Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Регионы, второй квартал 2024

21.11.2024

Version 1.3

Обзор второго квартала 2024 года ... 2
Общая статистика по регионам ... 2
Категории вредоносного ПО ... 4
Регионы. Некоторые особенности ... 21
Африка ... 22
Юго-Восточная Азия ... 32
Центральная Азия ... 42
Ближний Восток ... 52
Восточная Европа ... 63
Россия ... 72
Латинская Америка ... 81
Южная Азия ... 91
Восточная Азия ... 101
Южная Европа ... 111
Австралия и Новая Зеландия ... 120
США и Канада ... 130
Западная Европа ... 138
Северная Европа ... 147
Методика подготовки статистики ... 156

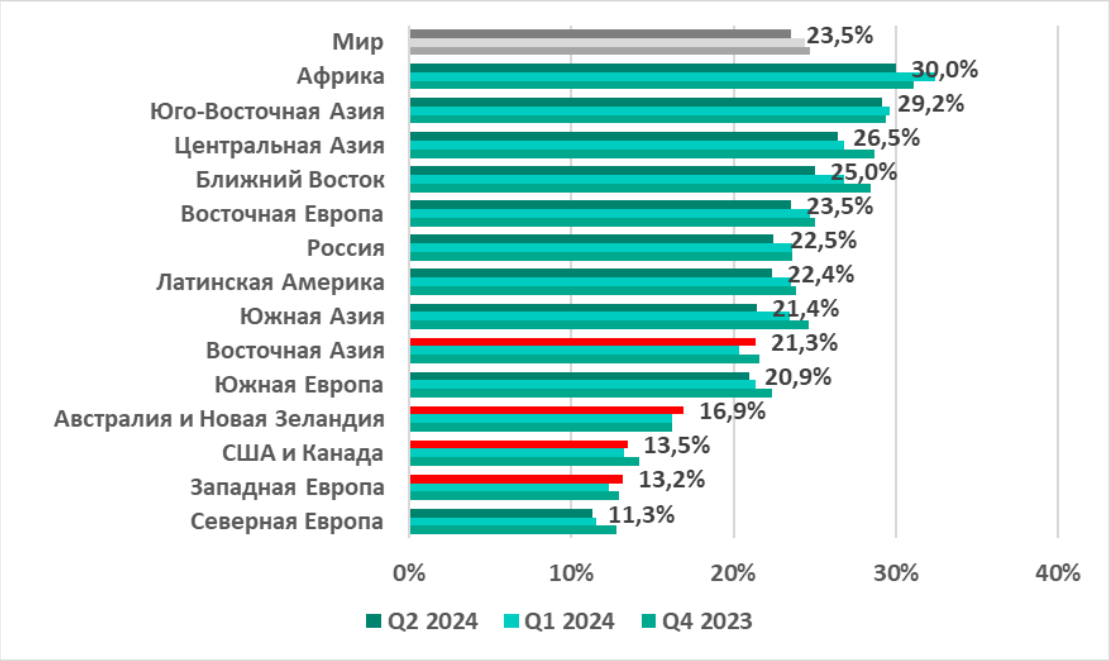
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Обзор второго квартала 2024 года

Общая статистика по регионам

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

Значение этого параметра в различных регионах разное — от 11,3% в Северной Европе до 30% в Африке.



В зависимости от значения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, все регионы можно разделить на три группы:

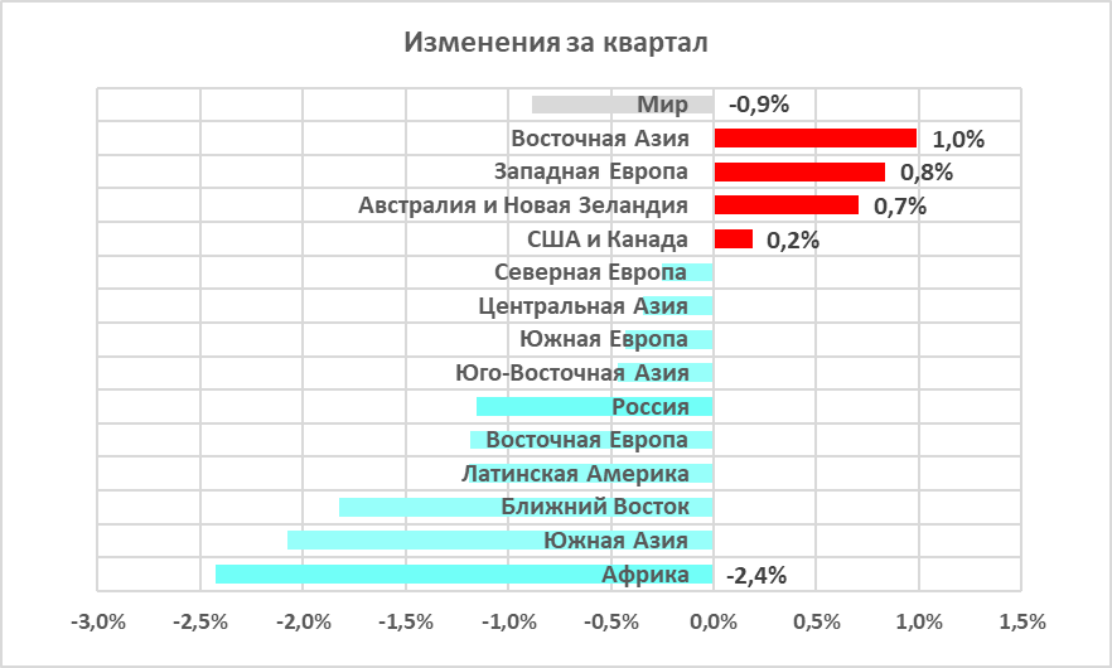
Больше 25%:

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

В регионах этой группы компьютеры в технологических сетях особенно подвержены киберугрозам. Характерной проблемой для этих регионов является недостаточный уровень инвестиций в кибербезопасность. Это касается как внедрения защитных инструментов и мер, так и решения проблем нехватки специалистов, формирования культуры кибербезопасности и повышения осведомленности.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

20–25%: Ближний Восток — 25,0% 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 испытывать специфические трудности при попытках изолировать свою технологическую инфраструктуру от некоторых киберугроз.
До 20%: Австралия и Новая Зеландия — 16,9% США и Канада — 13,5% Западная Европа — 13,2% Северная Европа — 11,3%	В эту группу входят регионы, наиболее благополучные с точки зрения доступности технологической инфраструктуры для киберугроз.



По сравнению с предыдущим кварталом, во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась в четырех регионах.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории вредоносного ПО

Доля компьютеров АСУ, на которых блокируется вредоносное ПО различных категорий, отличается в разных регионах. При этом позиции регионов в рейтингах по этому показателю не всегда совпадают с позициями в рейтинге по доле компьютеров АСУ, на которых была заблокирована какая-либо угроза.

Вредоносные объекты, используемые для первичного заражения

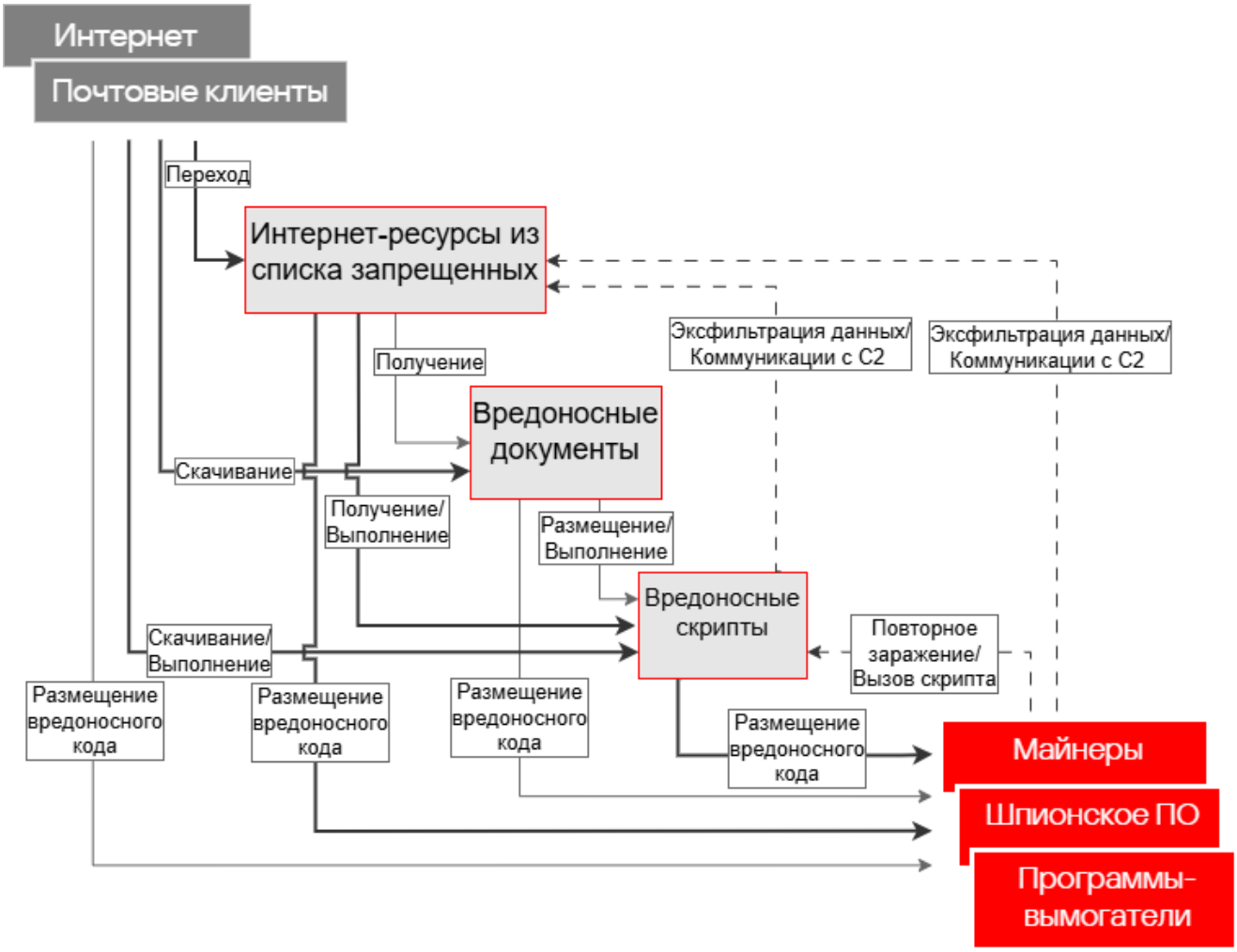
Вредоносные объекты, которые используются для первичного заражения компьютеров АСУ, — опасные ресурсы в интернете, которые попадают в списки запрещенных, вредоносные скрипты и фишинговые страницы, а также вредоносные документы.

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

Типовые атаки, блокируемые в сети АСУ, представляют собой многоступенчатый процесс, где каждый последующий шаг злоумышленников направлен на повышение привилегий и получение доступа к другим системам путем эксплуатации присутствующих уязвимостей в системах и сетях АСУ.

Стоит отметить, что в ходе атаки злоумышленники часто повторяют одни и те же шаги (TTP), например, когда используют вредоносные скрипты и установленные каналы связи с инфраструктурой управления и контроля (C2) для горизонтального перемещения внутри сети и продвижения атаки.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



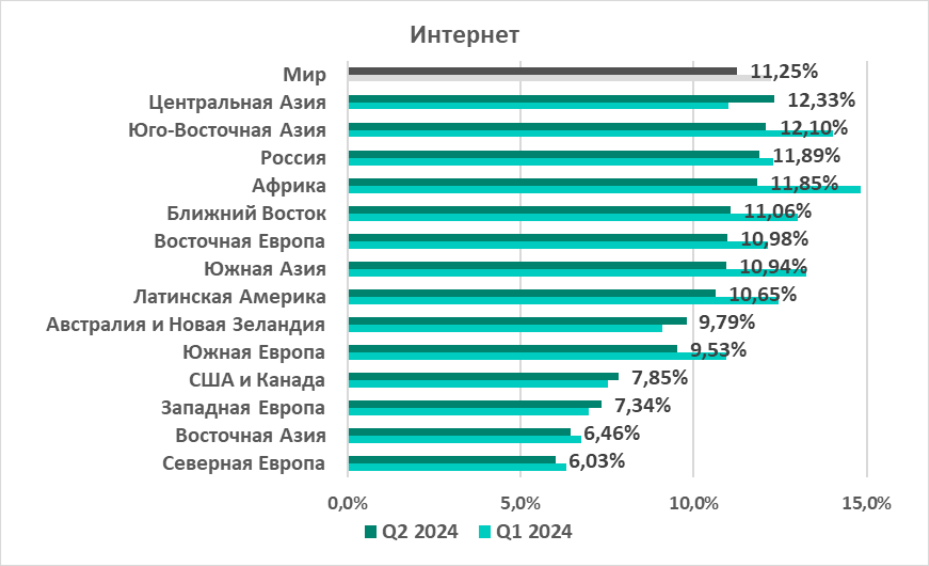
Цепочка атаки: от первичного заражения до вредоносного ПО следующего этапа

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

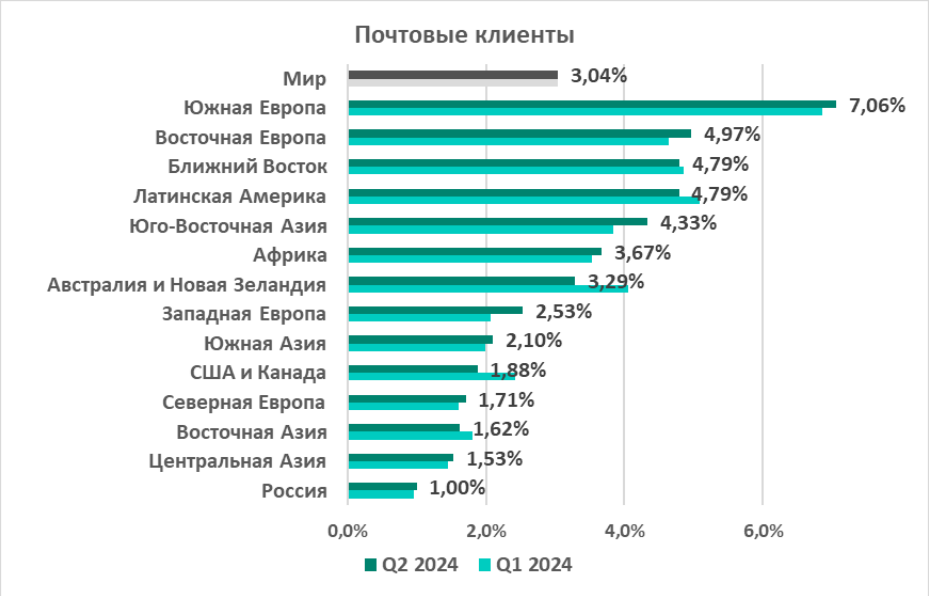
Источники большинства вредоносных объектов, используемых для первичного заражения, — это интернет и электронная почта.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Регионами, где во втором квартале 2024 года уровень угроз из интернета превысил среднемировое значение (11,25%), оказались **Центральная Азия, Юго-Восточная Азия, Россия** и **Африка**.



Регионами, где уровень угроз из почтовых клиентов превысил среднемировое значение (3,04%) стали **Южная Европа, Восточная Европа, Ближний Восток, Латинская Америка, Юго-Восточная Азия, Африка, Австралия и Новая Зеландия**.

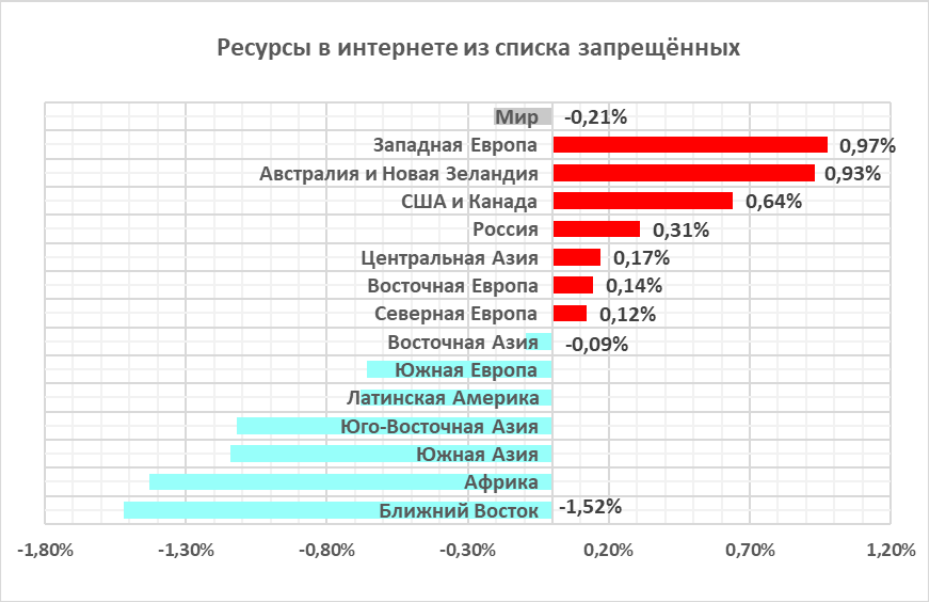


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Ресурсы в интернете из списка запрещенных

Среди регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, лидируют с показателями выше среднемирового значения (6,63%) **Россия, Центральная Азия, Африка** и **Восточная Европа**.

Тройку лидеров **по росту** этого показателя составляют Западная Европа, Австралия и Новая Зеландия, США и Канада.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносные скрипты и фишинговые страницы

Среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидируют с показателями выше среднемирового значения (5,69%) **Южная Европа, Ближний Восток, Юго-Восточная Азия, Австралия и Новая Зеландия, Латинская Америка, Африка** и **Восточная Европа**.

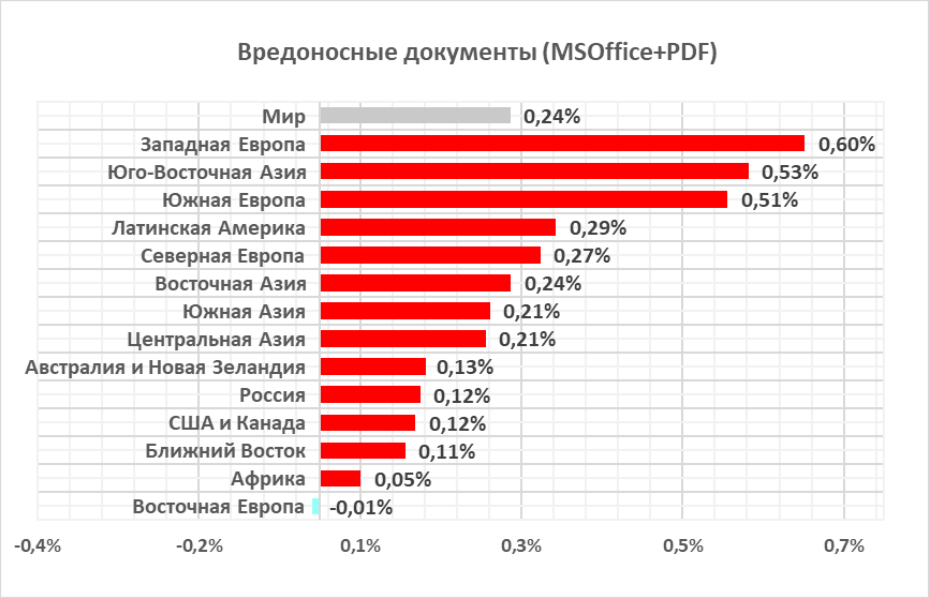
Тройку лидеров **по росту** этого показателя составляют Южная Европа, Восточная Азия и Западная Европа.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносные документы

Среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, лидируют с показателями выше среднемирового значения (1,96%) **Южная Европа, Латинская Америка, Юго-Восточная Азия, Восточная Европа** и **Ближний Восток**.

Тройку лидеров **по росту** этого показателя составляют Западная Европа, Юго-Восточная Азия и Южная Европа.

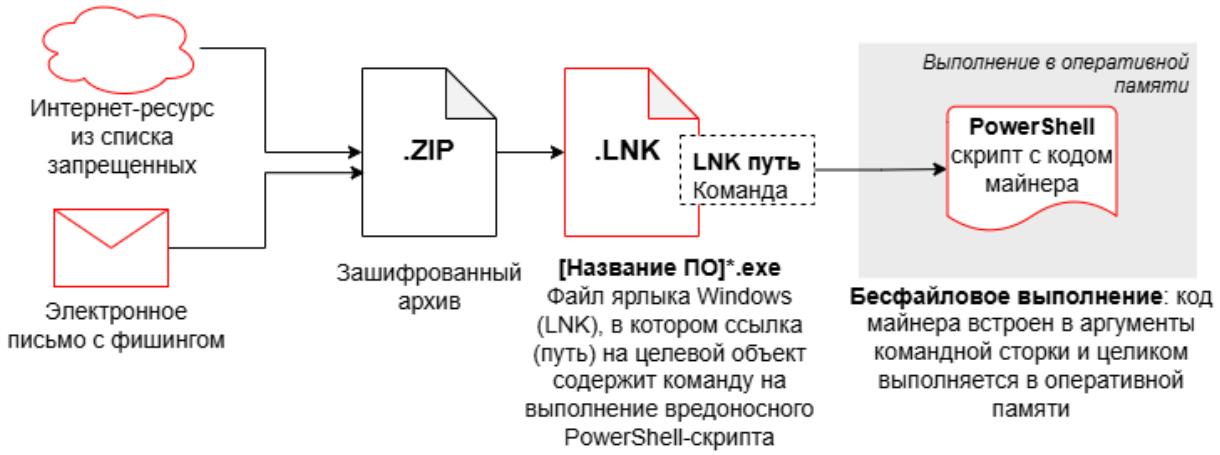


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

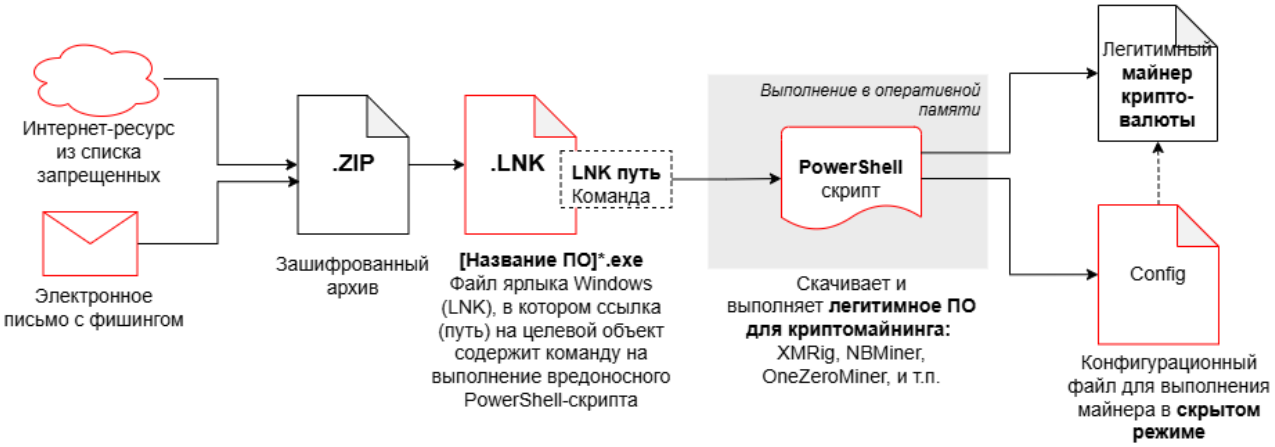
Значительная часть майнеров для Windows, обнаруженных на компьютерах АСУ во втором квартале 2024 года, представляла собой архивы с именами, имитирующими легальное программное обеспечение. В этих архивах не было ПО как такового, но содержался файл ярлыка Windows (LNK). Однако целевой объект (или путь), на который указывает LNK-файл, не является обычным приложением, а представляет собой команду, которая может выполнить вредоносный код, например, скрипт PowerShell. В последнее время злоумышленники все чаще используют PowerShell для выполнения вредоносного кода, включая майнеры, передавая вредоносный код непосредственно в аргументах командной строки. Передаваемый код целиком выполняется в оперативной памяти, обеспечивая бесфайловое выполнение майнера и делая проблематичным его обнаружение средствами защиты.



Цепочка атаки: пример бесфайлового исполнения в майнинговых атаках

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

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Цепочка атаки: пример с использованием легитимных криптомайнеров

Шпионские программы

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

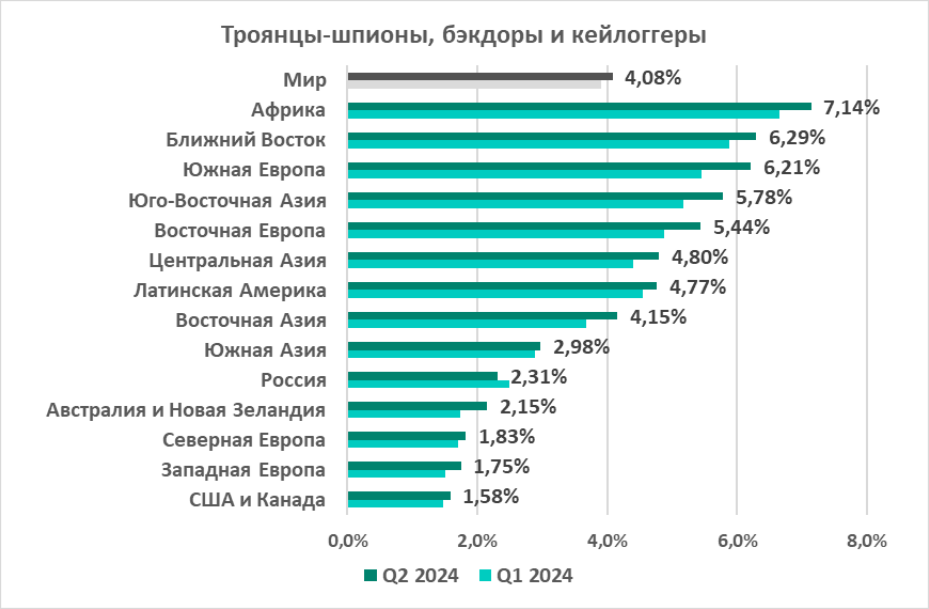
Шпионское ПО (троянцы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструментарий промежуточных этапов кибератаки (например, разведки и распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных.

Обнаружение шпионского ПО на компьютере АСУ обычно указывает на то, что вектор первоначального заражения сработал — будь то переход по вредоносной ссылке, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует об отсутствии или о неэффективности мер защиты периметра технологической сети (таких как контроль безопасности сетевых коммуникаций и выполнения политики использования съемных носителей).

Как и ожидалось, регионы с наибольшей долей компьютеров АСУ, на которых было заблокировано шпионское ПО, входят в списки лидеров по угрозам первичного заражения (за исключением России, в которой показатели, связанные со шпионским ПО, невысоки).

Регионы, где доля компьютеров АСУ, на которых были заблокированы вредоносные документы, превысила среднемировое значение (4,08%): **Африка, Ближний Восток, Южная Европа, Юго-Восточная Азия, Восточная Европа, Центральная Азия, Латинская Америка** и **Восточная Азия**.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Почти во всех регионах шпионские программы занимают не выше третьей строчки в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, за исключением следующих регионов:

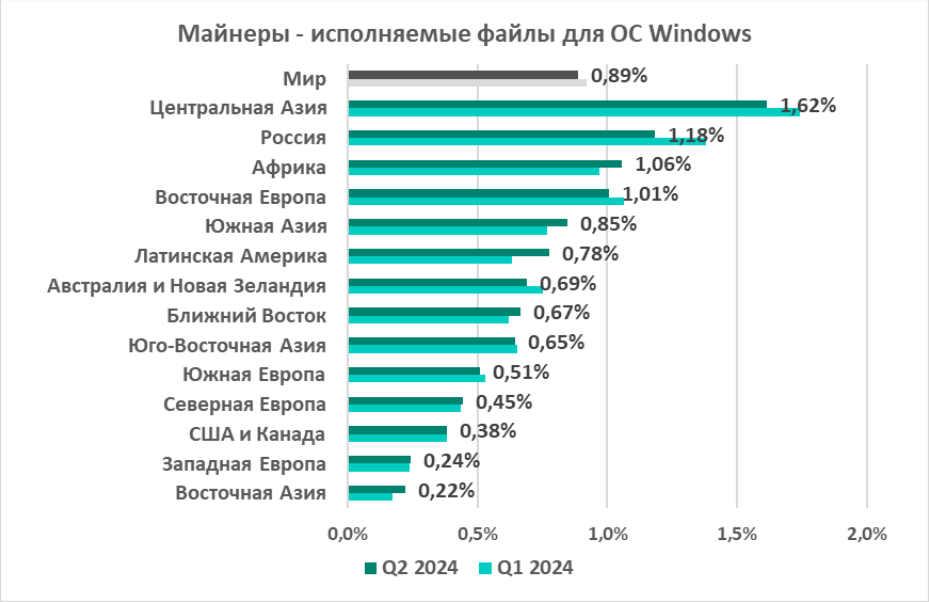
- Восточная Азия — в регионе программы-шпионы занимает первое место в рейтинге категорий вредоносного ПО по доле компьютеров АСУ, на которых они были заблокированы, — 4,15%.
- Центральная Азия, Африка, Ближний Восток и Южная Европа — в этих регионах шпионские программы находятся на втором месте в соответствующих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

Тройку лидеров **по росту** доли компьютеров АСУ, на которых были заблокированы шпионские программы, составляют Южная Европа, Юго-Восточная Азия и Восточная Европа.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

Среди регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, лидируют с показателями выше среднемирового значения (0,89%) **Центральная Азия, Россия, Африка** и **Восточная Европа**.

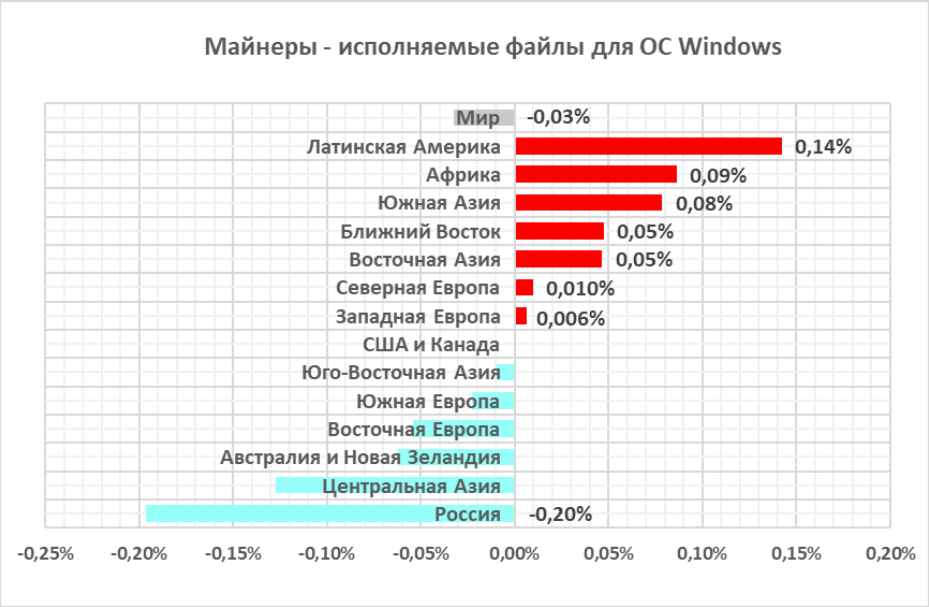


В мире в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows находятся на седьмом месте.

- В России в аналогичном рейтинге они — на четвертом месте.
- В Центральной Азии, Австралии и Новой Зеландии, а также Северной Европе они — на пятом месте.

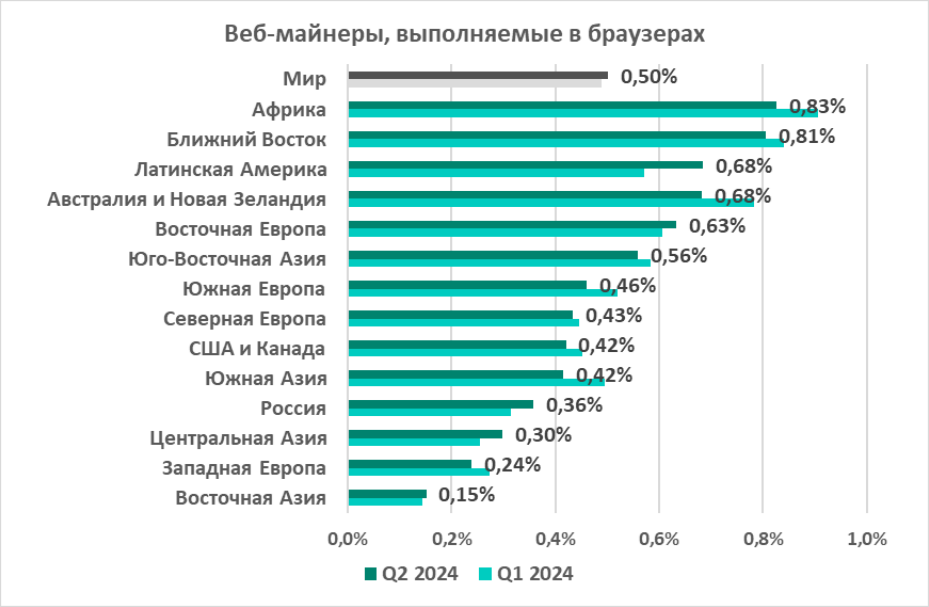
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Тройку лидеров **по росту** этого показателя составляют Латинская Америка, Африка и Южная Азия.



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

Среди регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, лидируют с показателями выше среднемирового значения (0,50%) **Африка, Ближний Восток, Латинская Америка, Австралия и Новая Зеландия, Восточная Европа** и **Юго-Восточная Азия**.

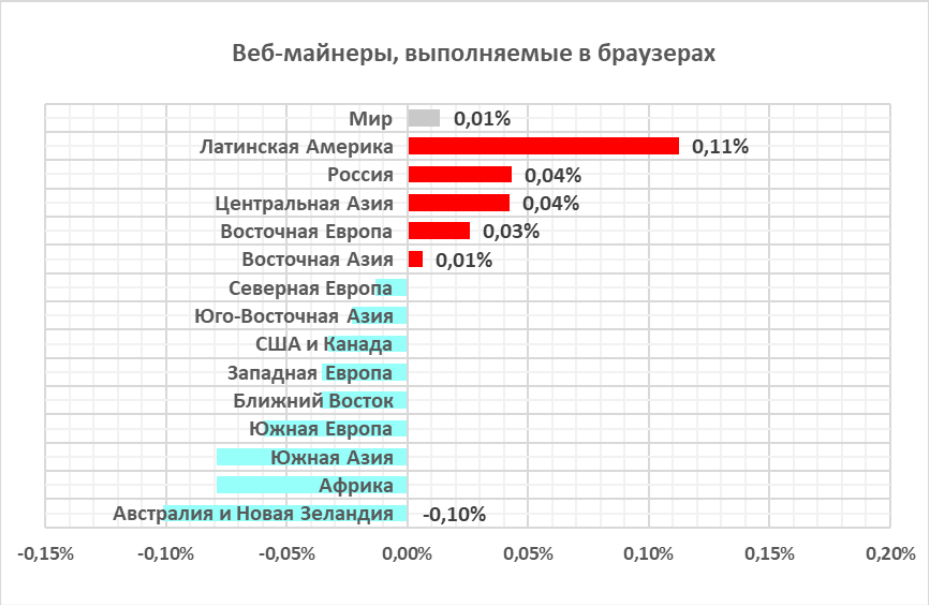


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В следующих региональных рейтингах категорий угроз веб-майнеры занимают более высокие позиции по доле компьютеров АСУ, на которых они были заблокированы, чем в мировом рейтинге (где они находятся на восьмом месте).

- В США и Канаде они — на пятом месте.
- В Северной Европе, Австралии и Новой Зеландии — на шестом месте.
- В Восточной, Западной и Южной Европе, а также на Ближнем Востоке — на седьмом месте.

Тройку лидеров **по росту** этого показателя составляют Латинская Америка, Россия и Центральная Азия.

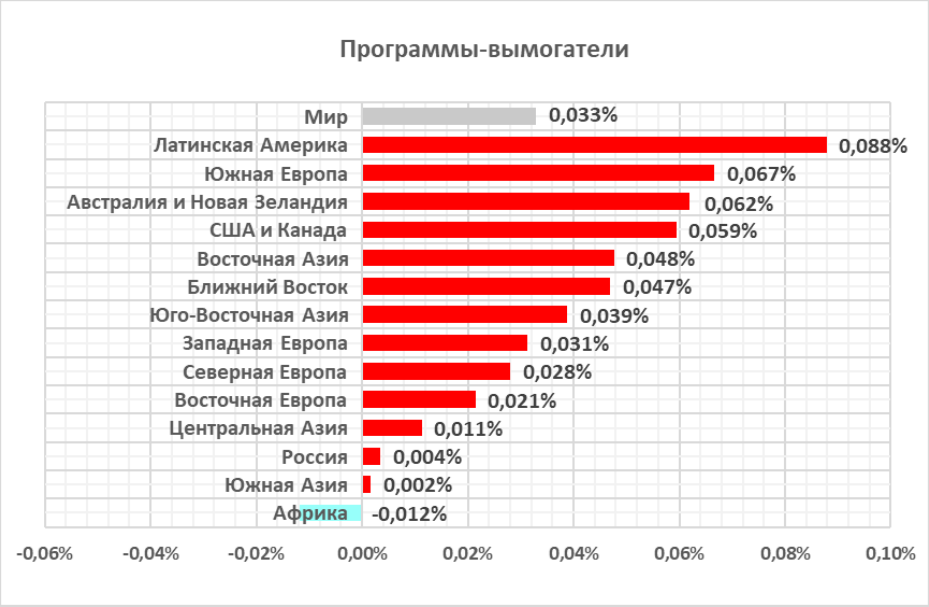


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Программы-вымогатели

Наиболее высокая доля компьютеров АСУ, на которых были заблокированы программы-вымогатели (с показателями выше среднемирового значения 0,18%), была отмечена на **Ближнем Востоке**, в **Африке, Юго-Восточной Азии, Южной Азии, Латинской Америке, Центральной Азии, Южной Европе** и **Восточной Азии**.

Тройку лидеров **по росту** этого показателя составляют Латинская Америка, Южная Европа, а также Австралия и Новая Зеландия.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Самораспространяющееся вредоносное ПО. Черви и вирусы

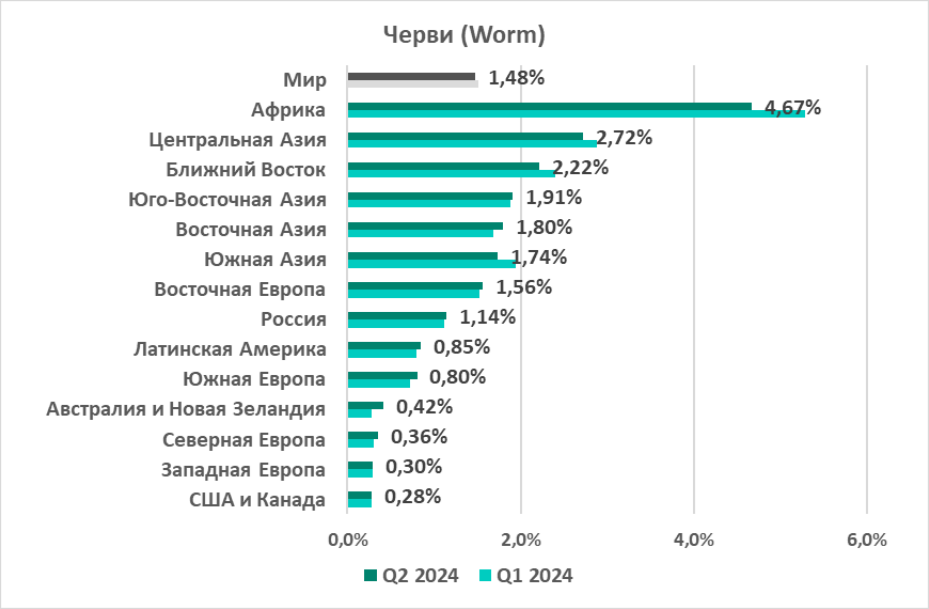
Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнет-сетей, приобрели черты угроз следующего этапа.

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 устройств.

Черви

Среди регионов по доле компьютеров АСУ, на которых были заблокированы черви, лидируют с показателями выше среднемирового значения (1,48%) **Африка, Центральная Азия, Ближний Восток, Юго-Восточная Азия, Восточная Азия, Южная Азия** и **Восточная Европа**.

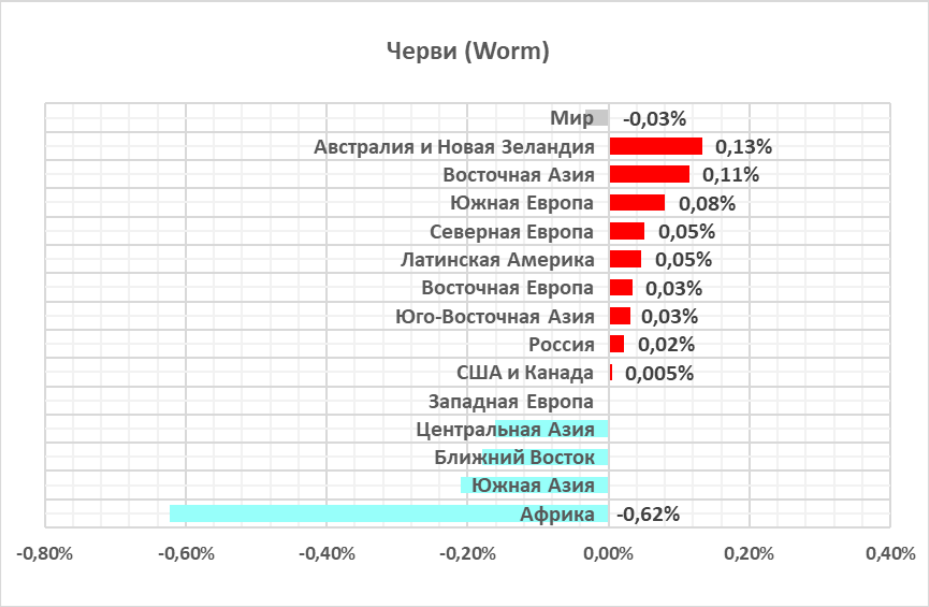


В мире черви находятся на шестой позиции в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. При этом **черви занимают более высокие места** в соответствующих рейтингах в следующих регионах:

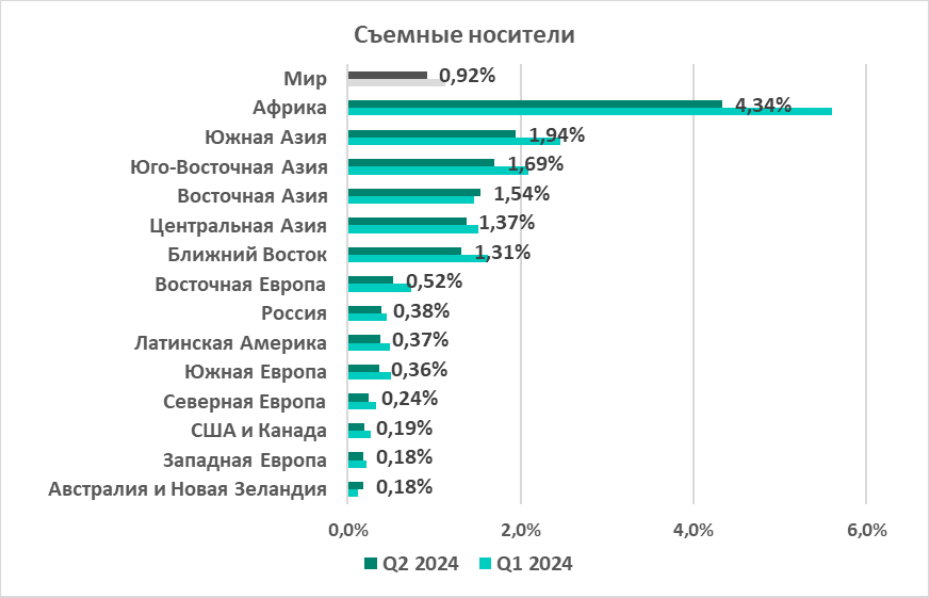
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Африка, Центральная Азия, Южная Азия — четвертое место;
- Восточная Азия, Ближний Восток, Латинская Америка, Россия, Восточная Европа, Западная Европа, Южная Европа — пятое место.

Тройку лидеров **по росту** этого показателя составляют Австралия и Новая Зеландия, Восточная Азия и Южная Европа.



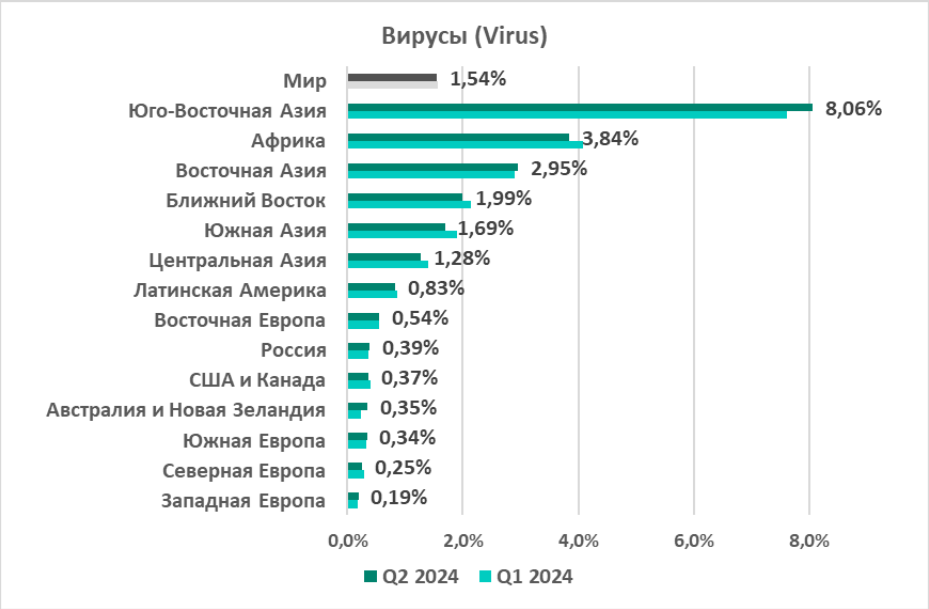
На верхних строчках рейтингов по червям располагаются те же регионы, что лидируют по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении **съемных носителей**. Это Африка, Южная Азия, Юго-Восточная Азия, Восточная Азия, Центральная Азия, Ближний Восток.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

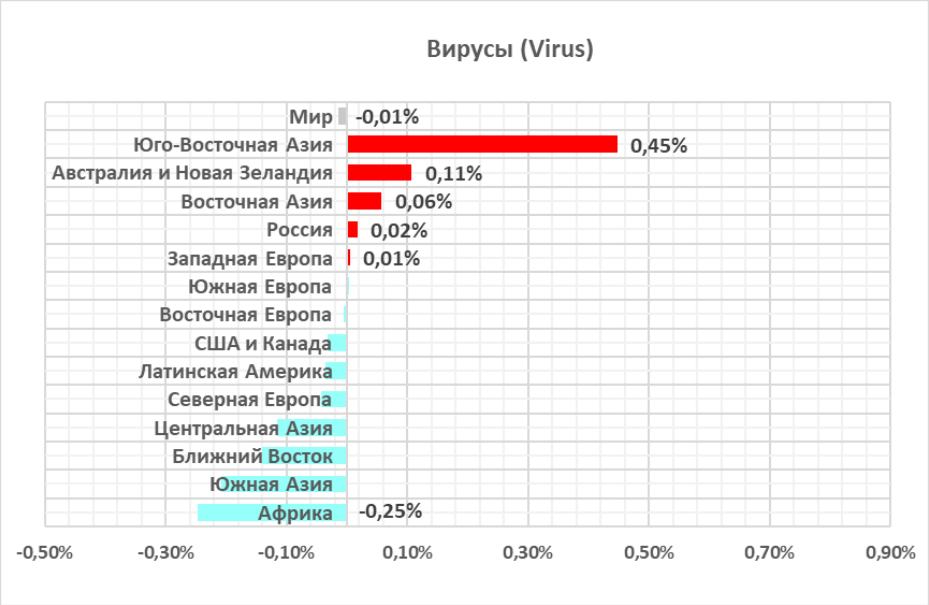
Вирусы

Среди регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, лидируют с показателями выше среднемирового значения (1,54%) **Юго-Восточная Азия, Африка, Восточная Азия, Ближний Восток, Южная Азия.**



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

Тройку лидеров **по росту** этого показателя составляют Юго-Восточная Азия, Австралия и Новая Зеландия, а также Восточная Азия.



