Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первый квартал 2024 — регионы

27.05.2024

Version 1.1

Цифры квартала 2
Все угрозы 2
Категории вредоносного ПО 3
Регионы. Рейтинги 8
Процент атакованных компьютеров АСУ 8
Категории вредоносных объектов 9
Источники угроз 20
Регионы. Некоторые особенности 22
Африка 23
Юго-Восточная Азия 29
Ближний Восток 32
Центральная Азия 37
Восточная Европа 40
Россия 44
Латинская Америка 47
Южная Азия 52
Южная Европа 56
Восточная Азия 60
Австралия и Новая Зеландия 64
США и Канада 68
Западная Европа 72
Северная Европа 74

Цифры квартала

Все угрозы

В мире в первом квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с предыдущим кварталом на 0,3 п.п. и составил 24,4%.

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

Больше 25%:

- Африка — 32,4%
- Юго-Восточная Азия — 29,7%
- Ближний Восток — 26,9%
- Центральная Азия — 26,8%

В регионах из этой группы кибербезопасность АСУ ТП требует пристального внимания и улучшения.

20 — 25%

- Восточная Европа — 24,7%
- Россия — 23,6%
- Латинская Америка — 23,5%
- Южная Азия — 23,5%
- Южная Европа — 21,4%
- Восточная Азия — 20,3%

До 20%

- Австралия и Новая Зеландия — 16,2%
- США и Канада — 13,3%
- Западная Европа — 12,3%
- Северная Европа — 11,5%

В третьей группе регионы, наиболее благополучные по критерию кибербезопасности.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал увеличился только в двух лидирующих по этому показателю регионах: в Африке (на 1,2 п.п.) и в Юго-восточной Азии (на 0,2 п.п.).

Категории вредоносного ПО

Вредоносные объекты, используемые для первичного заражения

Вредоносные объекты, которые используются для первичного заражения компьютеров, — опасные ресурсы в интернете, которые попадают в списки запрещённых, вредоносные скрипты и фишинговые страницы, вредоносные документы.

Логика атак злоумышленников предполагает, что такие вредоносные объекты активно распространяются. Как результат, они чаще остальных блокируются защитными решениями. Это отражается и в нашей статистике.

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

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

Угрозы из интернета

- Африка — 14,82%
- Юго-Восточная Азия — 14,01%

Угрозы из почты

- Южная Европа — 6,85%
- Латинская Америка — 5,09%

Ресурсы в интернете из списка запрещённых

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещённых, лидируют:

- Африка — 8,78%
- Россия — 7,49%
- Южная Азия — 7,48%

Вредоносные скрипты и фишинговые страницы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидируют:

- Латинская Америка — 7,23%
- Южная Европа — 6,96%
- Ближний Восток — 6,95%

Вредоносные документы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные документы, лидируют:

- Южная Европа — 3,24%
- Латинская Америка — 2,94%
- Восточная Европа — 2,33%

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.

Среди майнеров, предназначенных для запуска на ОС Windows, одними из наиболее распространённых являются майнеры, распространяемые злоумышленниками в форме инсталляционных NSIS файлов с легитимным ПО.

Шпионское ПО

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

Среди регионов в тройке лидеров по проценту компьютеров АСУ, на которых были заблокированы программы-шпионы, оказались регионы, лидирующие по вредоносному ПО из первой группы:

- Африка — 6,65%
- Ближний Восток — 5,89%
- Южная Европа — 5,45%

Почти во всех регионах в рейтингах категорий угроз по проценту компьютеров АСУ, на которых они были заблокированы,

шпионские программы не поднимаются выше третьего места. За исключением двух регионов:

- **Восточная Азия — в регионе программы-шпионы на первом месте в рейтинге категорий вредоносного ПО** по проценту компьютеров АСУ, на которых они были заблокированы — 3,68%.
- **Центральная Азия** — в регионе в аналогичном рейтинге программы-шпионы **на втором месте** — 4,40%.

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

- Центральная Азия — 1,78%
- Россия — 1,38%
- Восточная Европа — 1,06%

В мире в рейтингах категорий угроз по проценту компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows на седьмом месте.

- В России в аналогичном рейтинге они на четвертом месте.
- В Центральной Азии — на пятом.

Отметим, что в первом квартале 2024 года процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, увеличился во всех регионах, кроме России и Центральной Азии.

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

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, лидируют

- Африка — 0,91%
- Ближний Восток — 0,84%
- Австралия и Новая Зеландия — 0,78%

В региональных рейтингах категорий угроз по проценту компьютеров АСУ, на которых они были заблокированы, веб-майнеры оказались на пятом месте (в мире — на восьмом) в регионах:

- Австралия и Новая Зеландия — 0,78%
- США и Канада — 0,45%
- Северная Европа — 0,27%

В первом квартале 2024 года процент компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, увеличился во всех регионах, кроме России и Центральной Азии.

Программы-вымогатели

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, в регионах:

- Ближний Восток — 0,28%
- Африка — 0,27%
- Южная Азия — 0,22%

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.

В трех регионах процент компьютеров АСУ, на которых угрозы блокируются **при подключении съемных носителей, выше, чем** процент компьютеров АСУ, на которых блокируются **угрозы из почты** (в остальных — ниже):

- Африка — 5,6% (лидирует среди регионов по этому показателю)
- Южная Азия — 2,46%
- Центральная Азия — 1,51%

Черви

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы черви, лидируют:

- Африка — 5,29%
- Центральная Азия — 2,88%
- Ближний Восток — 2,40%

В мире черви на шестой позиции в рейтинге категорий угроз по проценту компьютеров АСУ, на которых они были заблокированы. В четырех регионах в аналогичных региональных рейтингах **черви — на четвертом месте**:

- Африка — 5,29%
- Центральная Азия — 2,88%
- Ближний Восток — 2,40%
- Южная Азия — 1,95%

В топах по червям оказались регионы, которые лидируют по проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении **съемных носителей**:

- Африка — 5,6%
- Южная Азия — 2,46%

Вирусы

Среди регионов по проценту компьютеров АСУ, на которых были заблокированы вирусы, лидируют:

- Юго-Восточная Азия — 7,61%
- Африка — 4,09%
- Восточная Азия — 2,89%

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

Отметим также, что два из трех регионов в топе лидирую также по проценту компьютеров АСУ, на которых были заблокированы **угрозы в сетевых папках**.

- Юго-Восточная Азия — 0,43%
- Восточная Азия — 0,32%

Вредоносные программы для AutoCAD

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

По проценту компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, лидируют те же регионы, что и в рейтинге по вирусам:

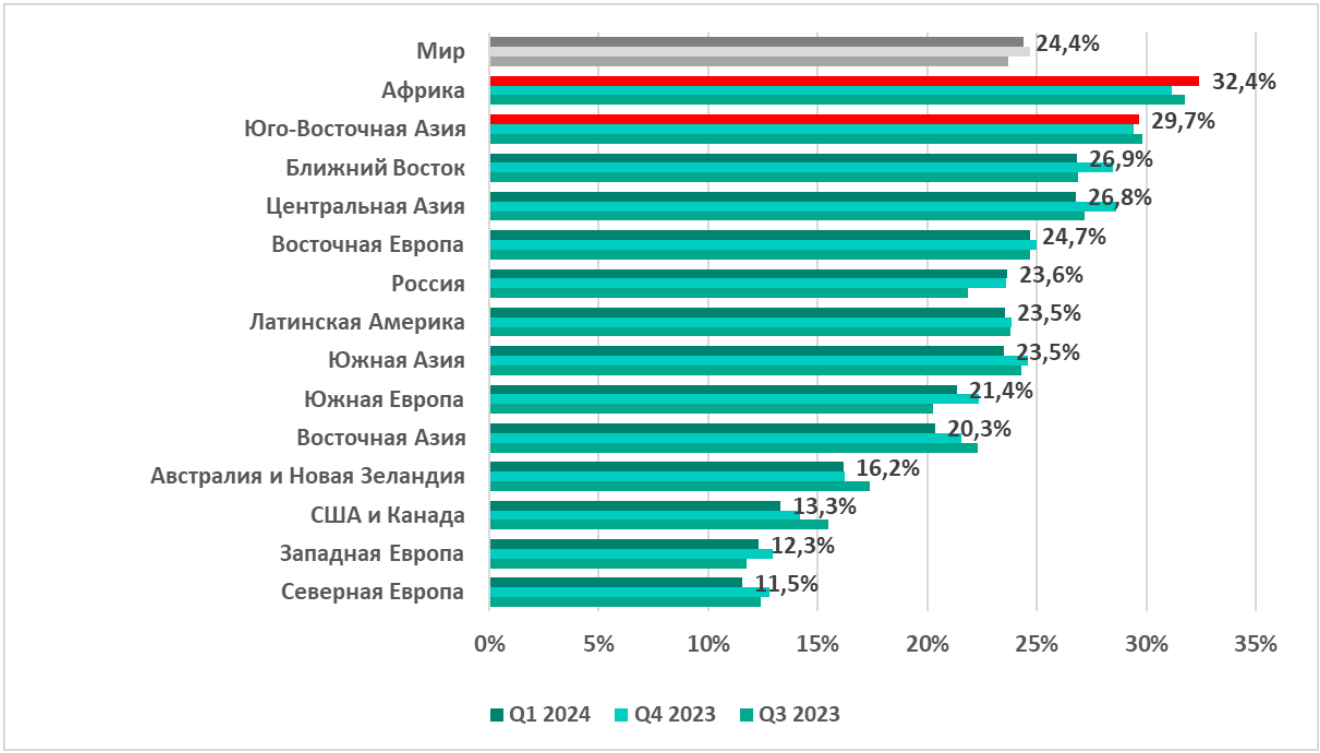
- Юго-Восточная Азия — 2,81%
- Восточная Азия — 1,49%
- Африка — 0,61%

Как правило, вредоносные программы для AutoCAD — это минорная угроза, которая занимает последние места в рейтинге категорий вредоносных объектов по проценту компьютеров АСУ, на которых они были заблокированы. В **Юго-Восточной Азии** в первом квартале 2024 года эта категория оказалась **на пятом месте**.

Регионы. Рейтинги

Процент атакованных компьютеров АСУ

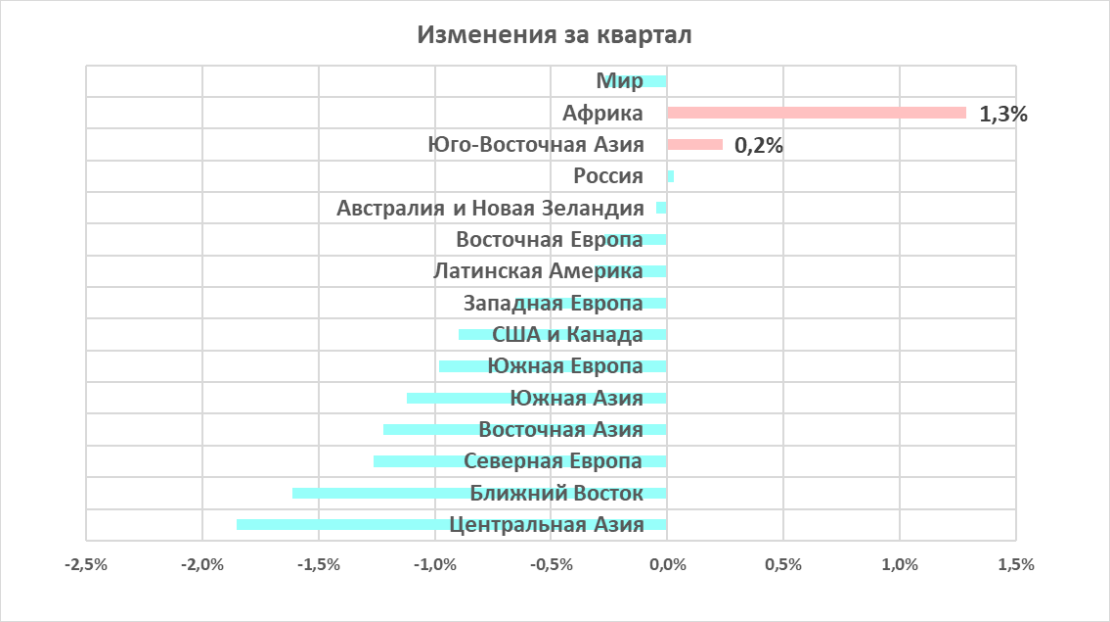
Процент компьютеров АСУ, на которых в течение квартала были заблокированы вредоносные объекты, варьирует в регионах от 34,2% в Африке до 11,5% в Северной Европе.



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

Процент увеличился по сравнению с предыдущим кварталом в двух регионах, лидирующих в рейтинге по проценту атакованных компьютеров АСУ, — в Африке и Юго-Восточной Азии.

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



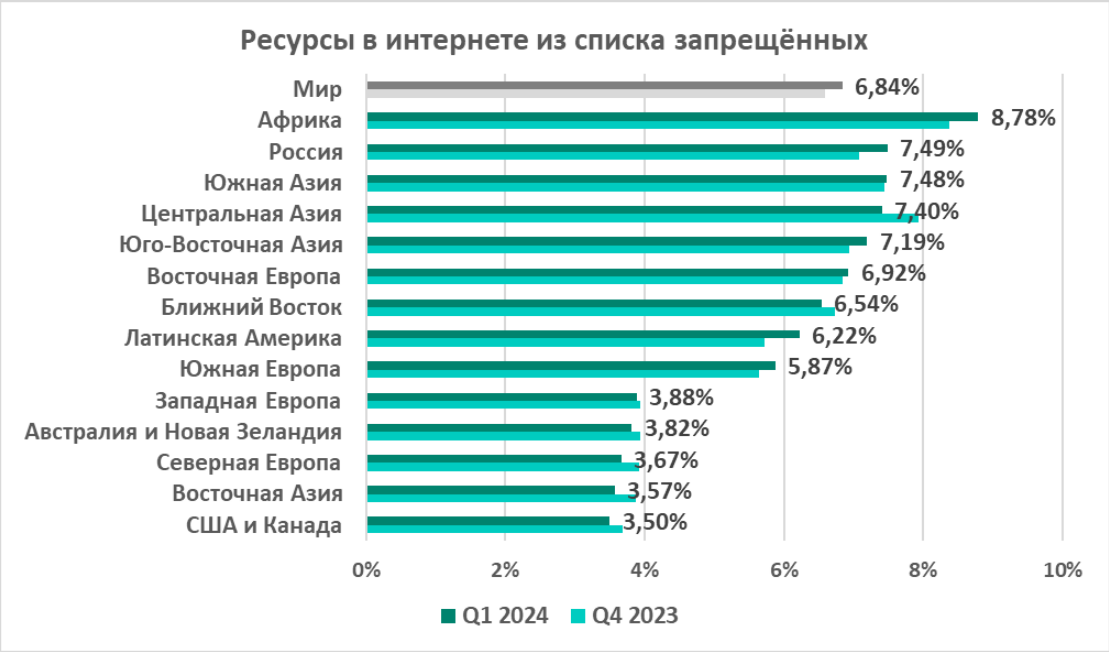
Категории вредоносных объектов

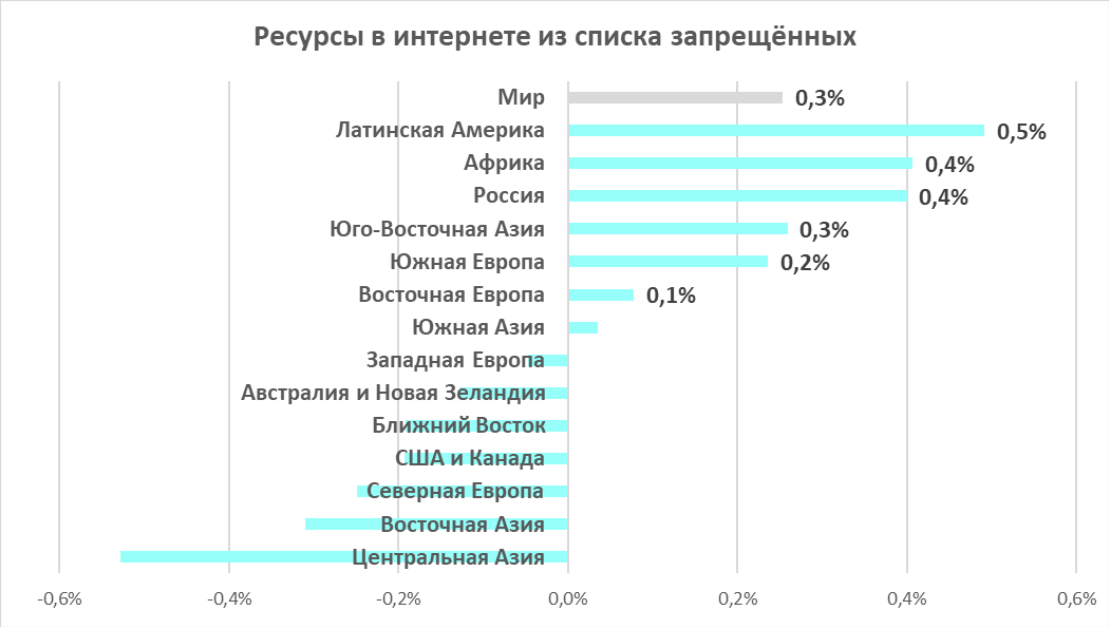
Процент компьютеров АСУ, на которых блокируется вредоносное ПО различных категорий, отличается в разных регионах. При этом позиции регионов в рейтингах по этому показателю не всегда совпадает с позицией в рейтинге по проценту компьютеров АСУ, на которых были заблокированных все угрозы.

На графиках ниже представлены рейтинги регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО определенной категории в первом квартале 2024 года.

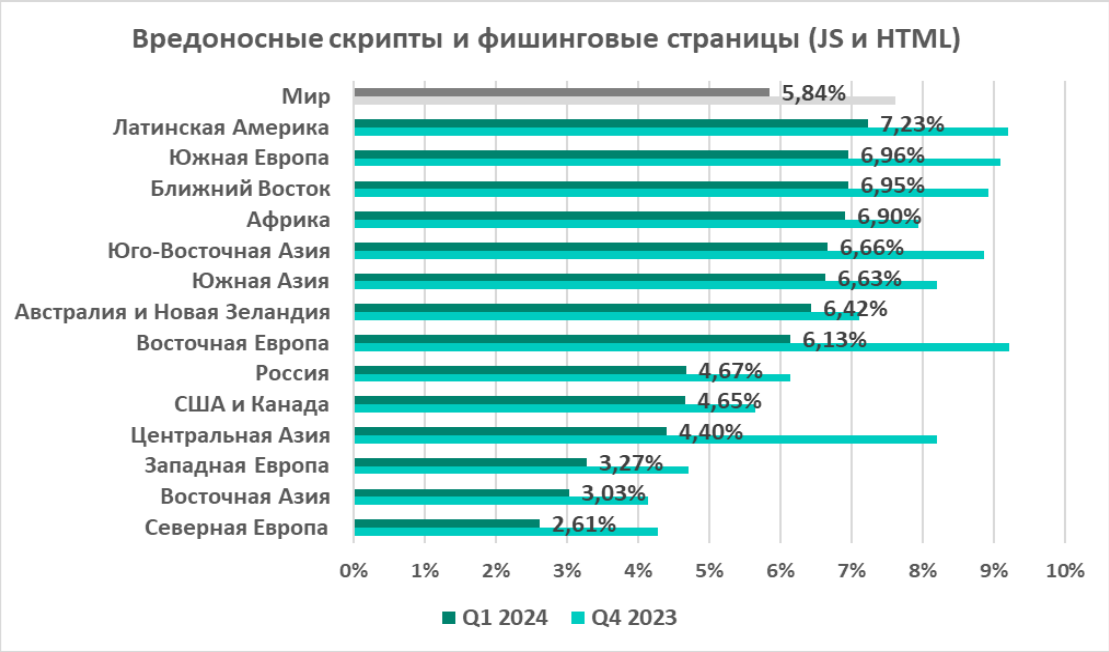
Вредоносные объекты, используемые для первичного заражения

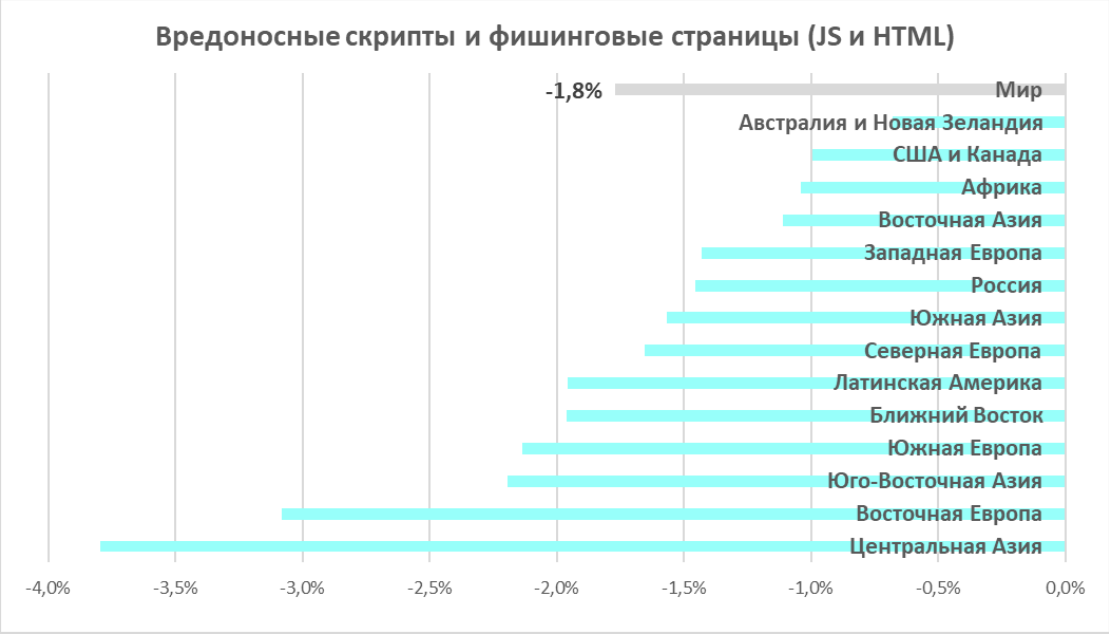
Ресурсы из интернета из списка запрещённых



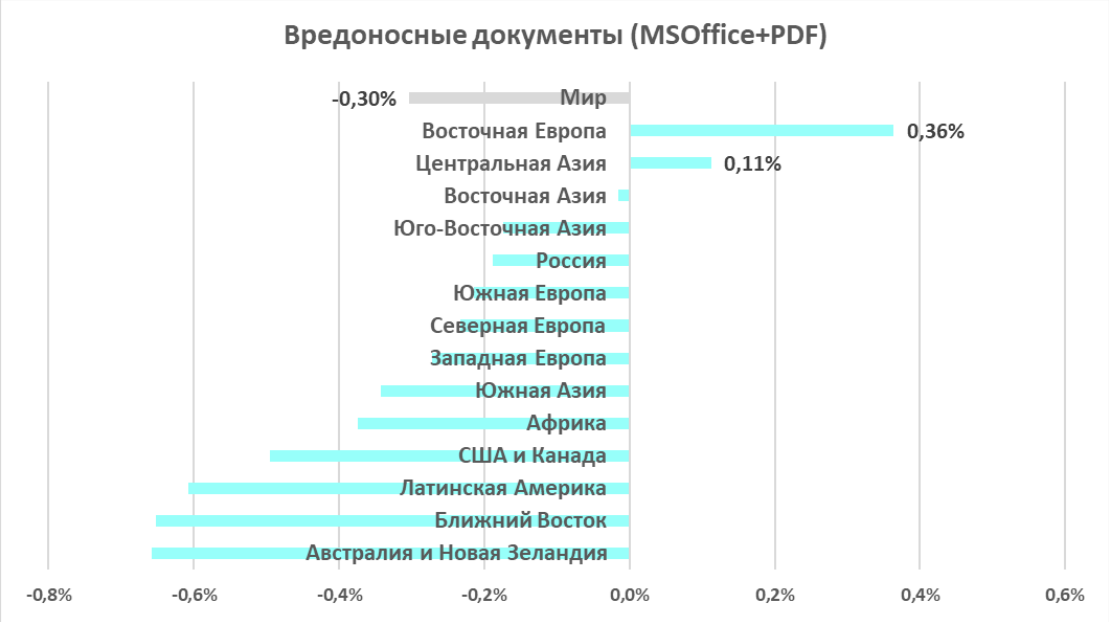


Вредоносные скрипты и фишинговые страницы (JS и HTML)



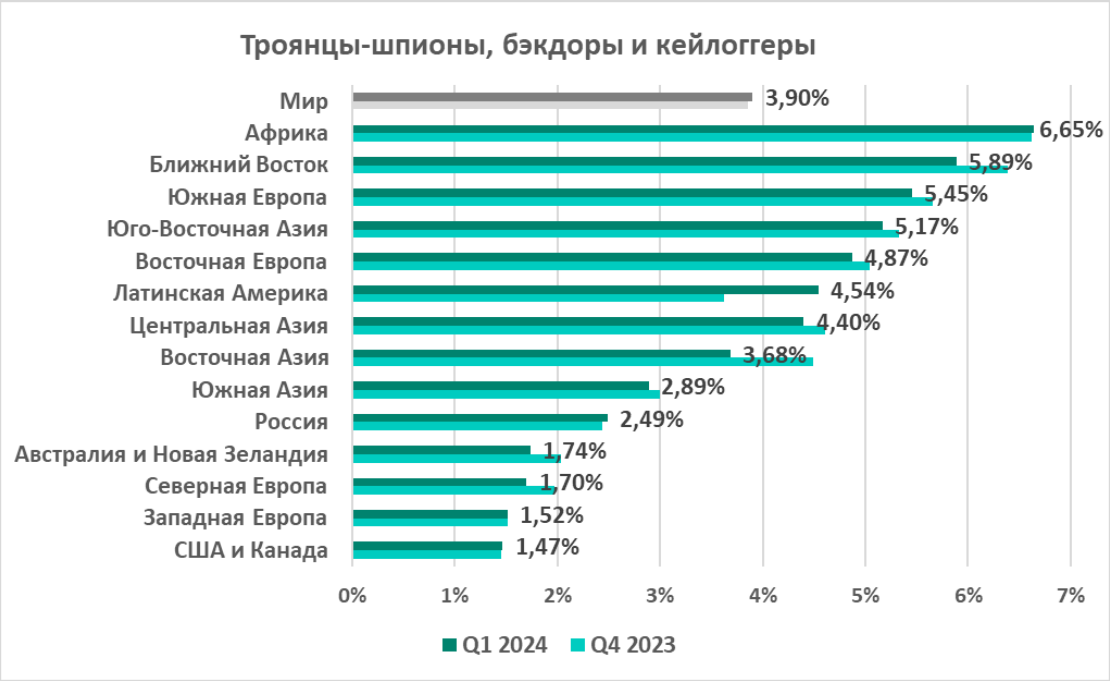


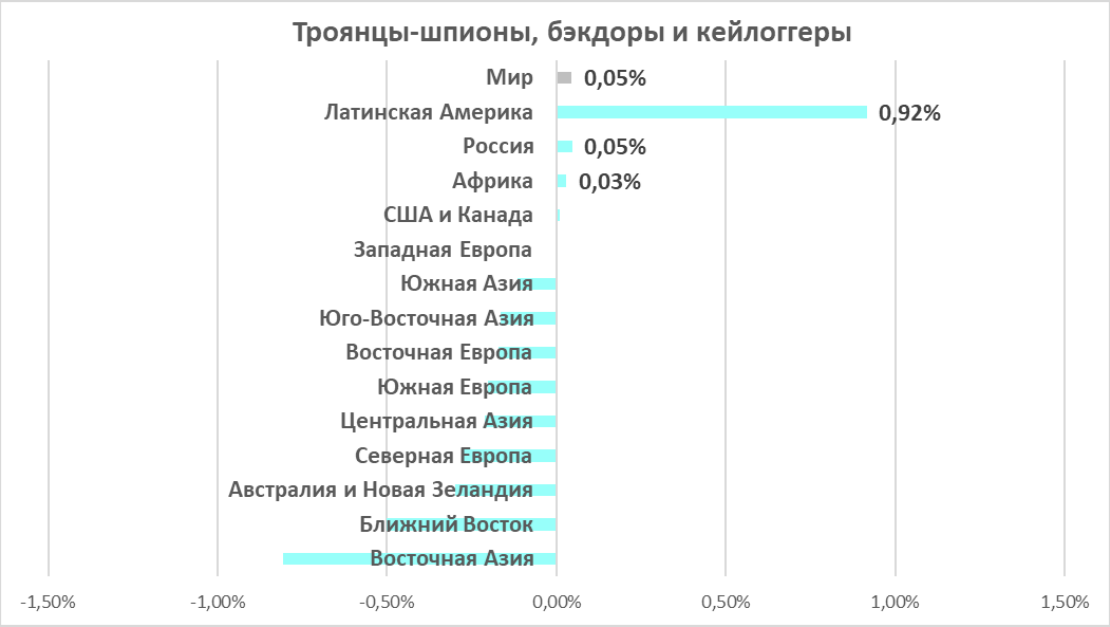
Вредоносные документы (MSOffice+PDF)



