

Ландшафт угроз для систем промышленной автоматизации

Регионы, четвертый квартал 2024

Обзор четвертого квартала 2024 года	3
Общая статистика по регионам.....	3
Категории вредоносного ПО.....	5
Регионы. Некоторые особенности	29
Африка	30
Юго-Восточная Азия	39
Ближний Восток	48
Центральная Азия	58
Восточная Азия	67
Восточная Европа.....	78
Латинская Америка	86
Южная Азия	93
Южная Европа.....	102
Россия	112
Австралия и Новая Зеландия.....	121
Западная Европа.....	127
Северная Европа.....	136
Методика подготовки статистики.....	143

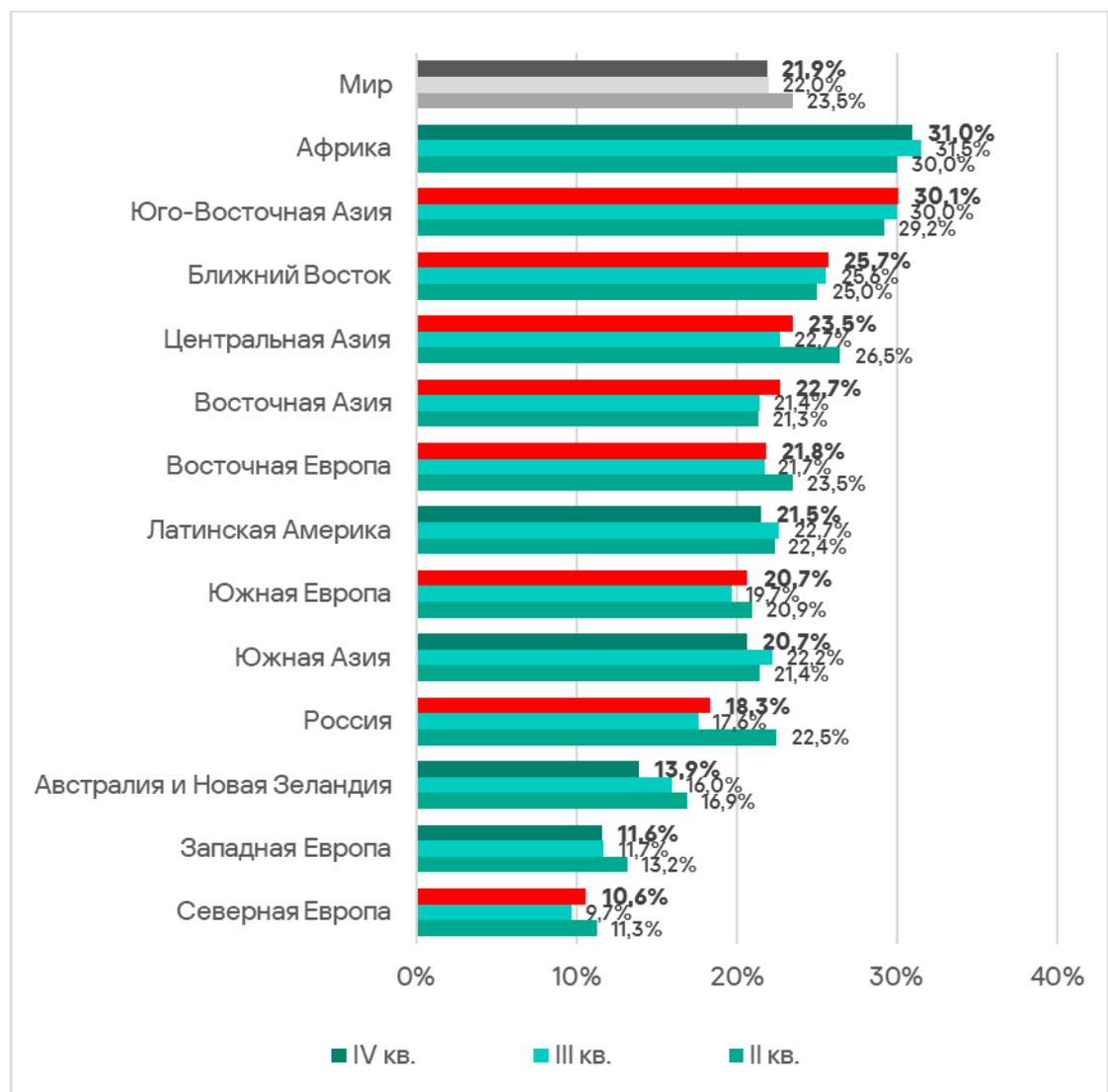
Обзор четвертого квартала 2024 года

Общая статистика по регионам

В мире в четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась по сравнению с предыдущим кварталом на 0,1 п. п. и составила 21,9%.

Значение этого параметра в различных регионах варьируется — от 10,6% в Северной Европе до 31,0% в Африке.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, за четвертый квартал 2024 года



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

Более 25%

- Африка — 31,0%
- Юго-Восточная Азия — 30,1%
- Ближний Восток — 25,7%

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.

20–25%

- Центральная Азия — 23,5%
- Восточная Азия — 22,7%
- Восточная Европа — 21,8%
- Латинская Америка — 21,5%
- Южная Европа — 20,7%
- Южная Азия — 20,7%

Регионы этой группы могут испытывать специфические трудности при попытках изолировать свою технологическую инфраструктуру от некоторых киберугроз.

Менее 20%

- Россия — 18,3%
- Австралия и Новая Зеландия — 13,9%
- Западная Европа — 11,6%
- Северная Европа — 10,6%

В эту группу входят регионы, наиболее благополучные с точки зрения доступности технологической инфраструктуры для киберугроз.

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

Регионы и мир.
Изменение доли атакованных компьютеров за четвертый квартал 2024 года



Категории вредоносного ПО

Вредоносные объекты, используемые для первичного заражения

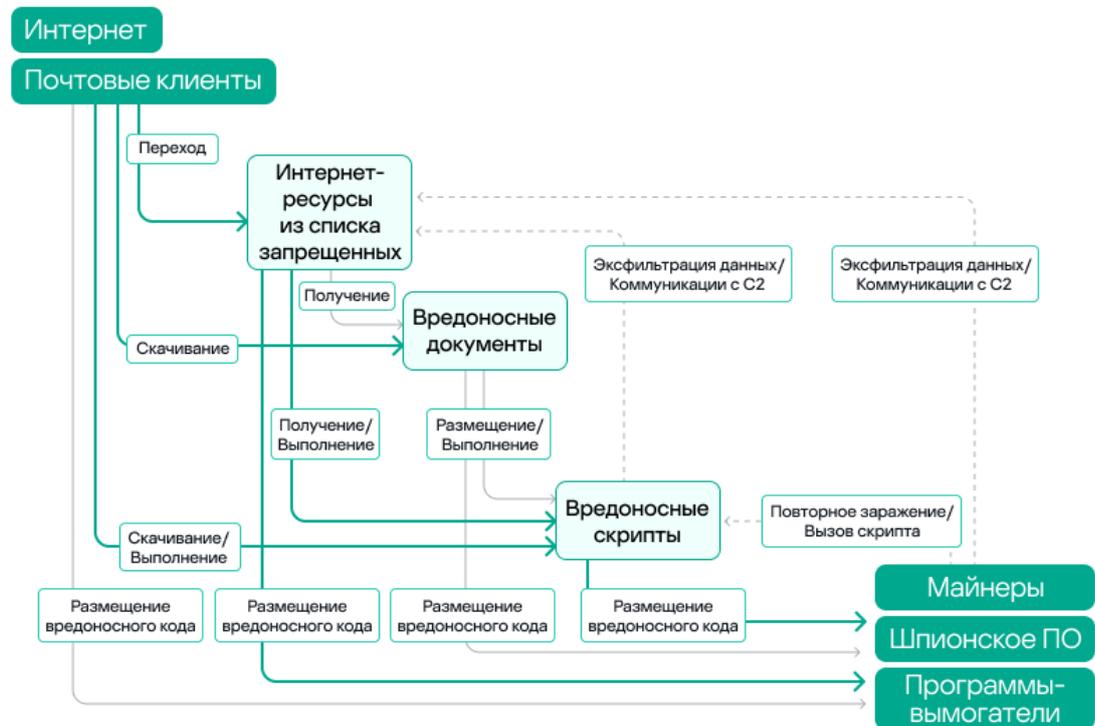
Вредоносные объекты, которые используются для первичного заражения компьютеров АСУ, — опасные ресурсы в интернете, которые попадают в списки запрещенных, вредоносные скрипты и фишинговые страницы, а также вредоносные документы.

