Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второй квартал 2024 — Россия

26.09.2024

Version 1.0

Цифры квартала

Процент компьютеров АСУ

Во втором квартале 2024 года средняя по миру доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась по сравнению с предыдущим кварталом на 0,9 п. п. и составила 23,5%.

Все регионы можно разделить на три группы по проценту компьютеров АСУ, на которых в течение второго квартала были заблокированы вредоносные объекты:

Больше 25%:

- Африка — 30,0%
- Юго-Восточная Азия — 29,2%
- Центральная Азия — 26,5%
- Ближний Восток — 25,0%

В регионах этой группы компьютеры в технологических сетях в целом чрезмерно подвержены киберугрозам. Для этих регионов характерен недостаточный уровень инвестиций в различные аспекты кибербезопасности — как в инструменты и меры по защите от угроз, так и в решение проблемы нехватки специалистов, формирование развитой культуры кибербезопасности и повышение осведомленности.

20–25%

- Восточная Европа — 23,5%
- Россия — 22,5%
- Латинская Америка — 22,4%
- Южная Азия — 21,4%
- Восточная Азия — 21,3%
- Южная Европа — 20,9%

Регионы этой группы могут сталкиваться с отдельными, характерными именно для них проблемами, связанными с изоляцией технологической инфраструктуры от потенциальных киберугроз.

До 20%

- Австралия и Новая Зеландия — 16.9%
- США и Канада — 13,5%
- Западная Европа — 13,2%
- Северная Европа — 11,3%

В третью группу входят наиболее благополучные регионы с точки зрения кибербезопасности технологической инфраструктуры.

По сравнению с предыдущим кварталом, во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась в четырех регионах: США и Канаде (на 0,2 п. п.), Австралии и Новой Зеландии (на 0,7 п. п.), Западной Европе (на 0,9 п. п.) и Восточной Азии (на 1,0 п. п.).

Категории вредоносного ПО

Вредоносные объекты, используемые для первичного заражения

Данная категория включает в себя опасные ресурсы в интернете, которые попадают в списки запрещённых, вредоносные скрипты и фишинговые страницы, а также вредоносные документы.

Логика атак злоумышленников предполагает, что такие вредоносные объекты активно распространяются. В результате они чаще остальных блокируются защитными решениями. Это отражает и наша статистика.

В мире и почти во всех регионах ресурсы в интернете из списка запрещённых, а также вредоносные скрипты и фишинговые страницы занимают первые места в рейтингах категорий вредоносного ПО по проценту компьютеров АСУ, на которых они были заблокированы.

Источники большинства вредоносных объектов, используемых для первичного заражения, — это интернет и электронная почта. В рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из этих источников, лидируют:

Угрозы из интернета — выше среднемирового значения 11,25%

- Центральная Азия — 12,33%
- Юго-Восточная Азия — 12,10%
- Россия — 11,89%
- Африка — 11,85%

Угрозы из электронной почты — выше среднемирового значения 3,04%

- Южная Европа — 7,06%
- Восточная Европа — 4,97%
- Ближний Восток — 4,79%
- Латинская Америка — 4,79%
- Юго-Восточная Азия — 4,33%
- Африка — 3,67%
- Австралия и Новая Зеландия — 3,29%

Ресурсы в интернете из списка запрещённых

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещённых, лидируют (с показателями выше среднемирового значения 6,63%):

- Россия — 7,80%
- Центральная Азия — 7,58%
- Африка — 7,35%
- Восточная Европа — 7,07%

Вредоносные скрипты и фишинговые страницы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидируют (с показателями выше среднемирового значения 5,69%):

- Южная Европа — 7,46%
- Ближний Восток — 6,90%
- Юго-Восточная Азия — 6,77%
- Австралия и Новая Зеландия — 6,73%
- Латинская Америка — 6,69%
- Африка — 5,87%
- Восточная Европа — 5,75%

Вредоносные документы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные документы, лидируют (с показателями выше среднемирового значения 1,96%):

- Южная Европа — 3,75%
- Латинская Америка — 3,23%
- Юго-Восточная Азия — 2,76%
- Восточная Европа — 2,32%
- Ближний Восток — 2,29%

Вредоносное ПО следующего этапа

Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа — шпионское ПО, программы-вымогатели и майнеры.

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 тех, кто внедряет майнеры криптовалют на компьютеры АСУ.

Во втором квартале 2024 года значительная часть майнеров для Windows, обнаруженных на компьютерах АСУ, представляла 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.

Другой популярный метод внедрения майнеров, обнаруживаемых на компьютерах АСУ, заключается в использовании таких майнеров криптовалют как XMRig, NBMiner, OneZeroMiner и т. д. Подобные майнеры, не являясь вредоносным ПО, детектируются защитными решениями как RiskTools. Злоумышленники используют их в сочетании со специфическими конфигурационными файлами, позволяющими визуально скрывать выполнение майнера от пользователя.

Шпионское ПО

Как правило, чем выше процент компьютеров АСУ, на которых блокируется вредоносное ПО, используемое для первичного заражения, тем выше соответствующий процент для вредоносного ПО следующего этапа.

В большинстве случаев шпионское ПО (включая троянские программы, бэкдоры и кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо в качестве инструментария промежуточных этапов кибератаки (например, разведки и распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных.

Если шпионское ПО обнаруживается на компьютере АСУ, это обычно указывает на то, что вектор первоначального заражения сработал — будь то нажатие пользователем на вредоносную ссылку, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует о том, что меры защиты периметра технологической сети (такие как контроль безопасности сетей и обеспечение выполнения политики использования съемных устройств) либо отсутствовали, либо были неэффективными.

Как и предполагалось, регионы, лидирующие по проценту компьютеров АСУ, на которых было заблокировано шпионское ПО, также являются лидерами по угрозам, связанным с первичным заражением (за исключением России, в которой показатели, связанные со шпионским ПО, невысоки).

Выше среднемирового значения 4,08%:

- Африка — 7,14%
- Ближний Восток — 6,29%
- Южная Европа — 6,21%
- Юго-Восточная Азия — 5,78%
- Восточная Европа — 5,44%
- Центральная Азия — 4,80%
- Латинская Америка — 4,77%
- Восточная Азия — 4,15%

Почти во всех регионах в рейтингах категорий угроз шпионские программы по проценту компьютеров АСУ, на которых они были заблокированы, не поднимаются выше третьего места, за исключением следующих регионов:

- **Восточная Азия** — в регионе программы-шпионы **на первом месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых они были заблокированы — 4,15%.
- **Центральная Азия, Африка, Ближний Восток и Южная Европа —** в этих регионах находятся шпионские программы **на втором месте** в соответствующих рейтингах.

Программы для скрытого майнинга криптовалюты. Майнеры — исполняемые файлы для ОС Windows

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, лидируют (с показателями выше среднемирового значения 0,89%):

- Центральная Азия — 1,62%
- Россия — 1,18%
- Африка — 1,06%
- Восточная Европа — 1,01%

В мировом рейтинге категорий угроз майнеры в форме исполняемых файлов для ОС Windows находятся на седьмом месте по проценту компьютеров АСУ, на которых они были заблокированы.

- В России в аналогичном рейтинге они на 4-м месте.
- В Центральной Азии, Австралии и Новой Зеландии, Северной Европе — на 5-м.

Отметим, что во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, снизился в таких регионах как Россия, Центральная Азия и Восточная Европа, но увеличился в Африке.

Программы для скрытого майнинга криптовалюты. Веб-майнеры, выполняемые в браузерах

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, лидируют (с показателями выше среднемирового значения 0,50%):

- Африка — 0,83%
- Ближний Восток — 0,81%
- Латинская Америка — 0,68%
- Австралия и Новая Зеландия — 0,68%
- Восточная Европа — 0,63%
- Юго-Восточная Азия — 0,56%

В региональных рейтингах категорий угроз веб-майнеры оказались на более высоких местах, чем в мировом рейтинге по проценту компьютеров АСУ, на которых они были заблокированы (в мире — на восьмом месте):

- США и Канада — на 5-м месте в региональном рейтинге
- Северная Европа, Австралия и Новая Зеландия — на 6-м месте в региональном рейтинге
- Западная, Восточная и Южная Европа, Ближний Восток — на 7-м месте в региональных рейтингах

Программы-вымогатели

Регионы, в которых была зафиксирована самая высокая доля компьютеров АСУ, на которых были заблокированы программы-вымогатели (с показателями выше среднемирового значения 0,18%):

- Ближний Восток — 0,33%
- Африка — 0,25%
- Юго-Восточная Азия, Южная Азия, Латинская Америка — 0,22%
- Центральная Азия, Южная Европа — 0,19%

Отметим, что во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, увеличился во всех регионах, кроме Африки.

Самораспространяющееся вредоносное ПО. Черви и вирусы

Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнет-сетей, приобрели черты угроз следующего этапа.

Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО.

Высокие показатели обнаружения самораспространяющегося вредоносного ПО и ПО, которое распространяется через сетевые папки, на уровне отрасли, страны или региона, вероятно, указывают на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных точек.

Черви

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы черви, лидируют (с показателями выше среднемирового значения 1,48%):

- Африка — 4,67%
- Центральная Азия — 2,72%
- Ближний Восток — 2,22%
- Юго-Восточная Азия — 1,91%
- Восточная Азия — 1,80%
- Южная Азия — 1,74%
- Восточная Европа — 1,56%

В мире черви занимают шестую позицию в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. Но в некоторых региональных рейтингах **черви находятся на более высоких местах**:

- Африка, Центральная Азия, Южная Азия — 4-е место в региональном рейтинге
- Восточная Азия, Ближний Восток, Латинская Америка, Россия, Восточная Европа, Западная Европа, Южная Европа — 5-е место в региональном рейтинге

Верхние строчки в рейтингах черви занимают в регионах, лидирующих по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении **съемных носителей**:

- Африка — 4,34%
- Южная Азия — 1,94%
- Юго-Восточная Азия — 1,69%
- Восточная Азия — 1,54%
- Центральная Азия — 1,37%
- Ближний Восток — 1,31%

Вирусы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вирусы, лидируют (с показателями выше среднемирового значения 1,54%):

- Юго-Восточная Азия — 8,06%
- Африка — 3,84%
- Восточная Азия — 2,95%
- Ближний Восток — 1,99%
- Южная Азия — 1,69%

В Юго-Восточной Азии вирусы занимают первое место (!) в рейтинге категорий угроз по проценту компьютеров АСУ, на которых они были заблокированы.

Отметим также, что четыре региона, которые находятся в топе по вирусам, лидируют и по проценту компьютеров АСУ, на которых были заблокированы **угрозы в сетевых папках**:

- Восточная Азия — 0,35%
- Юго-Восточная Азия — 0,34%
- Южная Азия — 0,21%
- Ближний Восток — 0,13%

Вредоносные программы для AutoCAD

Вредоносное ПО для AutoCAD может распространяться по-разному, поэтому его сложно отнести к конкретной категории.

По проценту компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, лидируют те же регионы, что и в рейтинге по вирусам (с показателями выше среднемирового значения 0,42%):

- Юго-Восточная Азия — 2,93%
- Восточная Азия — 1,57%
- Африка — 0,58%

Обычно вредоносное ПО для AutoCAD - незначительная угроза, которая, как правило, занимает последние места в рейтингах категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.

