Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Россия. Второй квартал 2025 года

23.09.2025

Версия 1.0

Россия 3
Актуальные угрозы 3
Статистика по всем угрозам 4
Источники угроз 4
Интернет 5
Почтовые клиенты 6
Съемные носители 7
Сетевые папки 7
Категории угроз 8
Ресурсы в интернете из списка запрещенных 9
Майнеры — исполняемые файлы для ОС Windows и черви 10
Отрасли 11
Источники и категории вредоносного ПО в отраслях: «горячие точки» 13
Методика подготовки статистики 17

Россия

Актуальные угрозы

Основной источник угроз в России — интернет

Основные категории угроз из интернета, блокируемые на компьютерах АСУ, — это интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы, а также майнеры.

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

- известные вредоносные URL и IP-адреса, используемые злоумышленниками для размещения вредоносных нагрузок и конфигураций;
- подозрительные (ненадежные) 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 полезных нагрузок и конфигураций следующего этапа.

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

Высокие значения параметра, как правило, свидетельствуют:

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

Майнеры — исполняемые файлы для ОС Windows и черви

Россия стабильно, с конца 2022 года, находится на втором месте среди регионов (выше — Средняя Азия и Закавказье) по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows.

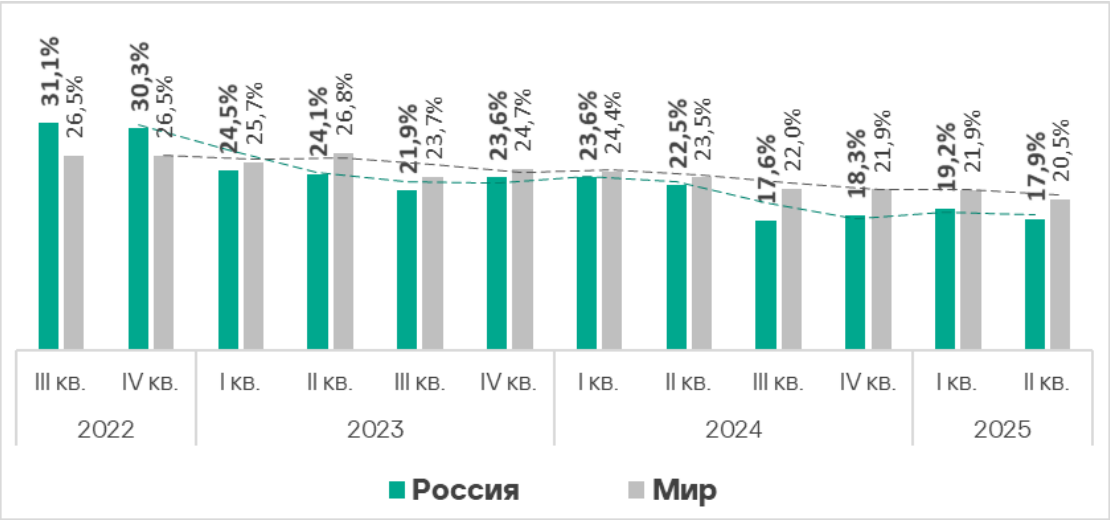
Черви во втором квартале 2025 года в рейтинге категорий угроз поднялись в России на четвертое место. Такая высокая позиция у этой категории угроз, кроме России, только в Средней Азии и Закавказье.

У этих двух категорий угроз динамика показателей в России очень схожая. Это объясняется тем, что майнеры для ОС Windows активно используют модули и компоненты, которые по сути являются червями и служат для доставки майнера на другие компьютеры в сети — автоматизированный lateral movement.

Статистика по всем угрозам

Россия занимает 10-е место в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