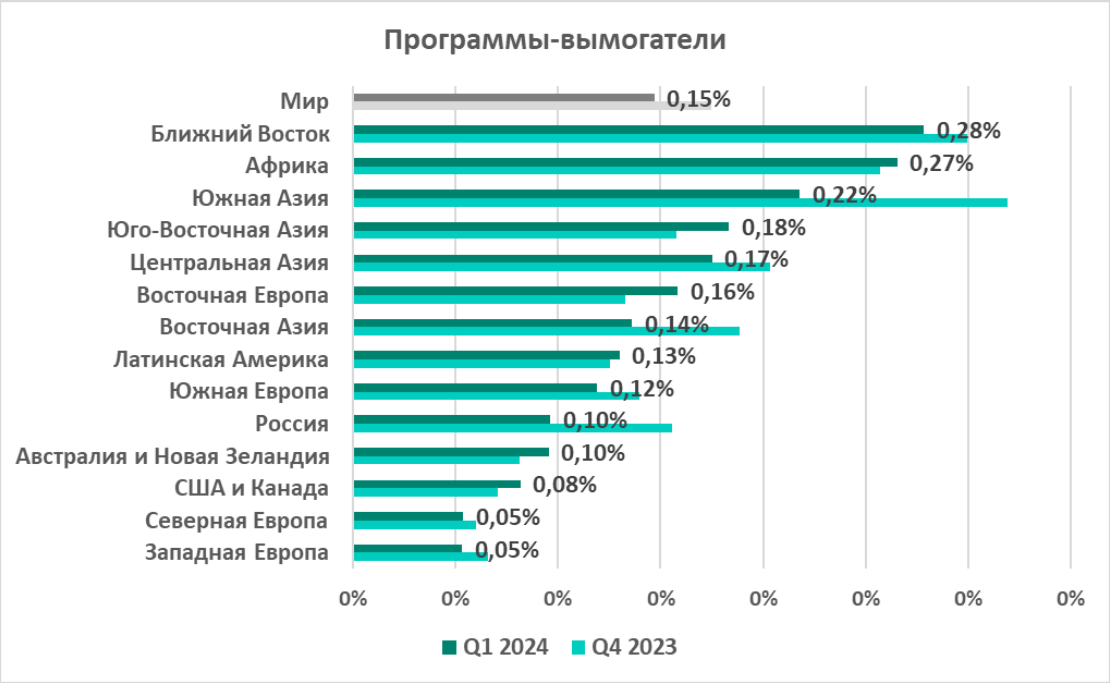
Вредоносное ПО следующего этапа

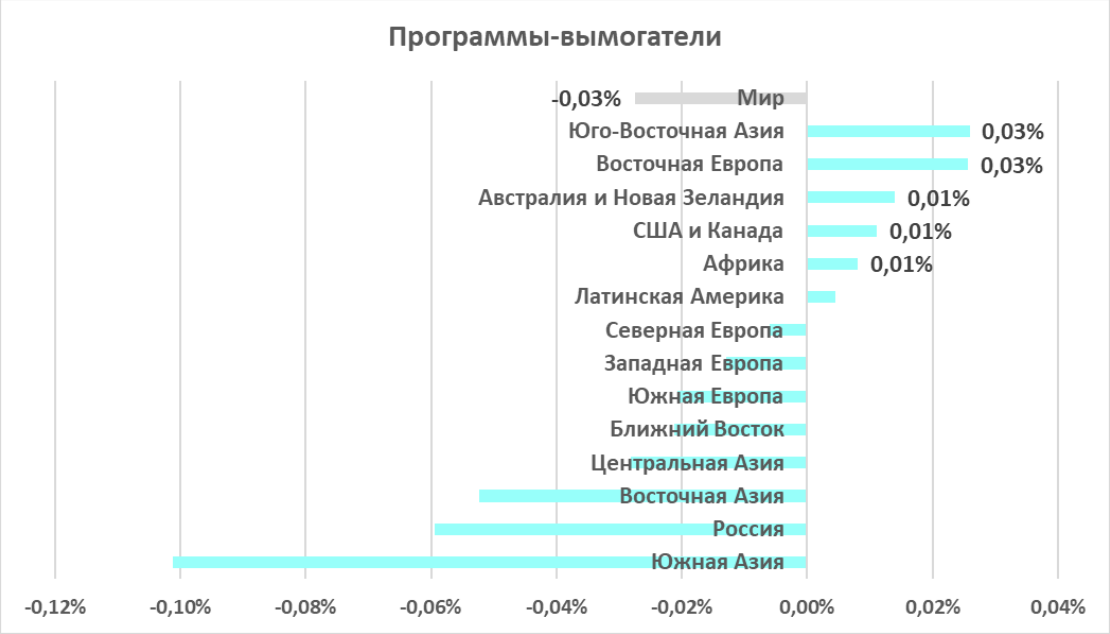
Программы-шпионы





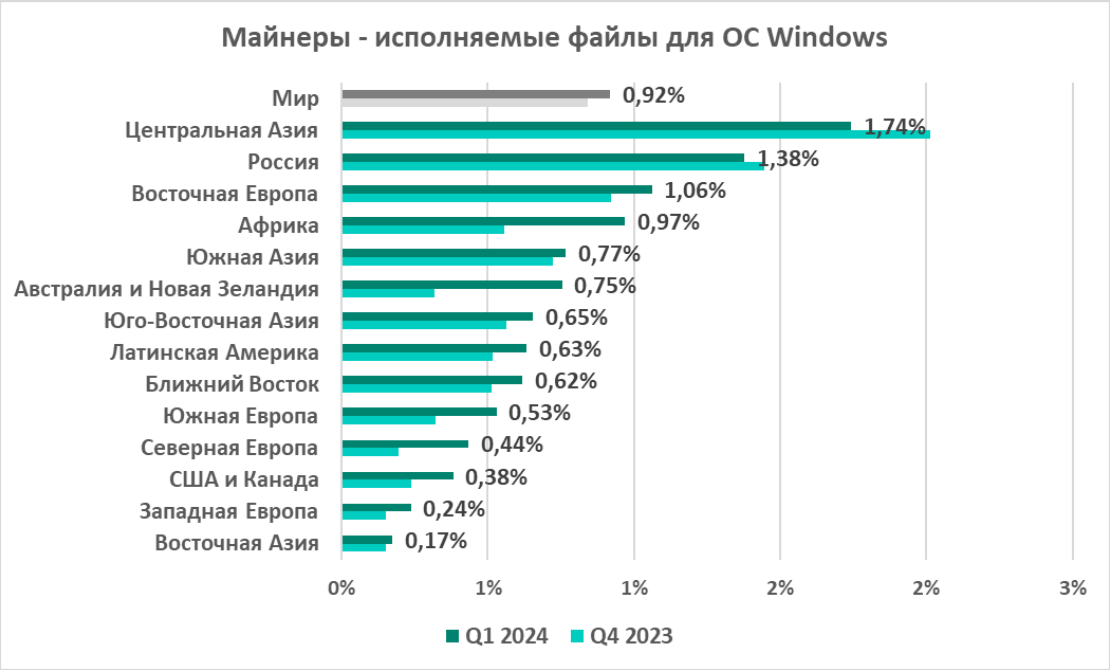
Программы-вымогатели

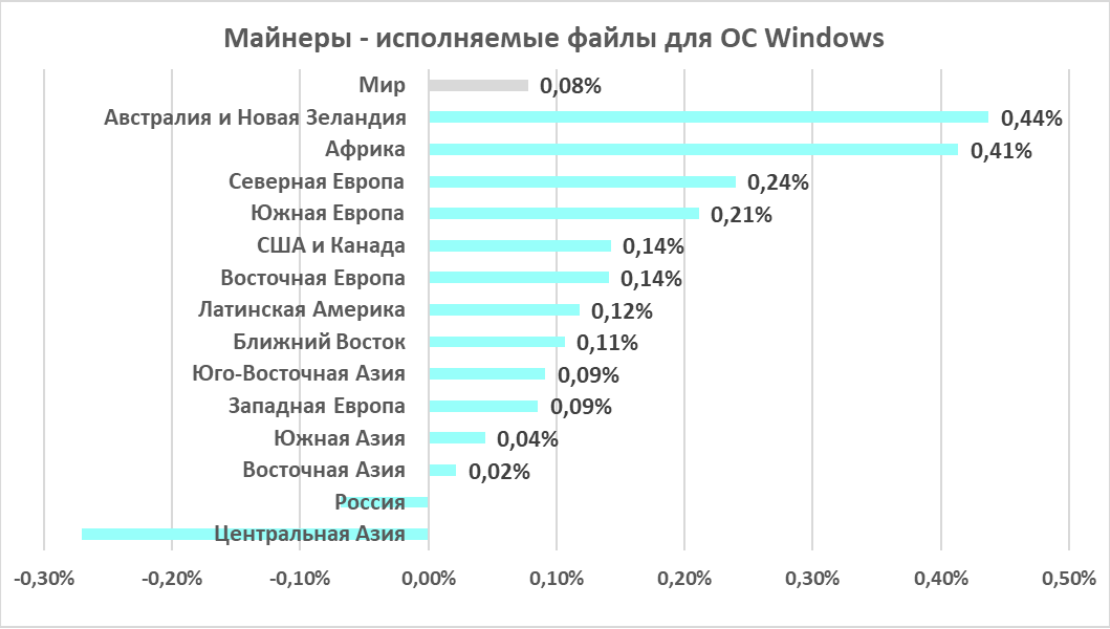




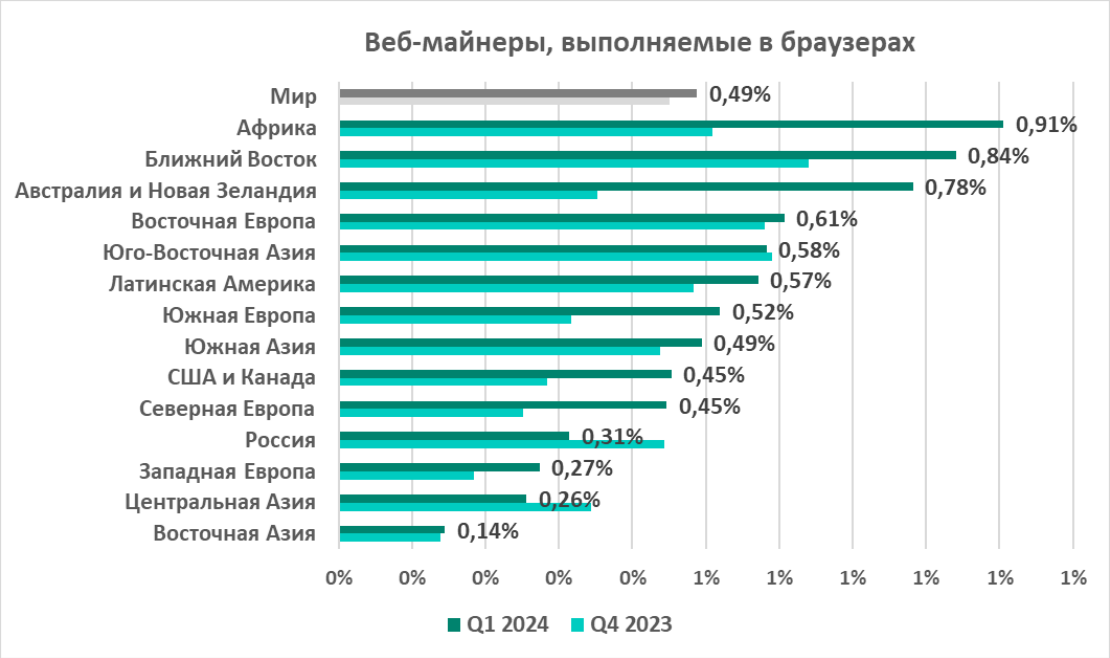
Вредоносные программы для скрытого майнинга криптовалюты

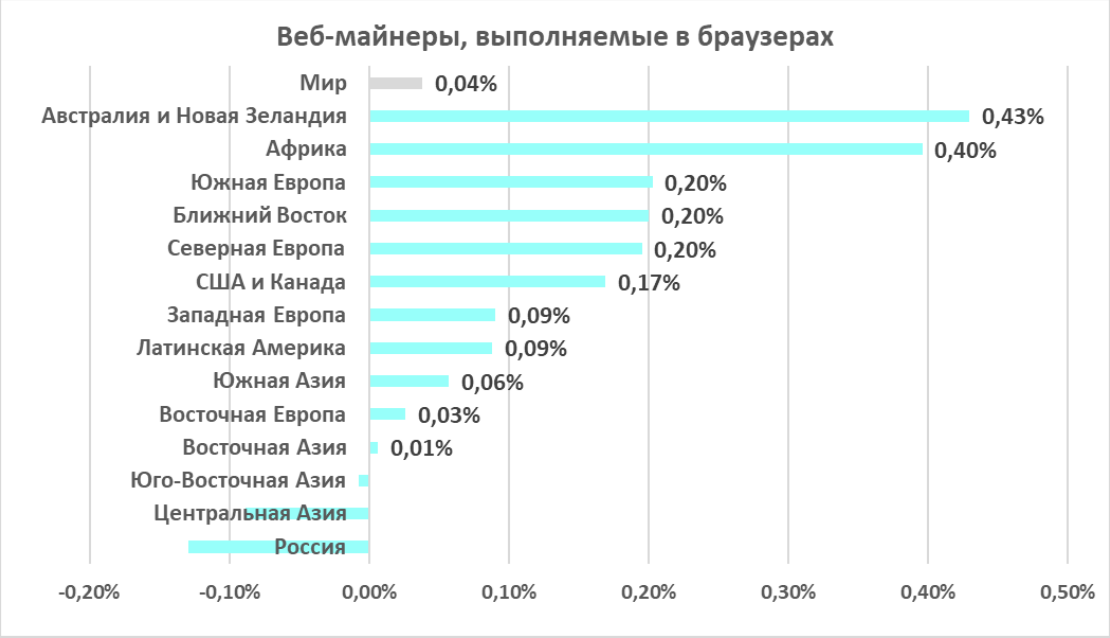
Майнеры — исполняемые файлы для ОС Windows





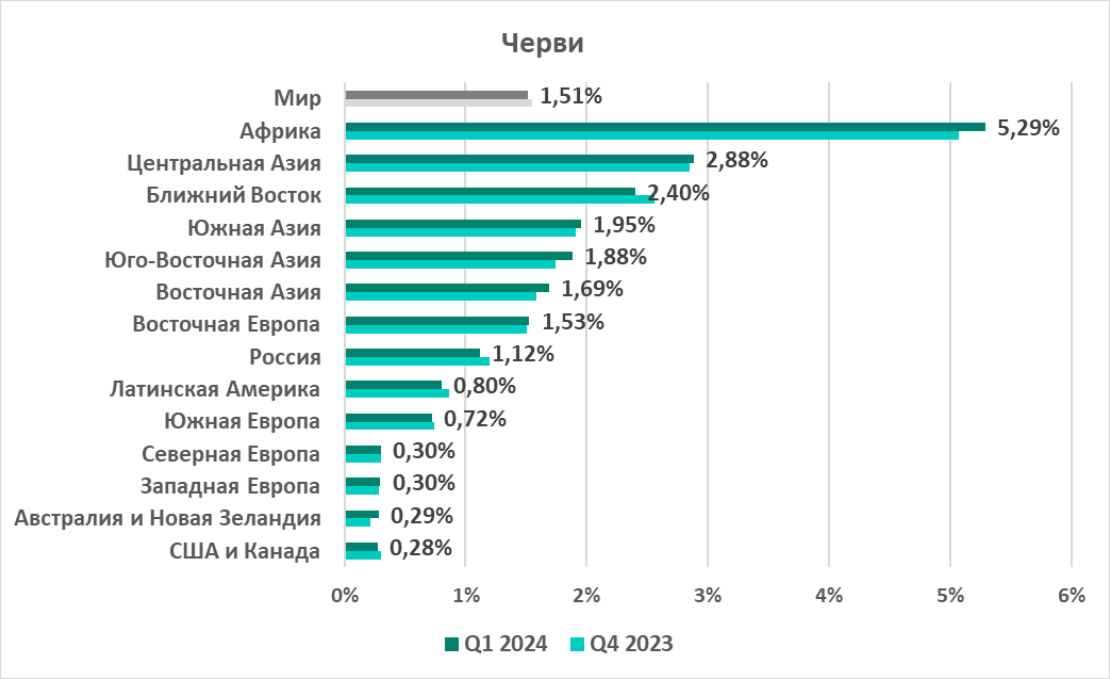
Веб-майнеры

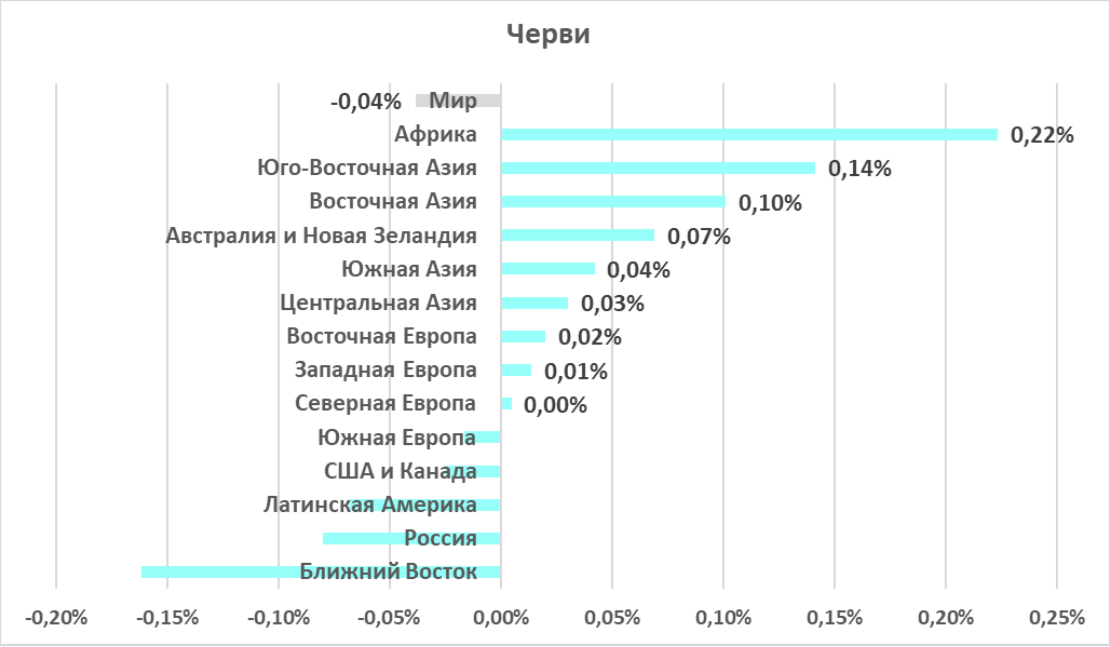




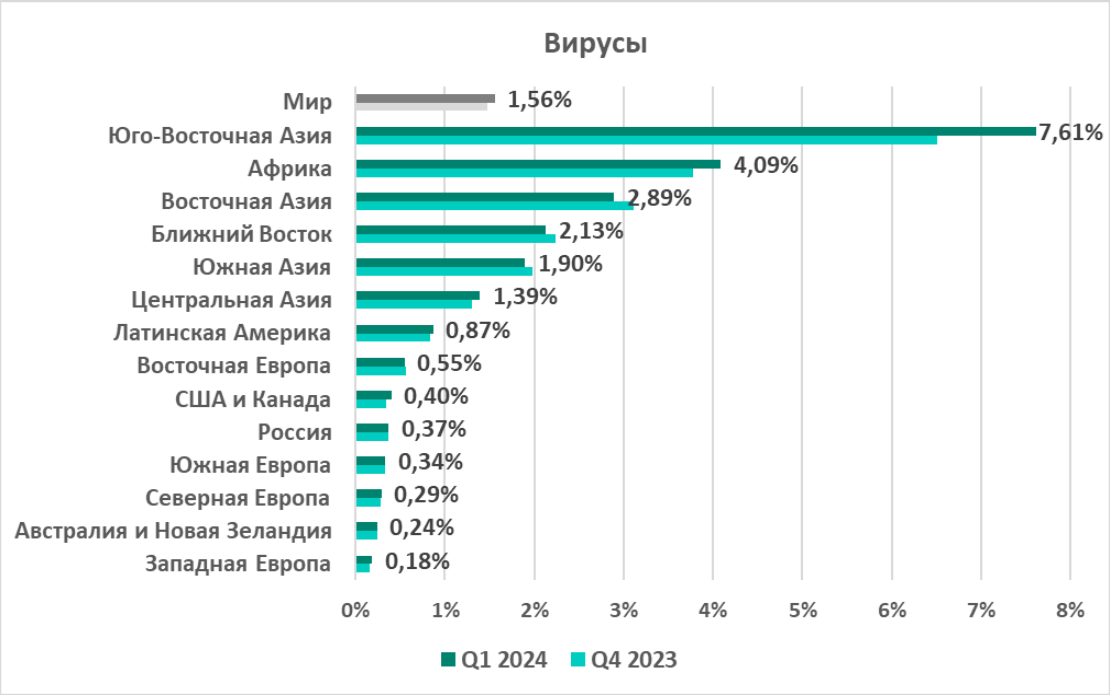
Самораспространяющееся вредоносное ПО. Вирусы и черви

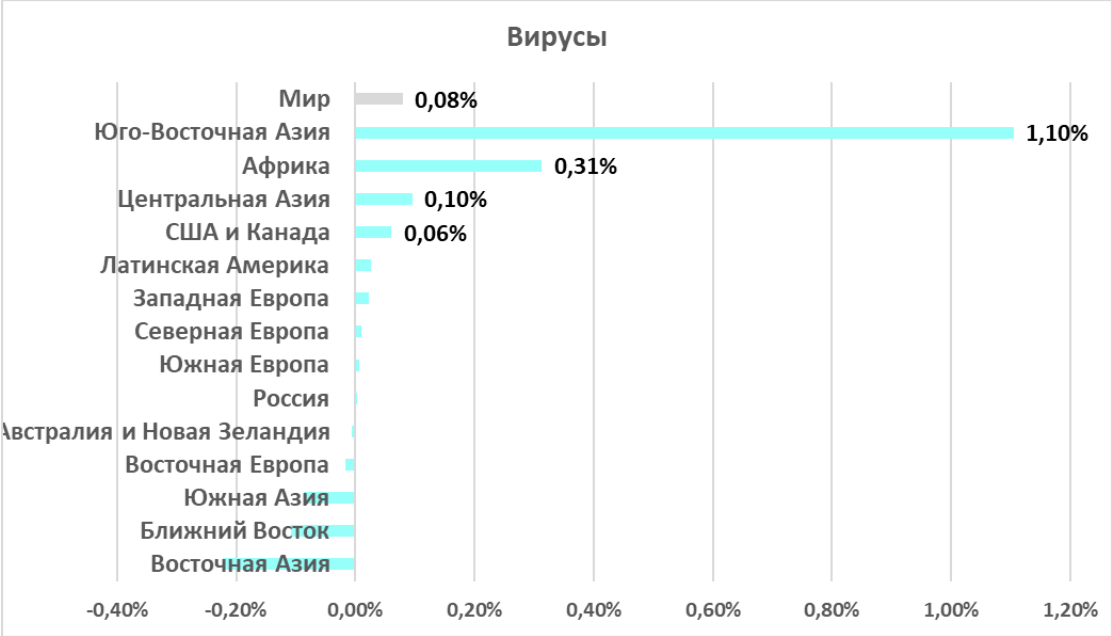
Черви



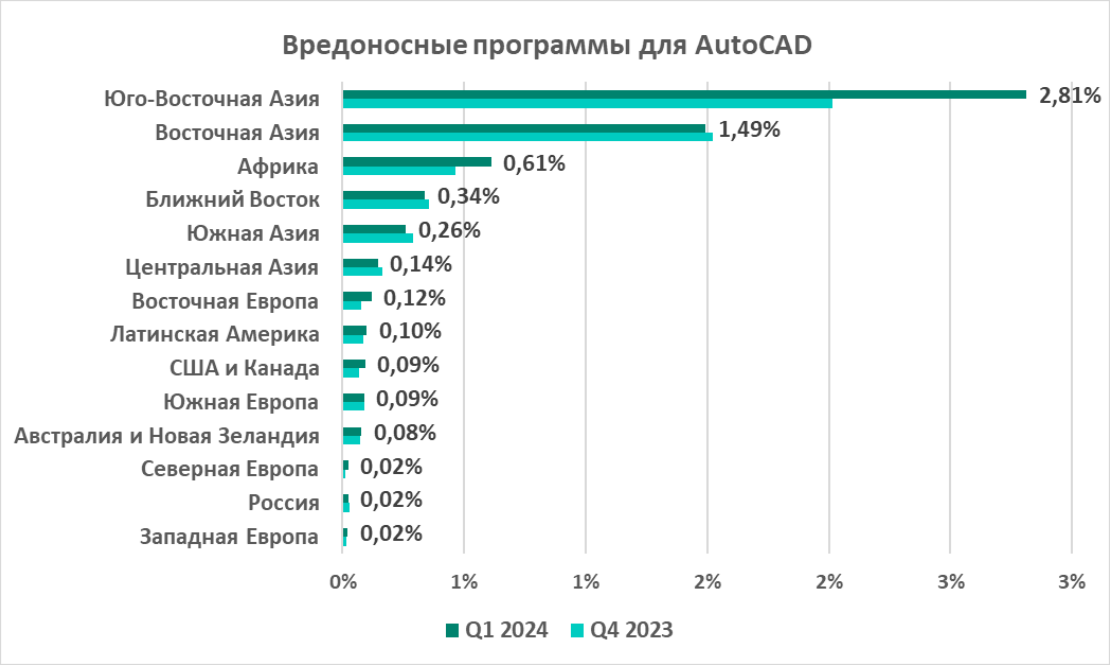


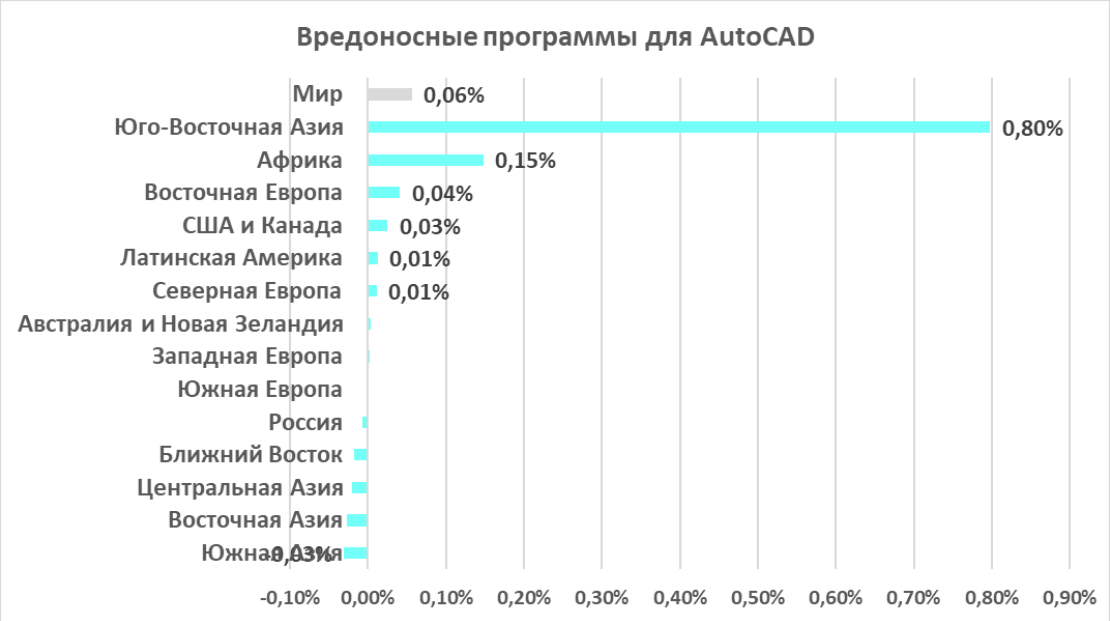
Вирусы





Вредоносные программы для AutoCAD





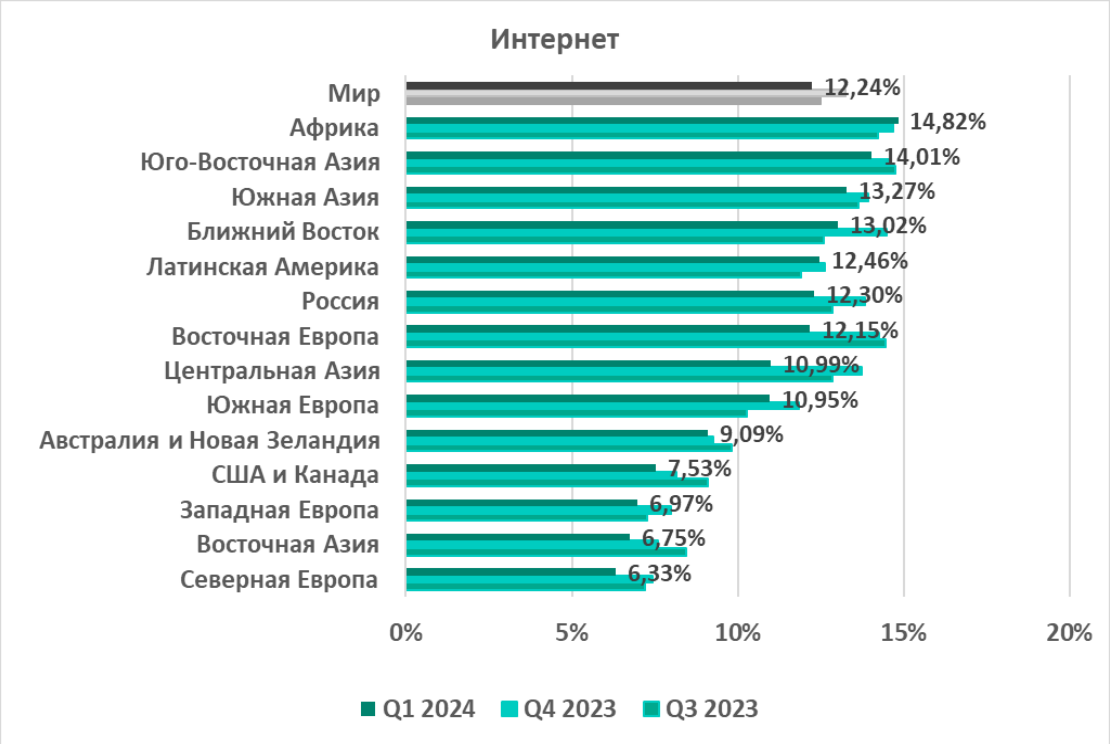
Источники угроз

Процент компьютеров АСУ, на которых блокируются угрозы из разных источников, как и в случае вредоносного ПО различных категорий, отличается в регионах.