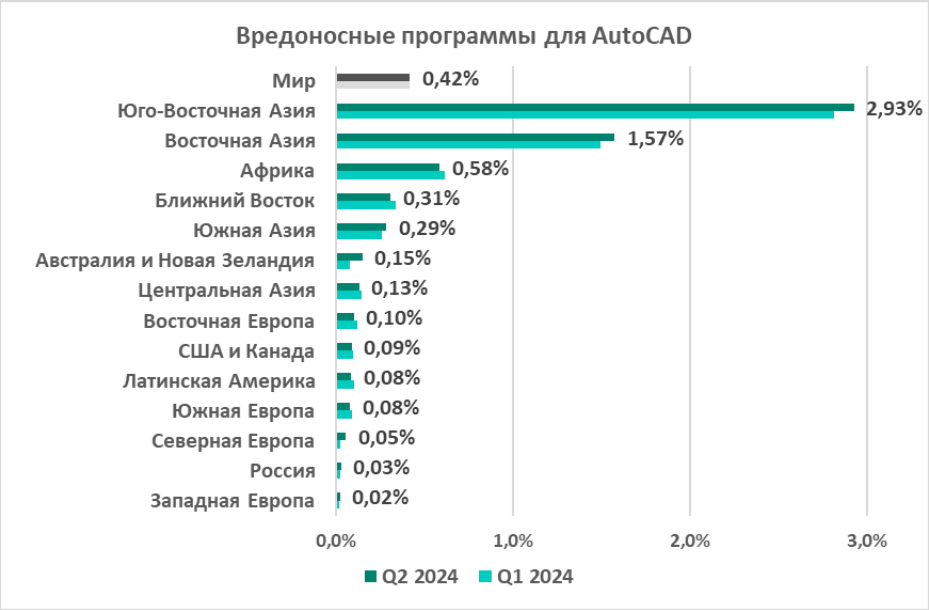
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отметим, что четыре региона в топе лидируют и по доле компьютеров АСУ, на которых были заблокированы **угрозы в сетевых папках**. Это Восточная Азия, Юго-Восточная Азия, Южная Азия и Ближний Восток.

Вредоносные программы для AutoCAD

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

По доле 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%). Это **Юго-Восточная Азия, Восточная Азия** и **Африка**.



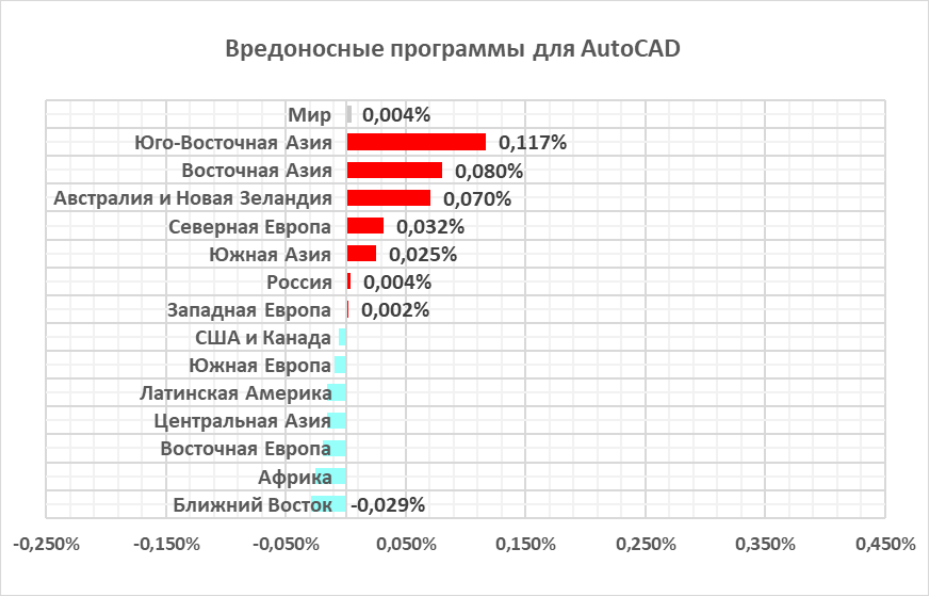
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Обычно вредоносное ПО для AutoCAD представляет собой незначительную угрозу и чаще всего занимает последние места в рейтингах категорий вредоносного ПО по доле компьютеров АСУ, на которых оно было заблокировано.

Однако во втором квартале 2024 года эта категория занимает более высокое место в региональных рейтингах по сравнению с глобальным (девятое место) в следующих регионах:

- Юго-Восточная Азия — пятое место;
- Восточная Азия — седьмое место.

Тройку лидеров **по росту** этого показателя составляют Юго-Восточная Азия, Восточная Азия, а также Австралия и Новая Зеландия.



Регионы. Некоторые особенности

Для выявления особенностей каждого региона стоит провести сравнение его показателей с показателями других регионов и глобальной статистикой.

В большинстве регионов, как и в целом по миру, верхние строчки в рейтинге по доле компьютеров АСУ, на которых были заблокированы определенные категории угроз, занимают программы-шпионы и вредоносные объекты, используемые для первичного заражения компьютеров. Что касается основных источников угроз, то во всех регионах лидирует интернет.

В то же время существуют некоторые региональные особенности и отличия, которые мы отметим далее.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Африка

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
7,35%

▼ снижение во II кв. 2024 г.
1,1x выше среднего по миру
3-е место в мире

-2 место-

Шпионские программы
7,14%

▲ **1,1x** рост во II кв. 2024 г.
1,8x выше среднего по миру
1-е место в мире

-3 место-

Скрипты и фишинговые страницы
5,87%

▼ снижение во II кв. 2024 г.
незначительно выше среднего по миру

Черви
4,67%

▼ снижение во II кв. 2024 г.
3,2x выше среднего по миру
1-е место в мире

Вирусы
3,84%

▼ снижение во II кв. 2024 г.
2,5x выше среднего по миру
2-е место в мире

Майнеры — исполняемые файлы
1,06%

▲ **1,1x** рост во II кв. 2024 г.
1,2x выше среднего по миру
3-е место в мире
2-е место в мире **по росту**

Веб-майнеры
0,83%

▼ снижение во II кв. 2024 г.
1,7x выше среднего по миру
1-е место в мире

Программы-вымогатели
0,25%

▼ снижение во II кв. 2024 г.
1,4x выше среднего по миру
2-е место в мире

Интернет
как источник угроз
11,85%

▼ снижение во II кв. 2024 г.
1,1x выше среднего по миру
4-е место в мире

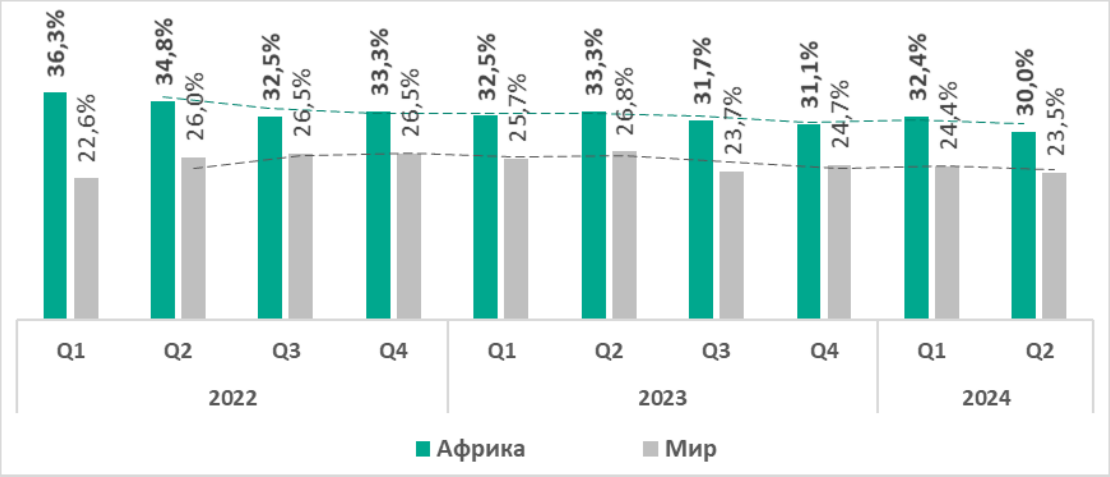
Съемные носители
как источник угроз
4,34%

▼ снижение во II кв. 2024 г.
4,7x выше среднего по миру
выше **почтовых угроз**
1-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Африка традиционно занимает **первое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Регион возглавляет многие рейтинги, в некоторых случаях с огромным отрывом. При этом здесь наблюдается незначительный нисходящий тренд с колебаниями.



Сравнительный анализ

Африка находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- первое место — шпионские программы, веб-майнеры, черви, угрозы на съемных носителях;
- второе место — программы-вымогатели, вирусы;
- третье место — ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows, вредоносные программы для AutoCAD.

Категории угроз

- **По сравнению с мировыми показателями**, в регионе выше доля компьютеров АСУ, на которых были заблокированы все категории угроз, за исключением вредоносных документов.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- В регионе значительно выше, чем в среднем по миру, доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - черви — в 3,2 раза;
  - вирусы — в 2,5 раза.

  Черви и вирусы занимают более высокие позиции в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, по сравнению с вредоносными документами. Черви находятся на четвертом месте (на шестом в мире). Как мы отмечали ранее, высокие показатели обнаружения самораспространяющегося вредоносного ПО в широких масштабах указывают на то, что значительная часть технологической инфраструктуры не имеет даже базовой защиты конечных устройств, что делает ее источником попыток заражения вредоносными программами.

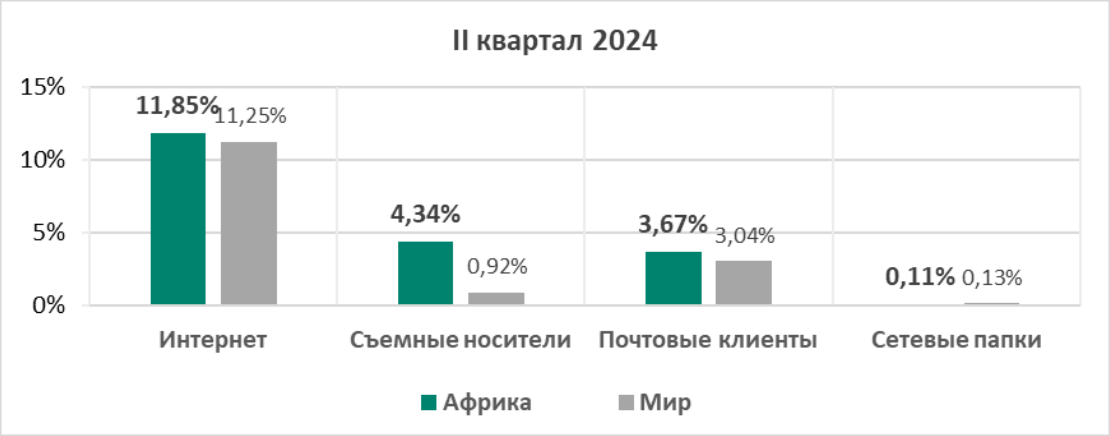
  - шпионские программы — в 1,7 раза;
  - веб-майнеры — в 1,7 раза;
  - вредоносные программы для AutoCAD — в 1,4 раза;
  - программы-вымогатели — в 1,4 раза.

Источники угроз

Съемные носители занимают второе место в регионе в рейтинге источников угроз по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников (третье место в мире).

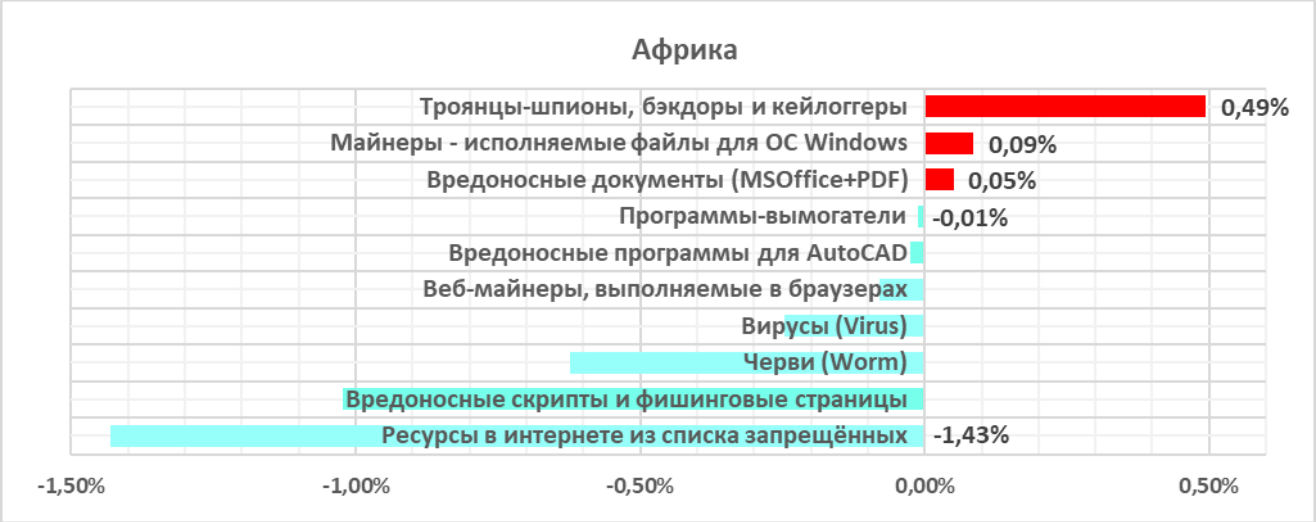
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Во втором квартале 2024 года Африка является единственным регионом, где доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, превышает соответствующий показатель с угрозами из почтовых клиентов. Этот тренд может носить долгосрочный характер. В целом, это может свидетельствовать о том, что технологические системы в регионе достаточно редко подключаются к корпоративным ресурсам, в том числе почтовым сервисам. Вместо этого для обмена данными в технологической инфраструктуре активно используются съемные носители.



Изменения за квартал и тренды

Категории угроз

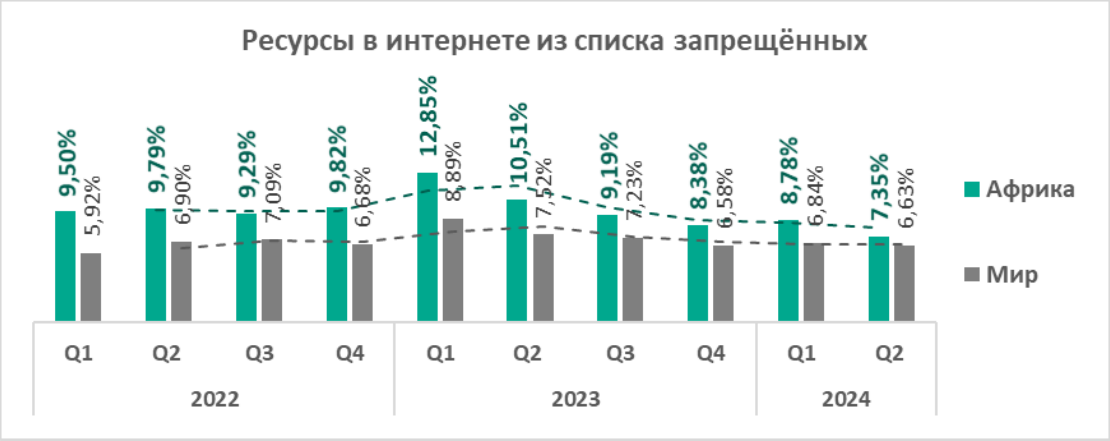


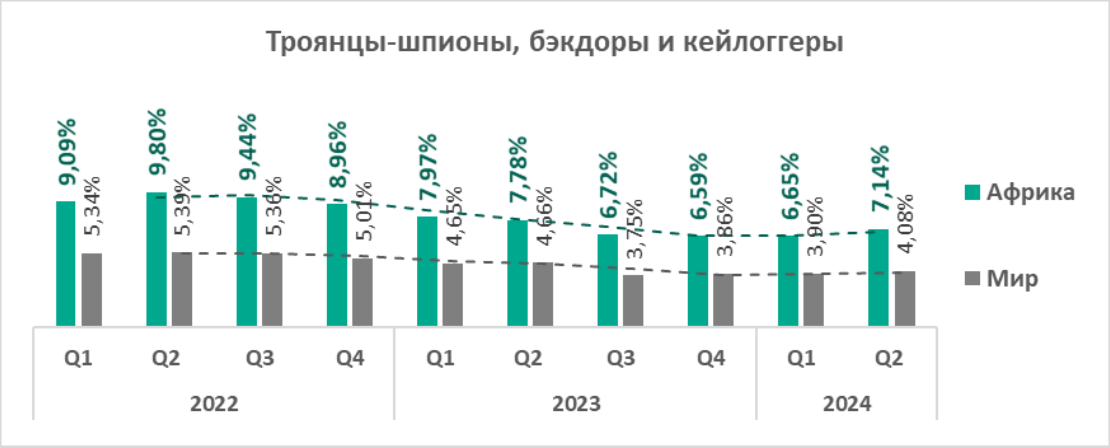
- **Наиболее существенно** во втором квартале 2024 года выросли доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

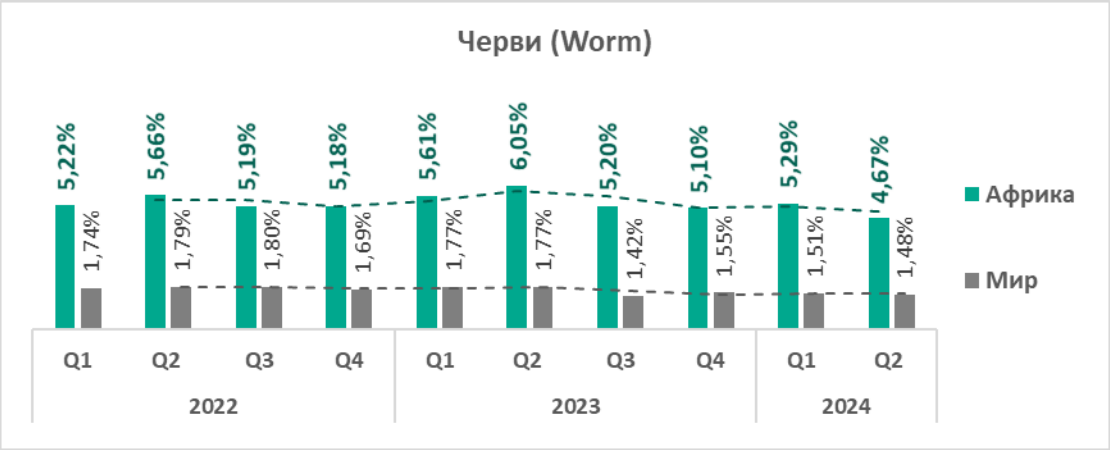
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- шпионские программы — в 1,1 раза, поднялись в регионе с третьего на второе место;
- майнеры — исполняемые файлы для ОС Windows — в 1,1 раза.

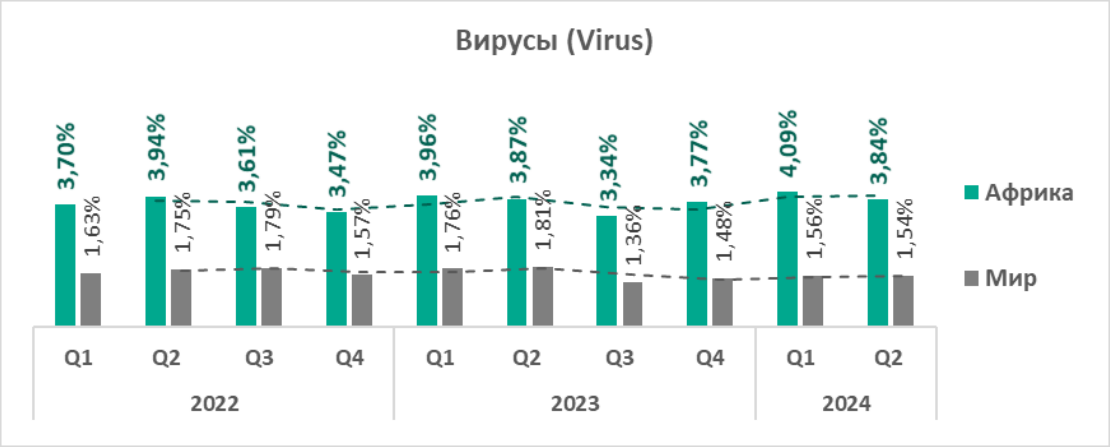
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

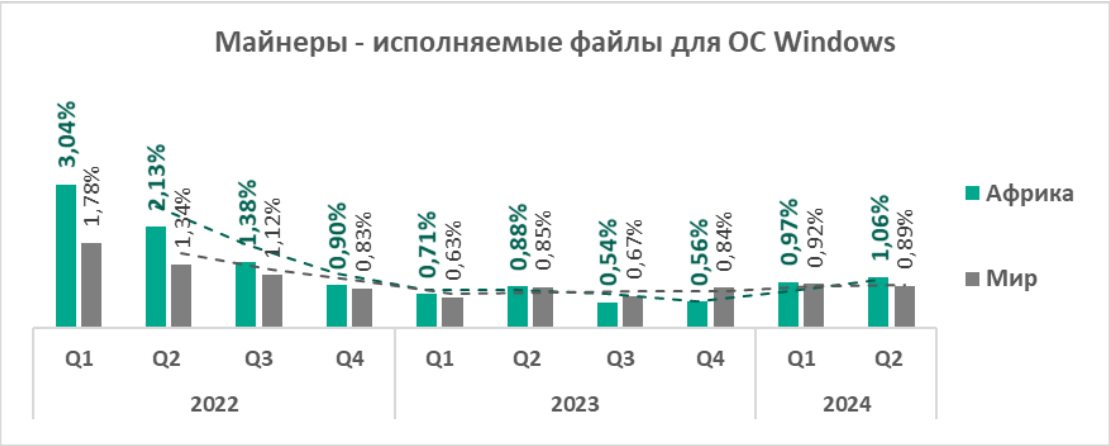


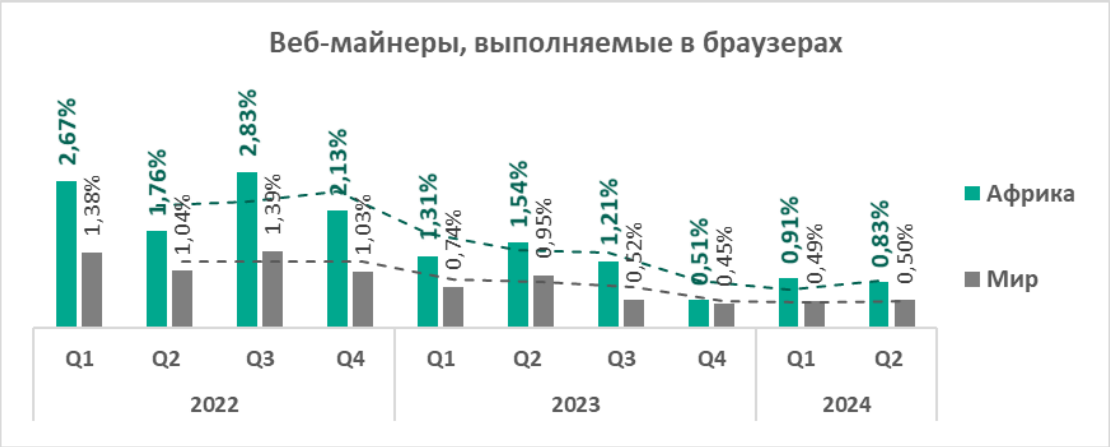




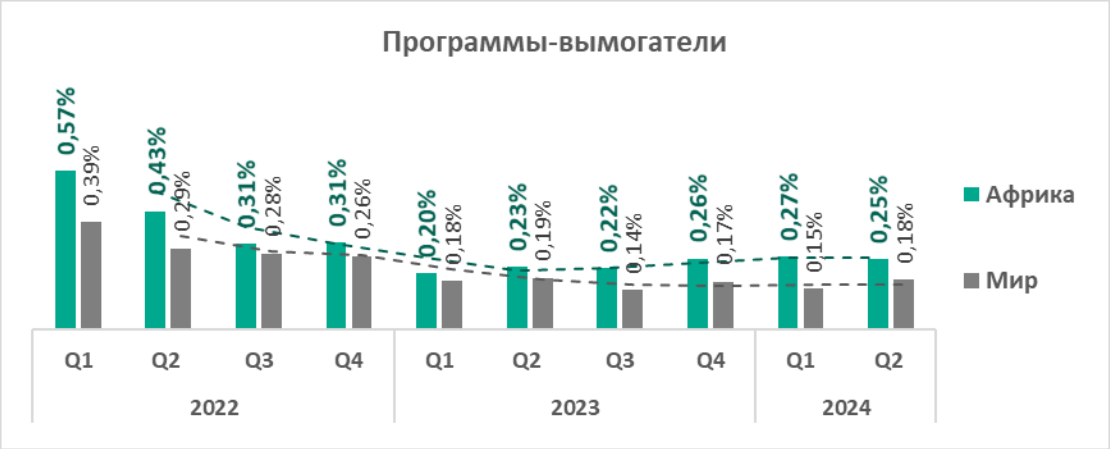
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»







© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



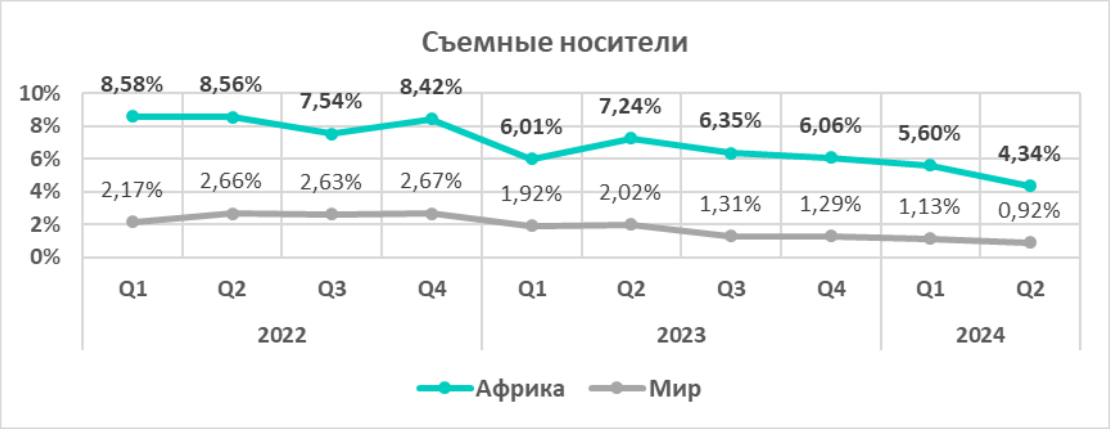
- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Африке за 2,5 года. С начала 2023 года ведущей категорией угроз в регионе являются **ресурсы в интернете из списка запрещенных**. **Шпионские программы** поднялись во втором квартале 2024 года с третьего места на второе, в то время как **вредоносные скрипты и фишинг** постепенно опустились с первого места, на котором они были в 2022 году, на третье место во втором квартале 2024 года.

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

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Источники угроз

- Уровень угроз на **съемных носителях** значительно превосходит среднемировое значение со второго квартала 2022 года и демонстрирует нисходящую динамику, которая преимущественно следует за общемировым трендом.



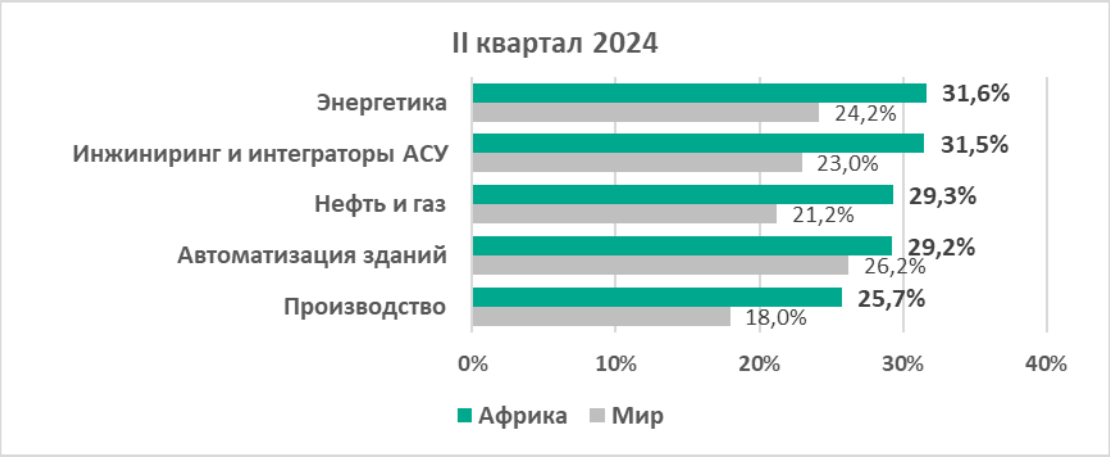
- Что касается **изменений за квартал,** почти все источники угроз демонстрируют нисходящую динамику.

Отрасли

- **Наиболее часто встречающиеся с угрозами отрасли** региона среди рассмотренных в отчете:
  - энергетика;
  - инжиниринг и интеграторы АСУ.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

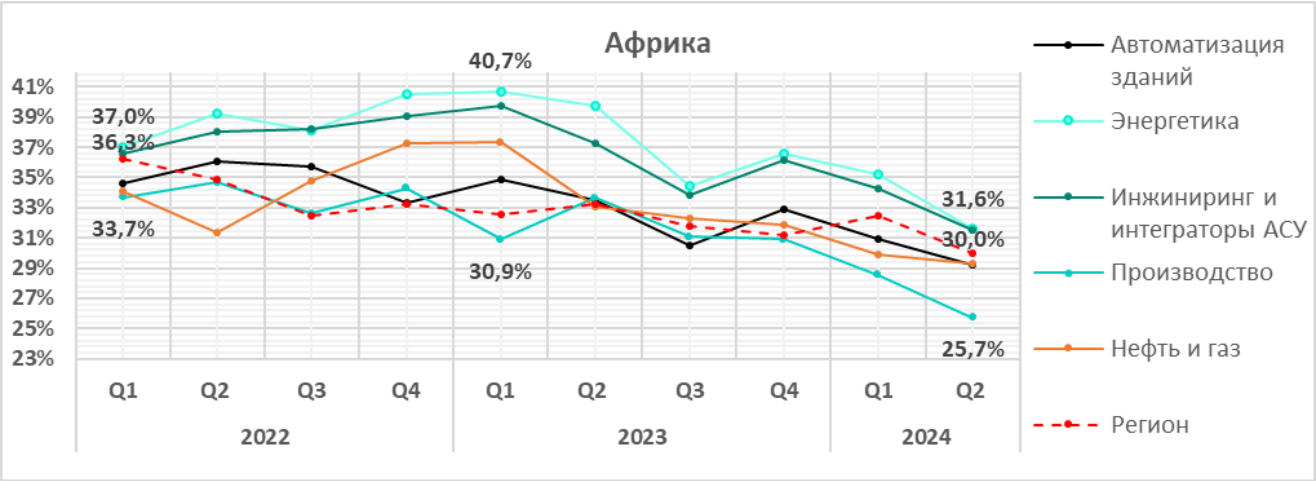
- По сравнению с соответствующими **среднемировыми показателями**, значительно более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:
  - производство — в 1,4 раза;
  - инжиниринг и интеграторы АСУ — в 1,4 раза;
  - нефть и газ — в 1,4 раза;
  - энергетика — в 1,3 раза.



- Во **втором квартале 2024 года** во всех рассмотренных отраслях региона зафиксировано снижение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Рассмотренные отрасли демонстрируют положительную динамику **долгосрочных трендов**.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Юго-Восточная Азия

Актуальные угрозы

-1 место-

Вирусы
8,06%

▲ **1,1x** рост во II кв. 2024 г.
5,2x выше среднего по миру
1-е место в мире

-2 место-

Скрипты и фишинговые страницы
6,77%

▲ незначительный рост во II кв. 2024 г.
1,2x выше среднего по миру
3-е место в мире

-3 место-

Интернет-ресурсы из списка запрещенных
6,07%

▼ снижение во II кв. 2024 г.

Шпионские программы
5,78%

▲ **1,1x** рост во II кв. 2024 г.
1,4x выше среднего по миру

Вредоносные программы для AutoCAD
2,93%

▲ незначительный рост во II кв. 2024 г.
7x выше среднего по миру
1-е место в мире

Вредоносные документы
2,76%

▲ **1,2x** рост во II кв. 2024 г.
1,4x выше среднего по миру
3-е место в мире

Программы-вымогатели
0,25%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру
3-е место в мире

Интернет
как источник угроз
12,10%

▼ снижение во II кв. 2024 г.
1,1x выше среднего по миру
2-е место в мире

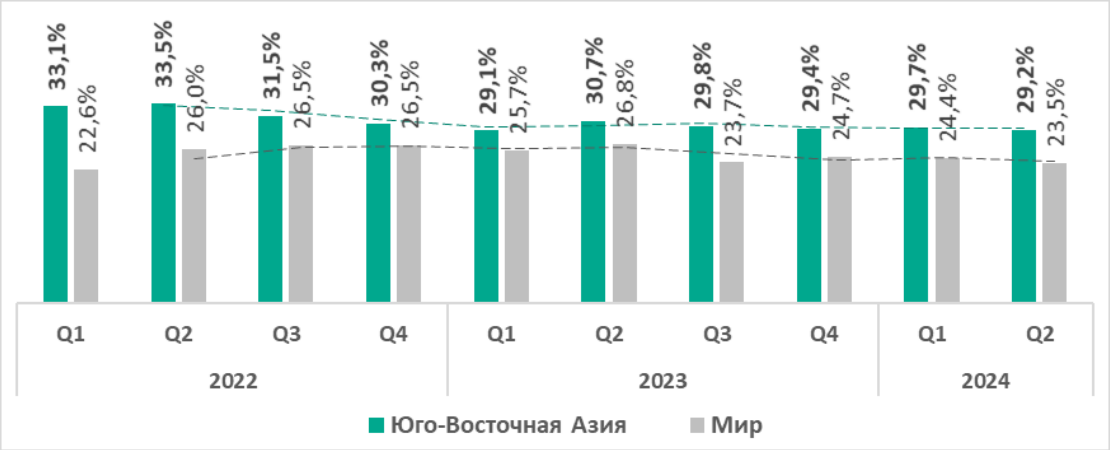
Сетевые папки
как источник угроз
0,34%

▼ снижение во II кв. 2024 г.
2,6x выше среднего по миру
2-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Юго-Восточная Азия занимает **второе место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Этот показатель превосходит среднемировое значение на протяжении всего периода наблюдения, при этом демонстрирует незначительное снижение с периодическими колебаниями.



Сравнительный анализ

Юго-Восточная Азия находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- первое место — вирусы, вредоносные программы для AutoCAD;
- второе место — угрозы из интернета, угрозы в сетевых папках;
- третье место — вредоносные скрипты и фишинговые страницы, вредоносные документы, программы-вымогатели.

Категории угроз

Вирусы занимают первое место в рейтинге категорий вредоносных программ по доле компьютеров АСУ, на которых они были заблокированы. В Юго-Восточной Азии этот показатель в 5,2 раза превышает среднемировой уровень.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносные программы для AutoCAD в этом рейтинге находится на пятом месте (в мире доля компьютеров АСУ, на которых было заблокировано такое вредоносное ПО, одна из самых низких среди всех категорий).

По сравнению с мировыми показателями, в регионе значительно выше доля компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

- вредоносные программы для AutoCAD — в 7 раз;
- вирусы — в 5,2 раза;
- шпионские программы — в 1,4 раза;
- вредоносные документы — в 1,4 раза;
- черви — в 1,3 раза;
- программы-вымогатели — в 1,2 раза;
- вредоносные скрипты и фишинговые страницы — в 1,2 раза.

Источники угроз

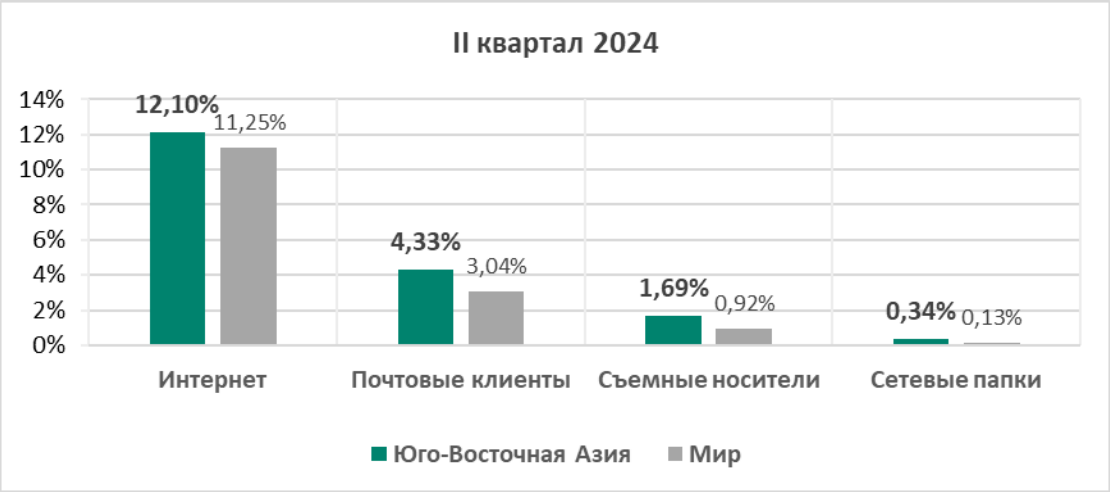
Юго-Восточная Азия занимает первое место в мире по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках**, с превышением среднемирового значения в 2,6 раза.

По угрозам из **интернета** регион находится на втором месте в мире, с незначительным превышением среднемирового показателя.

Регион занимает третье место в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты на **съемных носителях**, с превышением среднемирового показателя в 1,8 раза.

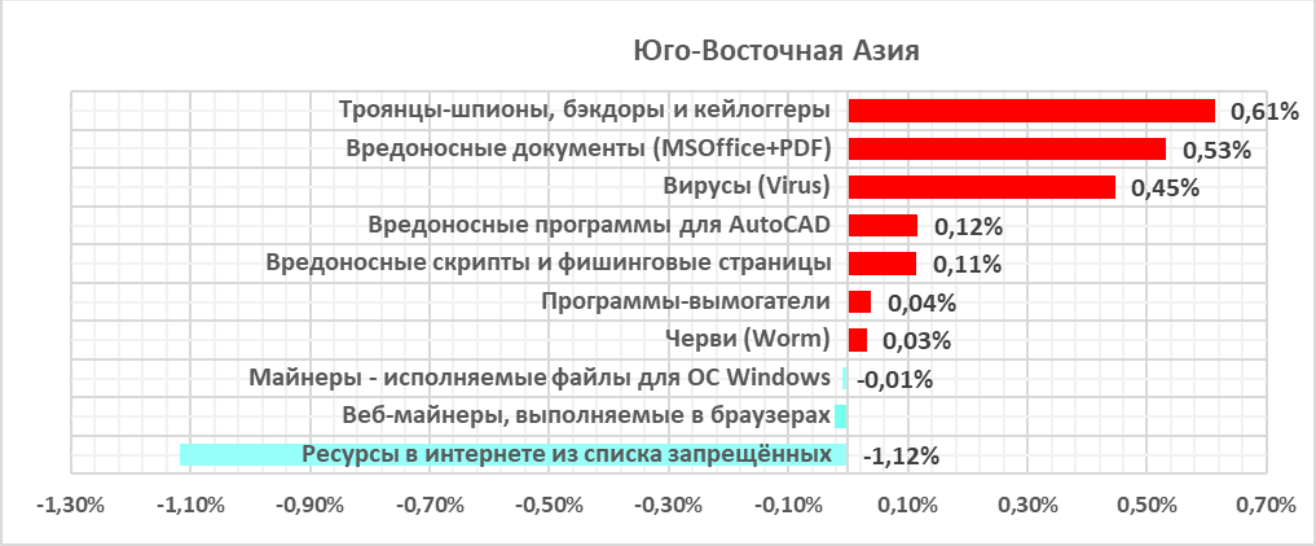
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

А доля компьютеров, на которых были заблокированы угрозы из **почтовых клиентов**, превышает среднемировой показатель в 1,4 раза.



Изменения за квартал и тренды

Категории угроз

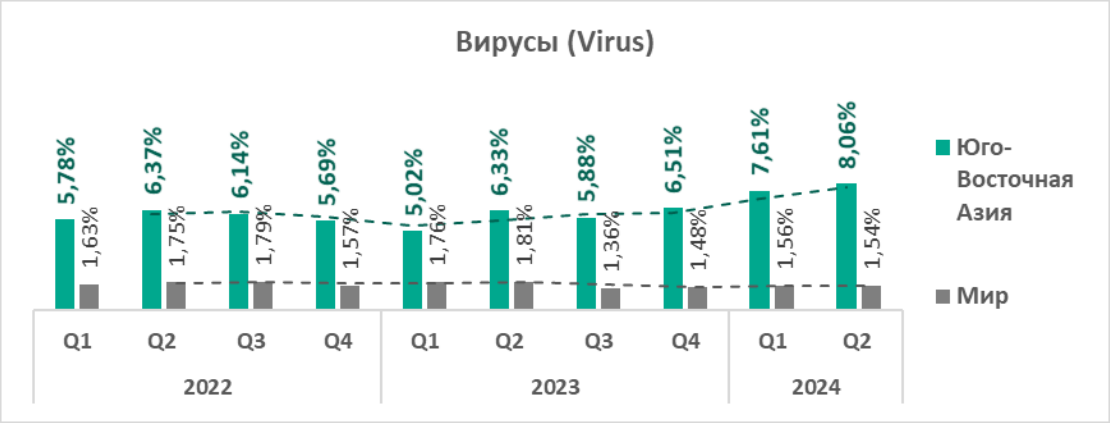


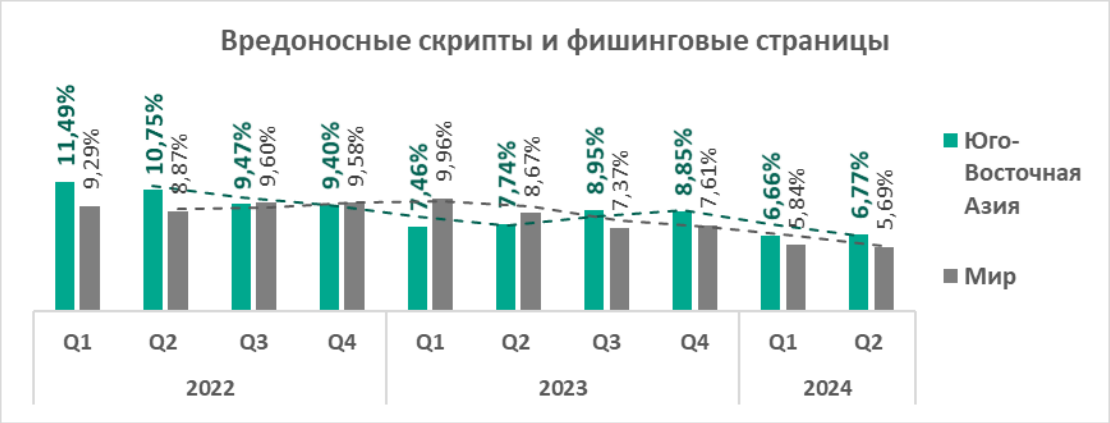
Наибольший рост за квартал был отмечен в доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

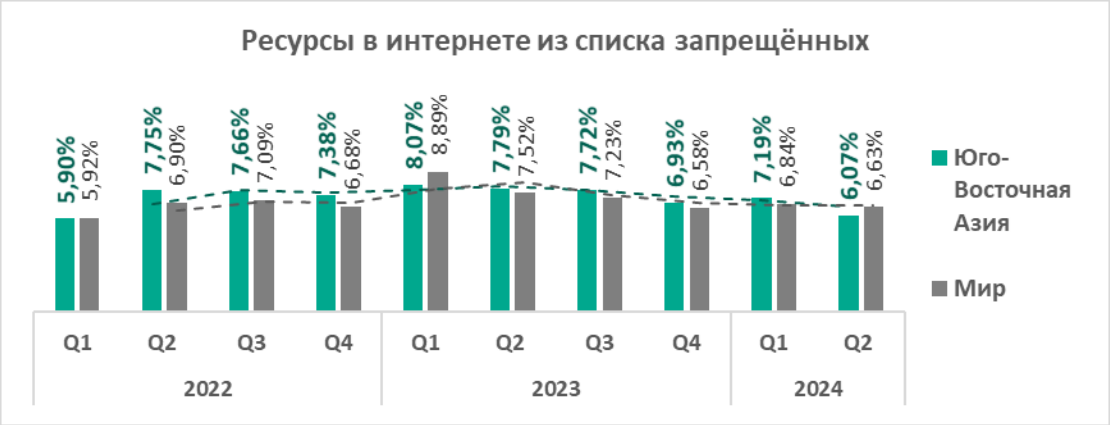
- вредоносные документы — в 1,2 раза;
- программы-вымогатели — в 1,2 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

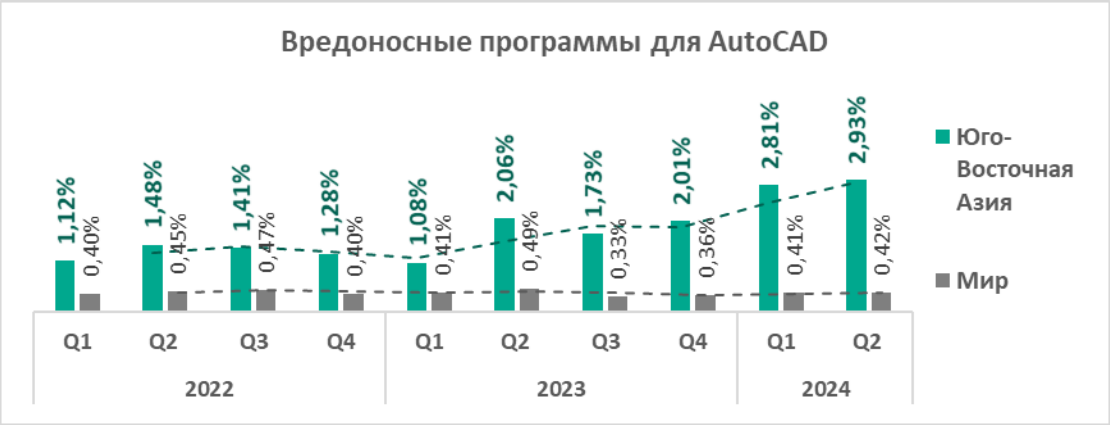
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.



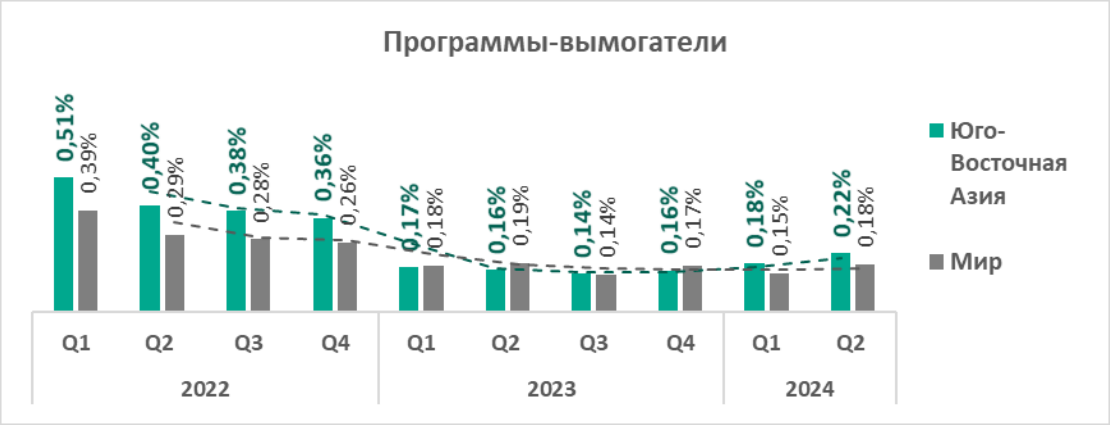




© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Юго-Восточной Азии за 2,5 года. **Вирусы** стали ведущей категорией угроз в регионе в первом квартале 2024 года. Во втором квартале 2024 года **вредоносные скрипты и фишинговые страницы** поднялись с третьего места на второе, а **ресурсы в интернете из списка запрещенных** постепенно опустились с первого места в первой половине 2023 года на третье во втором квартале 2024 года.

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

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Источники угроз

- Почти все источники угроз, за исключением почтовых клиентов, отметились снижением доли компьютеров АСУ, на которых они были заблокированы. Показатель почтовых клиентов вырос в 1,1 раза. Что касается **изменений за квартал**, все источники угроз демонстрируют преимущественно нисходящую динамику.

