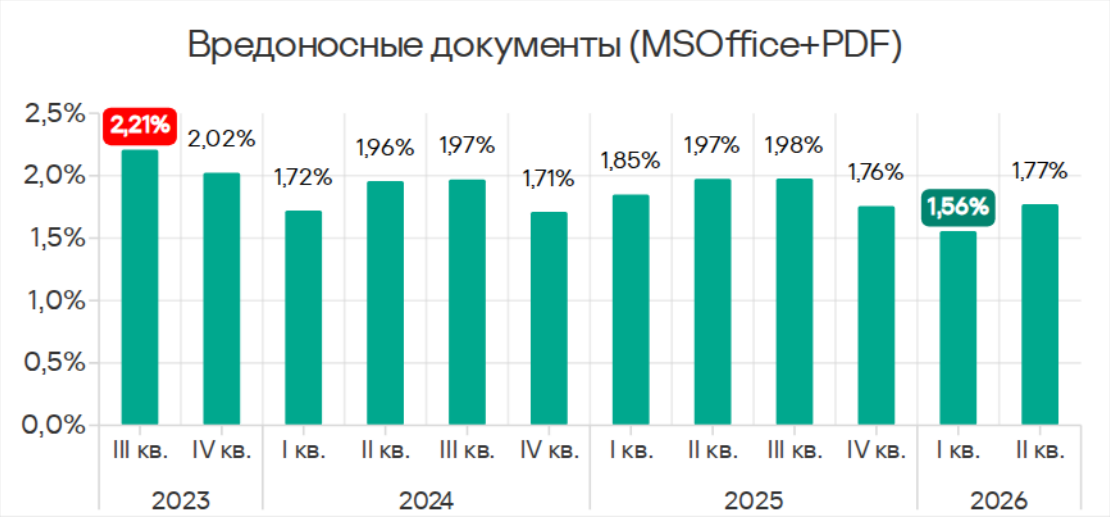
Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, II квартал 2026 года

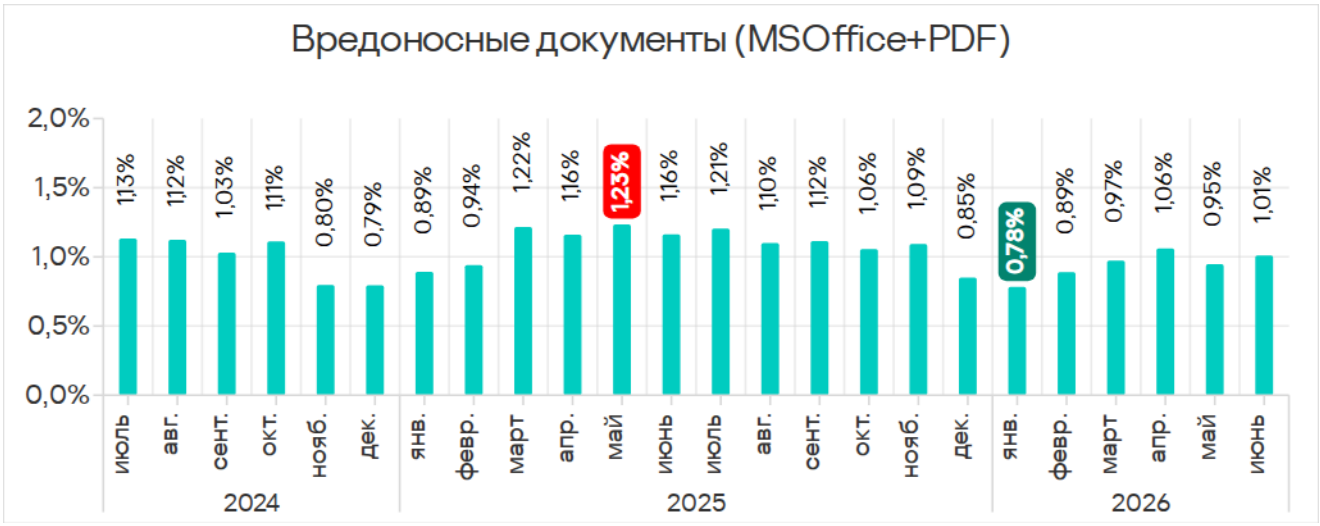
Вредоносные документы (MSOffice+PDF)

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, III квартал 2023 года – II квартал 2026 года

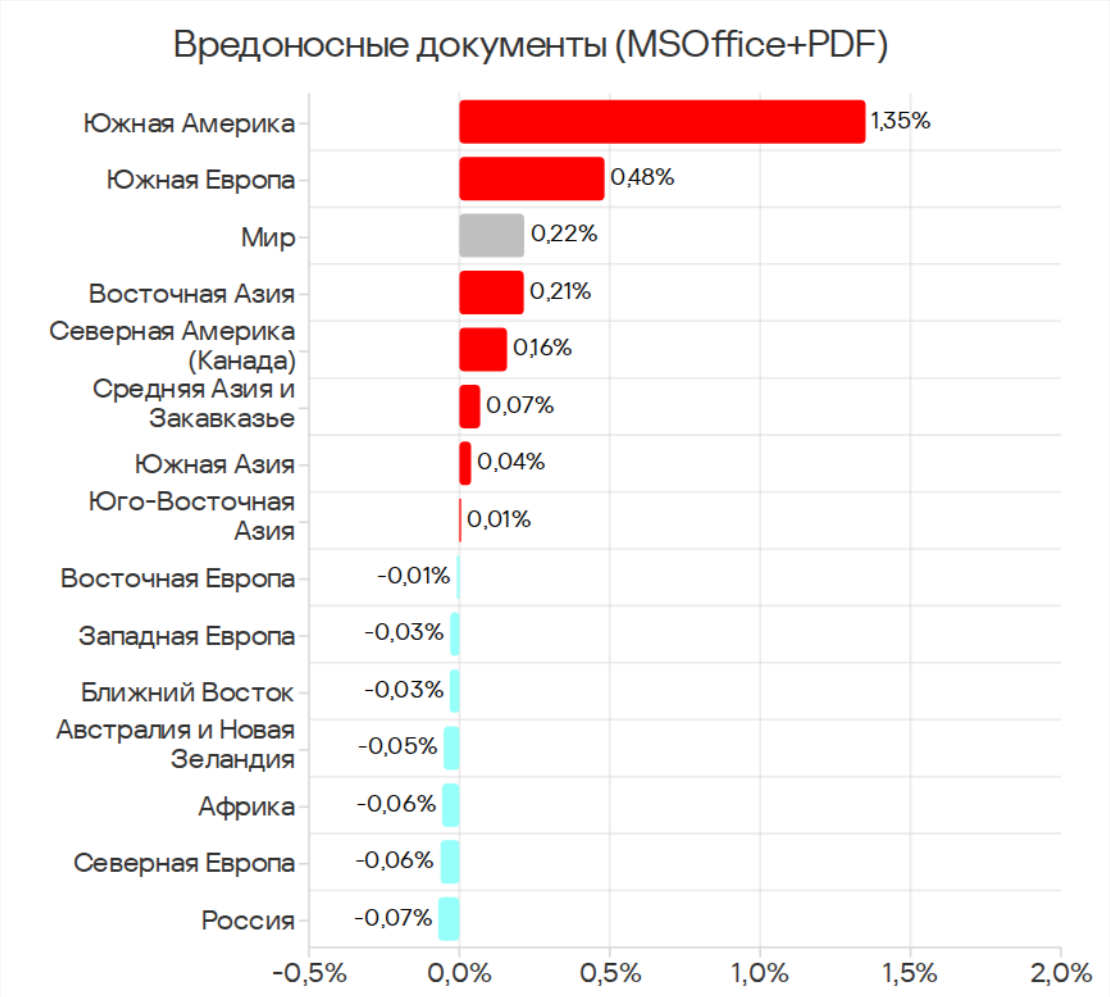




Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, июль 2024 года – июнь 2026 года

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

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные документы, II 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

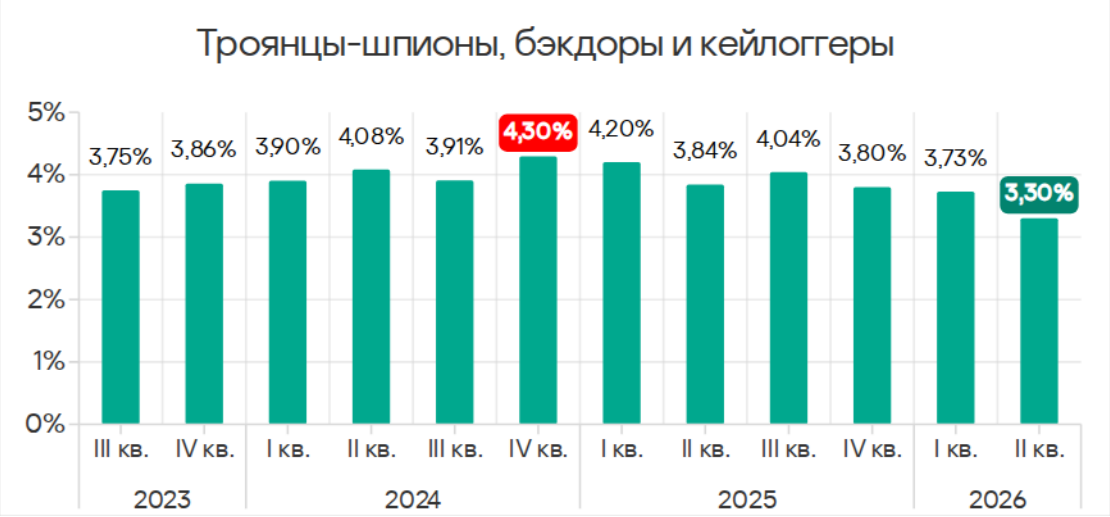
распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных. В большинстве случаев конечная цель атак с применением такого ПО – кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

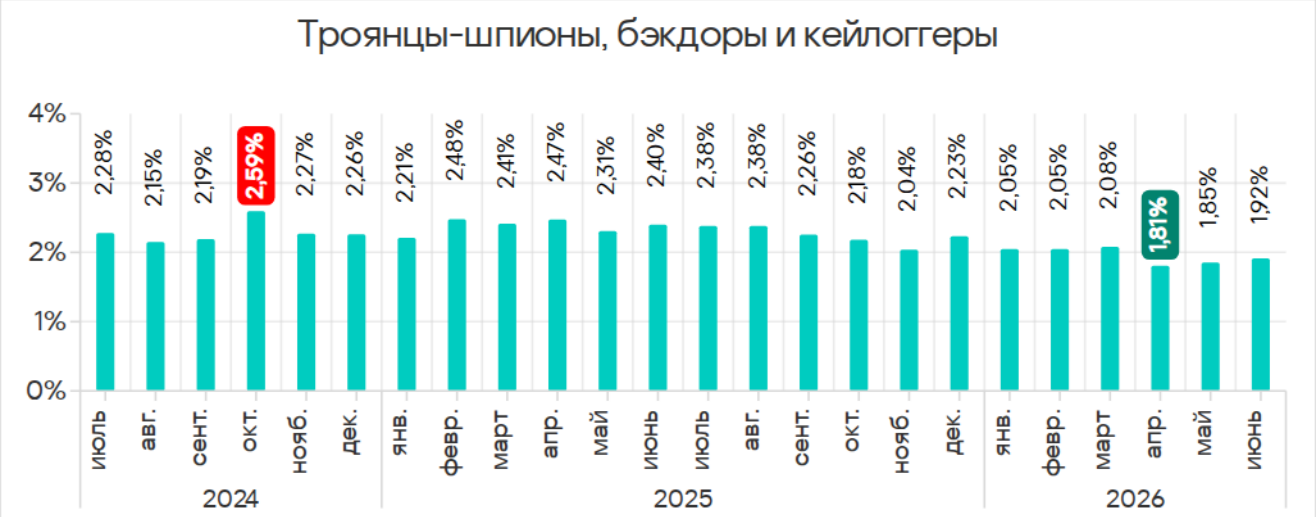
Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

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).

Во втором квартале 2026 года доля компьютеров АСУ, на которых были заблокированы шпионские программы, оказалась наименьшей с 2022 года.

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

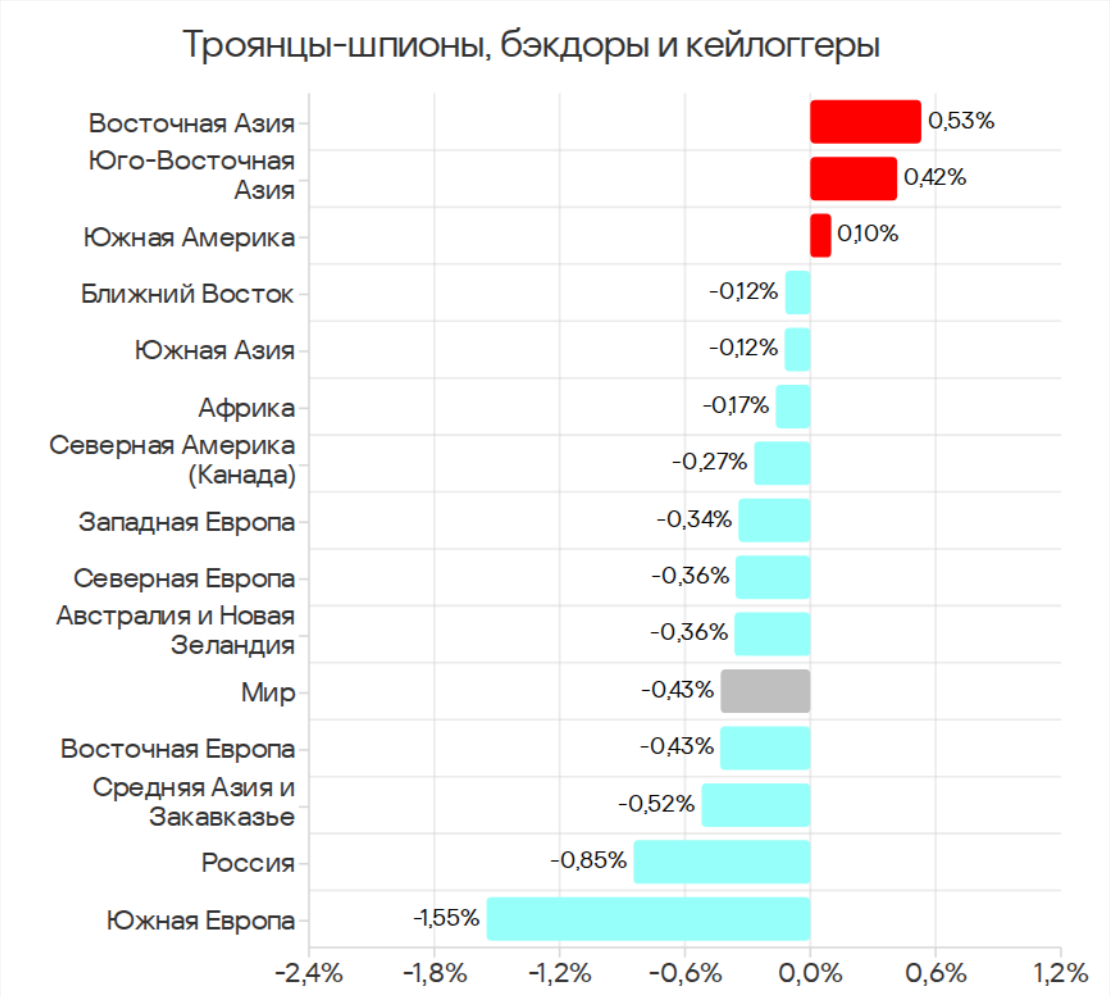




Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, июль 2024 года – июнь 2026 года