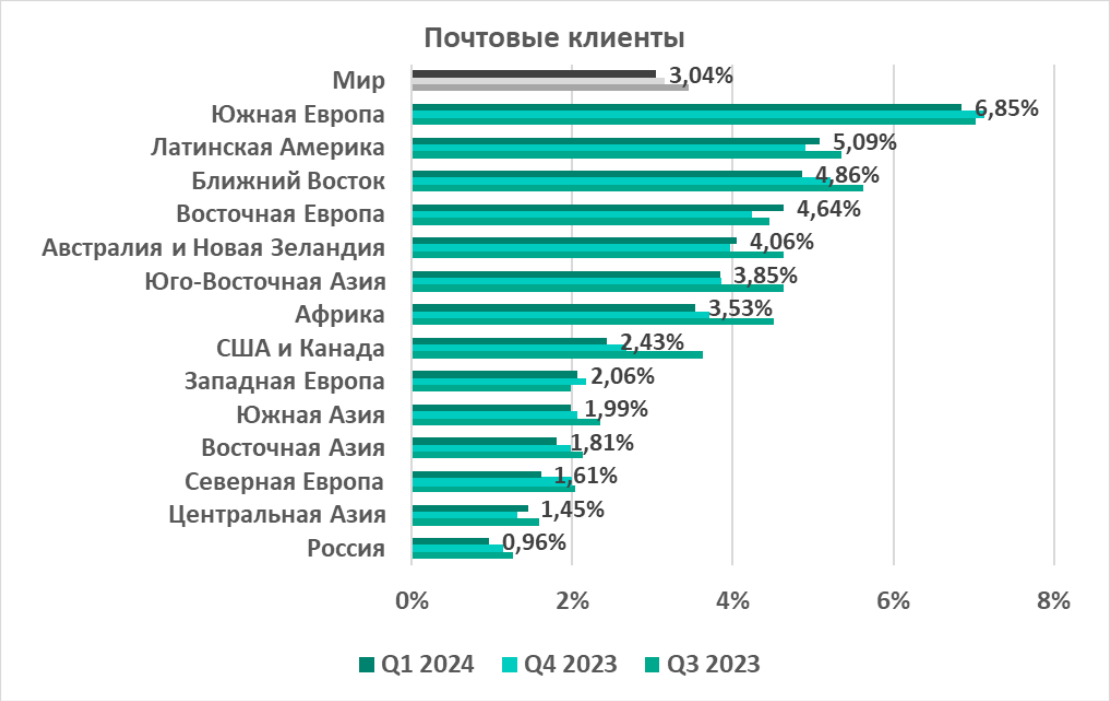
На графиках ниже представлены **рейтинги регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО из определенного источника в первом квартале 2024 года.**

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

Интернет

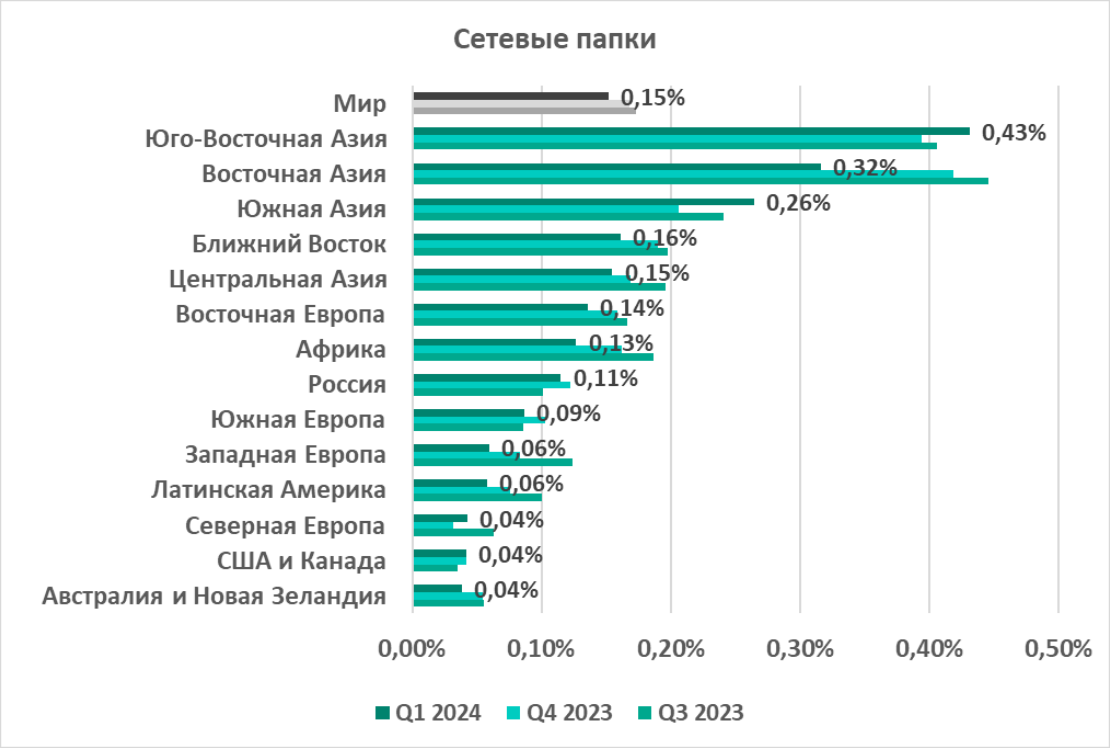


Почтовые клиенты



Съёмные носители

Сетевые папки



Регионы. Некоторые особенности

Чтобы увидеть особенности регионов, можно сравнить их с другими регионами и со статистикой в среднем по миру.

В большинстве регионов, как и в мире, первые позиции в рейтинге по проценту компьютеров АСУ, на которых были заблокированы определенные категории угроз, занимают вредоносные объекты, используемые для первичного заражения компьютеров, и программы-шпионы. А в рейтинге основных источников угроз во всех регионах лидирует интернет.

По некоторым позициям в регионах есть свои особенности и отличия, которые мы отметим ниже.

Африка

В сравнении с другими регионами

Первое место в рейтинге регионов. Один из двух регионов, где за квартал вырос процент атакованных компьютеров АСУ.

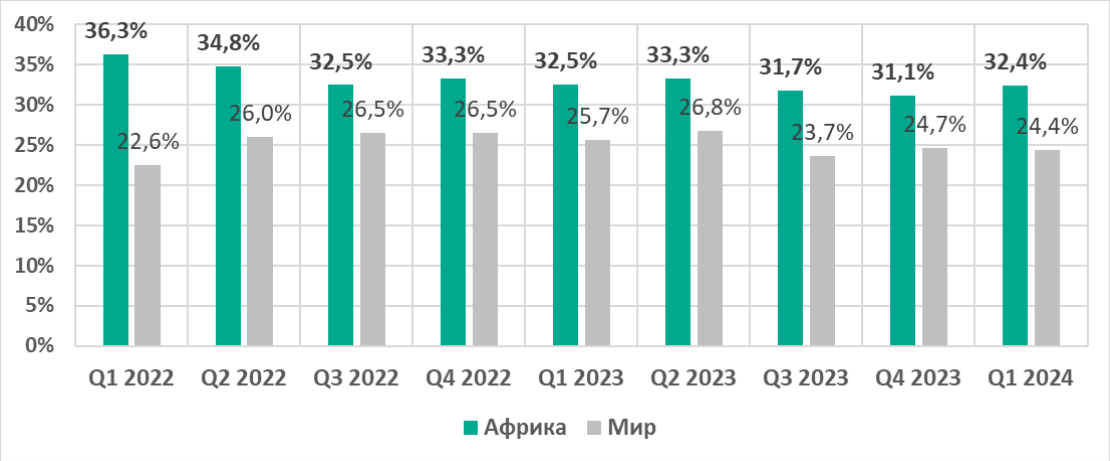
Из всех регионов в Африке традиционно самый высокий процент компьютеров АСУ, на которых были заблокированы вредоносные объекты. Соответственно, не удивительно, что Африка лидирует по многим позициям, по некоторым — с большим отрывом.

Среди регионов Африка лидирует

- По проценту компьютеров АСУ, на которых были заблокированы **ресурсы в интернете из списка запрещенных.**
- По проценту компьютеров АСУ, на которых были заблокированы **программы-шпионы.**
- По проценту компьютеров АСУ, на которых были заблокированы **веб-майнеры**.
- По проценту компьютеров АСУ, на которых были заблокированы угрозы **из интернета**.
- По проценту компьютеров АСУ, на которых детектируются **черви (с большим отрывом)**.
- По проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении **съёмных носителей (с большим отрывом)**.

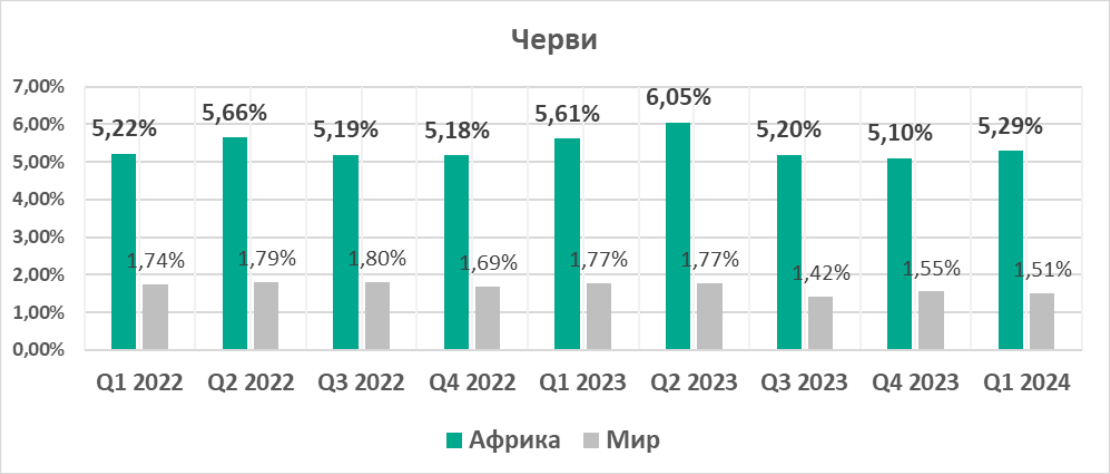
В сравнении с миром

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает средний по миру.

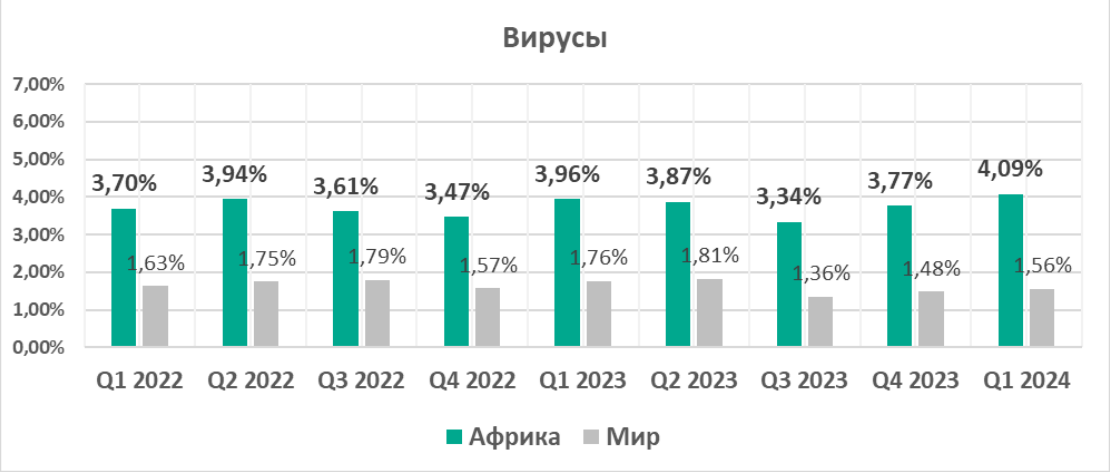


- В регионе выше, чем в мире, процент компьютеров АСУ, на которых были заблокированы все категории угроз.

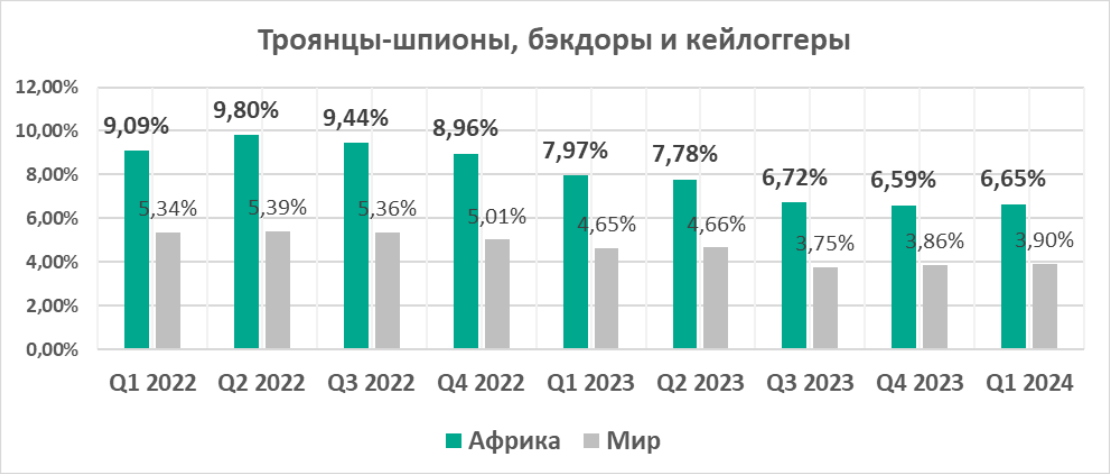
- Значительно выше, чем в мире, процент компьютеров АСУ, на которых были заблокированы:
  - Черви — в 3,5 раза



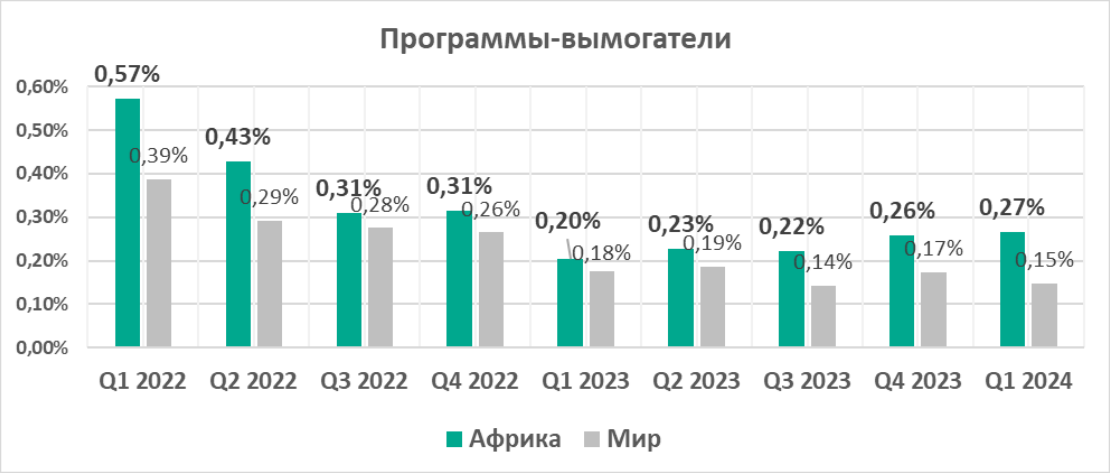
  - Вирусы — в 2,6 раза



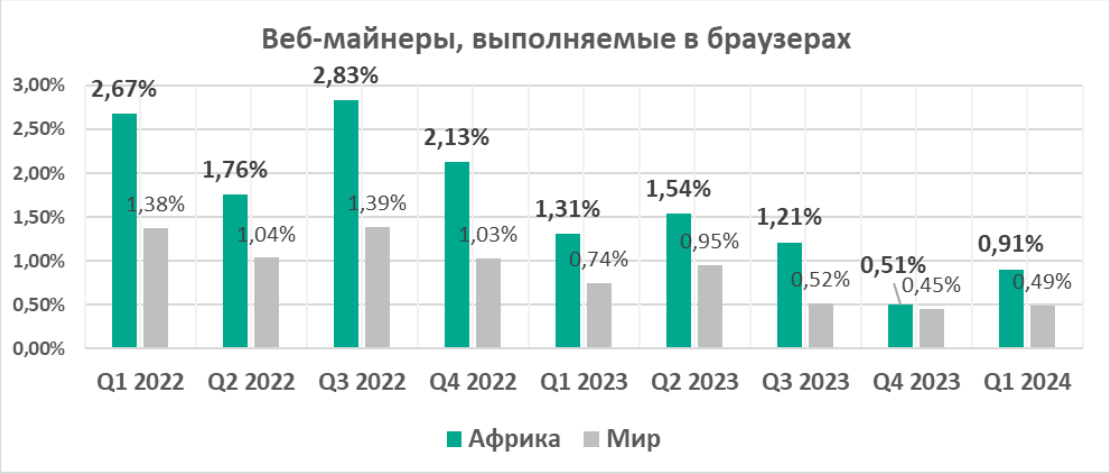
- Программы-шпионы — в 1,7 раза



- Программы-вымогатели — в 1,8 раза

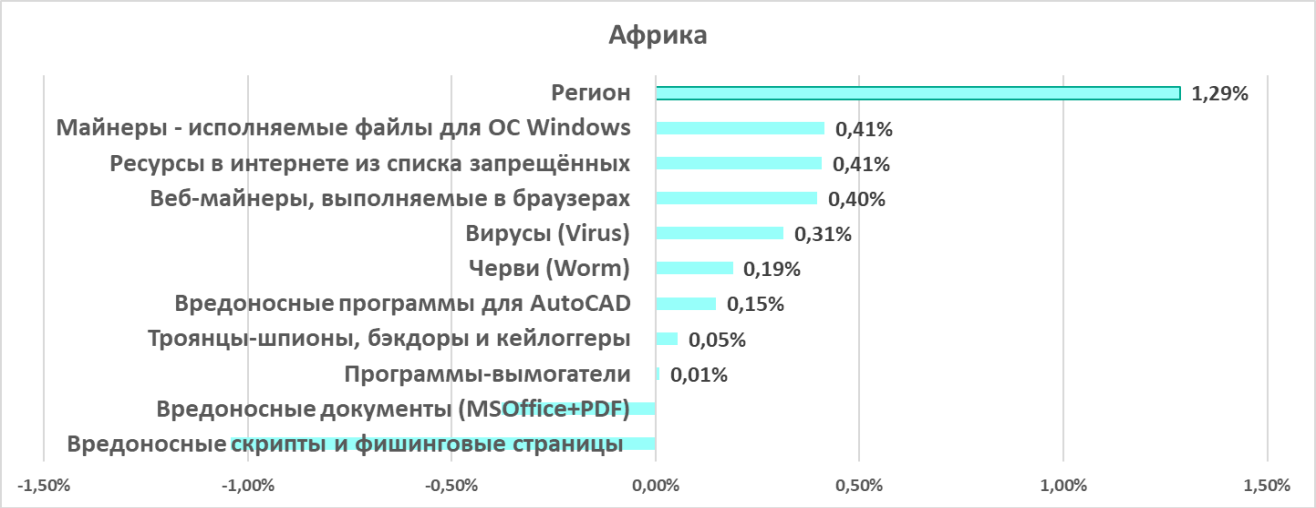


- Веб-майнеры — в 1,8 раза

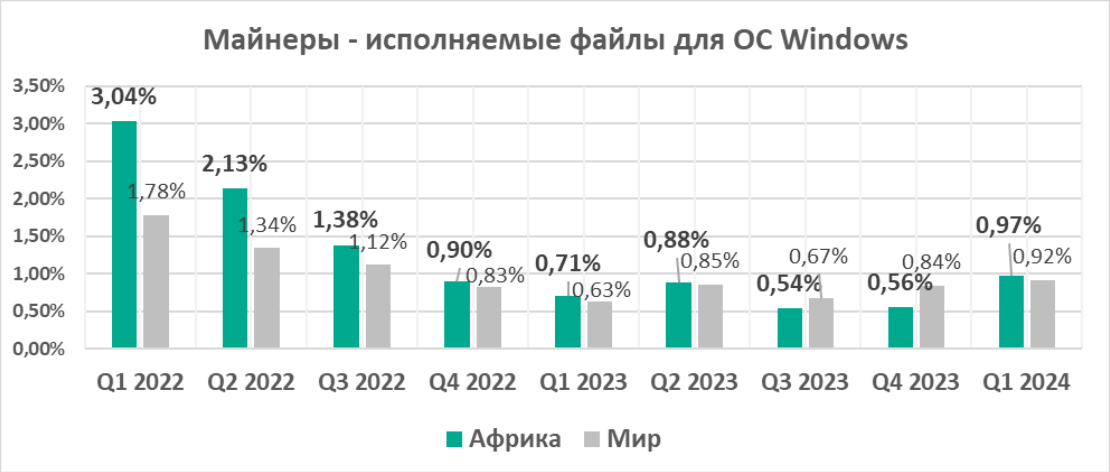


- **Черви и вирусы** в рейтинге категорий угроз по проценту компьютеров АСУ, на которых оно было заблокировано, потеснили вредоносные документы. Черви на четвертом месте (в мире — на шестом).
- **Съёмные носители** на втором месте в рейтинге источников угроз по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты из разных источников (в мире — на третьем). Африка — один из трех регионов, где процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съёмных носителей, превысил процент компьютеров АСУ, на которых были заблокированы угрозы из электронной почты.

Изменения за квартал



- Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы майнеры:
  - Веб-майнеры — в 1,8 раза
  - Майнеры — исполняемые файлы для ОС Windows — в 1,7 раза



Актуальные угрозы

- Угрозы, распространяющиеся через интернет
- Программы-шпионы
- Вредоносное ПО для скрытого майнинга криптовалюты
- Черви
- Вирусы
- Угрозы, распространяющиеся на съёмных носителях

В Африке самый высокий среди всех регионов процент компьютеров АСУ, на которых блокируются вредоносные объекты.

В первом квартале 2024 года отметим резкий рост процента компьютеров АСУ, на которых были заблокированы:

- Вредоносные майнеры

Юго-Восточная Азия

Среди регионов

Второе место в рейтинге регионов.

- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **вирусы** (с большим отрывом).

  В регионе отмечен самый значительный рост за квартал процента компьютеров АСУ, на которых были заблокированы вирусы (+1,1 п.п.).

- **Лидирует** по проценту компьютеров АСУ, на которых было заблокировано **вредоносное ПО для AutoCAD**. В Юго-Восточная Азия в первом квартале 2024 года отмечен самый большой среди всех регионов рост этого показателя (на 0,8 п.п.).

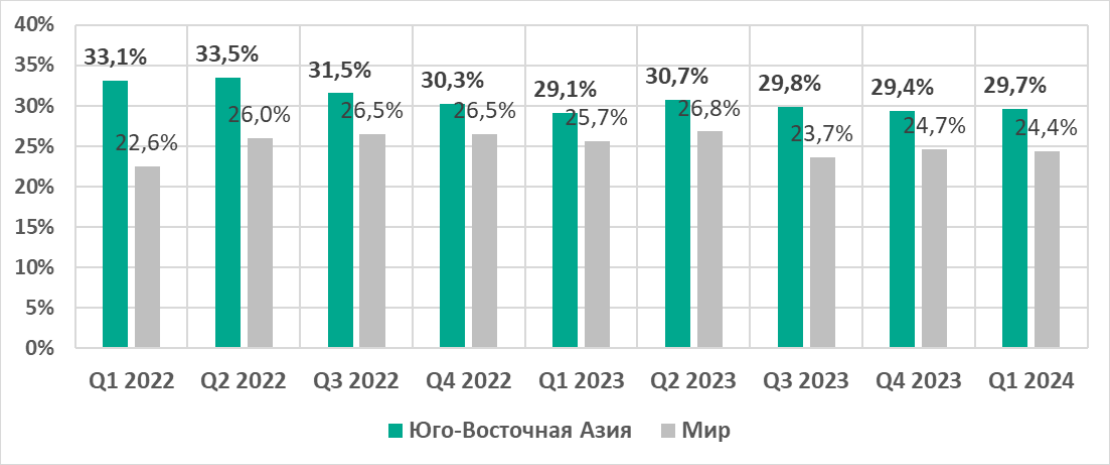
- **Лидирует** по проценту компьютеров АСУ, на которых вредоносное ПО было заблокировано **в сетевых папках**.

- **На втором месте** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **угрозы из интернета**.

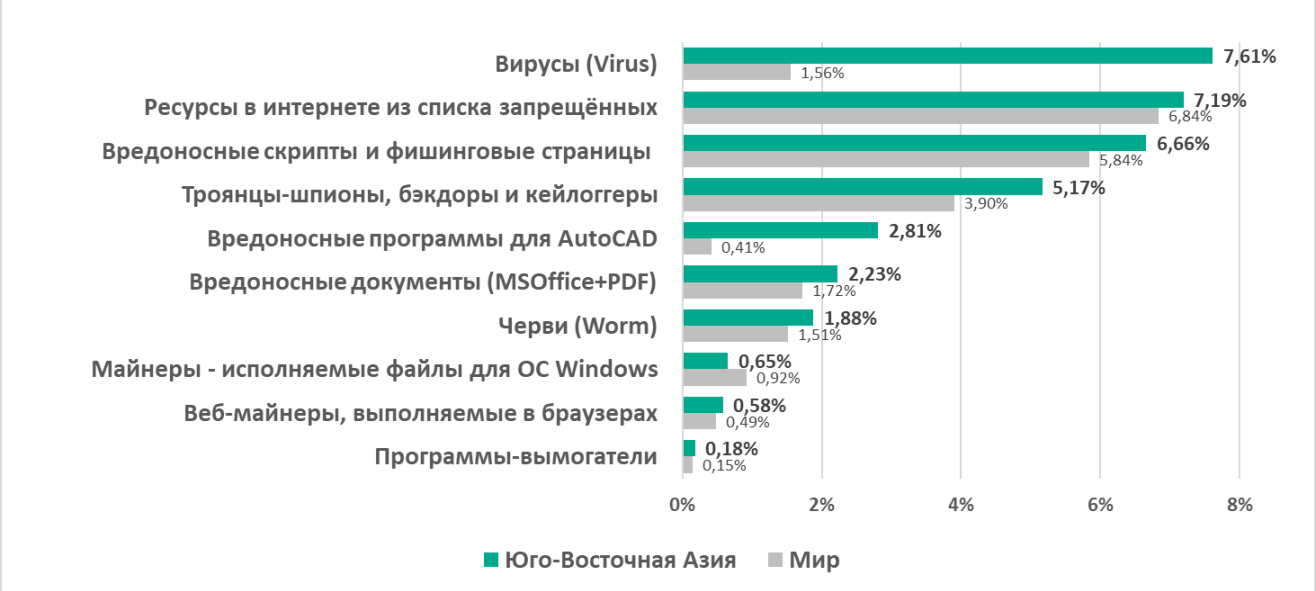
- **На третьем месте** среди регионов по проценту компьютеров АСУ, на которых вредоносное ПО было заблокировано при подключении **съёмных носителей**.