Показатели угроз на **съемных носителях** и в **сетевых папках** значительно превышают соответствующие среднемировые значения.

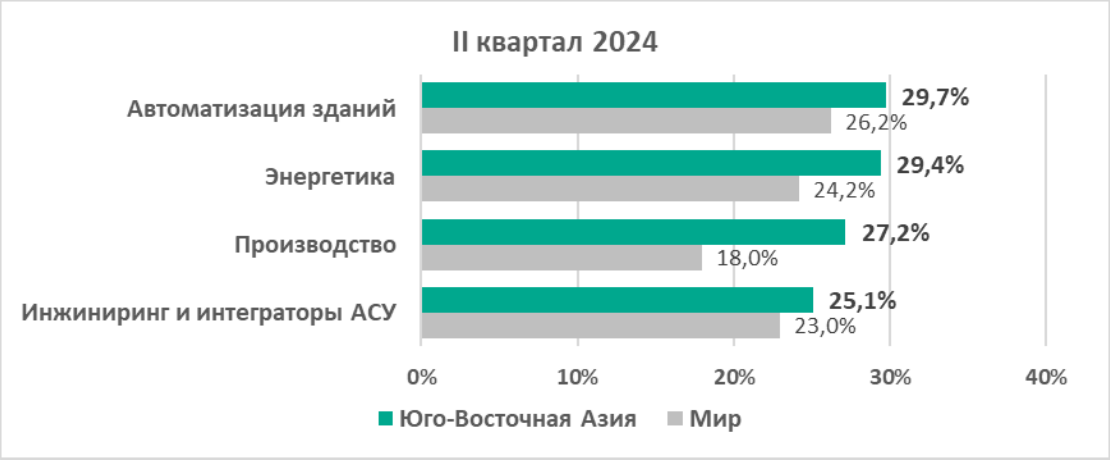
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отрасли

- **Наиболее часто встречающиеся с угрозами отрасли** региона среди рассмотренных в отчете:
  - автоматизация зданий;
  - энергетика.

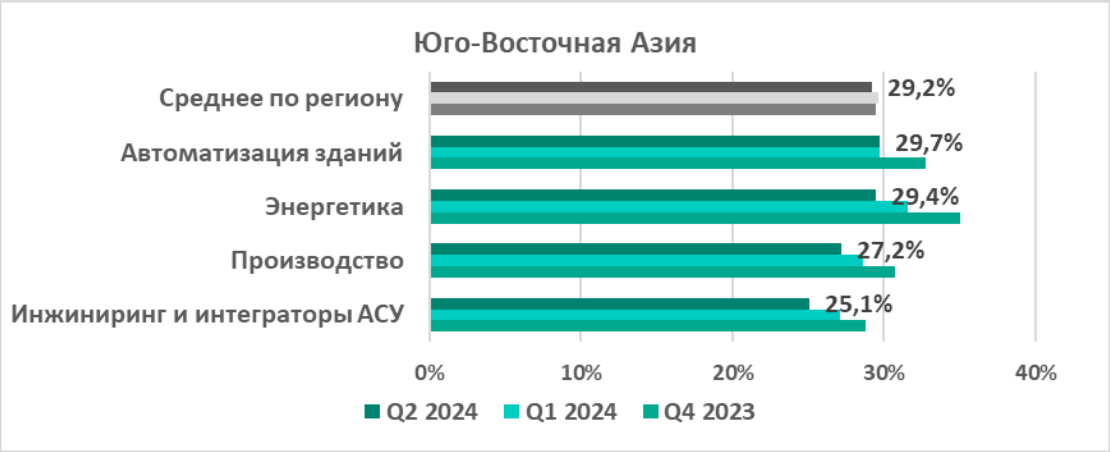
По сравнению с соответствующими **среднемировыми показателями**, значительно более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдалась в следующих отраслях:

- производство — в 1,5 раза;
- энергетика — в 1,2 раза.

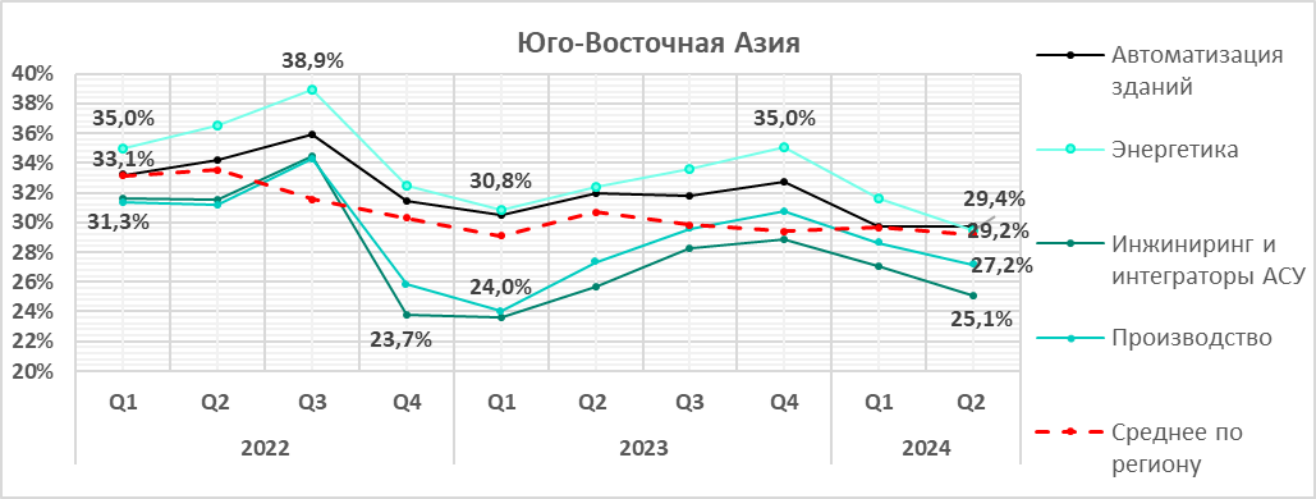


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Во **втором квартале 2024 года** во всех рассмотренных отраслях региона отмечено снижение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, за исключением автоматизации зданий, где показатель остался без изменений.



Тренды в рассмотренных отраслях демонстрируют в целом положительную динамику, хотя она сопровождается резкими скачками и продолжительными периодами медленного роста и снижения показателей.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Центральная Азия

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
7,58%

▲ незначительный рост во II кв. 2024 г.
1,1x выше среднего по миру
2-е место в мире

-2 место-

Шпионские программы
4,80%

▲ **1,1x** рост во II кв. 2024 г.
1,2x выше среднего по миру

-3 место-

Скрипты и фишинговые страницы
4,28%

▼ снижение во II кв. 2024 г.

Черви
2,72%

▼ снижение во II кв. 2024 г.
1,8x выше среднего по миру
2-е место в мире

Майнеры — исполняемые файлы
1,62%

▼ снижение во II кв. 2024 г.
1,8x выше среднего по миру
1-е место в мире

Программы-вымогатели
0,19%

▲ **1,1x** рост во II кв. 2024 г.
Незначительно выше среднего по миру

Интернет
как источник угроз
12,33%

▲ **1,1x** рост во II кв. 2024 г.
1,1x выше среднего по миру
1-е место в мире
1-е место в мире **по росту**

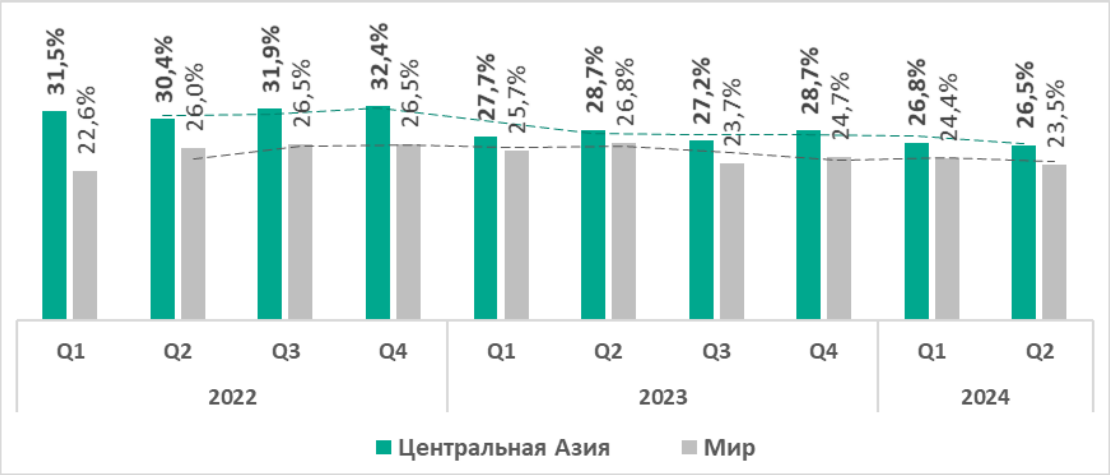
Съемные носители
как источник угроз
1,37%

▼ снижение во II кв. 2024 г.
1,5x выше среднего по миру

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Центральная Азия занимает **третье место** в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Хотя этот показатель все еще превышает среднемировое значение, с первого квартала 2023 года наблюдается тенденция к сокращению разрыва.



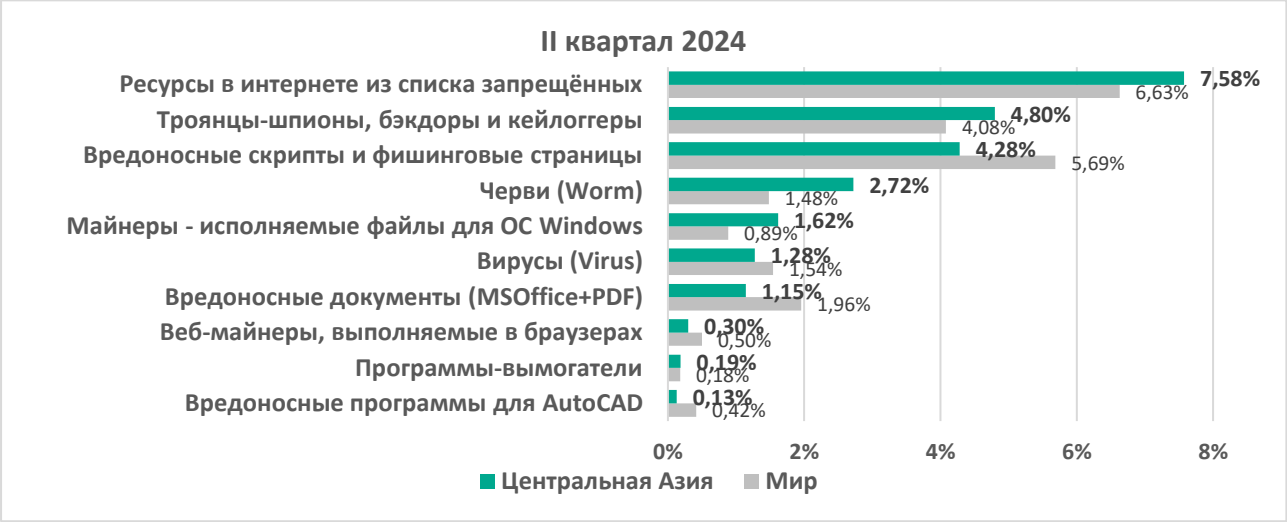
Сравнительный анализ

Центральная Азия находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- первое место — угрозы из интернета, майнеры — исполняемые файлы для ОС Windows;
- второе место — ресурсы в интернете из списка запрещенных, черви.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории угроз



По сравнению со среднемировыми показателями, в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории угроз:

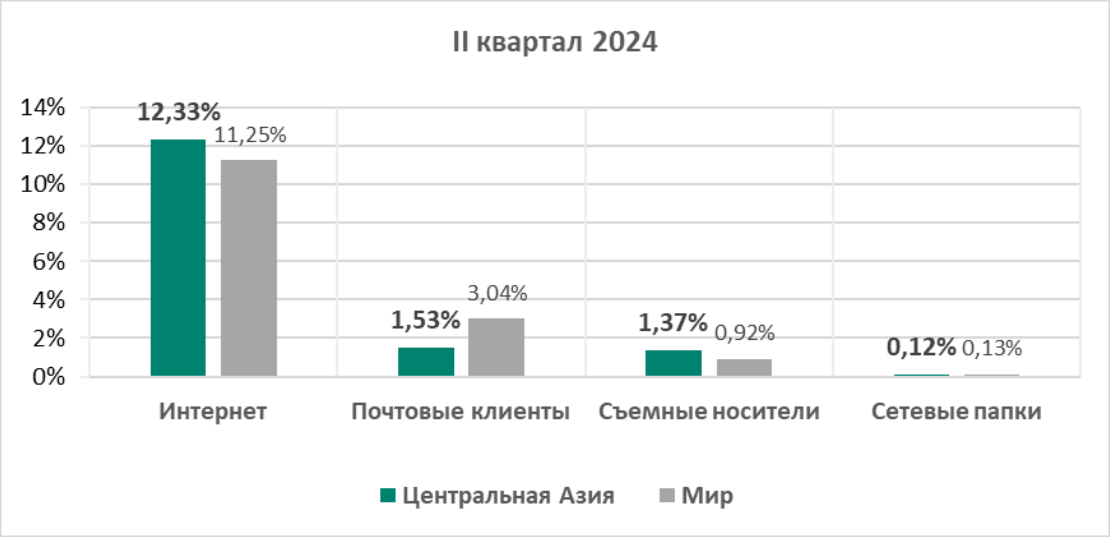
- черви — в 1,8 раз;
- майнеры — исполняемые файлы для ОС Windows — в 1,8 раз. Эта категория угроз находится в регионе на пятом месте (в мировом рейтинге — на седьмом месте);
- шпионские программы — в 1,2 раза;
- ресурсы в интернете из списка запрещенных — в 1,1 раза.

Источники угроз

Регион занимает первое место в мире по доле компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, с превышением среднемирового показателя в 1,1 раза.

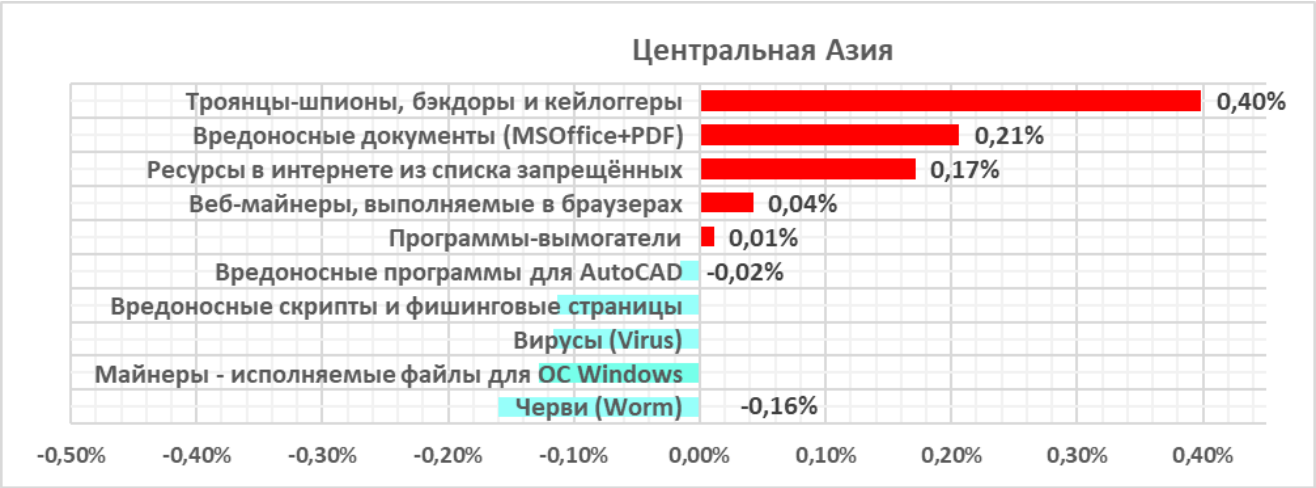
Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы на **съемных носителях**, превысила среднемировой показатель в 1,5 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Изменения за квартал и тренды

Категории угроз

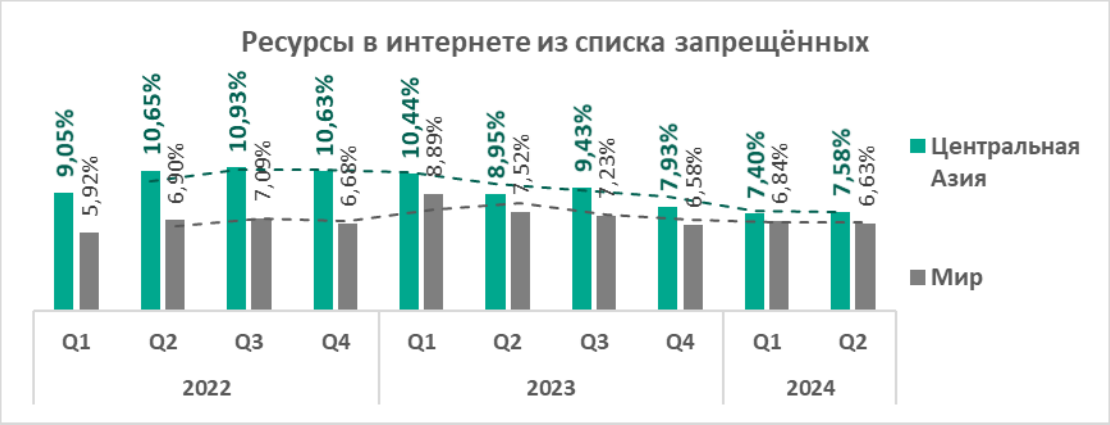


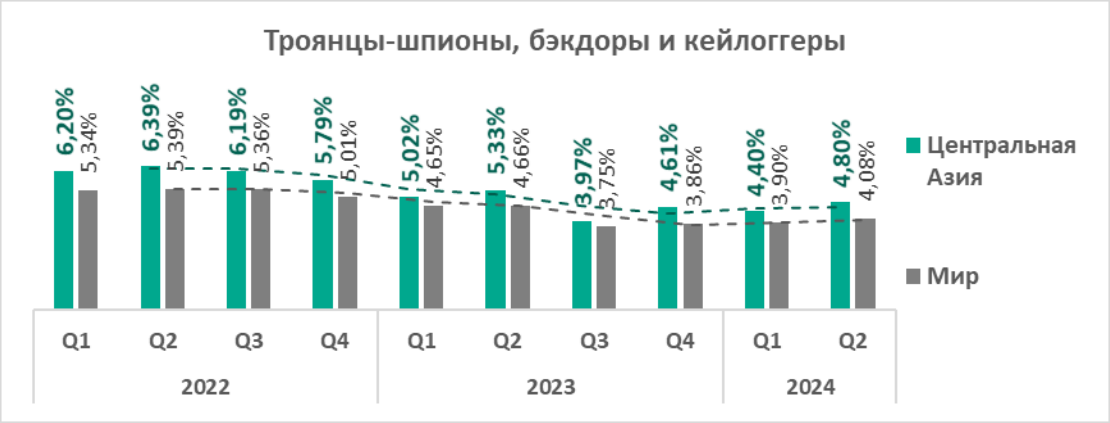
Наибольший рост за квартал зафиксирован в доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

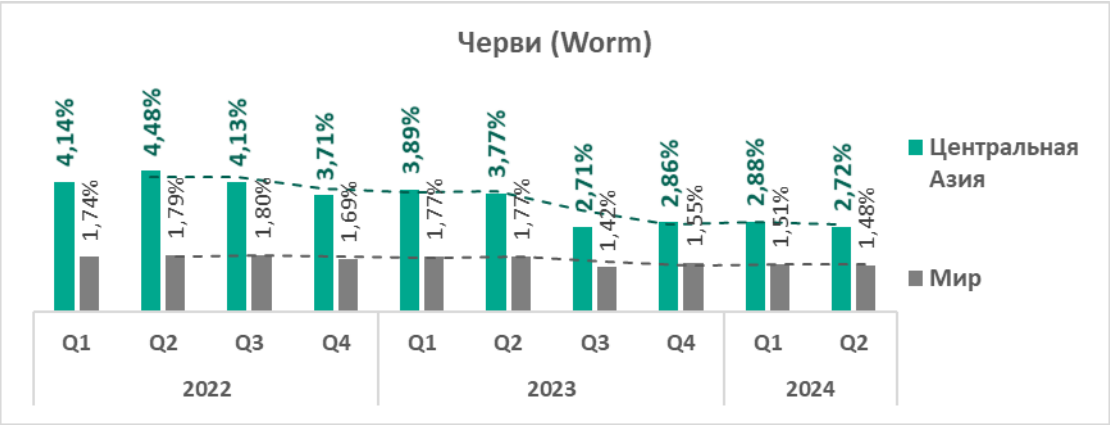
- вредоносные документы — в 1,2 раза;
- веб-майнеры — в 1,2 раза;
- шпионские программы — в 1,1 раза;
- программы-вымогатели — в 1,1 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.







© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Центральной Азии за 2,5 года. **Ресурсы в интернете из списка запрещенных** остаются ведущей категорией угроз в регионе с первого квартала 2022 года, за исключением четвертого квартала 2022 года и четвертого квартала 2023 года. **Шпионские программы** в первом квартале 2024 года поднялись с третьего на второе место.

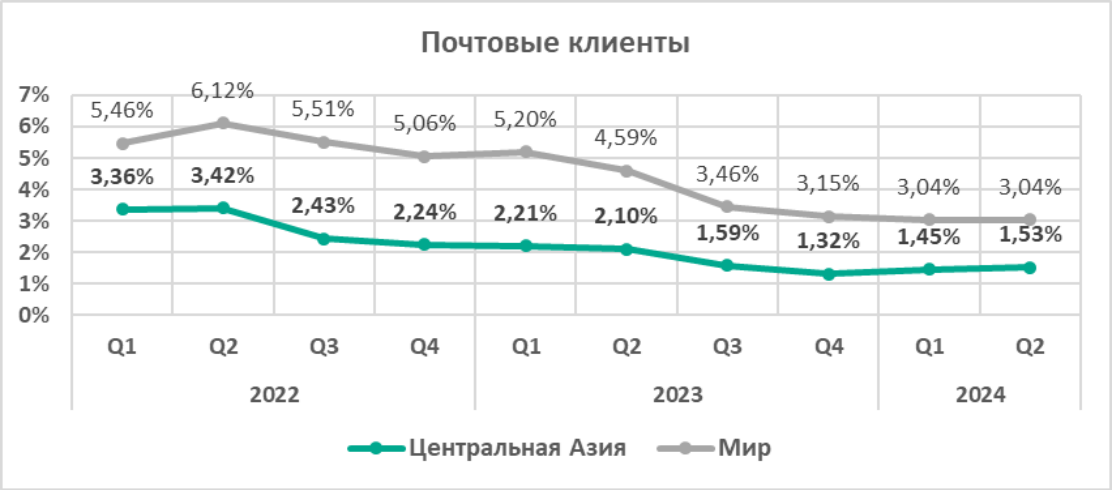
Центральная Азия	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Ресурсы в интернете из списка запрещенных	1	1	1	2	1	1	1	2	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	3	3	3	3	3	3	2	2
Вредоносные скрипты и фишинговые страницы (JS и HTML)	3	3	2	1	2	2	2	1	3	3
Черви	4	4	4	4	4	4	4	4	4	4
Майнеры — исполняемые файлы для ОС Windows	5	5	5	5	5	5	5	5	5	5
Вирусы	7	7	7	7	7	7	6	6	6	6
Вредоносные документы (MSOffice + PDF)	6	6	6	6	6	6	7	7	7	7
Веб-майнеры, выполняемые в браузерах	8	8	8	8	8	8	8	8	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

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Источники угроз

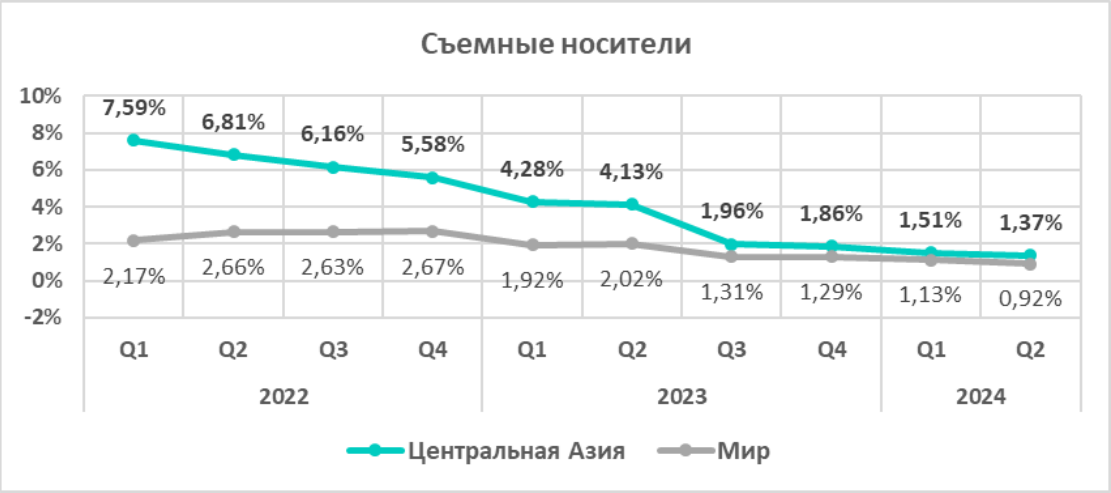
Во втором квартале 2024 года в регионе увеличилась доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, причем показатель превысил среднемировое значение в 1,1 раза.

Показатель угроз из **почтовых клиентов** также незначительно вырос во втором квартале 2024 года.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

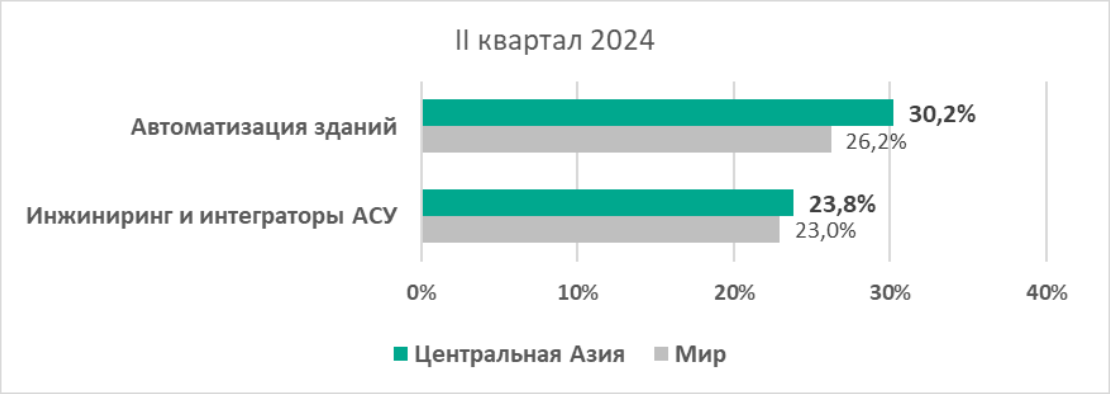
Показатель угроз на **съемных носителях** превышает среднемировое значение на протяжении всего периода наблюдения, но к третьему кварталу 2023 года разрыв значительно сократился по сравнению с началом 2022 года и с тех пор остается стабильным.



Отрасли

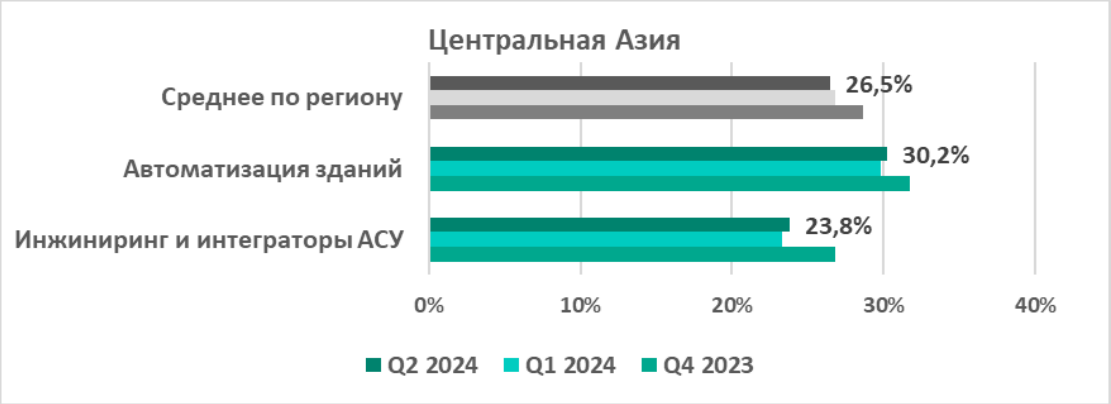
- **Наиболее часто встречающейся с угрозами отраслью** региона среди рассмотренных в отчете оказалась **автоматизация зданий**.

  В этой отрасли доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает среднемировой показатель в 1,2 раза.

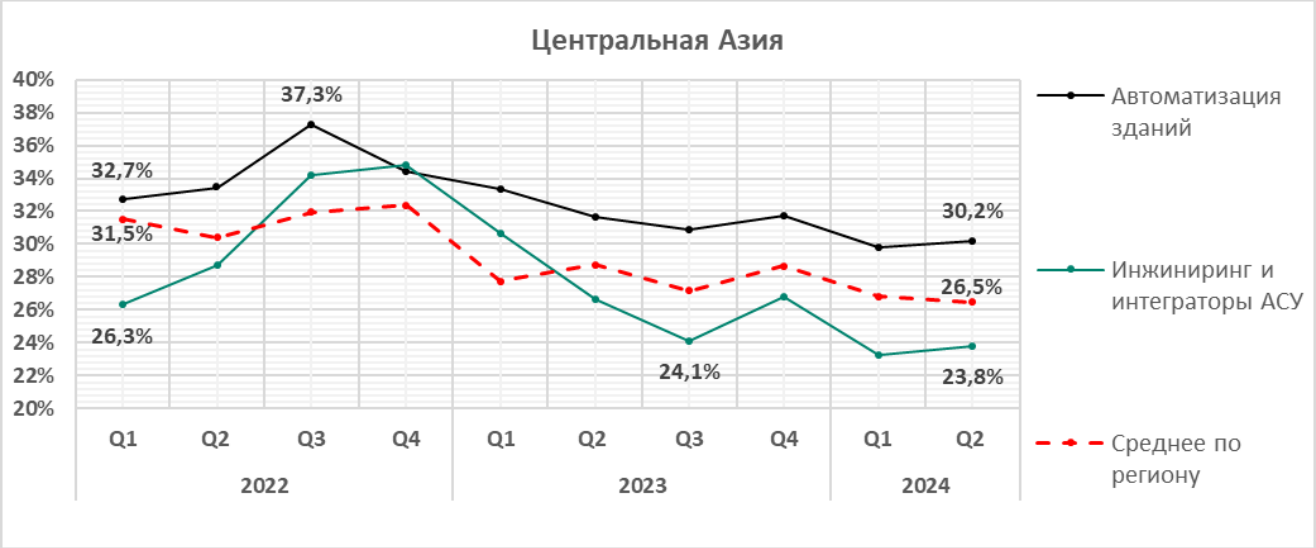


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Во **втором квартале 2024 года** в обеих рассмотренных отраслях зафиксирован незначительный рост доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



Тренды в рассмотренных отраслях демонстрируют в целом положительную динамику.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Ближний Восток

Актуальные угрозы

-1 место-

Скрипты и фишинговые страницы
6,90%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру
2-е место в мире

-2 место-

Шпионские программы
6,29%

▲ **1,1x** рост во II кв. 2024 г.
1,5x выше среднего по миру
2-е место в мире

-3 место-

Интернет-ресурсы из списка запрещенных
5,02%

▼ снижение во II кв. 2024 г.

Вредоносные документы
2,29%

▲ незначительный рост во II кв. 2024 г.
1,2x выше среднего по миру

Черви
2,22%

▼ снижение во II кв. 2024 г.
1,5x выше среднего по миру
3-е место в мире

Вирусы
1,99%

▼ снижение во II кв. 2024 г.
1,3x выше среднего по миру

Веб-майнеры
0,81%

▼ снижение во II кв. 2024 г.
1,6x выше среднего по миру
2-е место в мире

Программы-вымогатели
0,33%

▲ **1,2x** рост во II кв. 2024 г.
1,8x выше среднего по миру
1-е место в мире

Интернет
как источник угроз
11.06%

▼ снижение во II кв. 2024 г.

Почтовые клиенты
как источник угроз
4,79%

▼ снижение во II кв. 2024 г.
1,6x выше среднего по миру
3-е место в мире

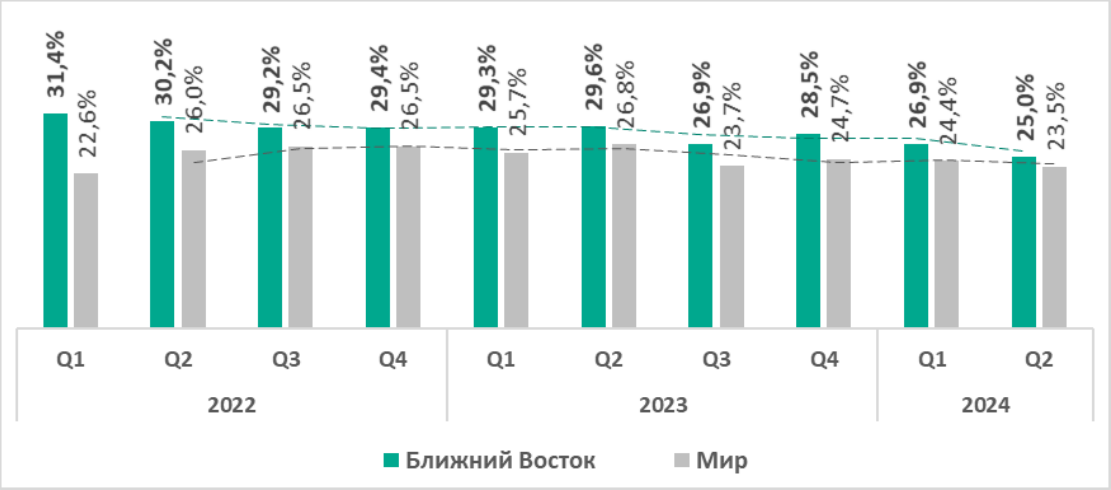
Съемные носители
как источник угроз
1,31%

▼ снижение во II кв. 2024 г.
1,4x выше среднего по миру

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Ближний Восток занимает **четвертое место** в мире по доле компьютеров АСУ, на которых заблокированы вредоносные объекты. Этот показатель превышает среднемировое значение начиная с первого квартала 2022 года.



Сравнительный анализ

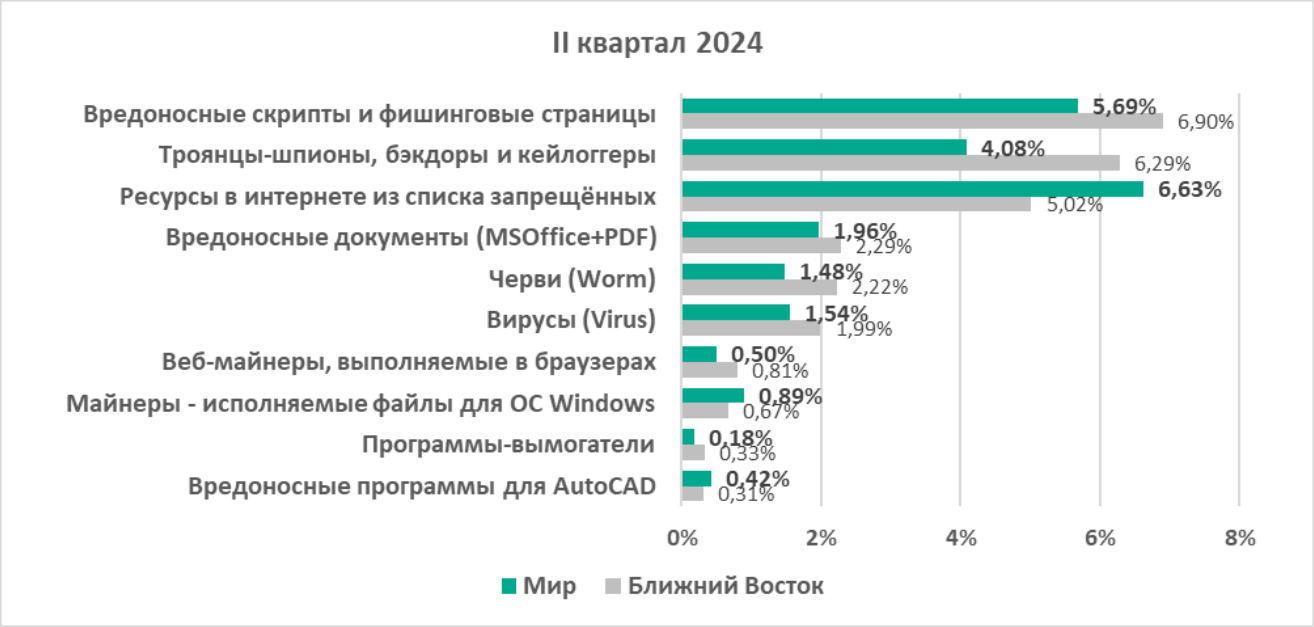
Ближний Восток находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- первое место — программы-вымогатели;
- второе место — шпионские программы, вредоносные скрипты и фишинговые страницы, веб-майнеры;
- третье место — черви, угрозы из почтовых клиентов.

Категории угроз

- **По сравнению с мировыми показателями**, в регионе выше доля компьютеров АСУ, на которых заблокированы все категории вредоносных объектов, за исключением ресурсов в интернете из списка запрещенных, майнеров — исполняемых файлов и вредоносных программ для AutoCAD.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Наиболее существенно по сравнению со среднемировыми значениями выросли показатели следующих категорий угроз:

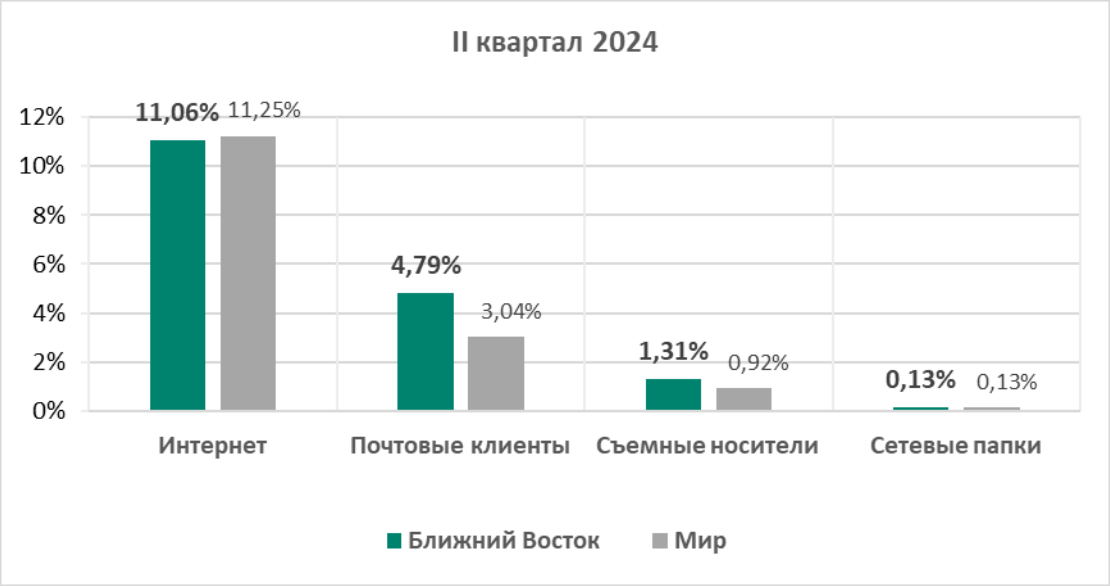
- программы-вымогатели — в 1,8 раза;
- веб-майнеры — в 1,6 раза;
- шпионские программы — в 1,5 раза;
- черви — в 1,5 раза;
- вирусы — в 1,3 раза;
- вредоносные скрипты и фишинговые страницы — в 1,2 раза;
- вредоносные документы — в 1,2 раза.

Источники угроз

Ближний Восток занимает **третье место в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, с превышением среднемирового значения в 1,6 раза.

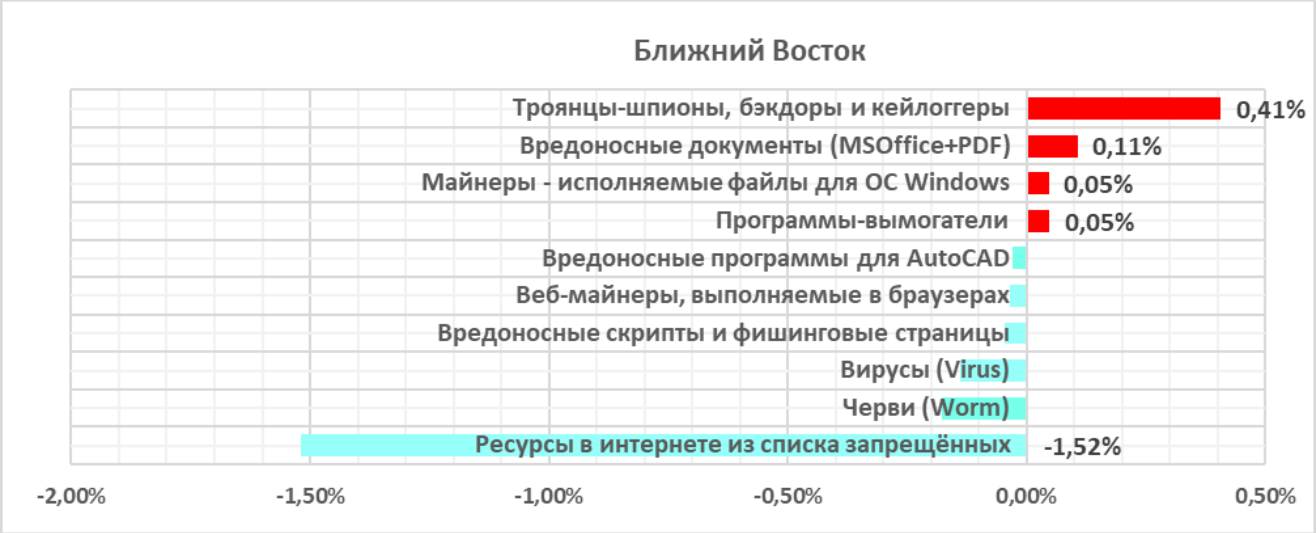
Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы на **съемных носителях**, превысила среднемировое значение в 1,4 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Изменения за квартал и тренды

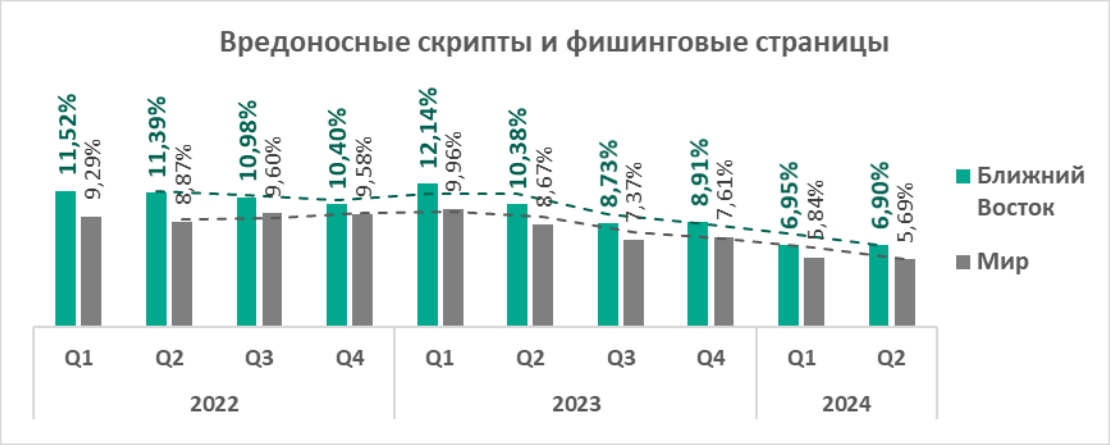
Категории угроз

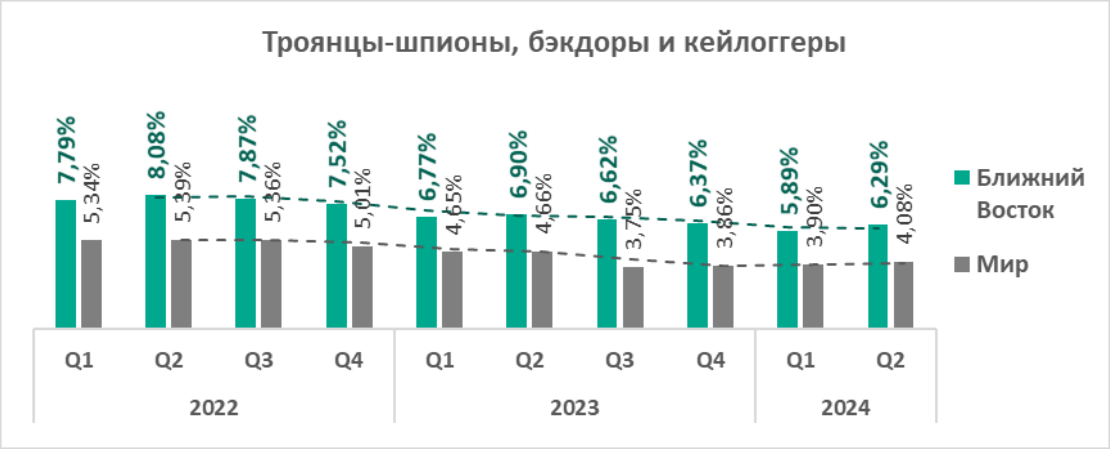


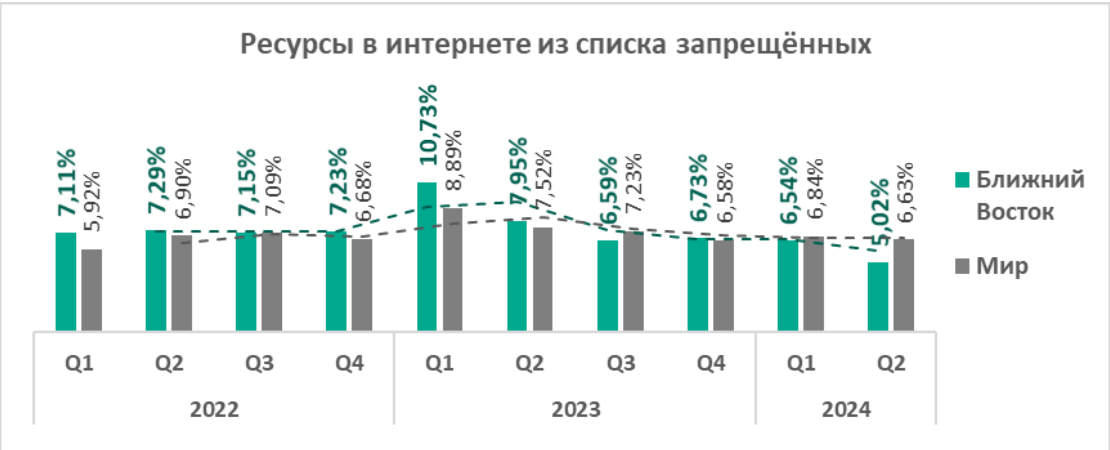
- **Наибольший рост за квартал** отмечен в доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
  - программы-вымогатели — в 1,2 раза;
  - майнеры — исполняемые файлы для ОС Windows — в 1,1 раза;
  - шпионские программы — в 1,1 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

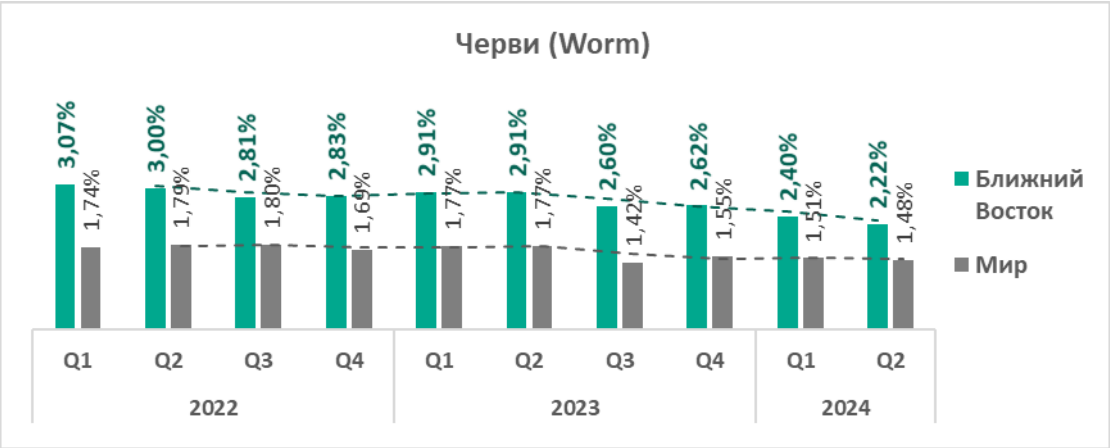
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

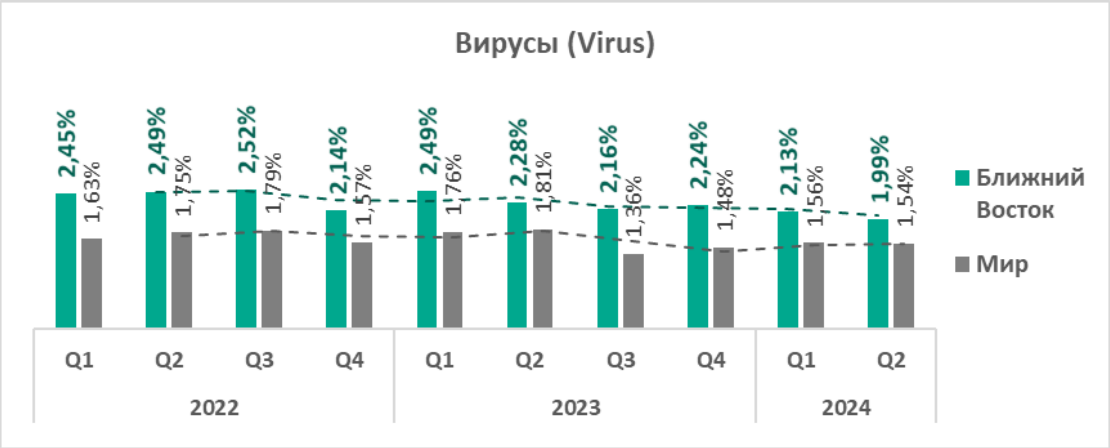




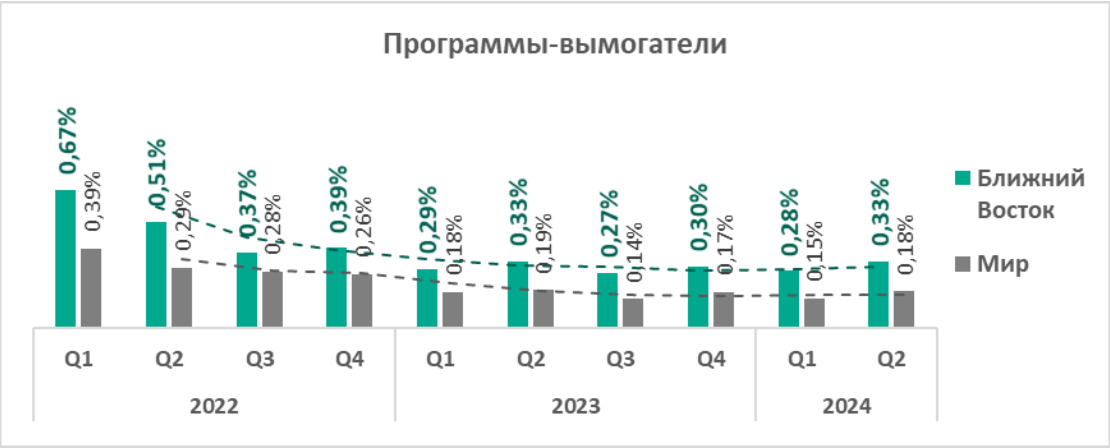


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

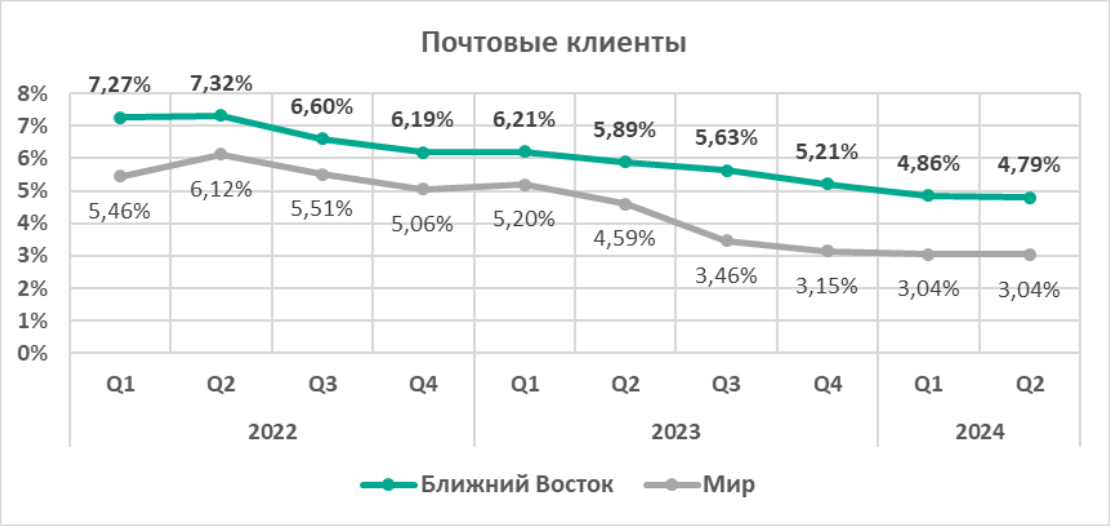
- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз на Ближнем Востоке за 2,5 года. **Вредоносные скрипты и фишинговые страницы** возглавляют рейтинг категорий угроз в регионе с первого квартала 2022 года. Во втором квартале 2024 года **шпионские программы** поднялись в рейтинге с третьего на второе место.