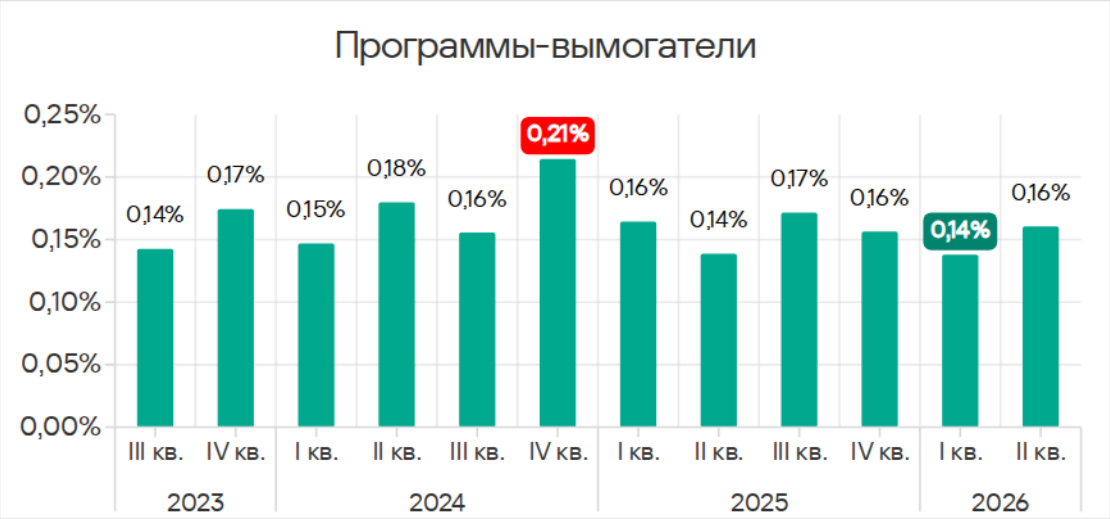
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы

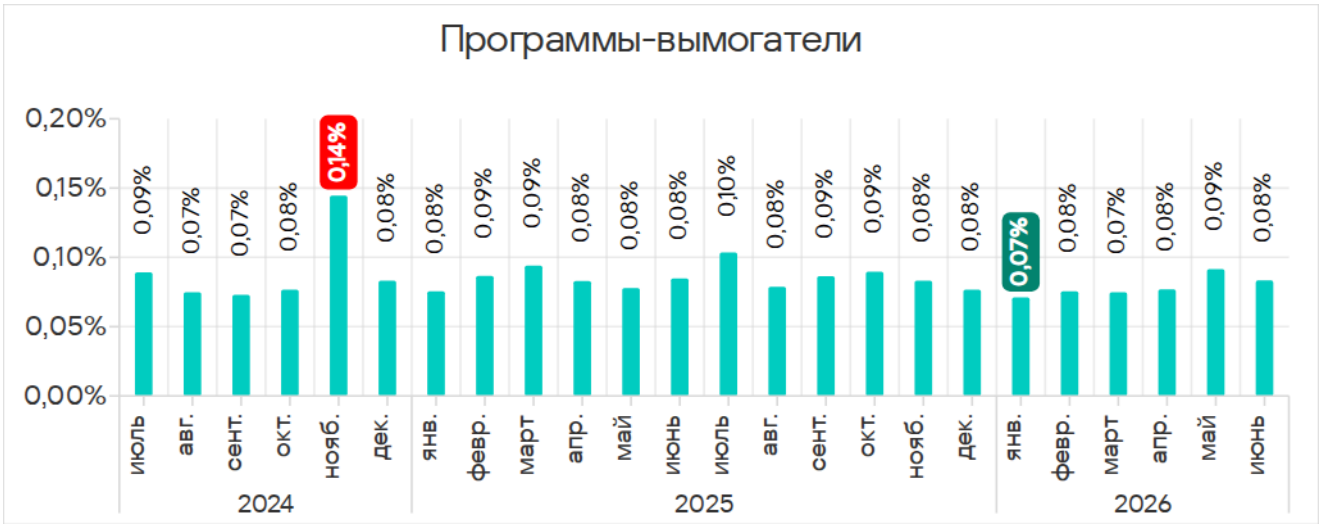
Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, II квартал 2026 года



Программы-вымогатели

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

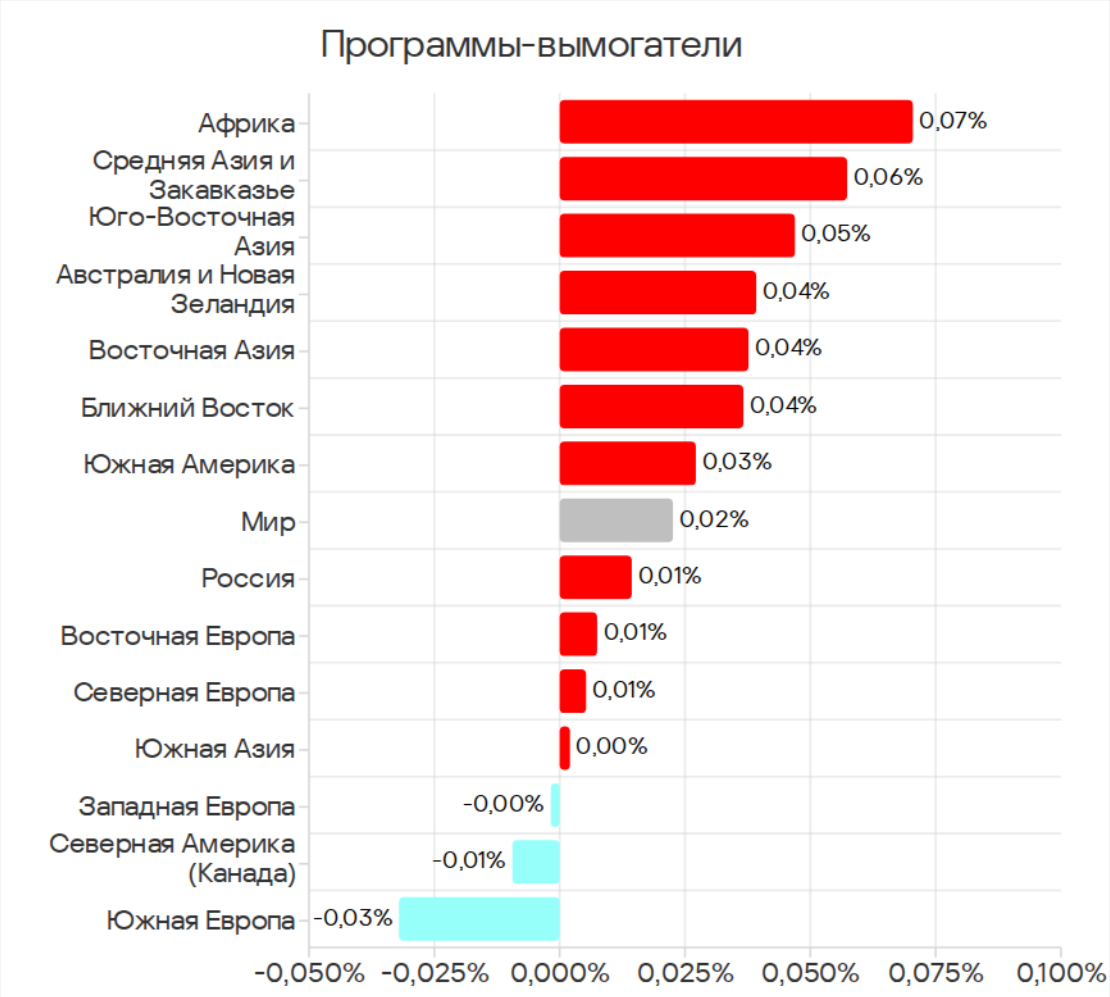




Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, июль 2024 года – июнь 2026 года

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

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



Майнеры – исполняемые файлы для ОС Windows

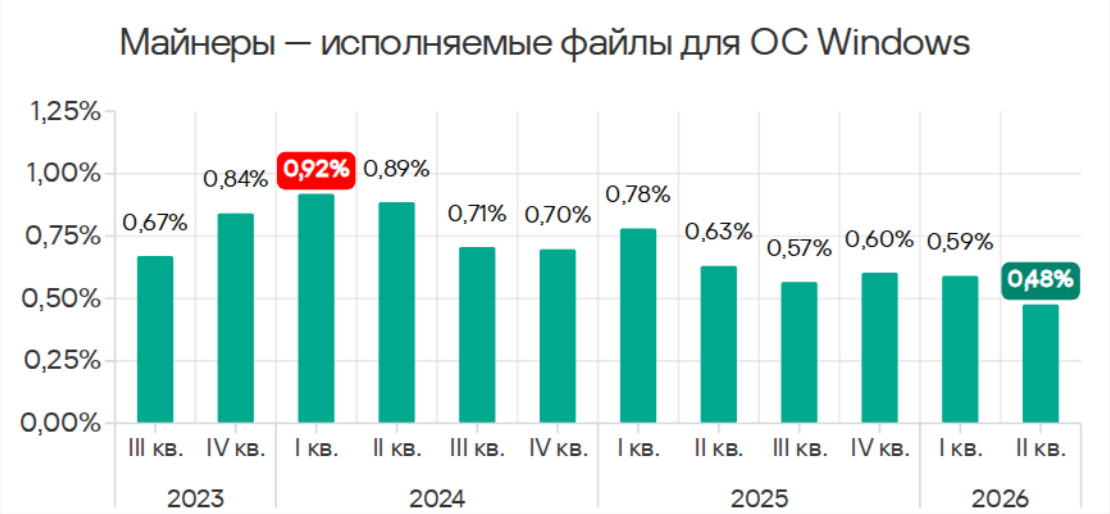
Наряду с «классическими» майнерами – приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют, – появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры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

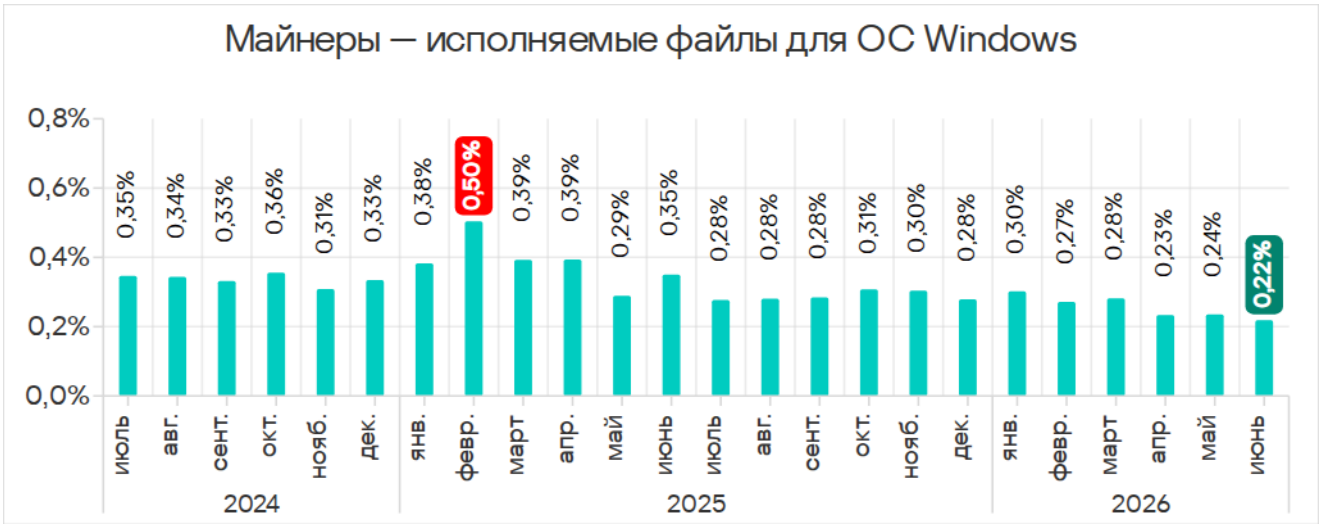
числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом. Бесфайловое выполнение майнера делает проблематичным его обнаружение средствами защиты.

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.

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

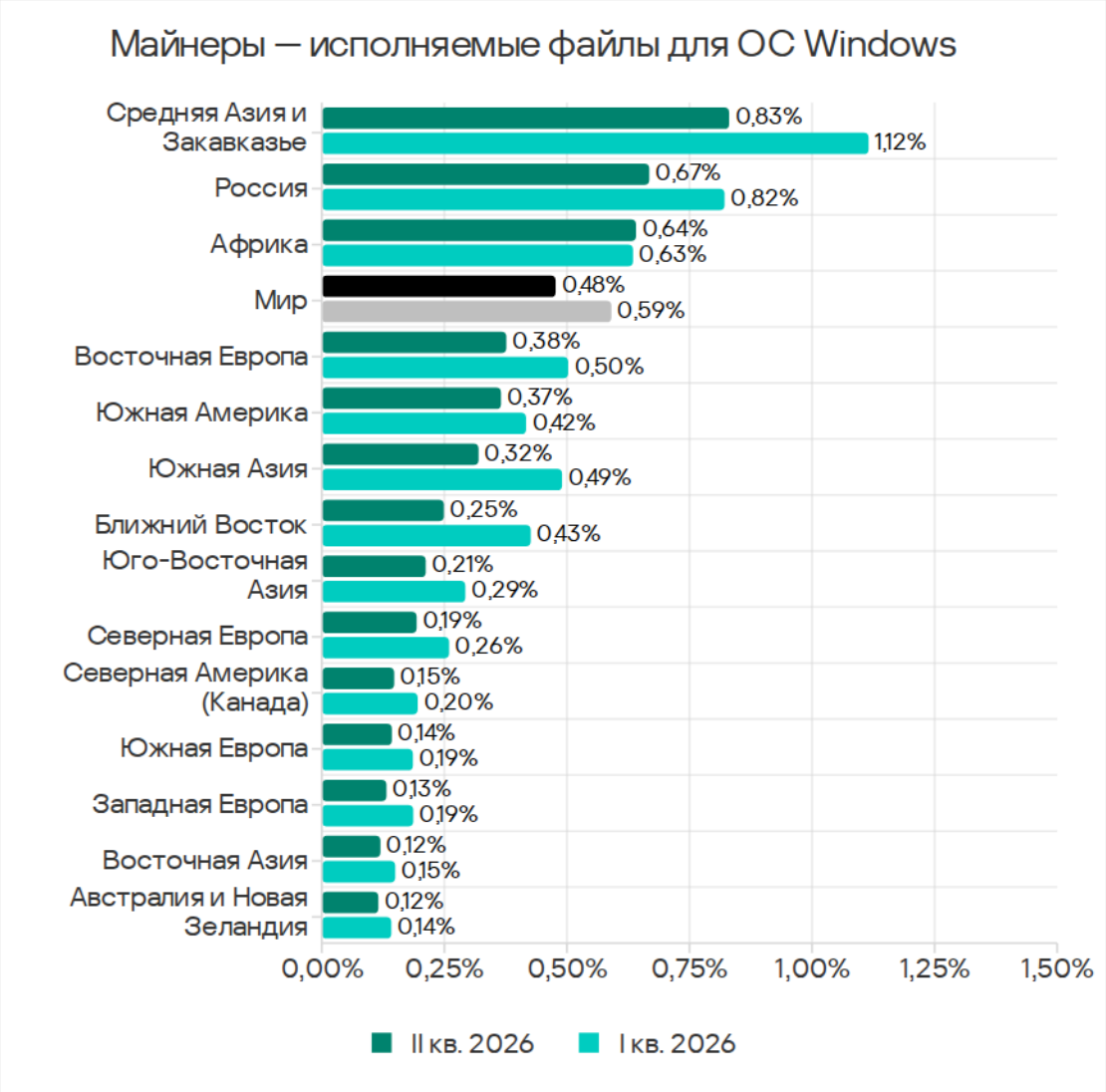


В июне 2026 года месячный показатель был наименьшим за три года.