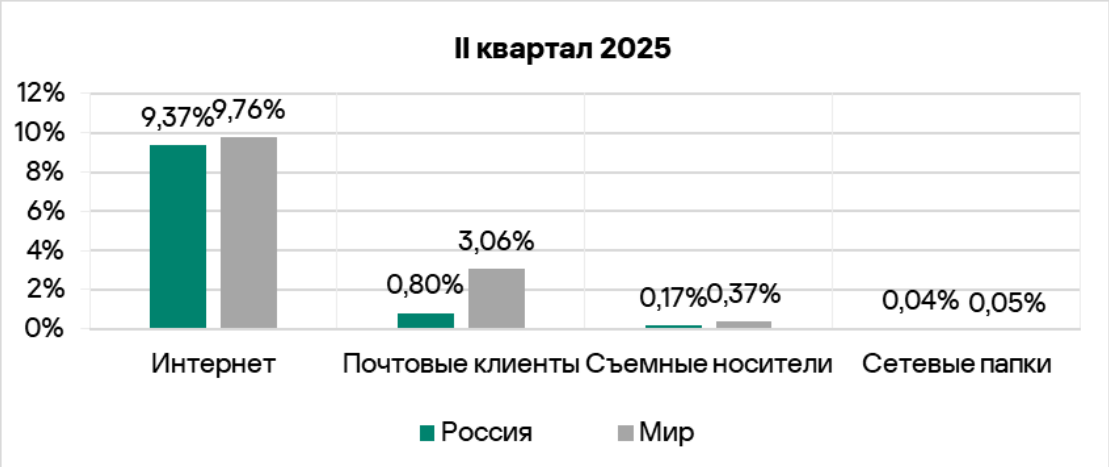
Во втором квартале 2025 года этот показатель уменьшился на 1,3 п. п. — до 17,9%.



Значение этого показателя в регионе остается ниже среднемирового с начала 2023 года. По сравнению с Северной Европой — регионом с наименьшим показателем, доля атакованных компьютеров в России выше в 1,6 раза.

Источники угроз

Значения доли компьютеров АСУ, на которых блокируются угрозы из разных источников, в России меньше среднемировых. Ближе всего показатели в регионе и в мире по угрозам из интернета.



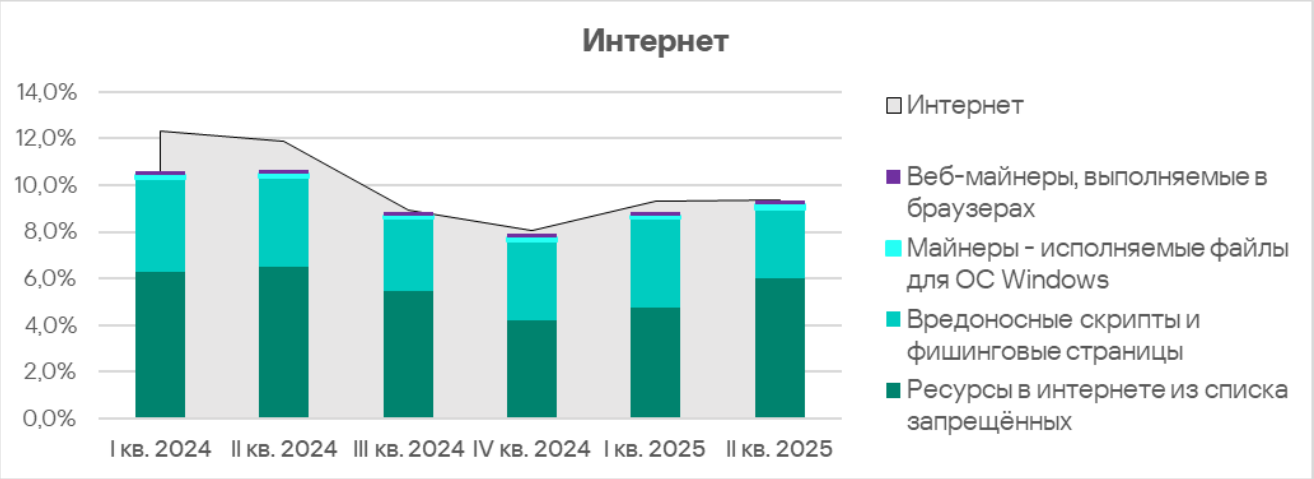
Интернет

В рейтинге регионов по доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, Россия занимает седьмое место. По сравнению с регионом, который замыкает этот рейтинг — Восточной Азией, показатель России выше в 1,5 раза.

Второй квартал подряд доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, в России растет. У остальных источников угроз показатели уменьшились.

Основные категории угроз из интернета, блокируемые на компьютерах АСУ, — это интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы, а также майнеры.

По показателю майнеров — исполняемых файлов для ОС Windows Россия находится на втором месте среди регионов, по показателю веб-майнеров — на третьем. Интернет — основной канал распространения этих угроз.