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.

Цепочка атаки: от первичного заражения до вредоносного ПО следующего этапа

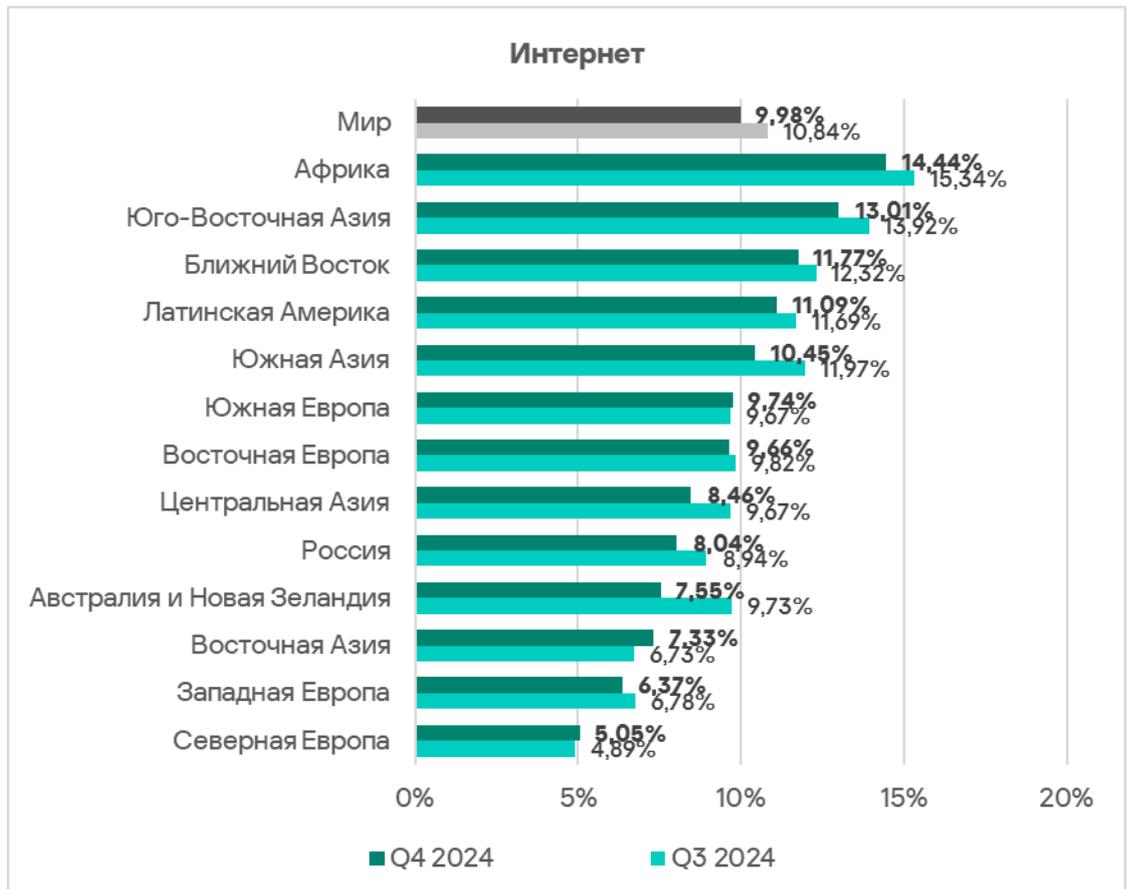


В мире и почти во всех регионах интернет-ресурсы из списка запрещенных, а также вредоносные скрипты и фишинговые страницы занимают первые места в рейтингах категорий вредоносных объектов по доле компьютеров АСУ, на которых они были заблокированы.

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

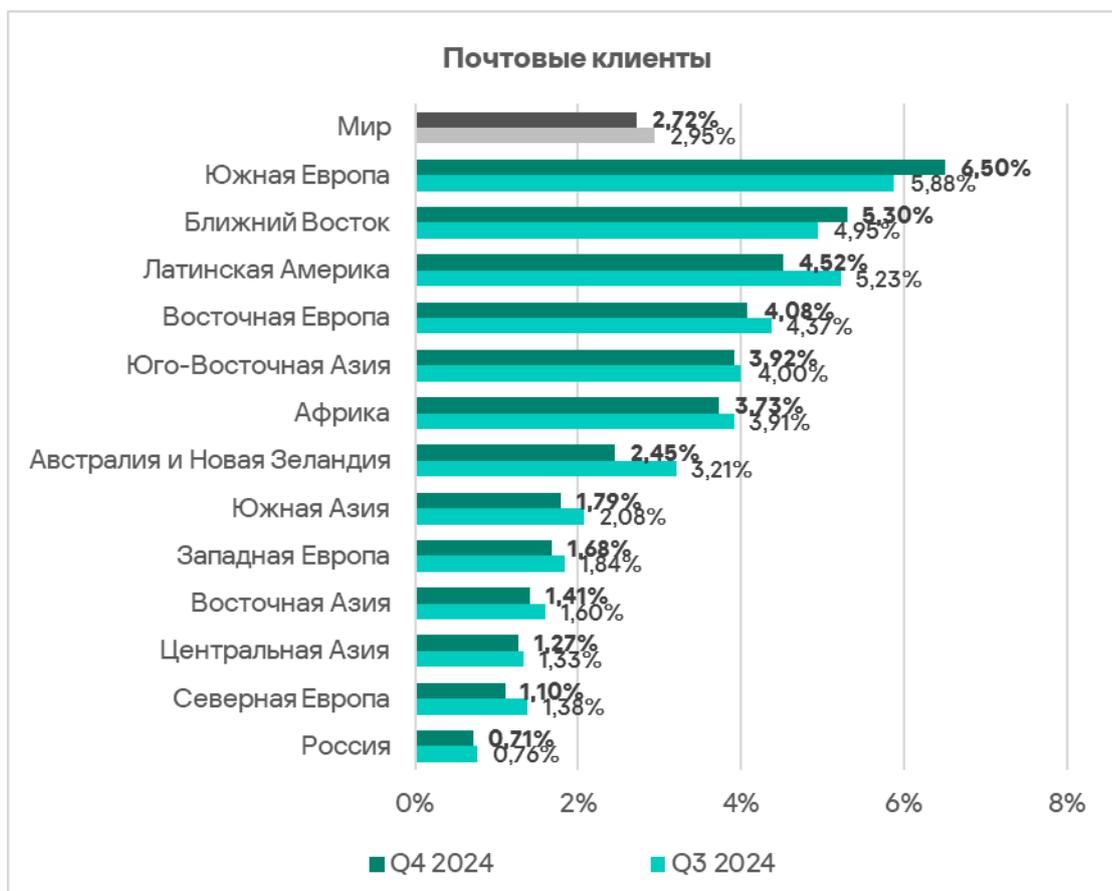
Топ 3 регионов по доле компьютеров АСУ, на которых в четвертом квартале 2024 года были заблокированы угрозы из интернета: **Африка, Юго-Восточная Азия** и **Ближний Восток**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, за четвертый квартал 2024 года



Топ 3 регионов по уровню угроз из почтовых клиентов: **Южная Европа, Ближний Восток** и **Латинская Америка**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, за четвертый квартал 2024 года



Ресурсы в интернете из списка запрещенных

Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных: **Африка, Юго-Восточная Азия** и **Центральная Азия**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, за четвертый квартал 2024 года



Во всех регионах, за исключением **Восточной Азии**, наблюдалось **снижение** доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных.