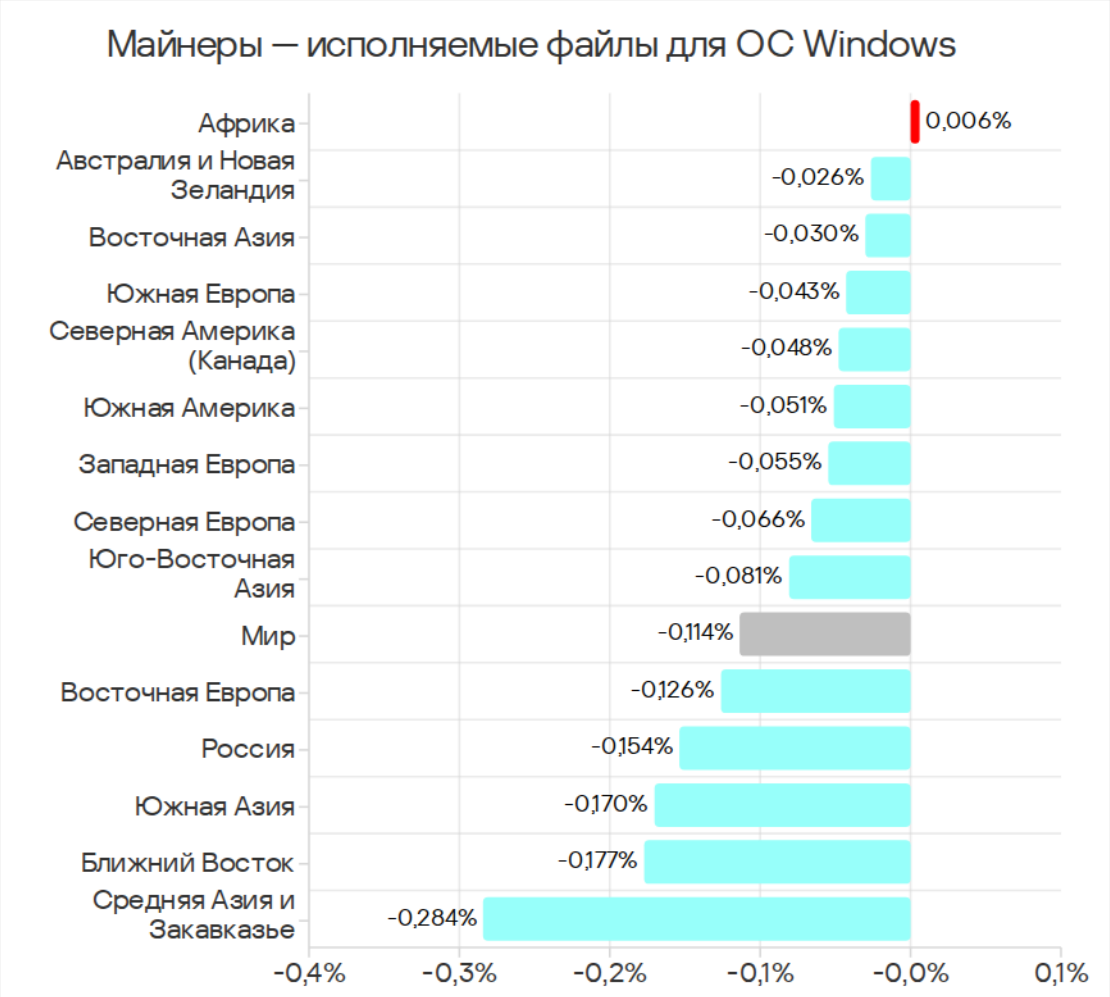


Доля компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows, июль 2024 года – июнь 2026 года

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, II квартал 2026 года



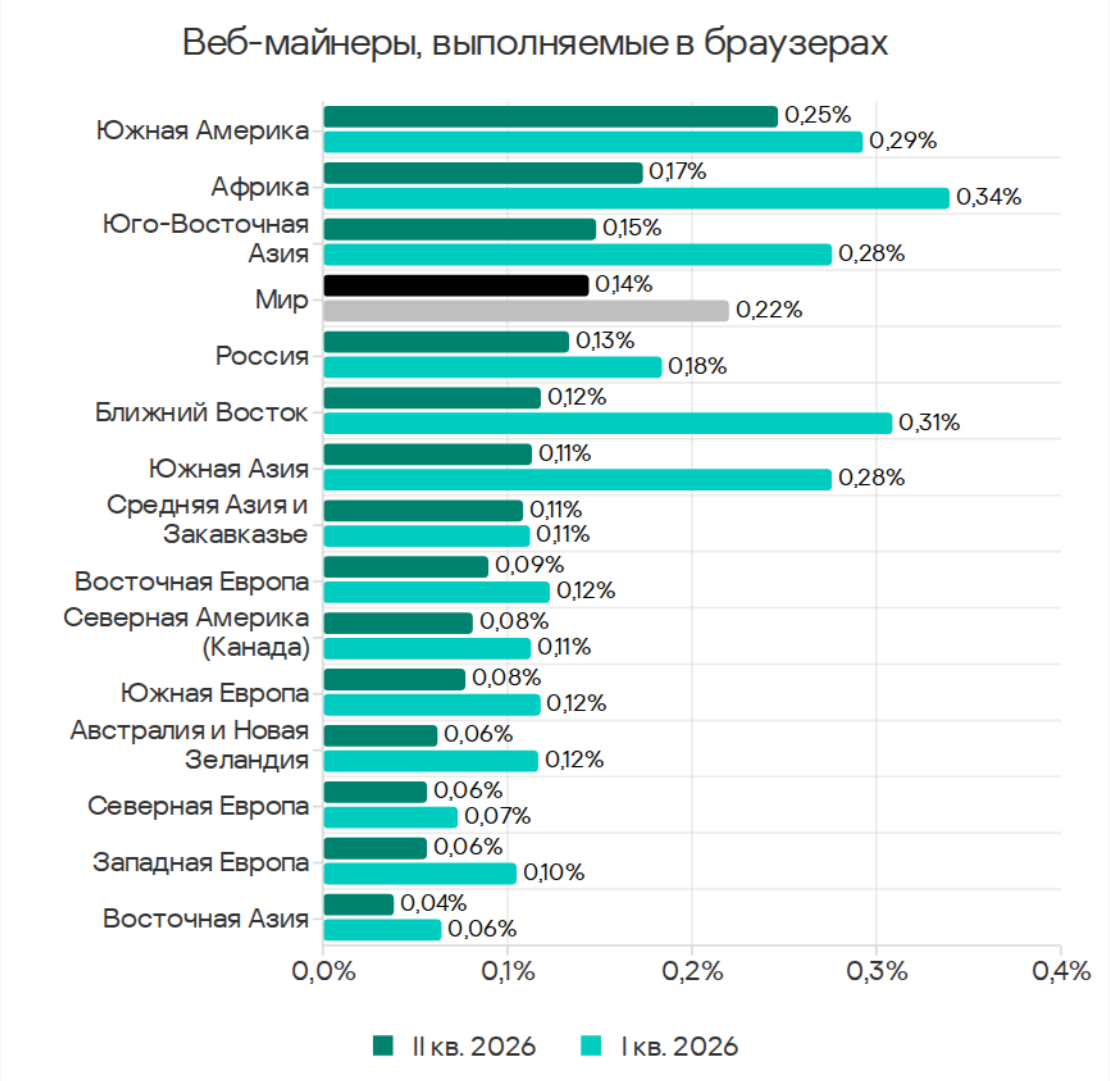
Веб-майнеры

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

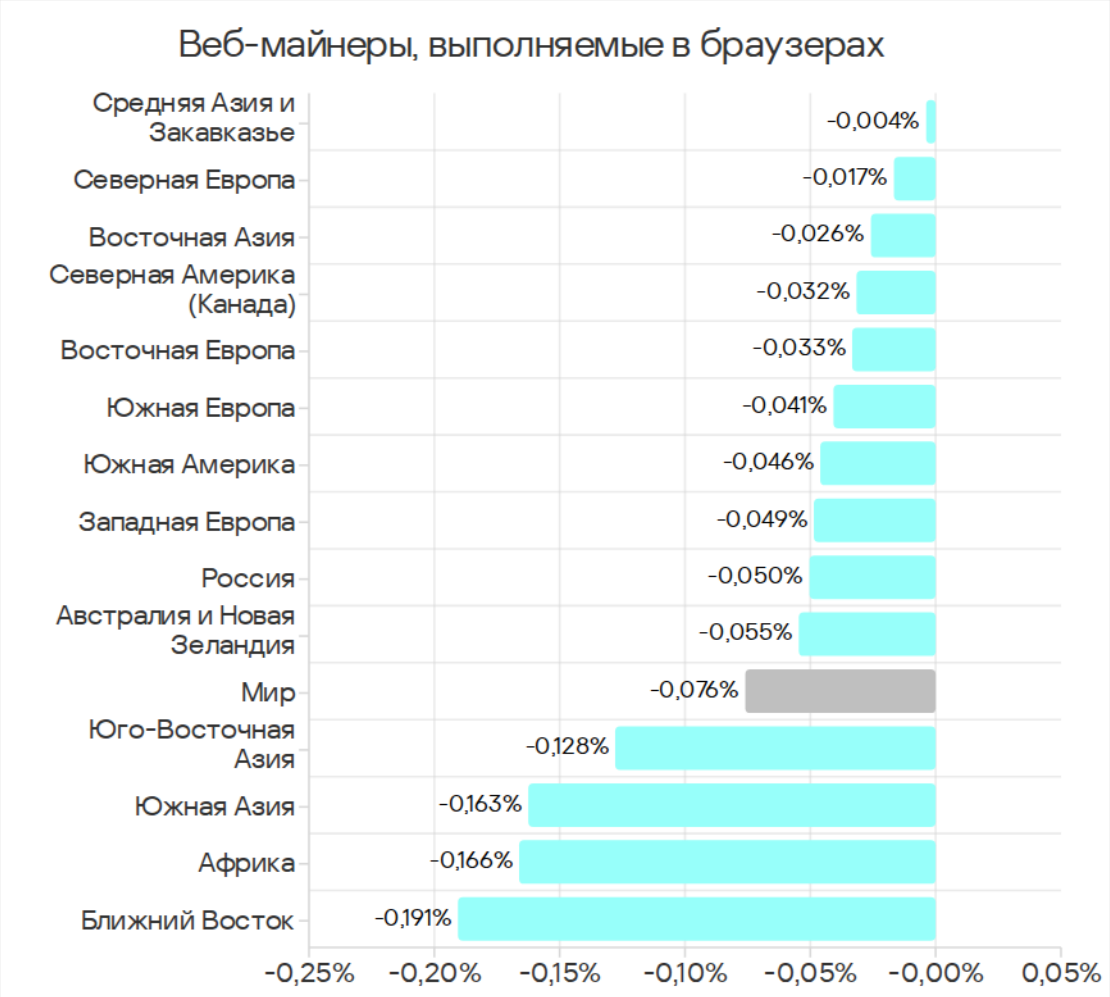
В июне 2026 года месячный показатель веб-майнеров, как и у майнеров в формате исполняемых файлов, был наименьшим за три года.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, июль 2024 года – июнь 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, II 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.

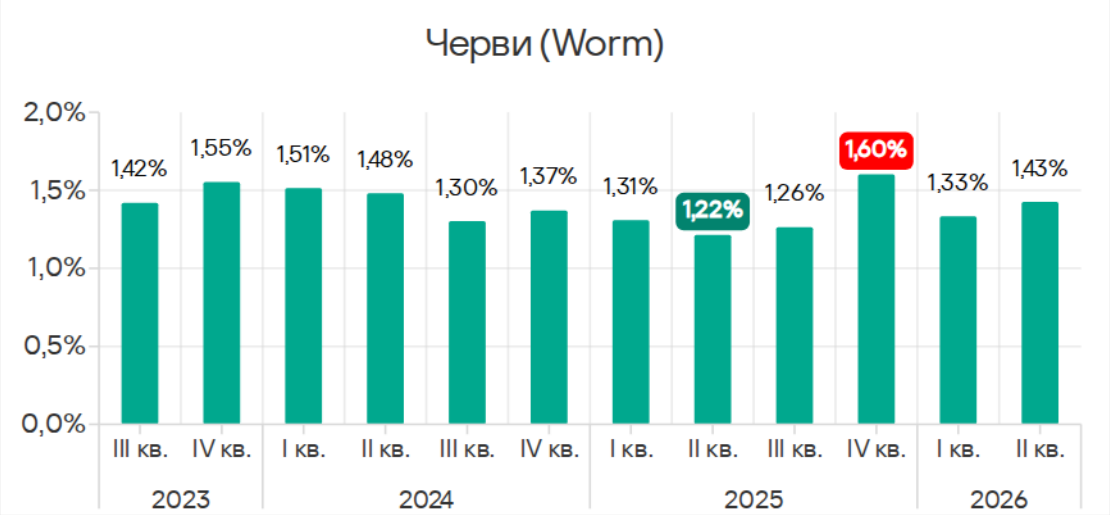
Современные версии червей встречаются в сетях АСУ не часто, но наносимый в случае заражения ущерб всегда значительный – даже простое обслуживание сети, зараженной майнерами-червями, становится кратно дороже из-за большего времени простоя (downtime) и дополнительных человеко-часов, необходимых для восстановления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

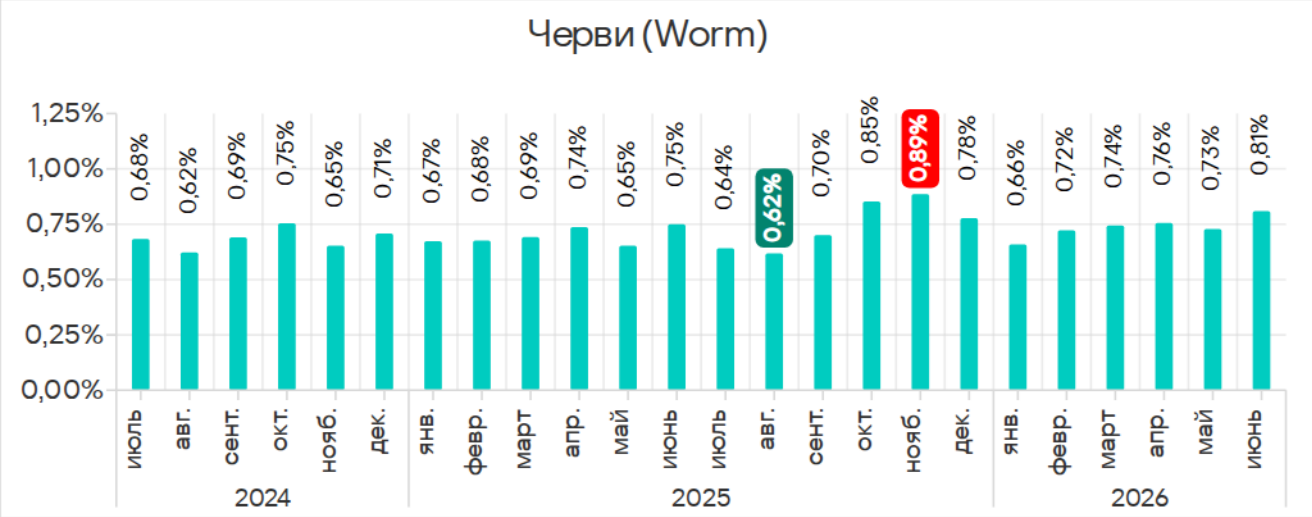
Вместе с тем, среди распространяющихся вирусов и червей довольно много старых модификаций, их командные серверы уже отключены. Тем не менее, они не только ослабляют безопасность зараженных систем – например, открывая сетевые порты и изменяя конфигурацию, но также могут приводить к сбоям в работе ПО,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