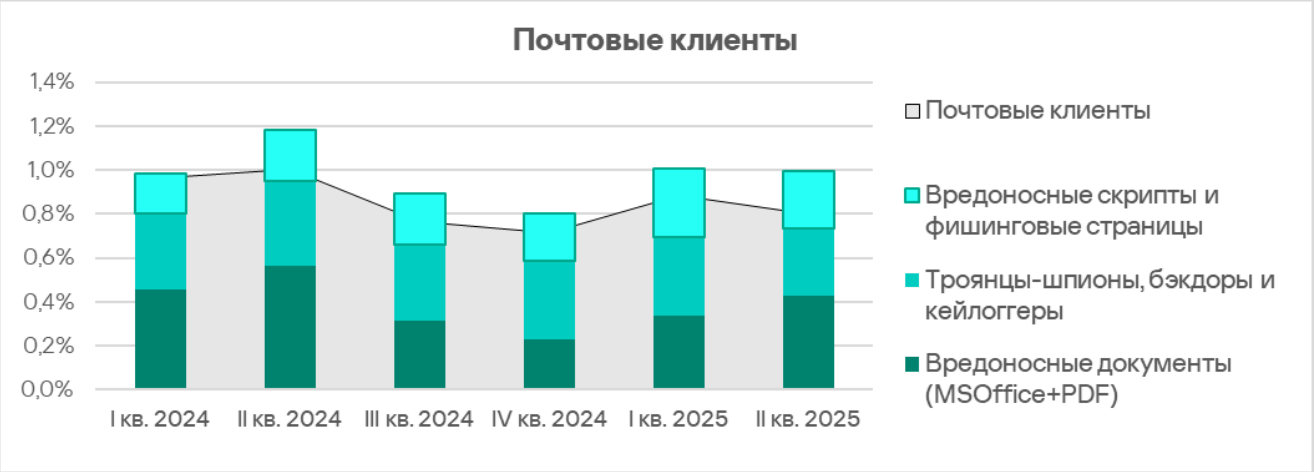


Почтовые клиенты

Доля компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, в России во втором квартале 2025 года оказалась наименьшей из всех регионов — 0,8%.

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

Для вредоносных документов и шпионских программ электронная почта — основной канал распространения.

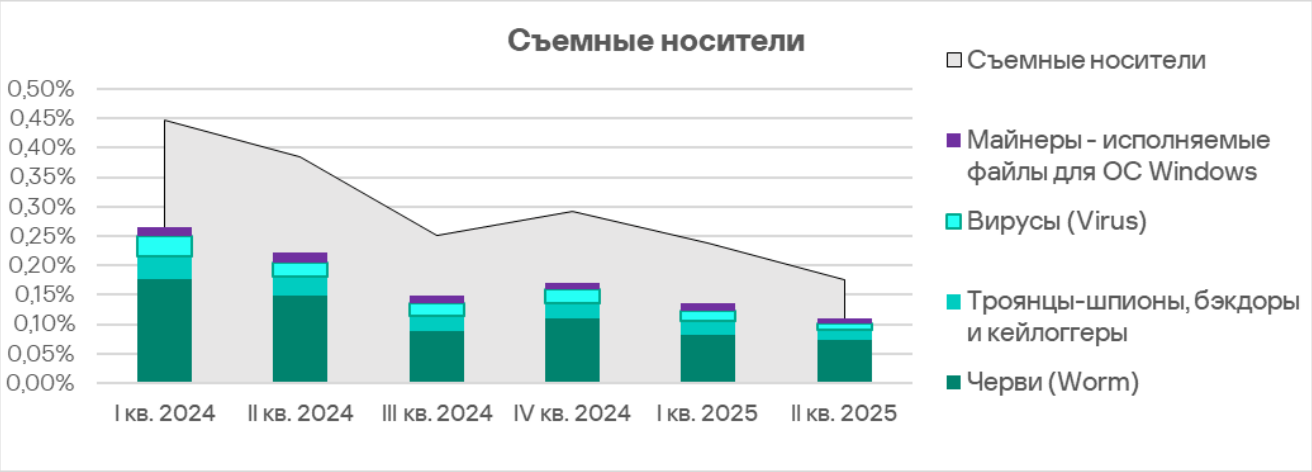


Съемные носители

По доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, Россия находится на восьмом месте в соответствующем рейтинге регионов с 0,17%. Этот показатель в 6,5 раза больше, чем в Северной Америке (Канада), которая замыкает рейтинг.