Однако во втором квартале 2024 года эта категория заняла более высокое место, чем в соответствующем глобальном рейтинге (9-е место), в следующих регионах:

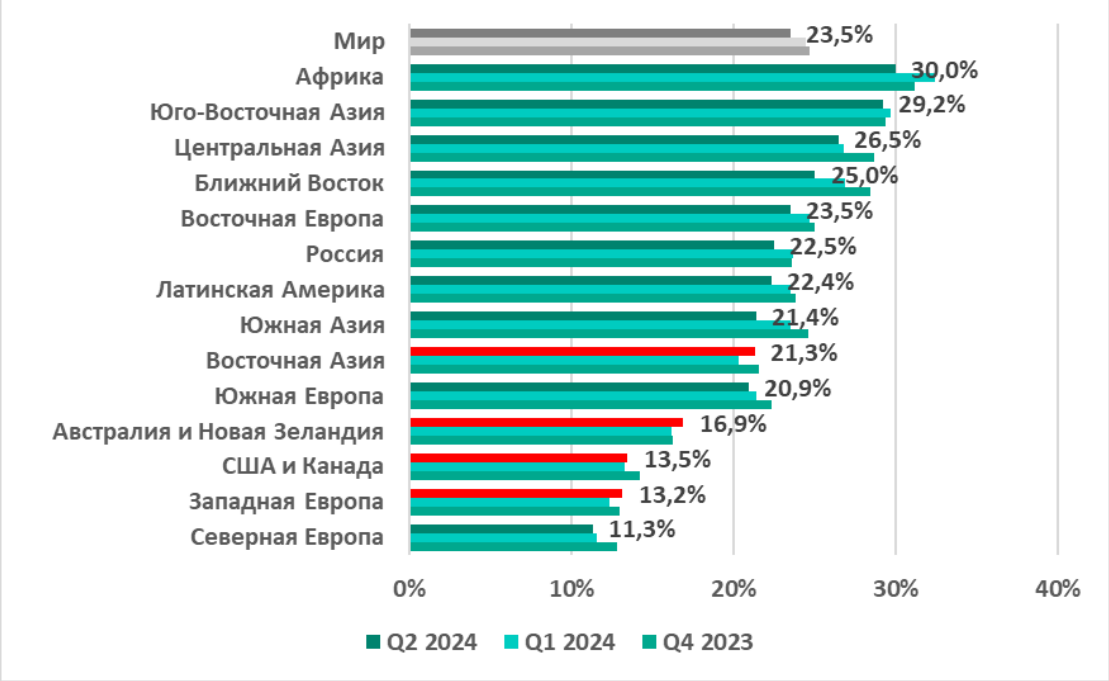
- Юго-Восточная Азия — 5-е место в региональном рейтинге
- Восточная Азия — 7-е место в региональном рейтинге

Регионы. Рейтинги

Процент атакованных компьютеров АСУ

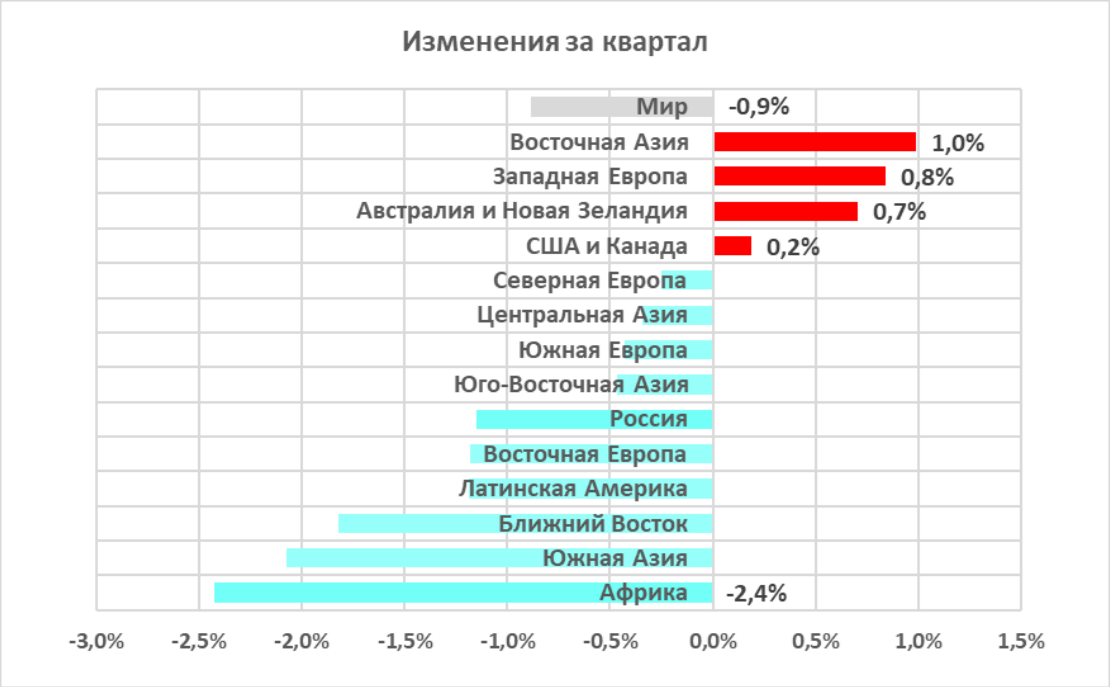
Доля компьютеров АСУ, на которых в течение квартала были заблокированы вредоносные объекты, в регионах варьируется от 11,3% в Северной Европе до 30,0% в Африке.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором квартале 2024 года



В четырех регионах — Восточной Азии, Австралии и Новой Зеландии, США и Канаде, а также Восточной Европе — показатели выросли по сравнению с предыдущим кварталом.

Регионы и мир. Изменение процента атакованных компьютеров за первый квартал 2024 года



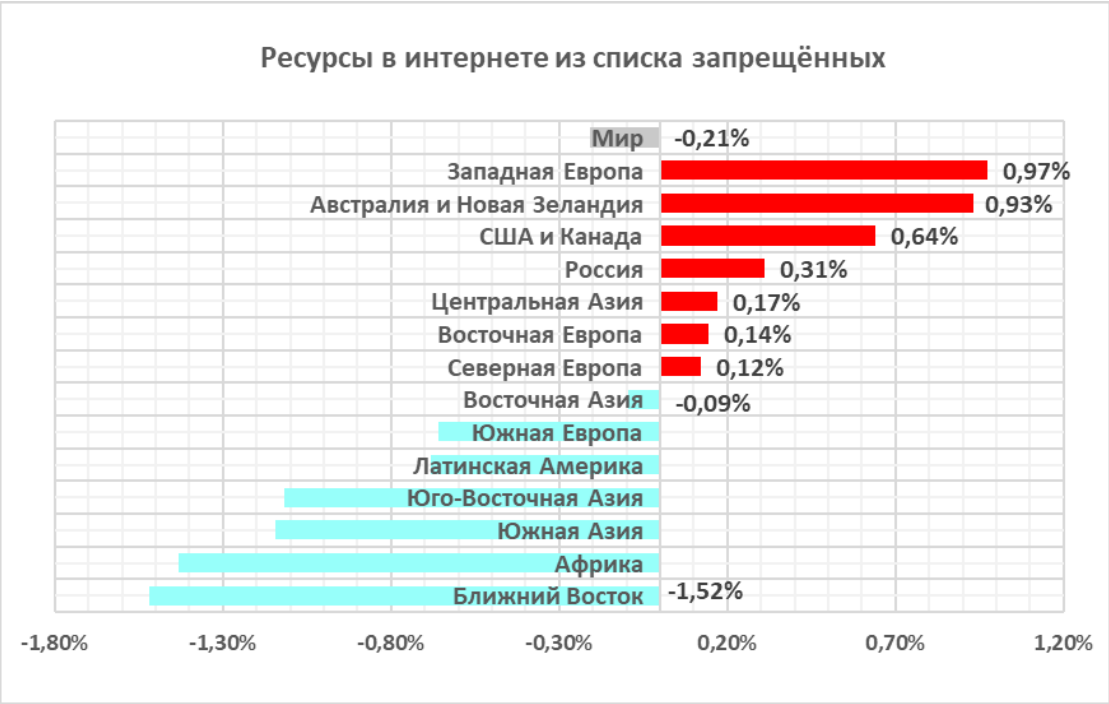
Категории вредоносных объектов

Процент компьютеров АСУ, на которых блокируется вредоносное ПО отдельной категории, отличается в разных регионах. При этом позиция региона в рейтинге по проценту компьютеров АСУ, на которых была заблокирована угроза из отдельно взятой категории, не всегда совпадают с позицией региона в рейтинге регионов по общему проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты любых категорий.

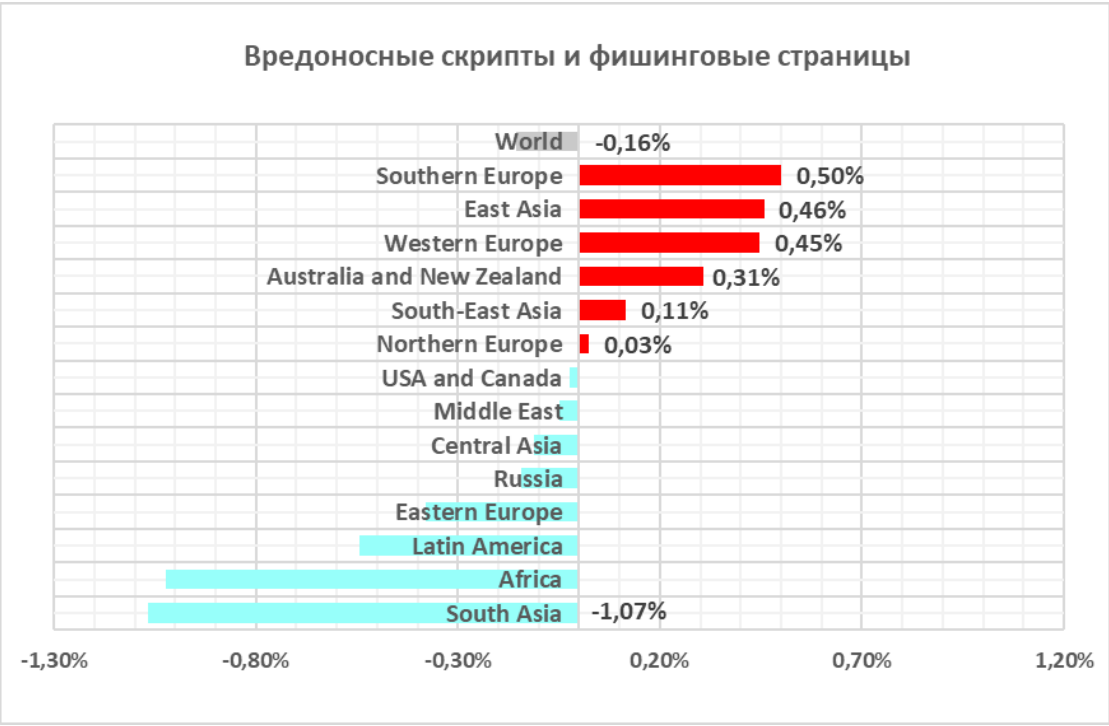
На графиках ниже представлены **рейтинги регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО определенной категории** во втором квартале 2024 года, и изменения процента по сравнению с предыдущим кварталом.

Вредоносные объекты, используемые для первичного заражения

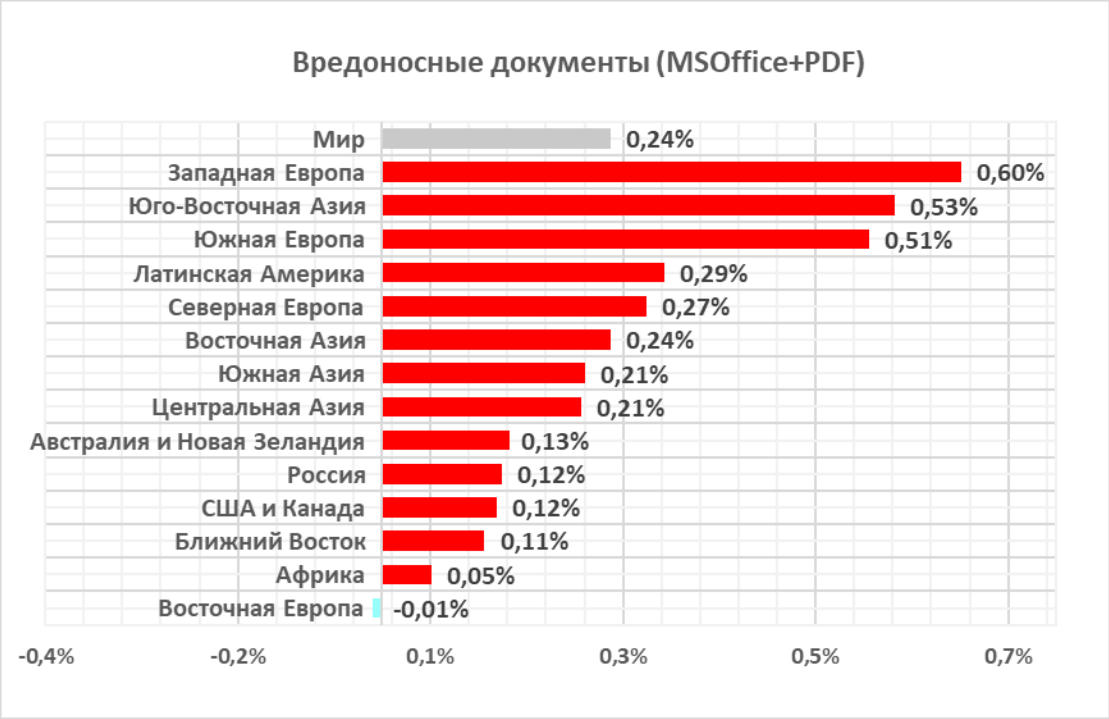
Ресурсы в интернете из списка запрещённых