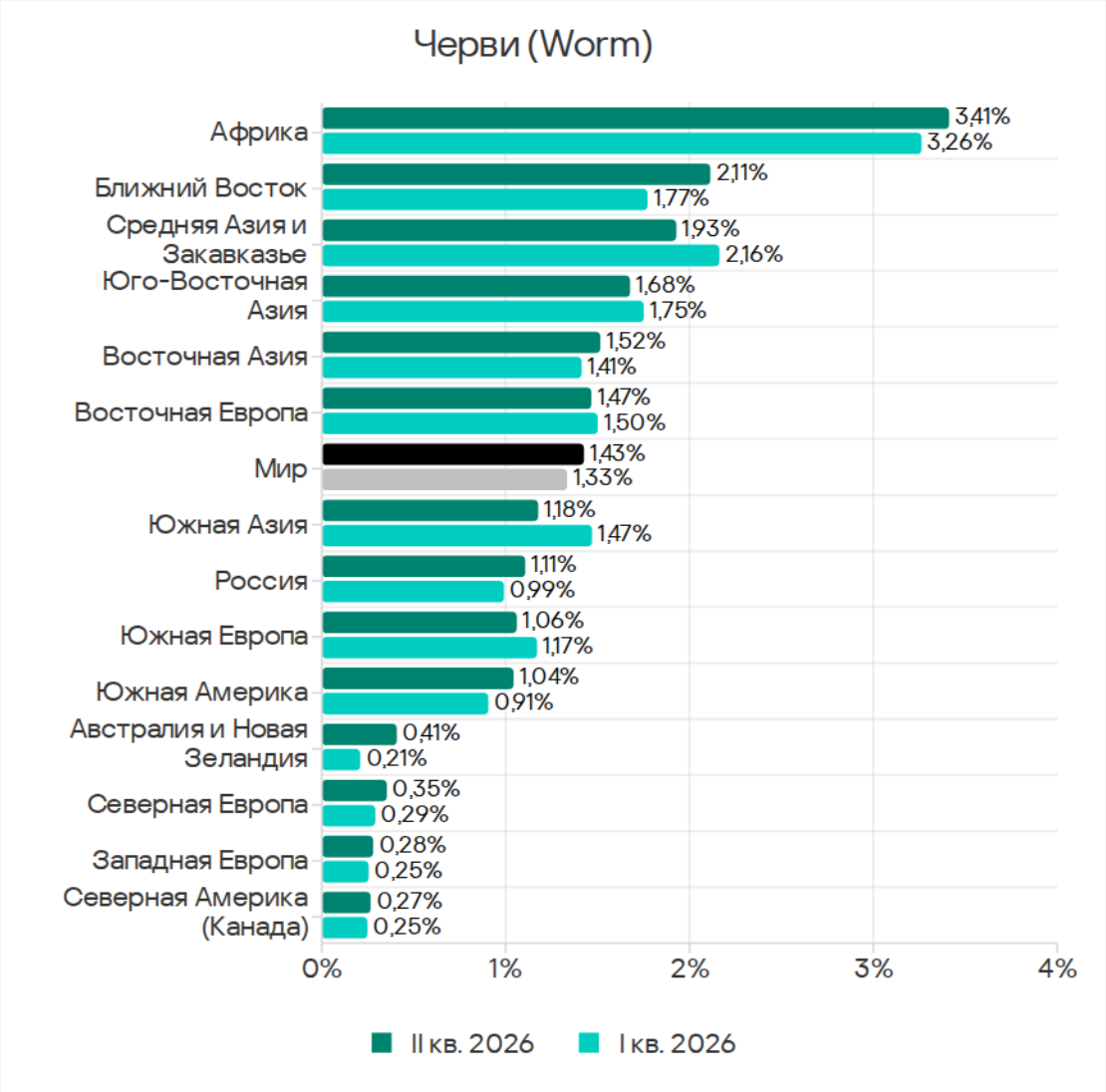
Доля компьютеров АСУ, на которых были заблокированы черви, III квартал 2023 года – II квартал 2026 года



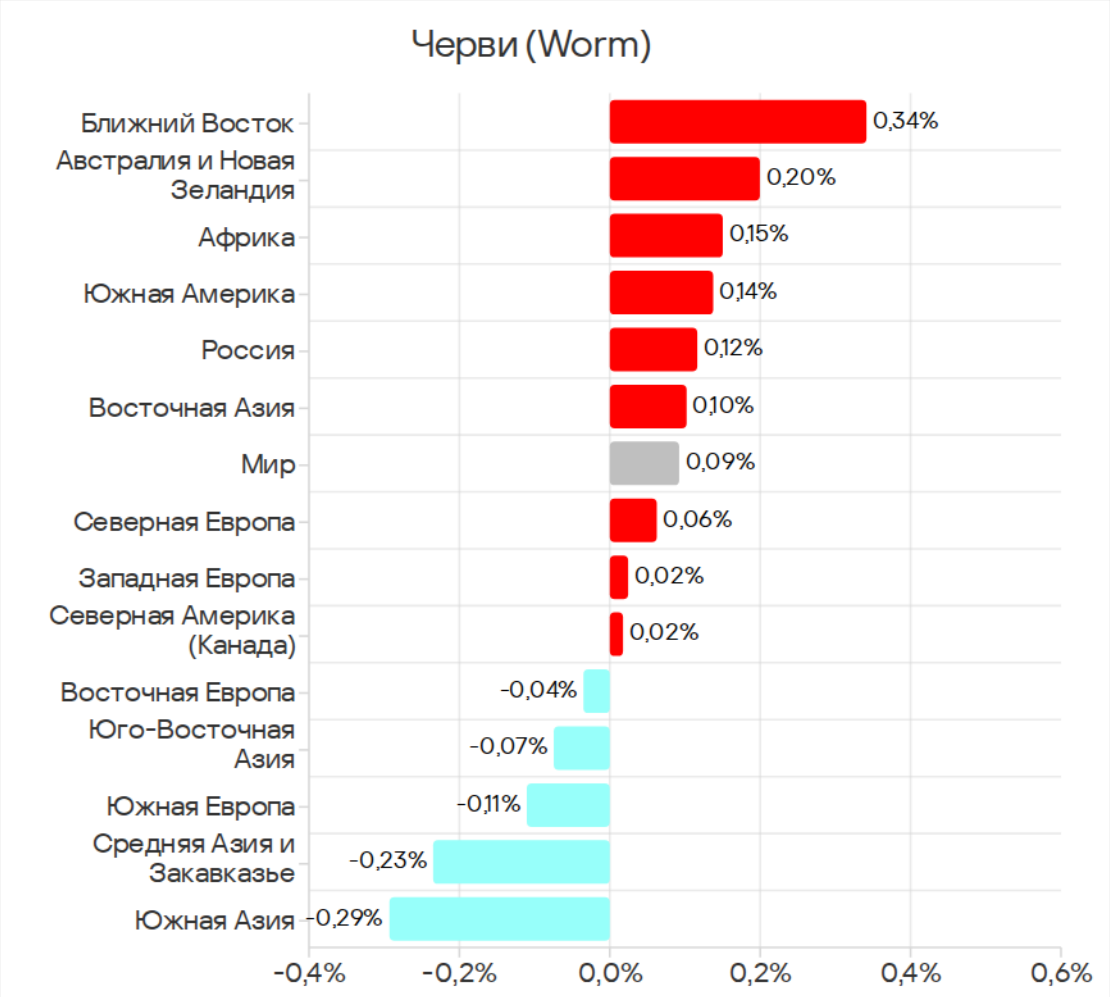


Доля компьютеров АСУ, на которых были заблокированы черви, июль 2024 года – июнь 2026 года

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

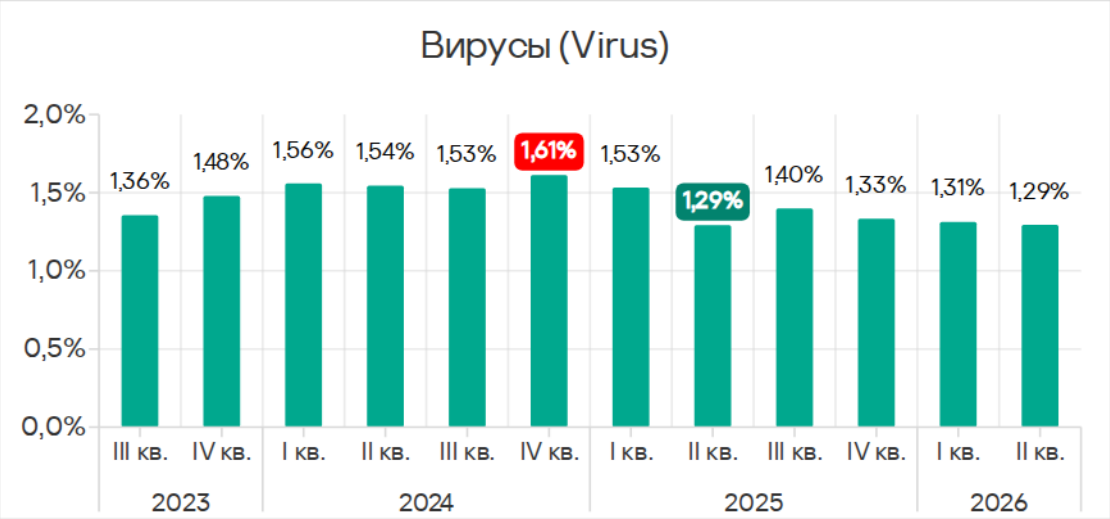


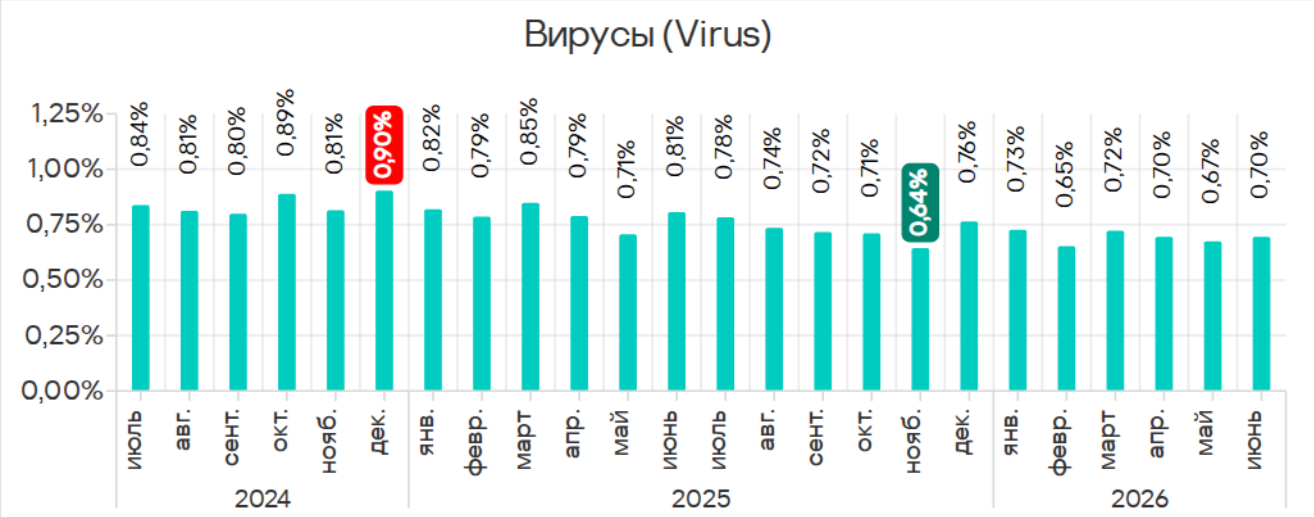
Изменение доли компьютеров АСУ, на которых были заблокированы черви, II квартал 2026 года



Вирусы

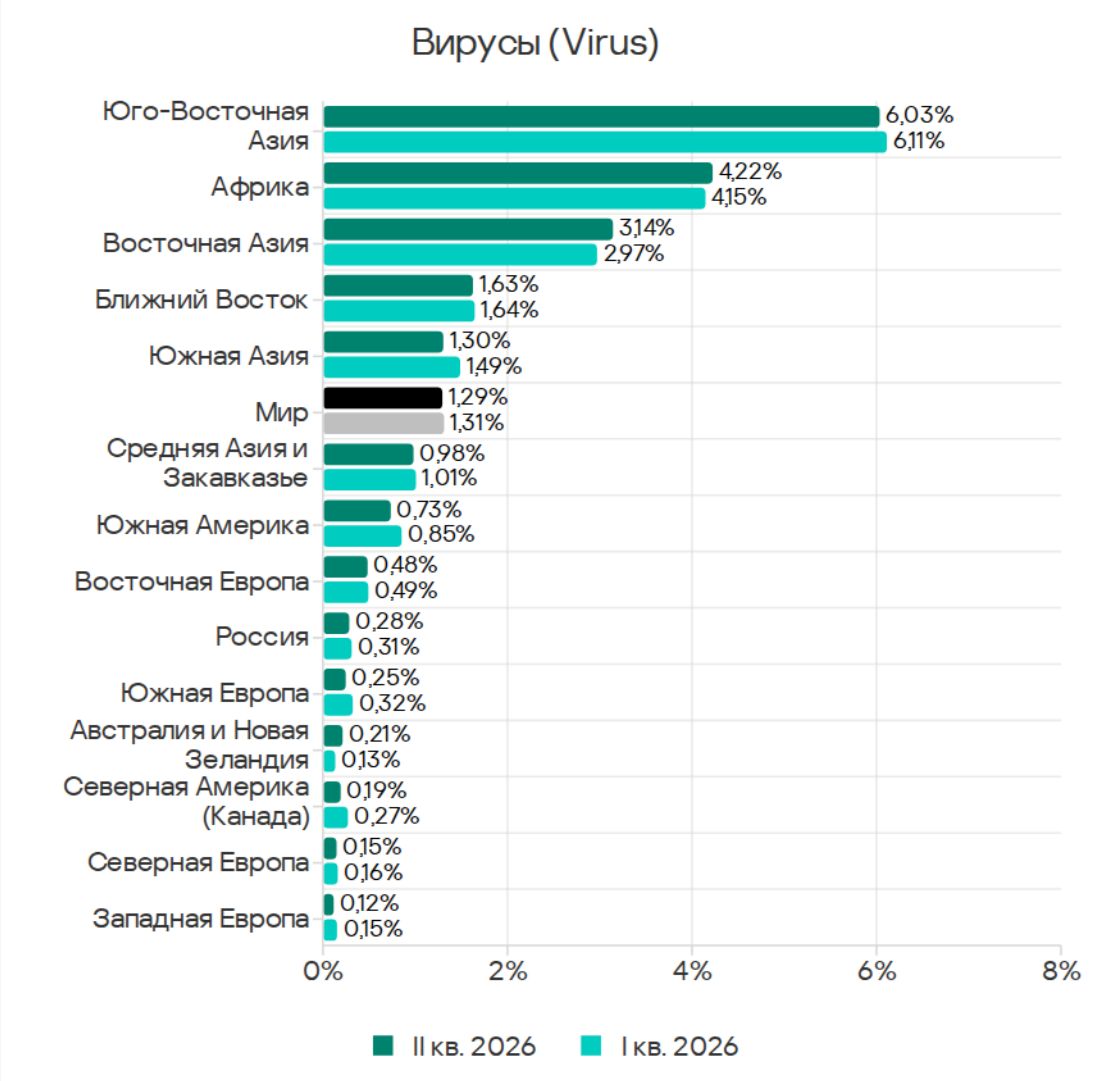
Доля компьютеров АСУ, на которых были заблокированы вирусы, III квартал 2023 года – II квартал 2026 года