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

Для червей съемные носители — основной способ распространения.

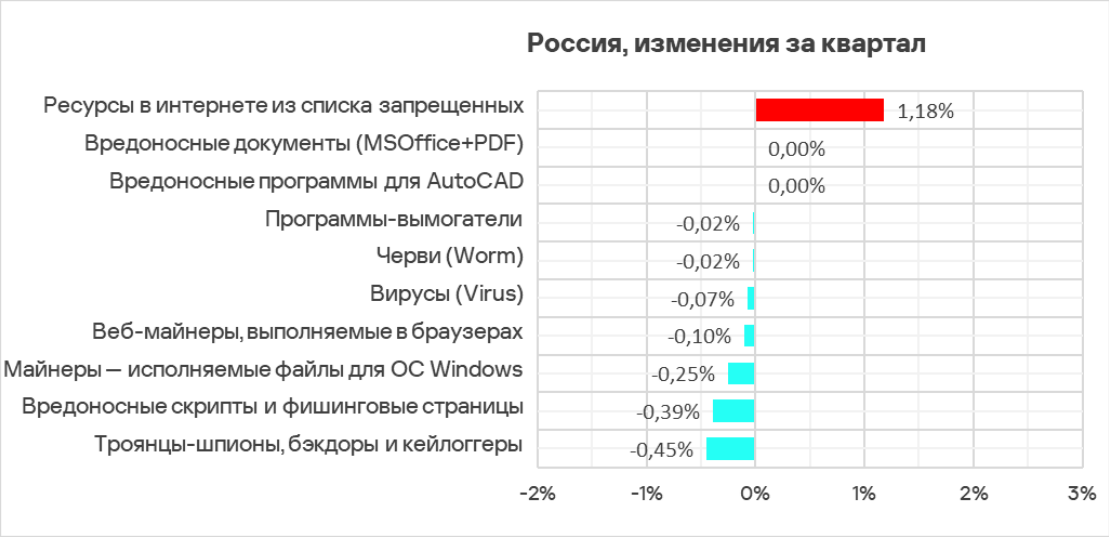


Сетевые папки

По доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, Россия находится на шестом месте в соответствующем рейтинге регионов с 0,04%. Этот показатель в 3,9 раза больше, чем в Северной Европе, где он наименьший из всех регионов.

Основные категории угроз, которые блокируются в сетевых папках: черви, шпионские программы и вирусы.

Категории угроз



В России у двух категорий угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения:

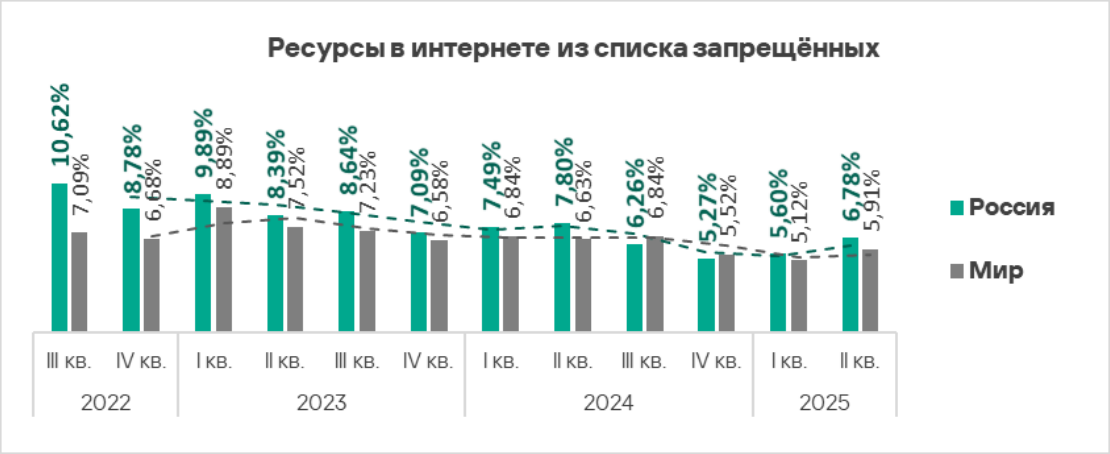
- ресурсы в интернете из списка запрещенных — в 1,1 раза;
- майнеры — исполняемые файлы для ОС Windows — в 1,3 раза.