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

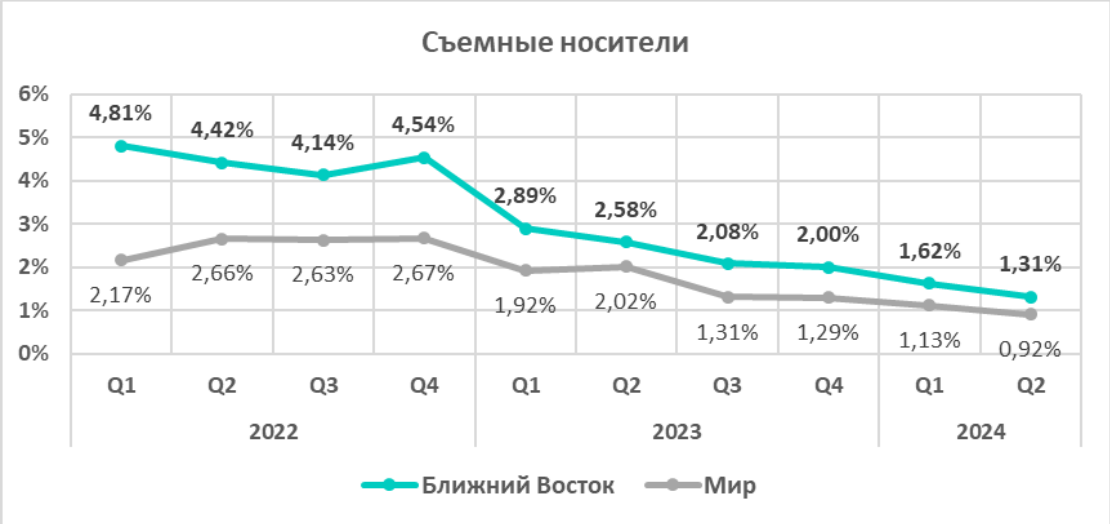
Источники угроз

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Уровень угроз из **почтовых клиентов** стабильно превышает среднемировой показатель на протяжении всего периода наблюдений. В третьем квартале 2023 года разрыв существенно увеличился и с тех пор постепенно сужается.



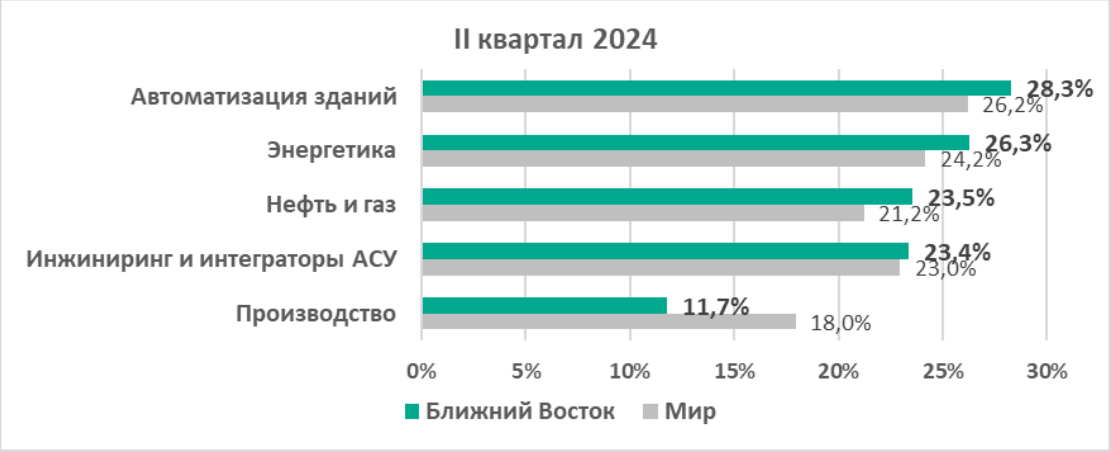
Показатель угроз на **съемных носителях** превышает среднемировое значение на протяжении всего периода наблюдений. Однако ко второму кварталу 2023 года разница между региональным и среднемировым значениями существенно сократилась и с тех пор сохраняется примерно на одном уровне.



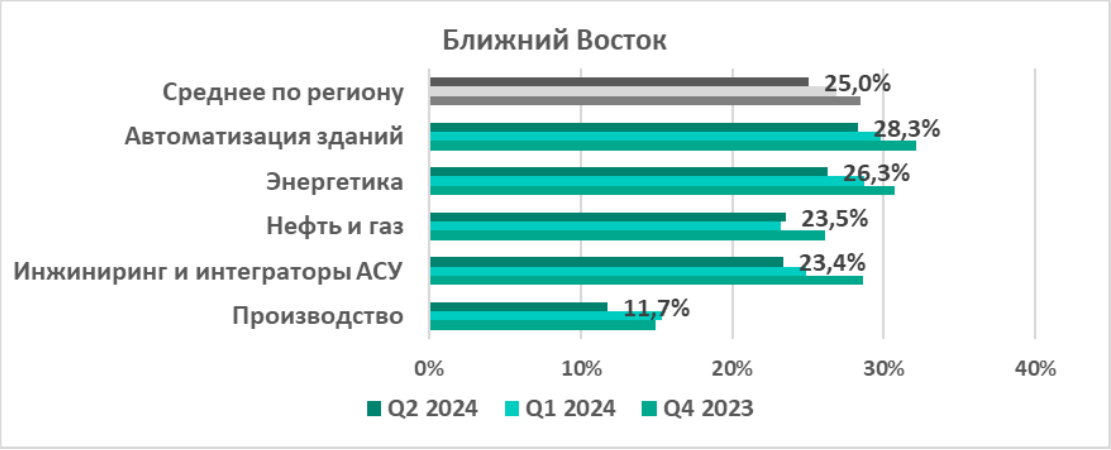
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** региона среди рассмотренных в отчете является **автоматизация зданий**.
- Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **превышает среднемировые значения** в следующих отраслях:
  - автоматизация зданий — в 1,1 раза;
  - энергетика — в 1,1 раза;
  - нефть и газ — в 1,1 раза.

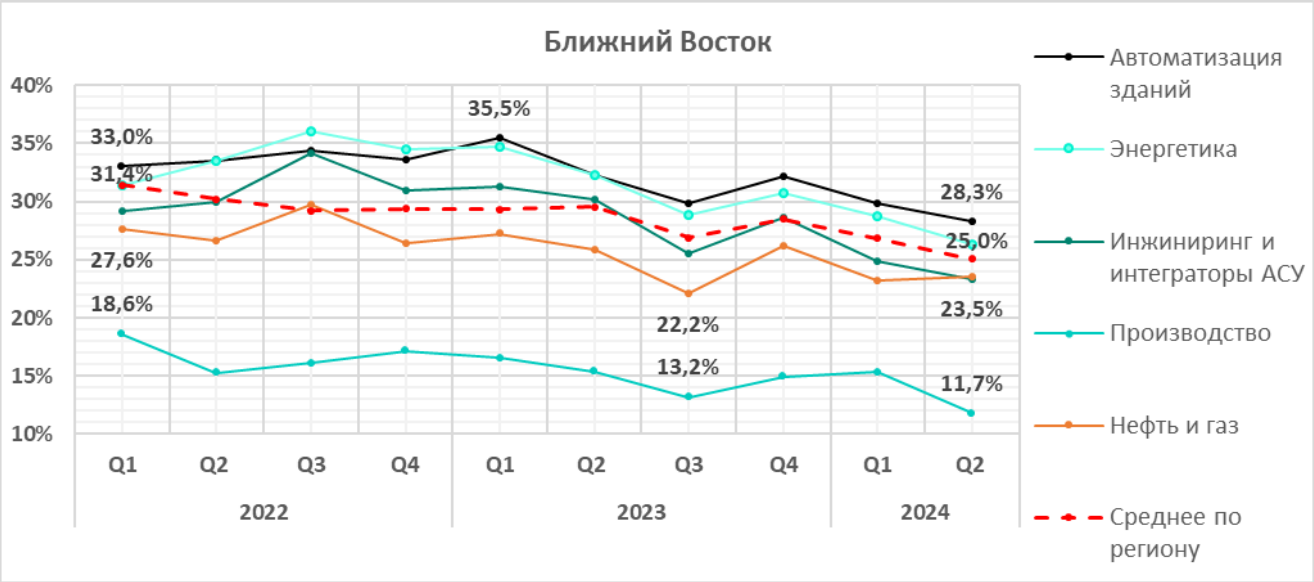


- Во **втором квартале 2024 года** в **нефтегазовой** отрасли отмечено незначительное увеличение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, в то время как в остальных отраслях этот показатель уменьшился.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Тренды в рассмотренных отраслях демонстрируют в целом положительную динамику.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Восточная Европа

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
7,07%

▲ незначительный рост во II кв. 2024 г.
1,1x выше среднего по миру
4-е место в мире

-2 место-

Скрипты и фишинговые страницы
5,75%

▼ снижение во II кв. 2024 г.
выше среднего по миру

-3 место-

Шпионские программы
5,44%

▲ **1,1x** рост во II кв. 2024 г.
1,3x выше среднего по миру
3-е место в мире **по росту**

Вредоносные документы
2,32%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру
4-е место в мире

Черви
1,56%

▲ незначительный рост во II кв. 2024 г.
1,1x выше среднего по миру

Майнеры — исполняемые файлы
1,01%

▼ снижение во II кв. 2024 г.
1,1x выше среднего по миру
4-е место в мире

Веб-майнеры
0,63%

▲ незначительный рост во II кв. 2024 г.
1,3x выше среднего по миру
4-е место в мире

Программы-вымогатели
0,18%

▲ **1,1x** рост во II кв. 2024 г.

Интернет
как источник угроз
10,98%

▼ снижение во II кв. 2024 г.

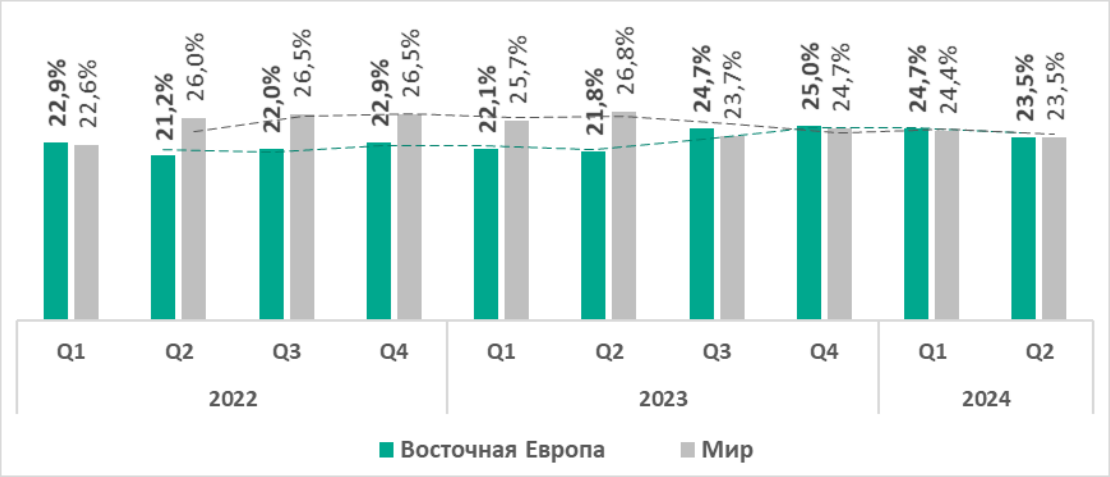
Почтовые клиенты
как источник угроз
4,97%

▲ **1,1x** рост во II кв. 2024 г.
1,6x выше среднего по миру
2-е место в мире
3-е место в мире **по росту**

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Восточная Европа занимает **пятое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Ранее, до второго квартала 2023 года, регион не поднимался выше девятого места. Во втором квартале 2024 года показатель сравнялся со среднемировым значением.



Сравнительный анализ

Категории угроз

По сравнению с мировыми показателями, в регионе выше доля компьютеров АСУ, на которых были заблокированы все категории угроз, за исключением вирусов и вредоносных программ для AutoCAD.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Наиболее существенно по сравнению со среднемировыми значениями выросли показатели следующих категорий угроз:

- шпионские программы — в 1,3 раза;
- веб-майнеры — в 1,3 раза;
- вредоносные документы — в 1,2 раза.

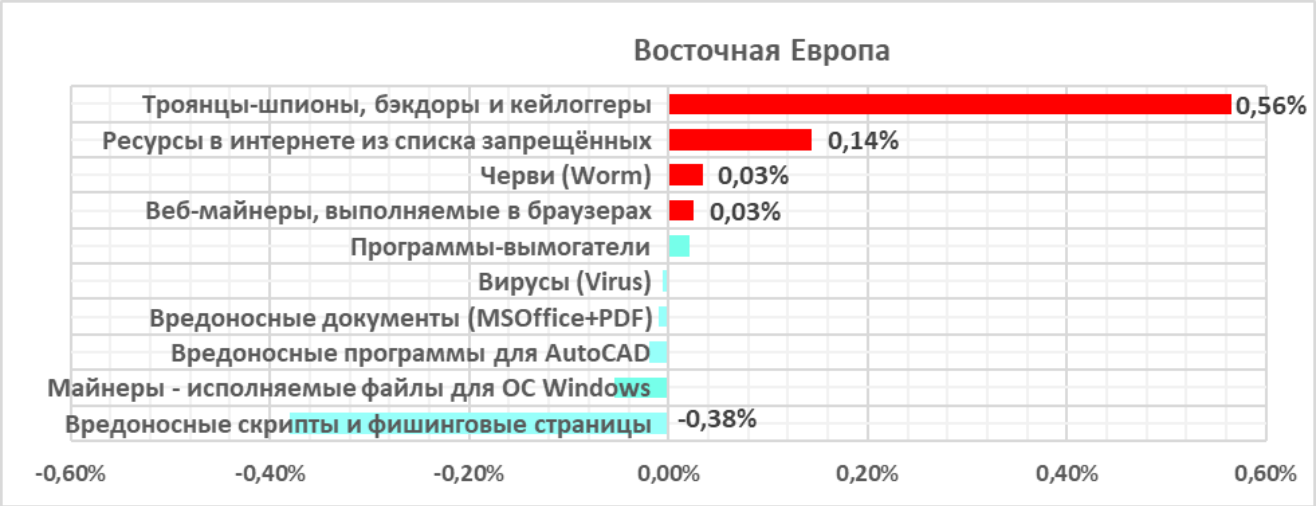
Источники угроз

Регион находится на втором месте в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, с превышением среднемирового значения в 1,6 раза.

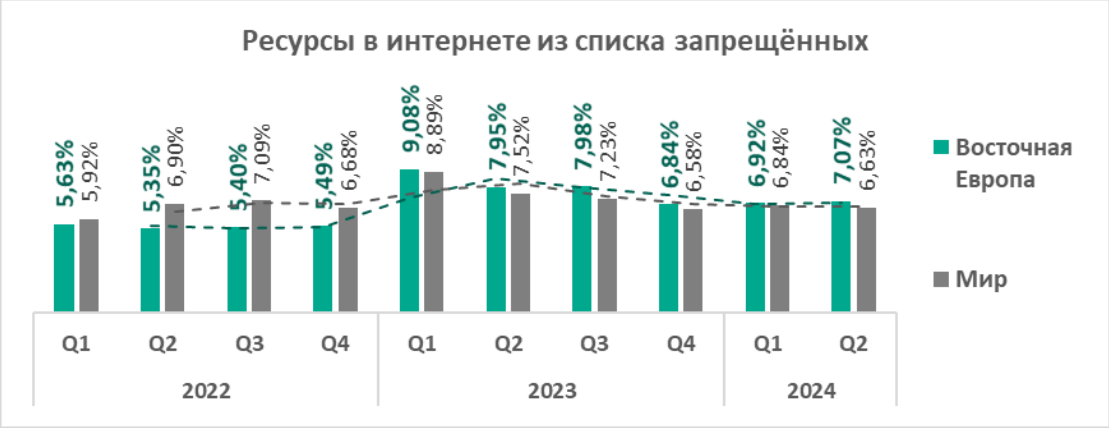
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменения за квартал и тренды

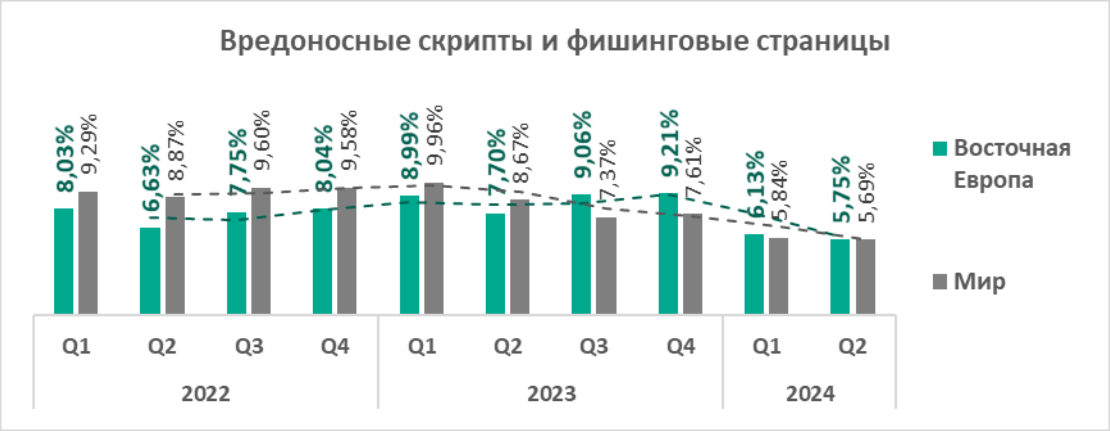
Категории угроз

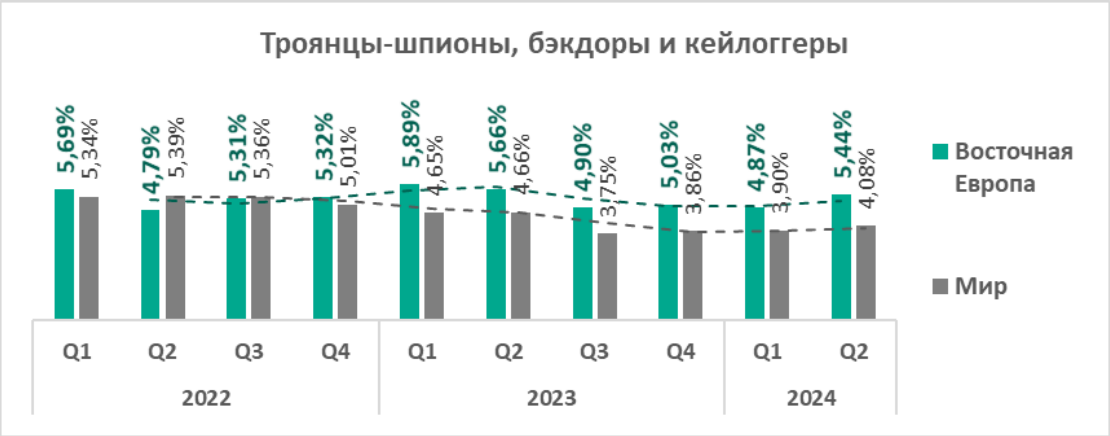


- **Наибольший рост за квартал** отмечен в доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - шпионские программы — в 1,1 раз; третье место в мире по величине роста;
  - программы-вымогатели — в 1,1 раза.
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

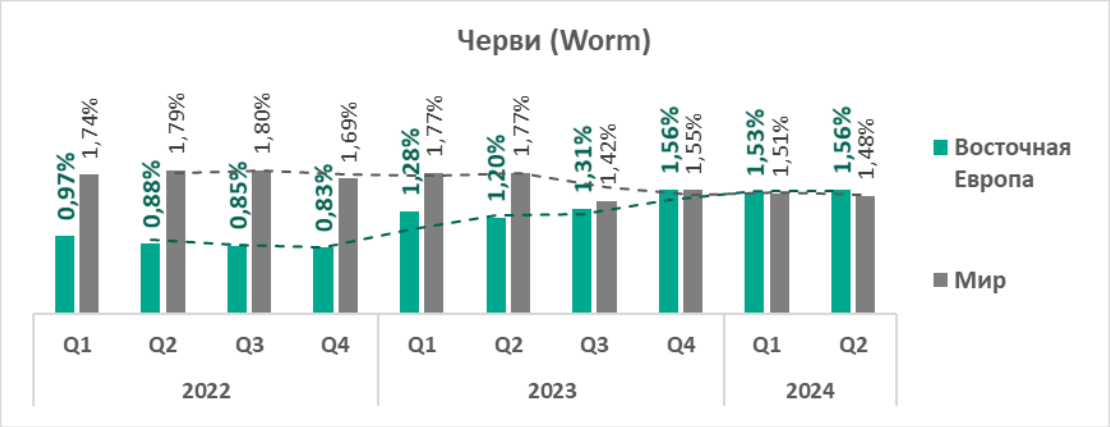


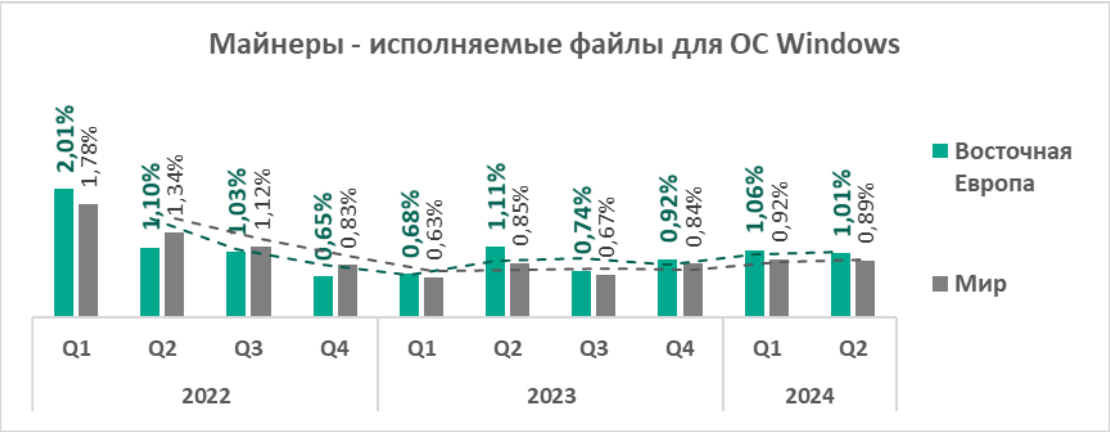
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



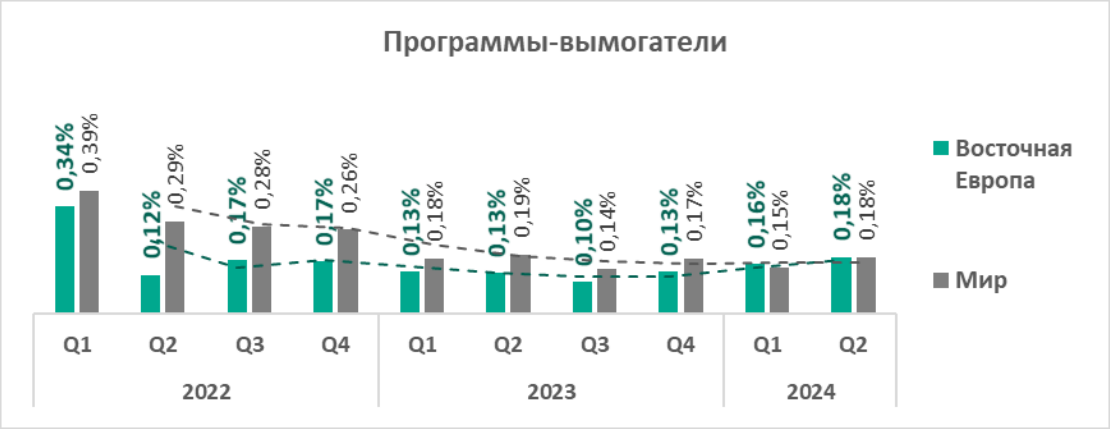


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Европе за 2,5 года. Ведущей категорией угроз в регионе с первого квартала 2024 года являются **ресурсы в интернете из списка запрещенных,** а **вредоносные скрипты и фишинговые страницы** тогда опустились с первого на второе место.

Восточная Европа	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Ресурсы в интернете из списка запрещенных	3	2	2	2	1	1	2	2	1	1
Вредоносные скрипты и фишинговые страницы (JS и HTML)	1	1	1	1	2	2	1	1	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	3	3	3	3	3	3	3	3	3
Вредоносные документы (MSOffice + PDF)	4	4	4	4	4	4	4	4	4	4
Черви	7	6	7	6	5	6	5	5	5	5
Майнеры — исполняемые файлы для ОС Windows	5	5	6	7	7	7	6	6	6	6
Веб-майнеры, выполняемые в браузерах	6	7	5	5	6	5	7	7	7	7
Вирусы	8	8	8	8	8	8	8	8	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

Во втором квартале 2024 года угрозы из **почтовых клиентов** в Восточной Европе занимают третье место в мире по величине роста. Показатель остается выше среднемирового значения на протяжении всего периода

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

наблюдений. Разрыв начал заметно увеличиваться во втором квартале 2023 года и достиг своего максимума во втором квартале 2024 года.

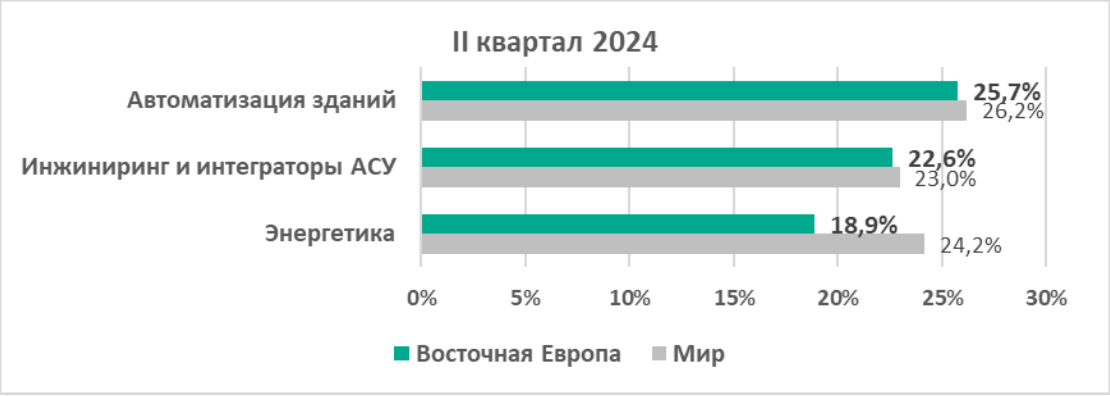
Угрозы из **интернета** и на **съемных носителях** показывают нисходящие тренды в течение последних трех кварталов.

Отрасли

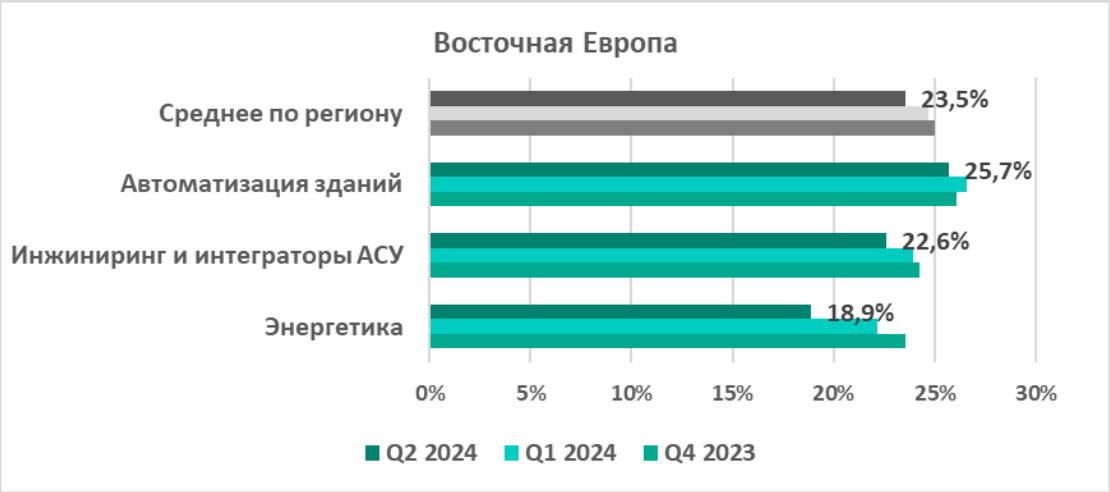
- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий**.

  По сравнению с **среднемировыми показателями**, во всех рассмотренных отраслях зафиксирована более низкая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты.

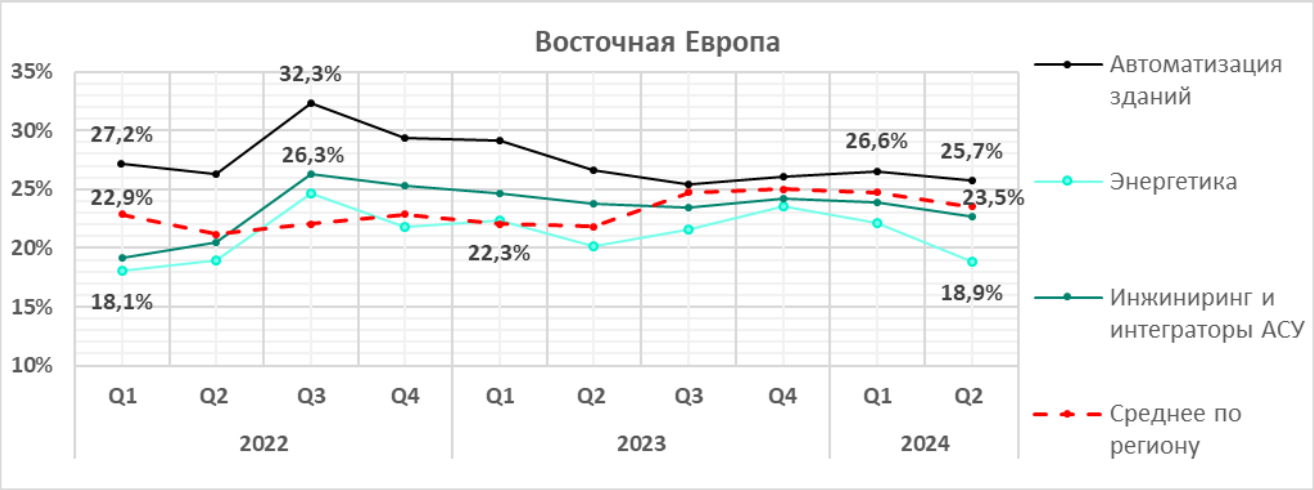
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Во **втором квартале 2024 года** во всех рассматриваемых отраслях наблюдалось снижение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



В целом, **тренды** в рассмотренных отраслях указывают на стабилизацию после значительного роста в 2022 году.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Россия

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных

7,80%

▲ незначительный рост во II кв. 2024 г.
1,2x выше среднего по миру
1-е место в мире

-2 место-

Скрипты и фишинговые страницы

4,53%

▼ снижение во II кв. 2024 г.

-3 место-

Шпионские программы

2,31%

▼ снижение во II кв. 2024 г.

Майнеры — исполняемые файлы

1,18%

▼ снижение во II кв. 2024 г.
1,3x выше среднего по миру
2-е место в мире

Вредоносные документы

0,90%

▲ **1,2x** рост во II кв. 2024 г.

Интернет
как источник угроз

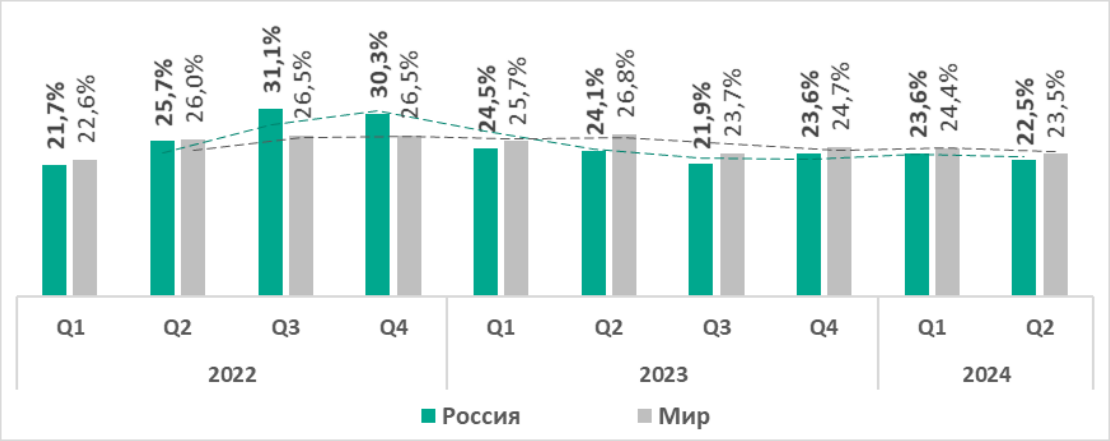
11,89%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру
3-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Россия занимает **шестое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Этот показатель немного ниже среднемирового значения, за исключением третьего и четвертого кварталов 2022 года.



Сравнительный анализ

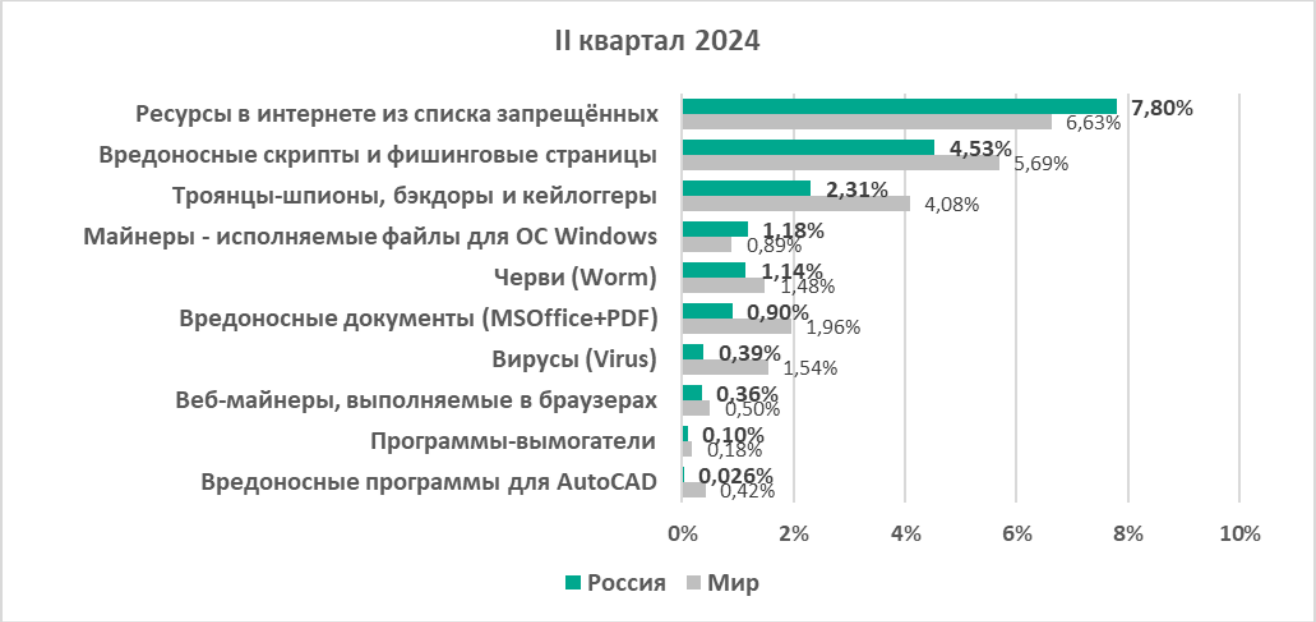
- Россия находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - первое место — ресурсы в интернете из списка запрещенных;
  - второе место — майнеры — исполняемые файлы для ОС Windows;
  - третье место — угрозы из интернета.

Категории угроз

По сравнению с мировыми показателями, в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории угроз:

- майнеры — исполняемые файлы для ОС Windows — в 1,3 раза;
- ресурсы в интернете из списка запрещенных — в 1,2 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Источники угроз

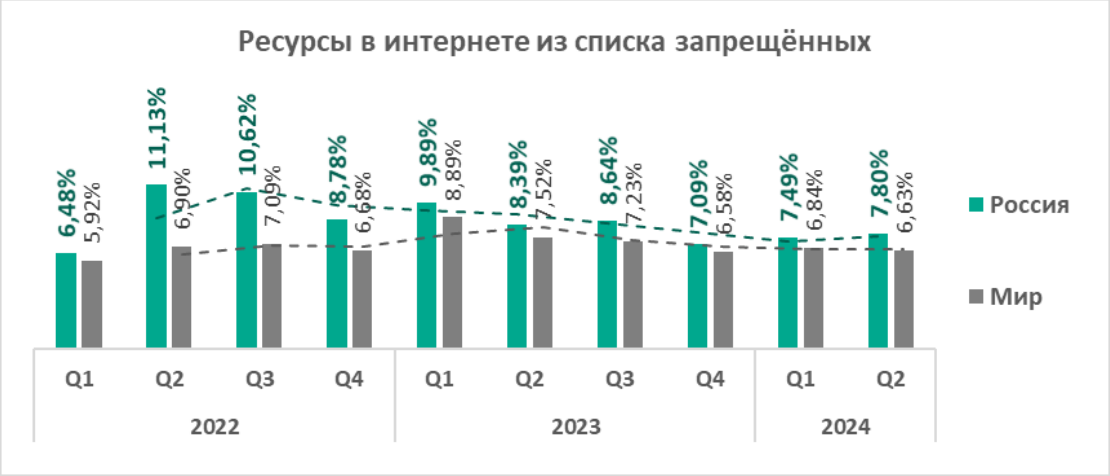
Россия находится **на третьем месте в мировом рейтинге** по доле компьютеров АСУ, на которых заблокированы угрозы из **интернета**, с показателем, незначительно превышающим среднемировое значение.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

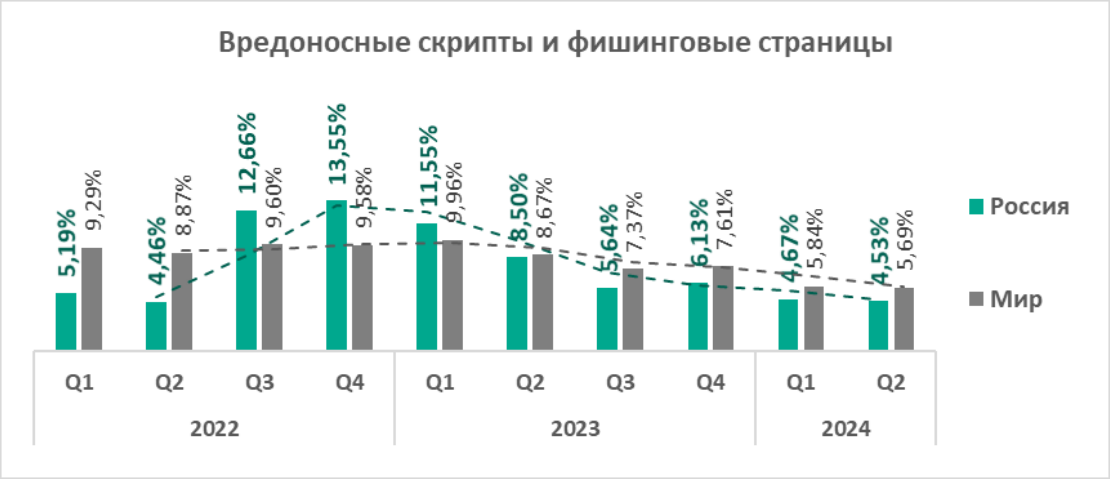
Изменения за квартал и тренды

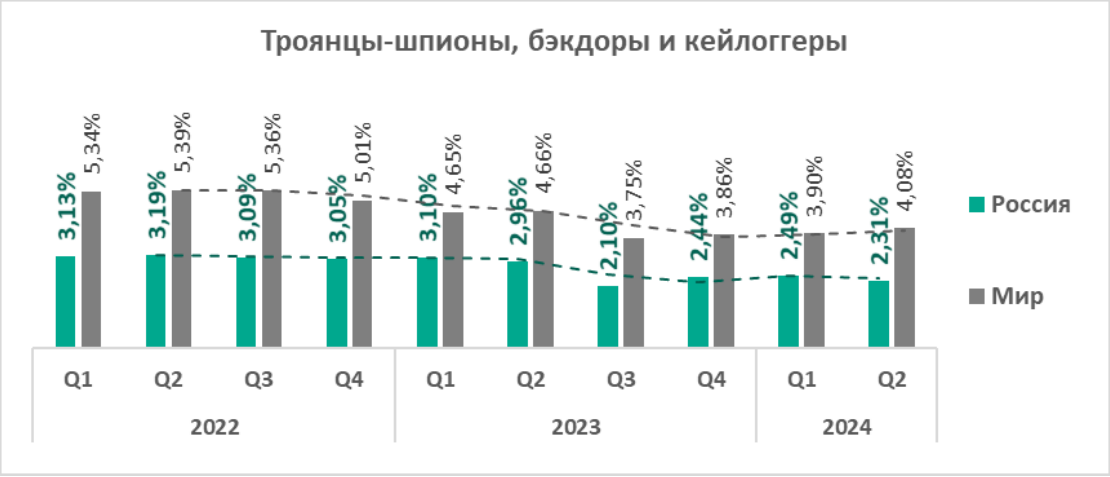
Категории угроз

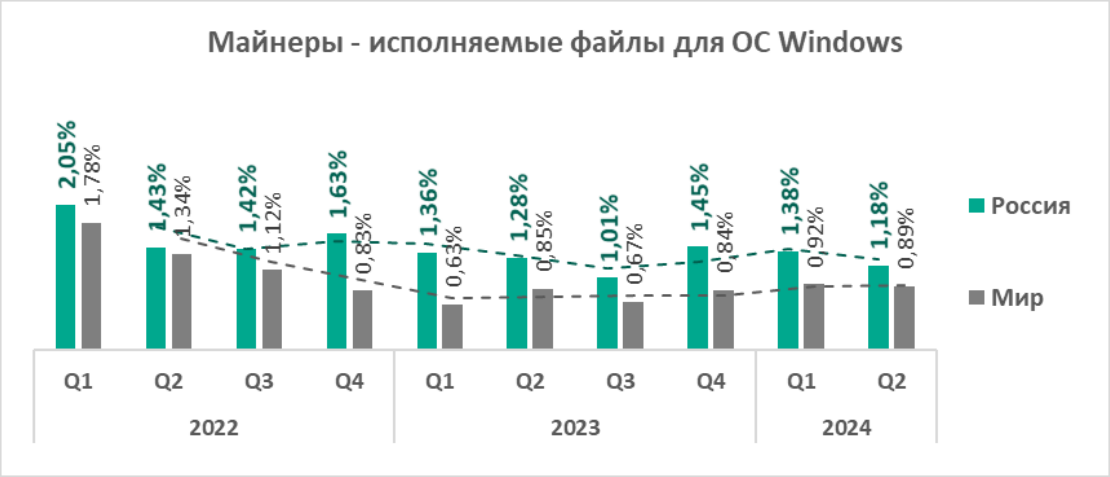
- **Наиболее сильно** во втором квартале 2024 года выросла доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - вредоносные документы — в 1,2 раза;
  - вредоносные программы для AutoCAD — в 1,2 раза.
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»







© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в России за 2,5 года. Ведущей категорией угроз в регионе, начиная с третьего квартала 2023 года, являются **ресурсы в интернете из списка запрещенных**.