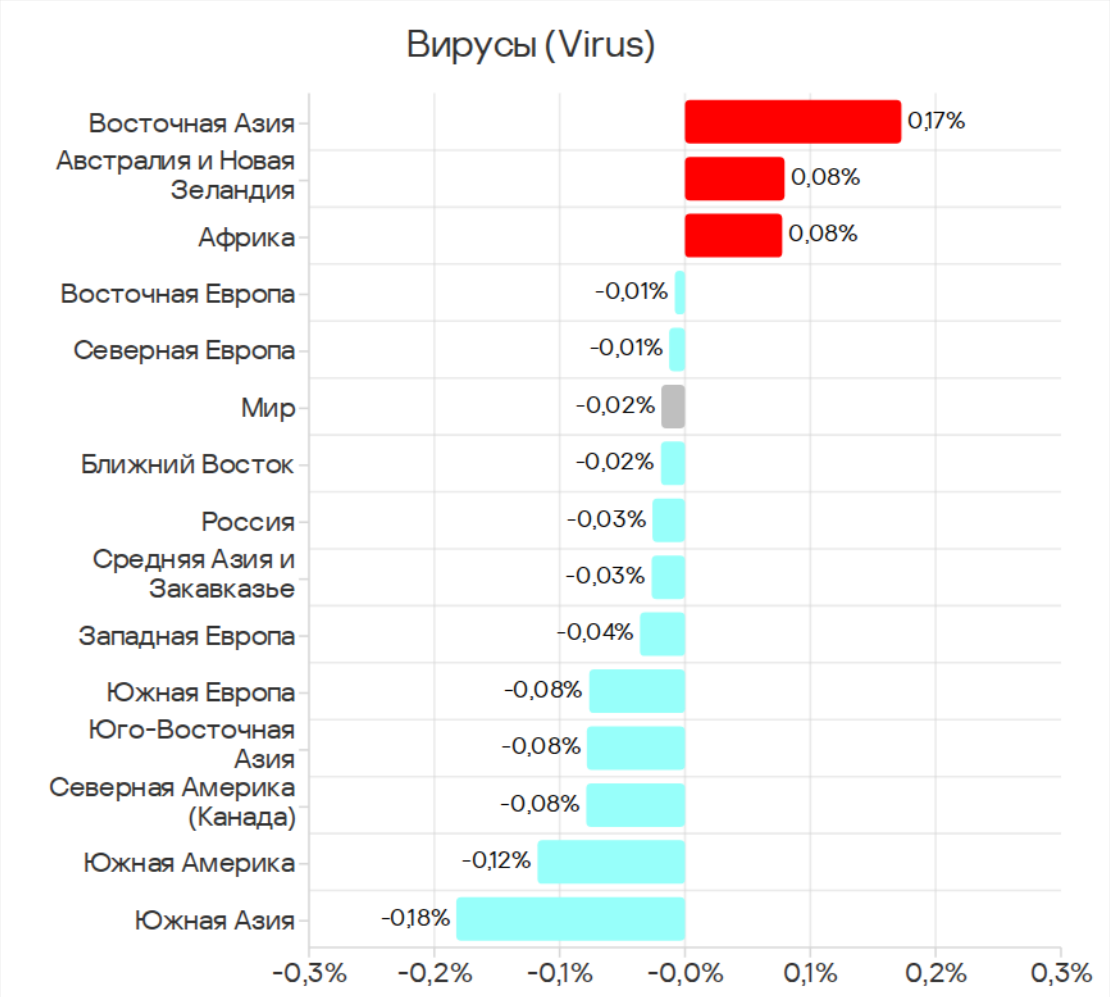


Доля компьютеров АСУ, на которых были заблокированы вирусы, июль 2024 года – июнь 2026 года

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



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

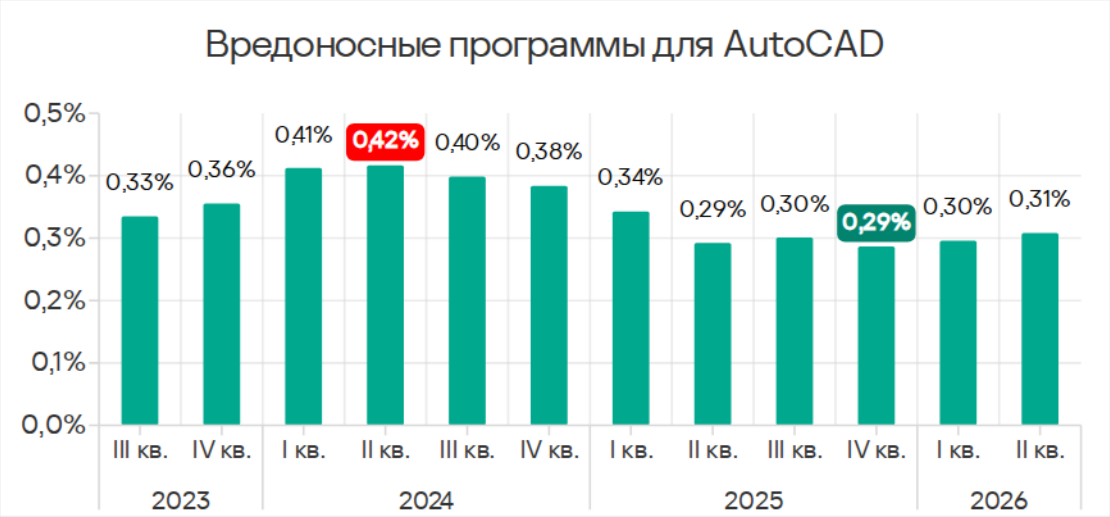


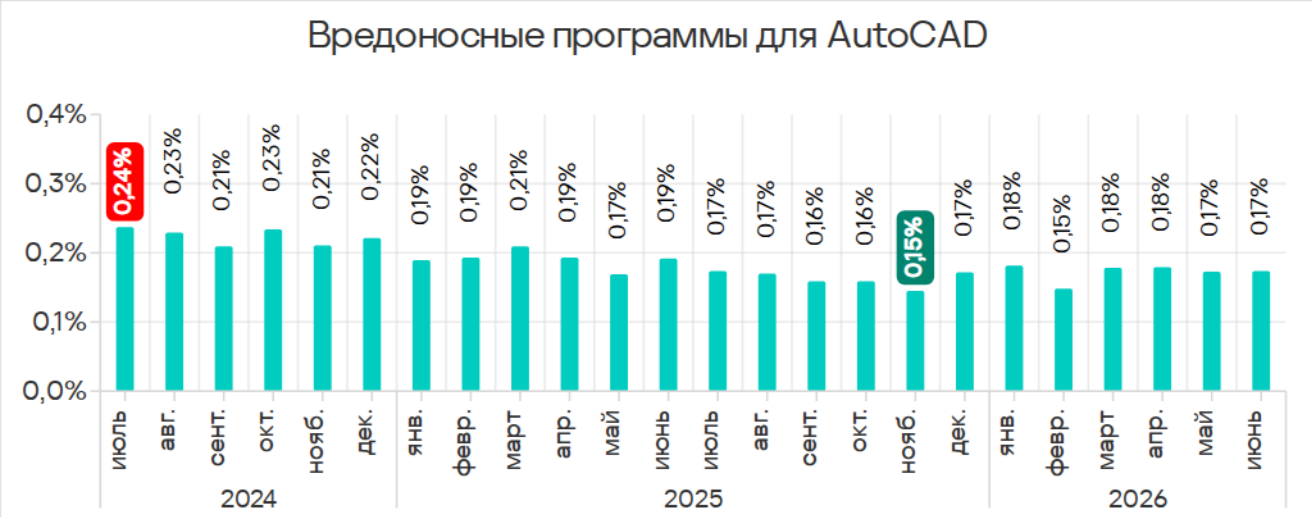
Вредоносные программы для AutoCAD

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.

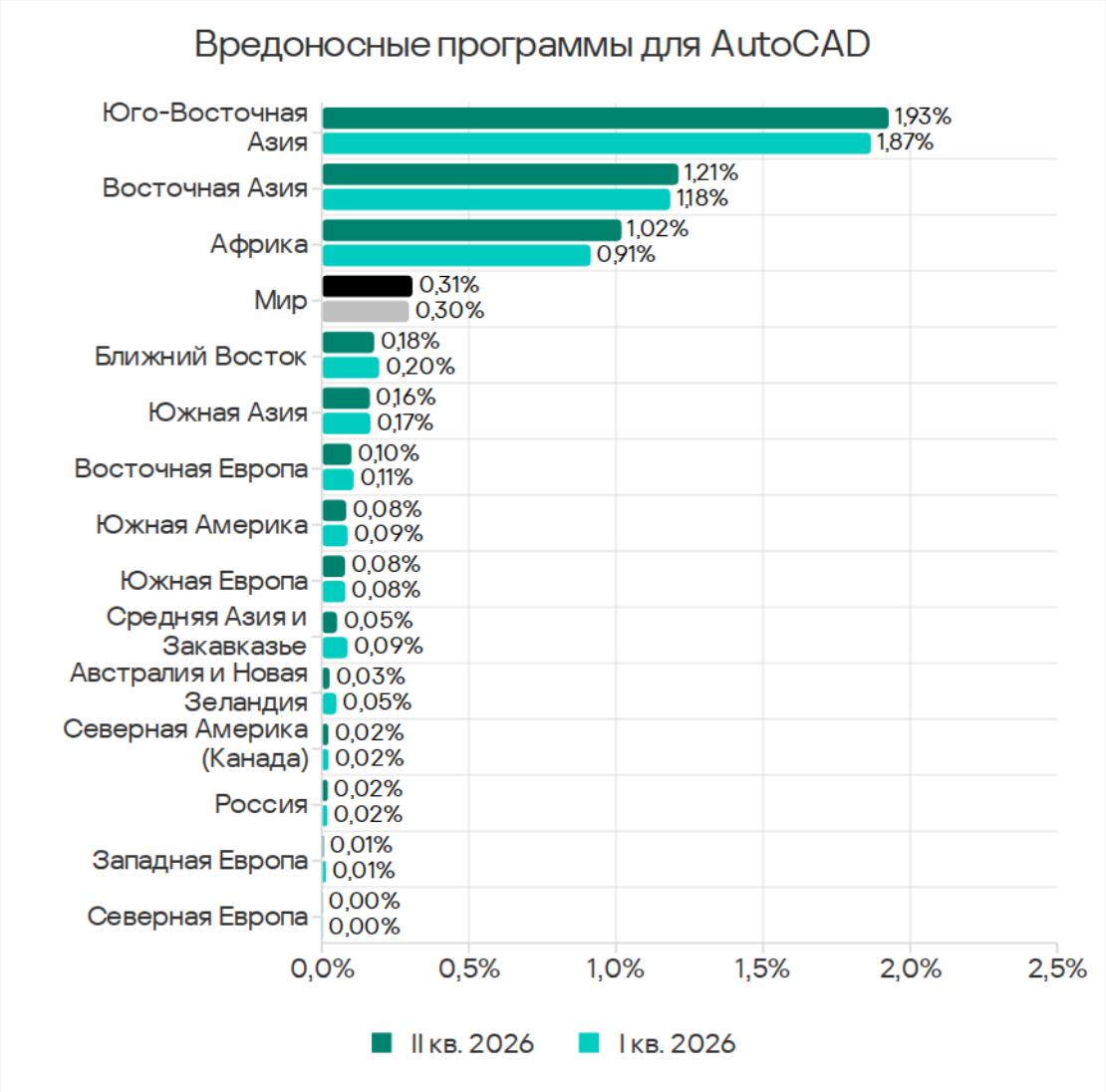
Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, III квартал 2023 года – II квартал 2026 года



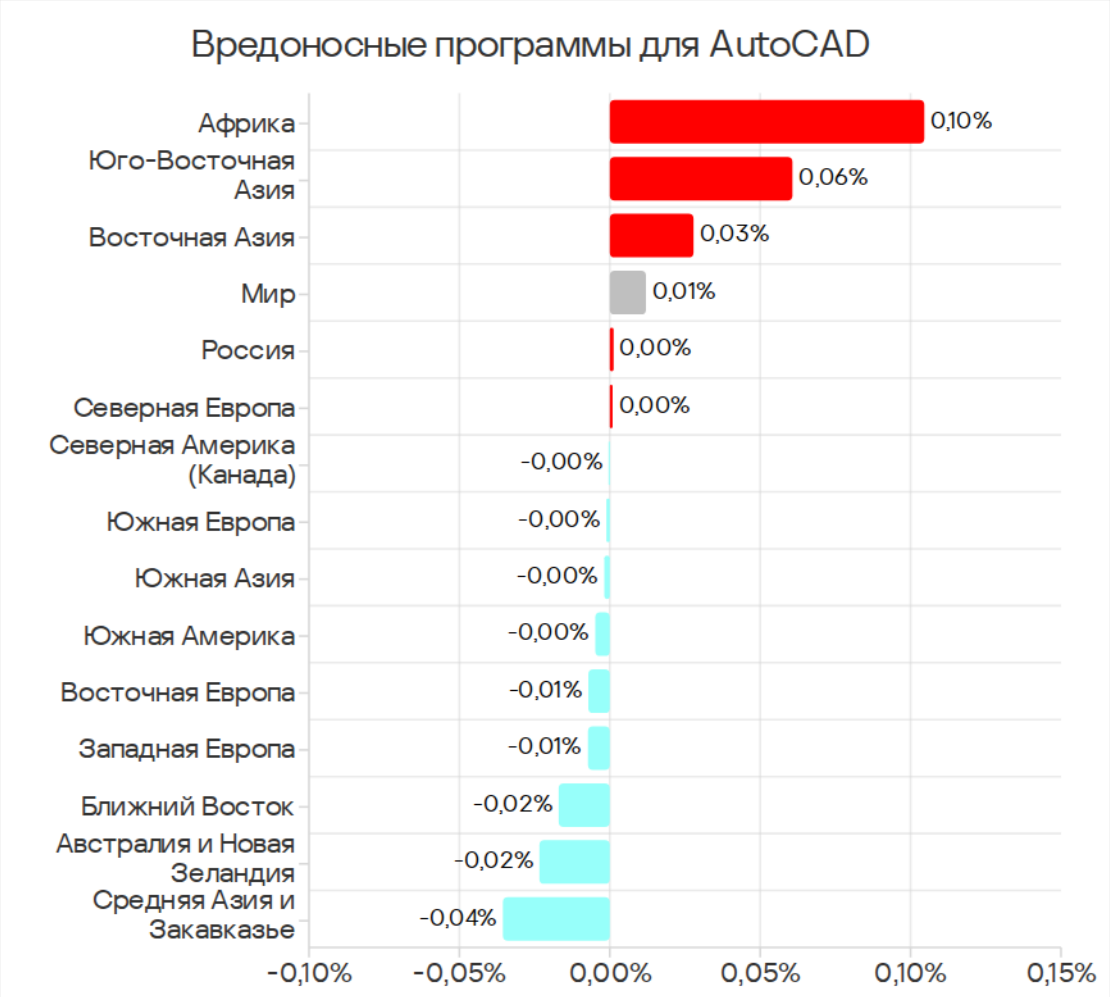


Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, июль 2024 года – июнь 2026 года