По показателям обеих этих категорий Россия занимает второе место в региональных рейтингах.

Ресурсы в интернете из списка запрещенных

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются опасные веб-ресурсы, Россия находится на втором месте, уступая только Африке. Показатель России превышает показатель региона, замыкающего этот рейтинг — Восточной Азии, в 2,1 раза.

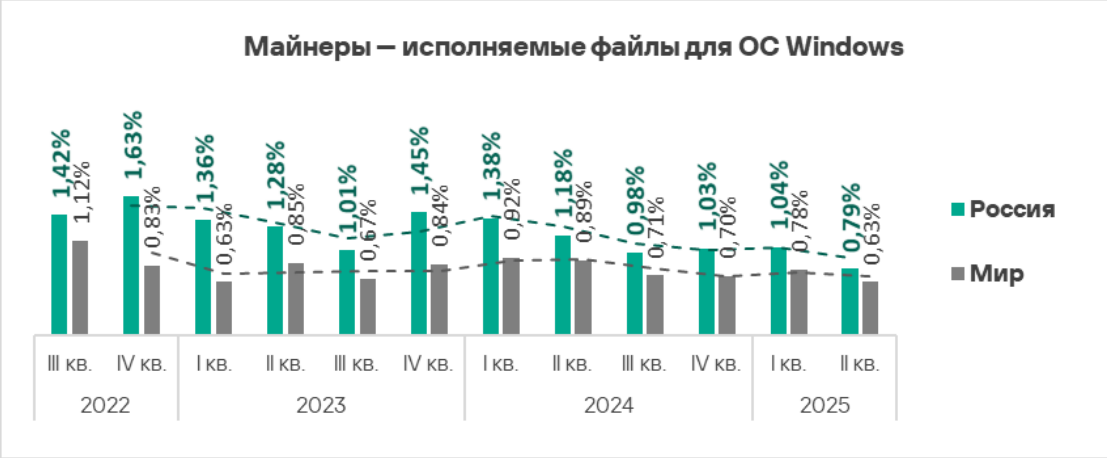
Ресурсы в интернете из списка запрещенных — постоянный лидер рейтинга категорий угроз в регионе. Это единственная категория, показатель которой во втором квартале 2025 года в России вырос.



Майнеры — исполняемые файлы для ОС Windows и черви

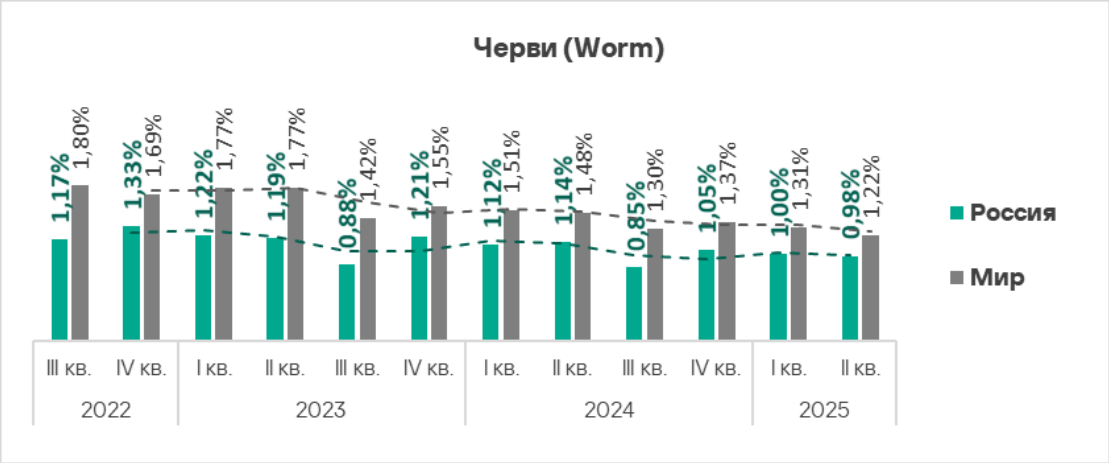
Среди регионов Россия находится на втором месте по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, уступая только Средней Азии и Закавказью. Этот показатель в России больше, чем в регионе с его минимальным значением — Восточной Азии — в 4,2 раза.