Регион vs мир

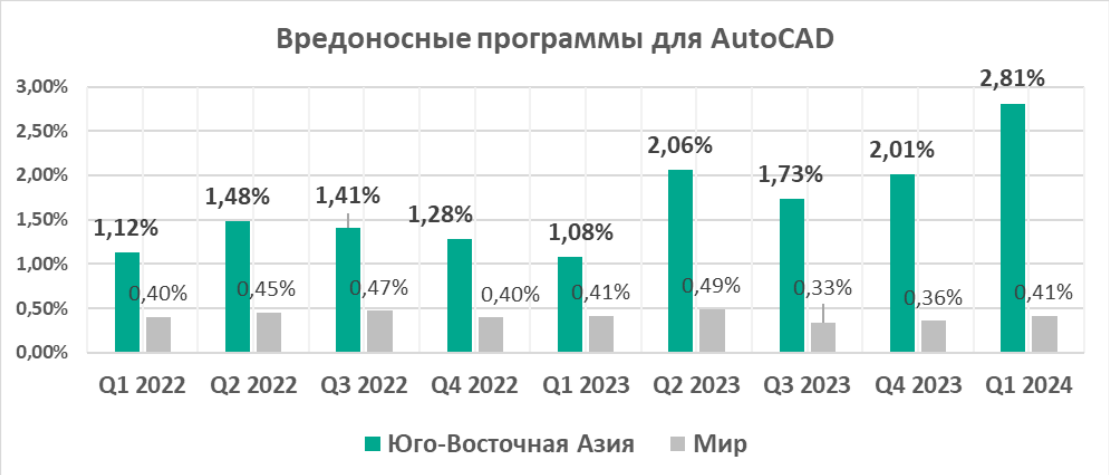
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает средний по миру.



- **Вирусы на первом месте (!)** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано. В Юго-Восточной Азии этот процент в 5 раз больше, чем в среднем по миру.



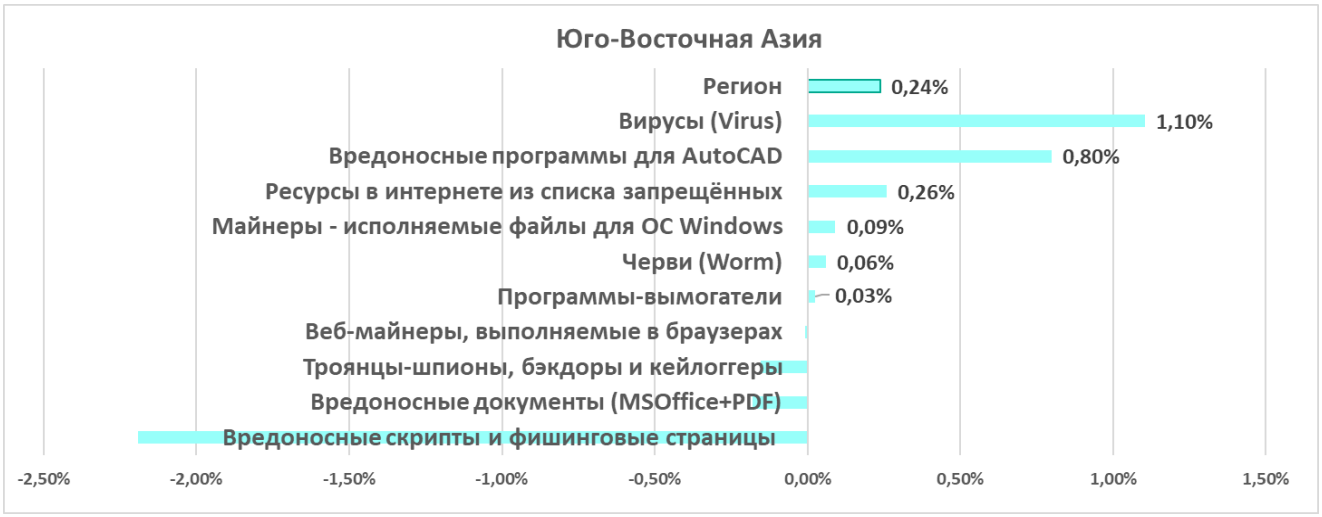
- **Вредоносное ПО для AutoCAD** — на пятом месте в этом рейтинге (в мире процент компьютеров АСУ, на котором блокируется такое вредоносное ПО, наименьший среди всех категорий).
- В регионе значительно выше, чем в мире, процент компьютеров АСУ, на которых были заблокированы:
  - Вредоносные программы для AutoCAD — в 6,8 раза



- Вирусы — в 4 раза

- Программы-шпионы — в 1,3 раза
- Вредоносные документы — в 1,3 раза
- Программы-вымогатели — в 1,2 раза

Изменения за квартал



Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Вредоносные программы для AutoCAD — в 1,4 раза
- Вирусы — в 1,2 раза

Актуальные угрозы

- **Вирусы. Лидирующая по проценту атакованных компьютеров АСУ категория угроз.** В мире эта категория на пятом месте, в других регионах не поднимается в рейтинге выше четвертого места (Восточная Азия).
- Программы-шпионы
- Программы-вымогатели
- Вредоносные программы для AutoCAD
- Угрозы, распространяющиеся на съемных носителях

Промышленным организациям в регионе нужно лучше обеспечивать покрытие своих систем в технологической сети хотя бы минимальным набором защитных мер и средств.

Ближний Восток

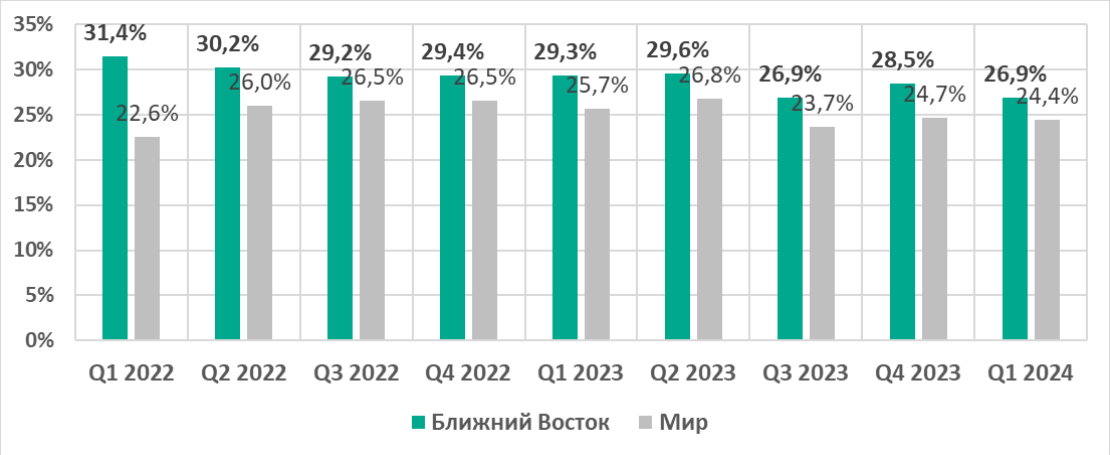
Среди регионов

Третье место в рейтинге регионов.

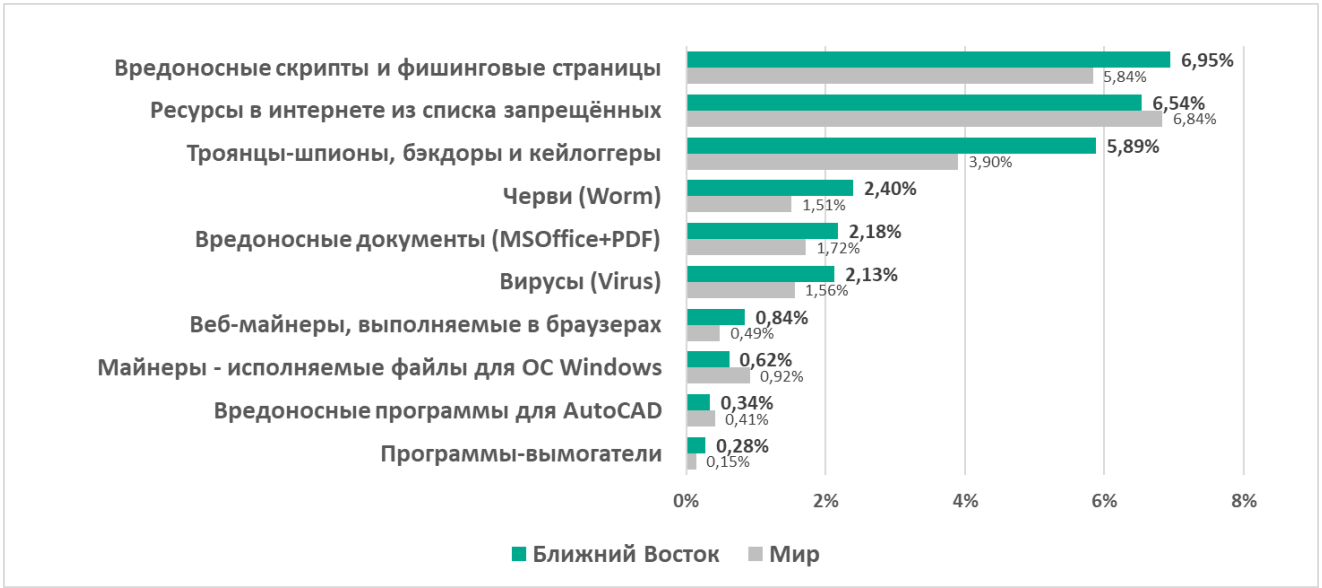
- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **программы-вымогатели.**
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **программы-шпионы**.
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **веб-майнеры.**
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **черви**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **угрозы из почты**.

Регион vs мир

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает средний по миру.



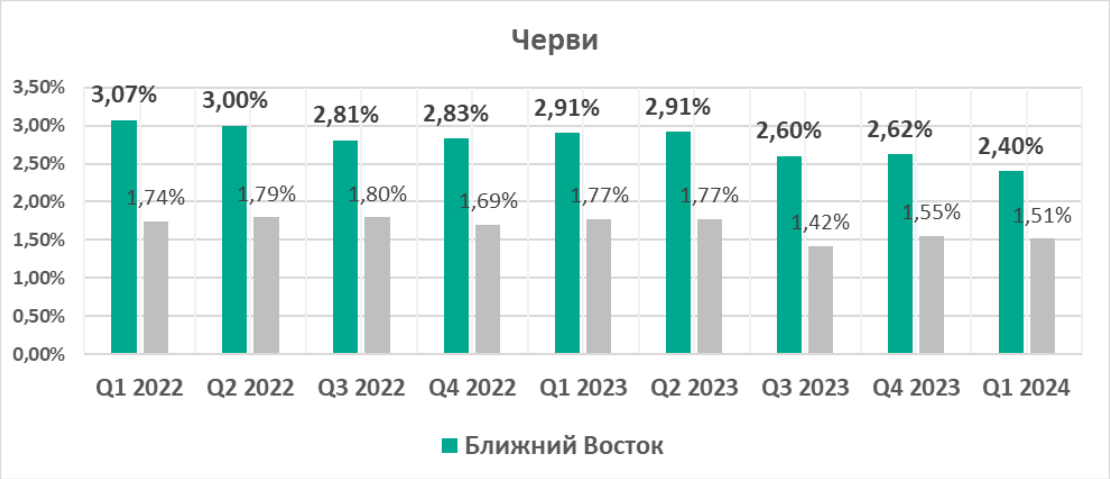
- В регионе выше, чем в мире, процент компьютеров АСУ, на которых были заблокированы все категории угроз, кроме ресурсов в интернете из списка запрещённых.



- В регионе заметно выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Программы-вымогатели — в 1,9 раза

  - Веб-майнеры — в 1,7 раза

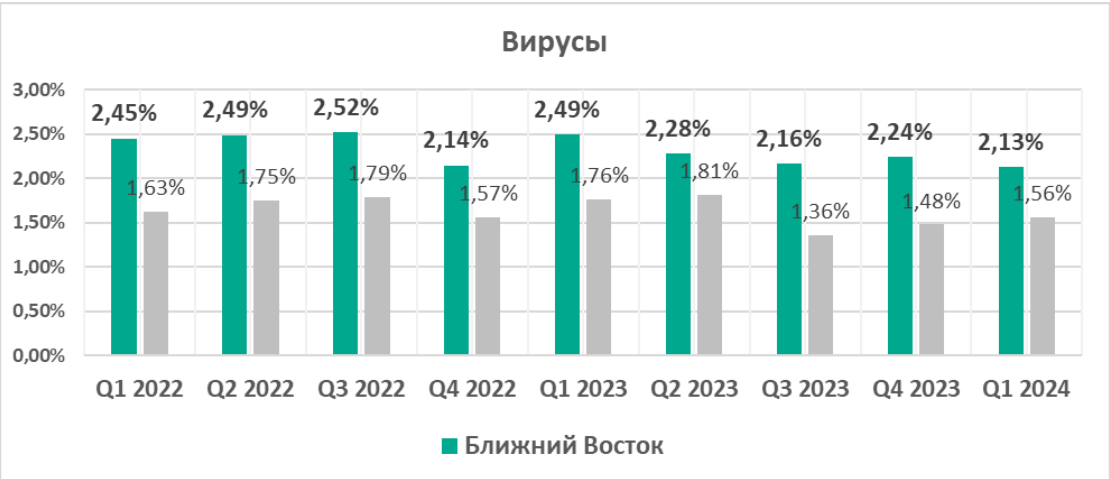
- Черви — в 1,6 раза



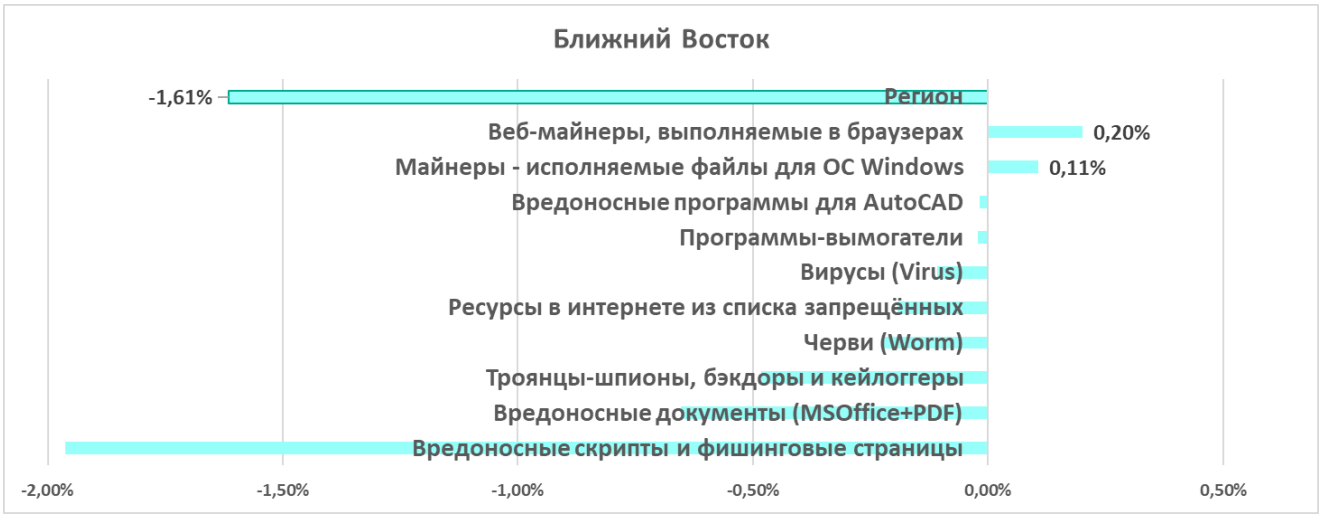
Черви на четвертом месте в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на шестом).

- Программы-шпионы — в 1,5 раза

- Вирусы — в 1,5 раза



Изменения за квартал



Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты:

- Веб-майнеры — в 1,3 раза
- Майнеры — исполняемые файлы для ОС Windows — в 1,2 раза

Актуальные угрозы

- **Программы-вымогатели**
  С четвертого квартала 2022 года по третий квартал 2023 года Ближний Восток занимал вторую позицию в рейтинге регионов по этой категории угроз. С четвертого квартала 2023 года — лидирует.
- Шпионские программы
- Черви и вирусы
- Вредоносные майнеры
- Угрозы из почты

Центральная Азия

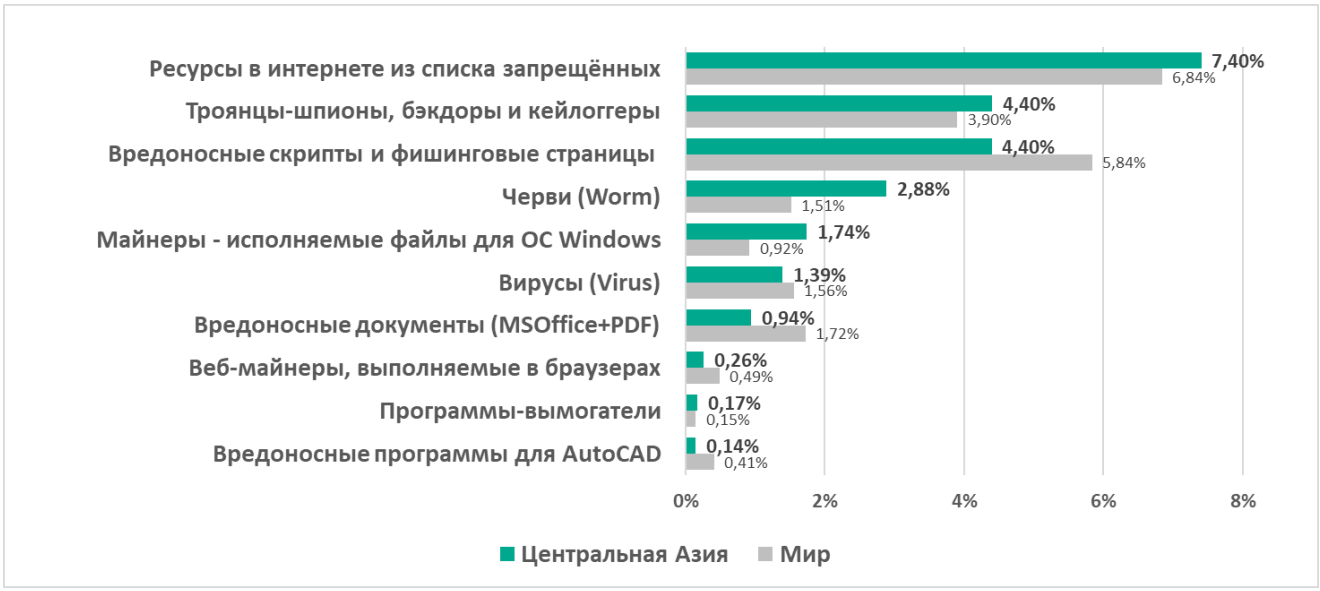
Среди регионов

Четвертое место в рейтинге регионов.

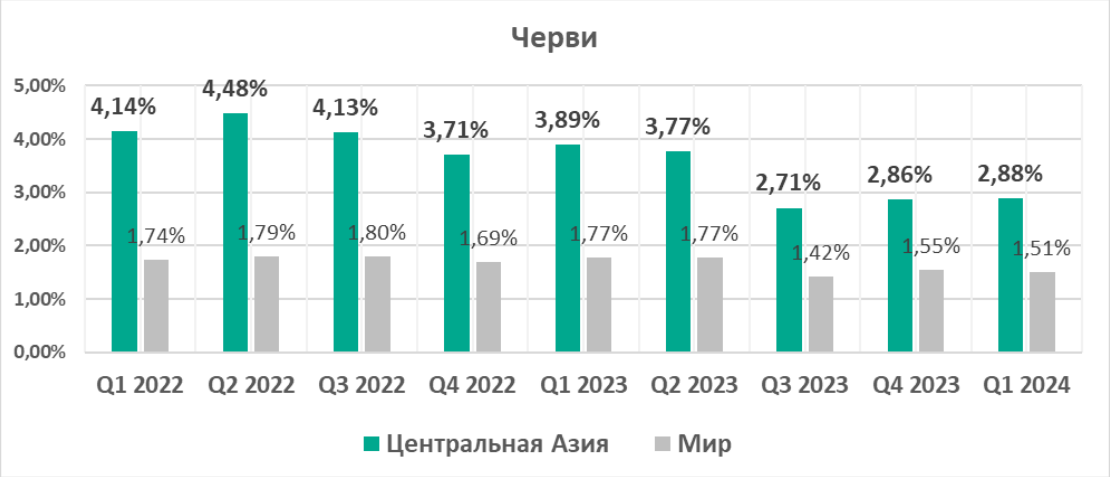
- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows**.
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **черви**.

Регион vs мир

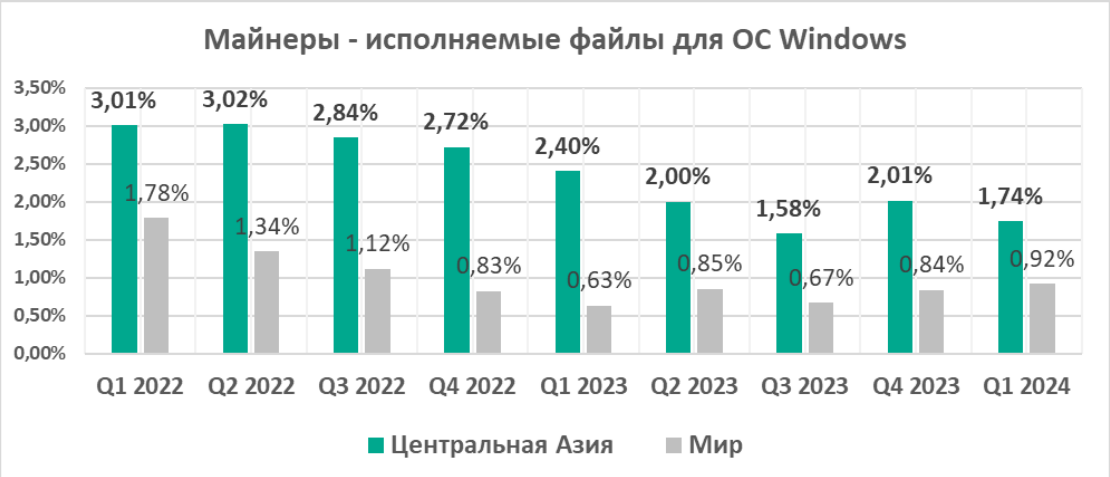
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает средний по миру.



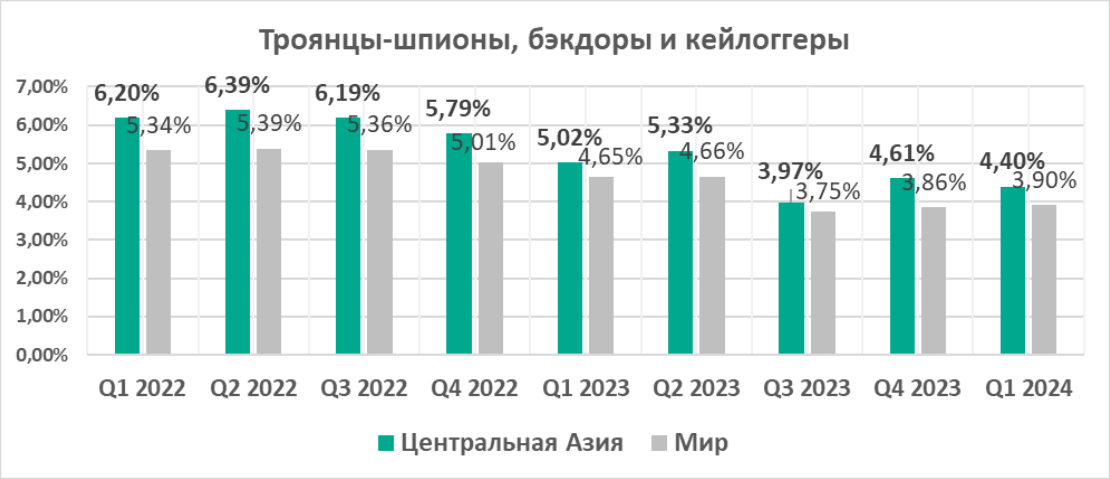
- В регионе выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Черви — в 1,9 раза. Черви на четвертом месте в рейтинге (в мире — на шестом).



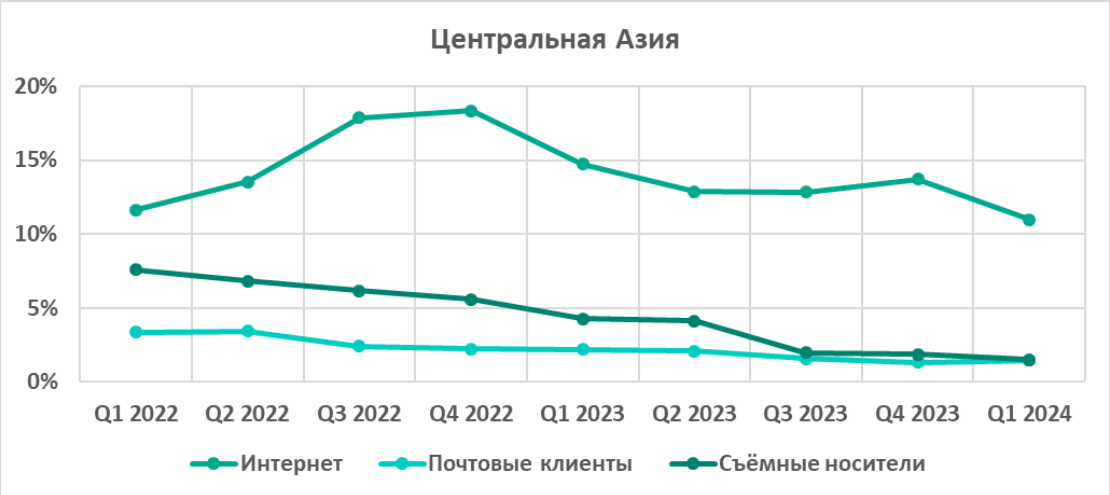
  - Майнеры — исполняемые файлы для ОС Windows — в 1,9 раза. Эта категория угроз на пятом месте в рейтинге (в мире — на седьмом)



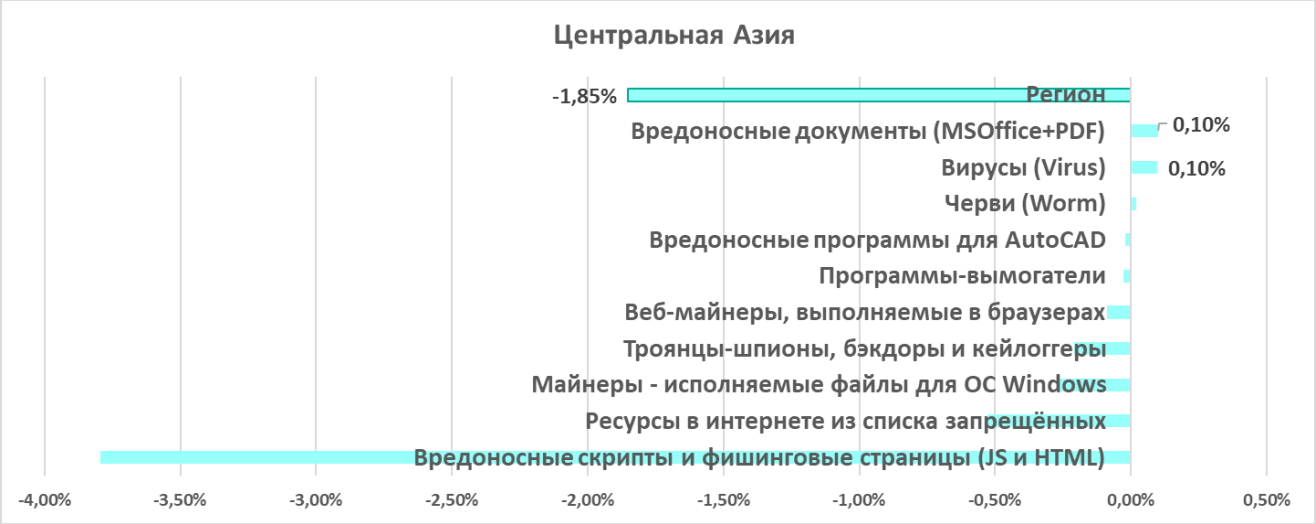
- **Шпионское ПО на втором месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.



- В регионе **съёмные носители** на втором месте в рейтинге источников угроз по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты из разных источников. Один из трех регионов, где процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съёмных носителей, превысил процент компьютеров АСУ, на которых были заблокированы угрозы из электронной почты.