Как отмечалось в нашем [отчете за третий квартал 2024 года](#), увеличение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, главным образом обусловлен ростом количества вновь созданных доменных имен и IP-адресов, используемых киберпреступниками в качестве инфраструктуры управления и контроля (C2) для распространения вредоносного ПО и фишинговых атак.

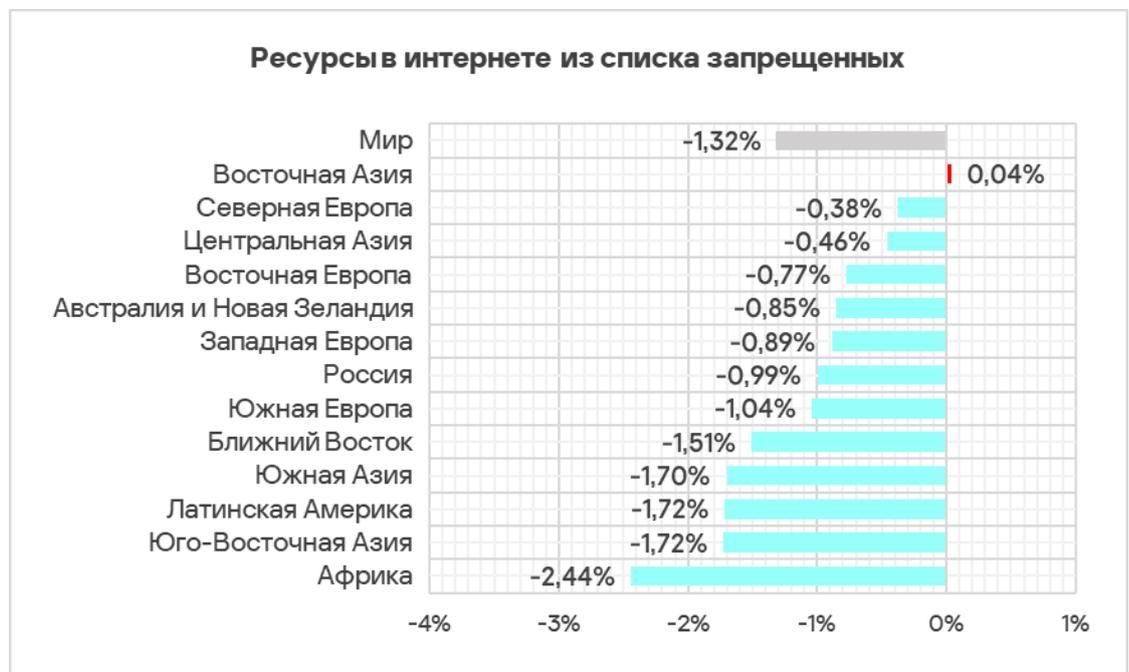
На снижение доли вредоносных и потенциально опасных веб-ресурсов в ноябре-декабре 2024 года, вероятно, повлияли не только решительные меры по противодействию угрозам, реализуемые на различных уровнях — начиная от владельцев ресурсов, хостинг- и интернет-провайдеров и заканчивая правоохранными органами. Другой один возможный фактор —

стремление злоумышленников менять доменные имена и IP-адреса в попытке избежать обнаружения на первом этапе — по списку уже известных интернет ресурсов.

На практике это означает, что до тех пор, пока вредоносный интернет-ресурс не будет обнаружен и добавлен в список запрещенных, он не отражается в статистике, что, очевидно, ведет к снижению показателя по опасным веб-ресурсам.

Но вместе с тем в четвертом квартале наблюдался рост доли для следующего компонента в цепочке атаки — вредоносных скриптов и фишинговых страниц, шпионского ПО и программ-вымогателей.

Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, за четвертый квартал 2024 года



Вредоносные скрипты и фишинговые страницы

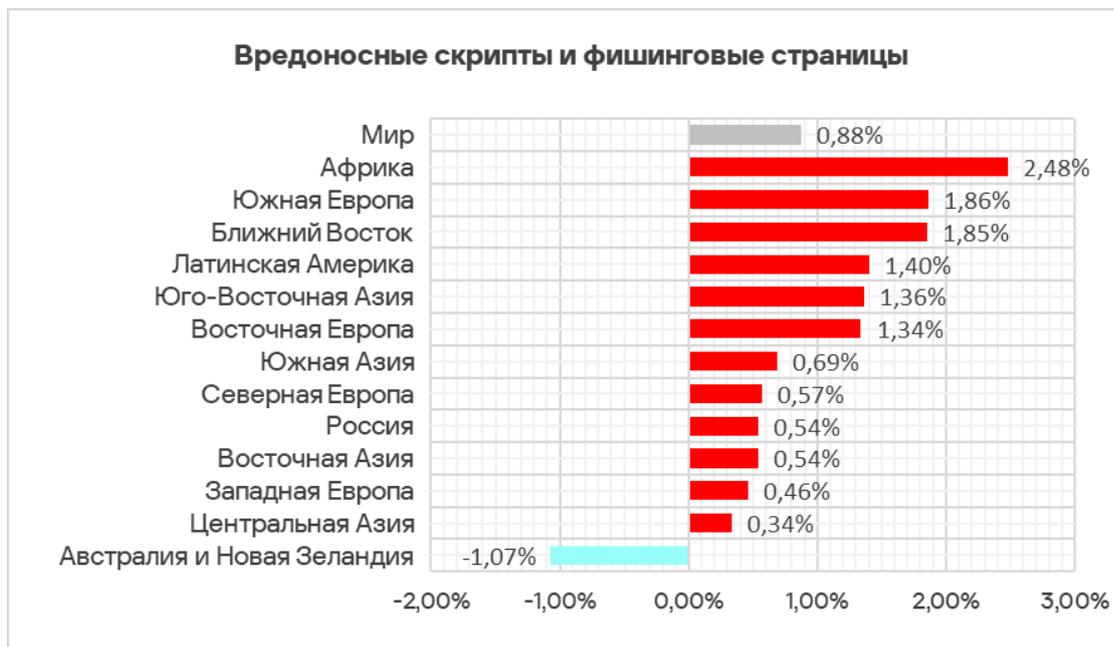
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы: **Африка, Южная Европа и Латинская Америка.**

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, за четвертый квартал 2024 года



Тройку лидеров **по росту** этого показателя составляют **Африка, Южная Европа и Ближний Восток.**

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, за четвертый квартал 2024 года