Вредоносные скрипты и фишинговые страницы (JS и HTML)

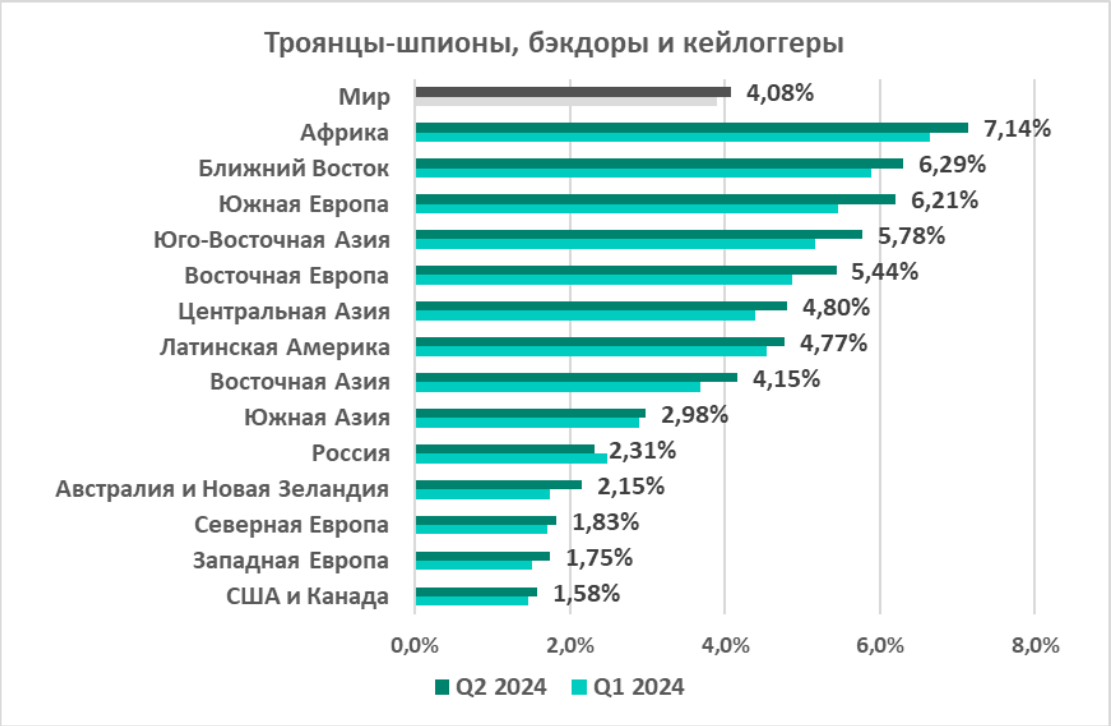


Вредоносные документы (MSOffice+PDF)

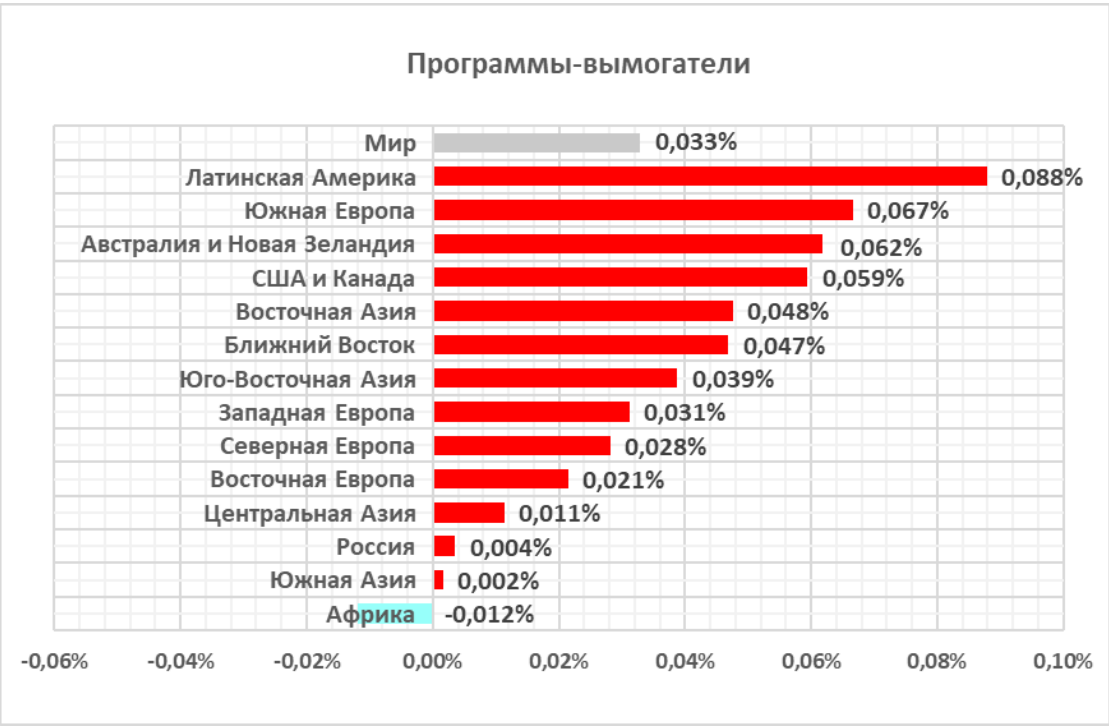


Вредоносное ПО следующего этапа

Программы-шпионы

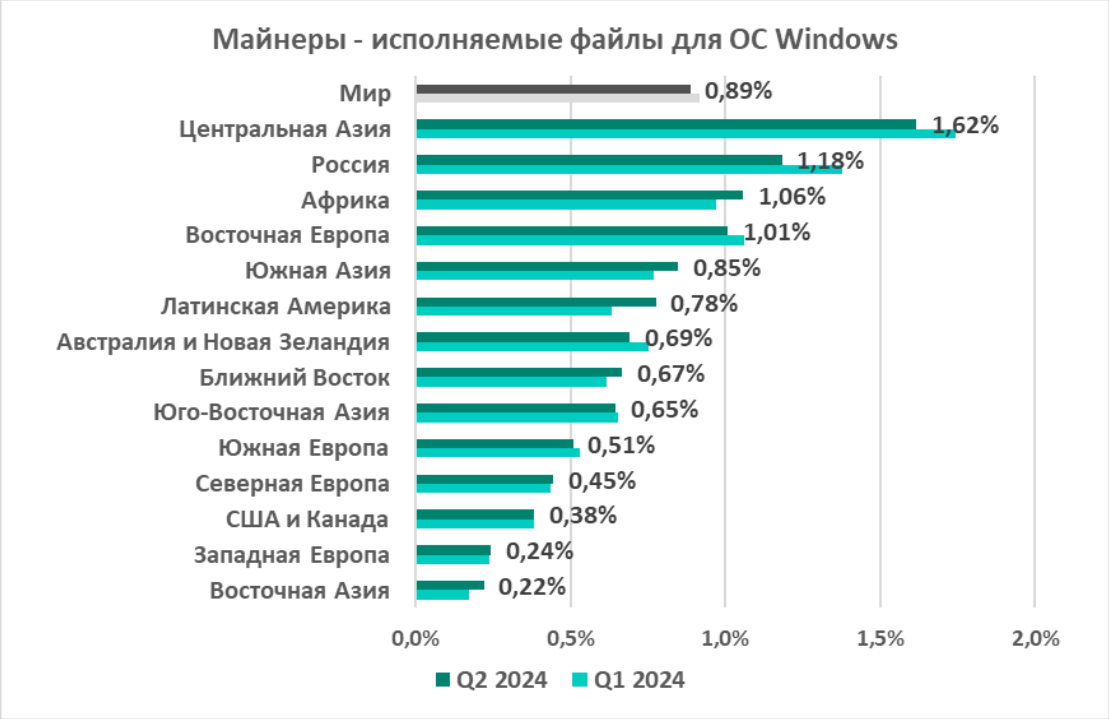


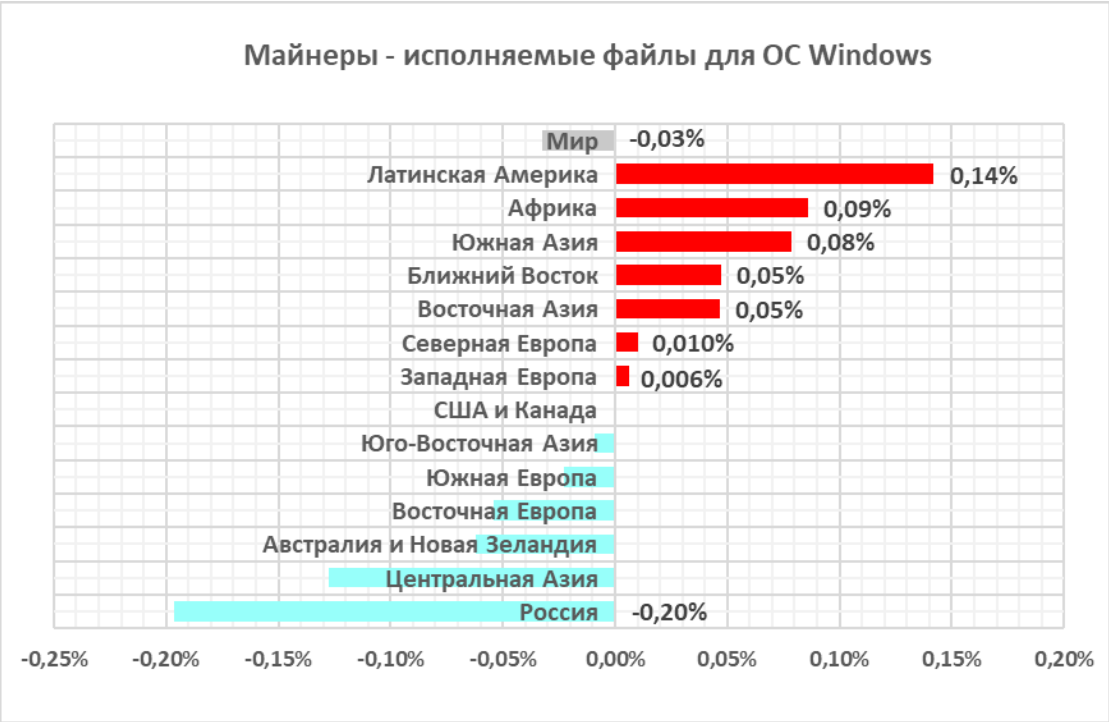
Программы-вымогатели



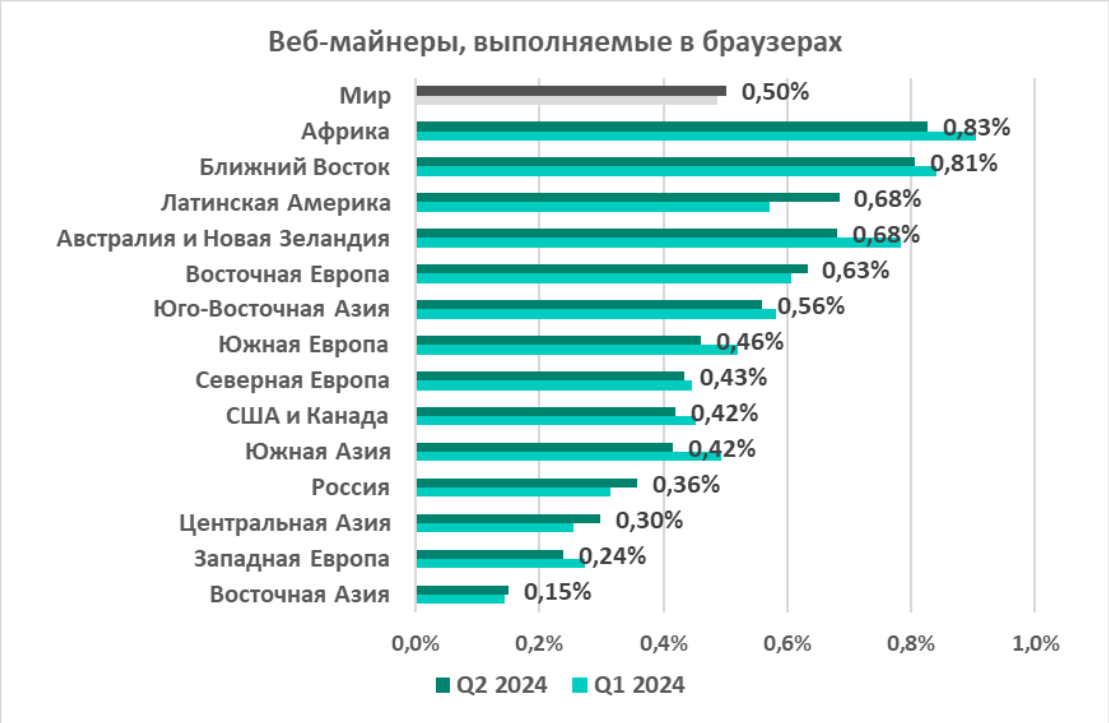
Вредоносные программы для скрытого майнинга криптовалюты