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, II квартал 2026 года

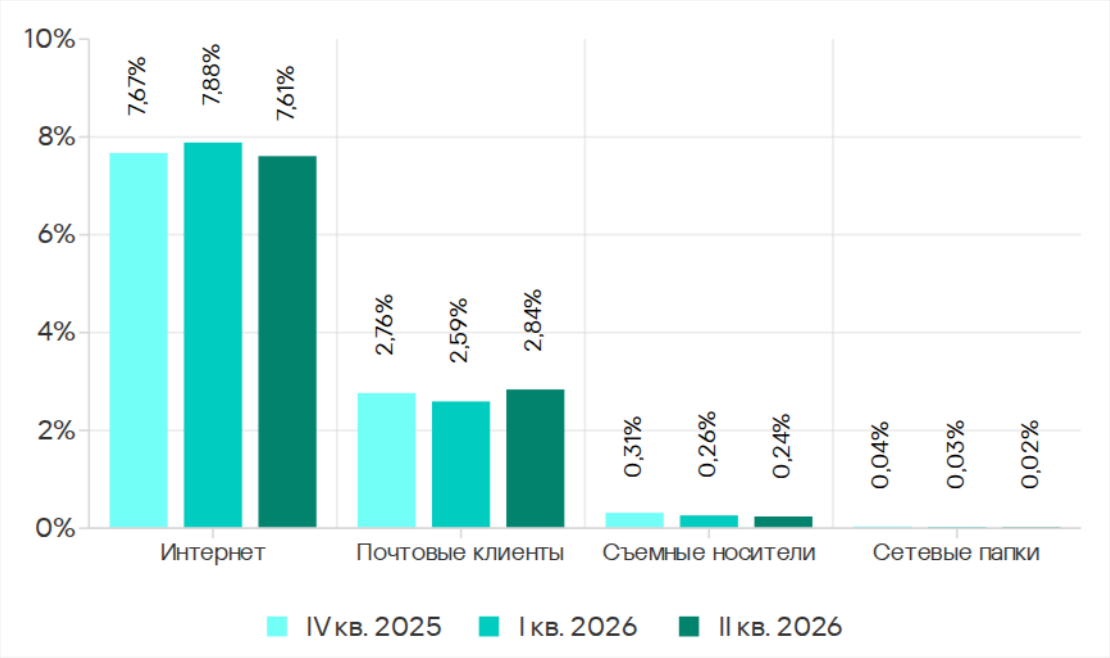


Основные источники угроз

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

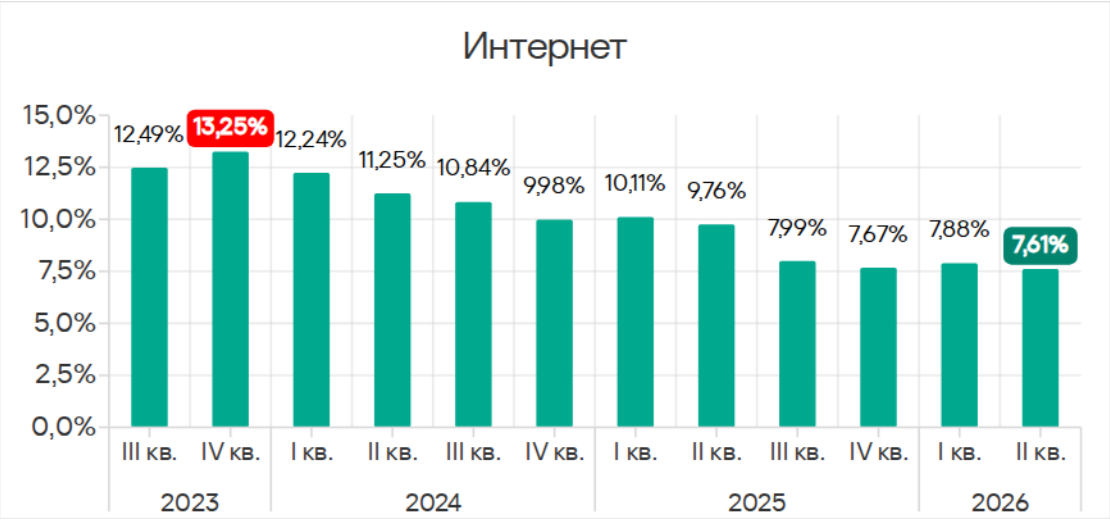


Во втором квартале 2026 года из всех источников угроз показатель вырос только у почтовых клиентов.

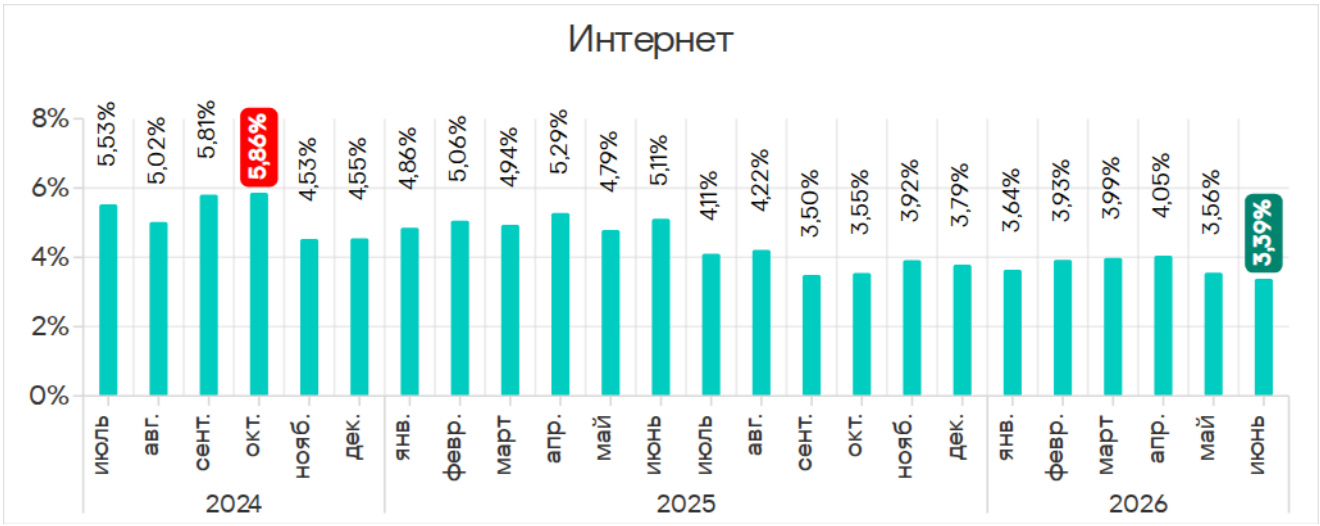
Интернет

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, III квартал 2023 года – II квартал 2026 года



Месячный показатель в июне 2026 года оказался наименьшим за три года.



Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, июль 2024 года – июнь 2026 года

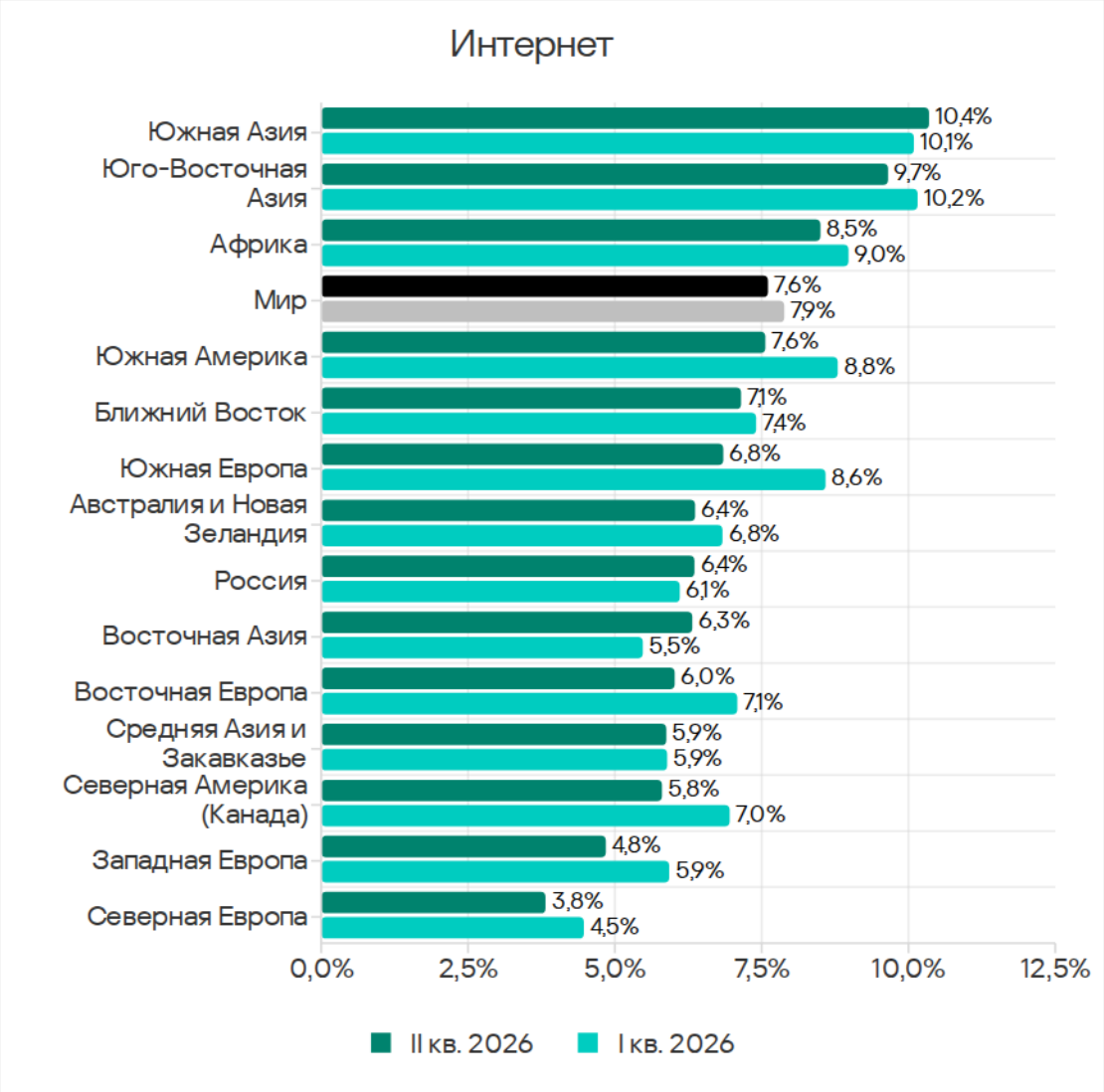
Основные категории угроз из интернета*, которые были заблокированы на компьютерах АСУ во втором квартале 2026 года, – это вредоносные скрипты и фишинговые страницы, а также ресурсы в интернете из списка запрещенных.

Угрозы из интернета и основные категории угроз из интернета, III квартал 2024 года – II квартал 2026 года

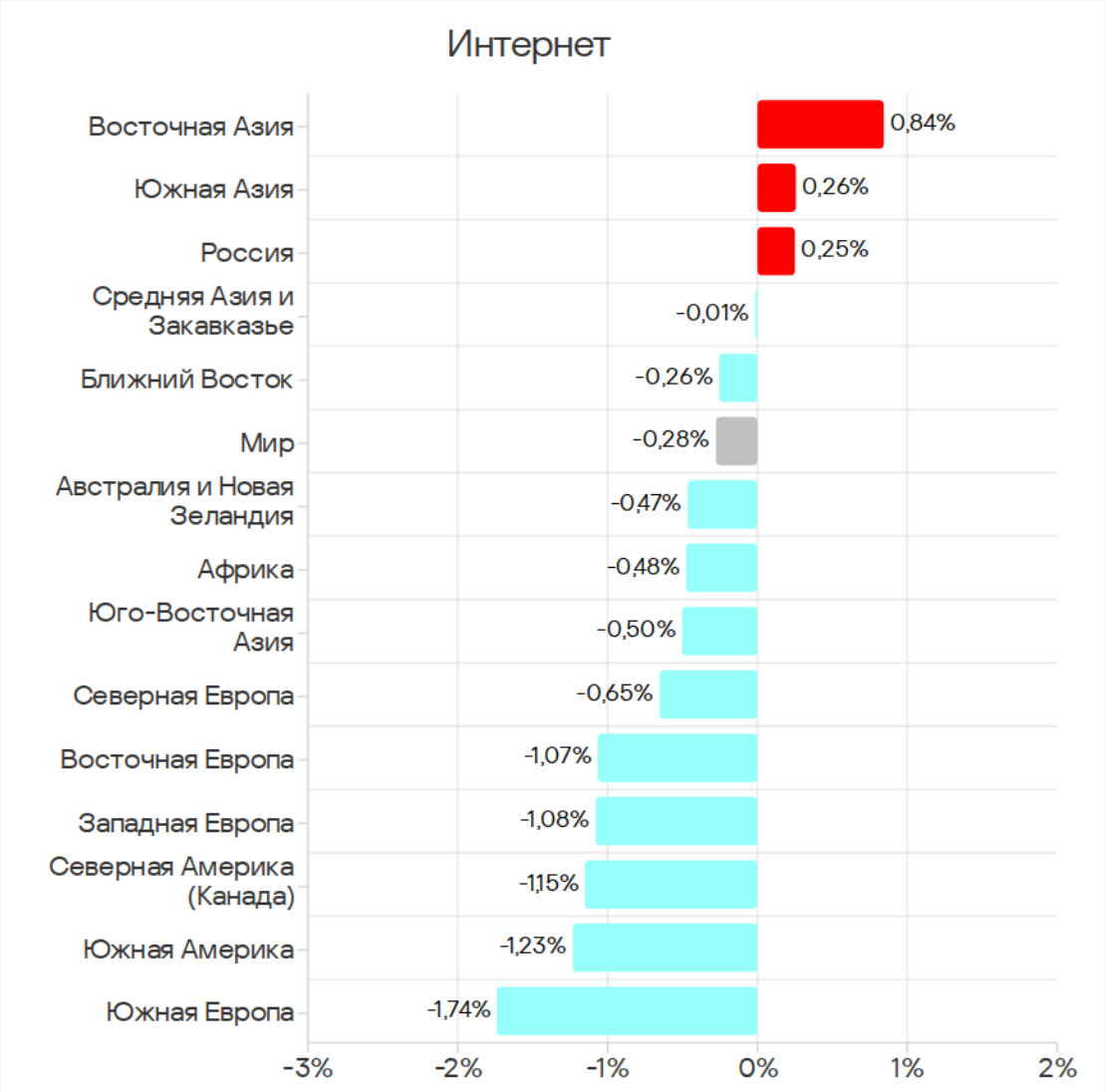
*Напомним, что один и тот же компьютер в течение квартала может быть атакован несколькими категориями вредоносного ПО, которое распространяется из одного источника. Такой компьютер будет учтен при подсчете процента атакованных компьютеров для каждой категории угроз, но для источника угрозы будет учитываться 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, II квартал 2026 года



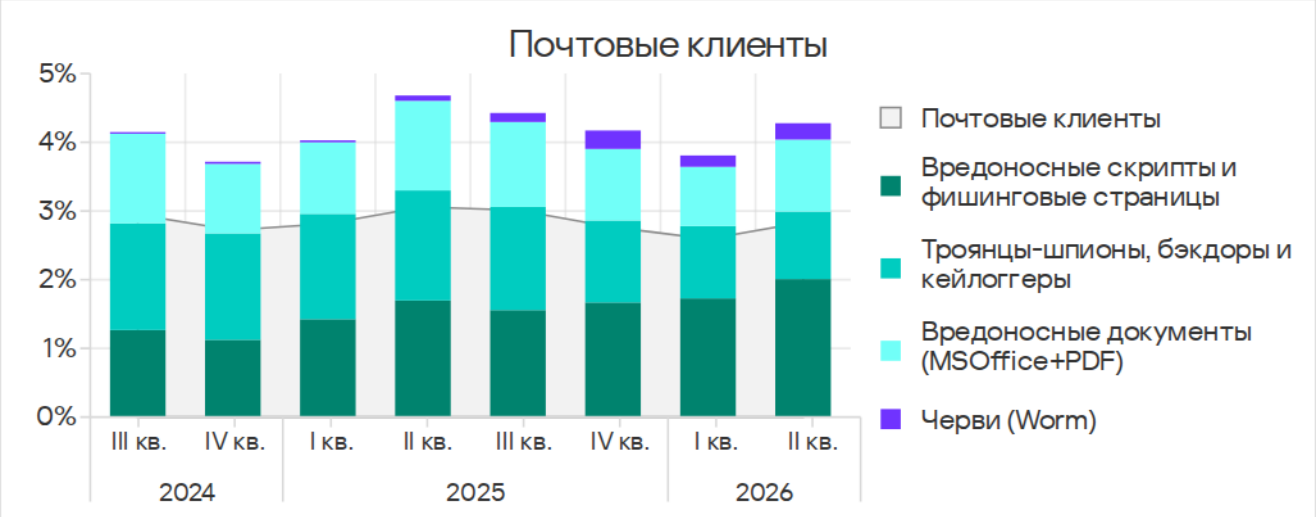
Почтовые клиенты

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, III квартал 2023 года – II квартал 2026 года

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, июль 2024 года – июнь 2026 года