Вредоносные документы

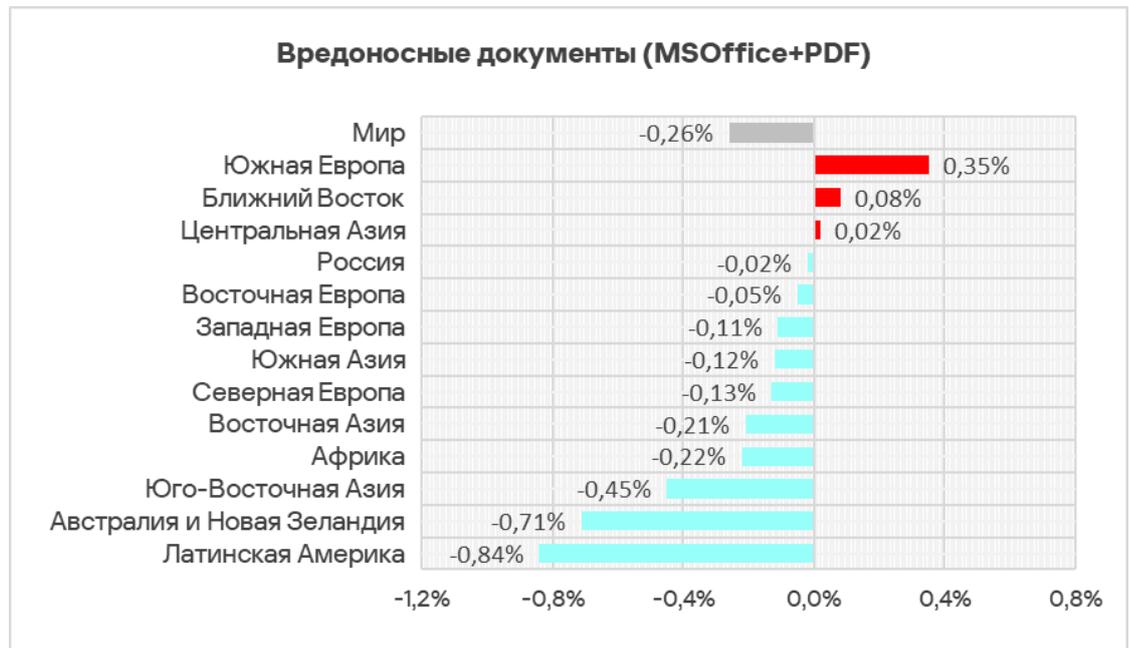
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы: **Южная Европа, Латинская Америка** и **Ближний Восток**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, за четвертый квартал 2024 года



Единственные регионы, где наблюдался **рост** этого показателя: **Южная Европа, Ближний Восток** и **Центральная Азия**.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные документы, за четвертый квартал 2024 года



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.

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.

Шпионские программы

Шпионское ПО (троянцы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструмент 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).

В четвертом квартале 2024 года **топ 3** регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, составили **Африка, Ближний Восток** и **Южная Европа**. Эти регионы также входят в число лидеров по угрозам первичного заражения.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, за четвертый квартал 2024 года



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** — здесь программы-шпионы занимают **первое место в рейтинге категорий** вредоносного ПО по доле компьютеров АСУ, на которых они были заблокированы;
- **Ближний Восток, Южная Европа и Центральная Азия** — 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, Россия** и **Центральная Азия**.

Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, за четвертый квартал 2024 года



Программы для скрытого майнинга криптовалюты Майнеры – исполняемые файлы для ОС Windows

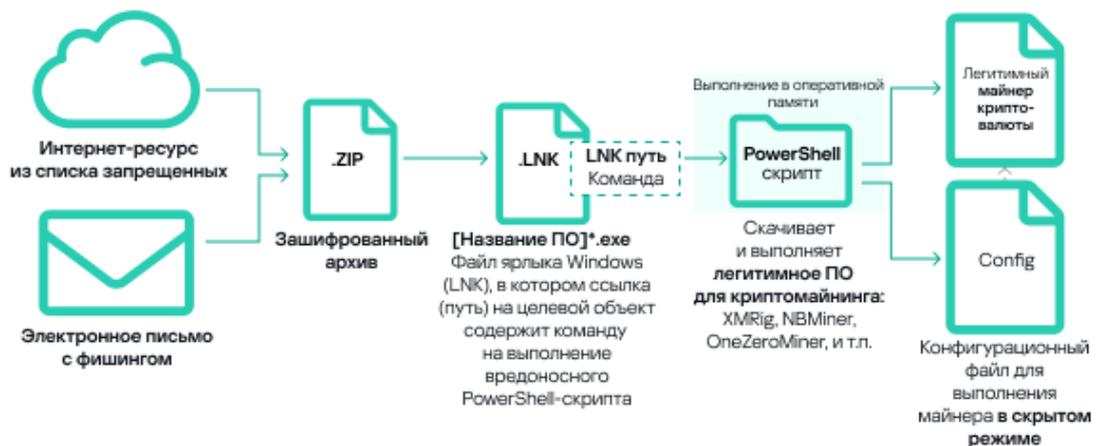
Значительная часть майнеров для ОС Windows, обнаруженных на компьютерах АСУ в четвертом квартале 2024 года, точно так же, как и кварталом ранее, представляла собой архивы с именами, имитирующими легальное программное обеспечение. В этих архивах не было ПО как такового, но содержался файл ярлыка Windows (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



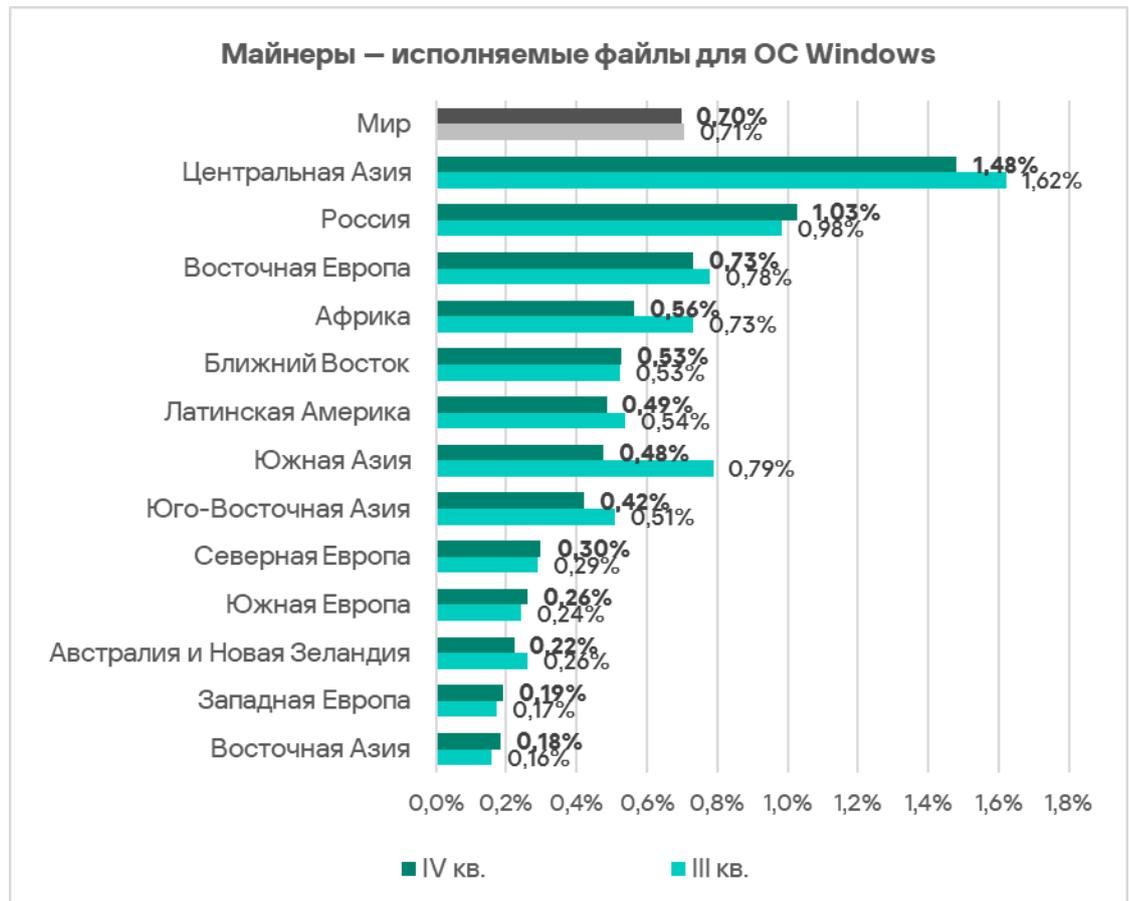
Еще одним популярным методом внедрения майнеров в технологическую инфраструктуру является использование легитимных криптомайнеров, таких как XMRig, NBMiner, OneZeroMiner и т. д. Сами по себе эти майнеры не являются вредоносными, однако защитные системы классифицируют их как [RiskTools](#). Злоумышленники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