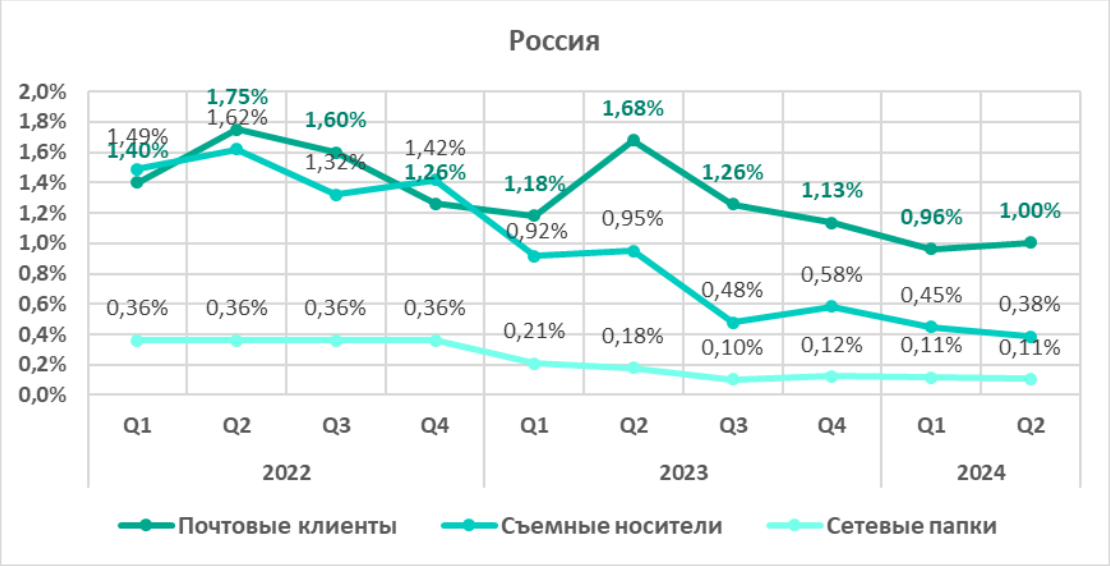
Россия	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Ресурсы в интернете из списка запрещенных	1	1	2	2	2	2	1	1	1	1
Вредоносные скрипты и фишинговые страницы (JS и HTML)	2	2	1	1	1	1	2	2	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	3	3	3
Майнеры — исполняемые файлы для ОС Windows	4	5	4	4	4	5	5	4	4	4
Черви	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	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 нисходящий тренд начиная с четвертого квартала 2022 года, а со второго квартала 2023 года этот показатель практически совпадает со среднемировым значением.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Другие источники угроз также демонстрируют преимущественно нисходящие тренды.

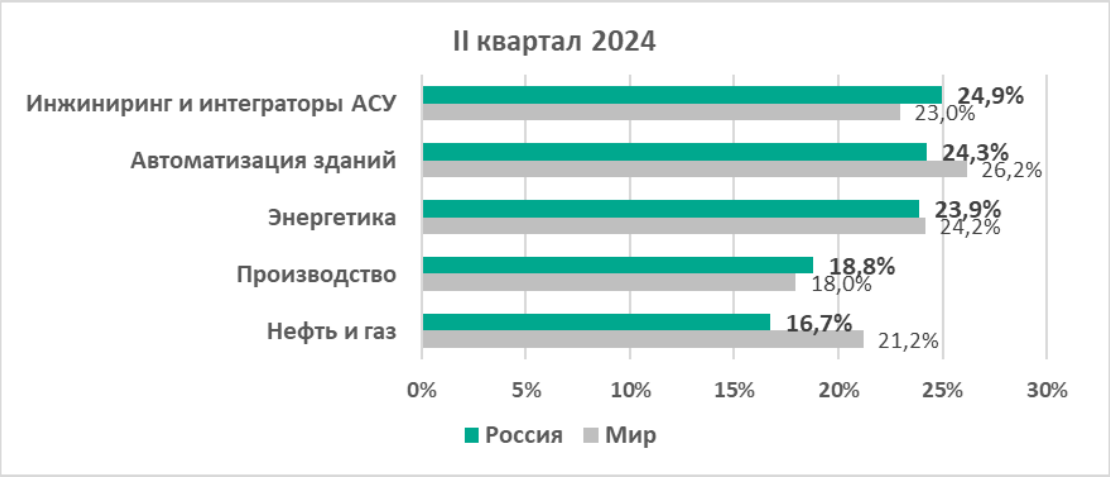


Отрасли

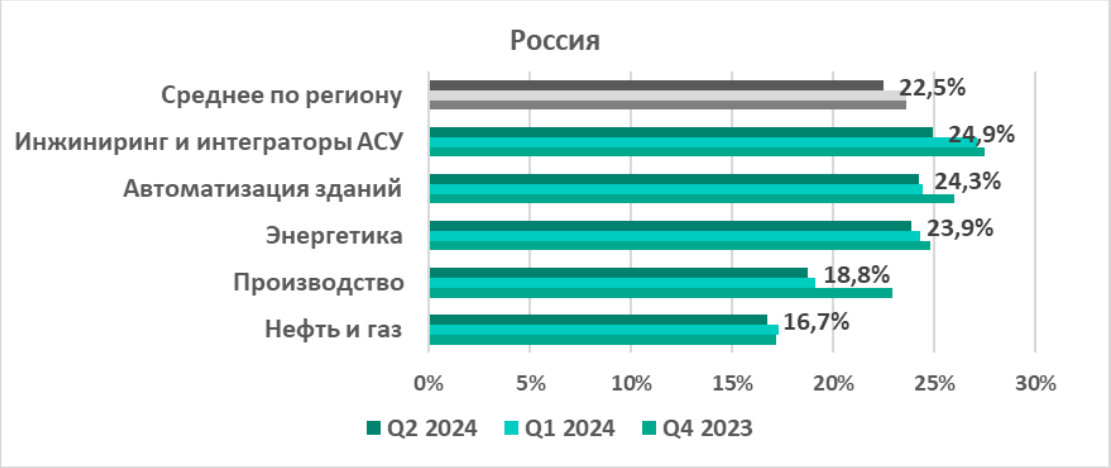
- **Наиболее часто встречающиеся с угрозами отрасли** региона среди рассмотренных в отчете:
  - инжиниринг и интеграторы АСУ;
  - автоматизация зданий;
  - энергетика.
- По сравнению с соответствующими **среднемировыми показателями**, более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, отмечена в следующих отраслях:

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- инжиниринг и интеграторы АСУ — в 1,1 раза;
- производство — незначительно.

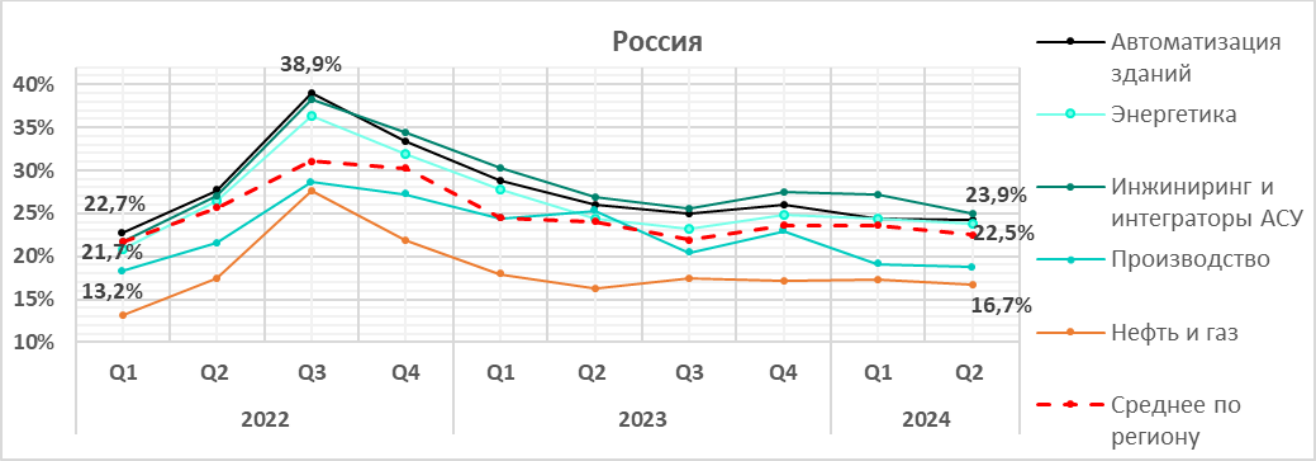


- **Во втором квартале 2024 года** во всех рассмотренных отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, снизилась.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Начиная с четвертого квартала 2022 года **тренды** рассмотренных отраслей демонстрируют преимущественно положительную динамику.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Латинская Америка

Актуальные угрозы

-1 место-

Скрипты и фишинговые страницы
6,69%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру

-2 место-

Интернет-ресурсы из списка запрещенных
5,54%

▼ снижение во II кв. 2024 г.

-3 место-

Шпионские программы
4,77%

▲ незначительный рост во II кв. 2024 г.
1,2x выше среднего по миру

Вредоносные документы
3,23%

▲ **1,1x** рост во II кв. 2024 г.
1,7x выше среднего по миру
2-е место в мире

Веб-майнеры
0,68%

▲ **1,2x** рост во II кв. 2024 г.
1,4x выше среднего по миру
3-е место в мире
1-е место в мире **по росту**

Программы-вымогатели
0,22%

▲**1,7x** рост во II кв. 2024 г.
1,2x выше среднего по миру
3-е место в мире
1-е место в мире **по росту**

Интернет
как источник угроз
10,56%

▼ снижение во II кв. 2024 г.

Почтовые клиенты
как источник угроз
4,79%

▼ снижение во II кв. 2024 г.
1,6x выше среднего по миру
3-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Латинская Америка занимает **седьмое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. В регионе наблюдается нисходящий тренд. В целом этот показатель находится немного ниже среднемирового значения, за исключением первой половины 2022 года.

Сравнительный анализ

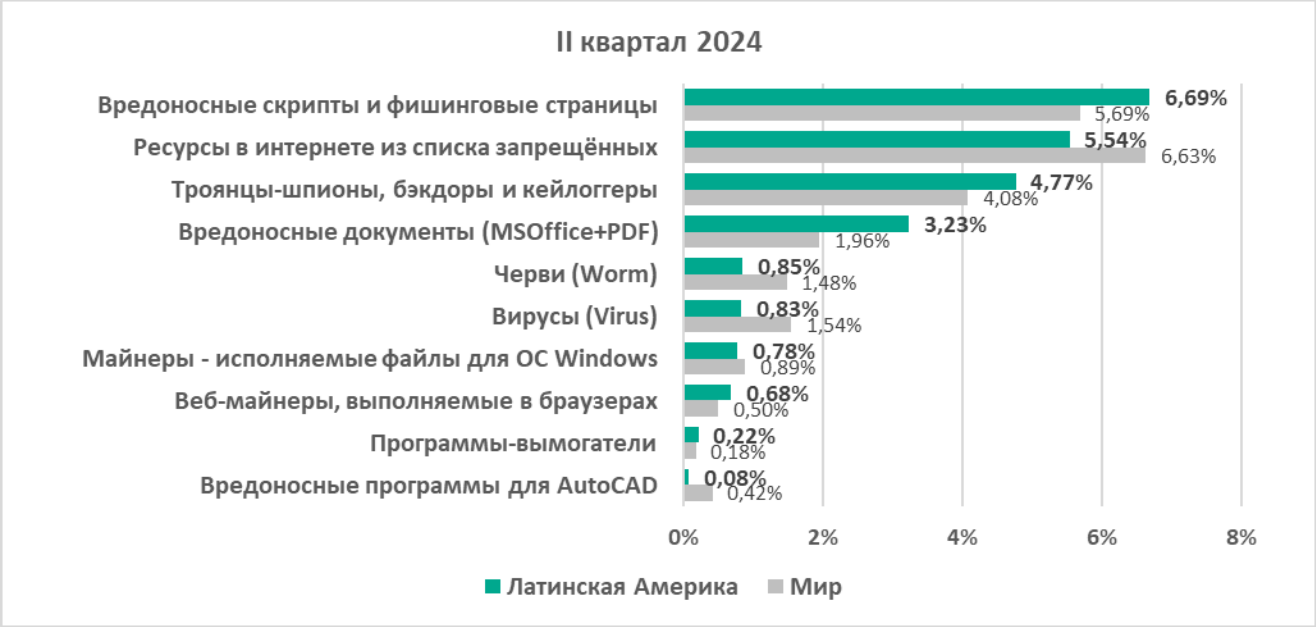
- Латинская Америка находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - второе место — вредоносные документы;
  - третье место — веб-майнеры, программы-вымогатели, угрозы из почтовых клиентов.

Категории угроз

По сравнению с мировыми показателями, в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- вредоносные документы — в 1,7 раза;
- веб-майнеры — в 1,4 раза;
- вредоносные скрипты и фишинговые страницы — в 1,2 раза;
- шпионские программы — в 1,2 раза;
- программы-вымогатели — в 1,2 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



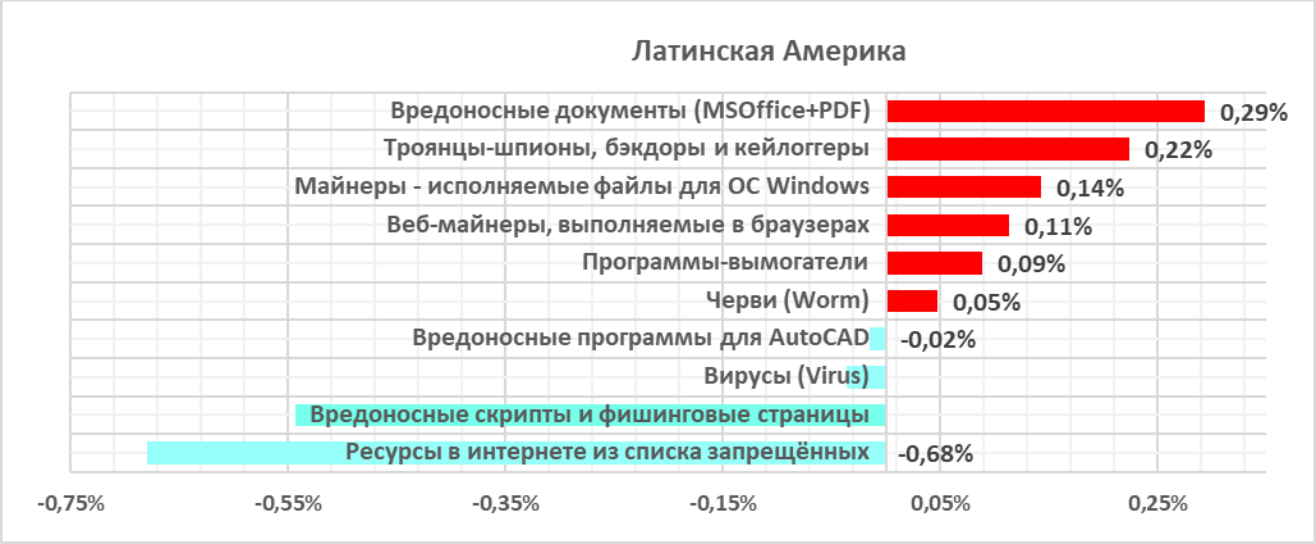
Источники угроз

Латинская Америка находится на **третьем месте в мировом рейтинге** по доле компьютеров АСУ, на которых заблокированы угрозы из **почтовых клиентов**, с превышением среднемирового значения в 1,6 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

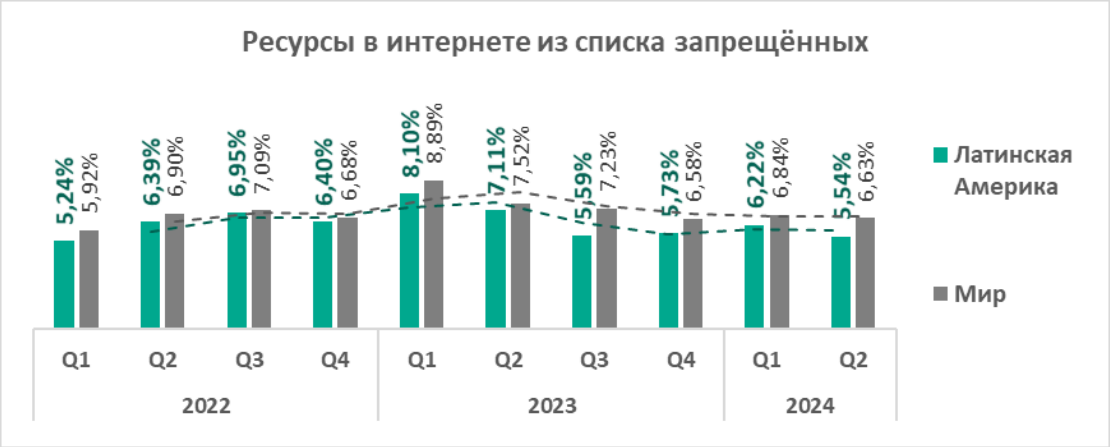
Изменения за квартал и тренды

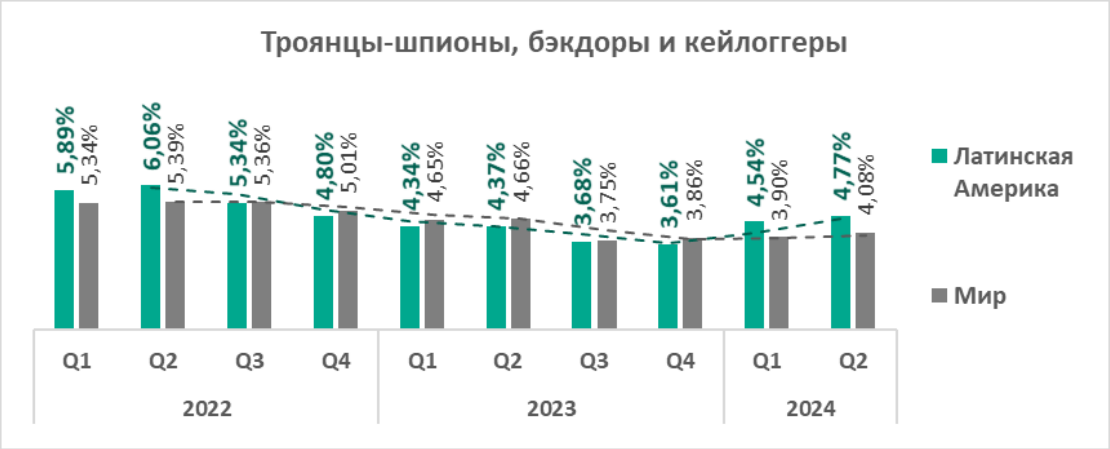
Категории угроз



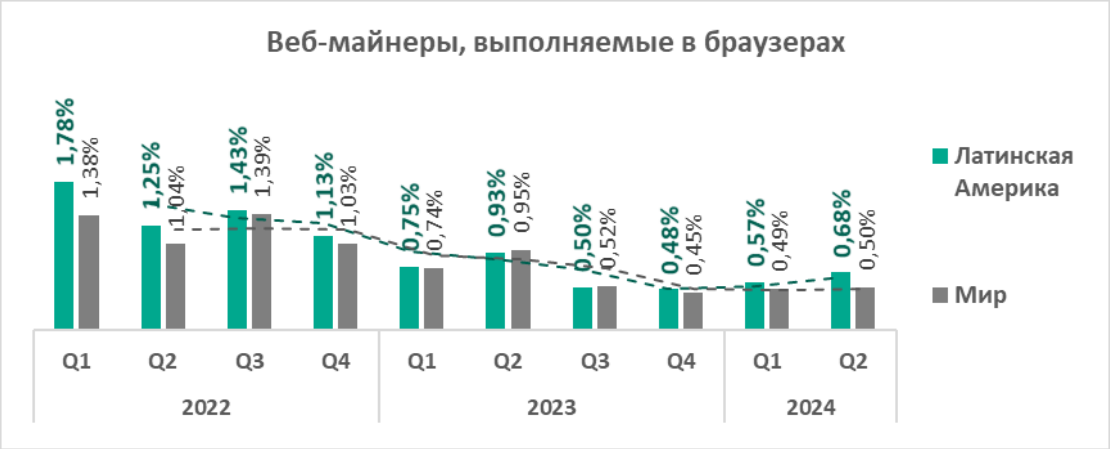
- **Наибольший рост за квартал** отмечен в доле компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
  - программы-вымогатели — в 1,7 раза;
  - веб-майнеры — в 1,2 раза;
  - майнеры — исполняемые файлы для ОС Windows — в 1,2 раза.
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

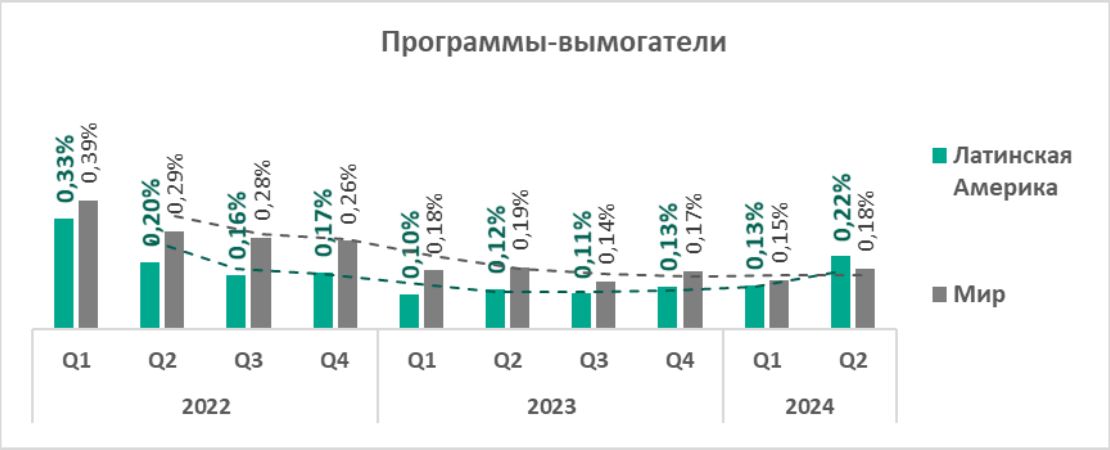
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Латинской Америке за 2,5 года. На протяжении всего этого времени **вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе. В четвертом квартале 2023 года **шпионские программы** поднялись с четвертого места на третье и с тех пор сохраняют свою позицию.

Латинская Америка	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Вредоносные скрипты и фишинговые страницы (JS и HTML)	1	1	1	1	1	1	1	1	1	1
Ресурсы в интернете из списка запрещенных	3	2	2	2	2	2	2	2	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	4	3	4	4	4	4	3	3	3
Вредоносные документы (MSOffice + PDF)	4	3	4	3	3	3	3	4	4	4
Черви	7	6	6	6	5	5	5	5	6	5
Вирусы	8	8	8	7	6	6	6	6	5	6
Майнеры — исполняемые файлы для ОС Windows	5	5	7	8	8	8	8	7	7	7
Веб-майнеры, выполняемые в браузерах	6	7	5	5	7	7	7	8	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 **почтовых клиентов** по доле компьютеров АСУ, на которых они были заблокированы, демонстрируют нисходящую динамику, которая соответствует общемировому тренду, при этом показатель существенно превышает среднемировое значение.

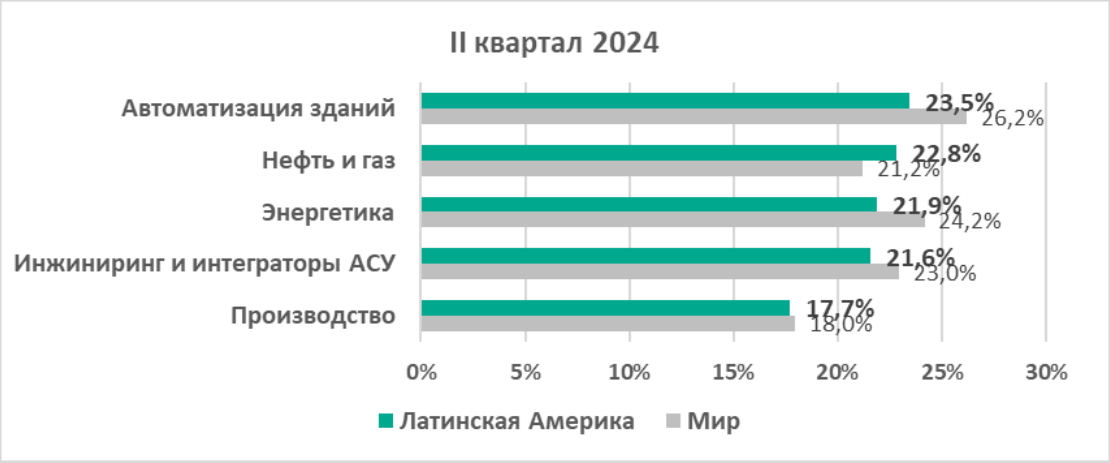
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- В целом, все основные источники угроз демонстрируют нисходящие тренды.

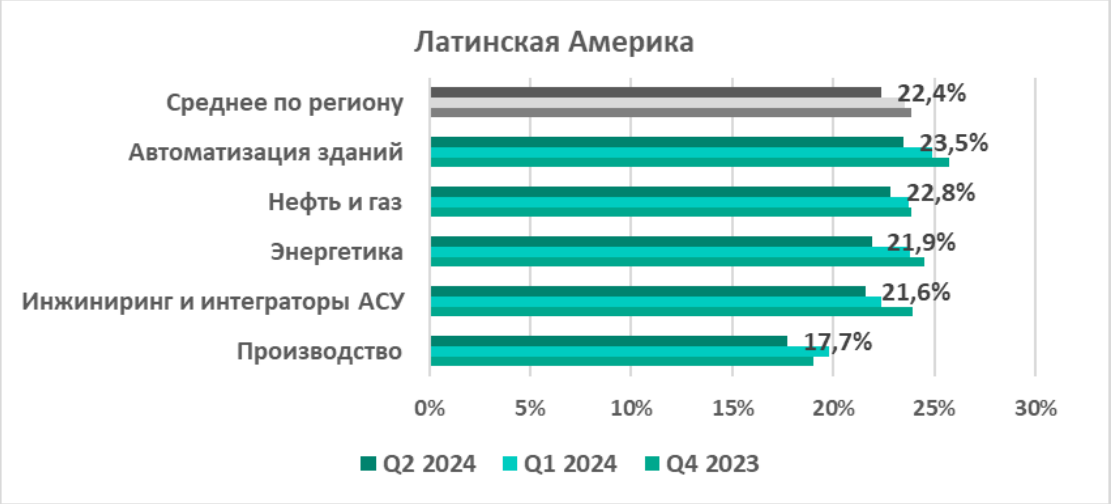
Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** в регионе из рассмотренных в отчете является **автоматизация зданий.**
- В нефтегазовой отрасли доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает **среднемировое значение** в 1,1 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

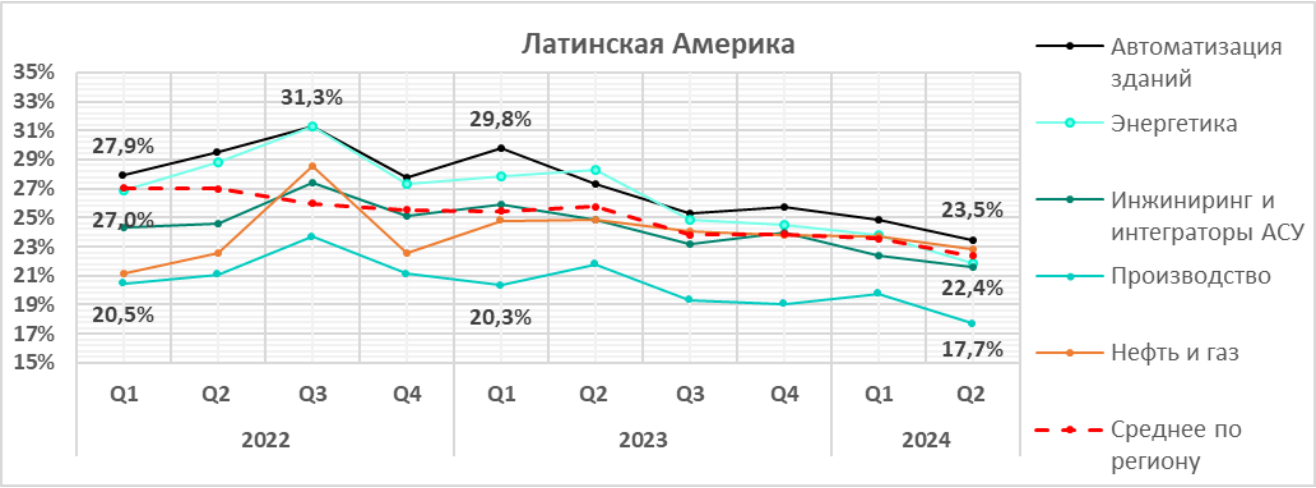


- Во **втором квартале 2024 года** во всех рассмотренных отраслях региона отмечено снижение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Рассмотренные отрасли демонстрируют позитивную динамику долгосрочных **трендов** начиная с первого квартала 2023 года.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Южная Азия

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
6,33%

▼ снижение во II кв. 2024 г.

-2 место-

Скрипты и фишинговые страницы
5,57%

▼ снижение во II кв. 2024 г.

-3 место-

Шпионские программы
2,98%

▲ незначительный рост во II кв. 2024 г.

Черви
1,74%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру

Вирусы
1,69%

▼ снижение во II кв. 2024 г.
1,1x выше среднего по миру

Программы-вымогатели
0,22%

▼ снижение во II кв. 2024 г.
1,6x выше среднего по миру
3-е место в мире

Интернет
как источник угроз
10,94%

▼ снижение во II кв. 2024 г.

Съемные носители
как источник угроз
1,94%

▼ снижение во II кв. 2024 г.
2,1x выше среднего по миру
2-е место в мире

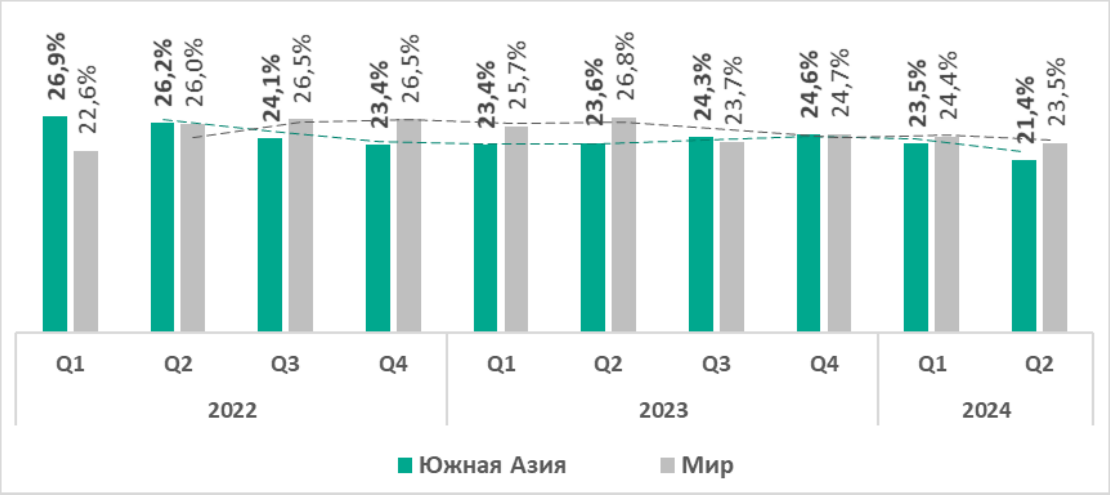
Сетевые папки
как источник угроз
0,21%

▼ снижение во II кв. 2024 г.
1,6x выше среднего по миру
3-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Южная Азия занимает **восьмое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Регион демонстрирует плавный нисходящий тренд с некоторыми колебаниями. Показатель здесь ниже среднемирового значения начиная с четвертого квартала 2023 года.



Сравнительный анализ

- Южная Азия находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
  - второе место — угрозы на съемных носителях;
  - третье место — программы-вымогатели, угрозы в сетевых папках.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории угроз

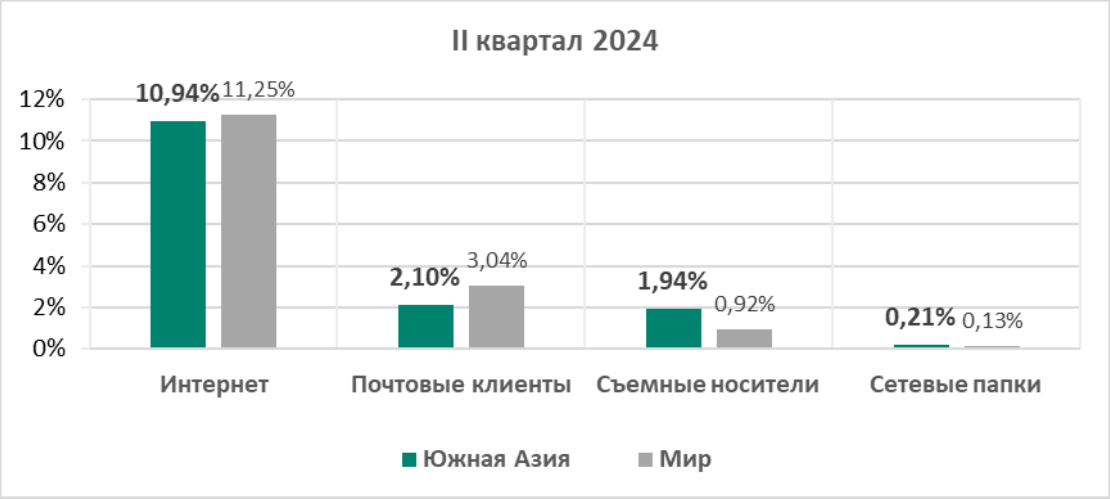
- **По сравнению со среднемировыми показателями**, в регионе заметно выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
  - программы-вымогатели — в 1,2 раза;
  - черви — в 1,2 раза.
    Черви находятся на четвертом месте в региональном рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых они были заблокированы (в мире — на шестом месте);
  - вирусы — в 1,1 раза.

Источники угроз

Южная Азия занимает **второе место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы **на съемных носителях**, с превышением среднемирового показателя в 2,1 раза.

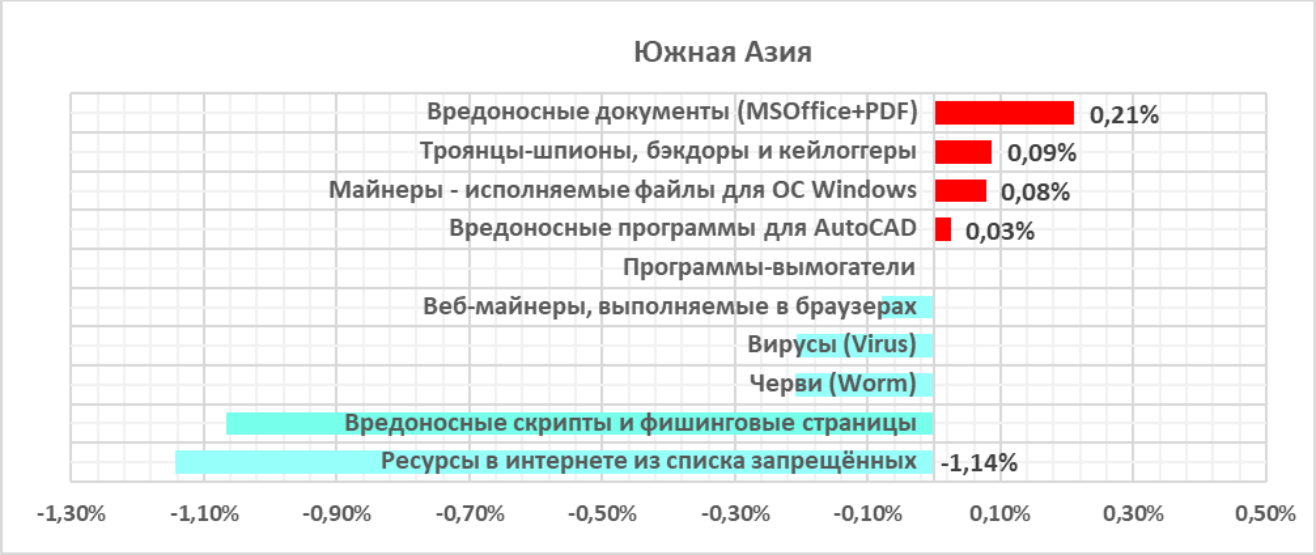
Кроме того, регион находится **на третьем месте** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках**, с показателем, превышающим среднемировое значение в 1,6 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Изменения за квартал и тренды

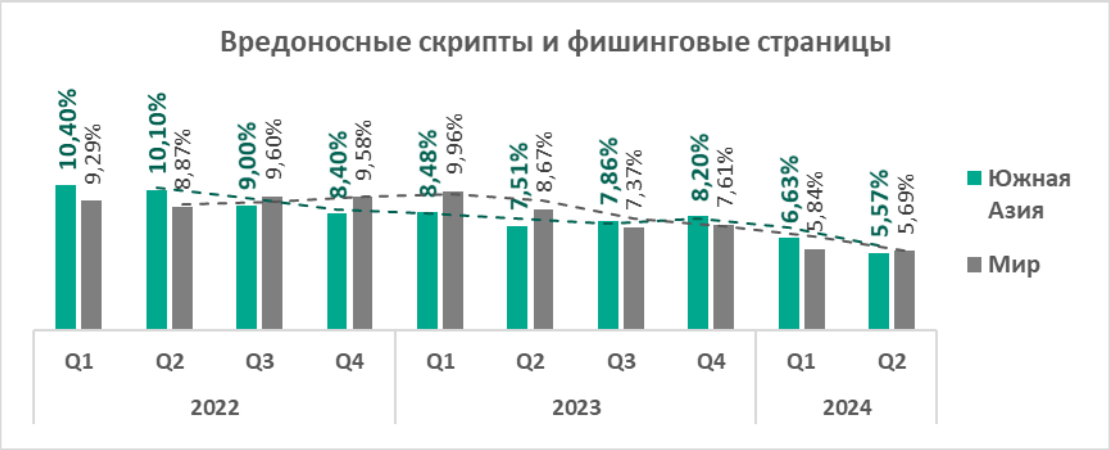
Категории угроз

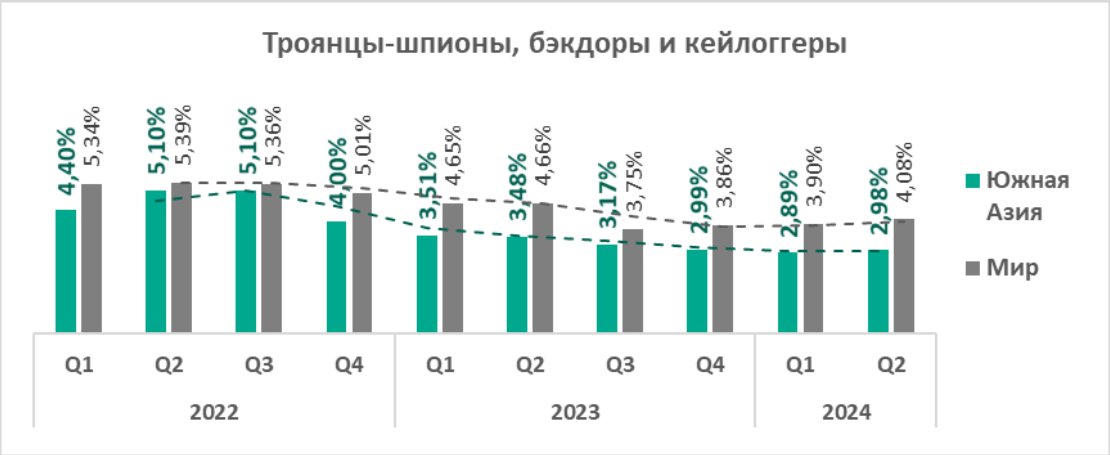


- **Наибольший рост за квартал** отмечен в доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
  - вредоносные документы — в 1,2 раза;
  - майнеры — исполняемые файлы для ОС Windows — в 1,1 раза;
  - вредоносные программы для AutoCAD — в 1,1 раза.

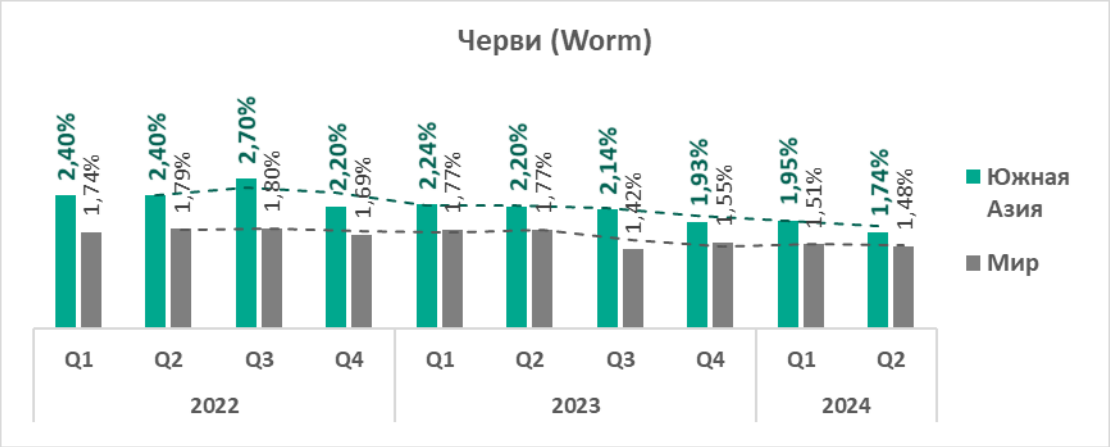
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

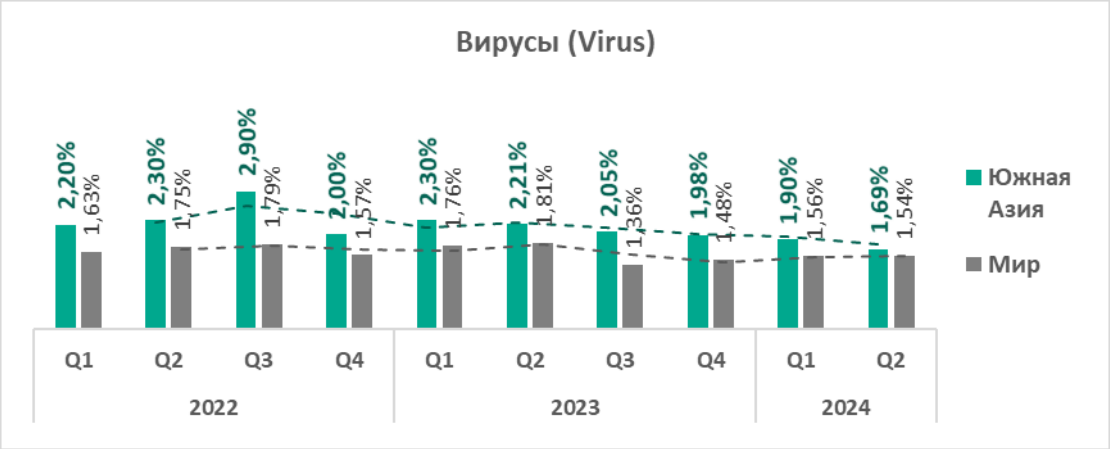
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

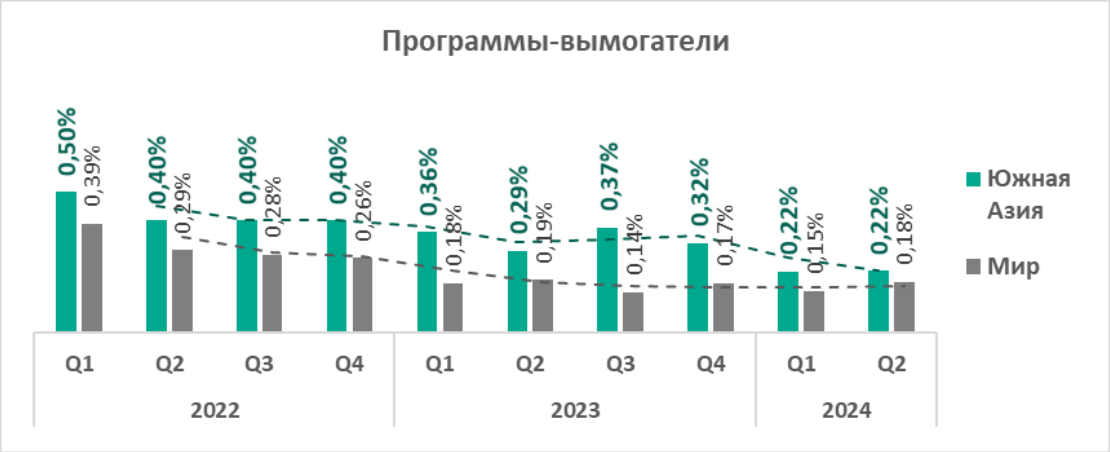




© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»







- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Азии за 2,5 года. С первого квартала 2023 года, за исключением четвертого квартала того же года, **ресурсы в интернете из списка запрещенных** являются здесь ведущей категорией угроз. Эта категория сместила тогда категорию **вредоносные скрипты и фишинговые страницы** на второе место. **Вирусы** и **черви** стабильно удерживают

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

высокие места, как правило, меняясь местами друг с другом на четвертой и пятой позициях.

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

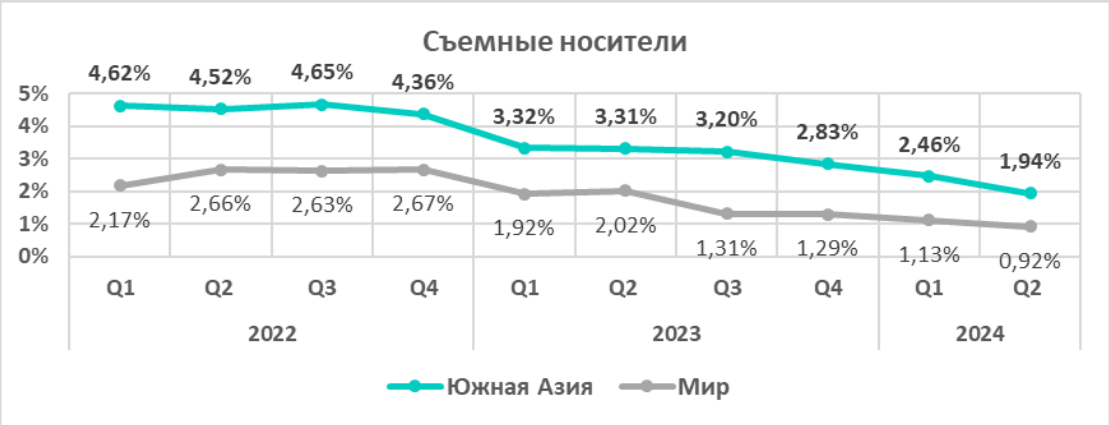
Источники угроз

Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, выросла в 1,1 раза по сравнению с предыдущим кварталом и таким образом поднялась на второе место в региональном рейтинге угроз (в первом квартале 2024 года она находилась на третьем).

С первого квартала 2022 года угрозы на **съемных носителях** в Южной Азии стабильно занимают второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников. Однако во втором квартале 2024 года уровень этой угрозы снизился, уступив место угрозам, распространяемым через почтовые клиенты.

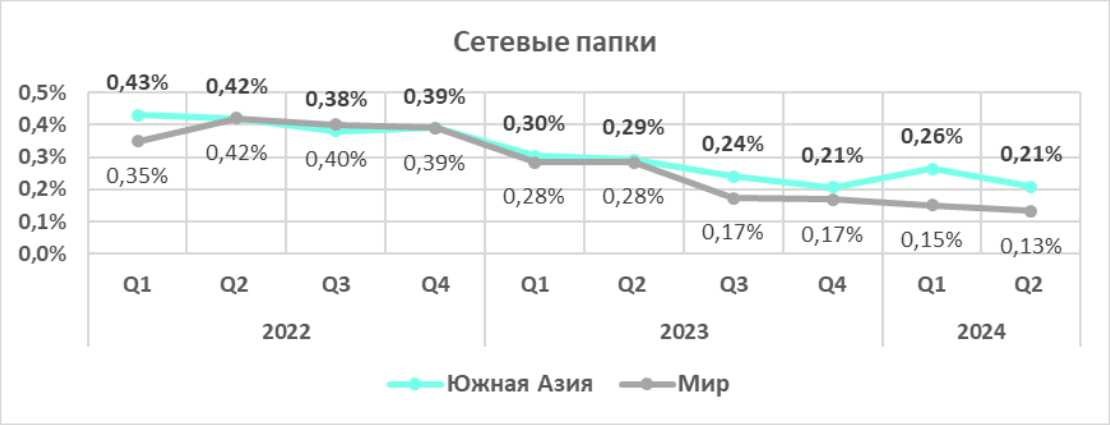
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

По сравнению с данными по миру, доля компьютеров АСУ, на которых в Южной Азии были заблокированы угрозы на **съемных носителях**, меняется в фарватере мирового тренда, хотя при этом существенно превышает среднемировое значение. Однако во втором квартале 2024 года разрыв между региональным и среднемировым показателями был минимальным со второго квартала 2022 года.