Показатель майнеров в формате исполняемых файлов для ОС Windows во втором квартале уменьшился.

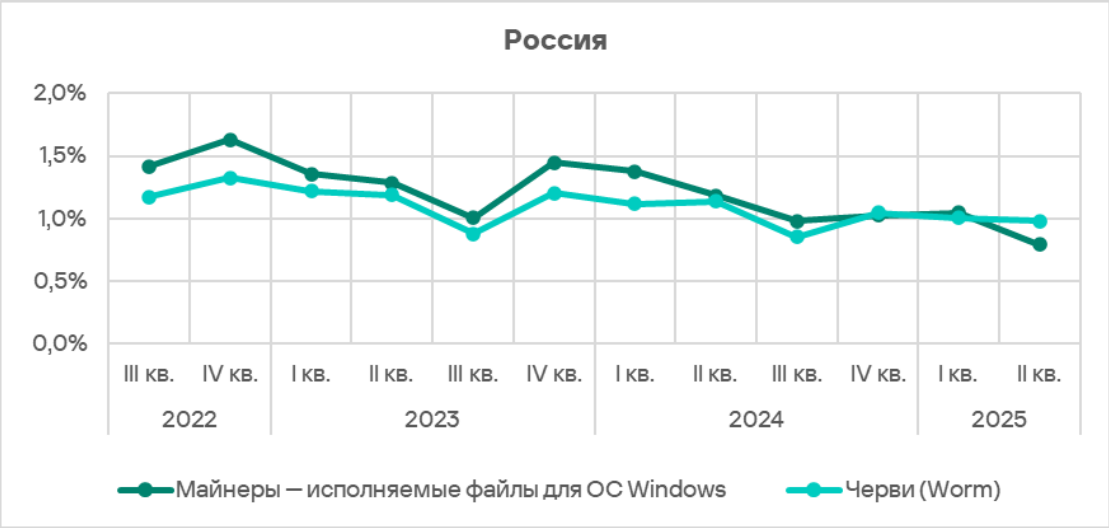


Майнеры для ОС Windows активно используют модули и компоненты, которые по сути являются червями и служат для доставки майнера на другие компьютеры в сети — автоматизированный lateral movement.

Черви во втором квартале 2025 года в рейтинге категорий угроз поднялись на четвертое место. На такой высокой позиции в региональном рейтинге эта категория угроз, кроме России, находится только в Средней Азии и Закавказье.



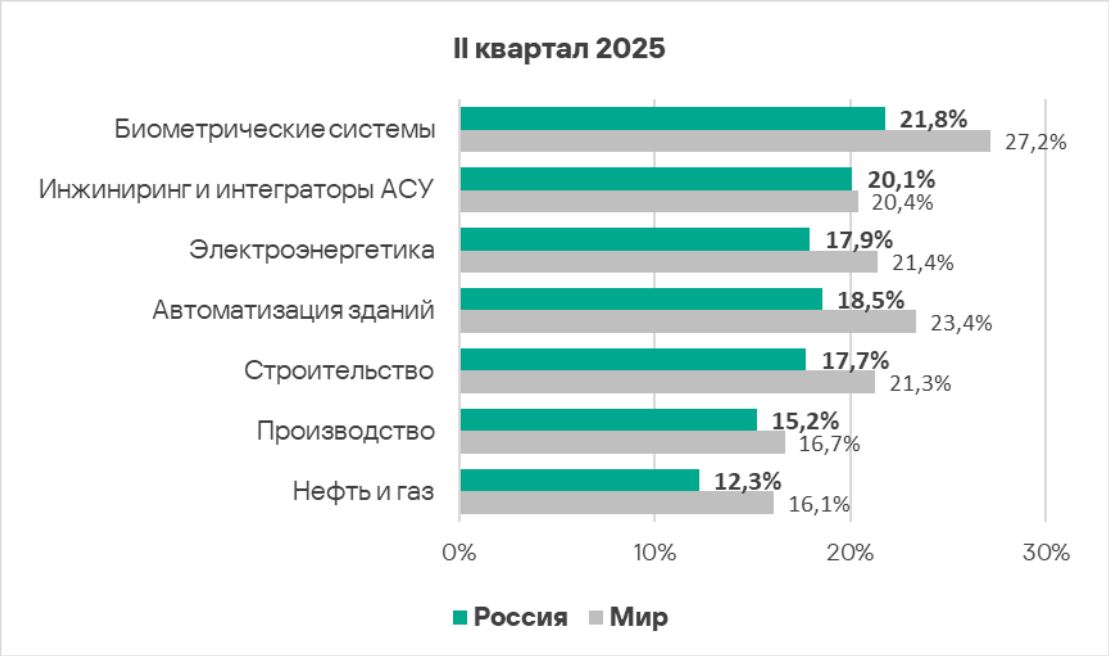
Динамика показателей у майнеров — исполняемых файлов и червей в России схожая.