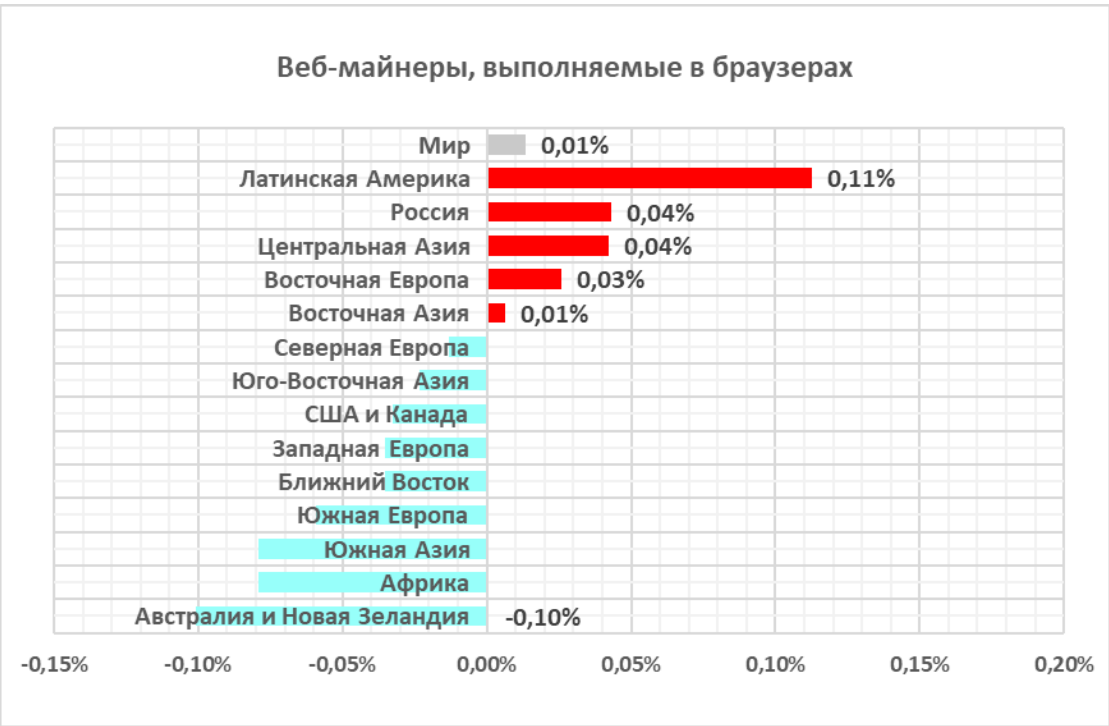
Майнеры — исполняемые файлы для ОС Windows





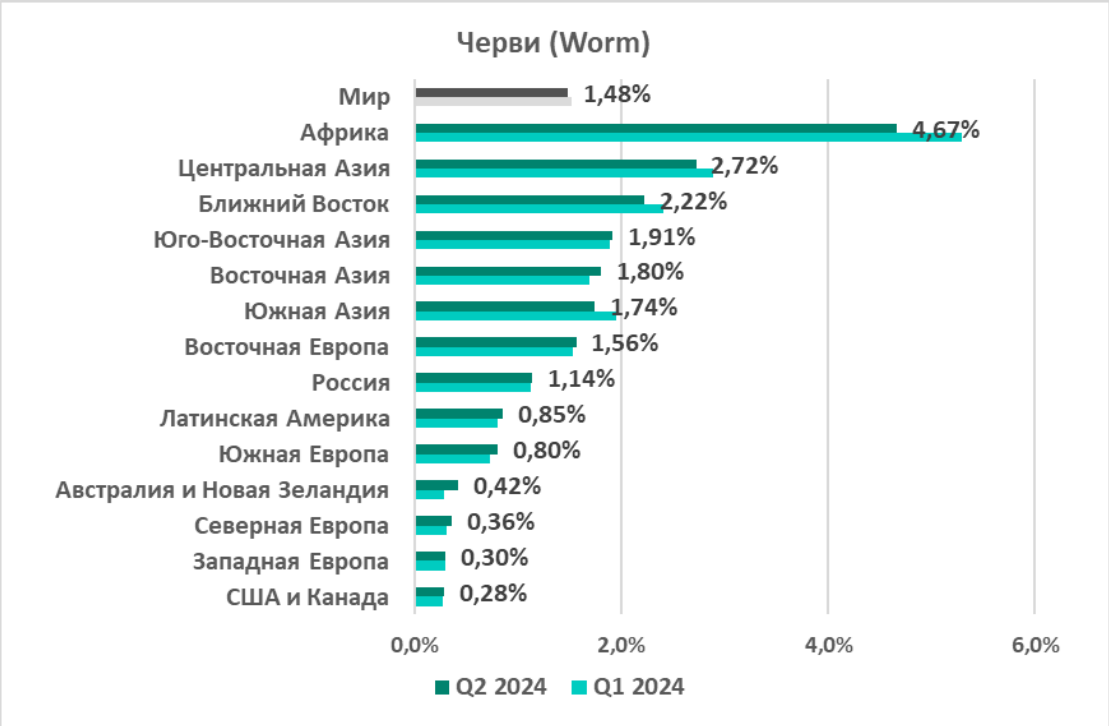
Веб-майнеры

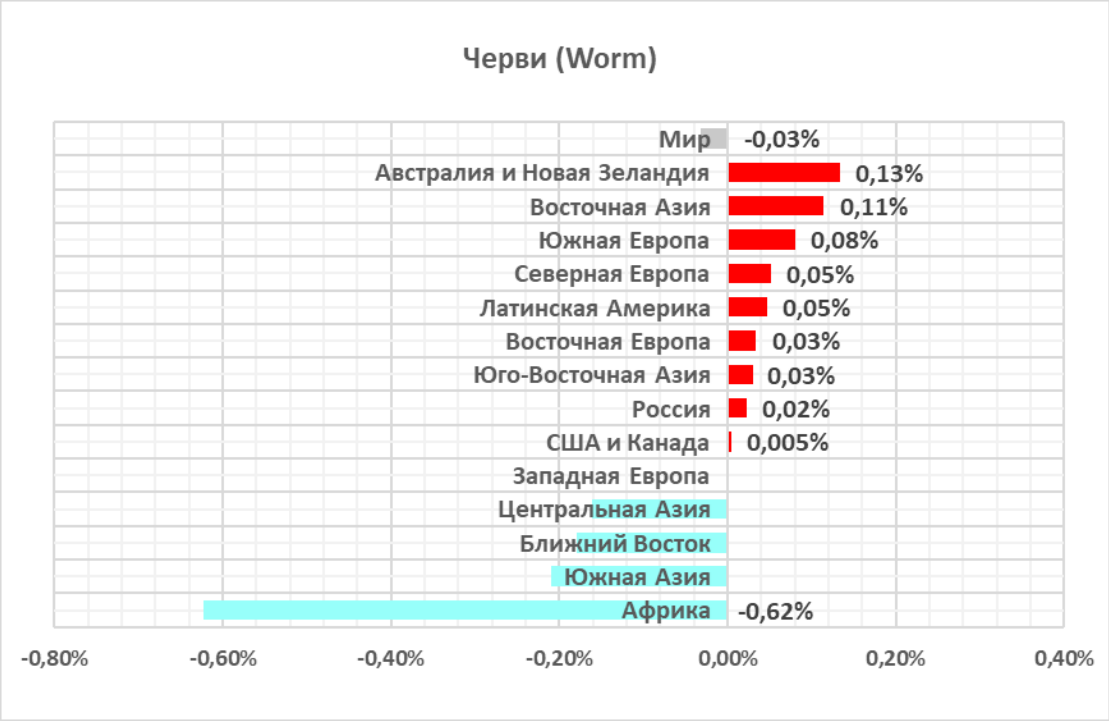




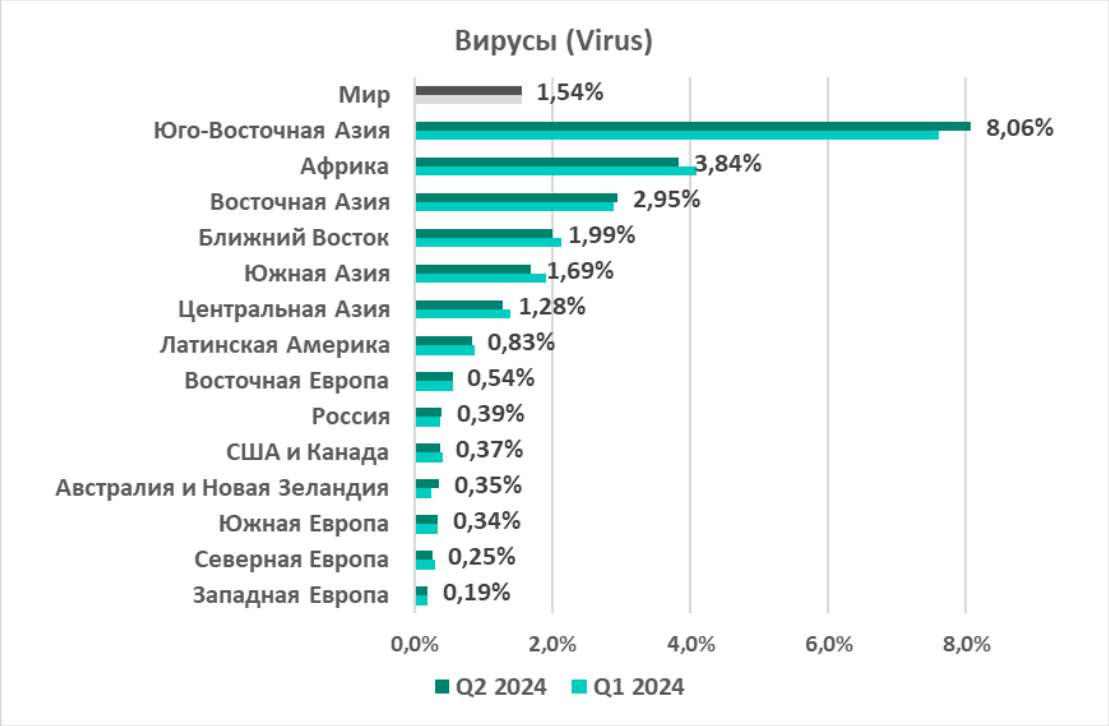
Самораспространяющееся вредоносное ПО. Вирусы и черви