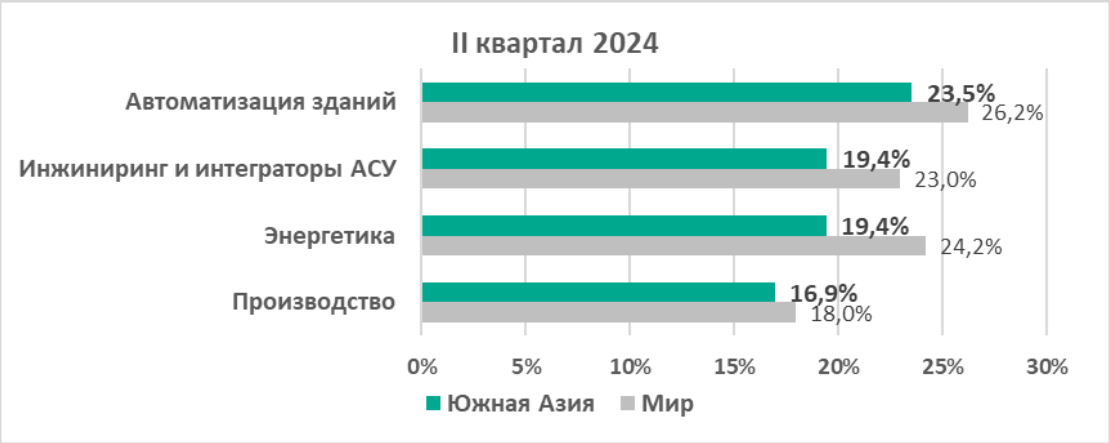
Динамика изменения доли компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках**, соответствует глобальному тренду. Только в третьем квартале 2023 года региональный тренд отклонился от мирового, когда показатель заметно превысил среднемировое значение.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



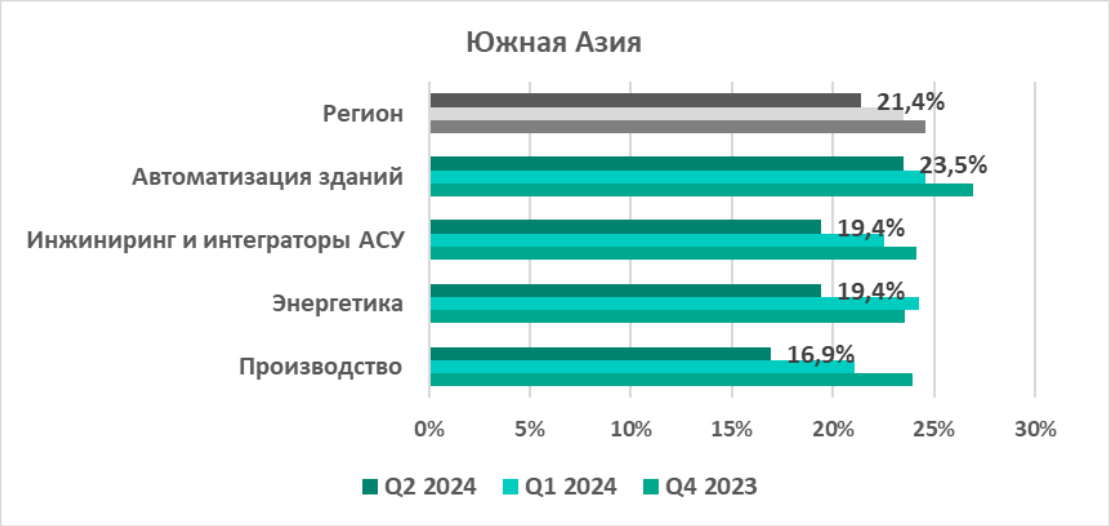
Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий.**
- **По сравнению с данными по миру**, во всех рассматриваемых отраслях доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, оказалась ниже соответствующих среднемировых значений.

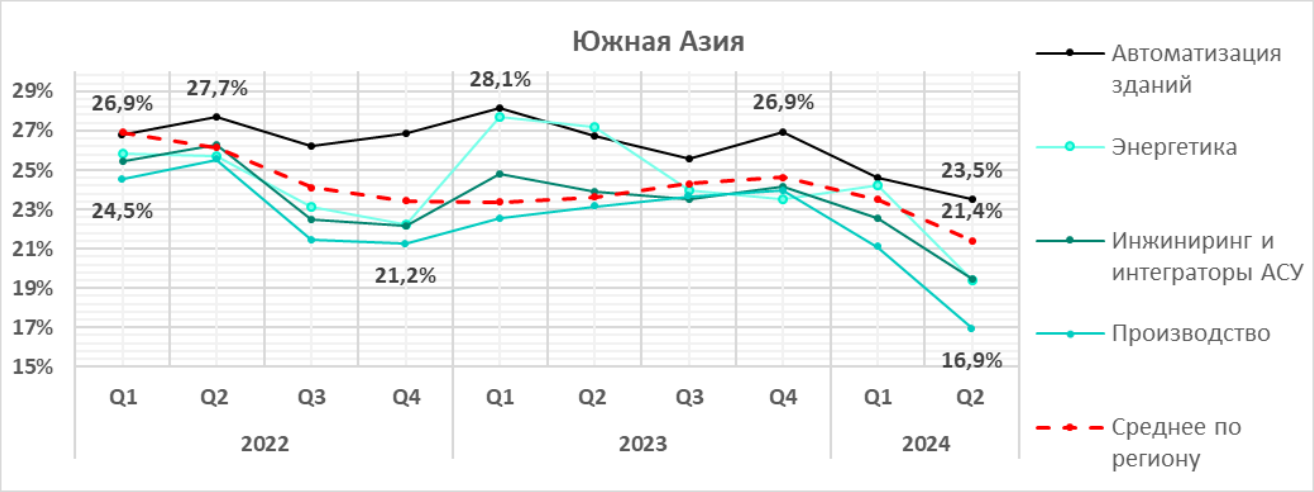


- Во **втором квартале 2024 года** во всех рассмотренных отраслях региона отмечено снижение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Рассмотренные отрасли в основном показывают положительную динамику долгосрочных **трендов** начиная с первого квартала 2024 года.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Восточная Азия

Актуальные угрозы

-1 место-

Шпионские программы
4,15%

▲ **1,1x** рост во II кв. 2024 г.
Незначительно выше среднего по миру

-2 место-

Скрипты и фишинговые страницы
3,49%

▲ **1,2x** рост во II кв. 2024 г.
2-е место в мире **по росту**

-3 место-

Интернет-ресурсы из списка запрещенных
3,47%

▼ снижение во II кв. 2024 г.

Вирусы
2,95%

▲ незначительный рост во II кв. 2024 г.
1,9x выше среднего по миру
3-е место в мире
3-е место в мире **по росту**

Черви
1,80%

▲ **1,1x** рост во II кв. 2024 г.
1,2x выше среднего по миру
2-е место в мире **по росту**

Вредоносное ПО для AutoCAD
1,57%

▲ **1,1x** рост во II кв. 2024 г.
1,6x выше среднего по миру
3-е место в мире
2-е место в мире **по росту**

Вредоносные документы
1,62%

▲ **1,2x** рост во II кв. 2024 г.

Программы-вымогатели
0,18%

▲ **1,3x** рост во II кв. 2024 г.

Интернет
как источник угроз
6,46%

▼ снижение во II кв. 2024 г.

Съемные носители
как источник угроз
1,54%

▲ незначительный рост во II кв. 2024 г.
1,7x выше среднего по миру
1-е место в мире **по росту**

Сетевые папки
как источник угроз
0,35%

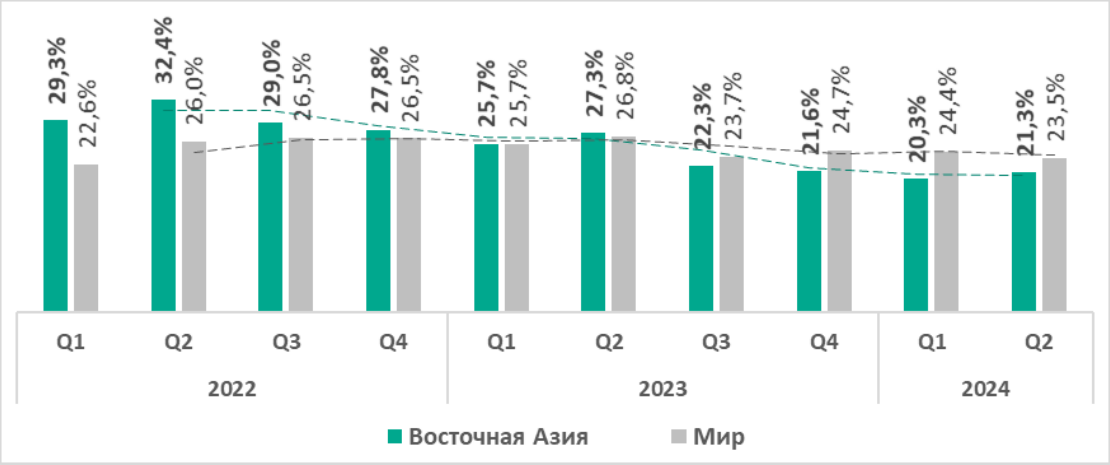
▲ **1,1x** рост во II кв. 2024 г.
2,6x выше среднего по миру
1-е место в мире
1-е место в мире **по росту**

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Восточная Азия занимает **девятое место** в мировом рейтинге по доле компьютеров АСУ, на которых заблокированы вредоносные объекты. Это один из четырех регионов, где данный показатель вырос.

Восточная Азия демонстрирует плавный нисходящий колебательный тренд. Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, здесь ниже среднемирового значения начиная с третьего квартала 2023 года.

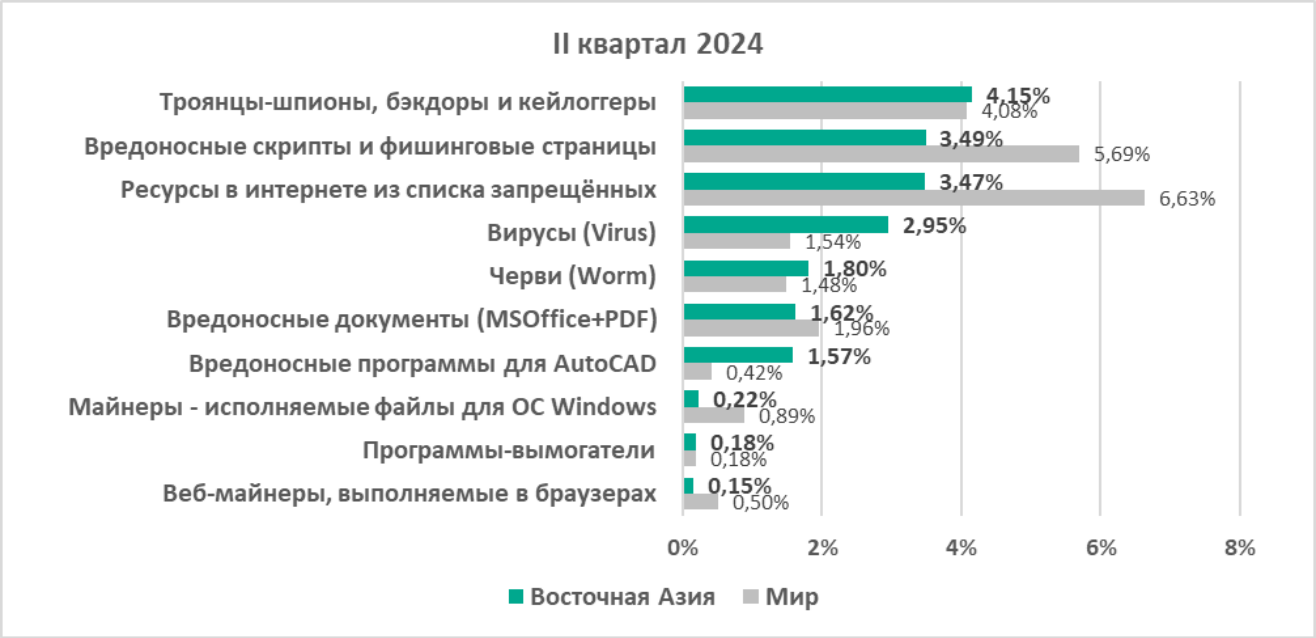


Сравнительный анализ

- Восточная Азия находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие категории угроз:
  - первое место — угрозы в сетевых папках;
  - второе место — вредоносные программы для AutoCAD;
  - третье место — вирусы.
- Это **единственный регион, в котором шпионские программы возглавили рейтинг категорий вредоносного ПО** доле компьютеров АСУ, на которых они были заблокированы.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории угроз



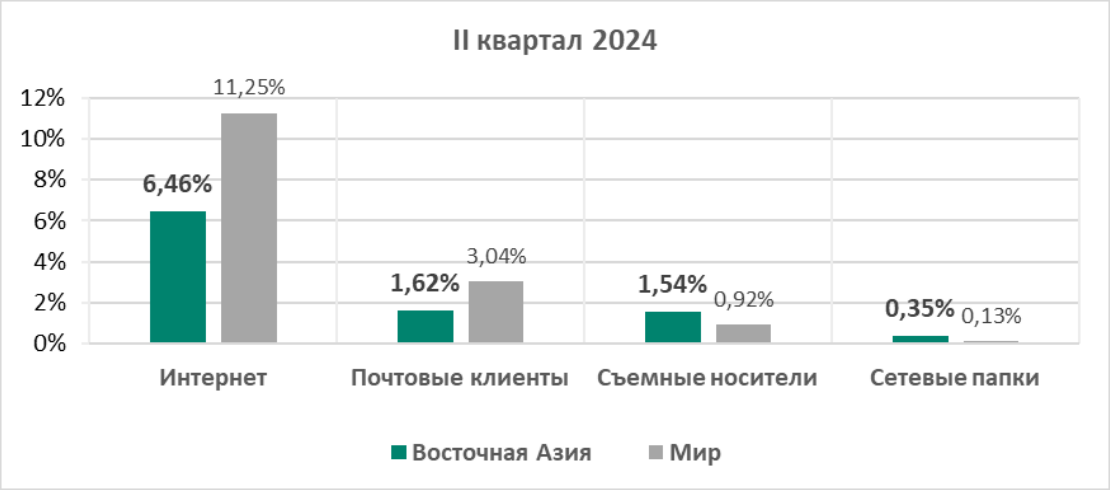
- **По сравнению со среднемировыми показателями**, в регионе заметно выше доля компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
    - вредоносные программы для AutoCAD — в 3,7раза;
    - вирусы — в 1,9 раза;
    - черви — в 1,2 раза.

Источники угроз

Восточная Азия занимает **первое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках**, с показателем, превышающим среднемировой в 2,7раза.

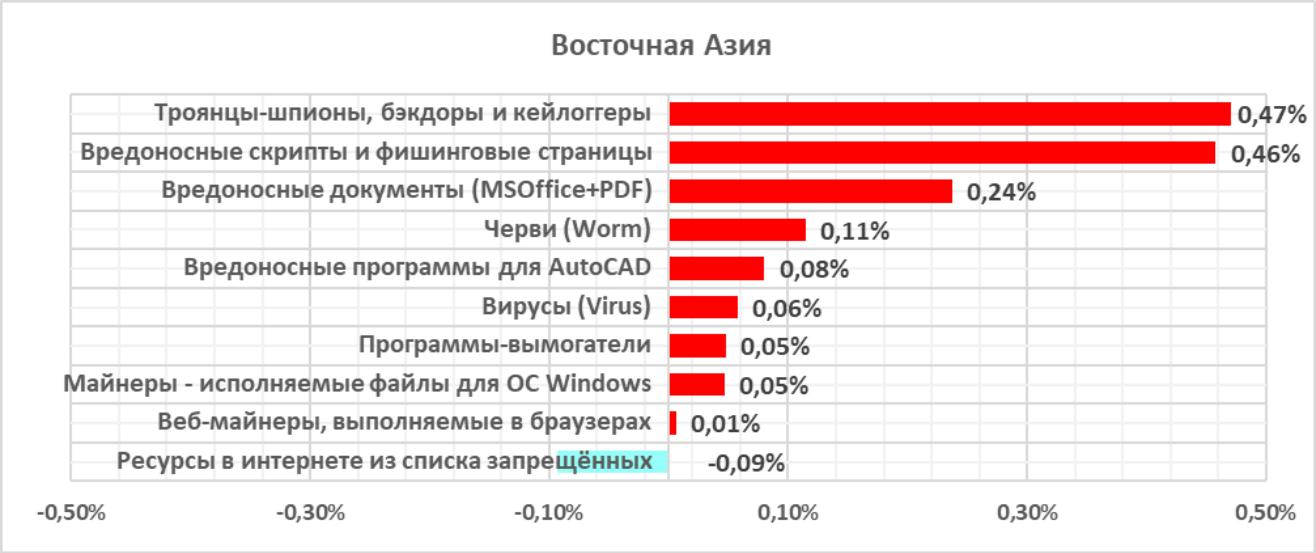
Доля компьютеров АСУ, на которых были заблокированы угрозы на **съемных носителях**, здесь **в 1,7 раза выше**, чем в среднем по миру.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Изменения за квартал и тренды

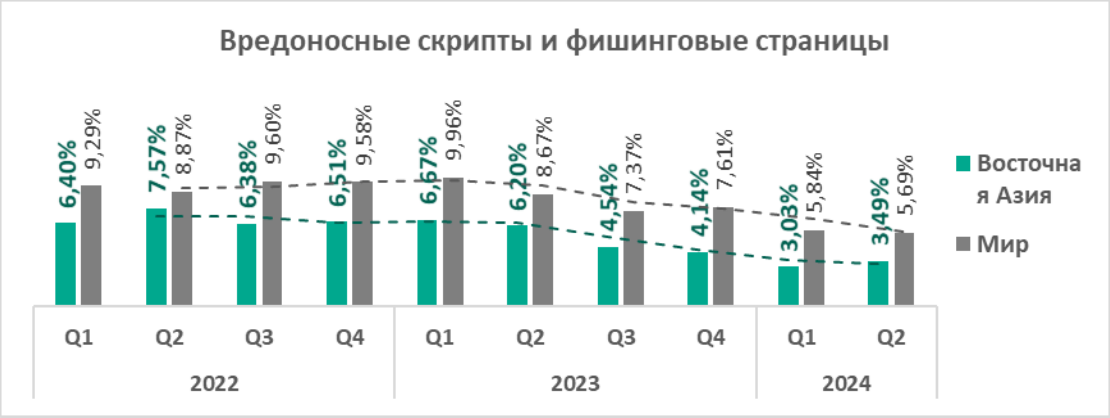
Категории угроз



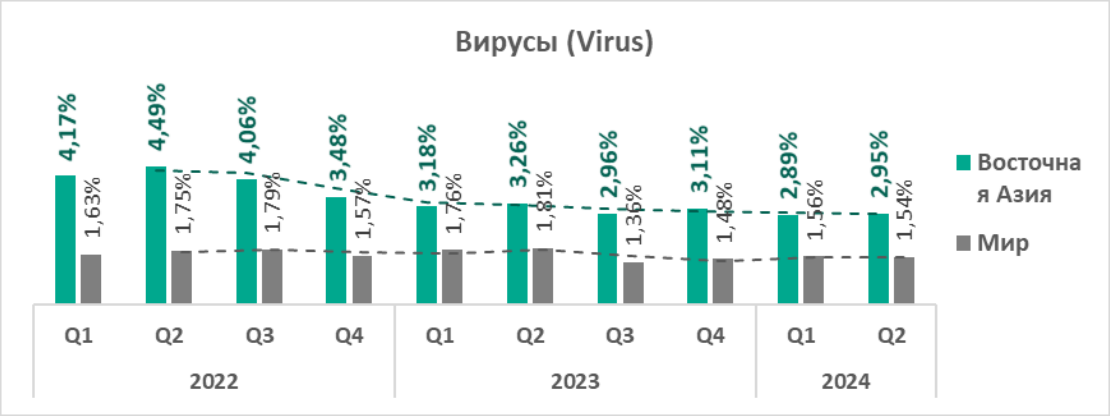
- Во втором квартале 2024 года отмечен рост уровня всех категорий угроз, за исключением ресурсов в интернете из списка запрещенных.
- **Наибольший рост за квартал** зафиксирован в доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
    - программы-вымогатели — в 1,3 раза;
    - майнеры — исполняемые файлы для ОС Windows — в 1,3 раза;
    - вредоносные документы — в 1,2 раза;
    - вредоносные скрипты и фишинговые страницы — в 1,2 раза.

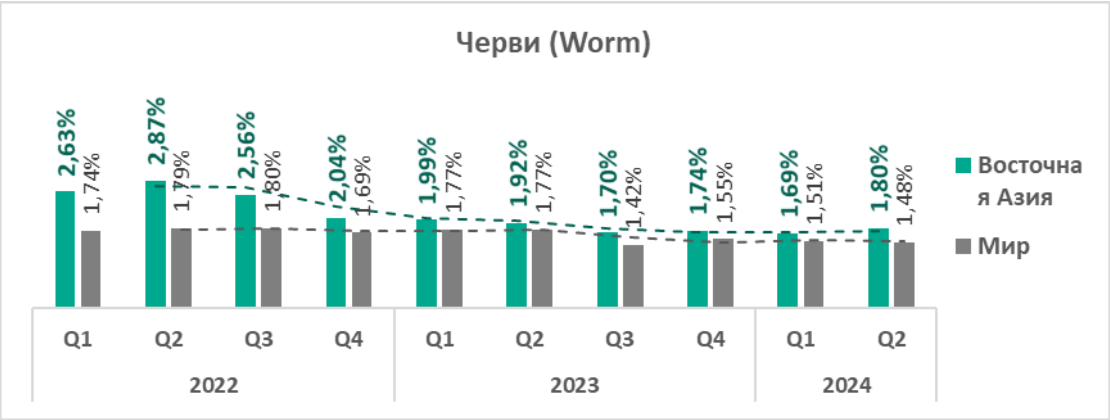
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

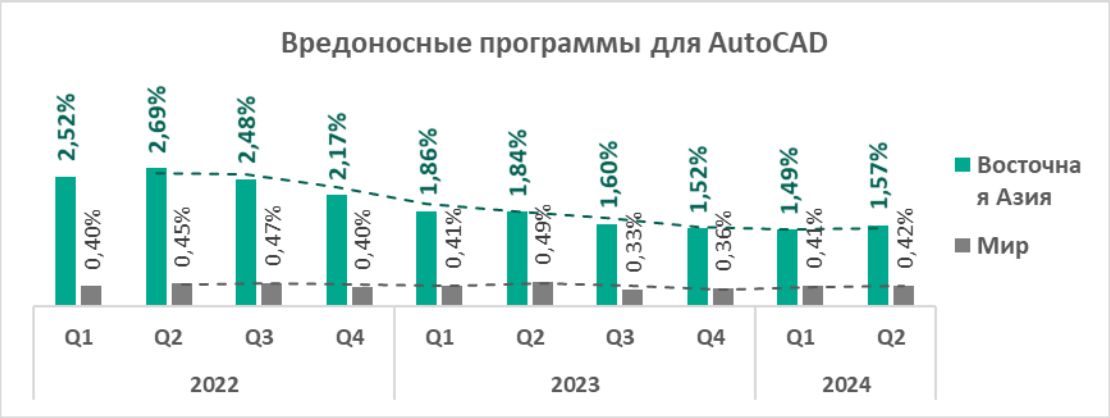
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.



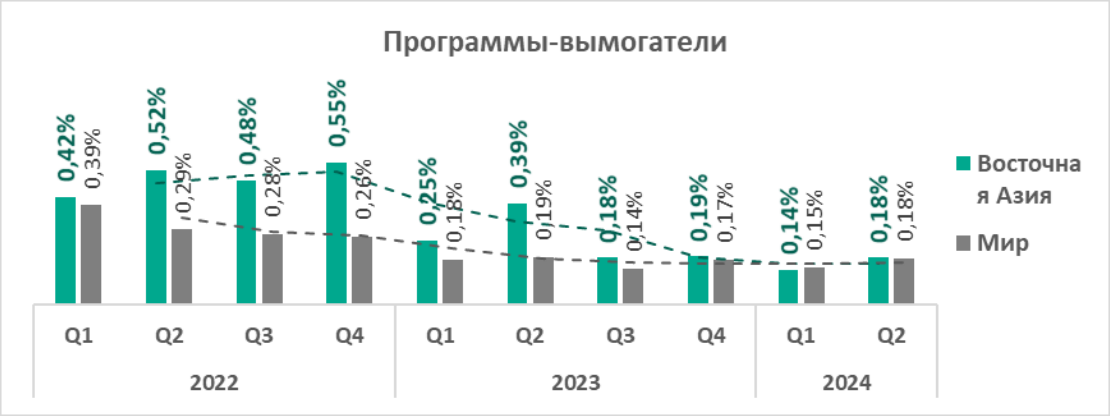
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»







© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Азии за 2,5 года. **Шпионские программы** являются ведущей категорией угроз в регионе начиная с четвертого квартала 2023 года, когда они перепрыгнули с третьего места на первое, сместив **вредоносные скрипты и фишинговые страницы** на второе и третье места.

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

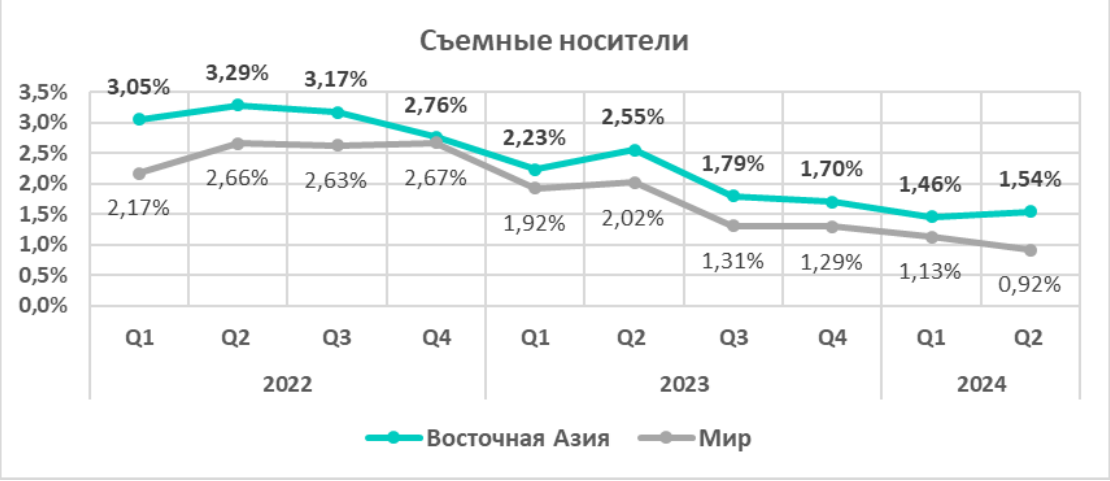
Источники угроз

- Угрозы в **сетевых папках**, заблокированные на компьютерах АСУ в Восточной Азии, в целом демонстрировали нисходящий тренд со второй половины 2022 года до первого квартала 2024 года, при этом их уровень оставался выше среднемирового значения. Хотя среднемировой показатель был относительно устойчивым и ниже регионального, разрыв

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

между ними постепенно сократился к первому кварталу 2024 года. Небольшой рост в Восточной Азии был замечен только во втором квартале 2024 года.

- Во втором квартале 2024 года в регионе отмечен рост угроз, распространяемых на **съемных носителях**, в отличие от среднемирового показателя.

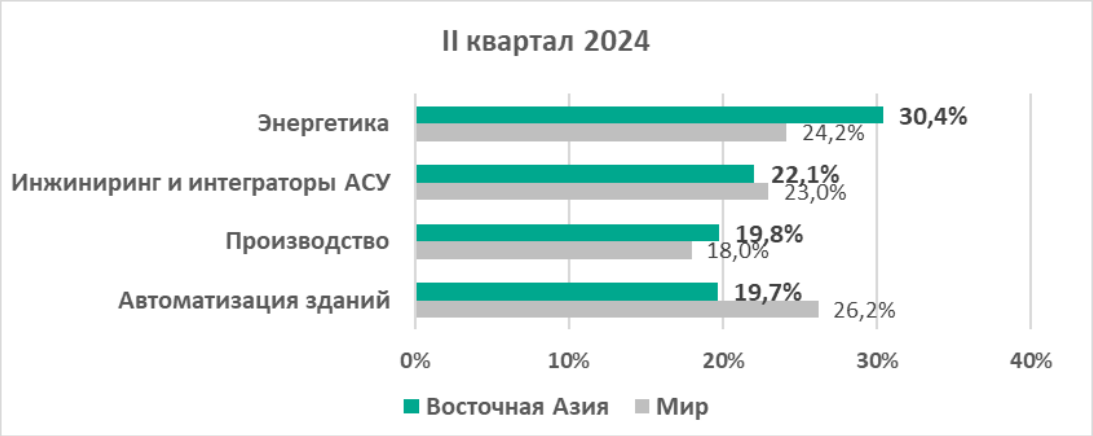


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- В целом, все основные источники угроз демонстрируют тенденцию к снижению.

Отрасли

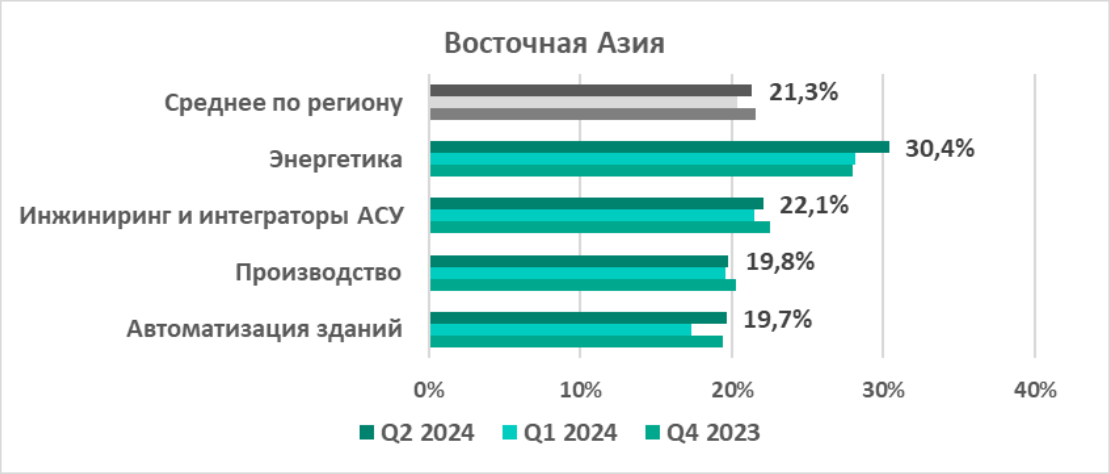
- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий**.
- По сравнению с соответствующими **среднемировыми значениями**, более высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:
  - энергетика — в 1,3 раза;
  - производство — в 1,1 раза.



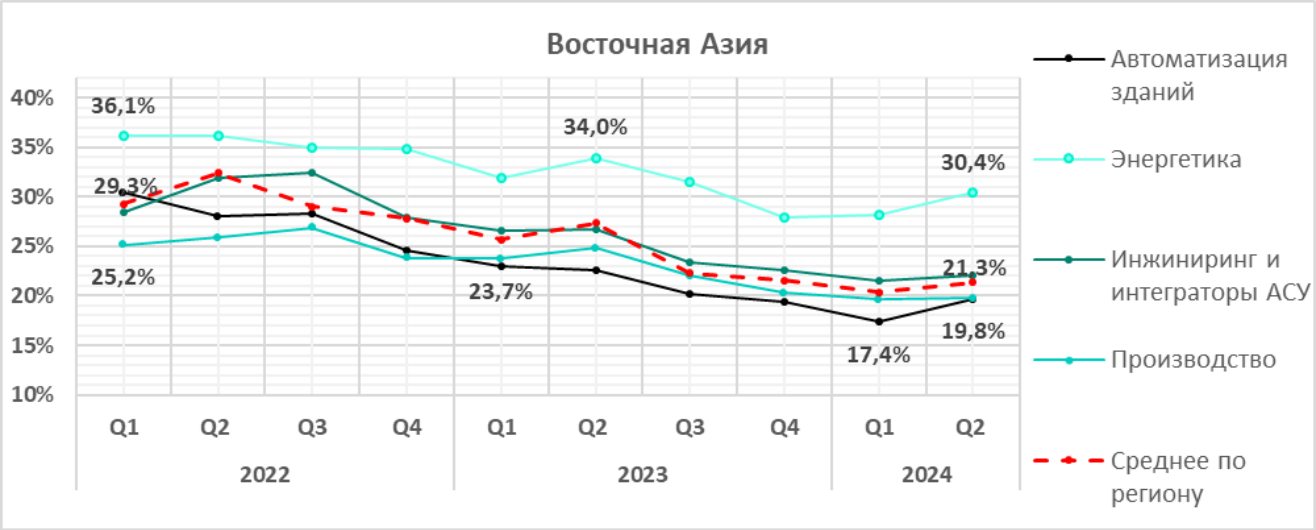
- Во **втором квартале 2024 года** во всех отраслях зафиксирован рост доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Значительное увеличение по сравнению с предыдущим кварталом отмечено в следующих отраслях:

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- автоматизация зданий — в 1,1 раза;
- энергетика — в 1,1 раза.



- В **энергетической** отрасли на протяжении всего периода наблюдений сохраняется самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, причем этот показатель значительно превышает среднемировое значение. В других отраслях, напротив, с 2022 года до первого квартала 2024 года прослеживался нисходящий тренд, который сменился ростом во втором квартале 2024 года.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Южная Европа

Актуальные угрозы

-1 место-

Скрипты и фишинговые страницы
7,46%

▲ **1,1x** рост во II кв. 2024 г.
1,3x выше среднего по миру
1-е место в мире
1-е **место** в мире **по росту**

-2 место-

Шпионские программы
6,21%

▲ **1,1x** рост во II кв. 2024 г.
1,5x выше среднего по миру
3-е место в мире
1-е место в мире **по росту**

-3 место-

Интернет-ресурсы из списка запрещенных
5,22%

▼ снижение во II кв. 2024 г.

Вредоносные документы
3,75%

▲ **1,2x** рост во II кв. 2024 г.
1,9x выше среднего по миру
1-е место в мире
3-е место в мире **по росту**

Программы-вымогатели
0,19%

▲ **1,6x** рост во II кв. 2024 г.
выше среднего по миру
2-е место в мире **по росту**

Интернет
как источник угроз
9,53%

▼ снижение во II кв. 2024 г.

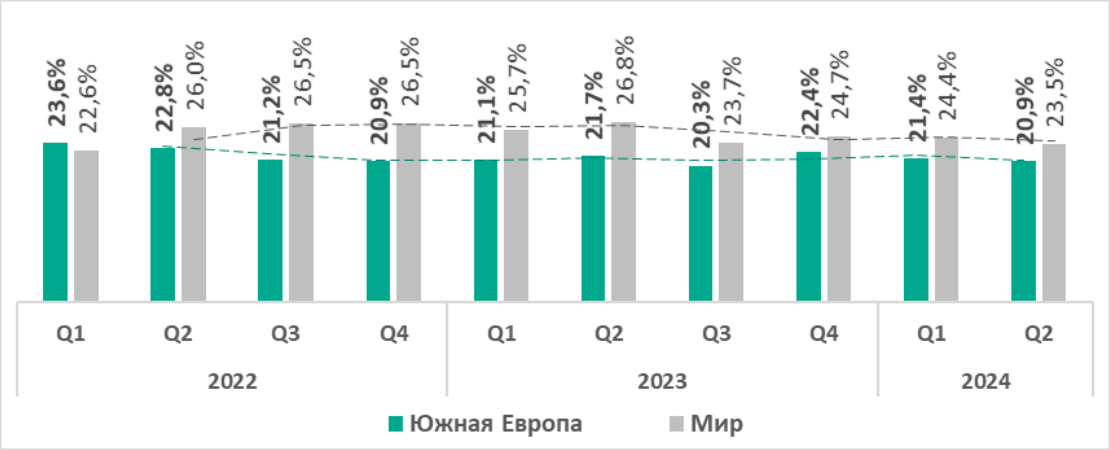
Почтовые клиенты
как источник угроз
7,06%

▲ незначительный рост во II кв. 2024 г.
2,3x выше среднего по миру
1-е место в мире

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

Южная Европа занимает **десятое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Этот показатель, как правило, ниже среднемирового значения.



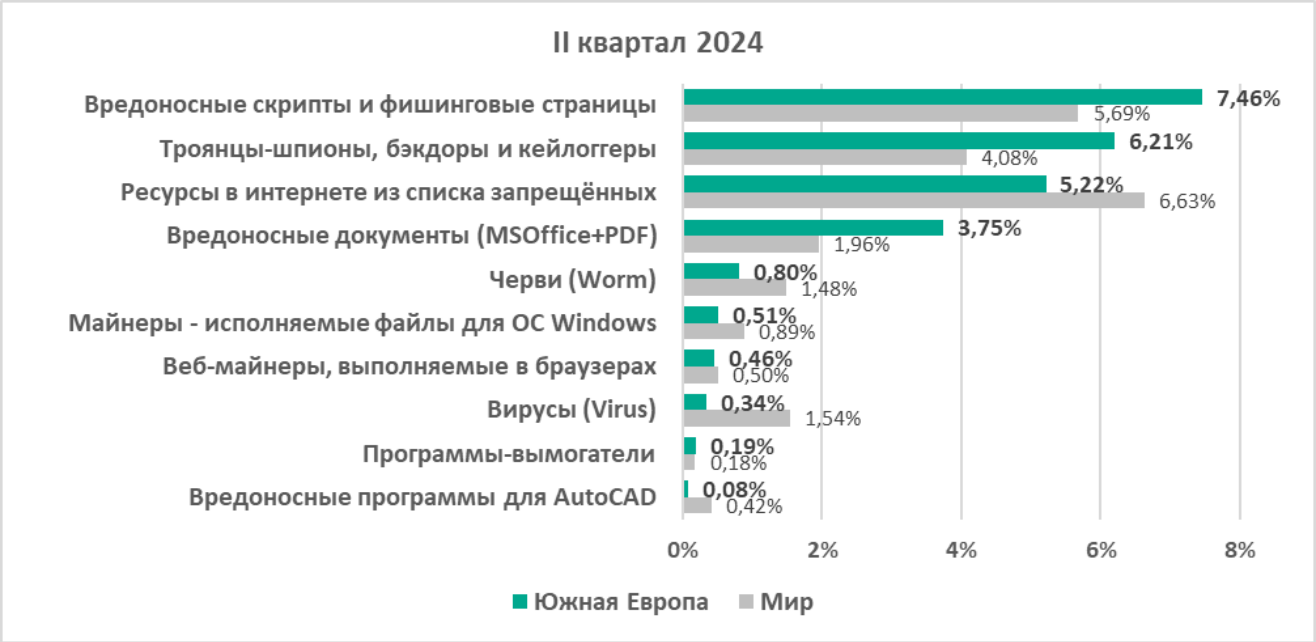
Сравнительный анализ

Южная Европа находится **в числе лидеров** среди регионов по доле компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

- первое место — угрозы из почтовых клиентов, вредоносные скрипты и фишинговые страницы, вредоносные документы;
- третье место — шпионские программы.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории угроз



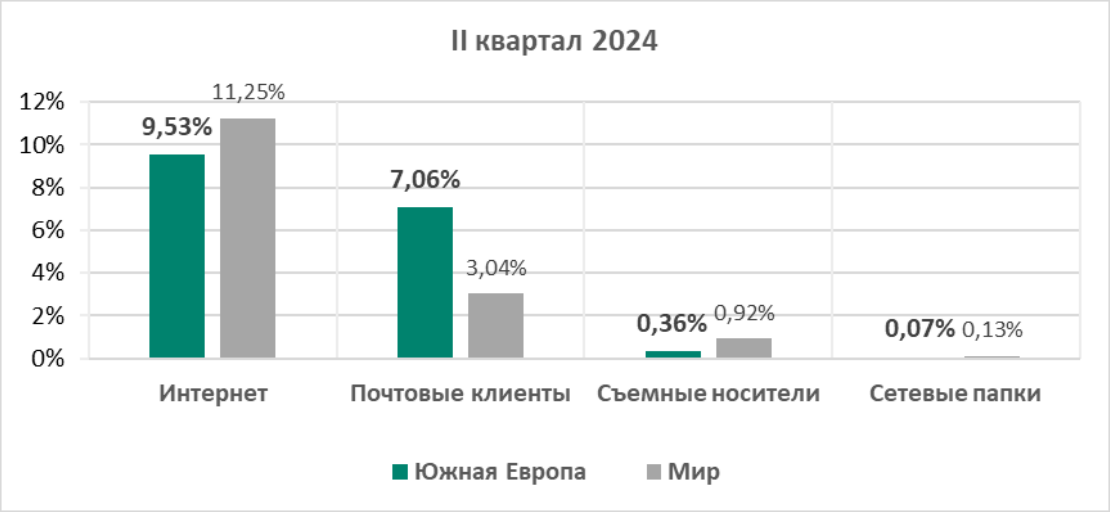
- **По сравнению со среднемировыми показателями**, в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
    - вредоносные документы — в 1,9 раза;
    - шпионские программы — в 1,5 раза;
    - вредоносные скрипты и фишинговые страницы — в 1,3 раза.

Источники угроз

Южная Европа находится **на первом месте в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, с показателем, превышающим среднемировое значение в 2,3 раза.

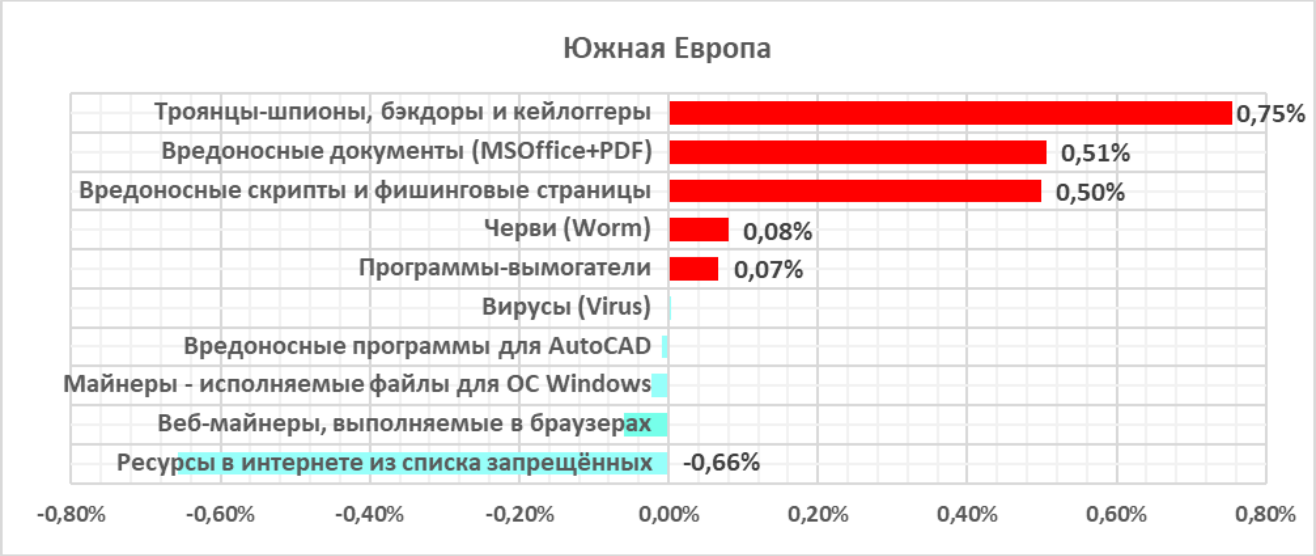
Показатели остальных источников угроз остаются ниже соответствующих среднемировых значений.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Изменения за квартал и тренды

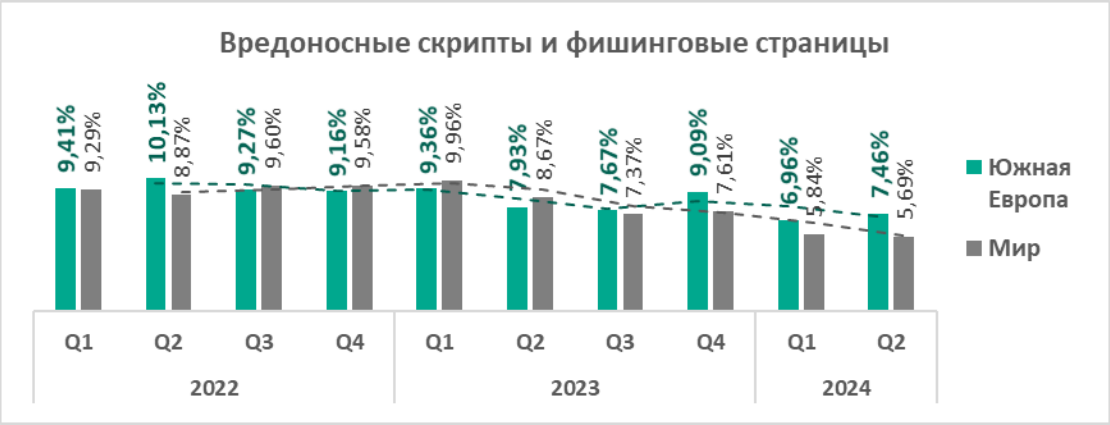
Категории угроз

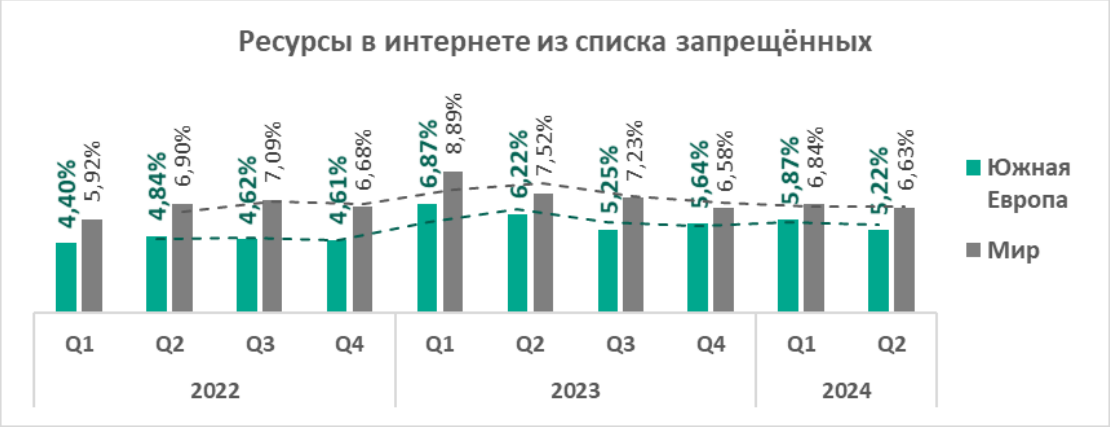


- **Наибольшее изменение за квартал** в абсолютных числах произошло в доле компьютеров АСУ, на которых были заблокированы шпионские программы. Что касается категорий угроз, показавших наибольший рост по сравнению с предыдущим кварталом, стоит выделить следующие:
  - программы-вымогатели — в 1,6 раза;
    вредоносные документы — в 1,2 раза.