Отрасли

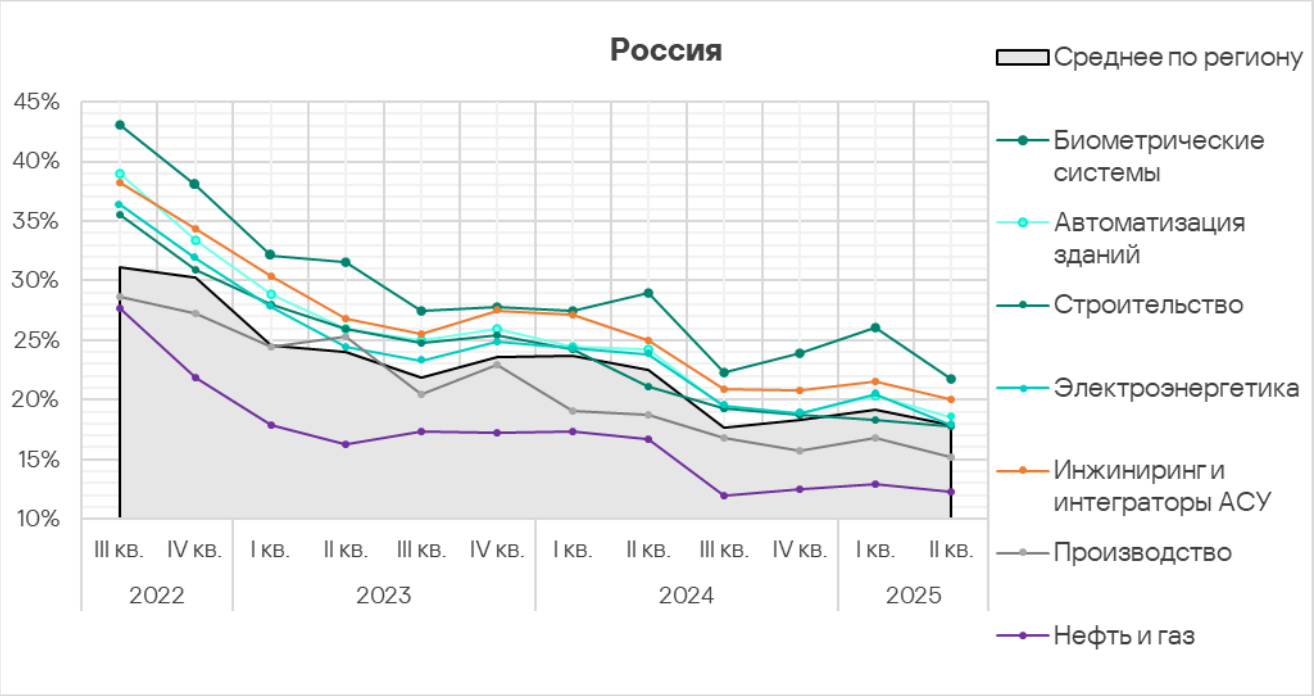
В России из всех рассмотренных в отчете отраслей и OT-инфраструктур чаще всего вредоносные объекты блокируются в биометрических системах.

Во всех отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, ниже соответствующих среднемировых показателей.



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

Во всех рассмотренных отраслях показатели с периодическими колебаниями постепенно снижаются.



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

При оценке проблем отраслей мы используем тепловые карты. На таких картах ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение для индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В России значения, наиболее близкие к максимальным, наблюдались в категории ресурсы в интернете из списка запрещенных, заблокированных в системах биометрии, а также интернет-угрозы в сфере инжиниринга и интеграции АСУ.