Цепочка атаки:
пример
с использова-
нием
легитимных
криптомайне-
ров



Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows: **Центральная Азия, Россия и Восточная Европа.**

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, за четвертый квартал 2024 года

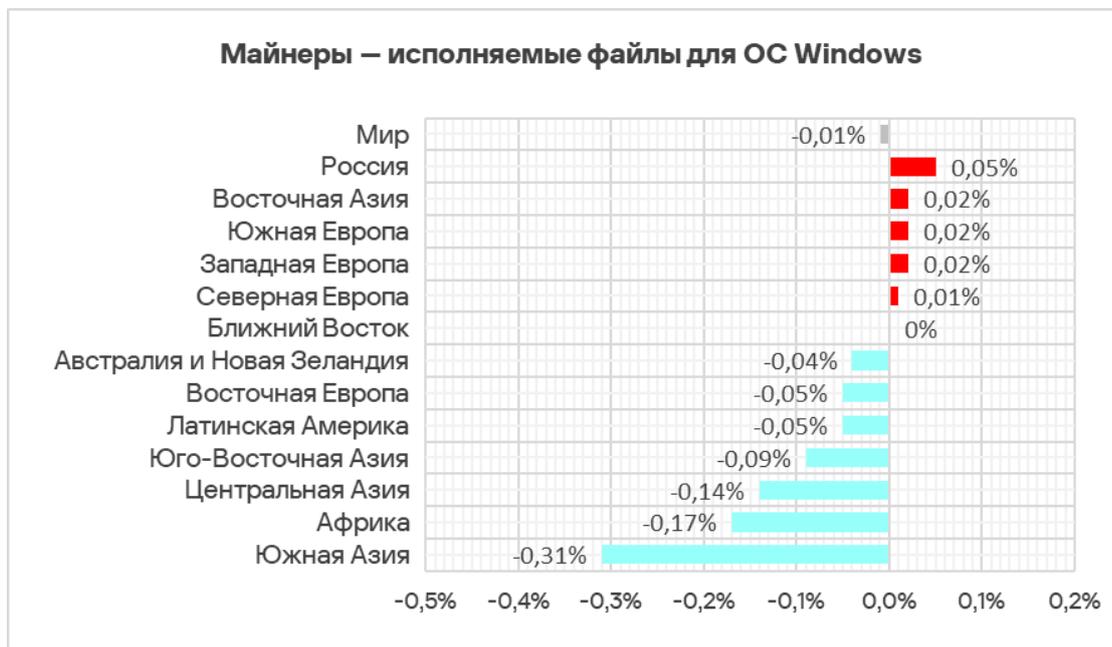


В мире в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows находятся на седьмом месте.

В аналогичном рейтинге в России, а также Австралии и Новой Зеландии они занимают пятое место.

Лидерами **по росту** этого показателя в четвертом квартале 2024 года являются **Россия, Восточная Азия, Южная Европа и Западная Европа.**

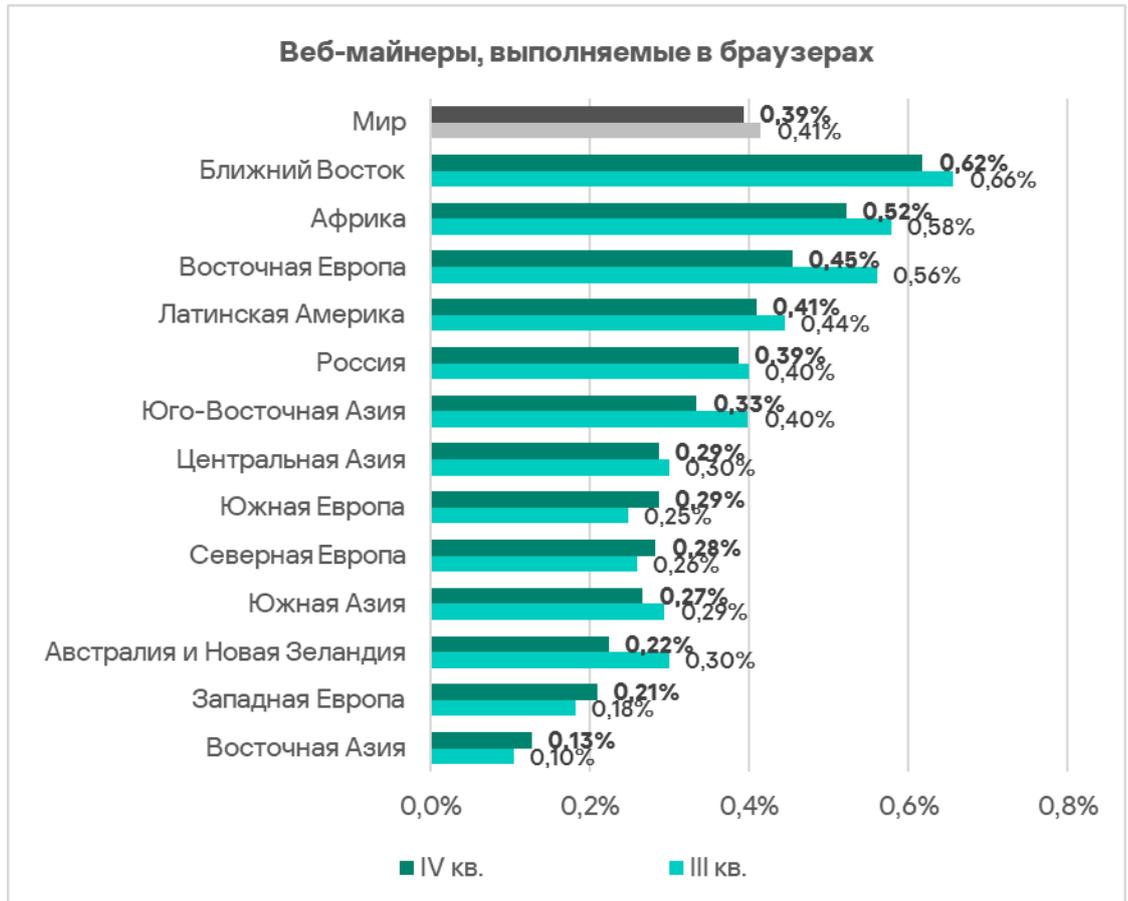
Изменение доли компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows, за четвертый квартал 2024 года



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

Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах: **Ближний Восток, Африка** и **Восточная Европа**.

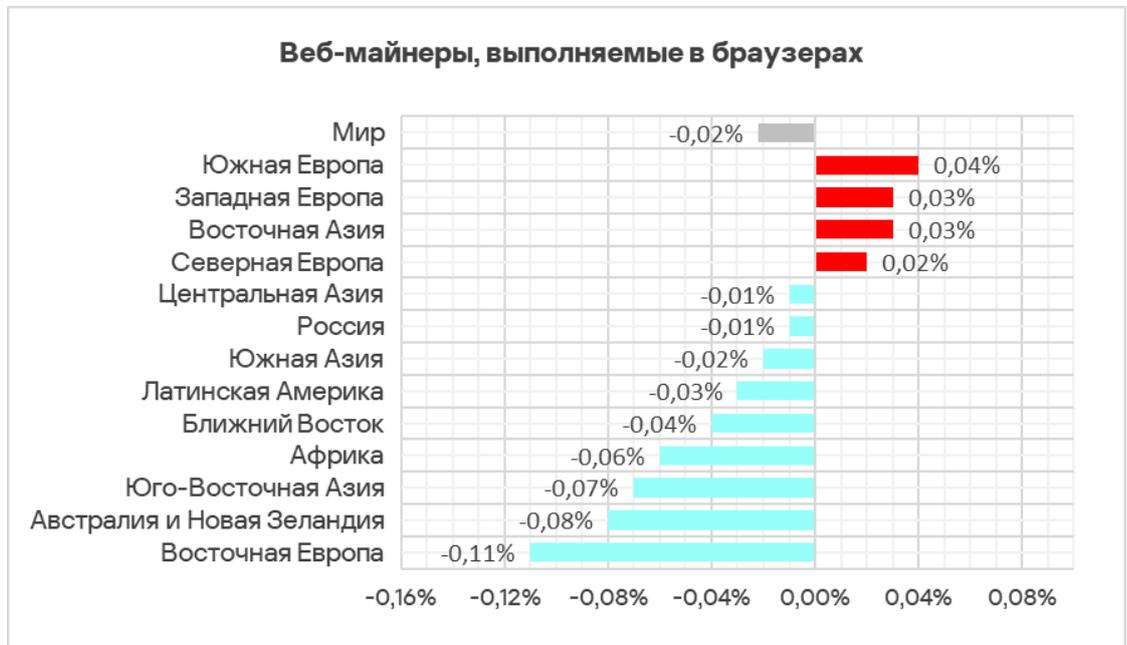
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, за четвертый квартал 2024 года