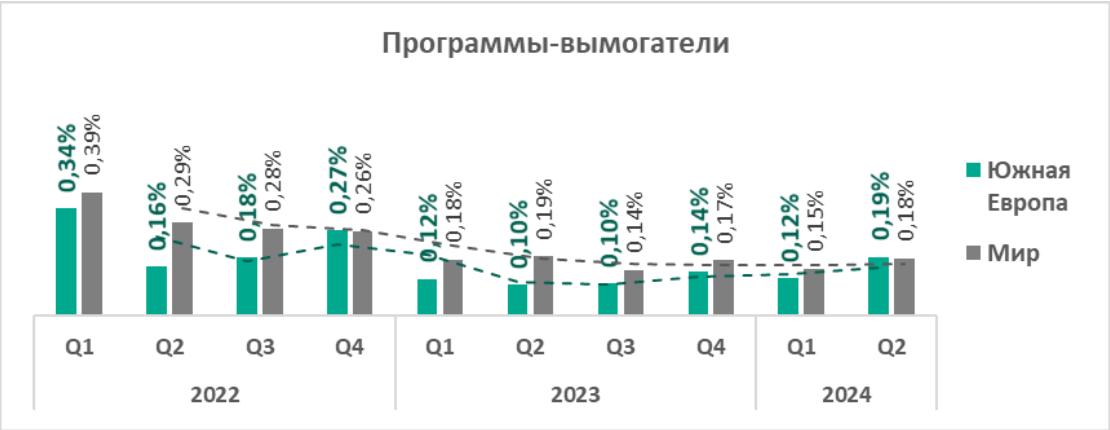
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



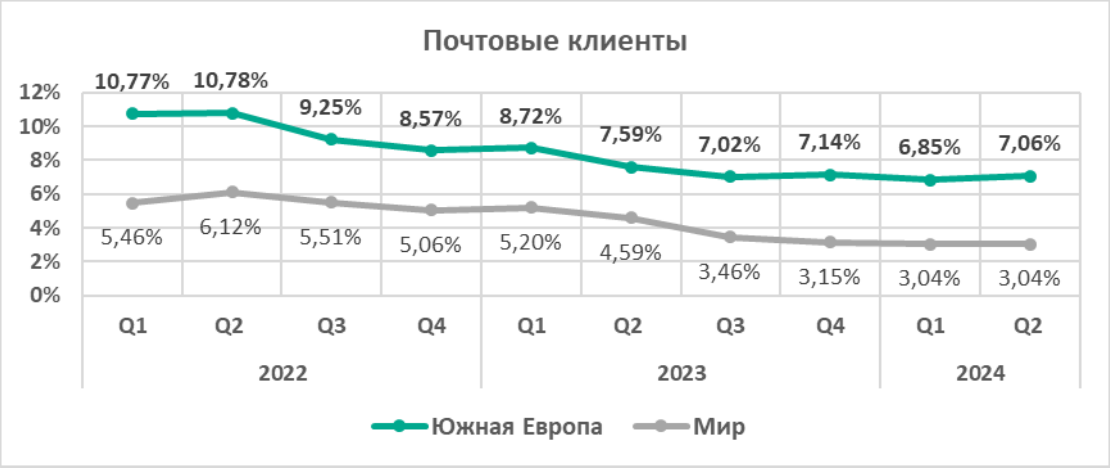
- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Европе за 2,5 года. **Вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе на протяжении всего периода наблюдения. Во втором квартале 2024 года **шпионские программы** поднялись с третьего места на второе. Эта категория угроз в течение всего срока попеременно занимает вторую и третью позиции в рейтинге.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

Источники угроз

Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов,** выросла по сравнению с предыдущим кварталом. Долгосрочные тренды для таких угроз — как региональные, так и глобальные — в основном совпадали вплоть до третьего квартала 2023 года. Однако в четвертом квартале 2023 года началось расхождение трендов.

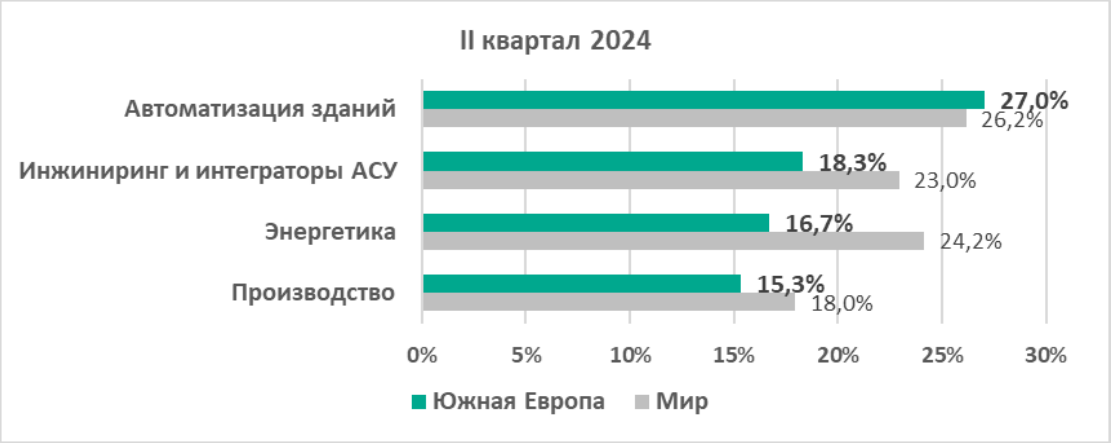


Региональные и глобальные долгосрочные тренды для угроз из интернета, начиная с третьего квартала 2023 года, в основном соответствуют друг другу. С первого квартала 2024 года отмечается снижение обоих трендов.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

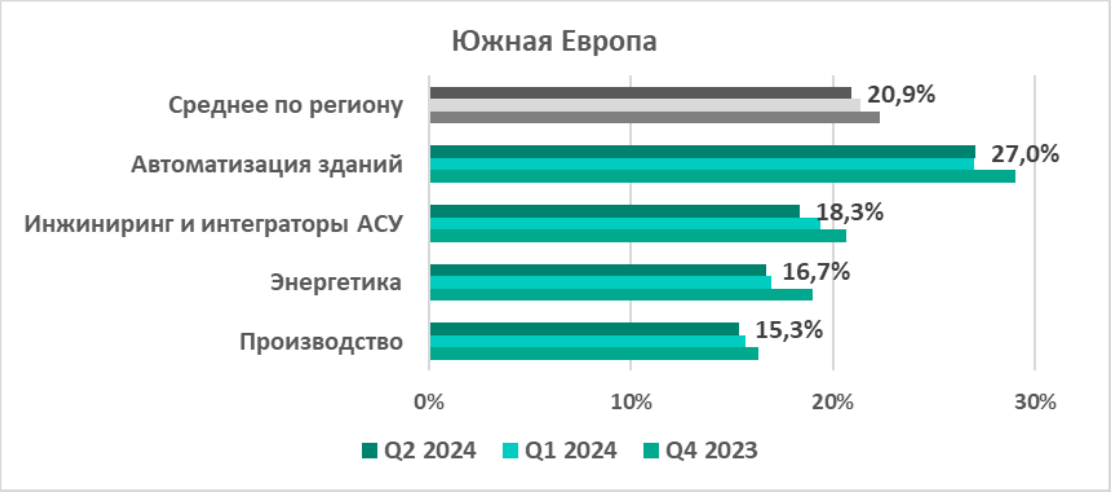
Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий.**
- По сравнению с соответствующими **среднемировыми показателями**, в этой отрасли зафиксирована наиболее высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты.

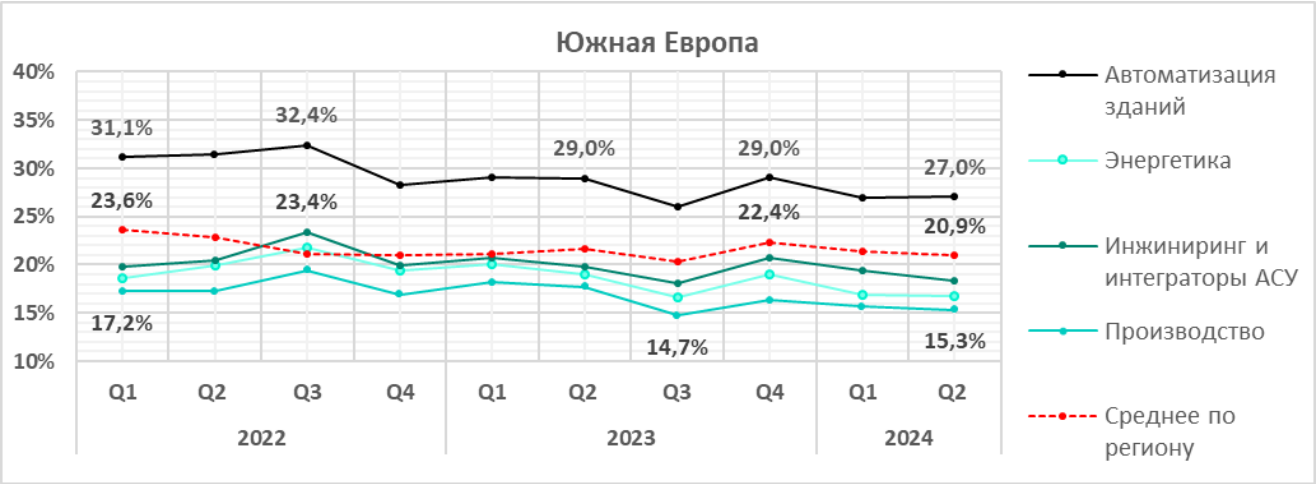


- Во **втором квартале 2024 года** автоматизация зданий является единственной отраслью из рассмотренных, где выросла доля компьютеров АСУ, на которых были заблокированы вредоносные объекты.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Все рассмотренные отрасли демонстрируют колебательные **тренды** изменения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Показатель отрасли **автоматизации зданий** значительно превышает среднее значение для региона на протяжении всего периода наблюдений. В то же время в других отраслях, начиная со второго квартала 2023 года, показатели снизились относительно среднего значения для региона, хотя и демонстрируют незначительные колебания.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Австралия и Новая Зеландия

Актуальные угрозы

-1 место-

Скрипты и фишинговые страницы
6,73%

▲ незначительный рост во II кв. 2024 г.
1,2x выше среднего по миру
4-е место в мире

-2 место-

Интернет-ресурсы из списка запрещенных
4,75%

▲ **1,2x** рост во II кв. 2024 г.
2-е место в мире **по росту**

-3 место-

Шпионские программы
2,15%

▲ **1,2x** рост во II кв. 2024 г.

Веб-майнеры
0,68%

▼ снижение во II кв. 2024 г.
1,4x выше среднего по миру
6-е место в регионе (8-е в глобальном рейтинге угроз)
3-е место в мире

Черви
0,42%

▲ **1,5x** рост во II кв. 2024 г.
1-е место в мире **по росту**

Вирусы
0,35%

▲ **1,5x** рост во II кв. 2024 г.
2-е место в мире **по росту**

Программы-вымогатели
0,16%

▲ **1,6x** рост во II кв. 2024 г.
близко к среднему по миру
3-е место в мире **по росту**

Интернет
как источник угроз
9,79%

▲ **1,1x** рост во II кв. 2024 г.
2-е место в мире **по росту**

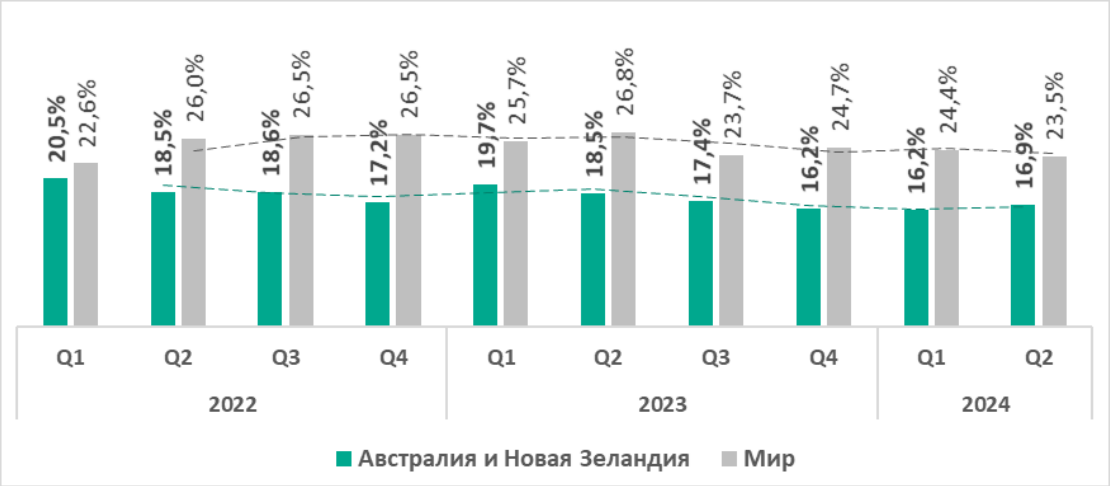
Почтовые клиенты
как источник угроз
3,29%

▼ снижение во II кв. 2024 г.
1,2x выше среднего по миру

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

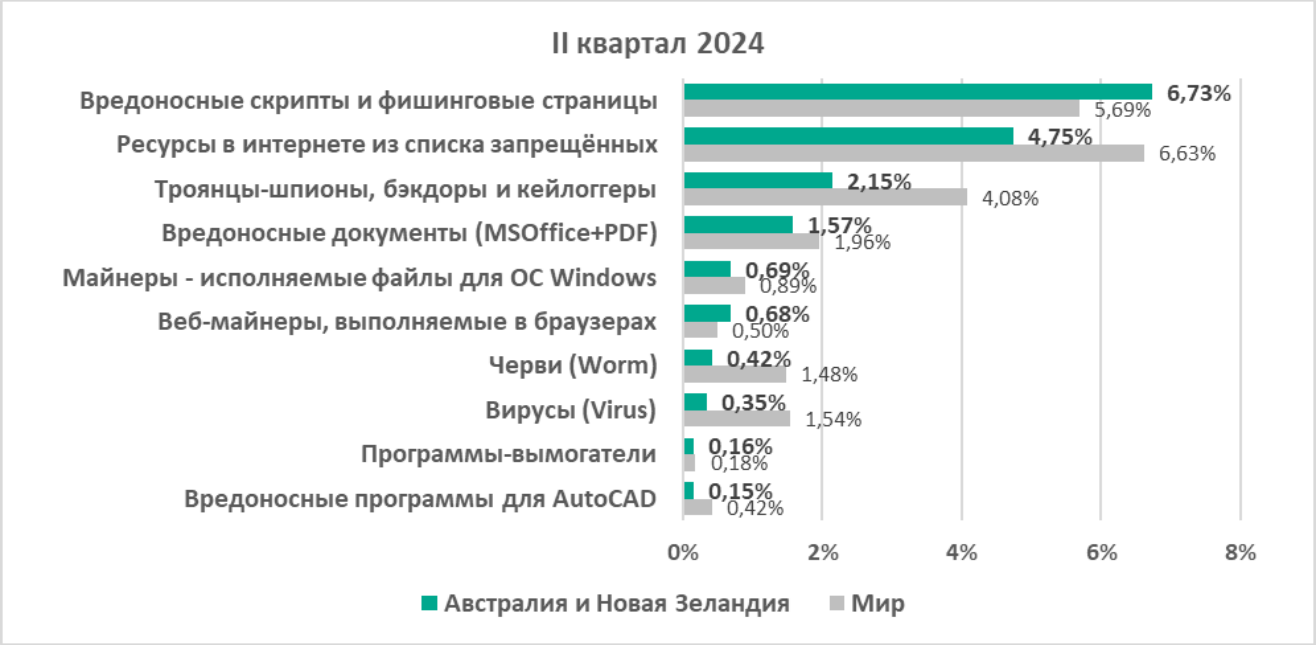
Общая ситуация

Австралия и Новая Зеландия занимают **одиннадцатое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Это один из четырех регионов, где данный показатель во втором квартале 2024 года вырос. Несмотря на это, он остается ниже среднемирового значения.



Сравнительный анализ

Категории угроз



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

По сравнению со среднемировыми показателями, в регионе выше доля компьютеров АСУ, на которых заблокированы следующие категории вредоносных объектов:

- веб-майнеры — в 1,4 раза;
- вредоносные скрипты и фишинговые страницы — в 1,2 раза.

Источники угроз

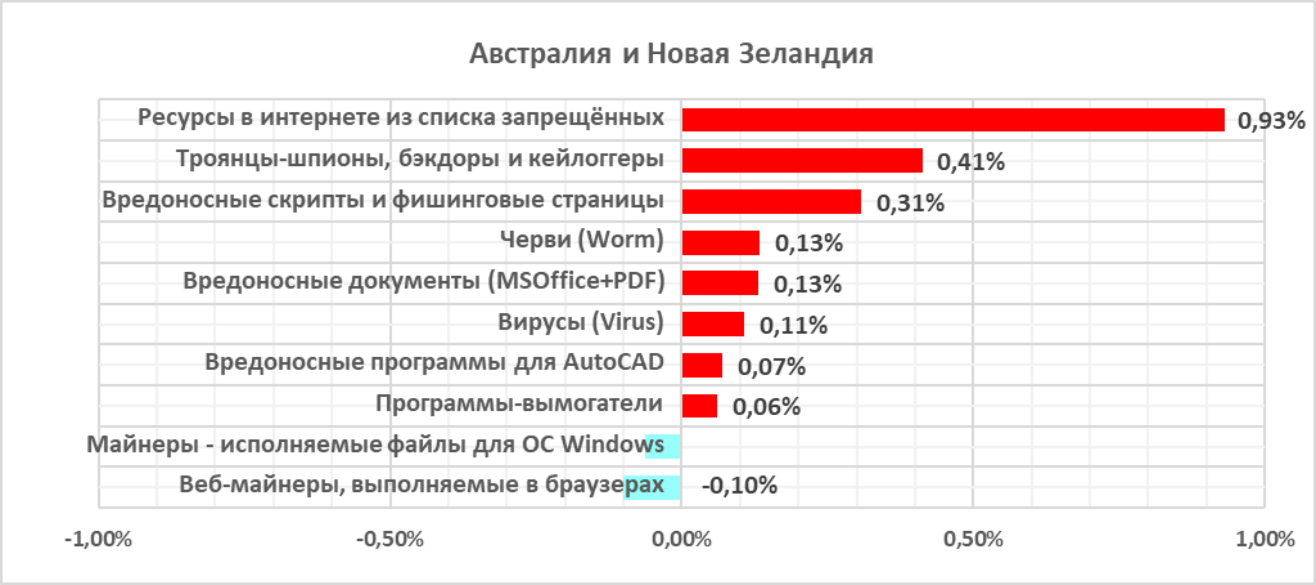
Доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, превышает среднемировой показатель в 1,1 раза.

Показатели остальных источников угроз остаются ниже соответствующих среднемировых значений.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

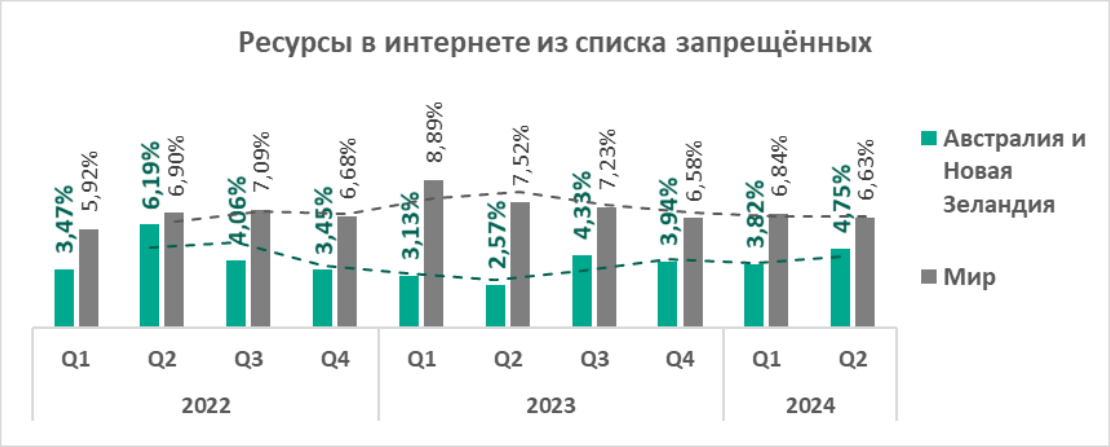
Изменения за квартал и тренды

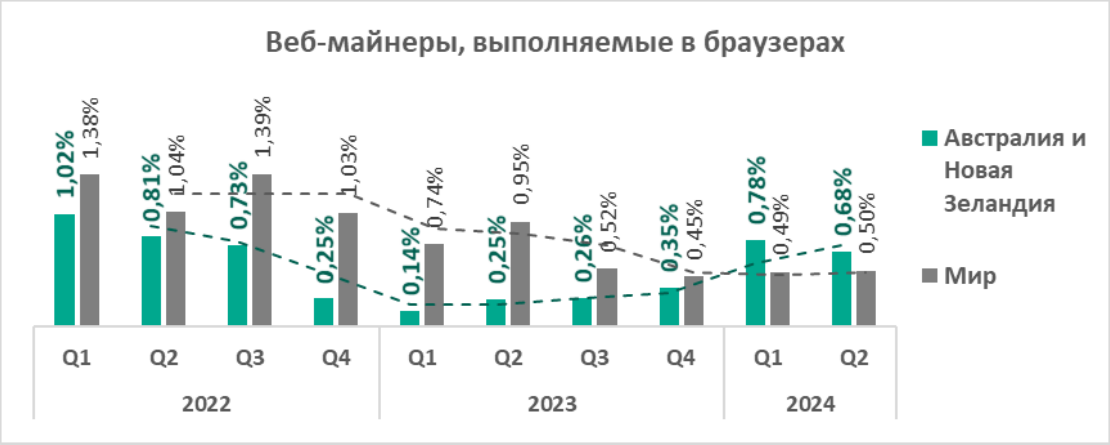
Категории угроз



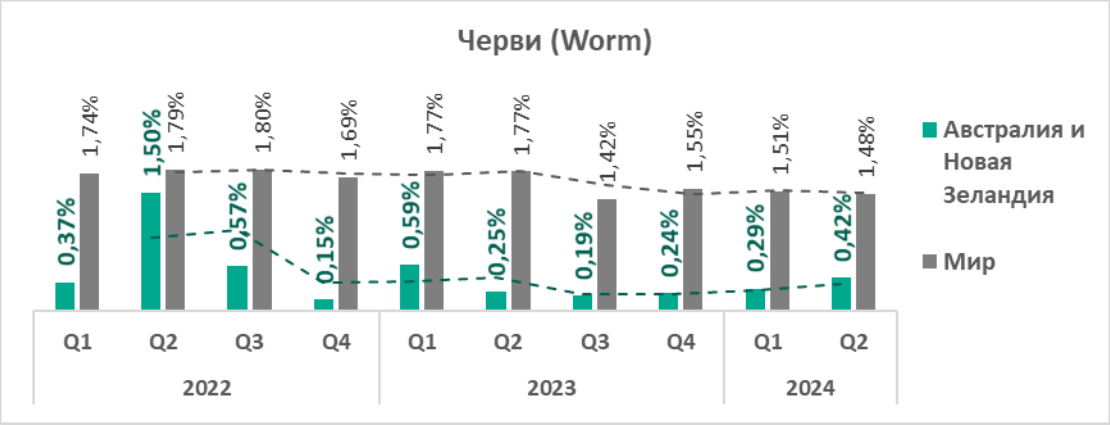
- **Наиболее сильно** по сравнению с предыдущим кварталом выросла доля компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
  - вредоносные программы для AutoCAD — в 1,9 раза;
  - программы-вымогатели — в 1,6 раза;
  - черви — в 1,5 раза;
  - вирусы — в 1,5 раза;
  - шпионские программы — в 1,2 раза;
  - ресурсы в интернете из списка запрещенных — в 1,2 раза.
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

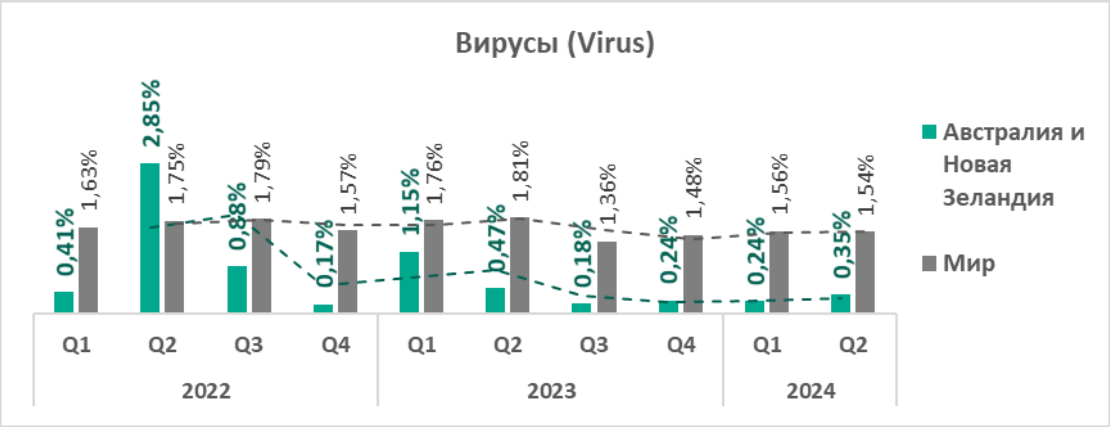
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

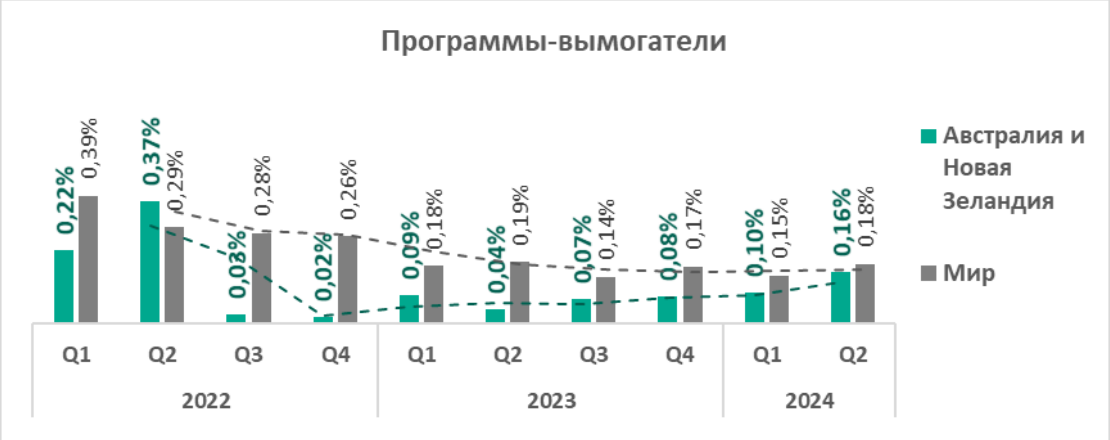




© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»







© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Австралии и Новой Зеландии за 2,5 года. **Вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе на протяжении всего периода, а **ресурсы в интернете из списка запрещенных** стабильно занимают второе место.

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

Источники угроз

Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, выросла по сравнению с предыдущим кварталом в 1,1 раза. Долгосрочные региональные и мировые тренды расходятся, двигаясь в противоположных направлениях.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Долгосрочный тренд для угроз из **почтовых клиентов** демонстрирует в основном снижение показателя, однако тот остается выше среднемирового значения на протяжении всего периода. При этом во втором квартале 2024 года разрыв значительно сократился.

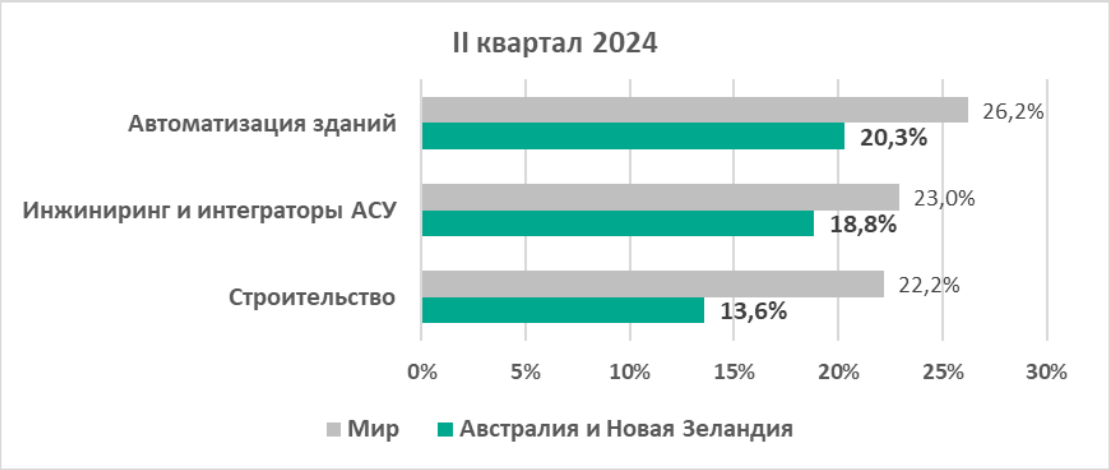
Долгосрочный тренд для угроз на **съемных носителях** находится значительно ниже среднемирового тренда на протяжении всего периода наблюдений. После резкого снижения в третьем квартале 2023 года региональный показатель оставался на этом уровне с некоторыми колебаниями вплоть до второго квартала 2024 года, когда был отмечен его рост.

Отрасли

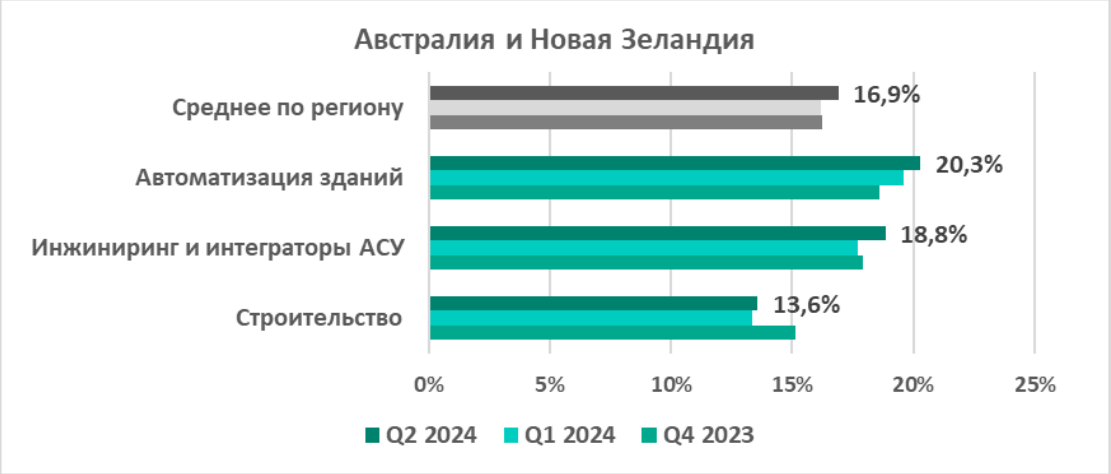
- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий.**

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- По сравнению с соответствующими **среднемировыми показателями**, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, ниже во всех рассматриваемых отраслях региона.



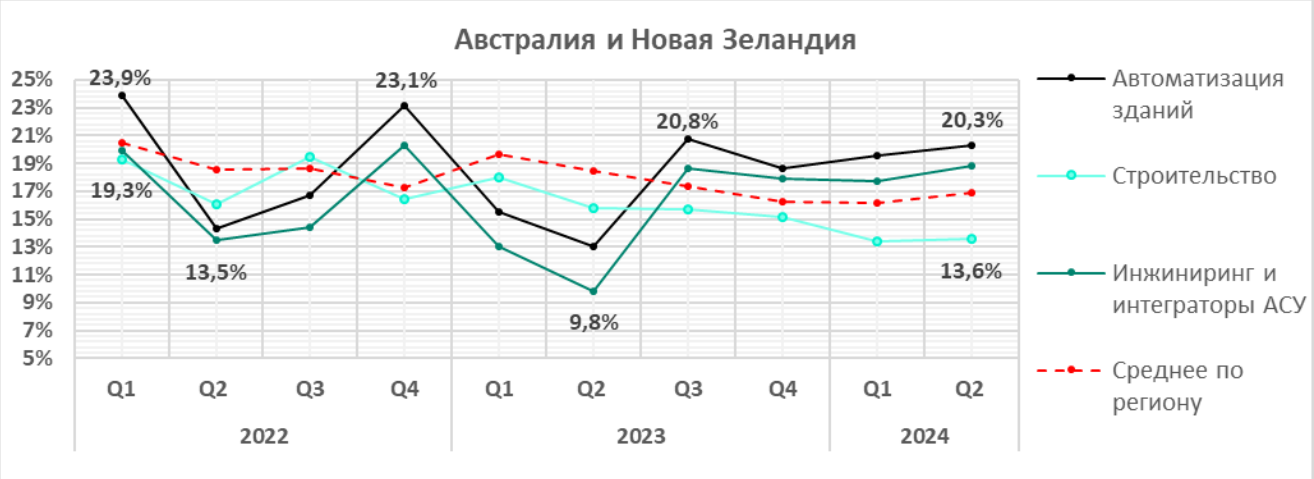
- Во **втором квартале 2024 года** во всех рассматриваемых отраслях наблюдается рост доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, по сравнению с предыдущим кварталом. Наиболее значительный рост — в 1,1 раза — отмечен в следующей отрасли: инжиниринг и интеграторы АСУ.



- **Автоматизация зданий**, а также **инжиниринг и интеграторы АСУ** до третьего квартала 2023 года демонстрировали **тренды** изменения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, с наиболее существенными колебаниями вблизи среднего для региона значения. Начиная с четвертого квартала 2023 года оба тренда стабилизировались на уровне, превышающем средний показатель по региону. В то же время **строительная** отрасль демонстрировала

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

преимущественно нисходящий тренд, оставаясь ниже среднего значения по региону начиная с четвертого квартала 2022 года.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

США и Канада

Актуальные угрозы

-1 место-

Скрипты и фишинговые страницы
4,63%

▲ **1,1x** рост во II кв. 2024 г.

-2 место-

Интернет-ресурсы из списка запрещенных
4,14%

▲ **1,2x** рост во II кв. 2024 г.
3-е место в мире **по росту**

-3 место-

Шпионские программы
1,58%

▲ **1,1x** рост во II кв. 2024 г.

Вредоносные документы
1,15%

▲ **1,1x** рост во II кв. 2024 г.

Веб-майнеры
0,42%

близко к среднему по миру
5-е место в рейтинге угроз в регионе и 8-е в мире

Программы-вымогатели
0,14%

▲ **1,7x** рост во II кв. 2024 г.
4-е место в мире **по росту**

Интернет
как источник угроз
7,85%

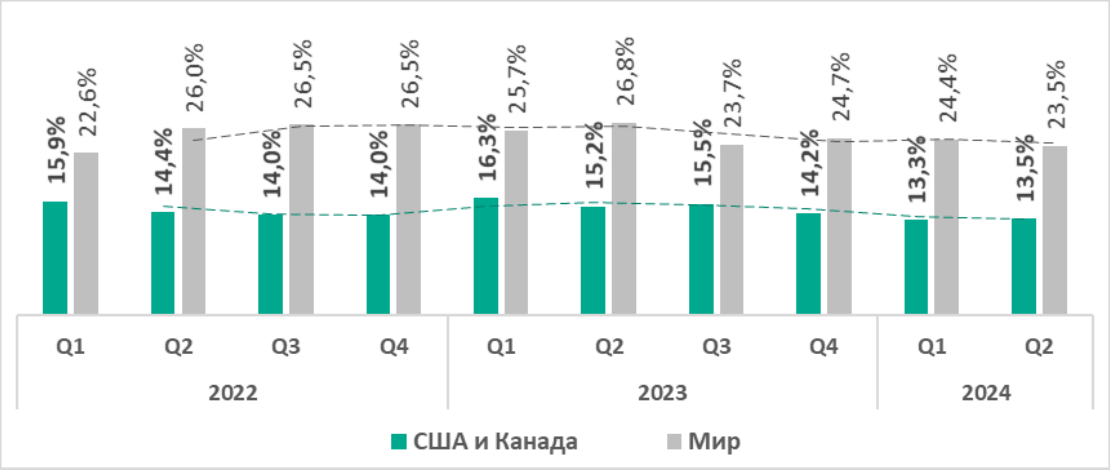
▲ незначительный рост во II кв. 2024 г.
4-е место в мире **по росту**

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

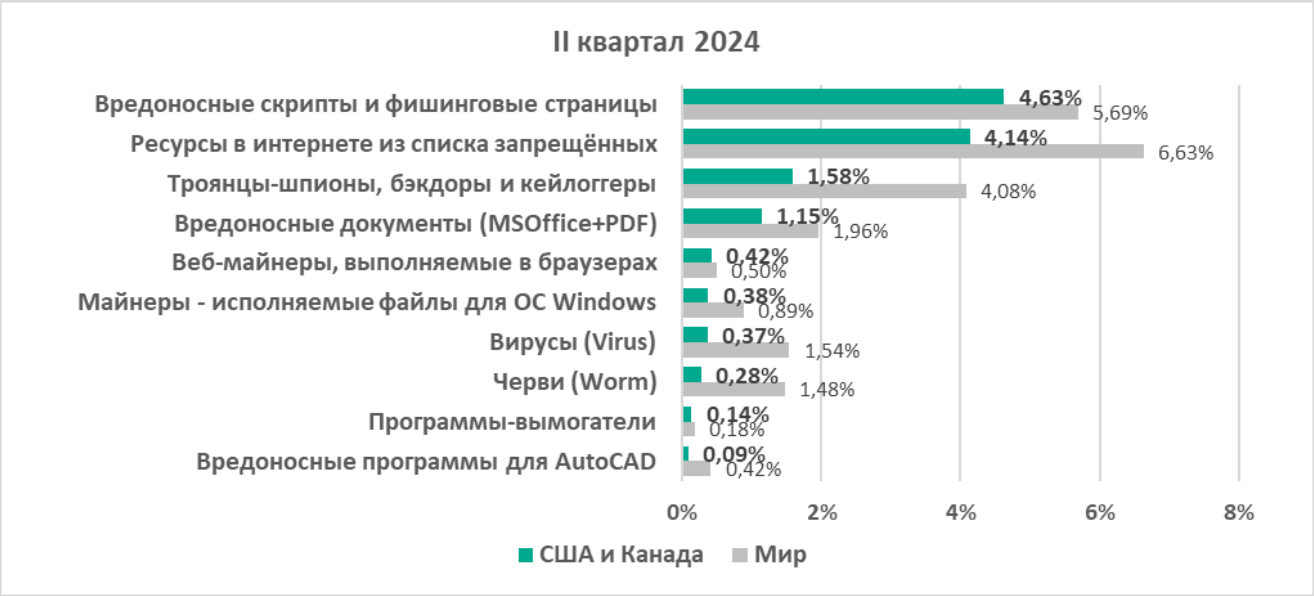
США и Канада занимают **двенадцатое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Это один из четырех регионов, где данный показатель во втором квартале 2024 года вырос; регион находится на четвертом месте по величине этого прироста. При этом показатель остается ниже среднемирового значения.

В целом, это один из наиболее безопасных регионов с малой долей компьютеров АСУ, на которых были заблокированы вредоносные объекты.



Сравнительный анализ

Категории угроз

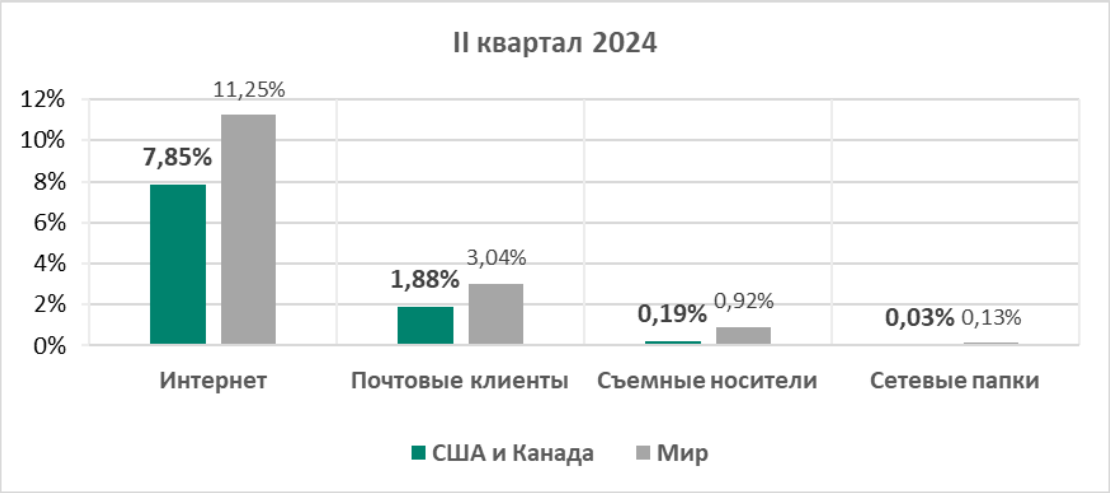


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- **По сравнению со среднемировыми показателями**, в регионе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, ниже для всех категорий угроз.
- **Веб-майнеры находятся на пятом месте** в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых они были заблокированы (в мире — на восьмом месте). С начала 2024 года доля компьютеров АСУ, на которых в регионе были заблокированы угрозы из этой категории, приблизилась к среднемировому значению.

Источники угроз

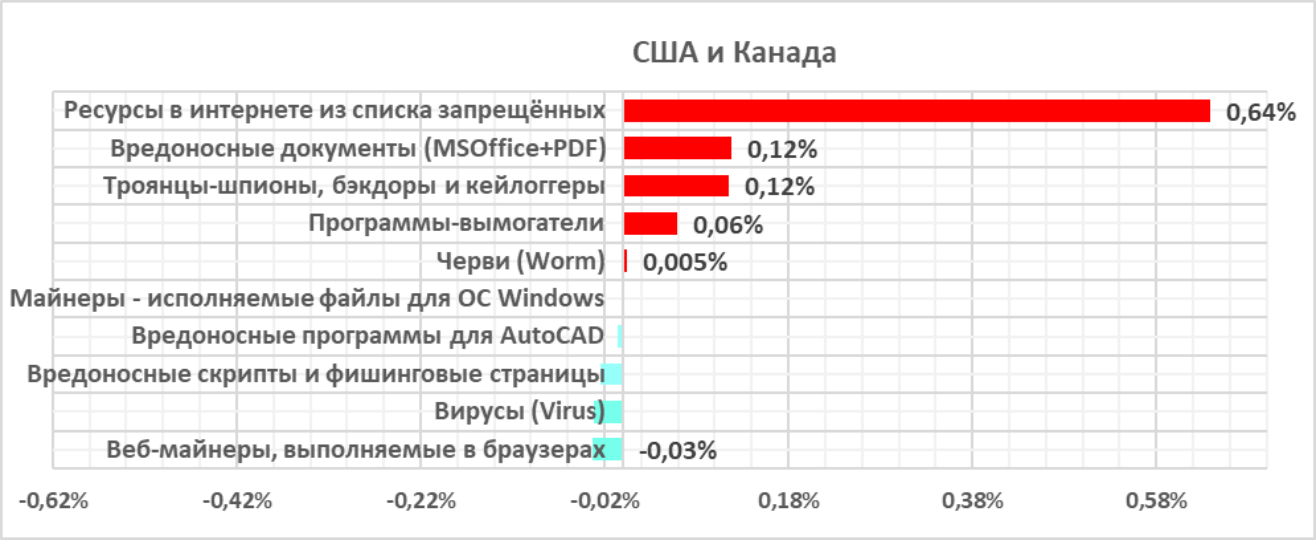
Показатели всех источников угроз были заметно ниже соответствующих среднемировых значений.



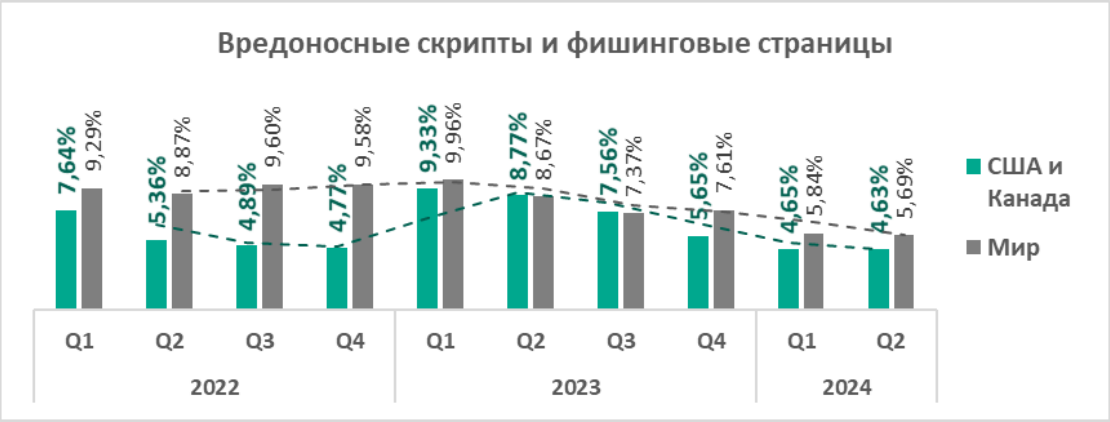
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменения за квартал и тренды

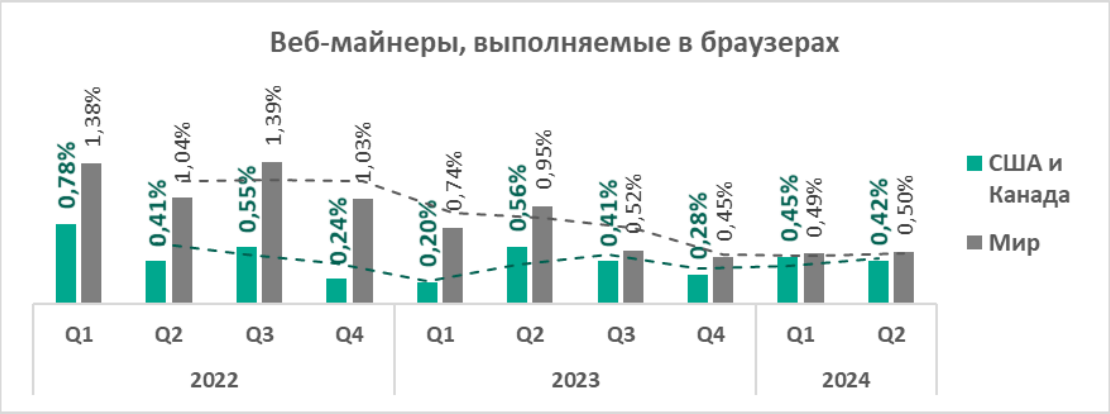
Категории угроз



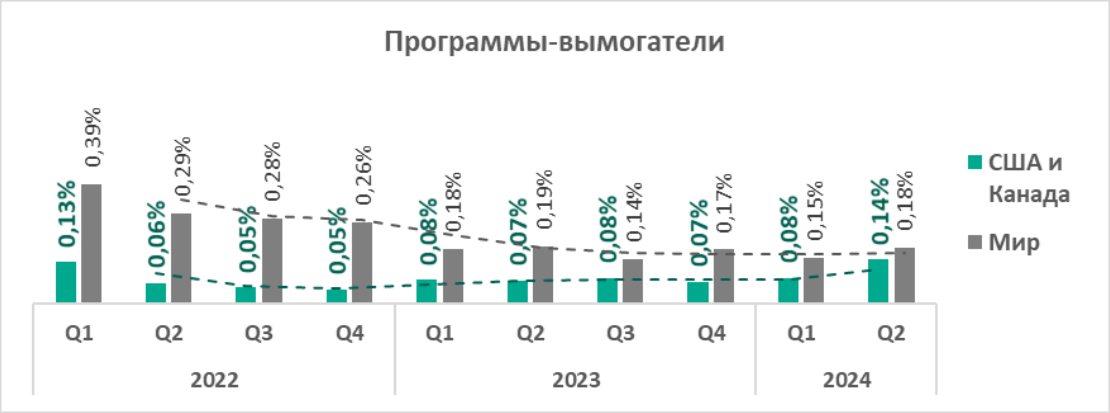
- **Наиболее сильно за квартал** выросла доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
  - программы-вымогатели — в 1,8 раза; третье место по величине роста. В итоге показатель программ-вымогателей в регионе приблизился к среднемировому;
  - ресурсы в интернете из списка запрещенных — в 1,2 раза; третье место в мире по величине роста;
  - шпионские программы — в 1,1 раза;
  - вредоносные документы — в 1,1 раза.
- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в регионе за 2,5 года. **Вредоносные скрипты и фишинговые страницы** остаются здесь ведущей категорией на протяжении всего периода, а **ресурсы в интернете из списка запрещенных** стабильно занимают второе место. **Шпионские программы** уже второй квартал подряд удерживаются на третьей строчке.