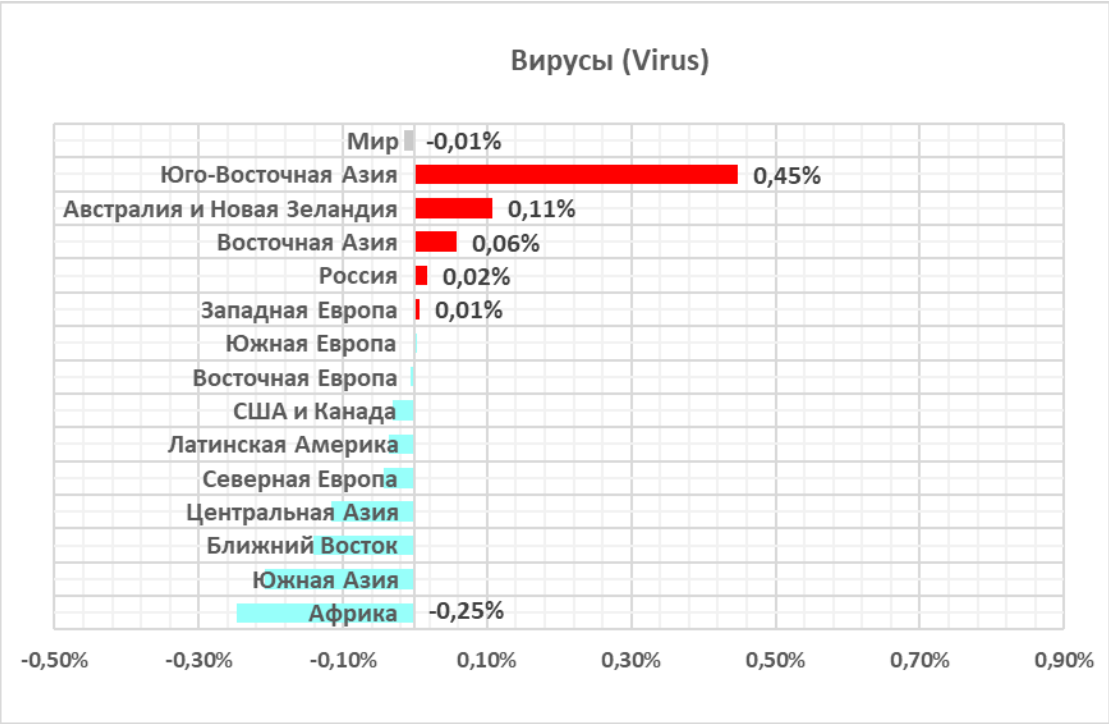
Черви



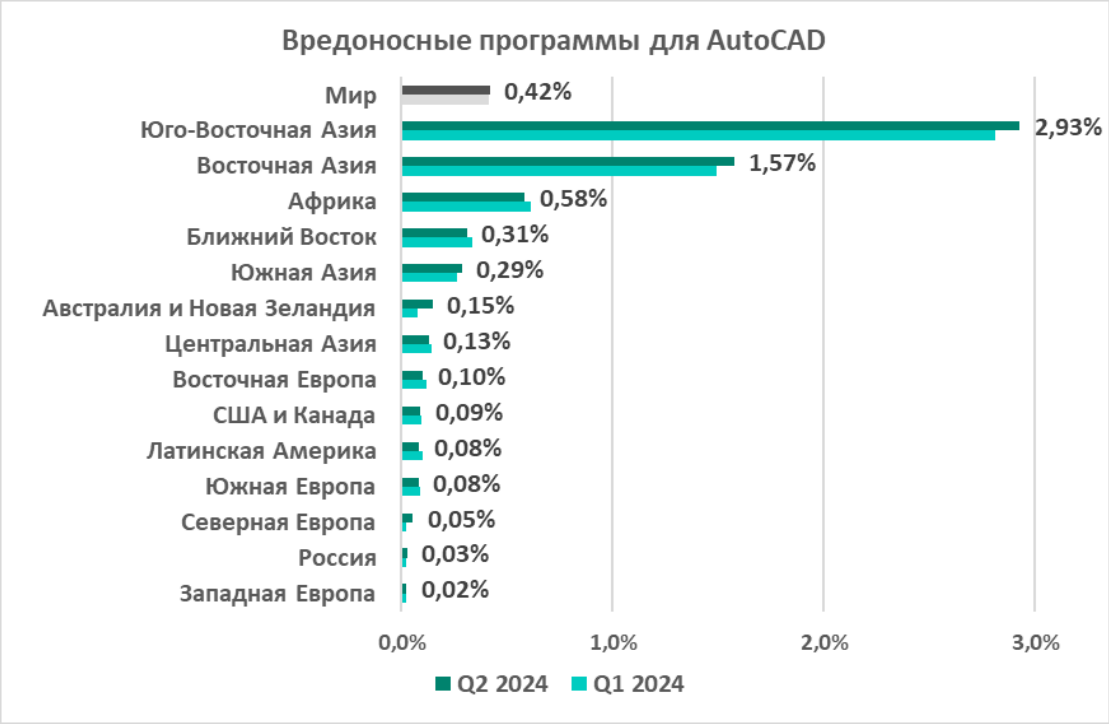


Вирусы





Вредоносные программы для AutoCAD



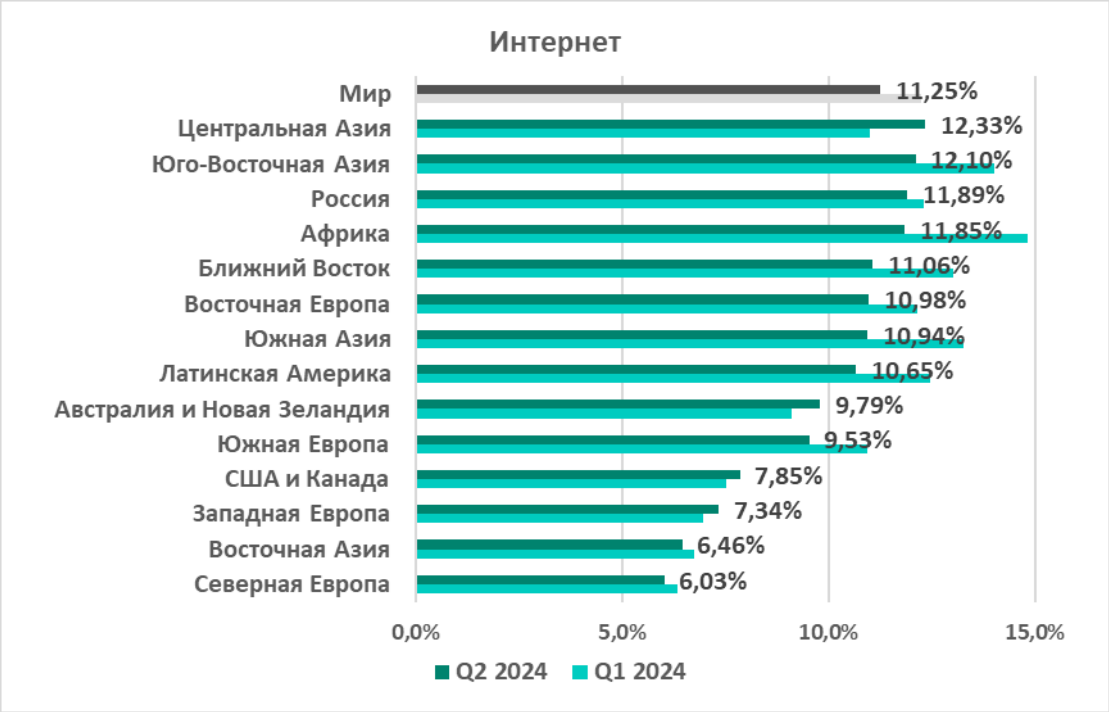
Источники угроз

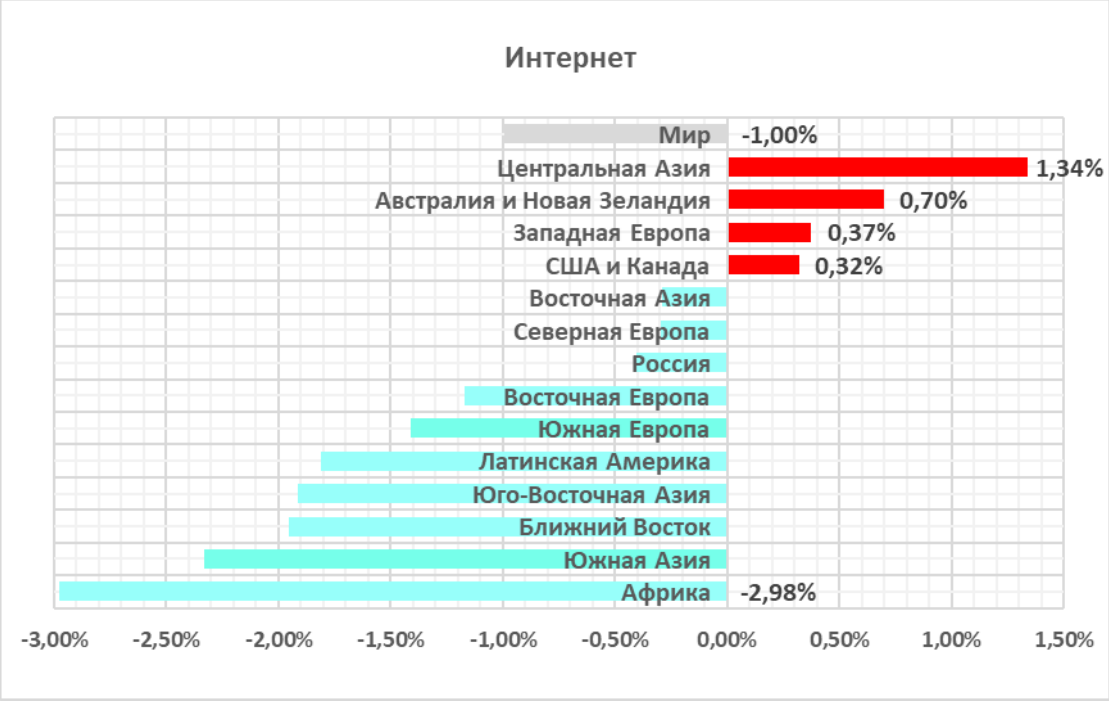
На графиках ниже представлены **рейтинги регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО**

из определенного источника во втором квартале 2024 года, и изменения процента по сравнению с предыдущим кварталом.

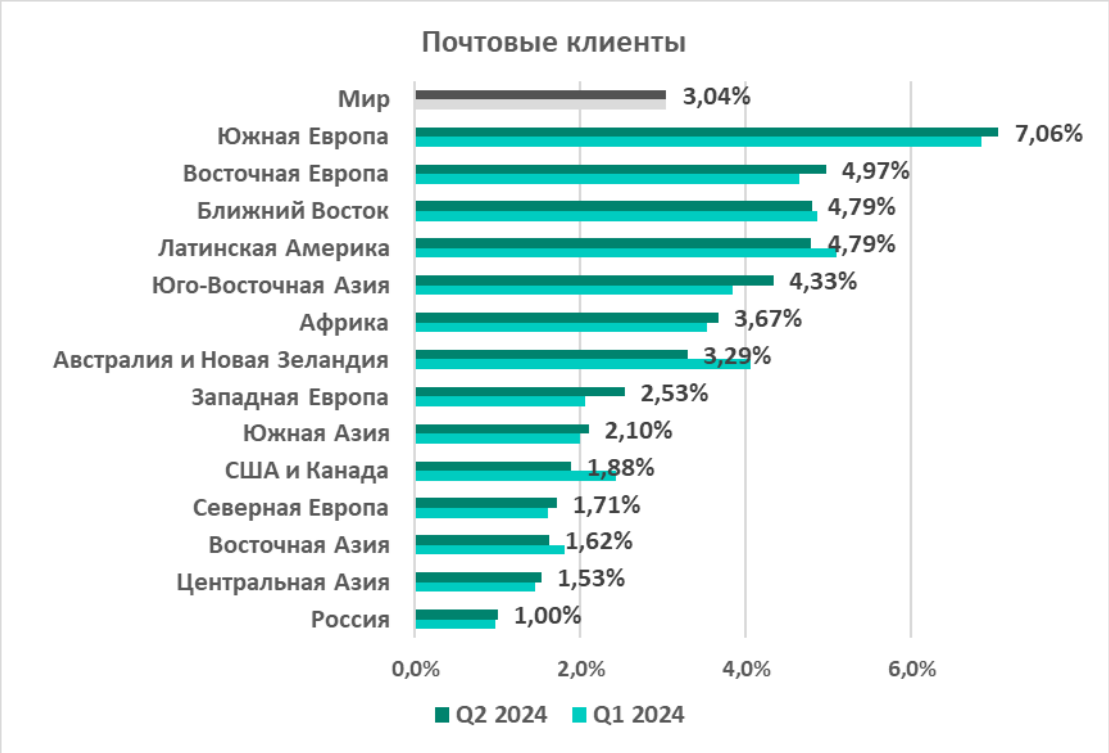
Отметим, что достоверно определить источник вредоносного ПО удается не во всех случаях.