В **Австралии и Новой Зеландии**, а также **Западной Европе** веб-майнеры занимают более высокую позицию по доле компьютеров АСУ, на которых они были заблокированы, чем в мировом рейтинге — шестое место в регионе против восьмого в мире.

В четвертом квартале 2024 года **рост** доли компьютеров АСУ, на которых были заблокированы веб-майнеры, зафиксирован в **Южной Европе, Западной Европе, Северной Европе и Восточной Азии.**

Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, за четвертый квартал 2024 года



Программы-вымогатели

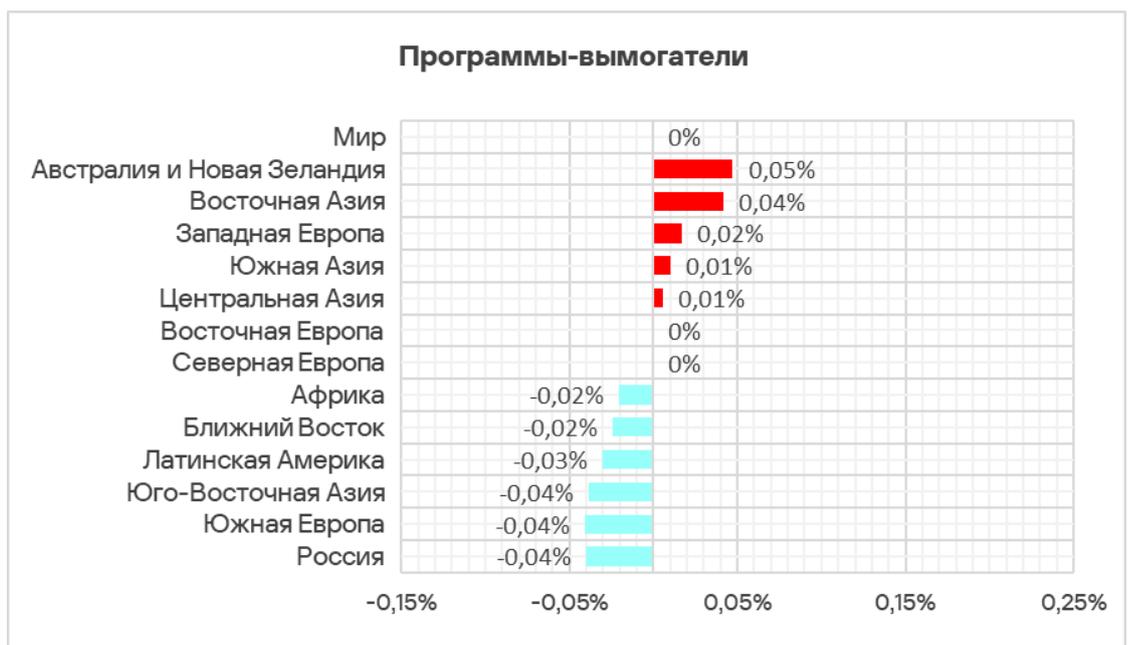
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели: **Ближний Восток, Африка и Южная Азия.**

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, за четвертый квартал 2024 года



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

Изменение доли компьютеров АСУ, на которых были заблокированы программы-вымогатели, за четвертый квартал 2024 года



Самораспространяющееся вредоносное ПО. Черви и вирусы

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

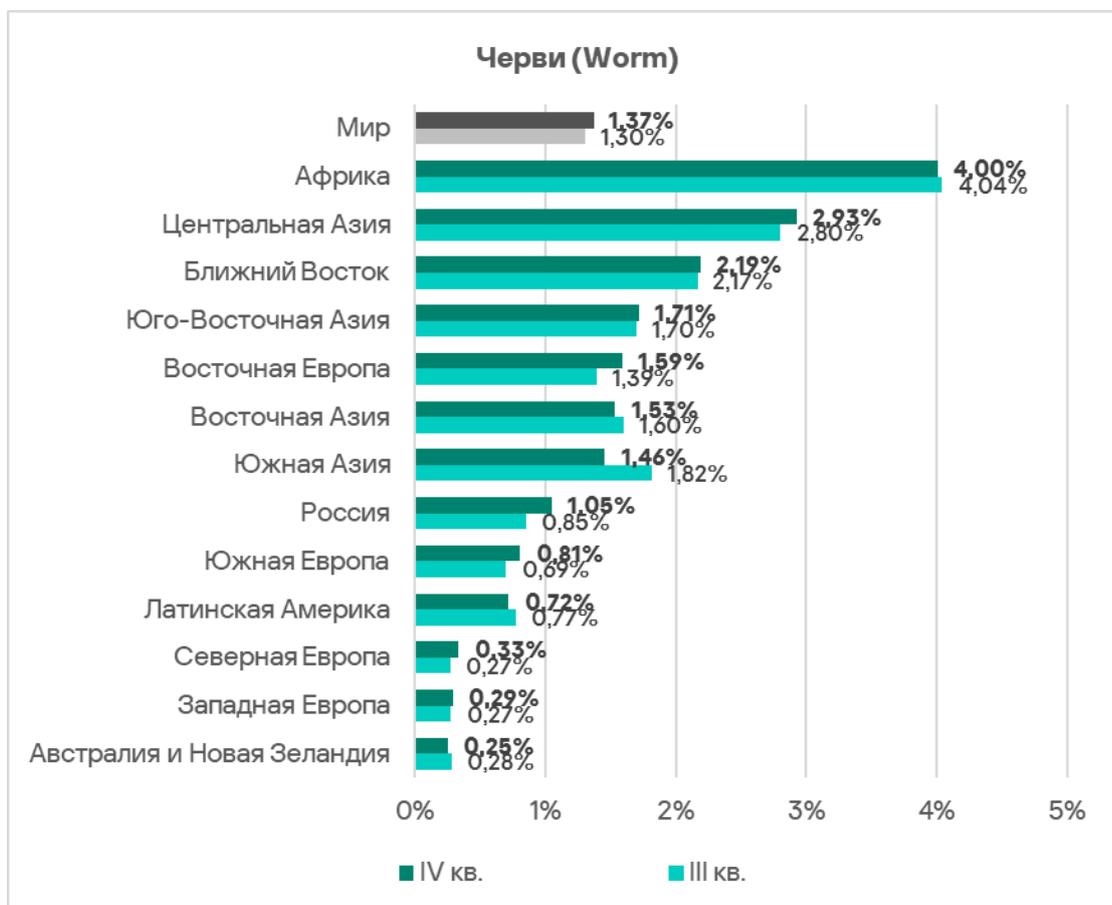
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО.

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

Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы черви: **Африка, Центральная Азия** и **Ближний Восток**.