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

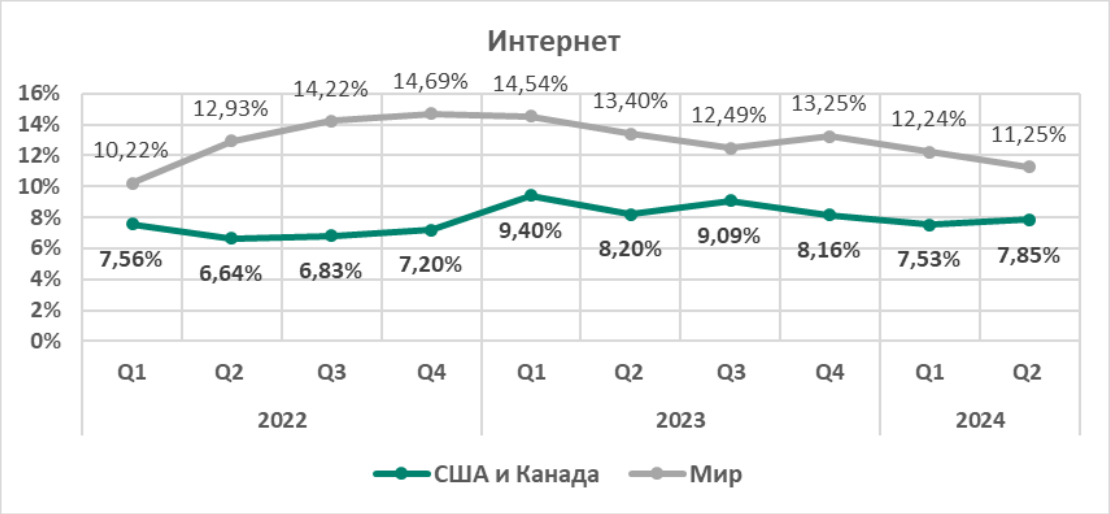
Источники угроз

Во втором квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, увеличилась в 1,1 раза по сравнению с предыдущим кварталом. США и Канада — один из четырех регионов,

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

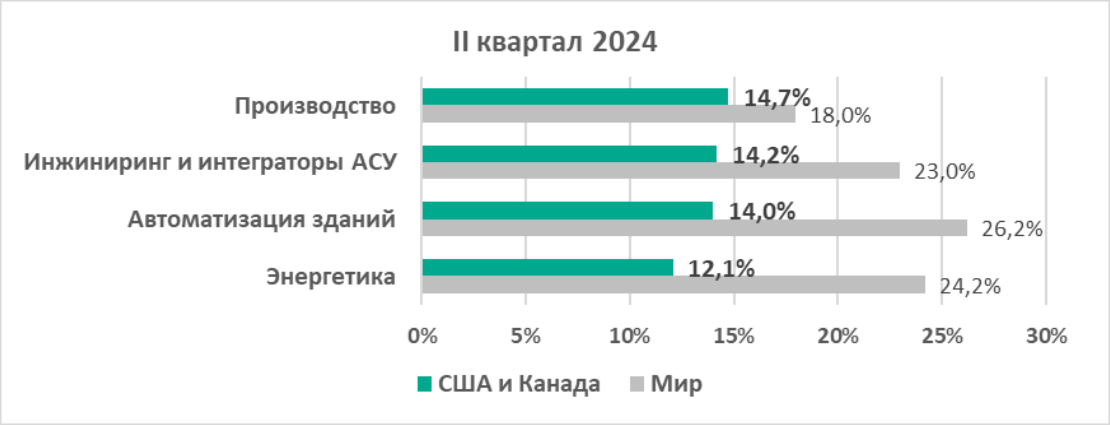
где был отмечен рост этого показателя, — находится на **четвертом месте в мире** по величине этого роста.

Долгосрочные тренды для угроз из интернета в регионе и мире расходятся, двигаясь в противоположных направлениях.



Отрасли

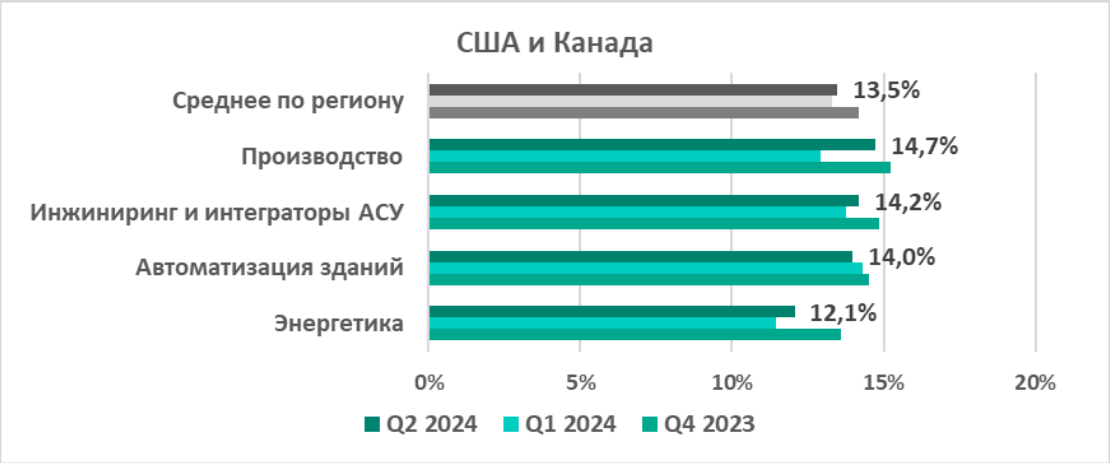
- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **производство**. В мировом рейтинге эта отрасль находится на пятом месте среди рассмотренных отраслей.
- По сравнению с соответствующими **среднемировыми показателями**, в регионе показатели всех отраслей остаются значительно ниже.



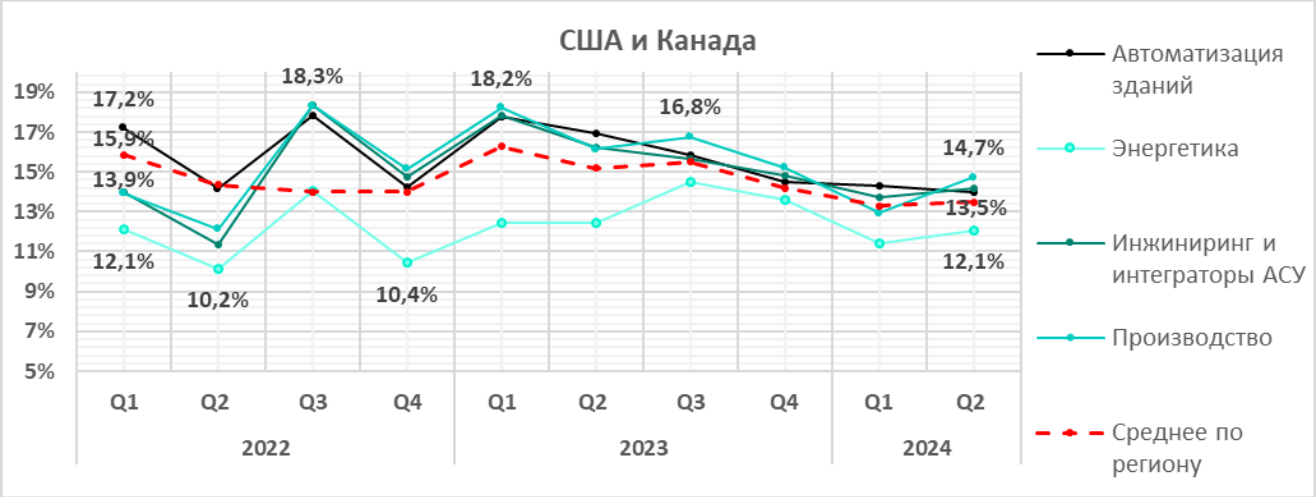
- Во **втором квартале 2024 года** во всех отраслях, за исключением автоматизации зданий, зафиксирован рост доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Наибольший рост отмечен в следующих отраслях:

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- производство — в 1,1 раза;
- энергетика — в 1,1 раза.



- Во всех рассмотренных отраслях до первого квартала 2023 года наблюдались **тренды** со значительными колебаниями доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. В третьем квартале 2023 года тренды стабилизировались вблизи среднего регионального значения и с тех пор следуют в основном нисходящей динамике.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Западная Европа

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
4,86%

▲ **1,3x** рост во II кв. 2024 г.
1-е место в мире **по росту**

-2 место-

Скрипты и фишинговые страницы
3,72%

▲ **1,1x** рост во II кв. 2024 г.
3-е место в мире **по росту**

-3 место-

Шпионские программы
1,75%

▲ **1,2x** рост во II кв. 2024 г.

Вредоносные документы
1,60%

▲ **1,6x** рост во II кв. 2024 г.
1-е место в мире **по росту**

Программы-вымогатели
0,08%

▲ **1,6x** рост во II кв. 2024 г.

Интернет
как источник угроз
7,34%

▲ **1,1x** рост
3-е место в мире **по росту**

Почтовые клиенты
как источник угроз
2,53%

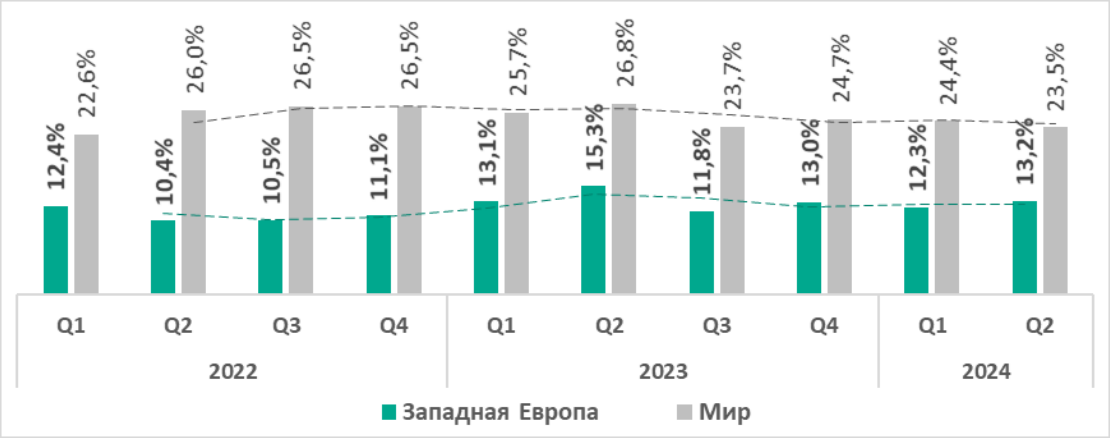
▲ **1,2x** рост
2-е место в мире **по росту**

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Общая ситуация

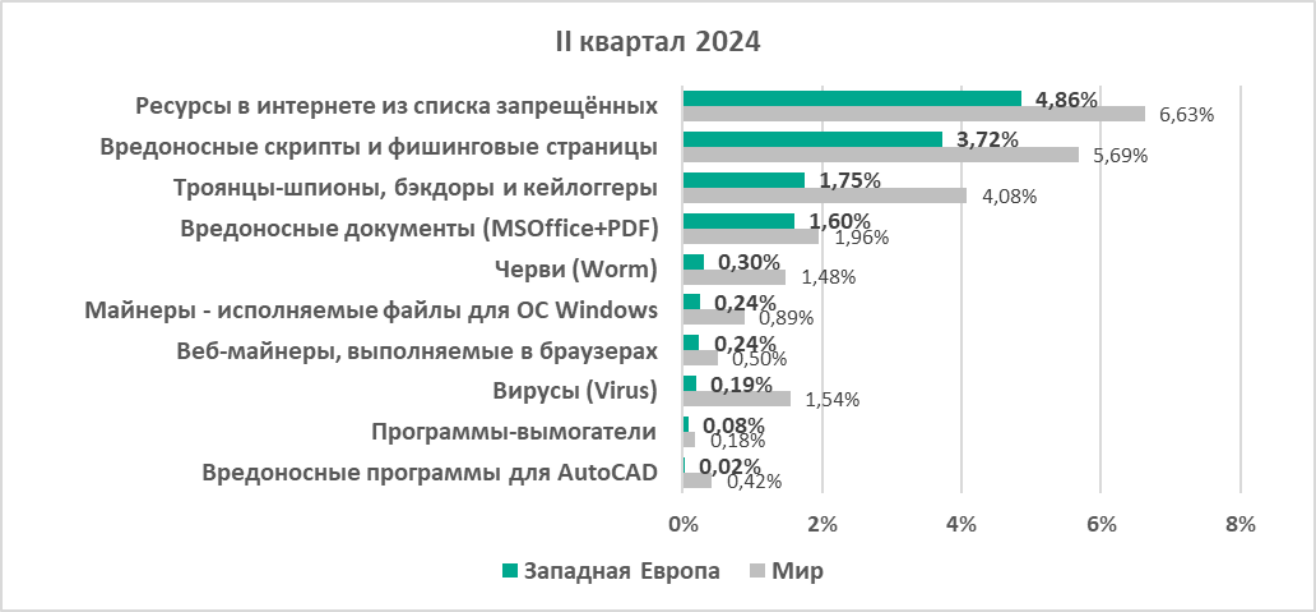
Западная Европа занимает **тринадцатое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Это один из четырех регионов, где данный показатель во втором квартале 2024 года вырос, причем в 1,1 раза. Регион находится на втором месте по величине прироста.

В целом, это один из наиболее безопасных регионов, где одно из наименьших значений доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Здесь этот показатель существенно ниже среднемирового значения.



Сравнительный анализ

Категории угроз

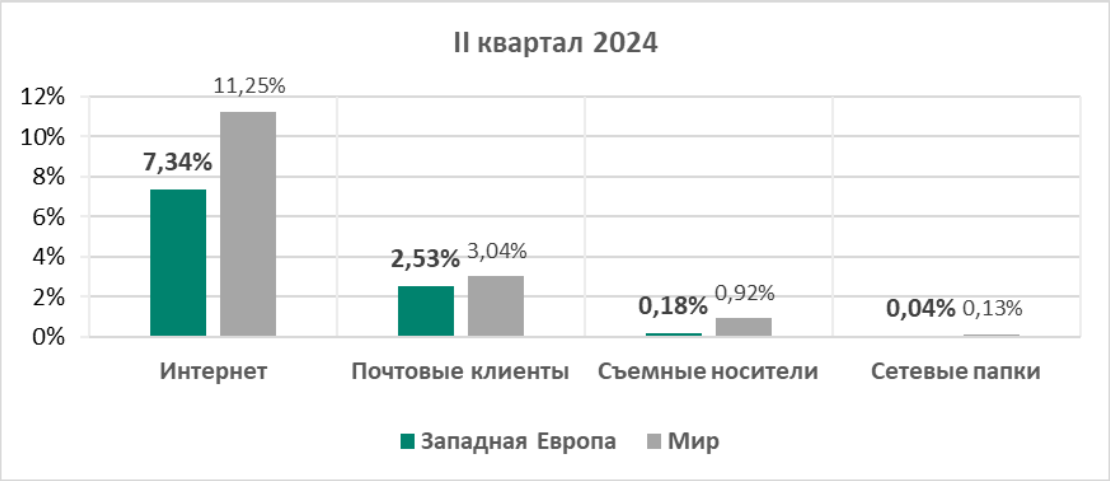


© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

По сравнению со среднемировыми показателями, в регионе доля компьютеров АСУ, на которых были заблокированы те или иные угрозы, заметно ниже для всех категорий угроз.

Источники угроз

Показатели всех источников угроз заметно ниже соответствующих среднемировых значений.



Изменения за квартал и тренды

Категории угроз

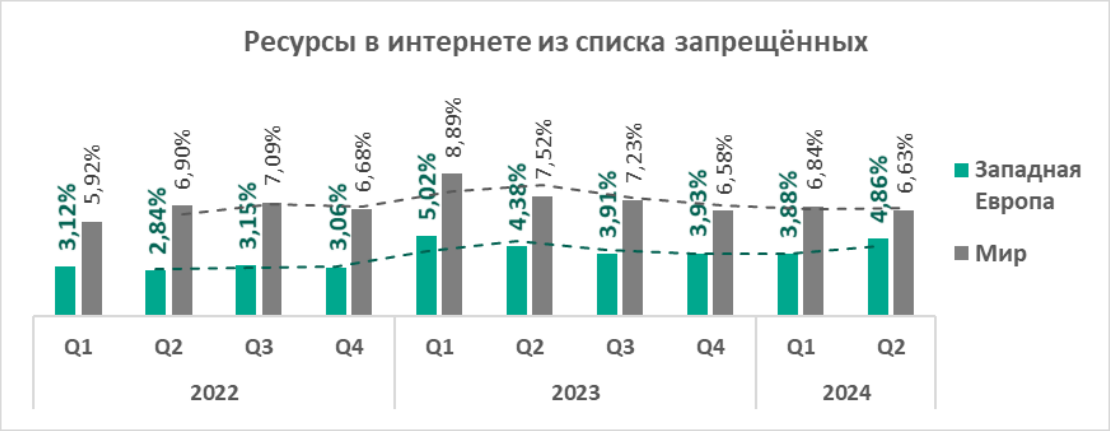
Большинство категорий угроз демонстрирует увеличение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.

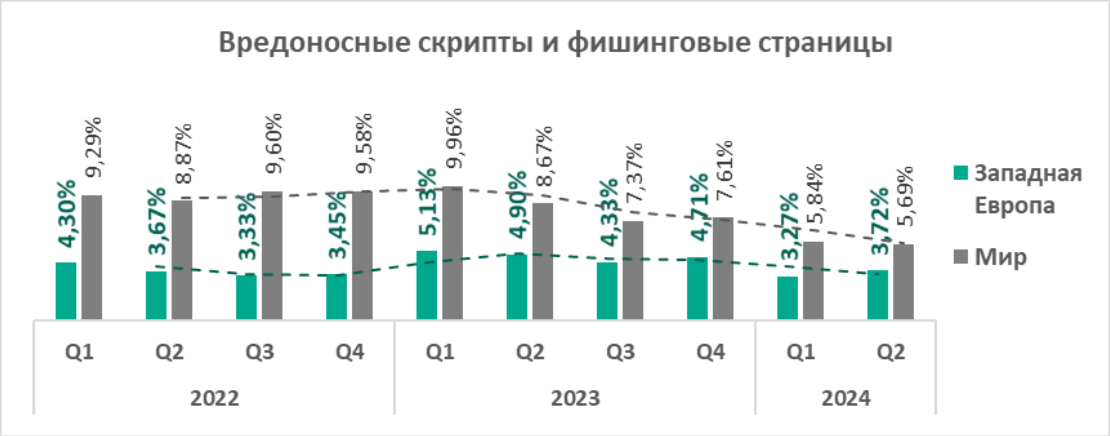
- **Наиболее существенно за квартал** выросли доли компьютеров АСУ, на которых были заблокированы следующие категории угроз:

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

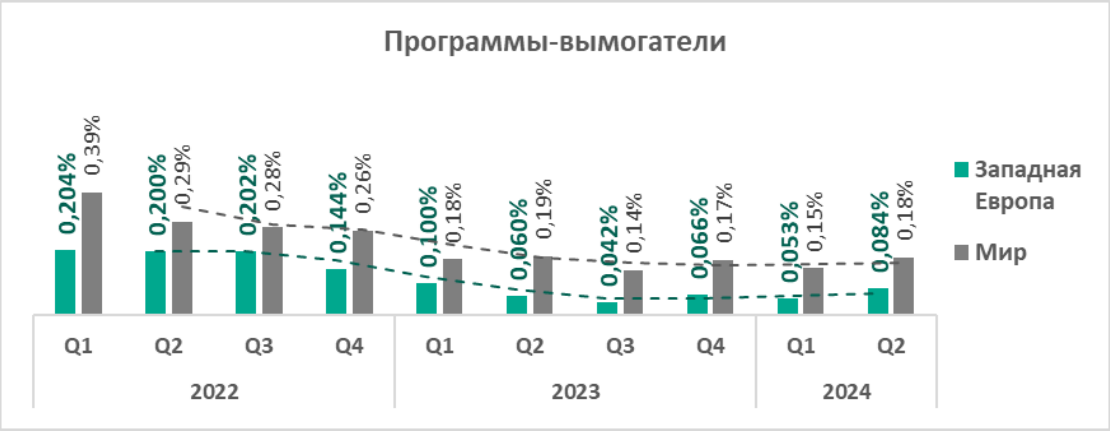
- вредоносные документы — в 1,6 раз; первое место в мире по величине роста;
- программы-вымогатели — в 1,6 раз;
- ресурсы в интернете из списка запрещенных — в 1,3 раза; первое место в мире по величине роста;
- шпионские программы — в 1,1 раза;
- вредоносные скрипты и фишинговые страницы — в 1,1 раза; третье место в мире по величине роста;
- вредоносные программы для AutoCAD — в 1,1 раза.

- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Западной Европе за 2,5 года. **Ресурсы в интернете из списка запрещенных,** традиционно занимавшие второе место, в первом квартале 2024 года переместились на первую строчку, сместив **вредоносные скрипты и фишинговые страницы** на вторую. **Черви** с некоторыми колебаниями поднялись и удерживаются на пятой позиции с четвертого квартала 2023 года.

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

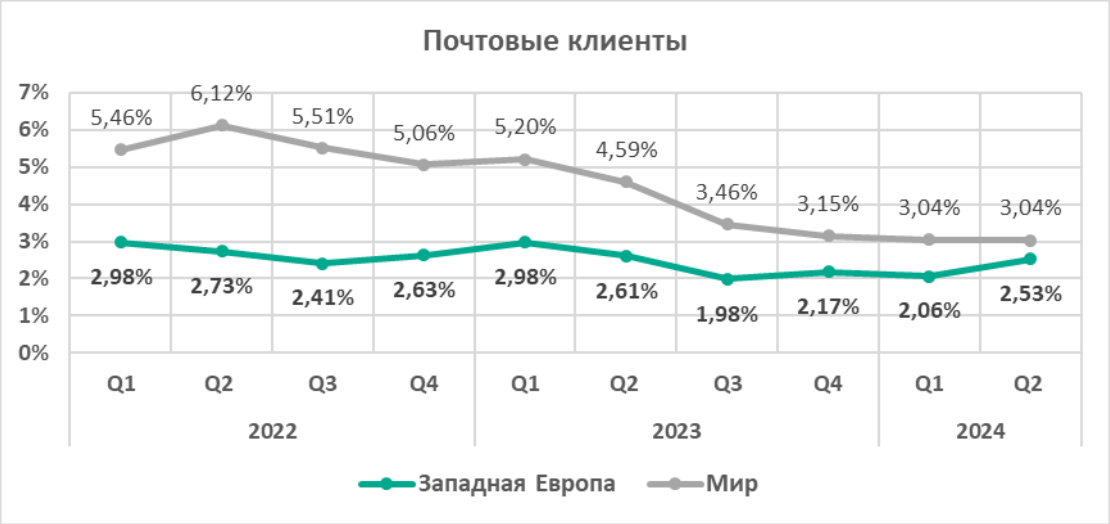
Источники угроз

- Западная Европа является одним из трех регионов, где отмечен рост доли компьютеров АСУ, на которых были заблокированы угрозы из **интернета**.

  Долгосрочные региональный и мировой тренды для угроз из **интернета** изначально имели разнонаправленный характер, однако начиная с первого квартала 2023 года разрыв между показателями постепенно сокращается.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

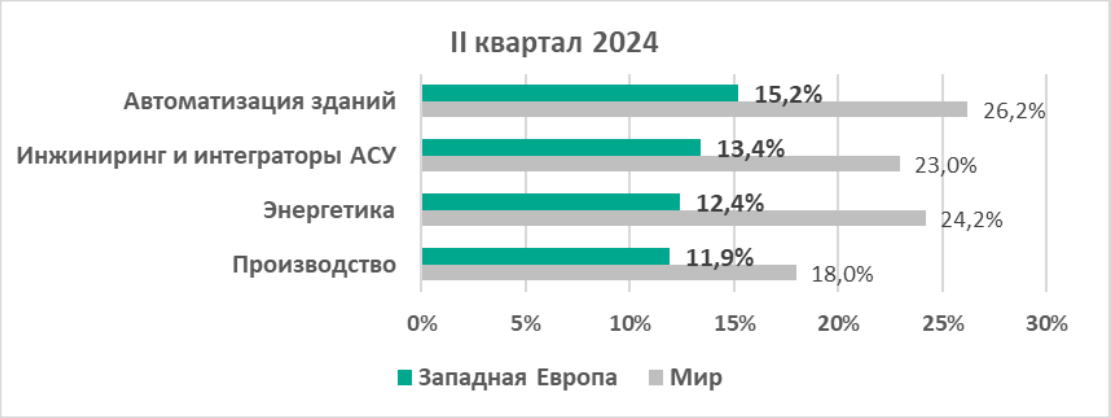
- Регион также занимает **второе место в мире** по росту доли компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через **почтовые клиенты**. Во втором квартале 2024 года разрыв между региональным и среднемировым значениями сократился до минимального за все время наблюдений.



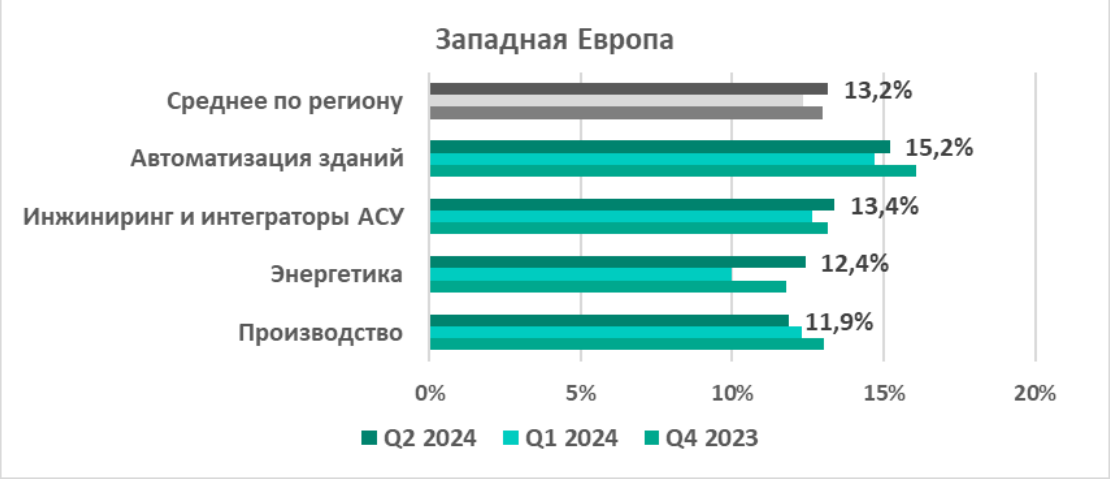
Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** из рассмотренных в отчете является **автоматизация зданий**.
- По сравнению со **среднемировыми значениями**, показатели всех отраслей в регионе остаются значительно ниже.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

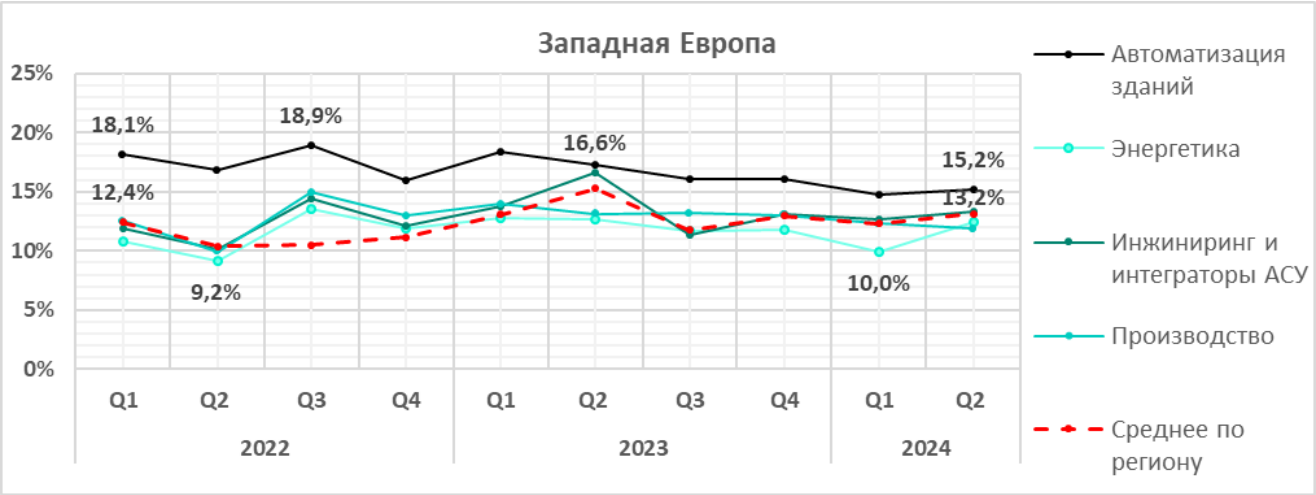


- Во **втором квартале 2024 года** во всех отраслях, кроме производства, зафиксирован рост доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Наибольший рост отмечен в следующих отраслях:
  - энергетика — в 1,2 раза;
  - инжиниринг и интеграторы АСУ — в 1,1 раза.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Все рассматриваемые отрасли демонстрируют колебательные **тренды** изменения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Тренд для автоматизации зданий указывает на плавное снижение показателя.



© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Северная Европа

Актуальные угрозы

-1 место-

Интернет-ресурсы из списка запрещенных
3,79%

▲ незначительный рост во II кв. 2024 г.

-2 место-

Скрипты и фишинговые страницы
2,64%

▲ незначительный рост во II кв. 2024 г.

-3 место-

Шпионские программы
1,83%

▲ **1,1x** рост во II кв. 2024 г.

Вредоносные документы
0,86%

▲ **1,5x** рост во II кв. 2024 г.

Майнеры — исполняемые файлы
0,45%

▲ **1,6x** рост во II кв. 2024 г.
6-е место в регионе
и 8-е место в мире

Программы-вымогатели
0,08%

▲ **1,5x** рост во II кв. 2024 г.

Интернет
как источник угроз
6,03%

▼ снижение во II кв. 2024 г.

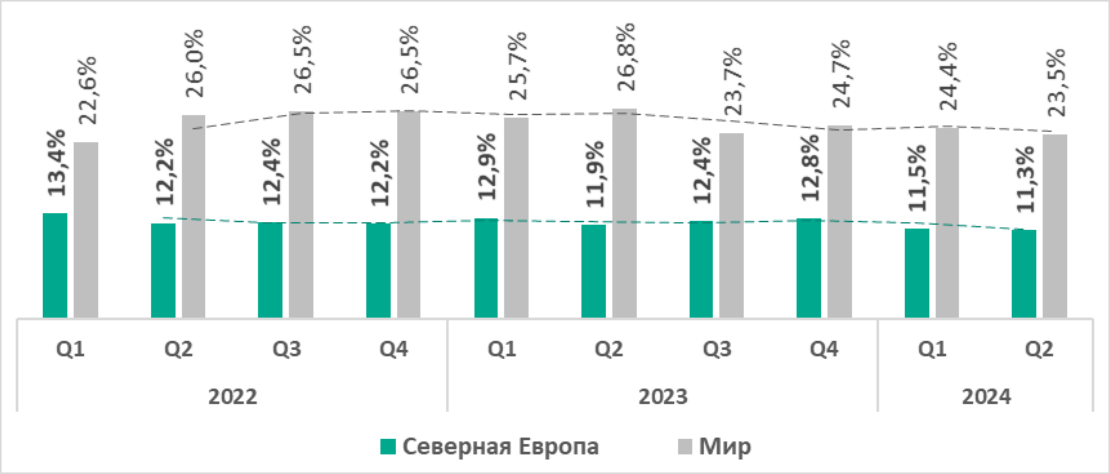
Почтовые клиенты
как источник угроз
1.71%

▲ **1,1x** рост во II кв. 2024 г.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

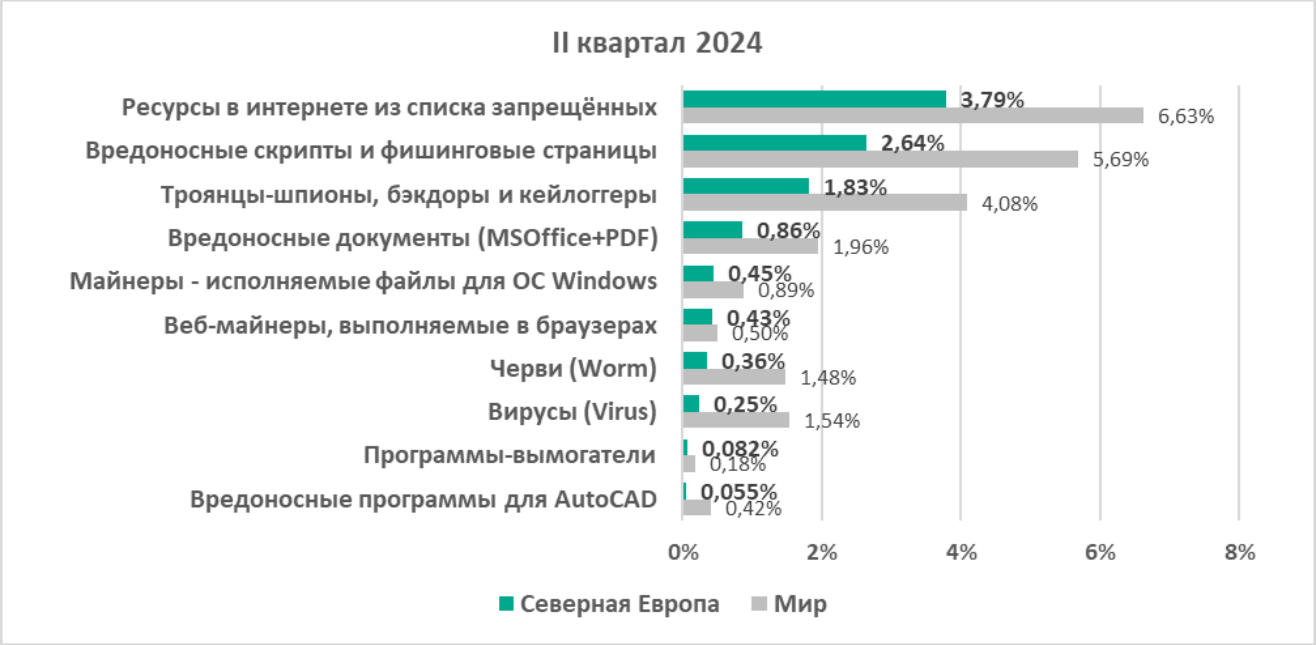
Общая ситуация

Северная Европа занимает **четырнадцатое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Этот показатель у региона традиционно самый низкий — существенно ниже среднемирового значения.



Сравнительный анализ

Категории угроз



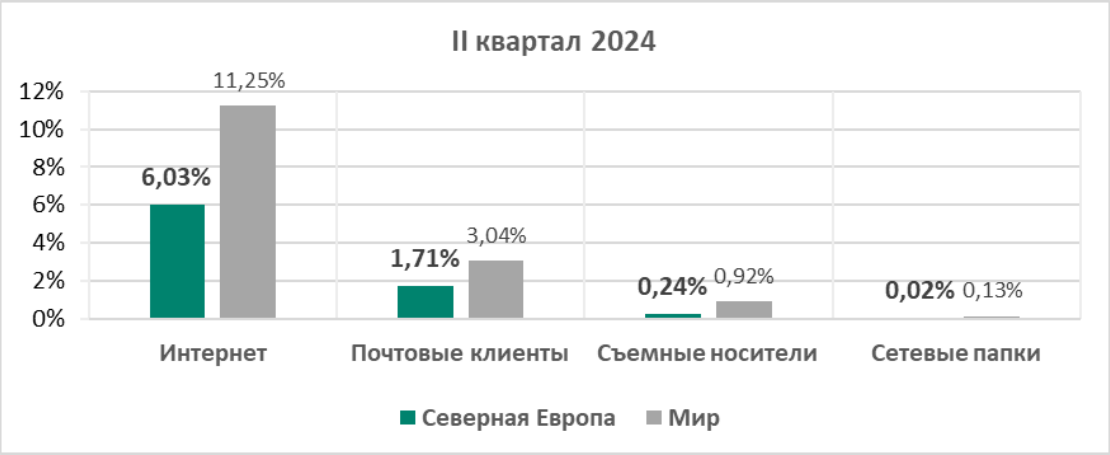
Для каждой категории угроз доля компьютеров АСУ, на которых эта категория была заблокирована, заметно ниже соответствующего среднемирового значения.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- **Майнеры — исполняемые файлы для ОС Windows занимают пятое место** в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых они были заблокированы (в мире — на седьмом месте). Этот показатель растет начиная с первого квартала 2024 года.
- **Веб-майнеры находятся на шестом месте** в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых они были заблокированы (в мире — на восьмом месте). Этот показатель близок к среднемировому значению.

Источники угроз

Показатели всех источников угроз заметно ниже соответствующих среднемировых значений.

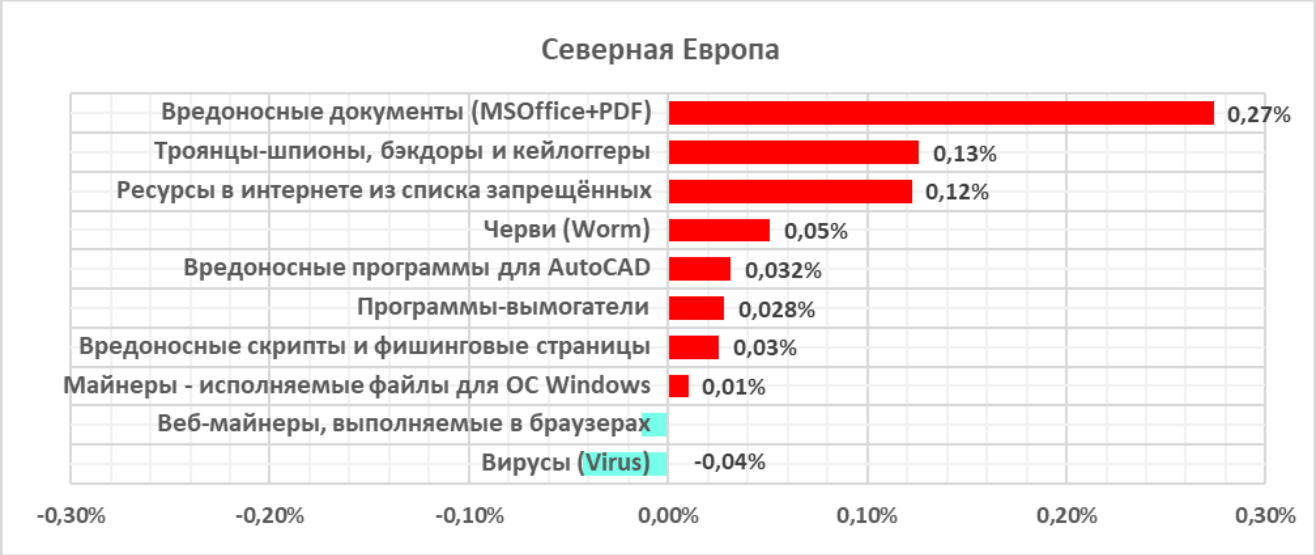


Изменения за квартал и тренды

Категории угроз

Большинство категорий угроз демонстрирует рост доли компьютеров АСУ, на которых вредоносные объекты из данных категорий были заблокированы.

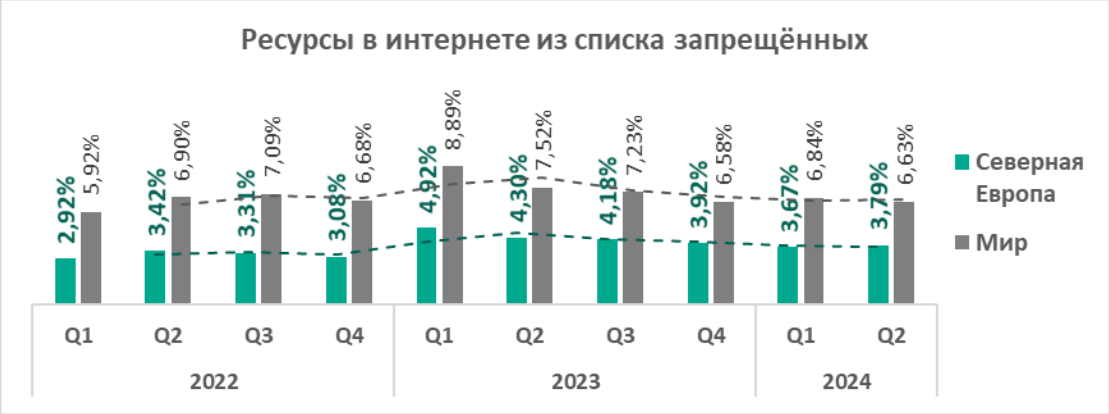
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



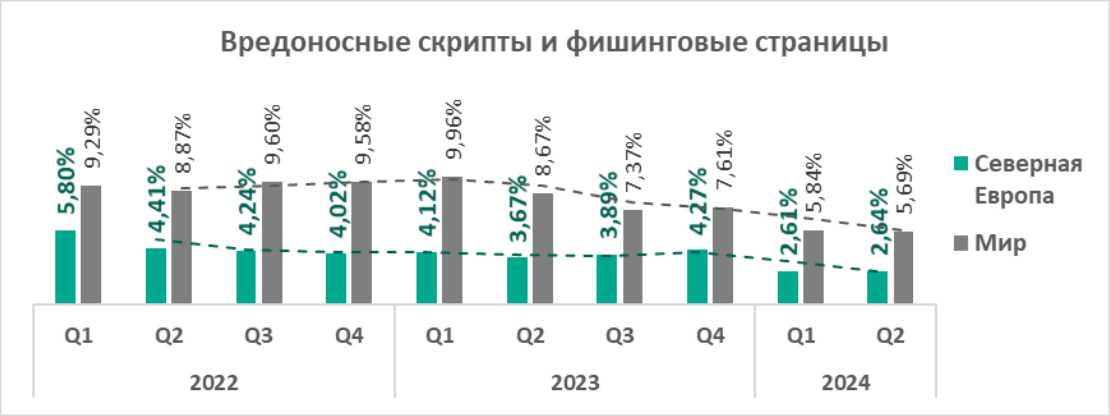
Наиболее существенно за квартал выросла доля компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

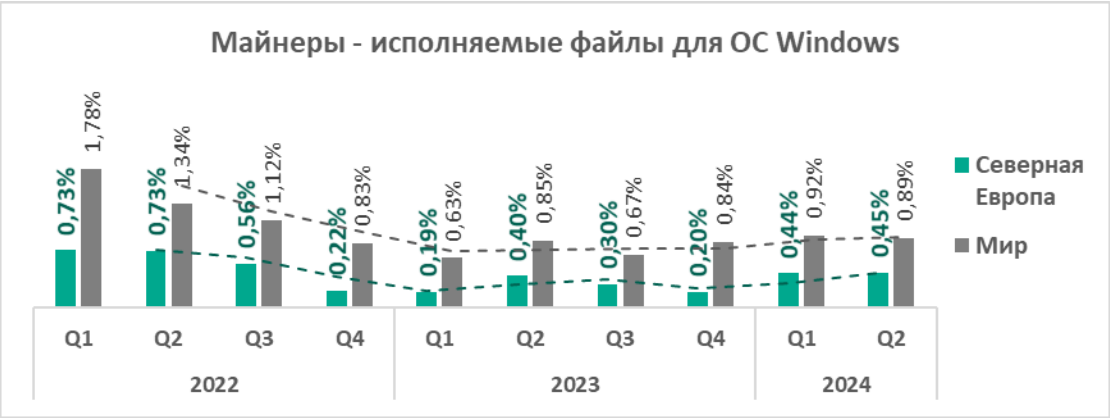
- вредоносные программы для AutoCAD — в 2,4 раза;
- вредоносные документы — в 1,5 раза;
- программы-вымогатели — в 1,5 раза;
- черви — в 1,2 раза.

- **Ведущие категории угроз** показывают разнонаправленную динамику за квартал.

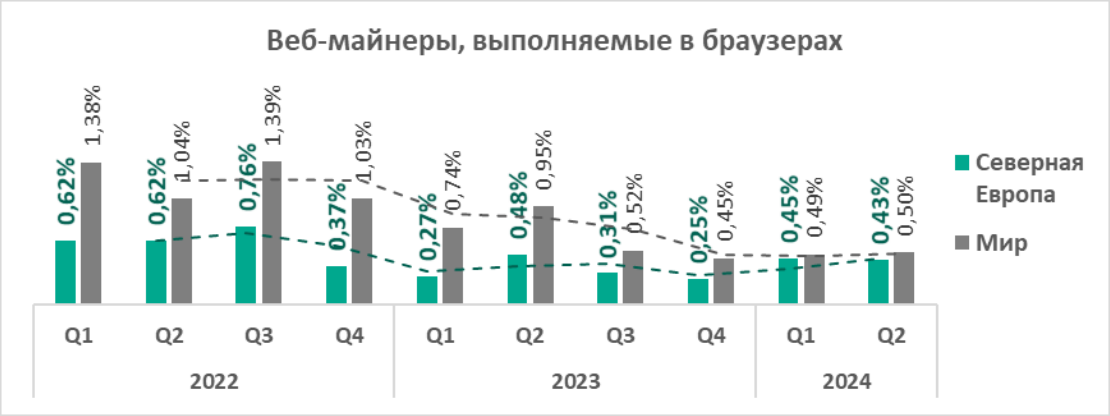


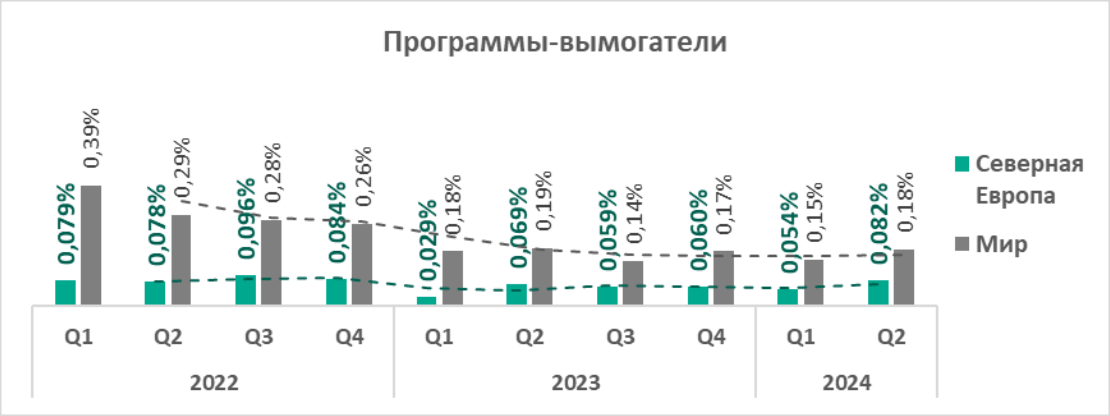
© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»





- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Западной Европе за 2,5 года. **Ресурсы в интернете из списка запрещенных** вернулись на первое место в первом квартале 2024года — ранее они занимали эту позицию с первого по третий квартал 2023 года, а в остальное время уступали ее категории **вредоносные скрипты и фишинговые страницы**.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

Источники угроз

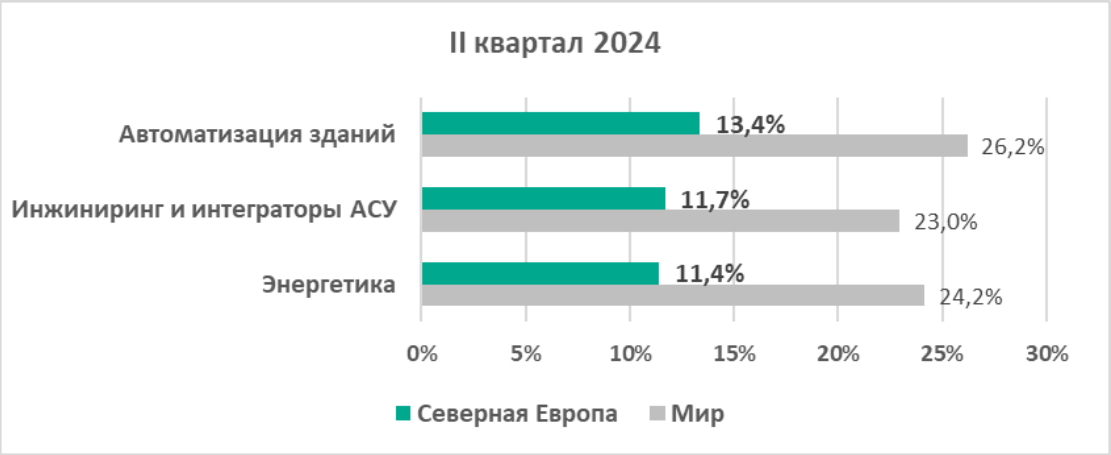
- В регионе отмечен рост доли компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через **почтовые клиенты**. В целом, тренд для таких угроз отличается преимущественно снижением.

- Тренд для угроз из интернета показывал плавный рост вплоть до четвертого квартала 2023 года, после чего началось снижение.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отрасли

- **Наиболее часто встречающаяся с угрозами отрасль** региона из рассмотренных в отчете — **автоматизация зданий**. В мировом рейтинге исследованных отраслей она занимает пятое место.
- По **сравнению со среднемировыми значениями**, показатели всех рассмотренных отраслей в регионе значительно ниже.



- Во **втором квартале 2024 года** в энергетической отрасли доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла в 1,2 раза.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Все рассматриваемые отрасли показывают колебательные **изменения** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Автоматизация зданий демонстрирует постепенно снижающийся тренд, энергетика, а также инжиниринг и интеграторы АСУ — продолжительные колебательные тренды.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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 хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human Machine Interface (HMI);
- компьютеры, используемые для администрирования технологических сетей;
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации.

[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.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Атакованными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете 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.

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»