Интернет

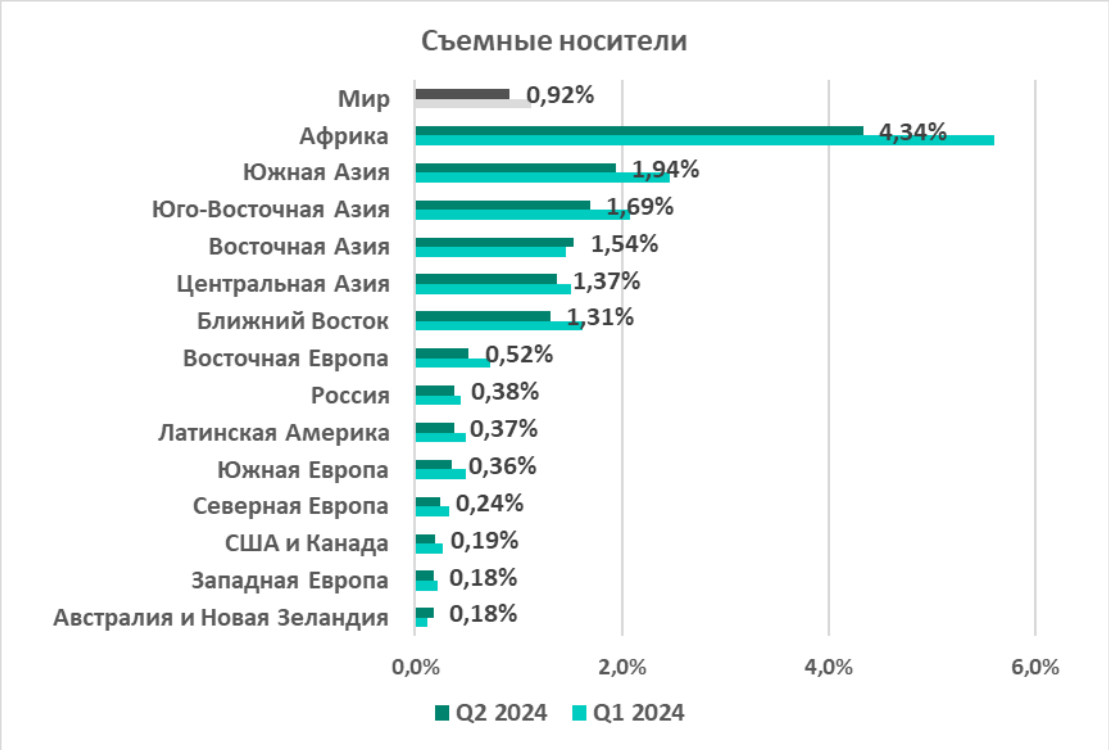


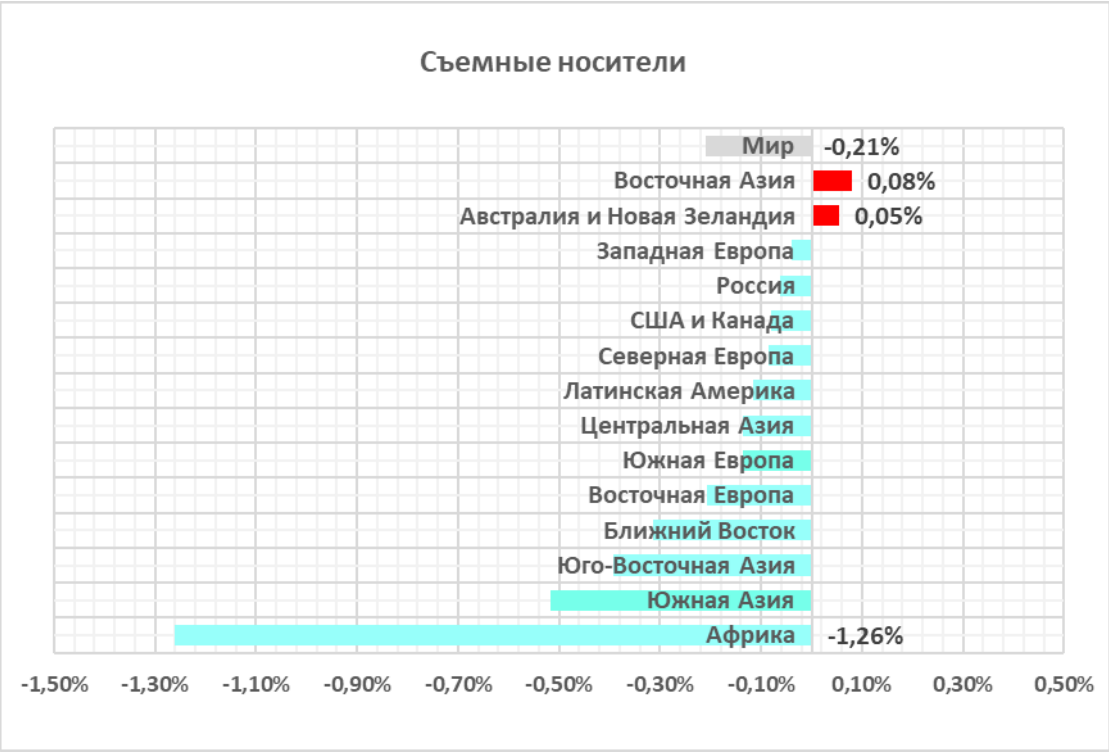


Почтовые клиенты

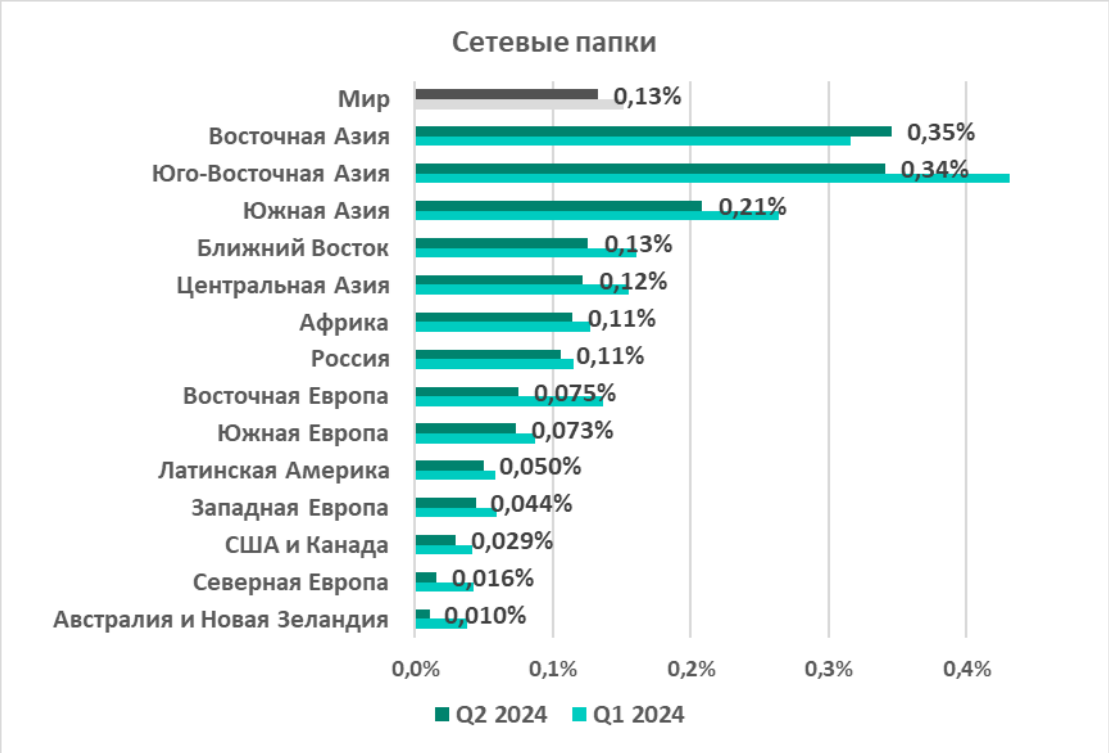


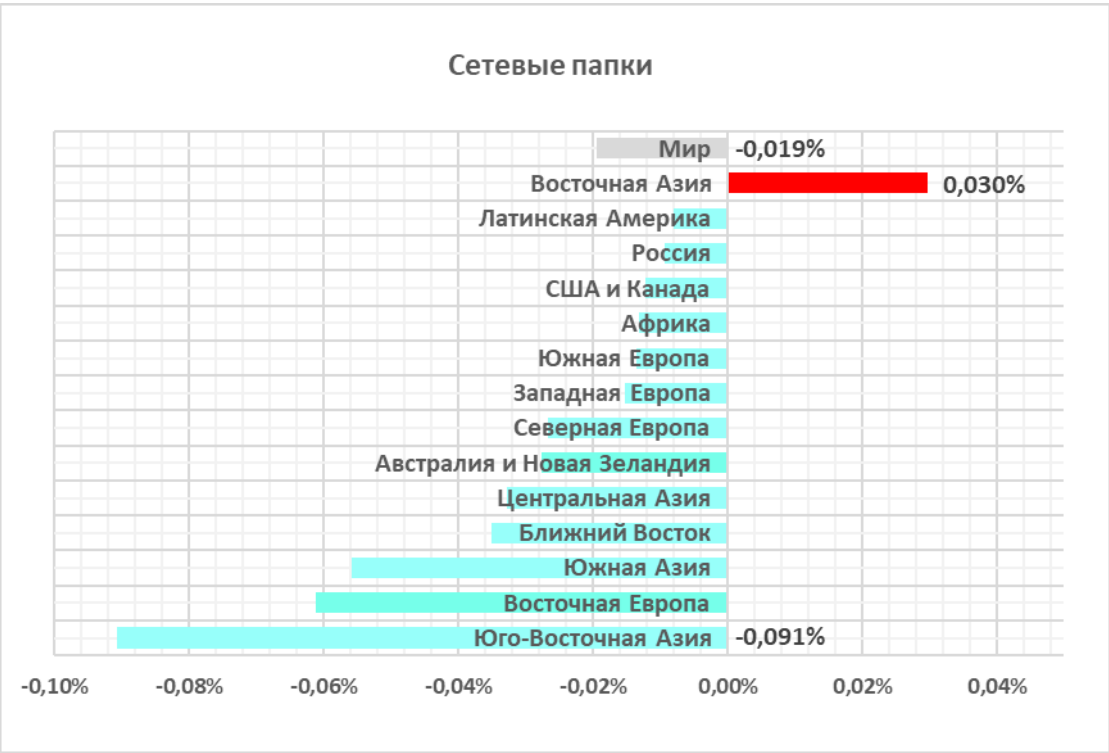
Съемные носители





Сетевые папки





Россия. Особенности

Основные угрозы

Угрозы из интернета
11,89%
▼ снижение в Q2
- 3-е место в мире
- в 1,2 раза выше среднего по миру

Ресурсы в интернете из списка запрещенных
7,8%
▲ рост в Q2
- 1-е место в мире
- в 1,2 раза выше среднего по миру

Вредоносные скрипты и фишинговые страницы
4,53%
▼ снижение в Q2
- сильный нисходящий тренд с Q1 2023

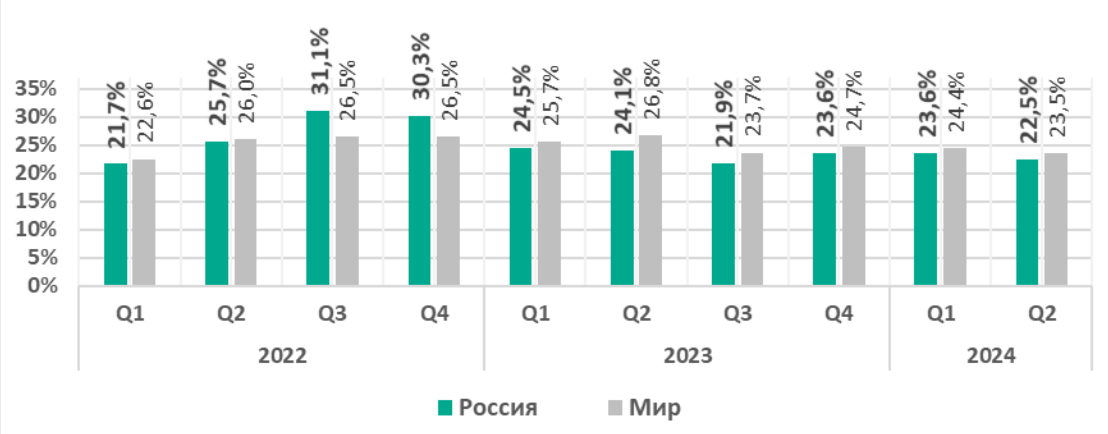
Шпионские программы
2,31%
▼ снижение в Q2
- нисходящий тренд с Q2 2023

Майнеры — исполняемые файлы
1,18%
▼ снижение в Q2
- 2 место в мире
- в 1,3 раза выше среднего по миру

Общая ситуация

Шестое место в мировом рейтинге по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты.