Изменения за квартал



Актуальные угрозы

- Шпионские программы
- Майнеры — исполняемые файлы для ОС Windows
- Черви
- Угрозы, распространяющиеся на съёмных носителях

Восточная Европа

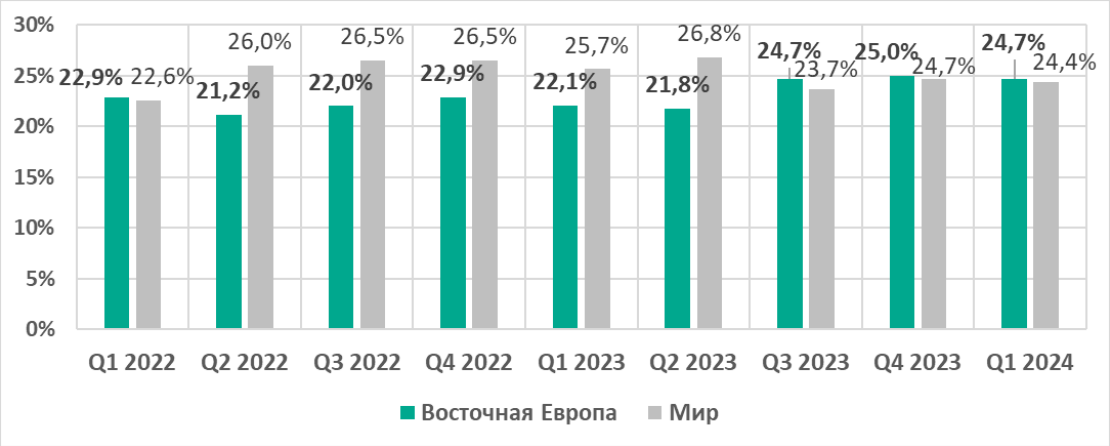
Среди регионов

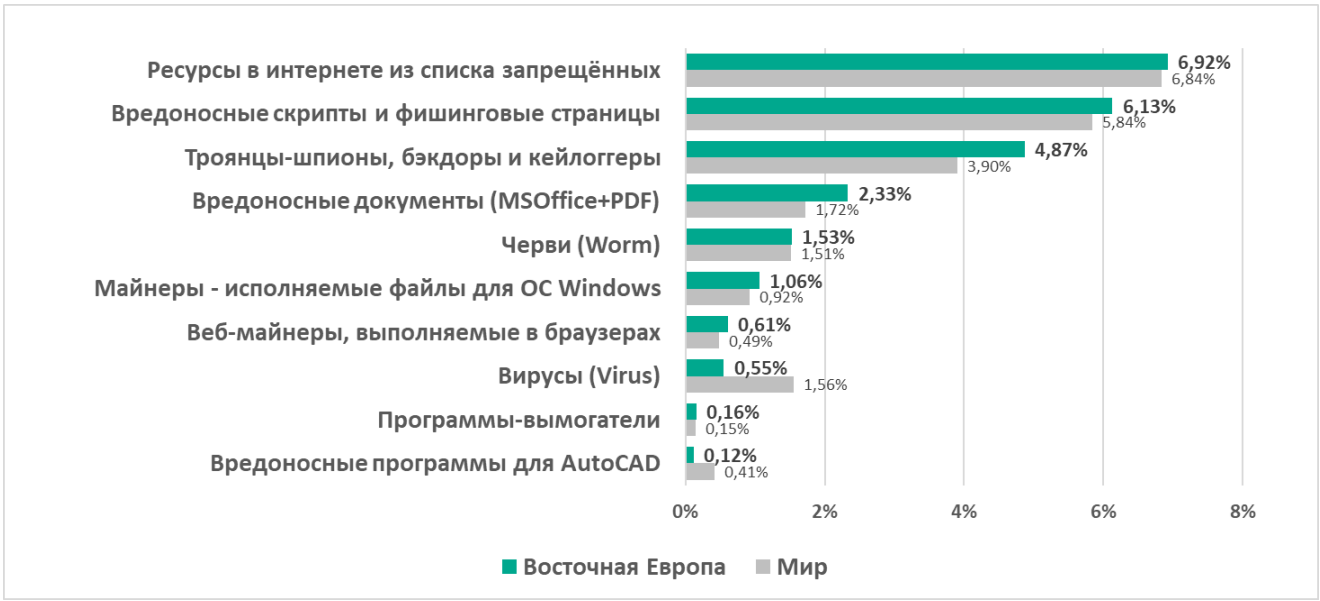
Пятое место в рейтинге регионов. До второго квартала 2023 года регион не поднимался в этом рейтинге выше девятого места.

- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные документы**. Один из двух регионов, где этот показатель вырос за квартал (на максимальные 0,36 п.п.).
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows**.
- **На четвертом месте** по проценту компьютеров АСУ, на которых были заблокированы **угрозы из почты**.
- **Единственный из регионов мира**, демонстрирующий с начала 2022 года рост доступности компьютеров ОТ для киберугроз.

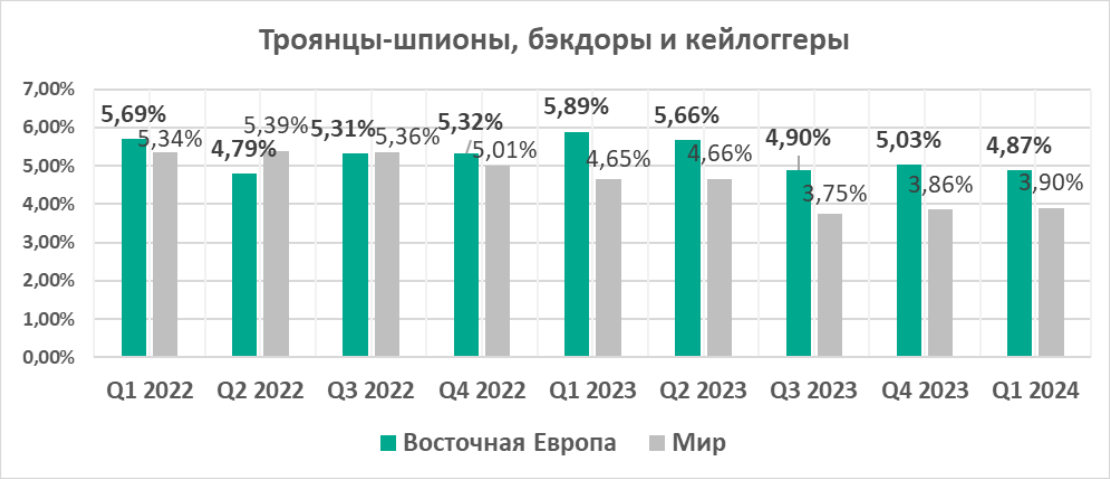
Регион vs мир

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, с третьего квартала 2023 года немного превышает средний по миру.

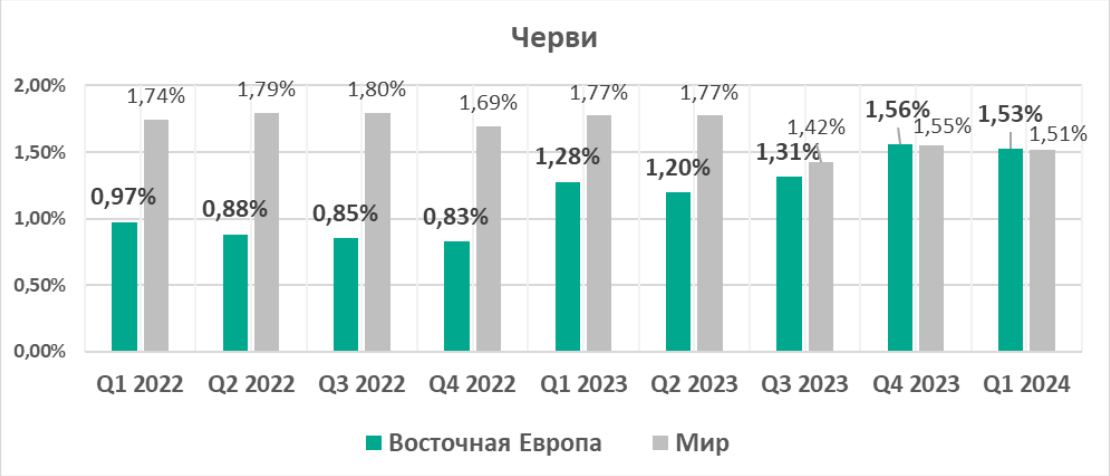




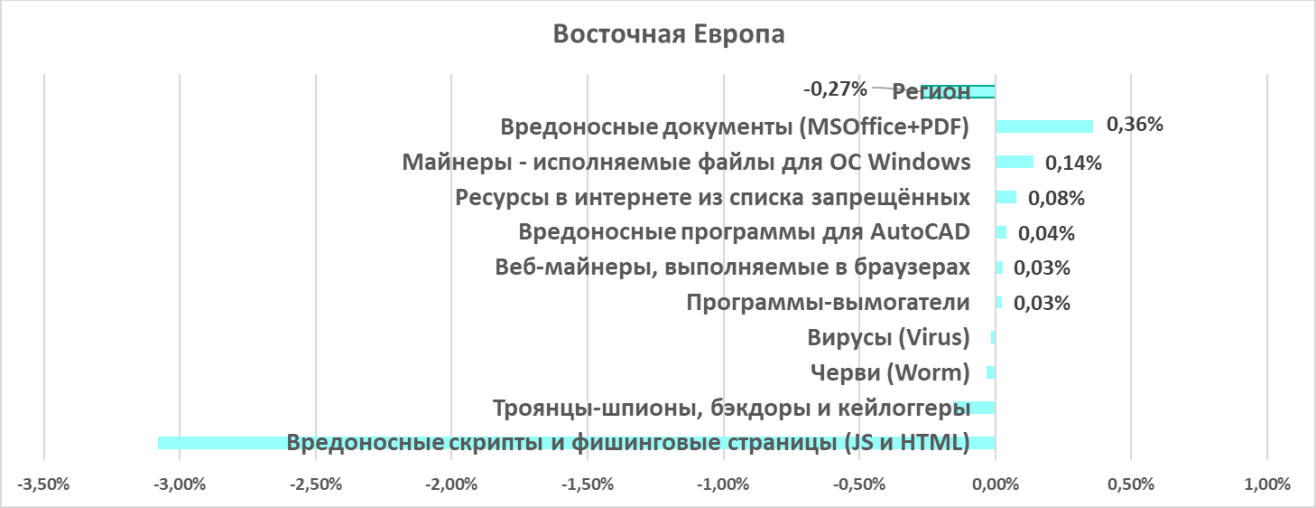
- В регионе заметно выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Программы-шпионы — в 1,2 раза



- С начала 2023 года в регионе растет процент компьютеров АСУ, на которых блокируются черви.

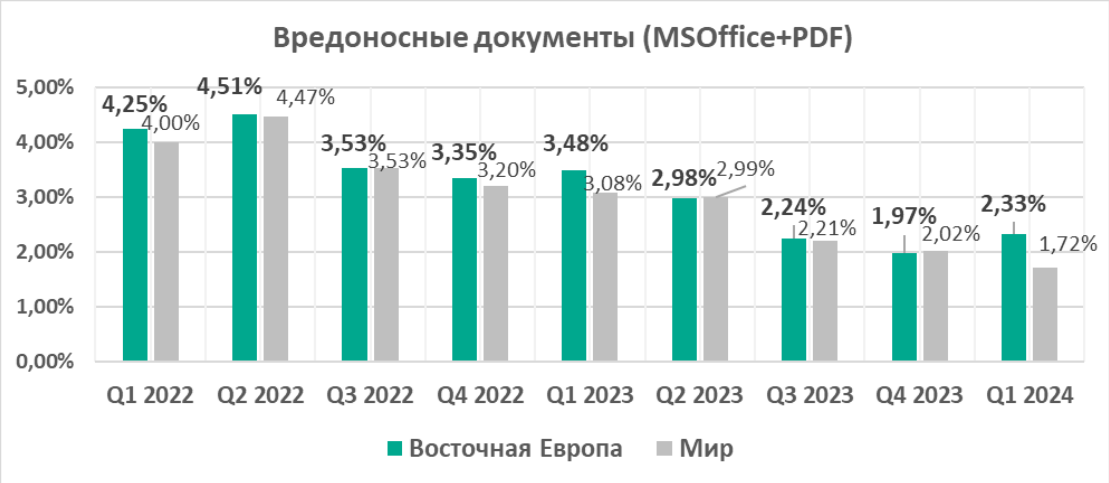


Изменения за квартал



Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Вредоносные документы — в 1,2 раза. В результате этого роста процент по вредоносным документам в регионе превысил аналогичный показатель в мире в 1,4 раза.



- Программы-вымогатели — в 1,2 раза. Процент растет уже второй квартал подряд и догнал средний по миру.

Актуальные угрозы

- Вредоносные документы
- Шпионские программы
- Программы-вымогатели
- Угрозы из почты
- Черви
- Майнеры — исполняемые файлы для ОС Windows

Доступность OT-систем для различного типа угроз растет, по всей видимости, в связи с общим для региона недостатком финансирования ИБ промышленных объектов. В частности, рост процента компьютеров АСУ, на которых обнаруживаются черви, означает недостаточное покрытие OT-инфраструктуры средствами защиты конечных узлов. Высокие показатели для угроз, распространяемых по электронной почте, а также высокий процент компьютеров, на которых были заблокированы вредоносные документы, означает повышенный риск компрометации промышленных инфраструктур с использованием фишинга.

Россия

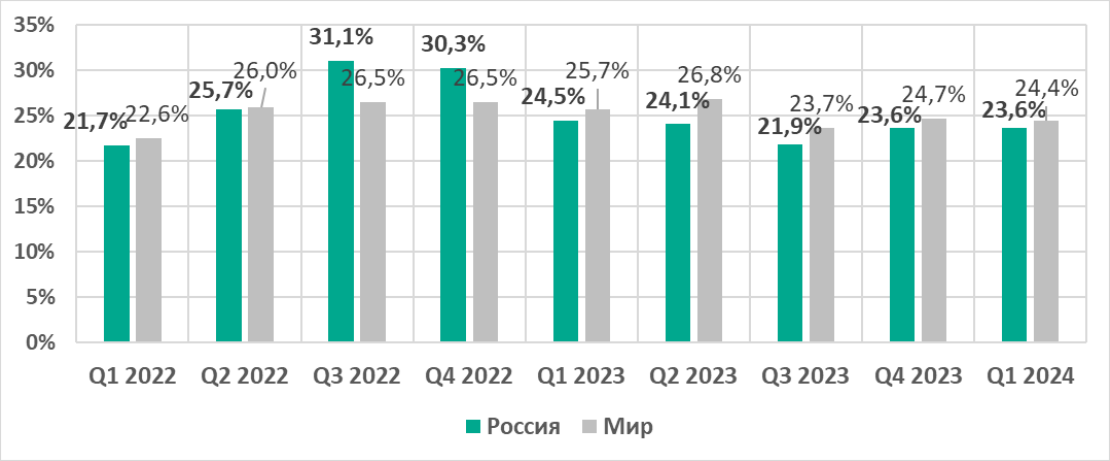
Среди регионов

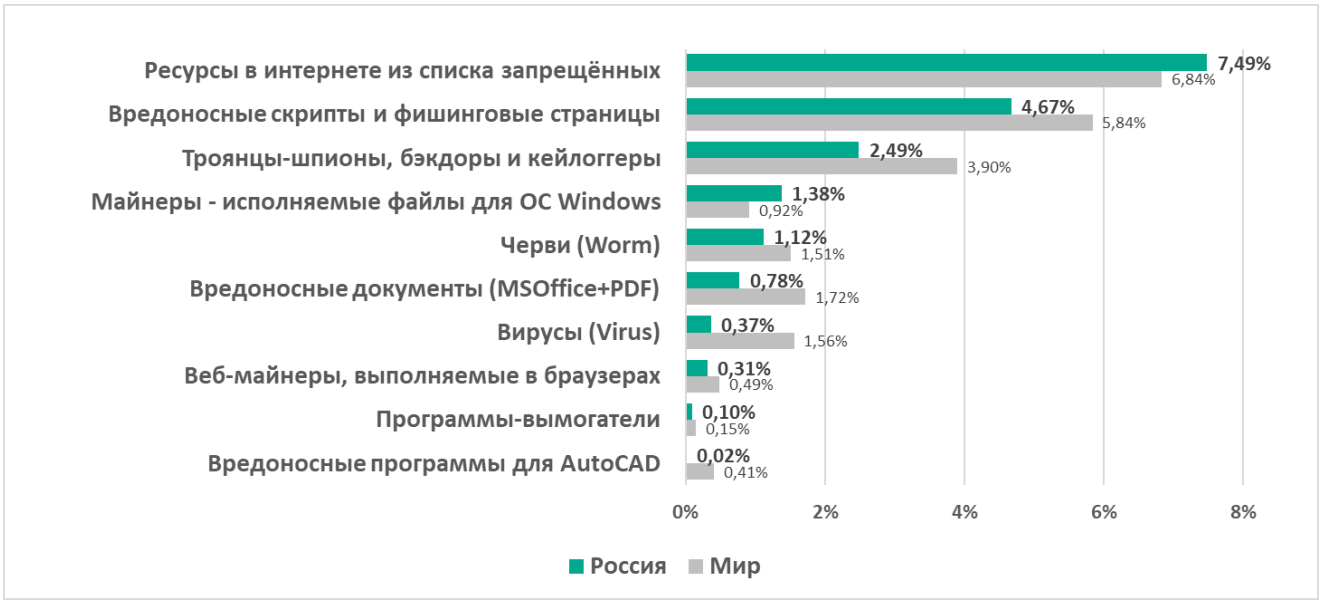
Шестое место в рейтинге регионов.

- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **ресурсы в интернете из списка запрещённых.**
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows**.

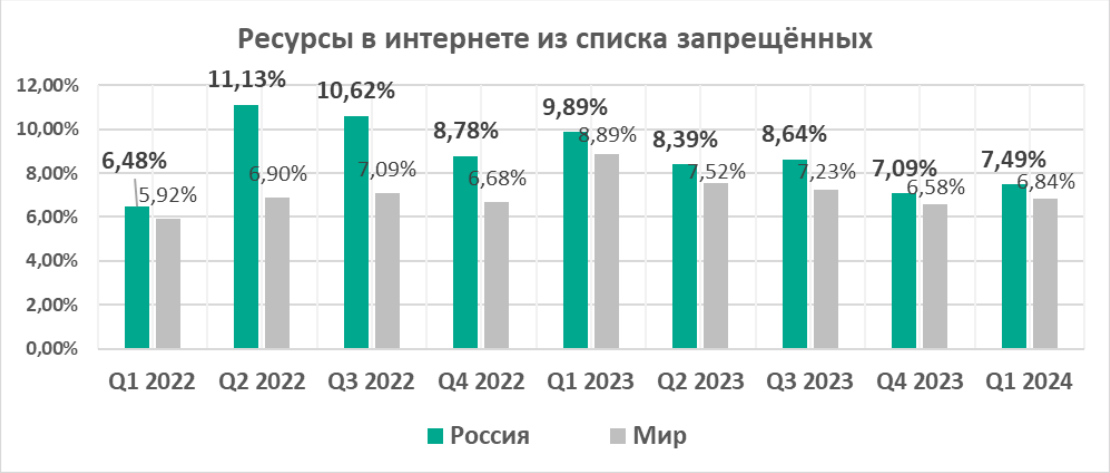
Регион vs мир

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, за исключением третьего и четвертого кварталов 2022 года, в регионе немного меньше среднего по миру.



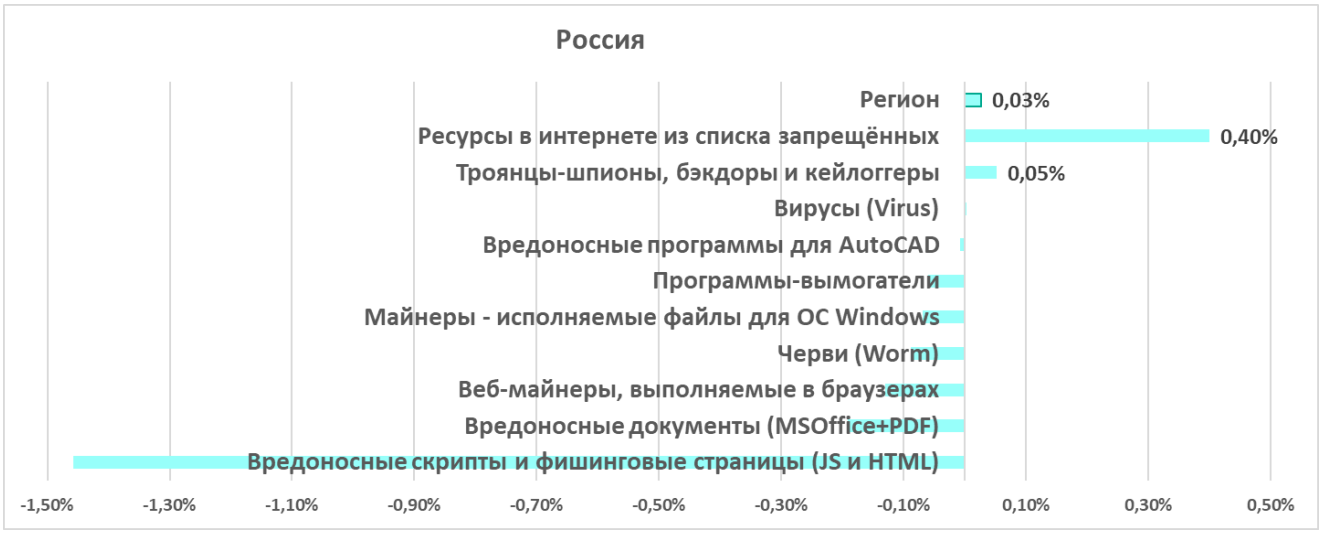


- В регионе выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Ресурсы в интернете из списка запрещённых



  - Майнеры — исполняемые файлы для ОС Windows — в 1,5 раза. В регионе такие майнеры на четвертом месте в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на седьмом).

Изменения за квартал



Актуальные угрозы

- Угрозы из интернета
- Майнеры — исполняемые файлы для ОС Windows

Промышленным организациям в России стоит всерьез озаботиться уменьшением доступности интернета на компьютерах АСУ и обучению сотрудников безопасной работе с интернет-ресурсами, когда доступ к ним действительно необходим. Сейчас уровень риска заражения непосредственно из интернета выше всех разумных пределов.

Латинская Америка

Среди регионов

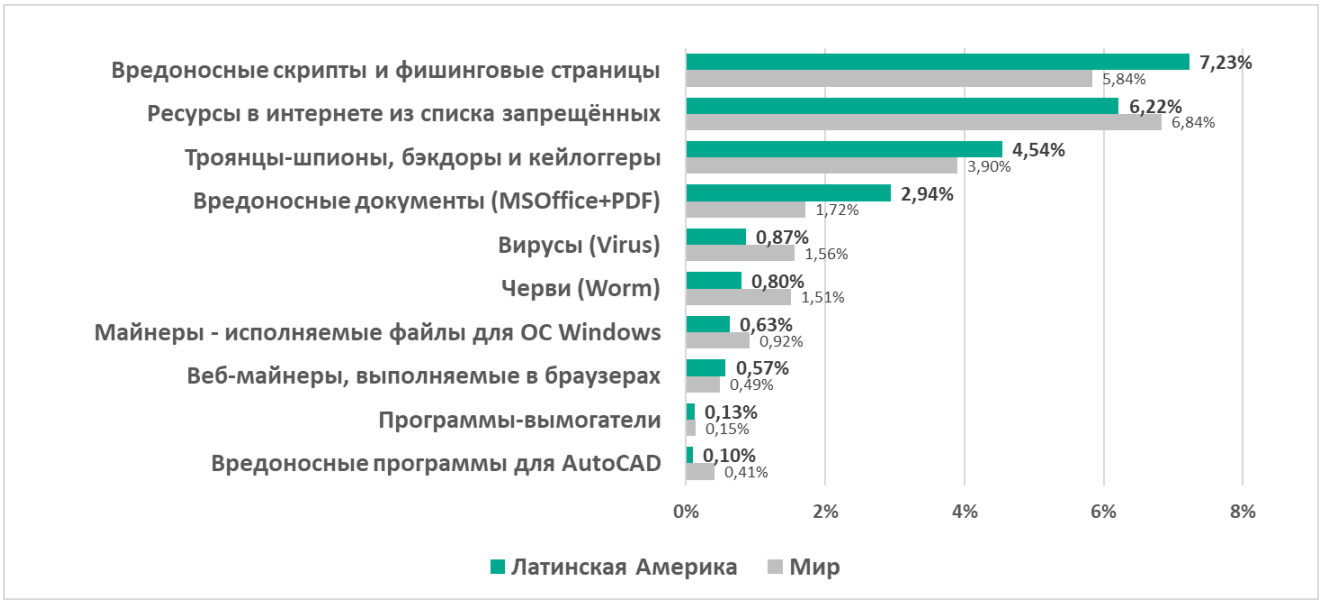
Седьмое место в рейтинге регионов.

- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы.**
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные документы**.
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **угрозы из почты** — вредоносные почтовые вложения и фишинговые ссылки.

- Регион, где за квартал процент компьютеров АСУ, на которых были заблокированы **программы-шпионы,** вырос на максимальные среди регионов 0,92 п.п.

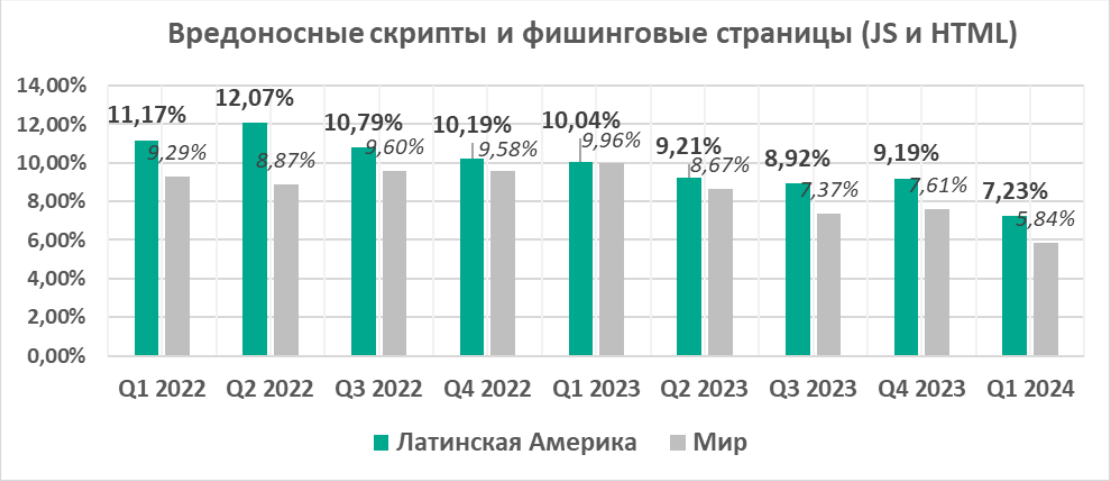
Регион vs мир

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, близок к среднему по миру.