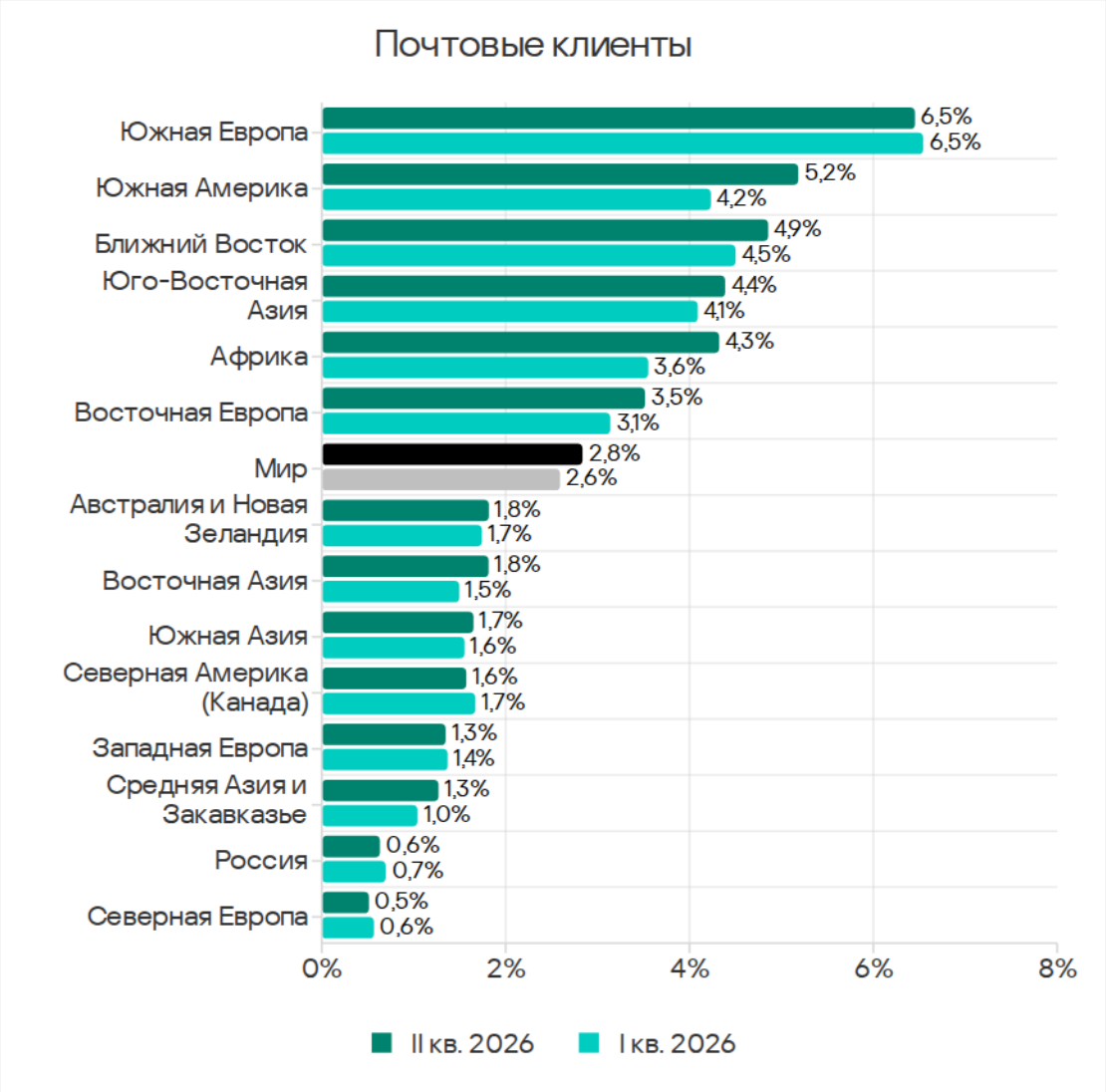
Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ во втором квартале 2026 года: вредоносные скрипты и фишинговые страницы, шпионское ПО, а также вредоносные документы. Доля компьютеров, на которых были заблокированы черви из почтовых клиентов, вновь подросла.



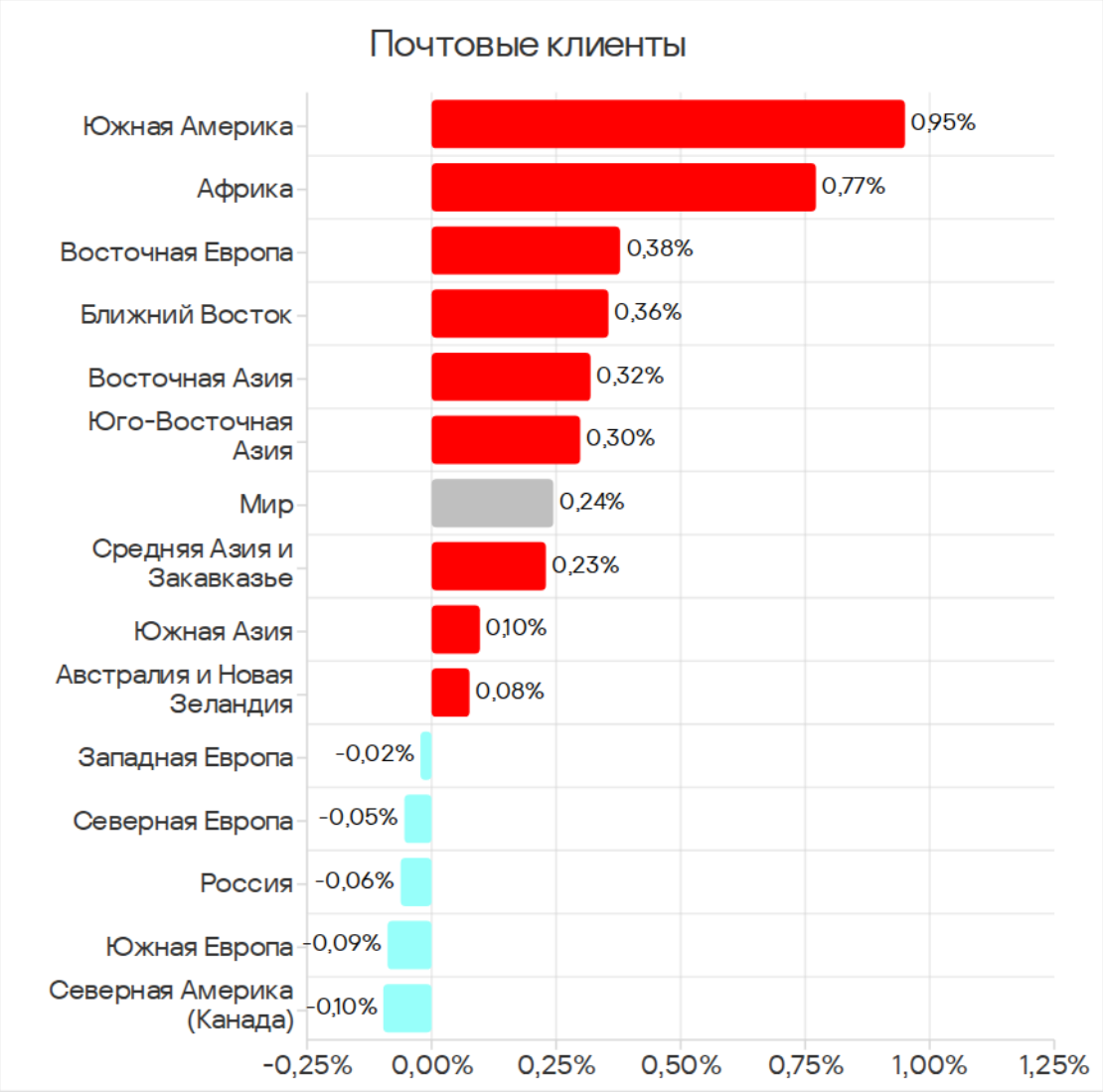
Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов, III квартал 2024 года – II квартал 2026 года

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

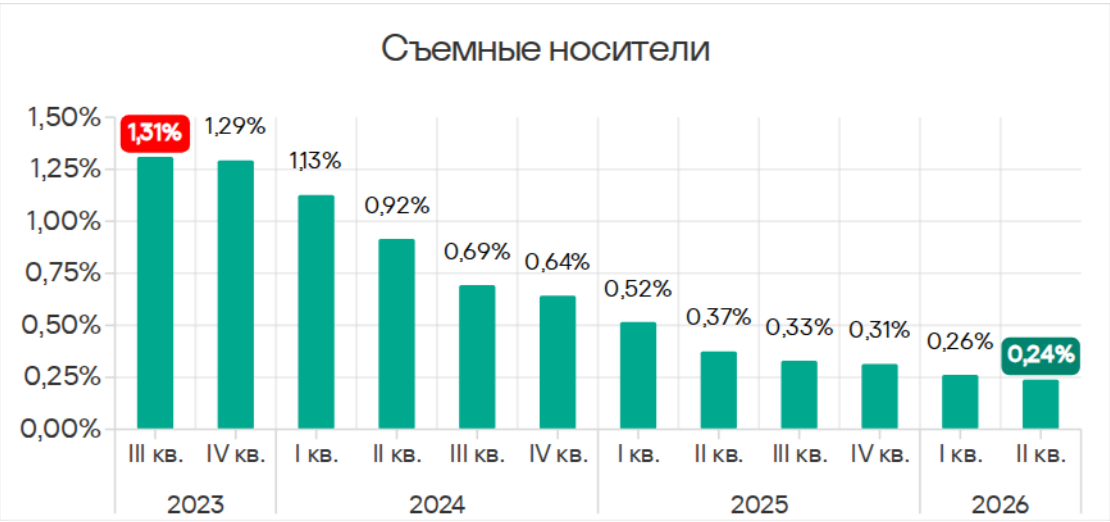


Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, II квартал 2026 года

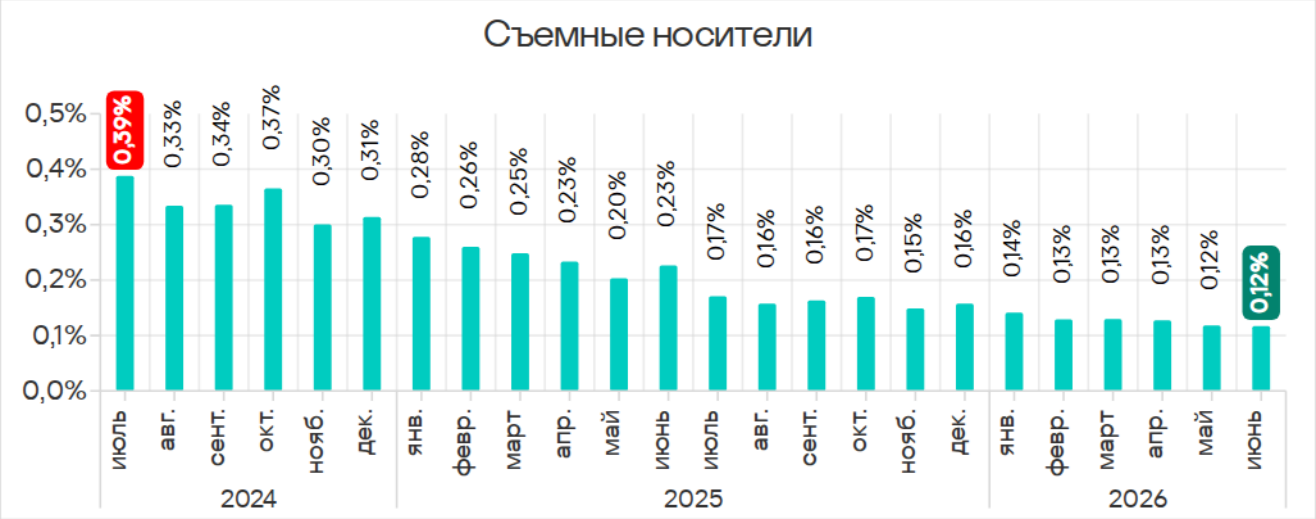


Съемные носители

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

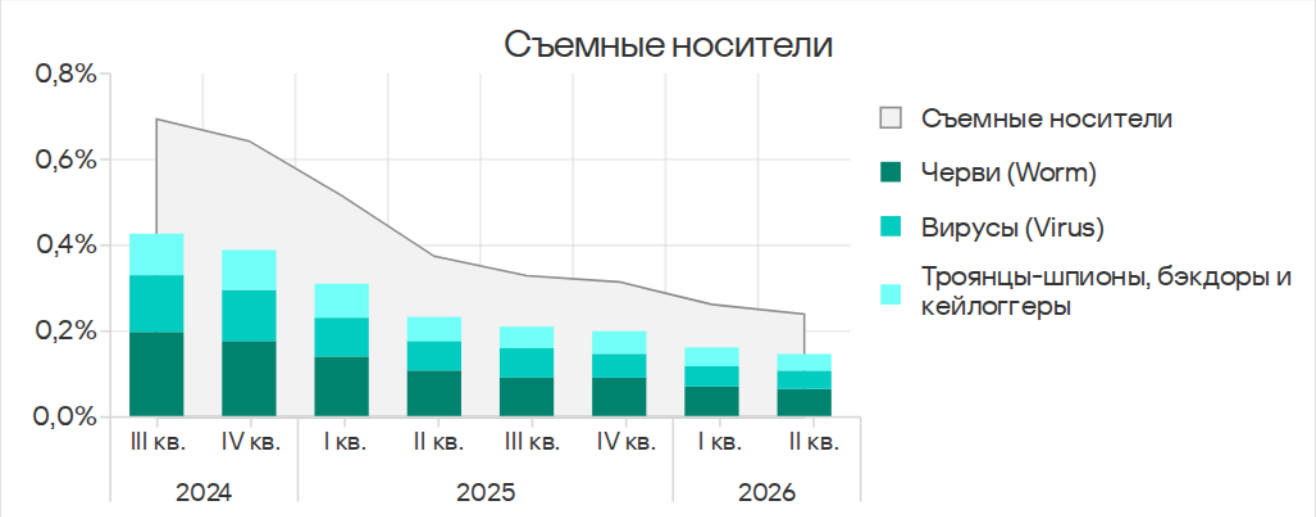


Месячный показатель в июне оказался наименьшим за исследуемый период.



Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, июль 2024 года – июнь 2026 года

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



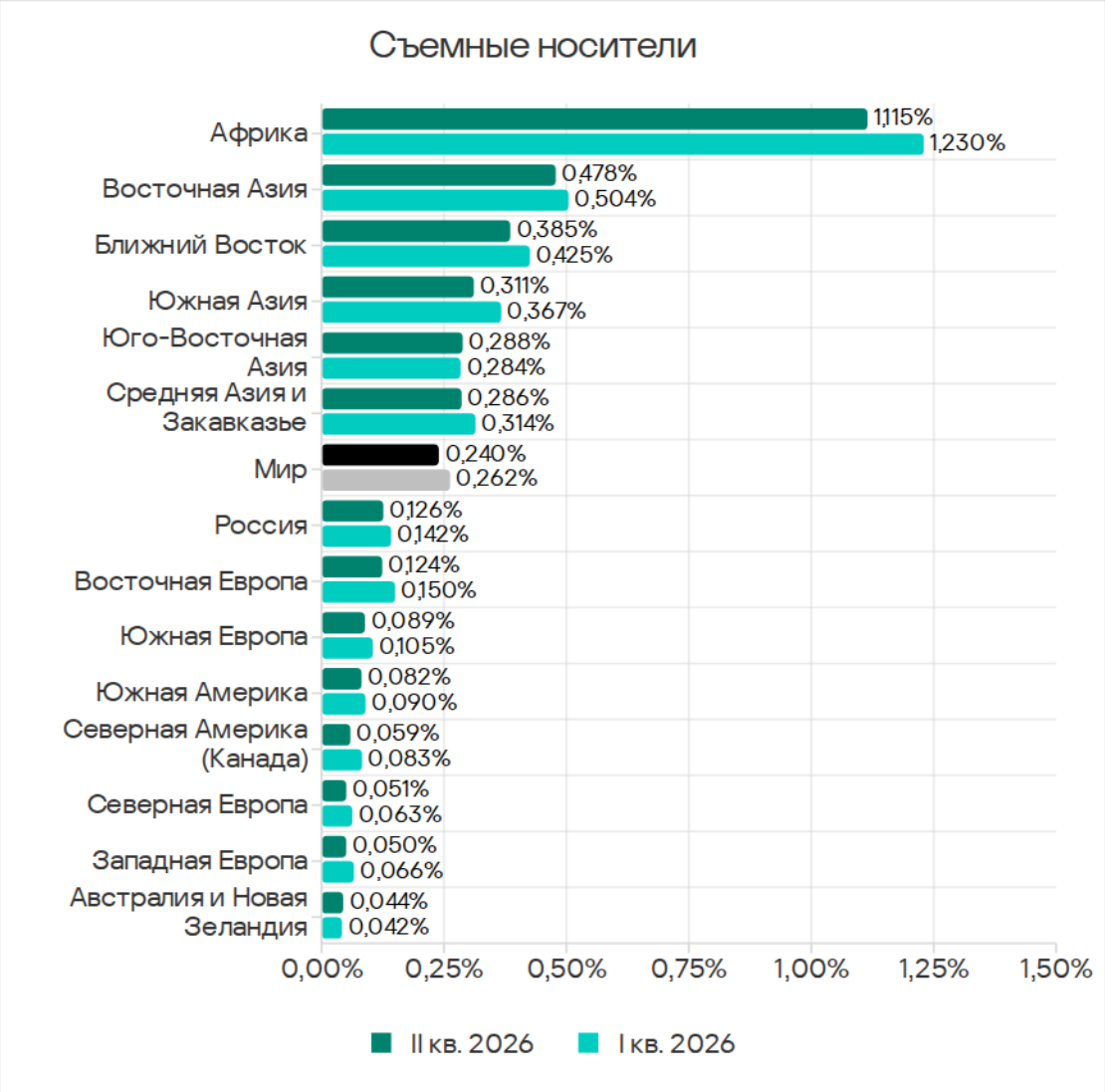
Угрозы на съемных носителях и основные категории угроз на съемных носителях, III квартал 2024 года – II квартал 2026 года

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

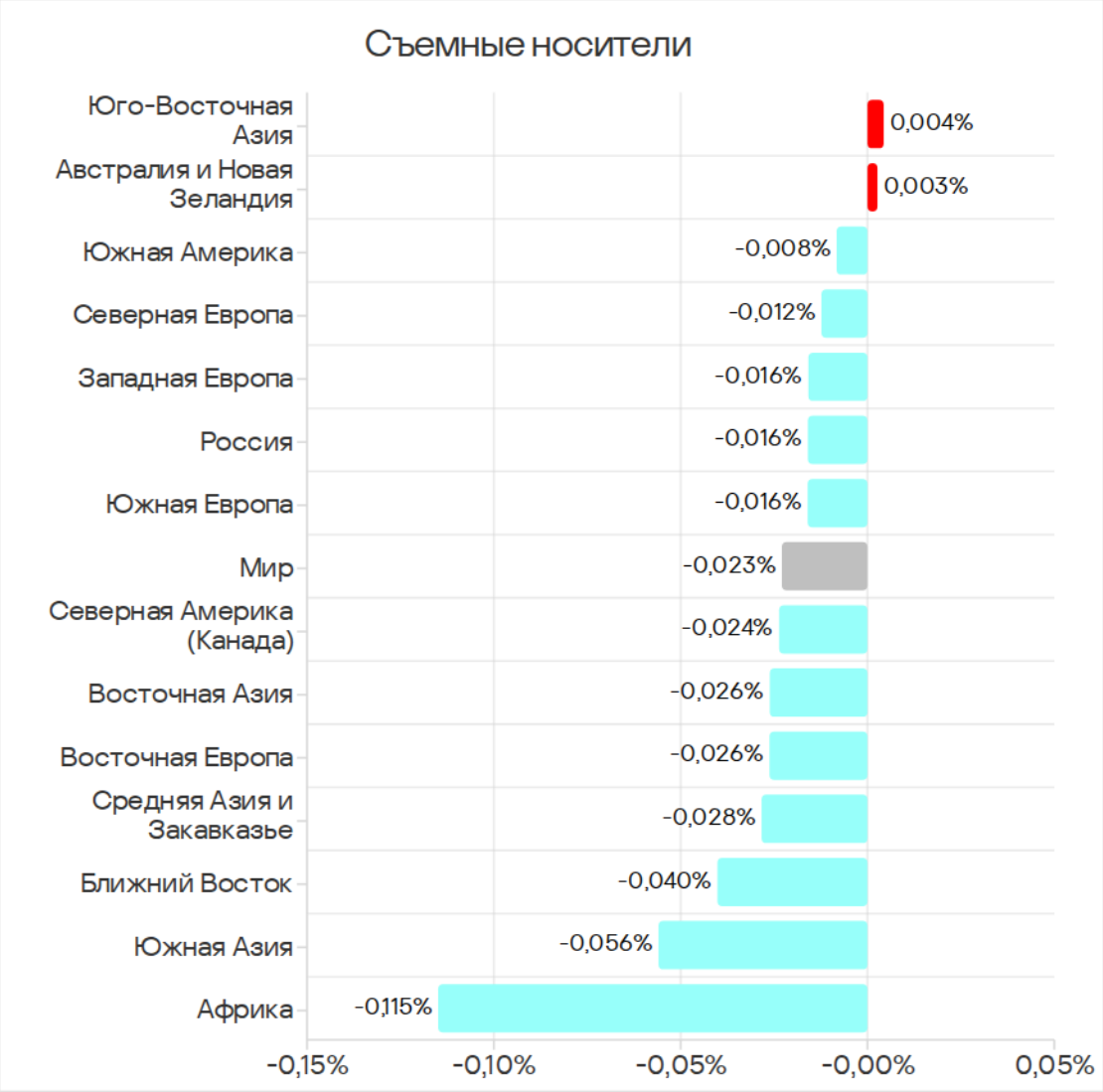
закрытые) и выполняя атаки на сетевые службы методом перебора (брутфорс).

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, II квартал 2026 года

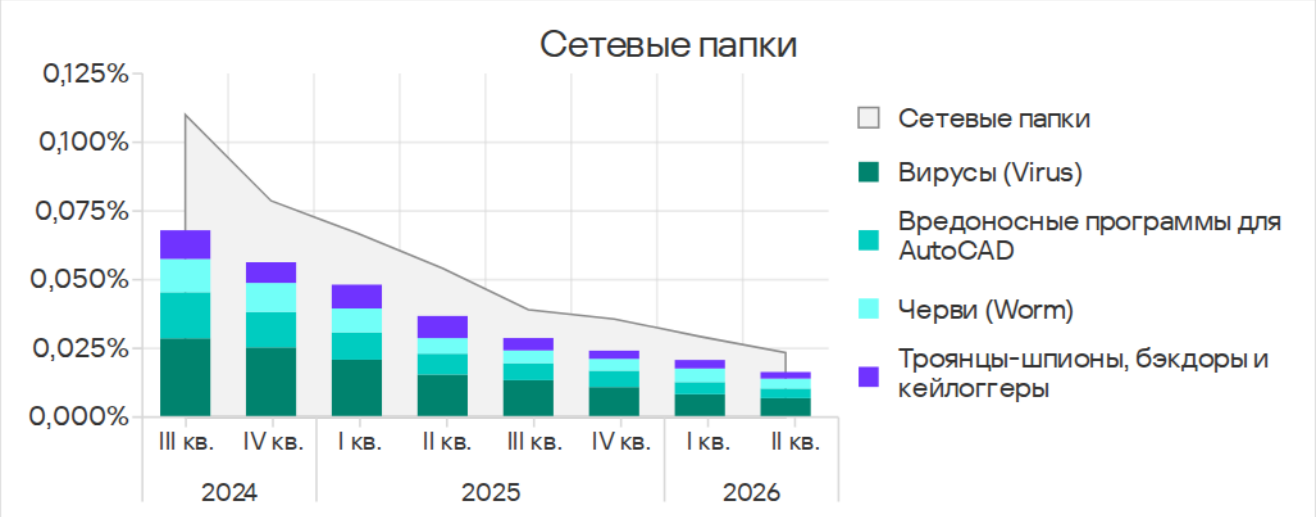


Сетевые папки

Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, III квартал 2023 года – II квартал 2026 года

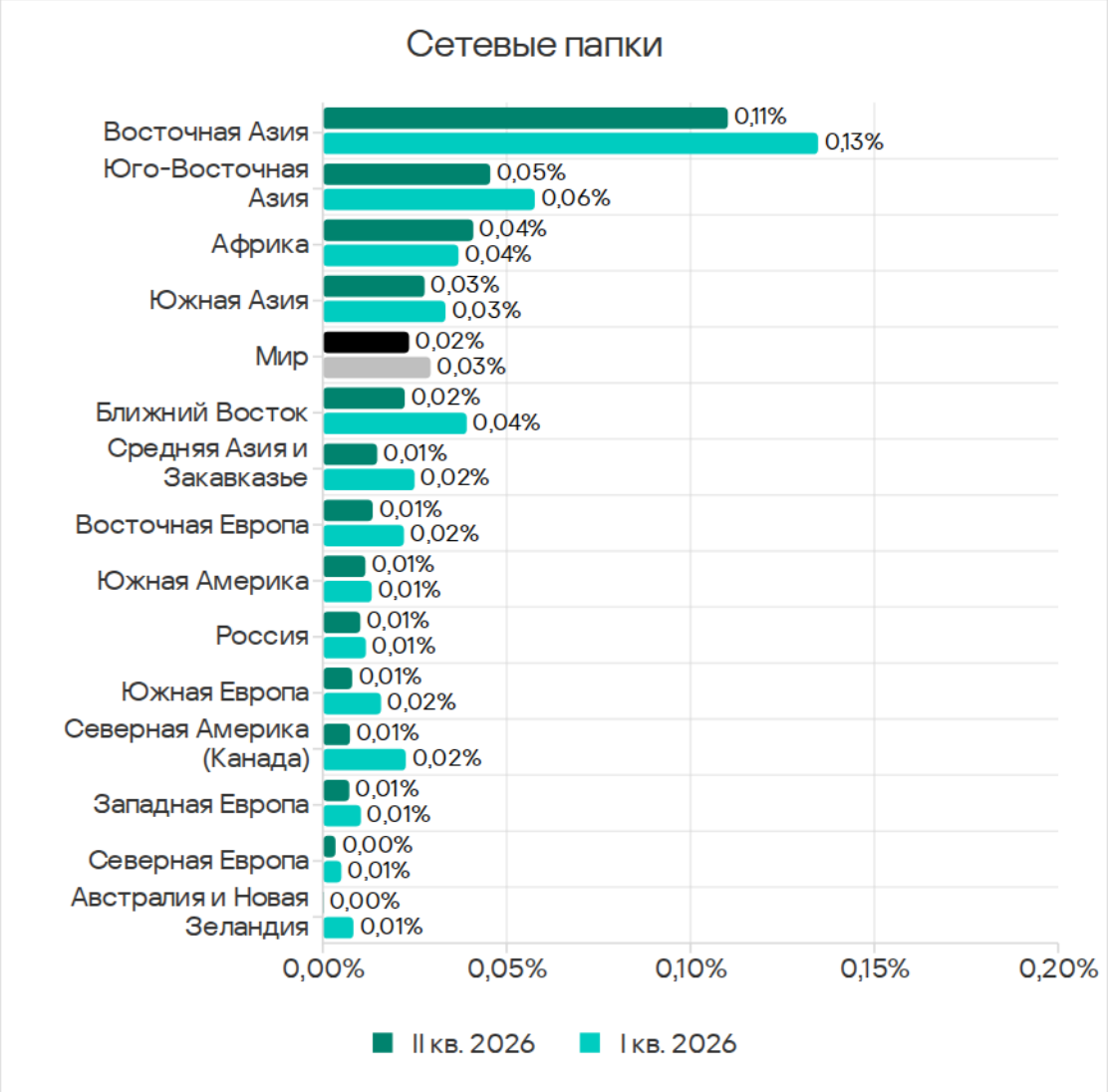
Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, июль 2024 года – июнь 2026 года

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

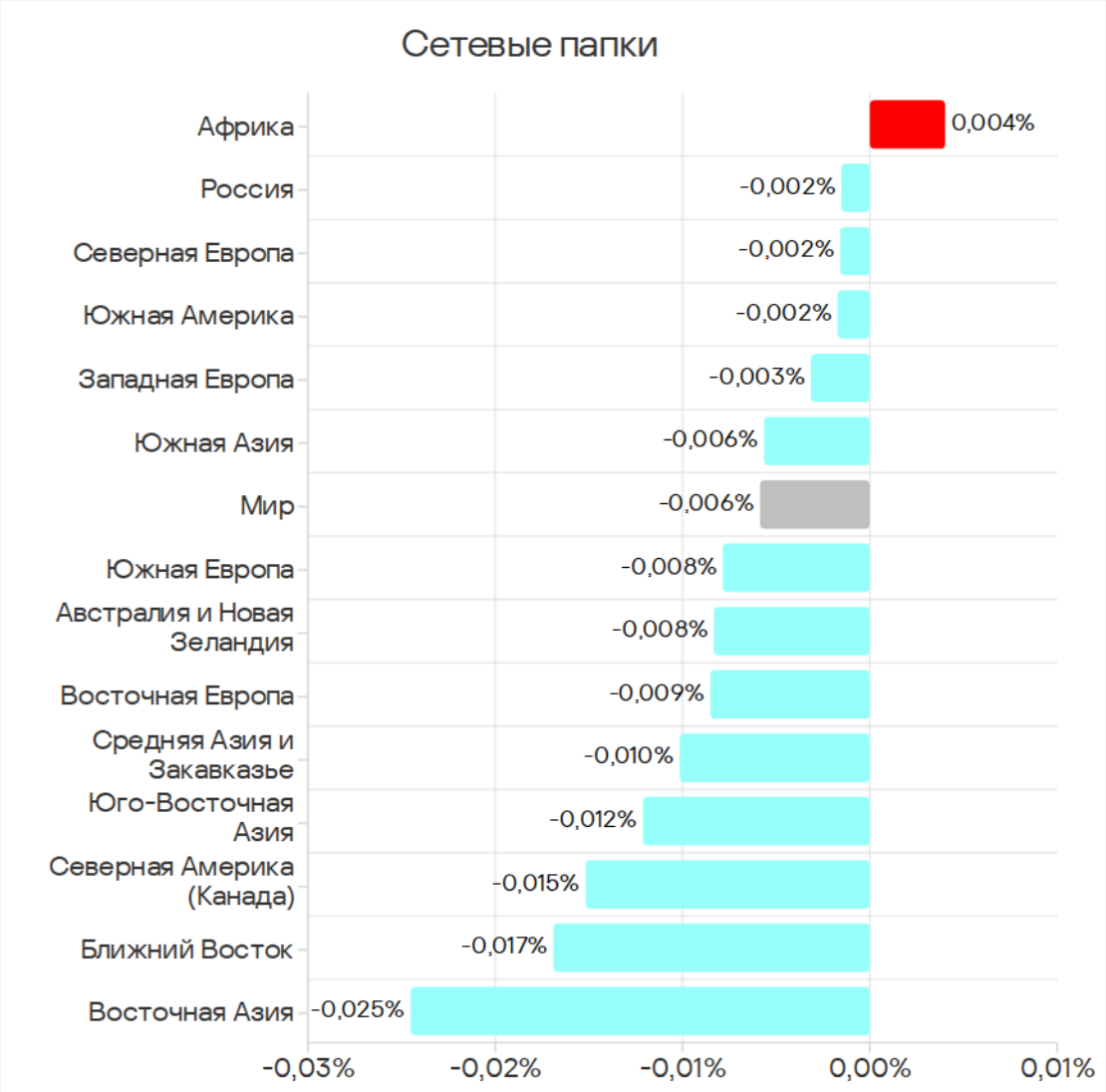


Угрозы в сетевых папках и основные категории угроз в сетевых папках, III квартал 2024 года – II квартал 2026 года

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, II 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