За исключением третьего и четвертого кварталов 2022 года, в России процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного ниже, чем в среднем по миру.



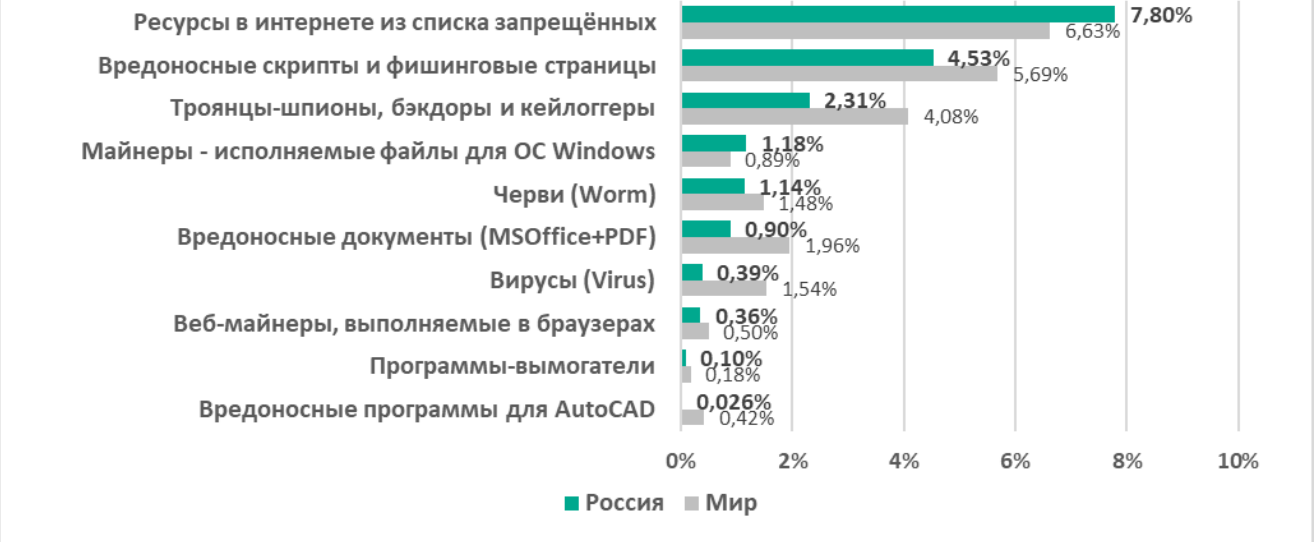
Сравнительный анализ

- Россия находится в числе лидеров среди регионов по проценту компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - 1-е место — интернет-ресурсы из списка запрещенных
  - 2-е место — майнеры — исполняемые файлы для ОС Windows
  - 3-е место — угрозы из интернета

Категории угроз

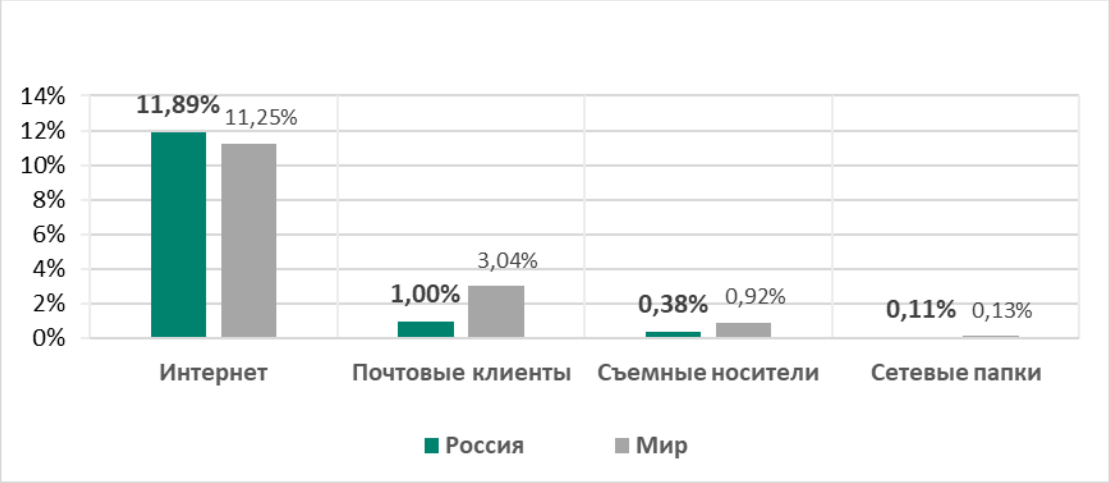
По сравнению с мировыми показателями, в России выше доля компьютеров АСУ, на которых заблокированы следующие угрозы:

- Интернет-ресурсы из списка запрещенных — в 1,2 раза
- Майнеры — исполняемые файлы для ОС Windows — в 1,3 раза



Источники угроз

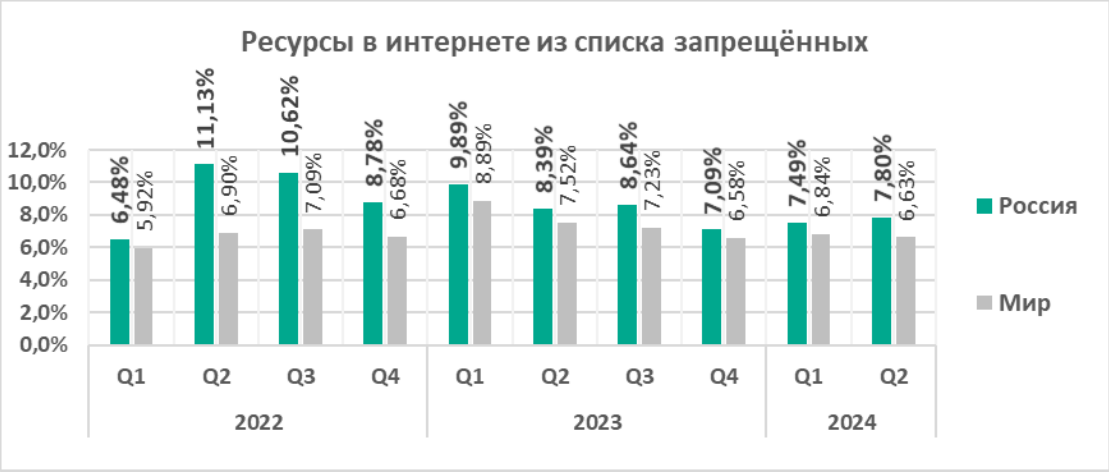
Россия занимает третье место в мире по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, с показателем, незначительно превышающим средний по миру.



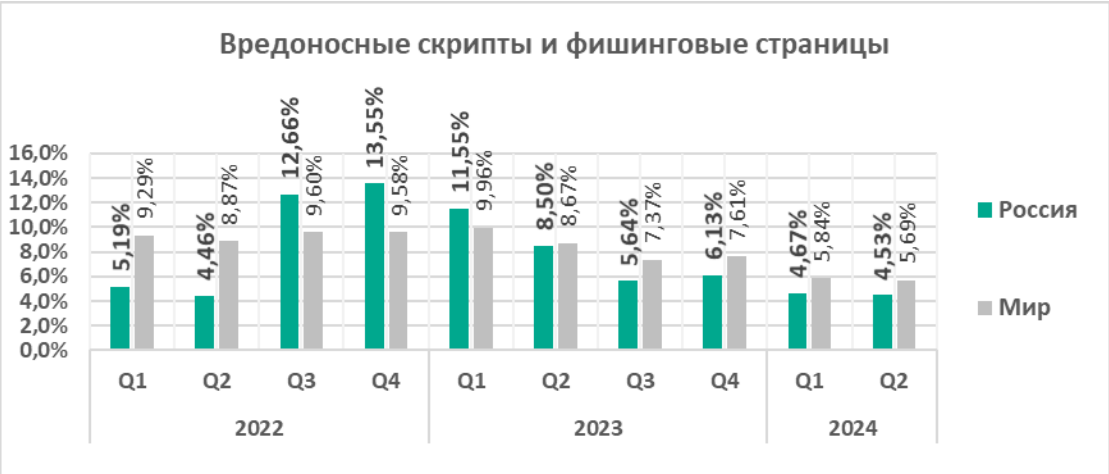
Изменения за квартал и тренды

Категории угроз

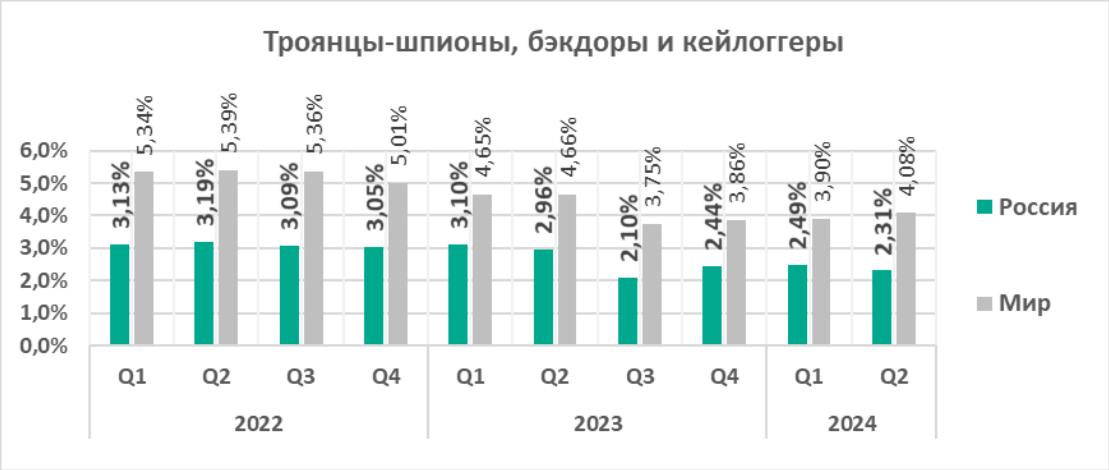
- По сравнению с предыдущим кварталом наиболее существенно выросли доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - **Вредоносные документы** — в 1,2 раза.
  - **Вредоносные программы для AutoCAD** — в 1,2 раза.
- Ведущие категории угроз показывают разнонаправленную динамику за квартал:
  - **Интернет-ресурсы из списка запрещенных —** колеблющийся нисходящий тренд, в основном соответствующий мировому тренду, с показателями выше средних по миру.