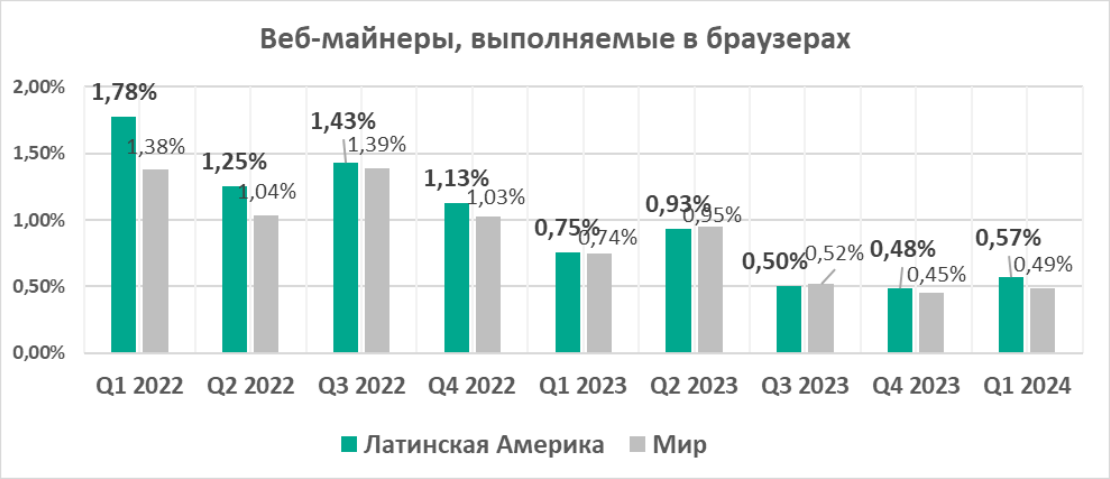
- В регионе выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Вредоносные документы — в 1,7 раза

  - Вредоносные скрипты и фишинговые страницы — в 1,2 раза

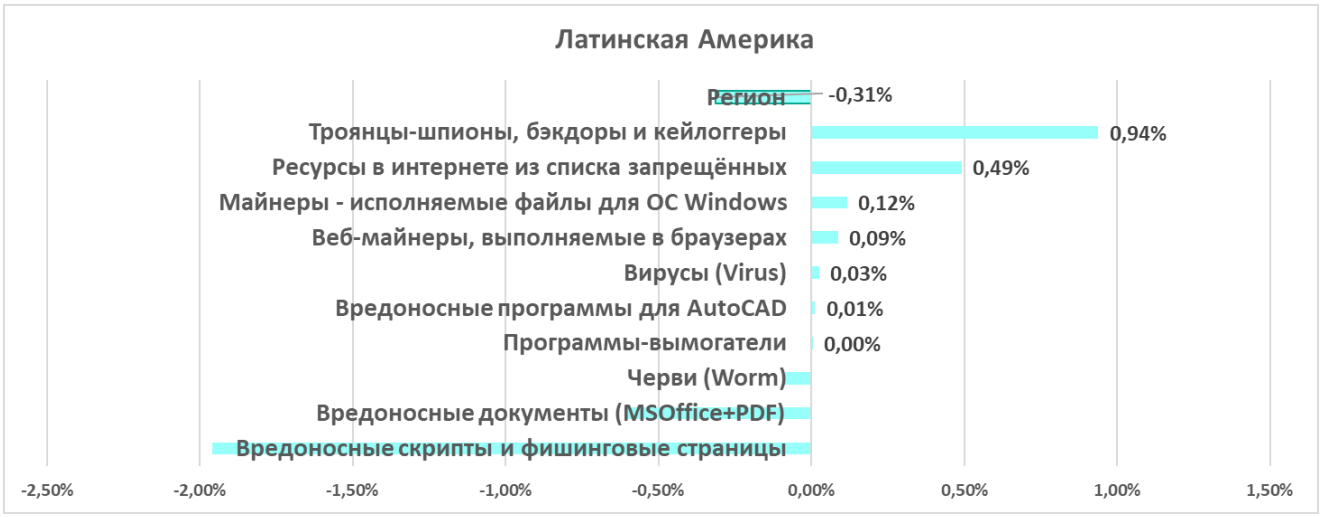


- Программы-шпионы — в 1,2 раза

- Веб-майнеры

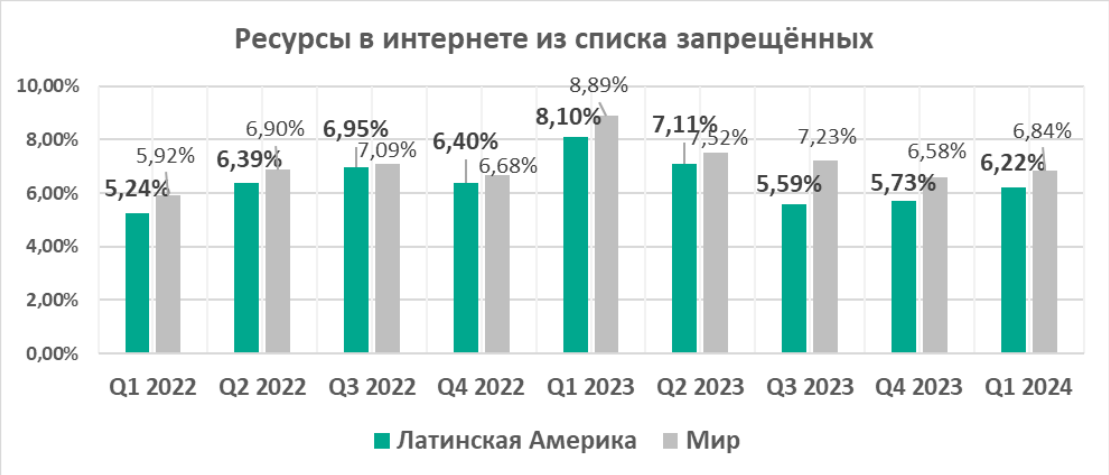


Изменения за квартал



Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Программы-шпионы — в 1,3 раза
- Ресурсы в интернете из списка запрещённых, потихоньку растет второй квартал подряд.



Актуальные угрозы

- Вредоносные скрипты и фишинговые страницы
- Вредоносные документы
- Программы-шпионы
- Угрозы из почты

Всё свидетельствует о том, что технологические системы в регионе сильно подвержены фишинговым атакам.

Промышленным организациям в регионе следует уделять больше внимания этой угрозе. Необходимо сфокусироваться как на использовании автоматизированных средств защиты от фишинга, так и на обучении сотрудников. В текущей ситуации следует оценивать риск целевых атак напрямую на технологические сегменты сети как высокий.

Южная Азия

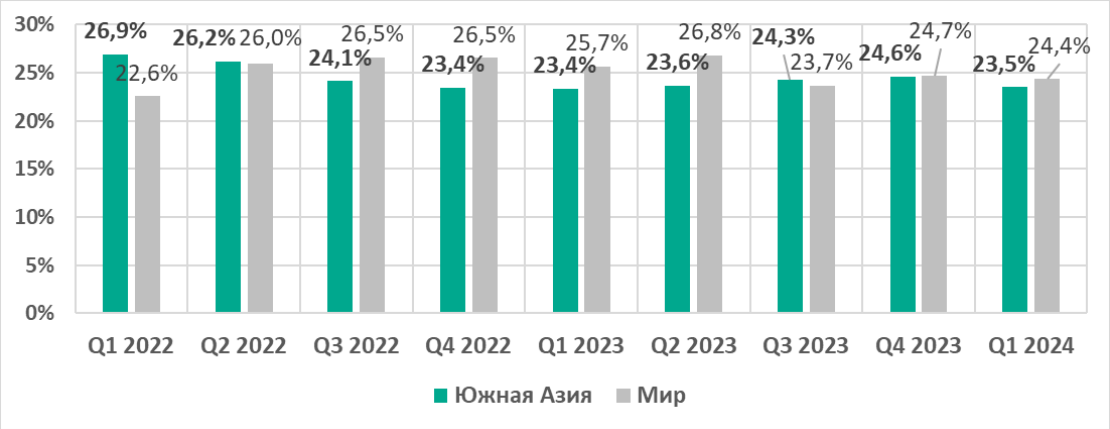
Среди регионов

Восьмое место в рейтинге регионов.

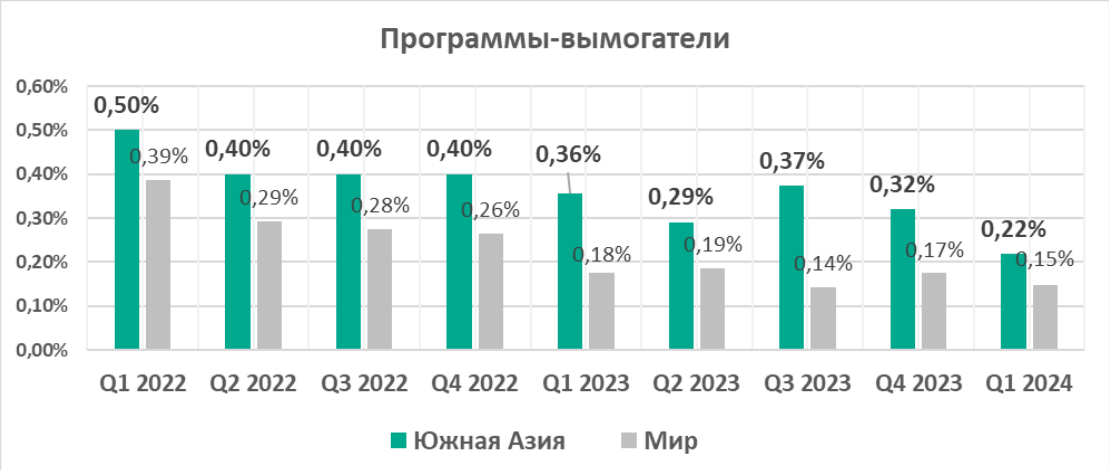
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы при подключении **съёмных носителей**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **угрозы в сетевых папках**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **угрозы из интернета**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **ресурсы в интернете из списка запрещённых**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **программы-вымогатели**.

Регион vs мир

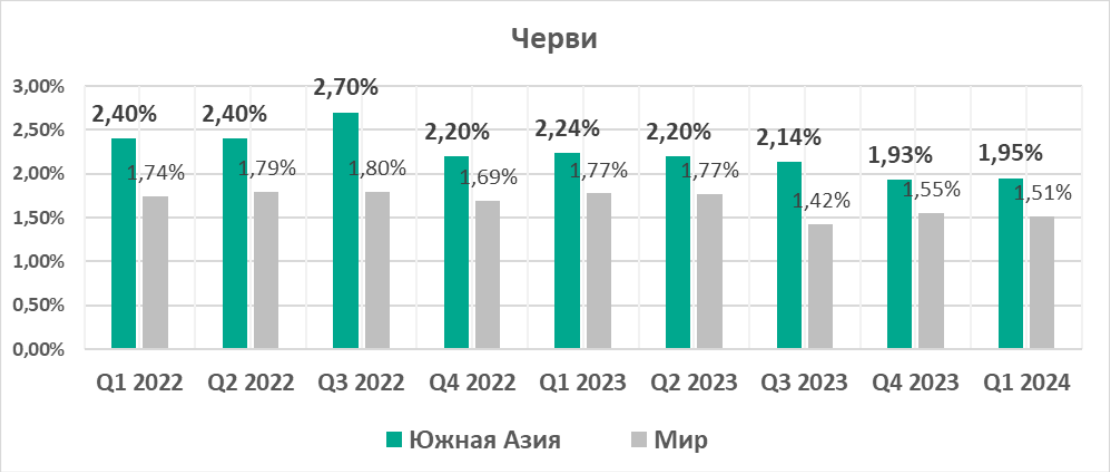
- С третьего квартала 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в регионе, близок к средним по миру показателям.



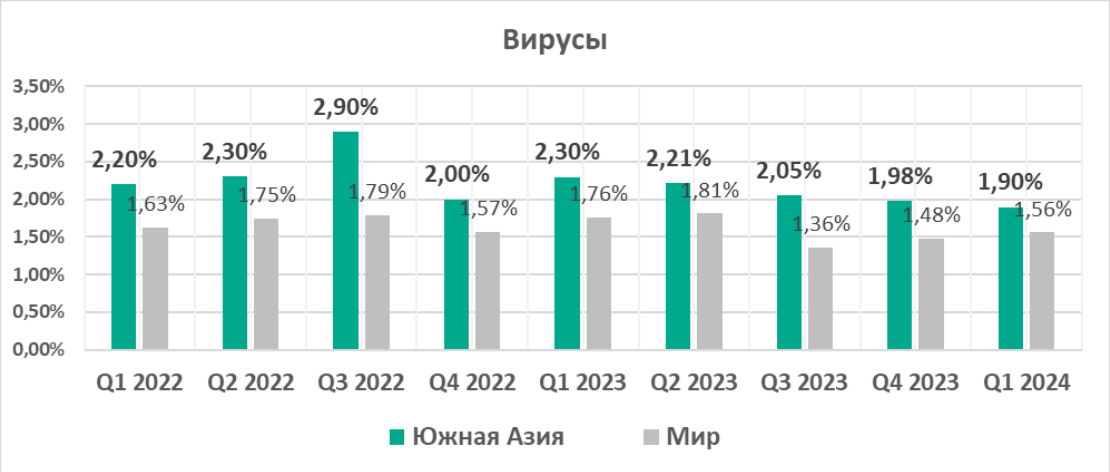
- В регионе заметно выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Программы-вымогатели — в 1,5 раза



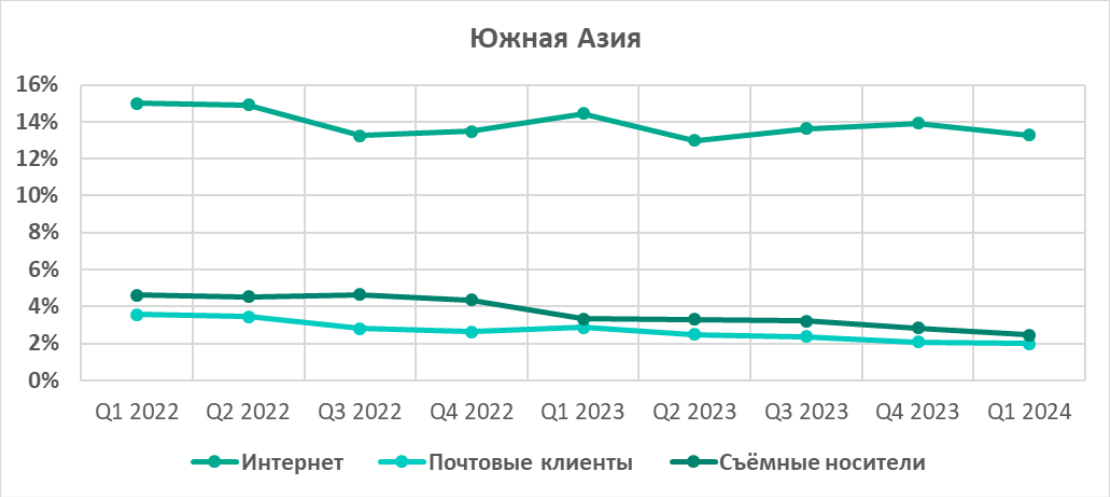
- Черви — в 1,3 раза. **Черви на четвертом месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на шестом).



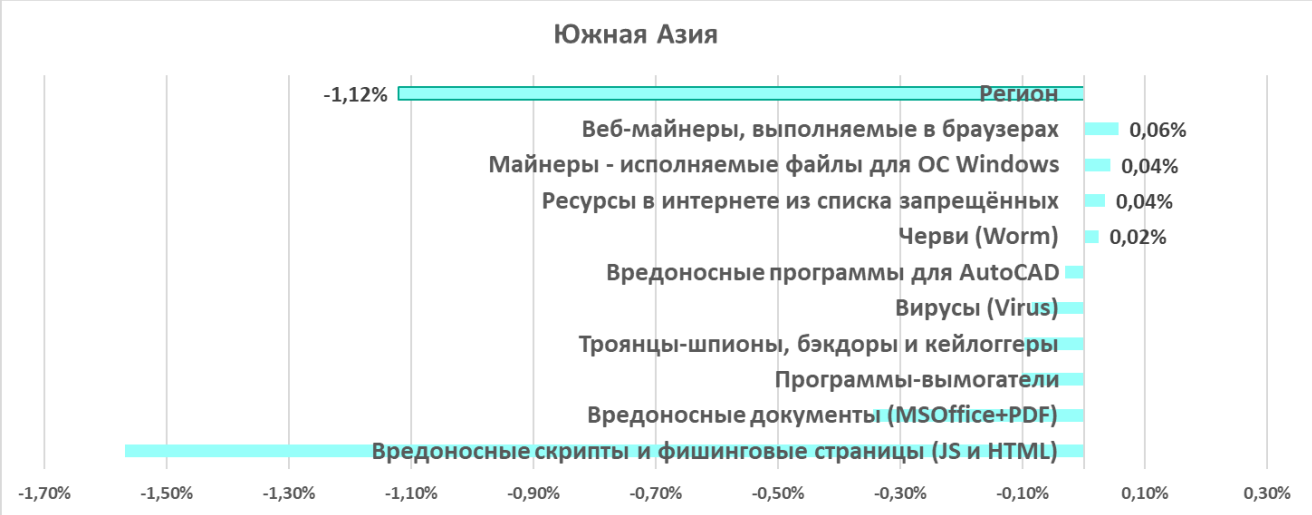
- Вирусы — в 1,2 раза



- **Съёмные носители** в Южной Азии на втором месте в рейтинге источников угроз по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты из разных источников.
  Один из трех регионов, где процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съёмных носителей, превысил процент компьютеров АСУ, на которых были заблокированы угрозы из электронной почты.



Изменения за квартал



Актуальные угрозы

- Скомпрометированные и вредоносные интернет-ресурсы
- Программы-вымогатели
- Черви
- Вирусы
- Угрозы, распространяющиеся на съёмных носителях
- Угрозы в сетевых папках

Высокий процент компьютеров, столкнувшихся с угрозами, распространяющимися через сетевые папки и съёмные носители, и высокие показатели по самораспространяющемуся вредоносному ПО говорят о том, что значительная часть промышленной инфраструктуры в регионе не защищена. Промышленным предприятиям в регионе следует также уделять больше внимания обучению сотрудников кибергигиене.

Южная Европа

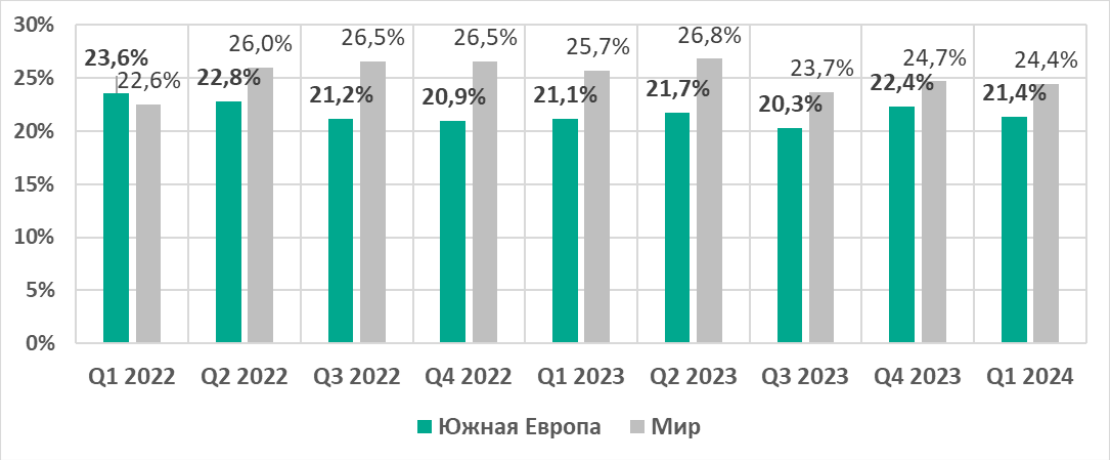
Среди регионов

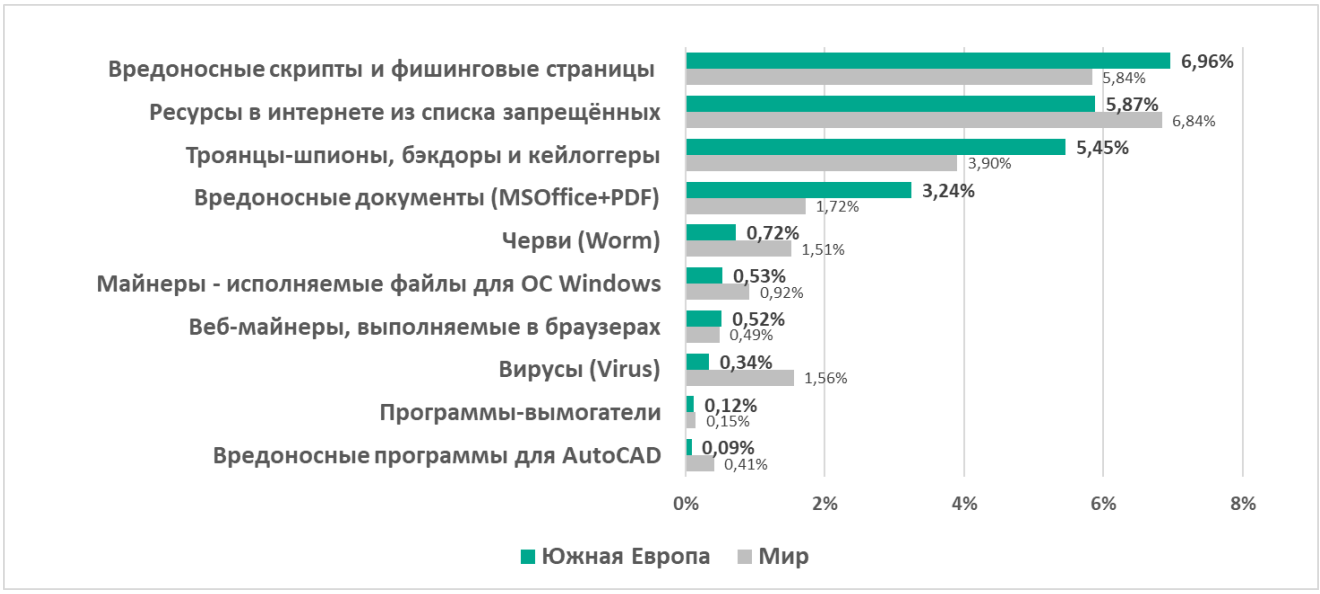
Девятое место в рейтинге регионов.

- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные документы**.
- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **угрозы из почты.**
- **На втором месте** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **программы-шпионы**.

Регион vs мир

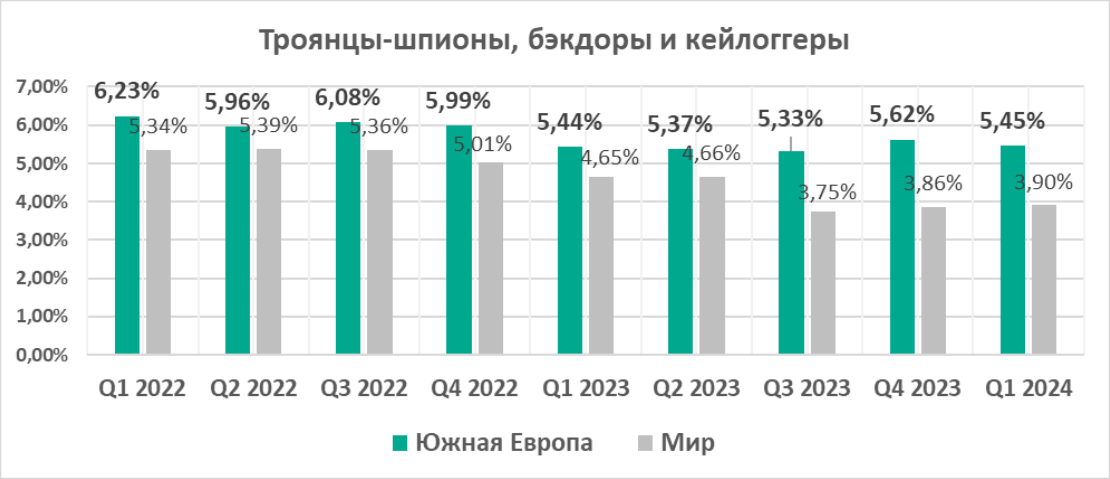
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в регионе, меньше, чем в среднем по миру.





- В регионе выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Вредоносные документы — в 1,9 раза

- Программы-шпионы — в 1,4 раза

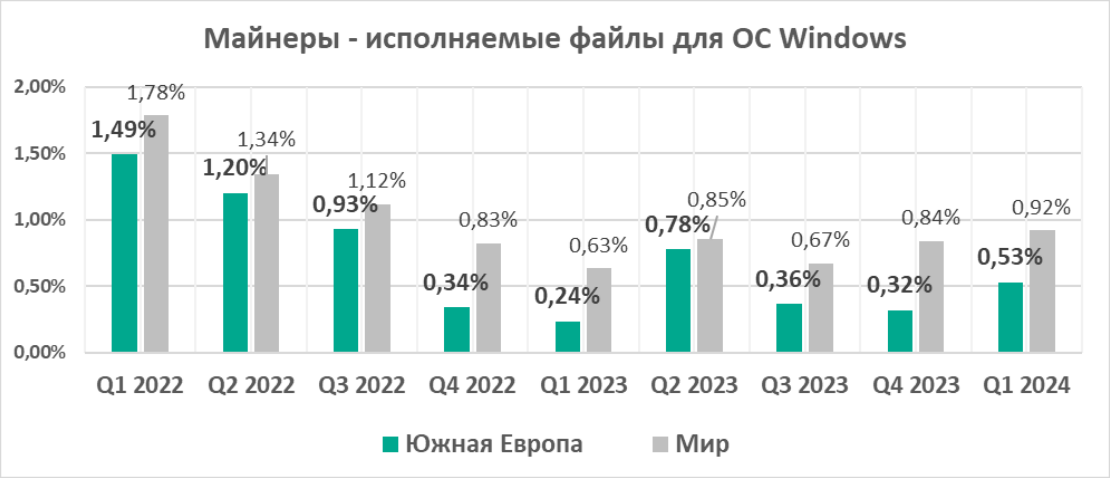


- Вредоносные скрипты и фишинговые страницы — в 1,2 раза

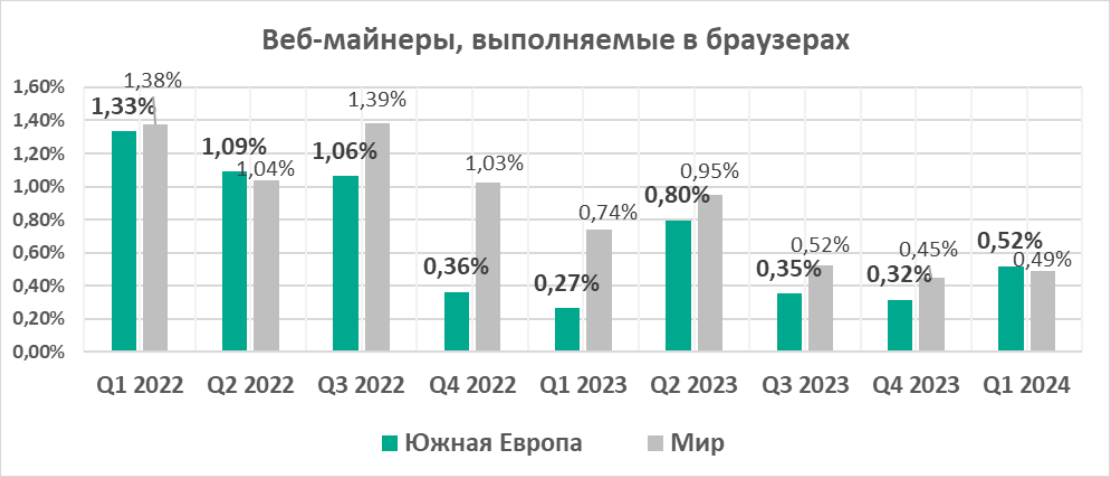
Изменения за квартал

Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты:

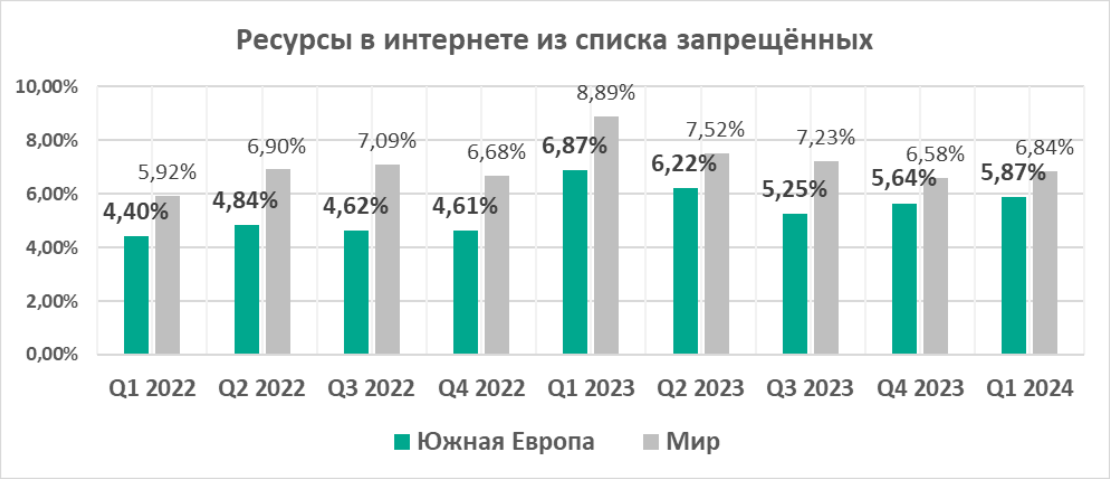
- Майнеры — исполняемые файлы для ОС Windows — в 1,7 раза



- Веб-майнеры — в 1,6 раза. В результате процент в регионе превысил процент в мире.



- Процент компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещённых, потихоньку растет в Южной Европе второй квартал подряд.



Актуальные угрозы

- Вредоносные документы
- Программы-шпионы
- Вредоносные скрипты и фишинговые страницы
- Угрозы из почты

Всё говорит о высоком уровне угрозы фишинговых атак на промышленную инфраструктуру в регионе. Фишинг — один из излюбленных способов первоначальной компрометации у злоумышленников, сосредоточенных на целевых атаках, — APT, вымогательстве, BEC и атаках хактивистов.