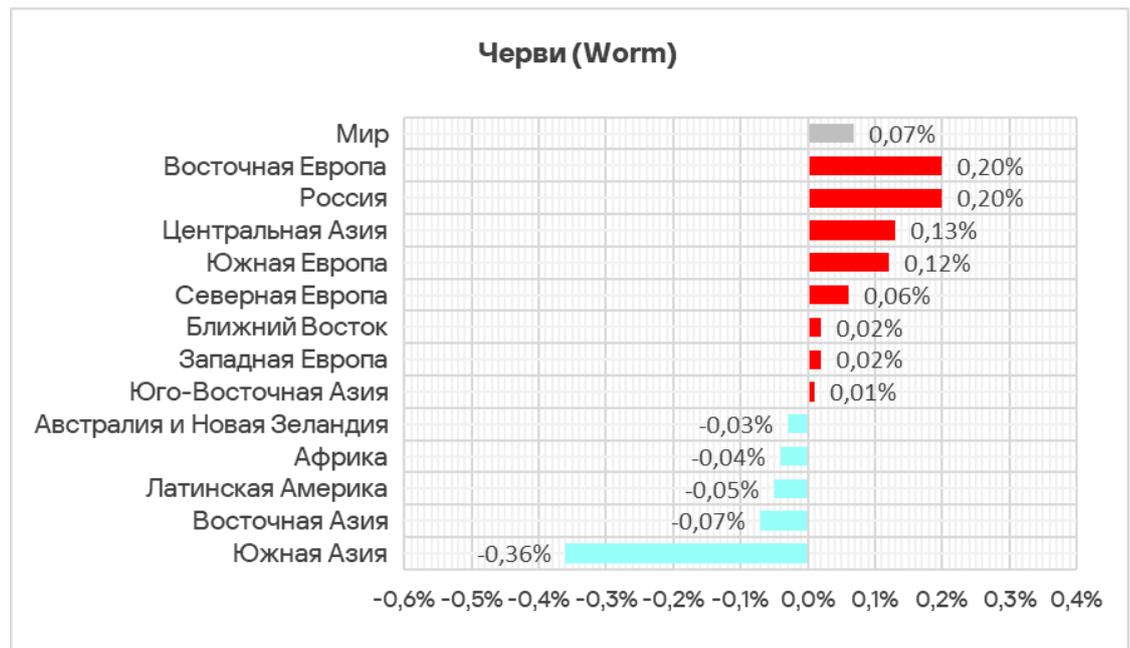
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы черви, за четвертый квартал 2024 года



В мире черви находятся на шестом месте в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. При этом в Африке, Центральной Азии и Южной Азии **черви занимают более высокую позицию** — четвертое место в соответствующих региональных рейтингах.

Тройку лидеров **по росту** этого показателя составляют **Восточная Европа, Россия и Центральная Азия**.

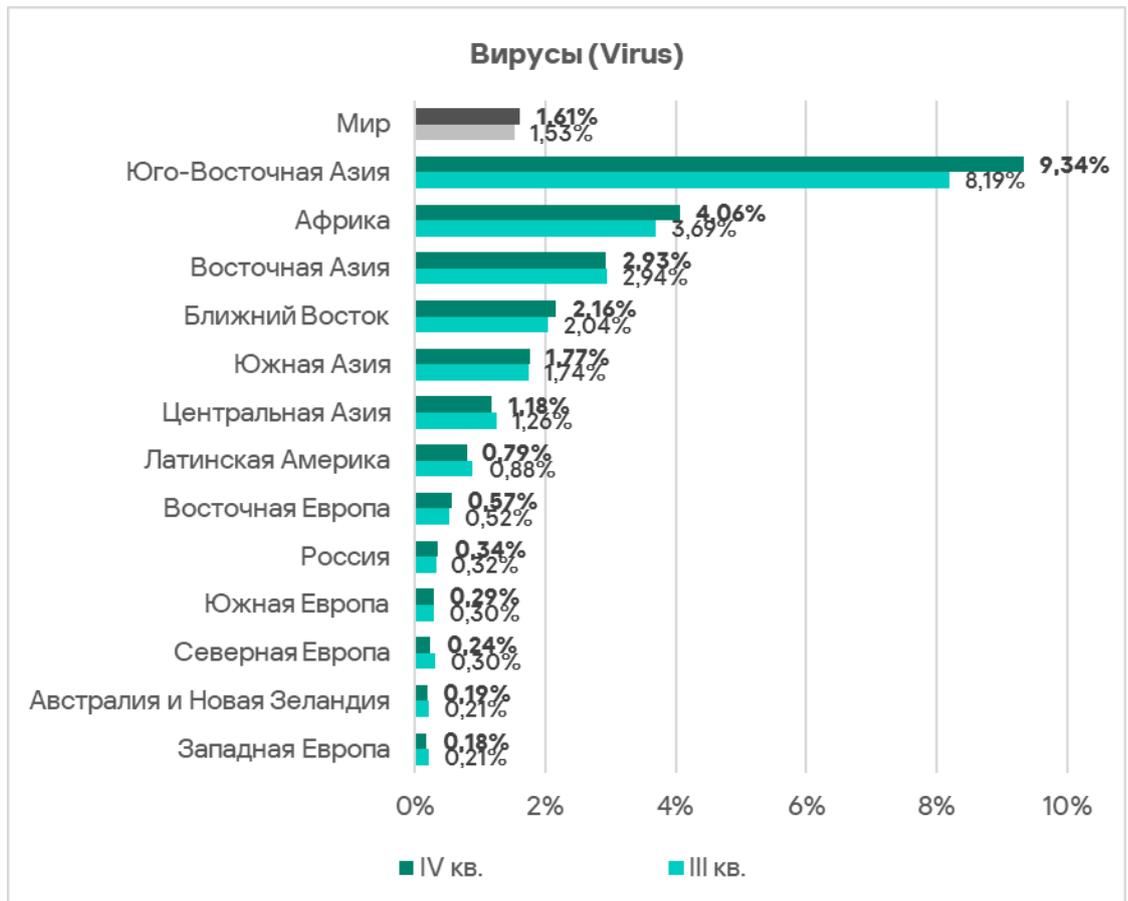
Изменение доли компьютеров АСУ, на которых были заблокированы черви, за четвертый квартал 2024 года



Вирусы

Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вирусы: **Юго-Восточная Азия, Африка и Восточная Азия**.

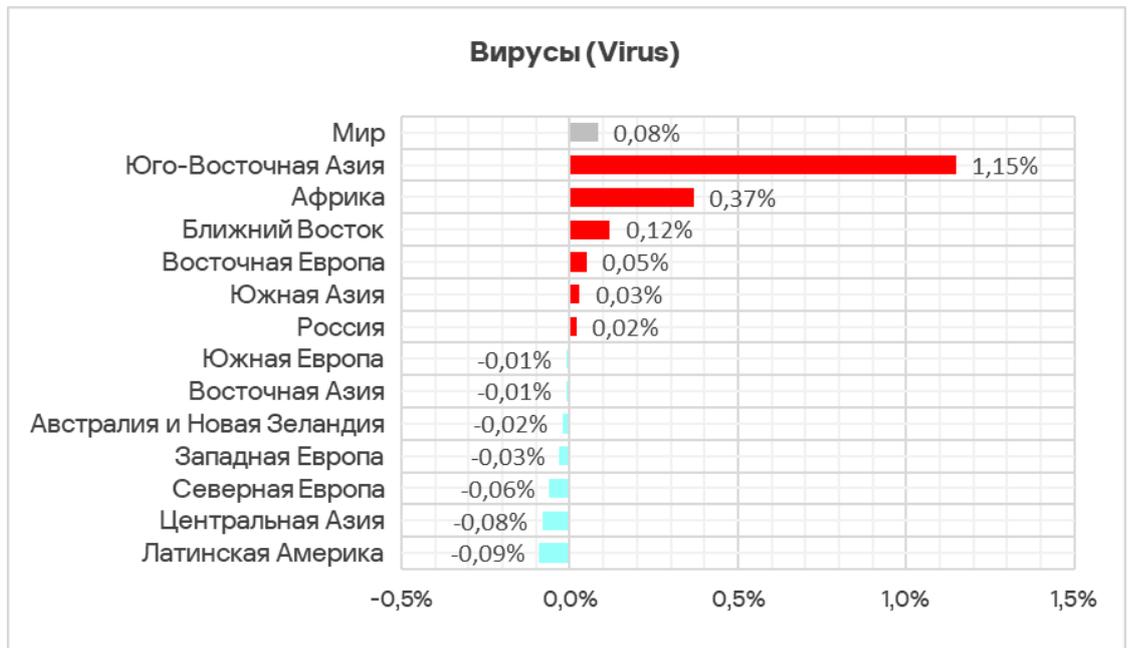
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, за четвертый квартал 2024 года