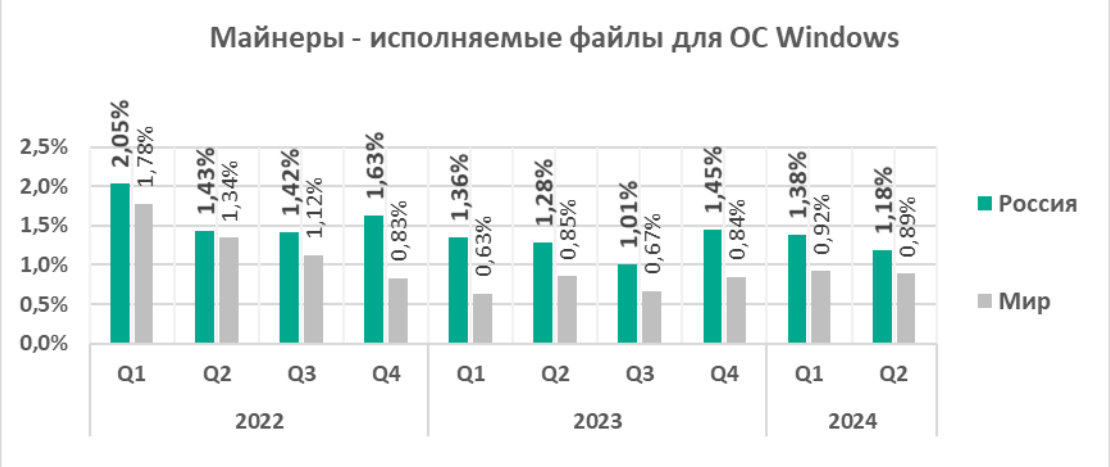
  - **Вредоносные скрипты и фишинговые страницы** — сильный нисходящий тренд с первого квартала 2023 года, в основном соответствующий мировому тренду, с показателями ниже средних по миру, за исключением последних двух кварталов 2022 года и начала 2023 года.



- **Шпионские программы** — медленный нисходящий тренд, отчасти расходящийся с мировым трендом, с показателями значительно ниже средних по миру.



- **Майнеры — исполняемые файлы для ОС Windows** — колеблющийся нисходящий тренд, преимущественно совпадающий с мировым трендом, с показателями выше средних по миру. Такие майнеры занимают четвертое место в региональном рейтинге по проценту компьютеров АСУ, на которых они были заблокированы (в сравнении с седьмым местом в мировом рейтинге).



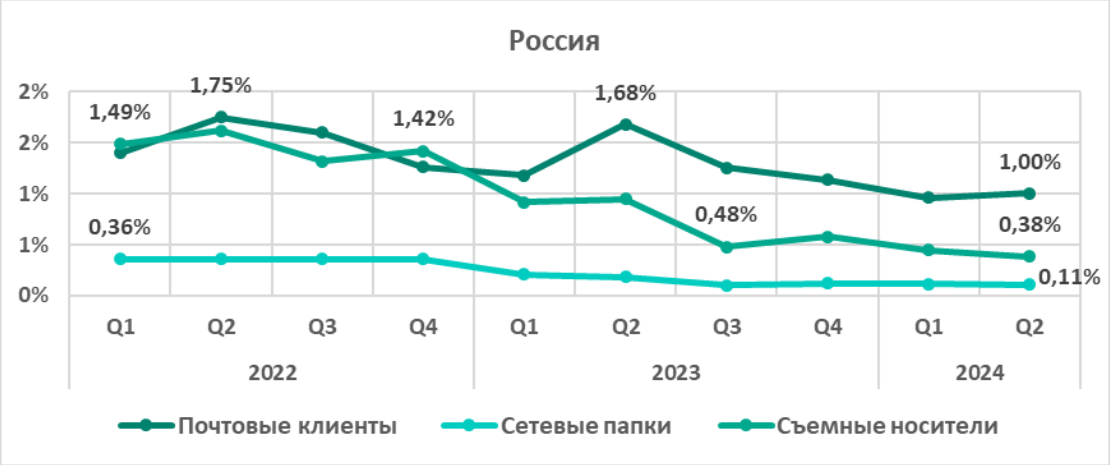
- Тепловая карта ниже иллюстрирует изменения в рейтингах категорий угроз в России за 2,5 года. Интернет-ресурсы из списка запрещенных — ведущая категория угроз в регионе, начиная с третьего квартала 2023 года.

	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Ресурсы в интернете из списка запрещённых	1	1	2	2	2	2	1	1	1	1
Вредоносные скрипты и фишинговые страницы	2	2	1	1	1	1	2	2	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	3	3	3
Майнеры — исполняемые файлы для ОС Windows	4	5	4	4	4	5	5	4	4	4
Черви (Worm)	5	6	6	5	5	7	6	5	5	5
Вредоносные документы (MSOffice+PDF)	7	4	5	7	7	4	4	6	6	6
Вирусы (Virus)	8	8	8	8	8	8	8	8	7	7
Веб-майнеры, выполняемые в браузерах	6	7	7	6	6	6	7	7	8	8
Программы-вымогатели	9	9	9	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	10

Источники угроз

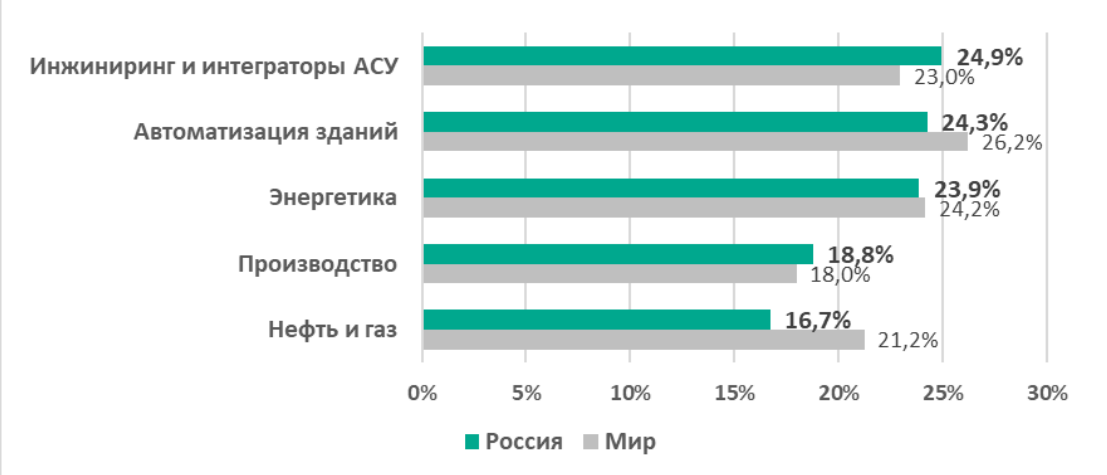
- Угрозы из интернета (по доле компьютеров АСУ, на которых они были заблокированы) демонстрируют с четвертого квартала 2022 года нисходящий тренд. Начиная со второго квартала 2023 года показатель остается близким к среднемировому показателю.

- Другие источники угроз также демонстрируют преимущественно нисходящие тренды.

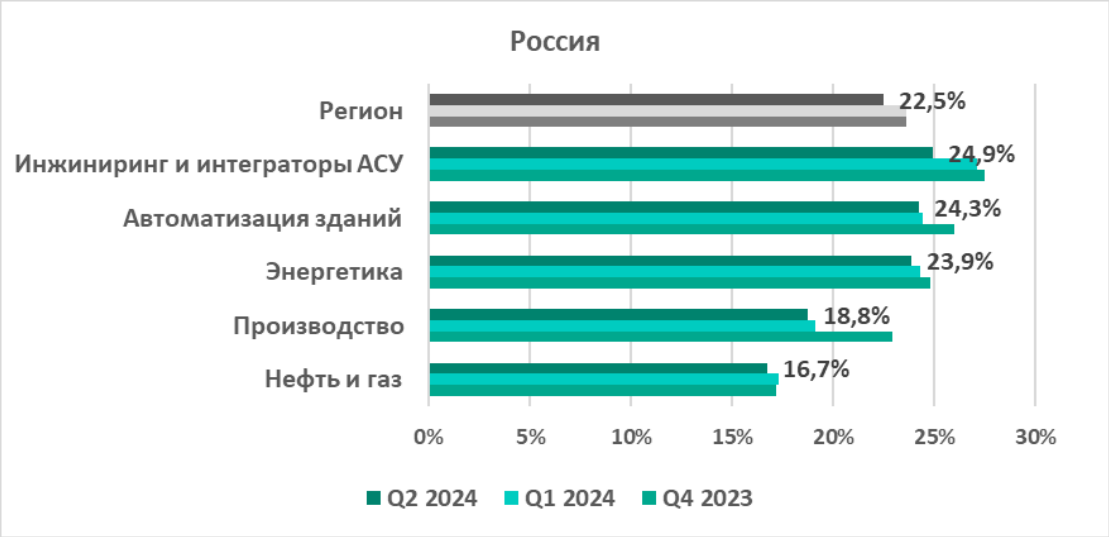


Отрасли

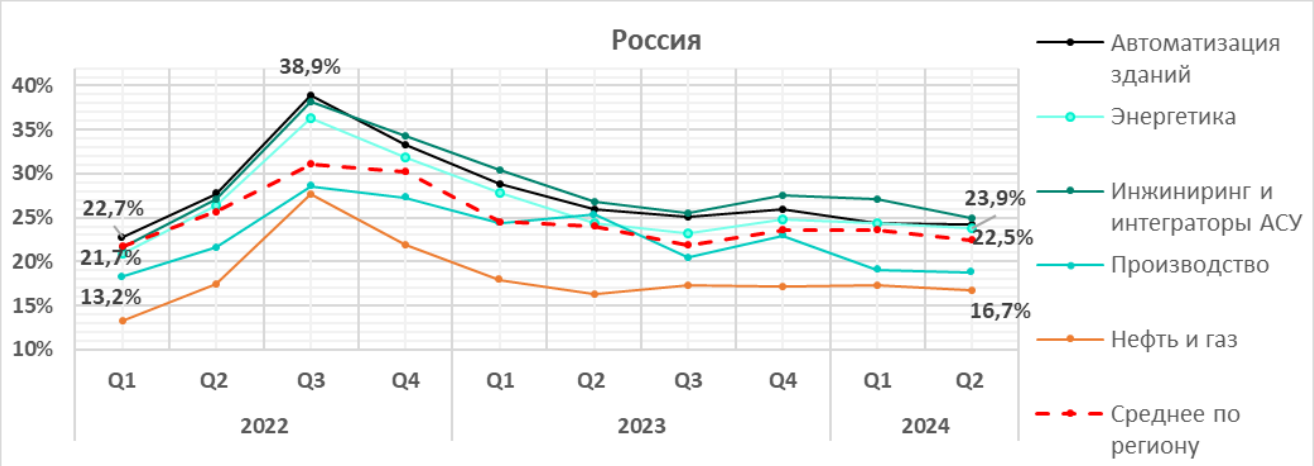
- **Наиболее подверженные угрозам отрасли** в регионе среди исследуемых в данном отчете:
  - инжиниринг и интеграторы АСУ
  - автоматизация зданий
  - энергетика
- **В сравнении с соответствующими среднемировыми показателями** более высокий процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в следующих отраслях:
  - инжиниринг и интеграторы АСУ — в 1,1 раза
  - производство



- **Во втором квартале 2024 года** во всех исследуемых отраслях в регионе наблюдалось снижение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты.



- Начиная с четвертого квартала 2022 года, **долгосрочные тренды** в отраслях в целом демонстрируют позитивную **динамику**.



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 даёт нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счёт обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за её объёма и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные в значительной мере не только 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 систем автоматизации зданий
- серверы хранения данных (Historian)
- шлюзы данных (OPC)
- стационарные рабочие станции инженеров и операторов
- мобильные рабочие станции инженеров и операторов
- человеко-машинный интерфейс (HMI)
- компьютеры, используемые для администрирования технологических сетей и сетей систем автоматизации зданий
- компьютеры, используемые для программирования АСУ/ПЛК

[1] Организациям, в отношении любых данных которых наложены ограничения на их передачу во вне периметра организации, рекомендуем рассмотреть вариант использования сервиса Kaspersky Private Security Network.

Компьютеры, участвующие в статистике, принадлежат организациям из различных отраслей. Наиболее распространены химическая промышленность, металлургия, проектирование и интеграция АСУ, нефть и газ, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность, фармацевтика. Сюда также входят системы от инжиниринговых и интеграционных фирм, которые работают с предприятиями в различных 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, квартал, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете процента 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», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com