Восточная Азия

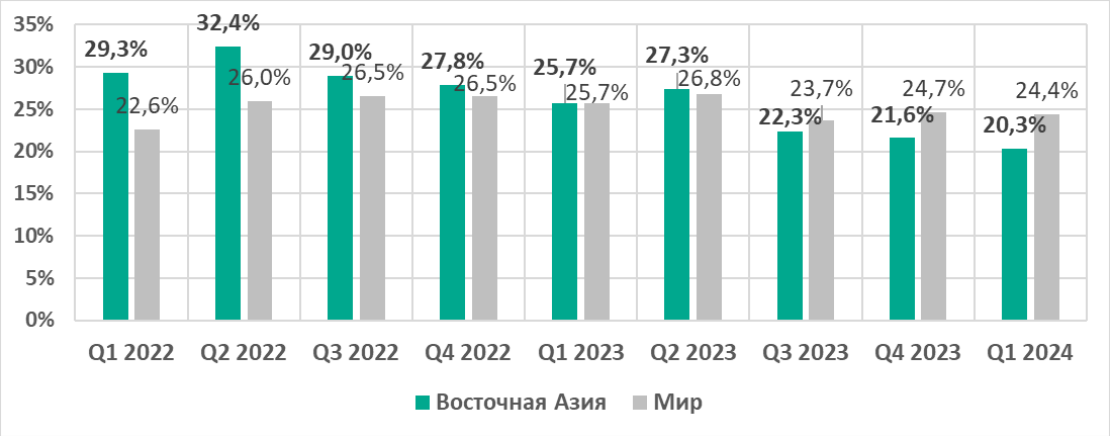
Среди регионов

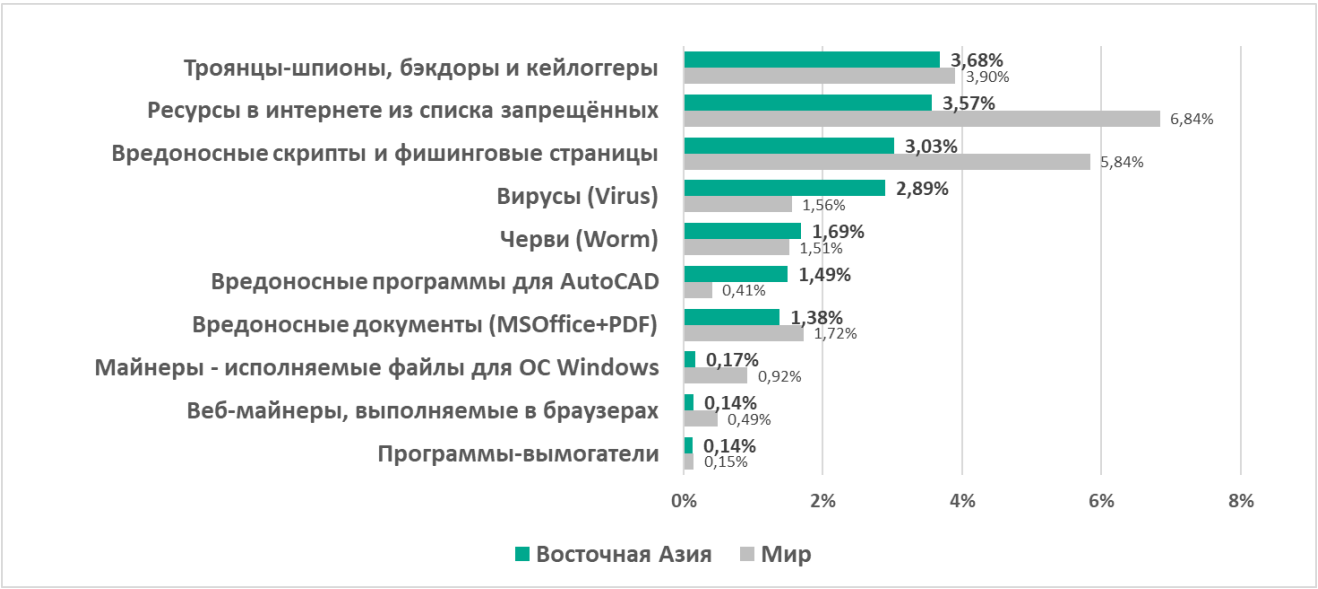
Десятое место в рейтинге регионов.

- **На втором месте** по проценту компьютеров АСУ, на которых было заблокировано **вредоносное ПО для AutoCAD**.
- **На третьем месте** по проценту компьютеров АСУ, на которых были заблокированы **вирусы**.
- **Единственный регион, в котором программы-шпионы на первом месте в рейтинге** категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.

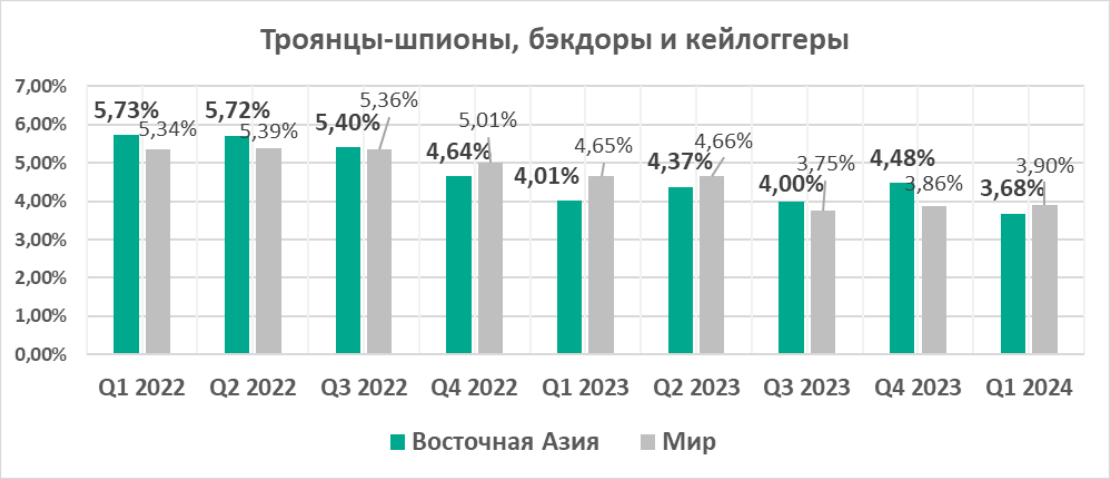
Регион vs мир

- С третьего квартала 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в регионе, меньше аналогичного показателя в мире.

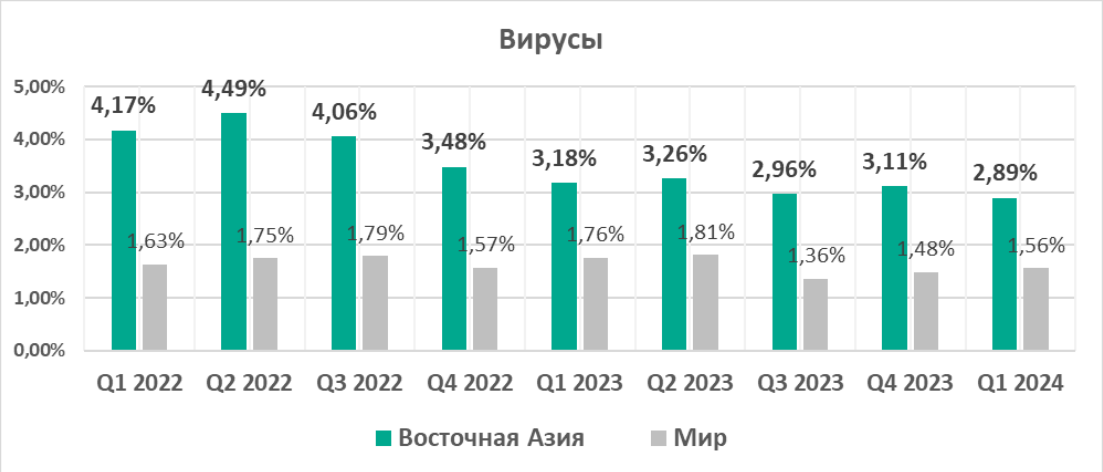




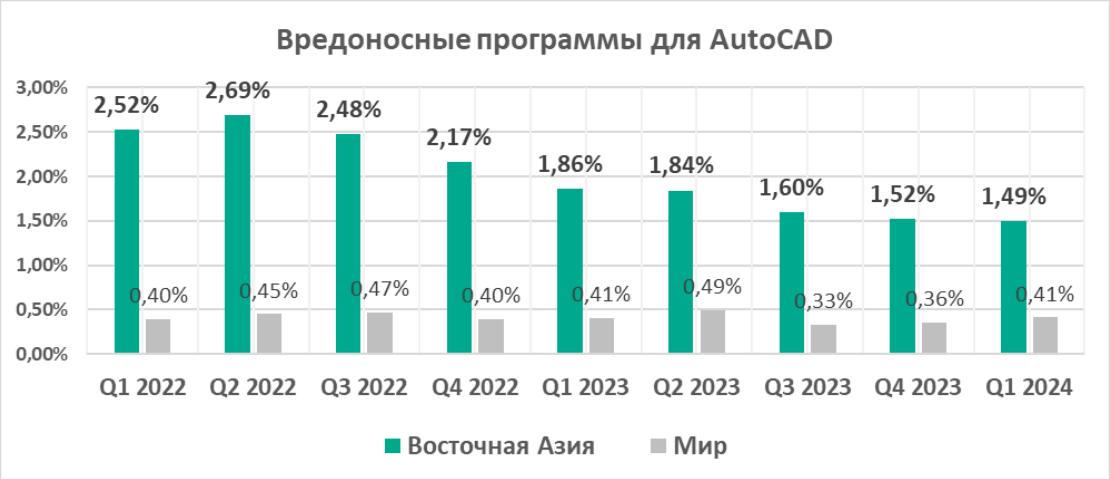
- **Программы-шпионы на первом** месте в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на третьем).



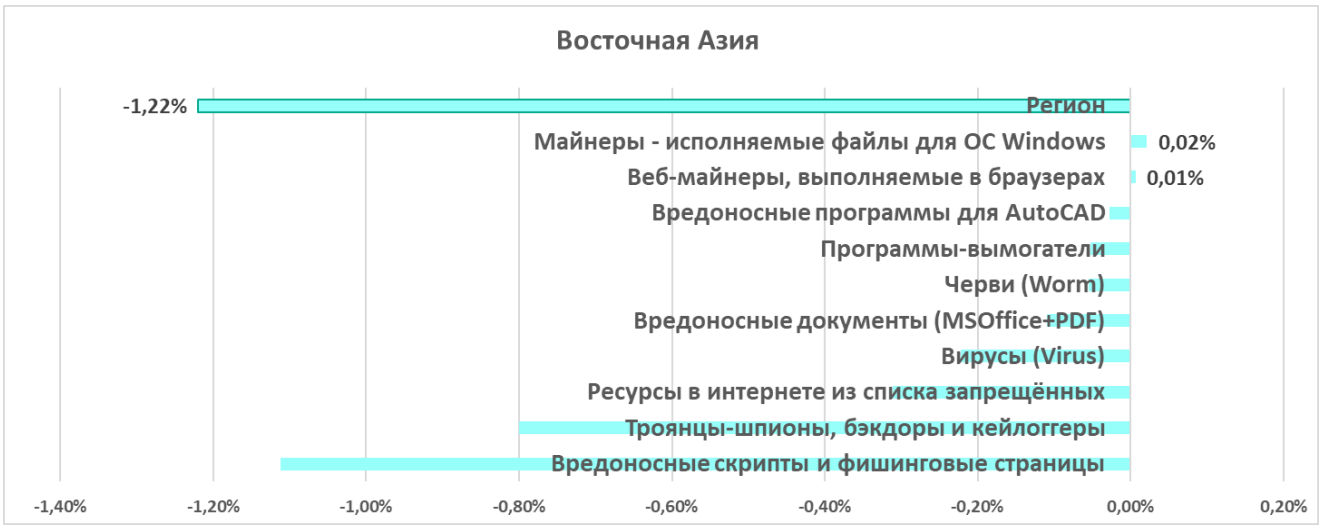
- В регионе заметно выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Вирусы — в 1,9 раза



- Вредоносные программы для AutoCAD — в 3,6 раза



Изменения за квартал



Актуальные угрозы

- Программы-шпионы
- Вирусы
- Вредоносные программы для AutoCAD

Вероятно, активное применение злоумышленниками шпионских программ приводит к высокому проценту скомпрометированных данных аутентификации в технологических системах промышленных предприятий — что существенно увеличивает риски последующих целевых атак.

Австралия и Новая Зеландия

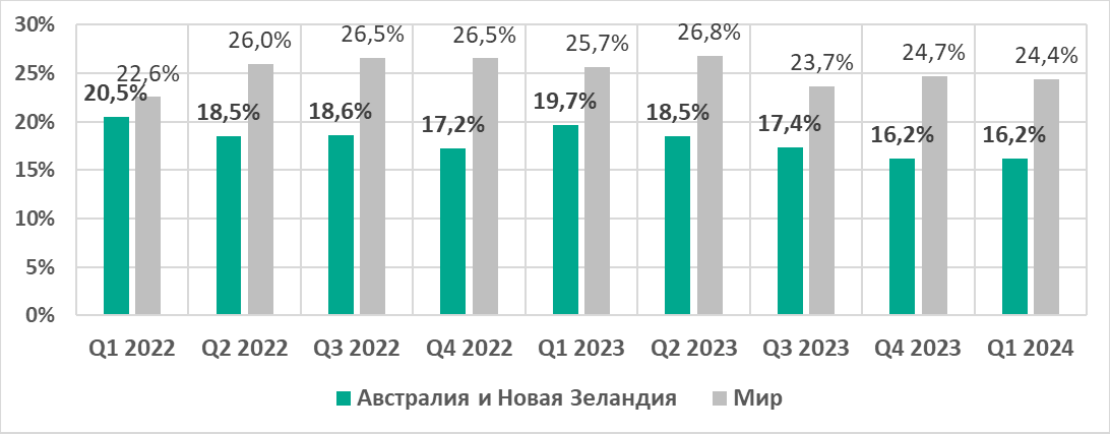
Среди регионов

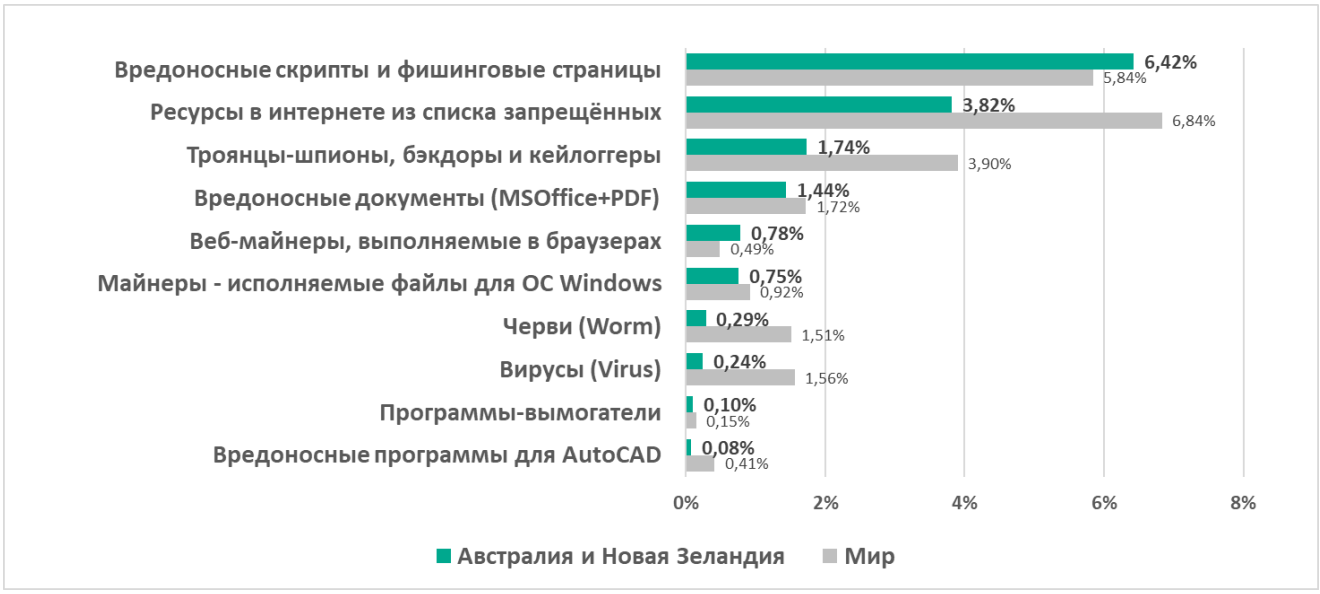
Одиннадцатое место в рейтинге регионов.

- На третьем месте по проценту компьютеров АСУ, на которых были заблокированы **веб-майнеры**.
- Один из трех регионов, где **веб-майнеры на пятом месте в рейтинге** категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в остальных регионах ниже, в мире — на восьмом).
- Процент компьютеров АСУ, на которых были заблокированы веб-майнеры, в Австралии и Новой Зеландии вырос на максимальные среди регионов 0,43 п.п.
- Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, в Австралии и Новой Зеландии вырос на максимальные среди регионов 0,44 п.п.

Регион vs мир

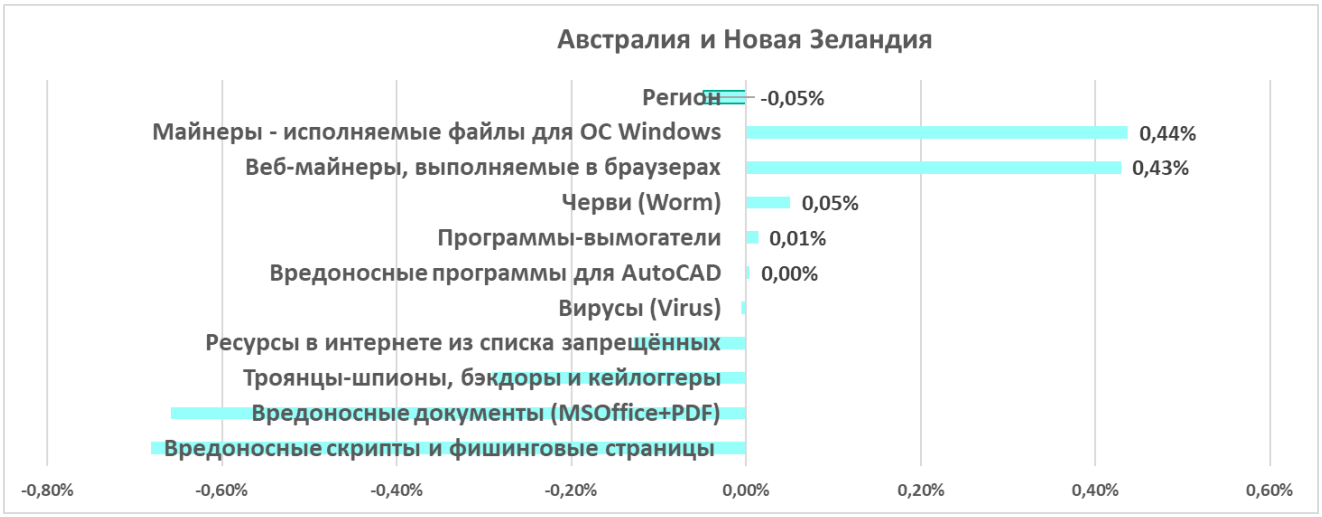
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионе меньше аналогичного показателя в мире.





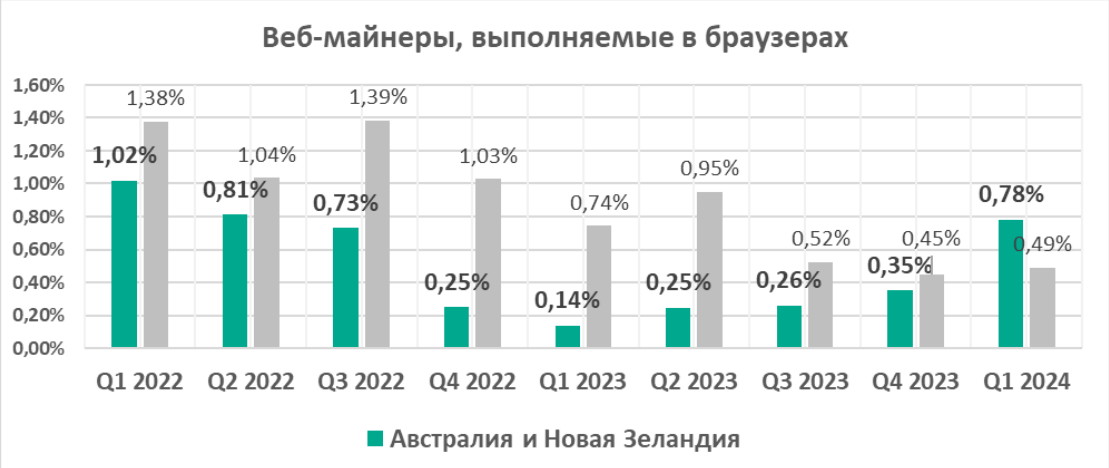
- В регионе выше, чем в среднем по миру, процент компьютеров АСУ, на которых были заблокированы:
  - Веб-майнеры — в 1,6 раза. Веб-майнеры на пятом месте в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на восьмом).
  - Вредоносные скрипты и фишинговые страницы

Изменения за квартал

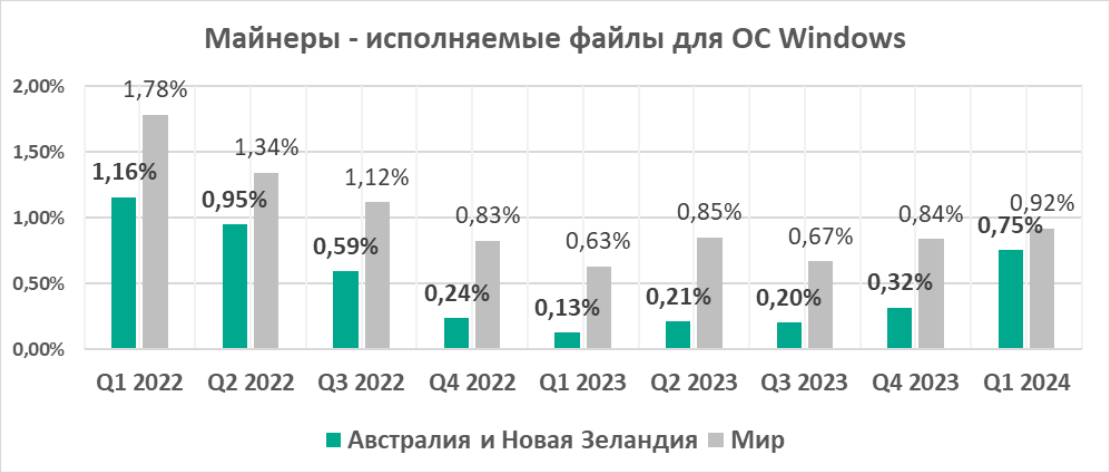


Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Веб-майнеры — в 2,2 раза. В результате процент в регионе превысил процент в мире.

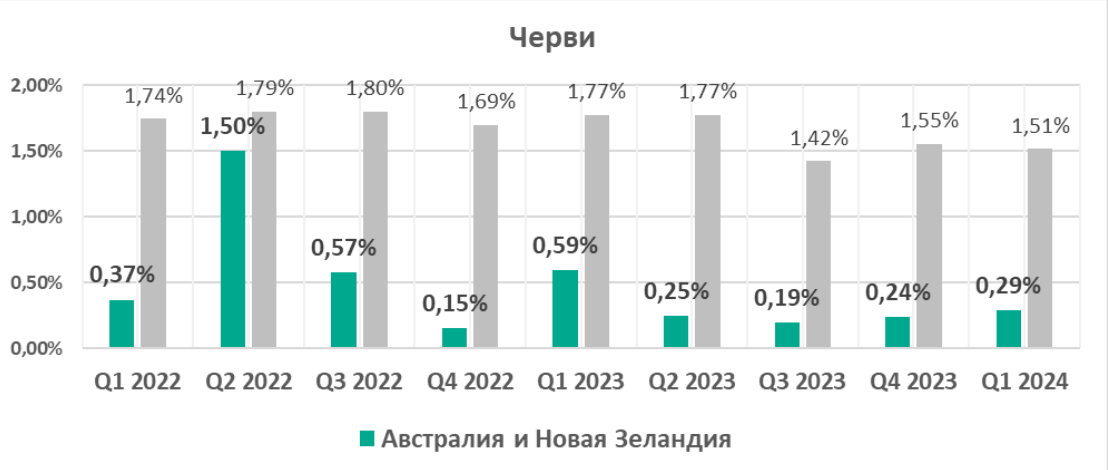


- Майнеры — исполняемые файлы для ОС Windows — в 2,4 раза



Процент компьютеров АСУ, на которых блокируются вредоносные майнеры, растет для обеих категорий со второго квартала 2023 года.

- Черви — в 1,2 раза. Процент по этой категории растет уже второй квартал подряд.



Актуальные угрозы

- Веб-майнеры
- Майнеры — исполняемые файлы для ОС Windows
- Вредоносные скрипты и фишинговые страницы

США и Канада

Среди регионов

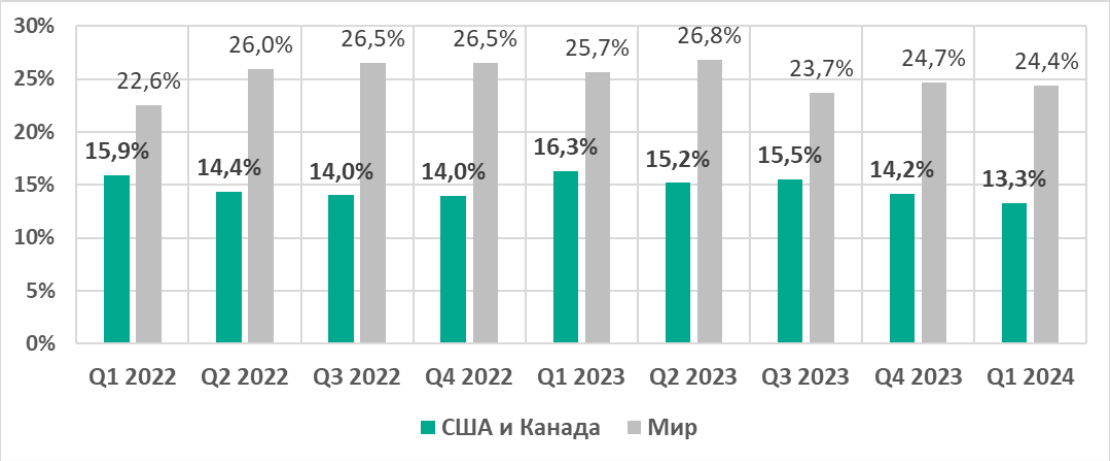
Двенадцатое место в рейтинге регионов.

Один их трех самых благополучных регионов, с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты.

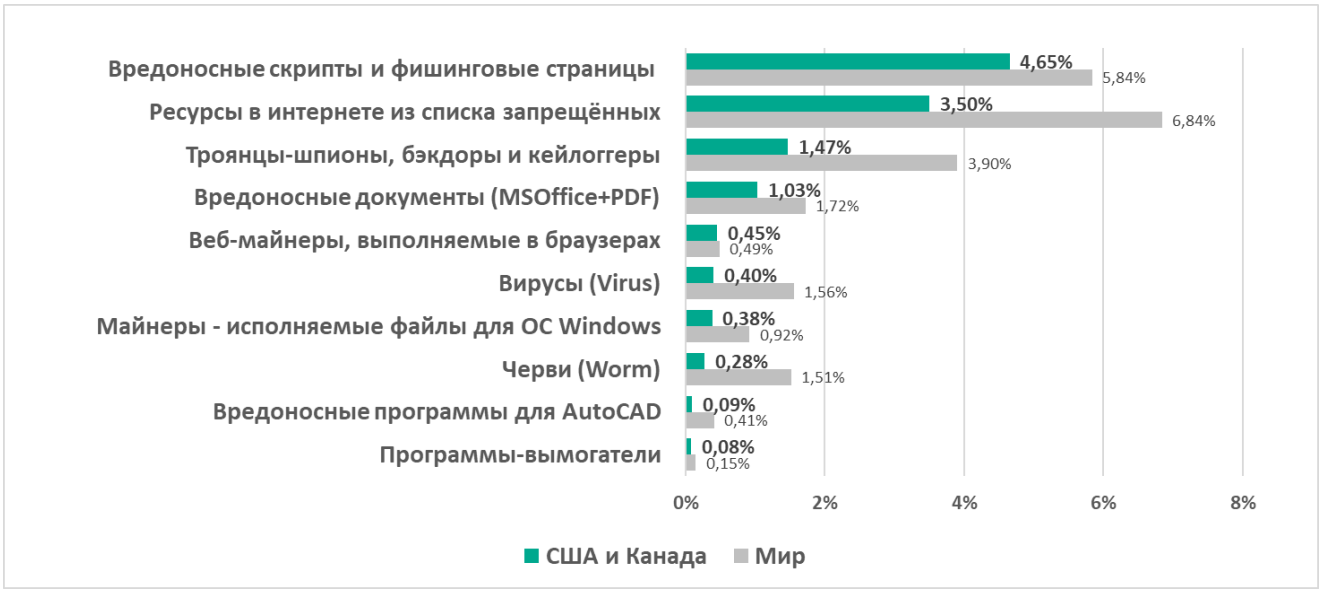
- Один из трех регионов, где **веб-майнеры на пятом месте в рейтинге** категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в остальных регионах ниже, в мире — на восьмом).