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

Показатели источников угроз в отраслях в России, II квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	10,54%	9,25%	9,81%	11,04%	5,58%	10,61%	6,44%	9,37%
Почтовые клиенты	3,49%	1,94%	1,12%	0,87%	0,87%	0,81%	0,74%	0,80%
Съемные носители	0,53%	0,22%	0,41%	0,22%	0,22%	0,37%	0,22%	0,17%
Сетевые папки	0,23%	0,04%	0,06%	0,02%	0,05%	0,03%	0,10%	0,04%
Показатель отрасли в регионе	21,76%	18,55%	17,92%	20,08%	12,25%	17,72%	15,21%	

Показатели категорий угроз в отраслях в России, II квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	8,26%	6,84%	7,56%	8,02%	4,52%	7,57%	4,99%	6,78%
Вредоносные скрипты и фишинговые страницы	5,16%	4,65%	5,07%	4,82%	3,10%	5,07%	3,17%	4,17%
Троянцы-шпионы, бэкдоры и кейлоггеры	4,25%	3,21%	2,97%	2,45%	2,32%	2,09%	2,24%	2,20%
Черви (Worm)	1,44%	1,20%	1,60%	0,91%	1,29%	1,08%	1,38%	0,98%
Майнеры - исполняемые файлы для ОС Windows	1,06%	0,89%	1,25%	1,06%	0,73%	1,19%	0,66%	0,79%
Вредоносные документы (MSOffice + PDF)	2,20%	1,74%	1,47%	0,90%	1,12%	0,78%	1,06%	0,77%
Вирусы (Virus)	0,76%	0,43%	0,97%	0,42%	0,62%	0,49%	0,86%	0,27%
Программы-вымогатели	0,53%	0,24%	0,22%	0,10%	0,19%	0,14%	0,10%	0,09%
Веб-майнеры, выполняемые в браузерах	0,61%	0,36%	0,60%	0,36%	0,41%	0,59%	0,27%	0,23%
Вредоносные программы для AutoCAD	0,23%	0,02%	0,07%	0,03%	0,16%	0,09%	0,10%	0,02%
Показатель отрасли в регионе	21,76%	18,55%	17,92%	20,08%	12,25%	17,72%	15,21%	

Для всех отраслей основной источник угроз — интернет. Как следствие, актуальны такие категории угроз как опасные ссылки из списка запрещенных, вредоносные скрипты и фишинговые страницы и программы-шпионы, которые распространяются через этот источник угроз. Для электроэнергетики, строительства и нефтегазовой отрасли высоки также показатели веб-майнеров.

«Горячие точки» отраслей

Биометрические системы

- Лидер среди отраслей по показателям всех источников угроз, кроме интернета (третье место).
- Лидер среди отраслей по всем категориям угроз, кроме червей (второе место), вирусов и майнеров для ОС Windows (третье место).

Инжиниринг и интеграторы АСУ

- Лидер среди отраслей по угрозам из интернета. Все остальные показатели — в границах ожидаемых.

Автоматизация зданий

- Второе место среди отраслей по угрозам из почты.
- Третье место по следующим категориям угроз: вредоносные документы, шпионские программы, программы-вымогатели.

Электроэнергетика

- Второе место среди отраслей по показателям угроз на съемных носителях. Третье — по почтовым клиентам и сетевым папкам.
- Лидер по показателям следующих категорий угроз: черви, вирусы, майнеры — исполняемые файлы для ОС Windows. Второе место – по показателям веб-майнеров, третье – по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, шпионское ПО, вредоносные документы, программы-вымогатели.

Строительство

- Второе место среди отраслей по угрозам из интернета. Третье — по показателю угроз на съемных носителях.
- Второе место по показателям вредоносных скриптов и фишинговых страниц, а также майнеров для ОС Windows. Третье – по показателям ресурсов из списка запрещенных, а также веб-майнеров.

Производство

- Второе место среди отраслей по угрозам в сетевых папках.
- Второе место по показателям вирусов и третье – по показателям червей и вредоносных программ для AutoCAD.

Нефтегазовая отрасль

- Четвертое место по показателям угроз из почтовых клиентов и сетевых папок.
- Второе место по показателям в категории вредоносные программы для AutoCAD. Четвертое место по показателям в следующих

категориях угроз: вредоносные документы, черви, вирусы, программы-вымогатели.

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