Регион vs мир

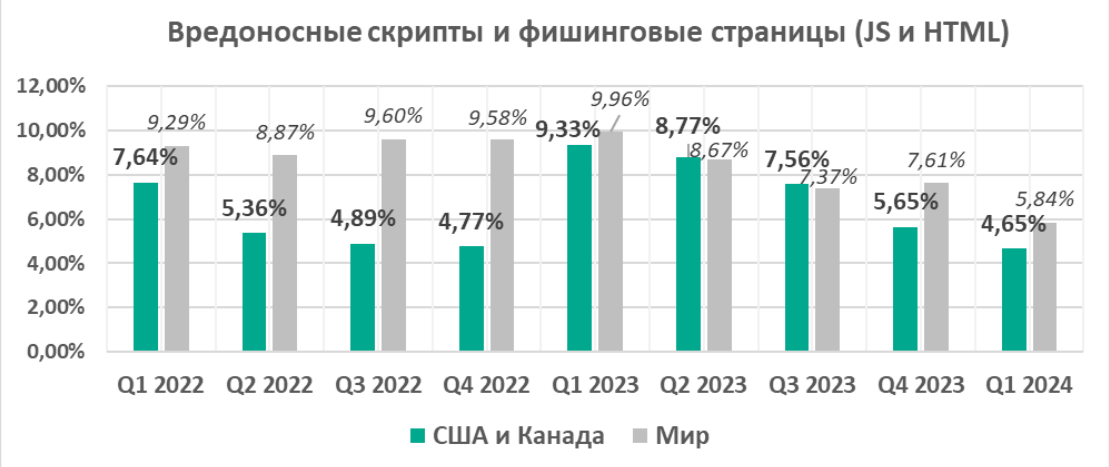
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионе заметно меньше аналогичного показателя в мире.



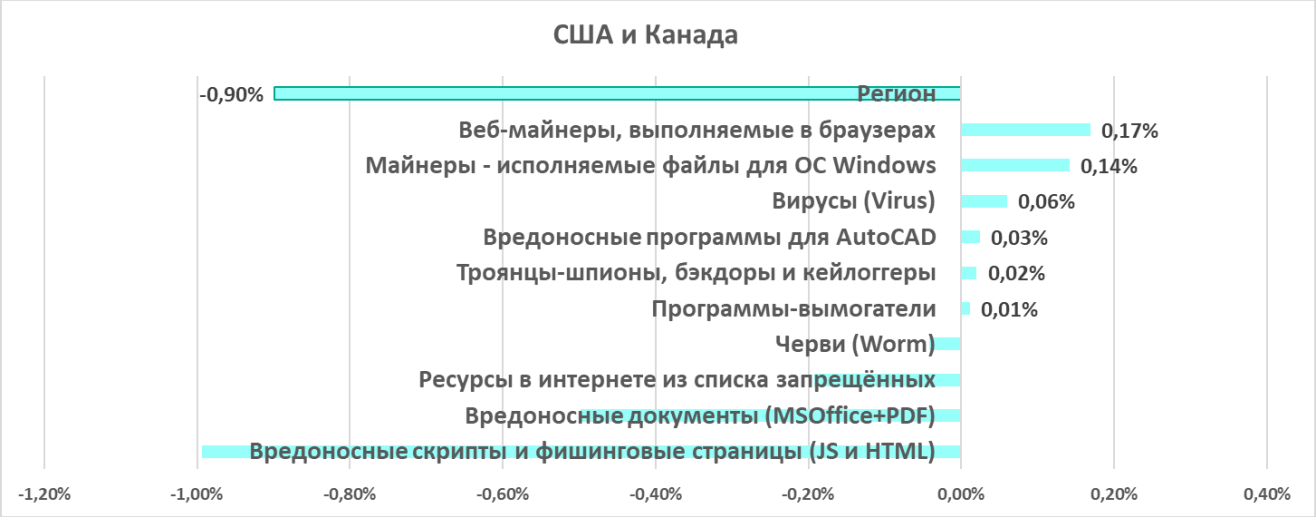
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, в регионе ниже, чем в среднем по миру, для всех категорий.



- **Веб-майнеры на пятом месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на восьмом).
- С 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы в регионе, близок к среднему в мире.

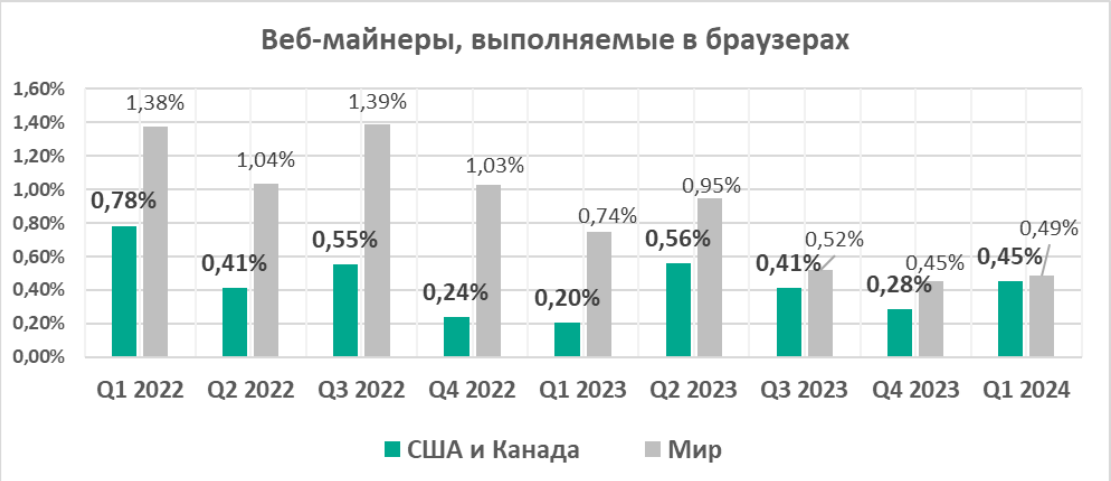


Изменения за квартал

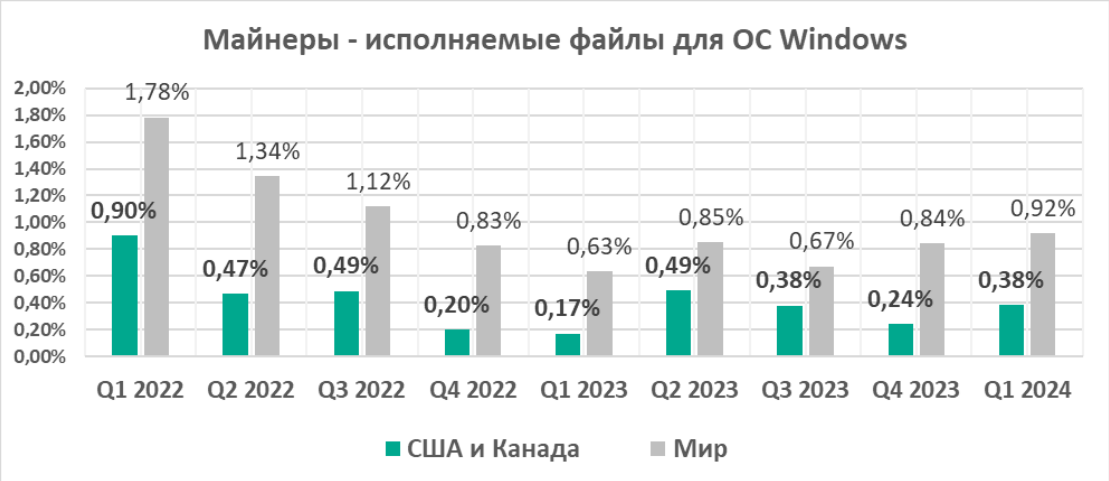


Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

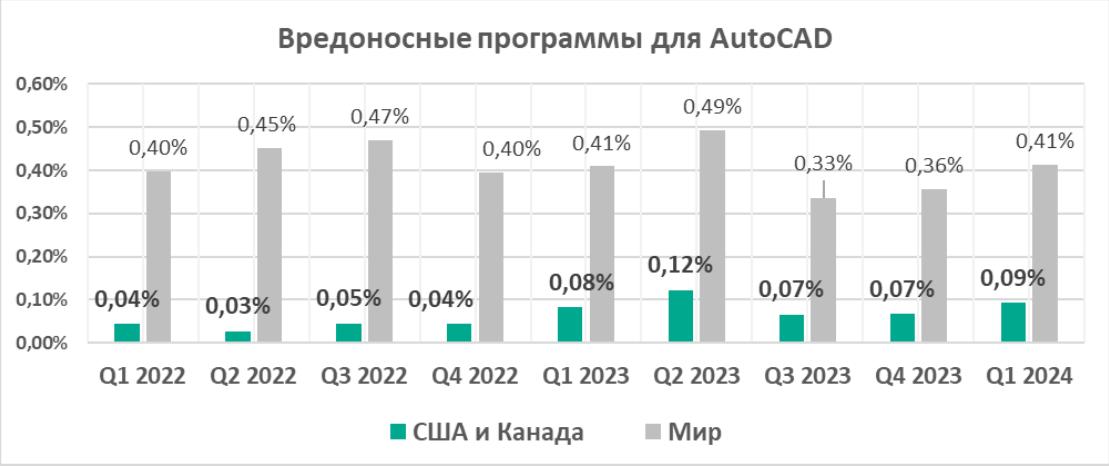
- Веб-майнеры — в 1,6 раза. В результате процент по веб-майнерам в регионе оказался близким к проценту в мире.



- Майнеры — исполняемые файлы для ОС Windows — в 1,6 раза



- Вредоносные программы для AutoCAD — в 1,4 раза



Актуальные угрозы

- Вредоносные скрипты и фишинговые страницы

В первом квартале 2024 года вырос процент компьютеров АСУ, на которых были заблокированы:

- Веб-майнеры
- Майнеры — исполняемые файлы для ОС Windows
- Вредоносные программы для AutoCAD

По совокупности показателей регион в целом благополучный.

Западная Европа

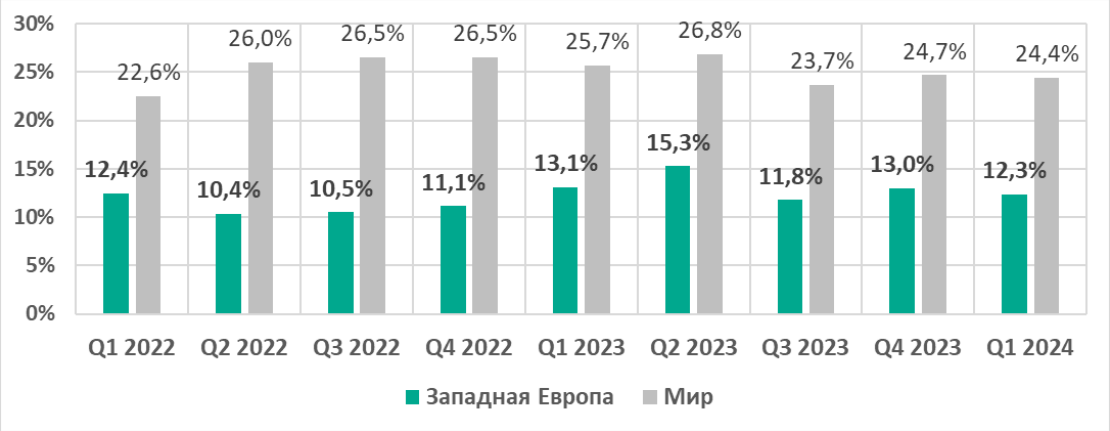
Среди регионов

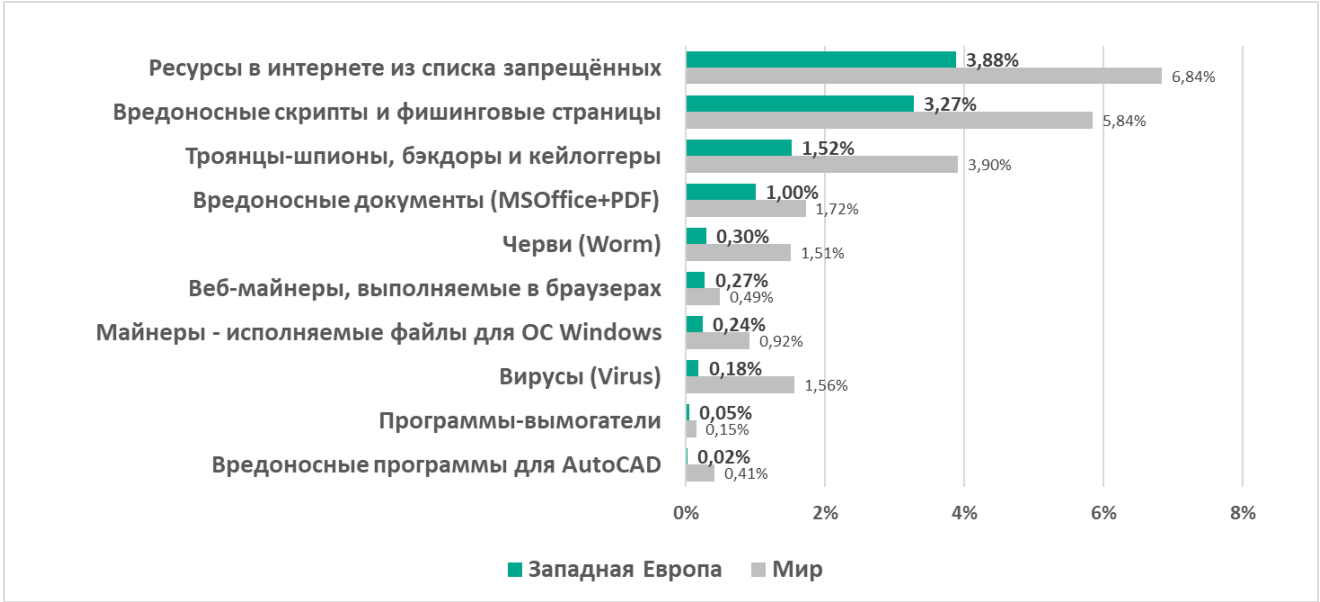
Тринадцатое место в рейтинге регионов.

Один их трех самых благополучных регионов, с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты.

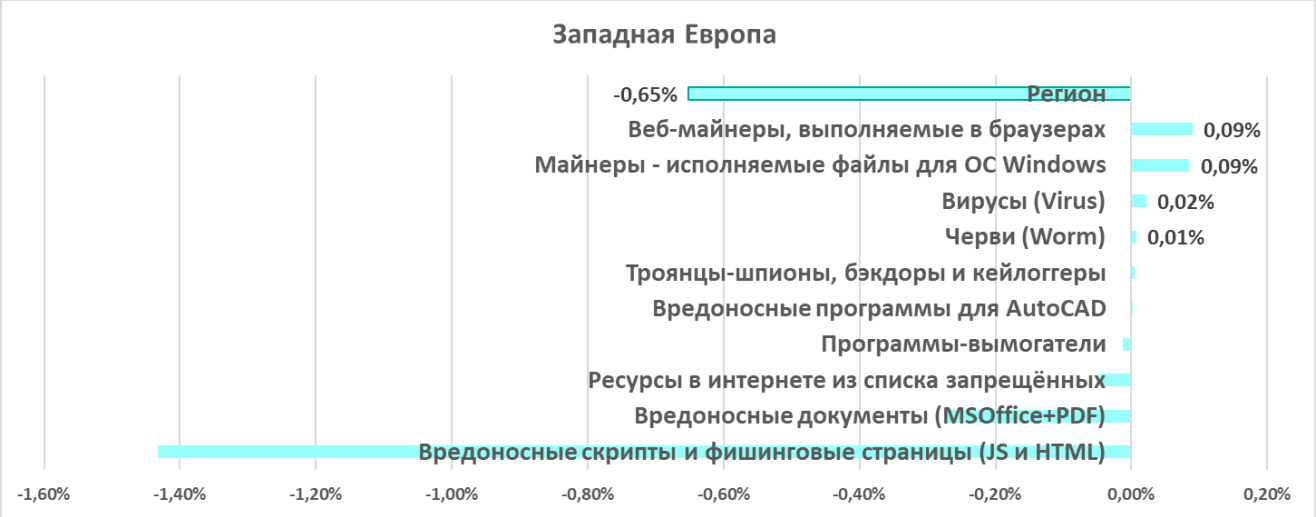
Регион vs мир

- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионе заметно меньше аналогичного показателя в мире.



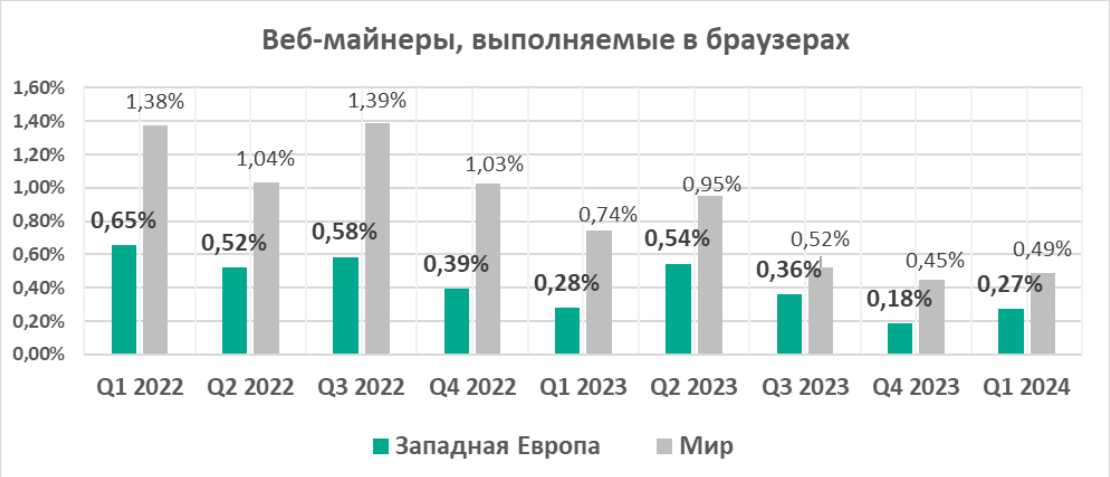


Изменения за квартал

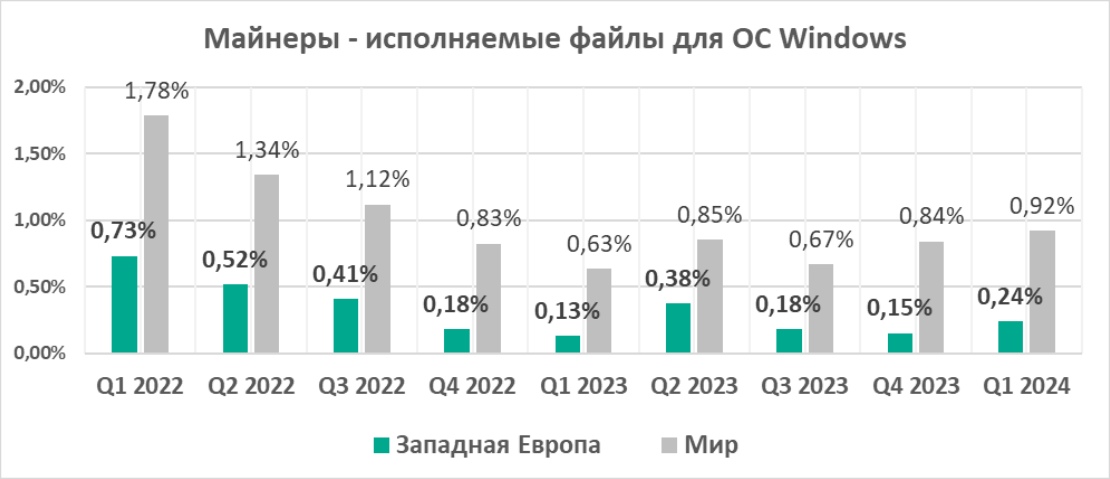


Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Веб-майнеры — в 1,5 раза



- Майнеры — исполняемые файлы для ОС Windows — в 1,5 раз



Актуальные угрозы

В первом квартале 2024 года вырос процент компьютеров АСУ, на которых были заблокированы:

- Майнеры — исполняемые файлы для ОС Windows
- Веб-майнеры

Регион в целом благополучный.

Северная Европа

Среди регионов

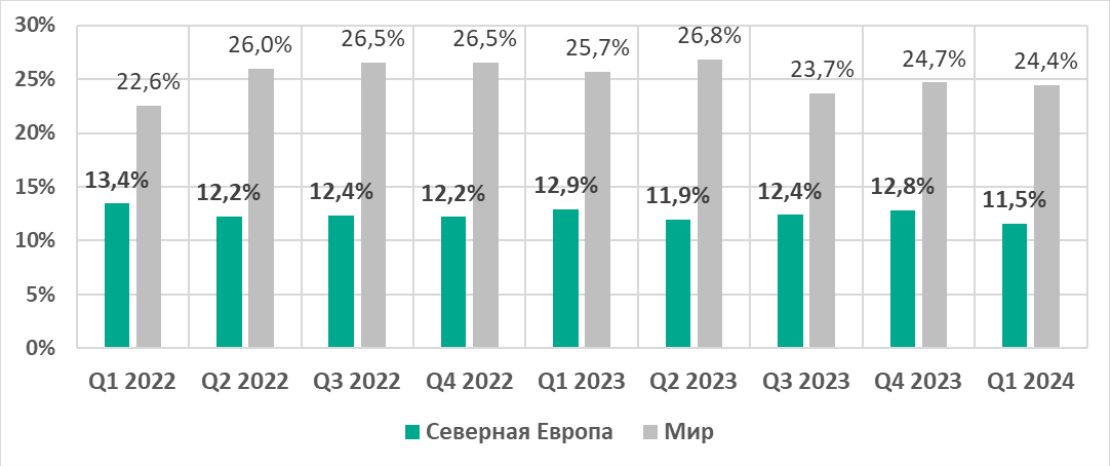
Четырнадцатое место в рейтинге регионов.

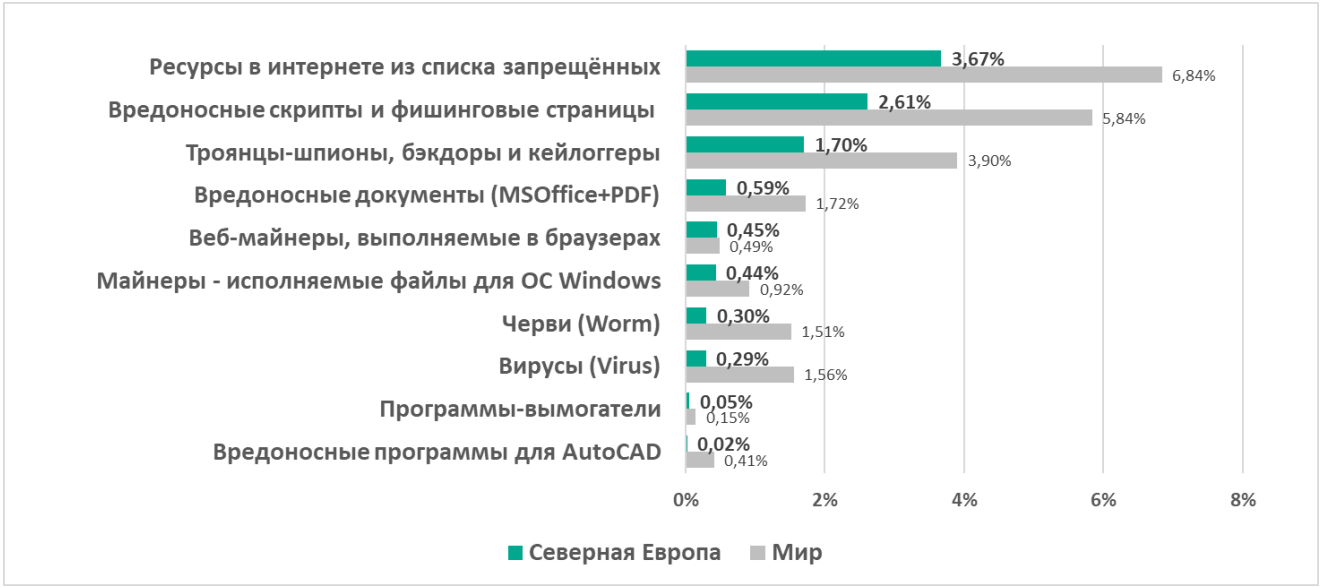
Традиционно регион с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты.

- Один из трех регионов, где **веб-майнеры на пятом месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на восьмом).

Регион vs мир

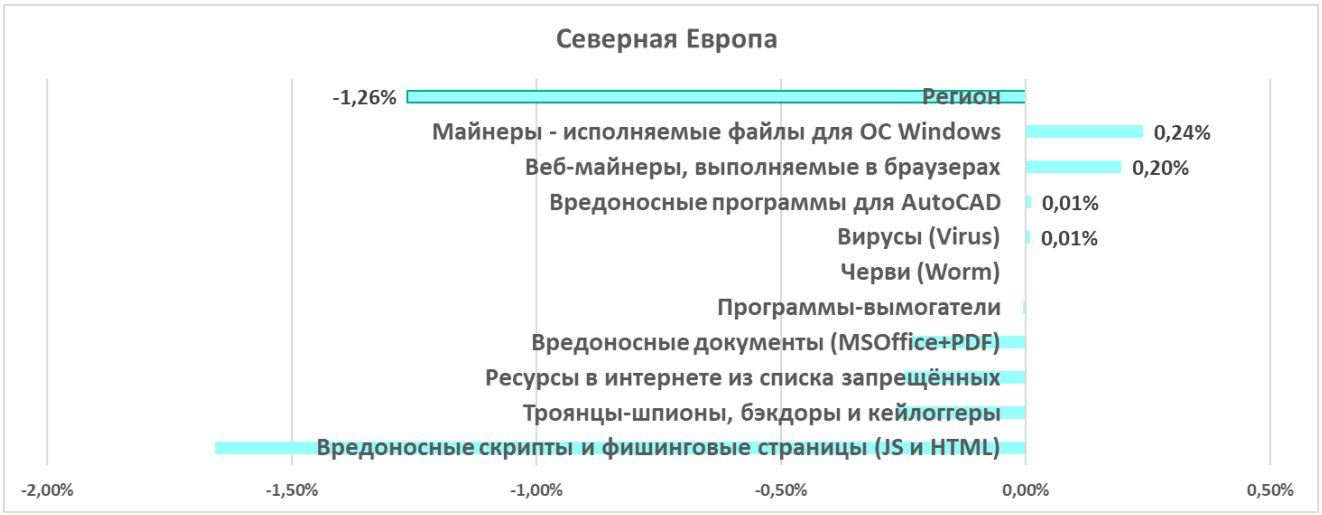
- Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионе заметно меньше аналогичного показателя в мире.





- **Веб-майнеры на пятом месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано (в мире — на восьмом).

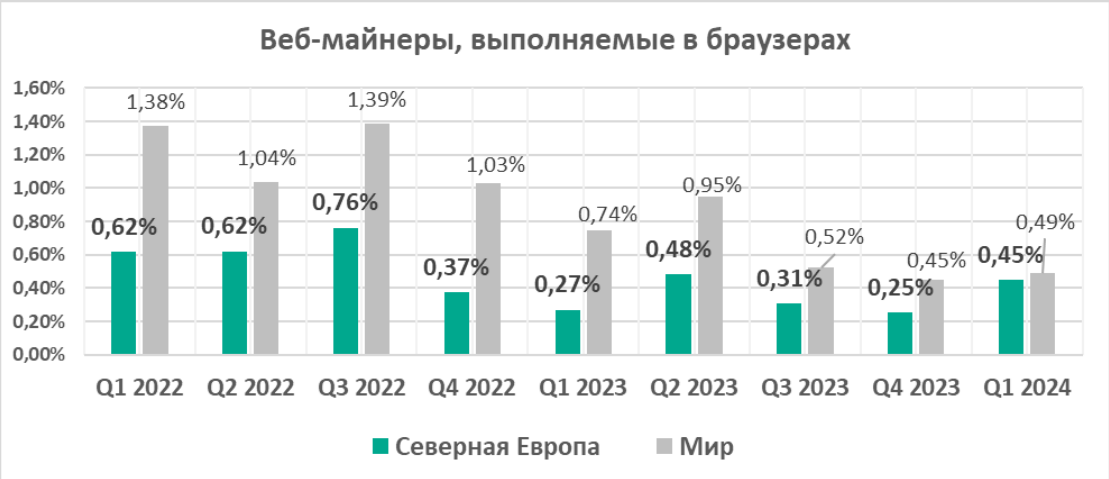
Изменения за квартал



Максимально за квартал вырос процент компьютеров АСУ, на которых были заблокированы:

- Майнеры — исполняемые файлы для ОС Windows — в 2,2 раза. Процент в первом квартале самый высокий с конца 2022 года.

- Веб-майнеры — в 1,8 раза. В результате процент по веб-майнерам в регионе оказался близким к проценту в мире.



Актуальные угрозы

Регион с наименьшим процентом атакованных компьютеров АСУ.

В первом квартале 2024 года вырос процент компьютеров АСУ, на которых были заблокированы:

- Майнеры — исполняемые файлы для ОС Windows
- Веб-майнеры

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