В **Юго-Восточной Азии** вирусы находятся **на втором месте** в региональном рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

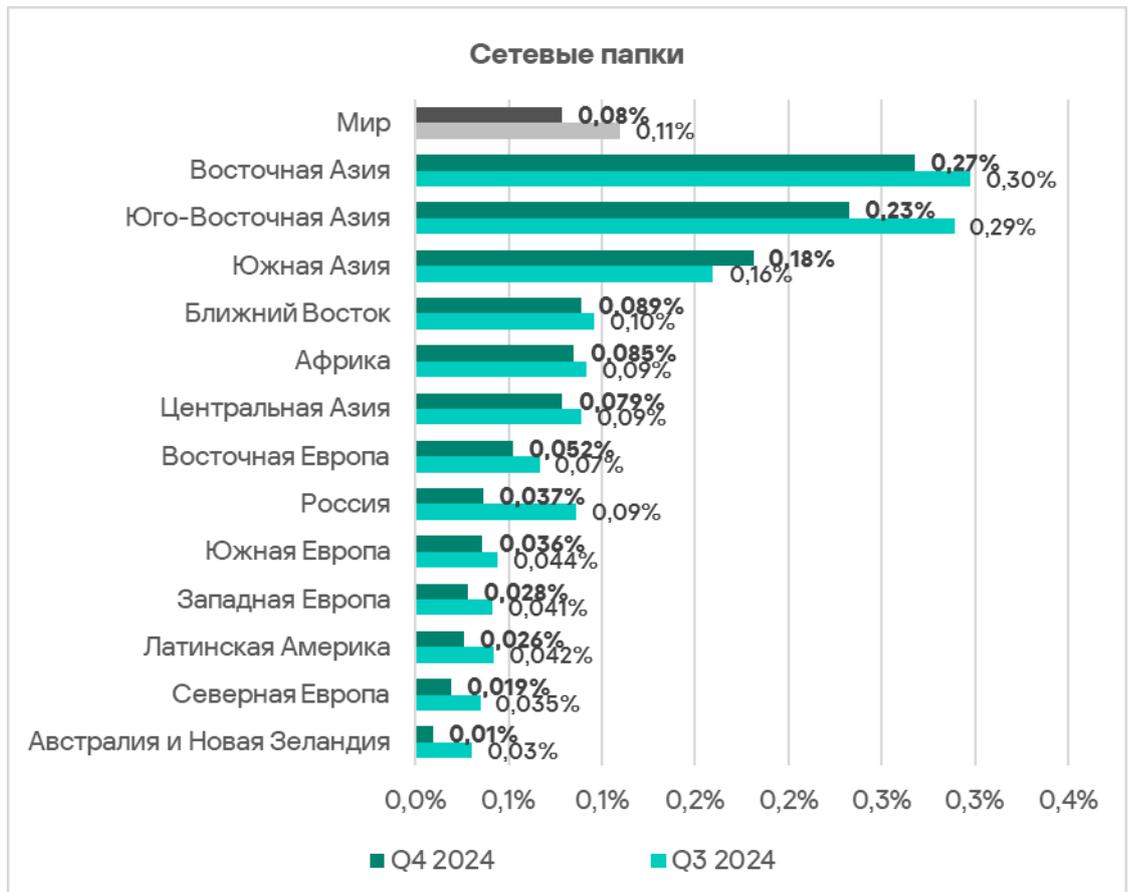
Тройку лидеров **по росту** этого показателя составляют **Юго-Восточная Азия, Африка** и **Ближний Восток**.

Изменение доли компьютеров АСУ, на которых были заблокированы вирусы, за четвертый квартал 2024 года



Отметим, что список регионов в верхней части рейтинга по доле компьютеров АСУ, на которых были заблокированы вирусы, во многом совпадает со списком регионов в верхней части рейтинга **угроз в сетевых папках**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, за четвертый квартал 2024 года



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. Это **Юго-Восточная Азия, Восточная Азия** и **Африка**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, за четвертый квартал 2024 года



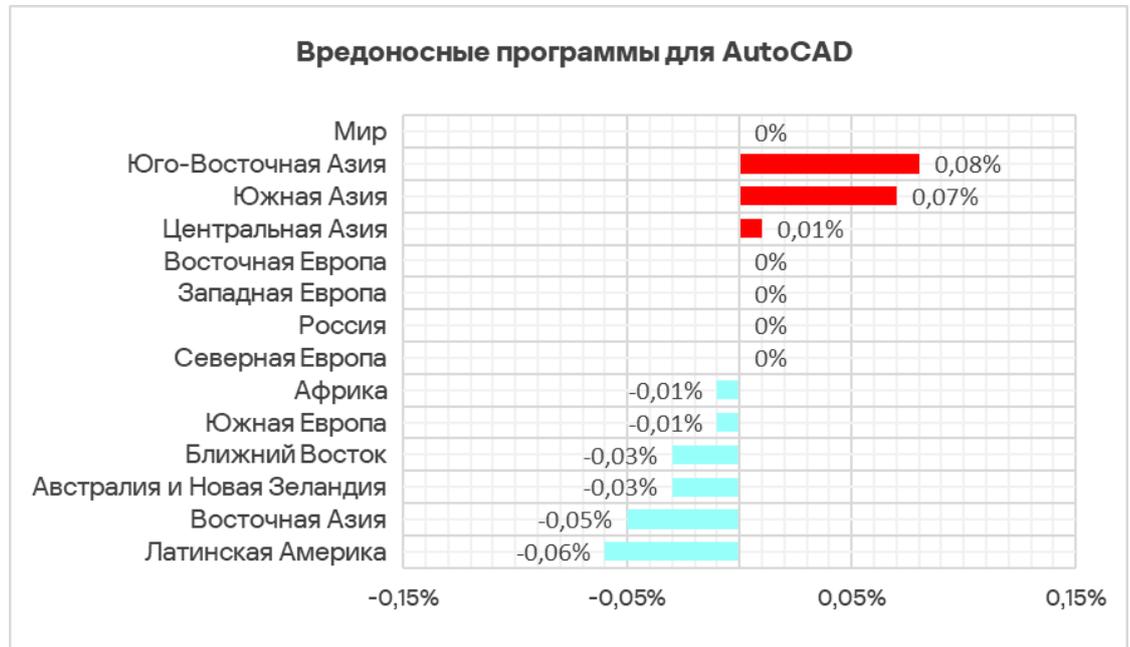
Обычно вредоносное ПО для AutoCAD представляет собой незначительную угрозу и чаще всего занимает последние места в рейтингах категорий вредоносного ПО по доле компьютеров АСУ, на которых оно было заблокировано.

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

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

Два региона-лидера **по росту** этого показателя: **Юго-Восточная Азия** и **Южная Азия**.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, за четвертый квартал 2024 года



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.

Африка

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>10,95% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,3x рост в IV кв. 2024 г. 2-е место по росту</p> <p>🌐 1-е место в мире 1,5x выше среднего по миру</p>	<p>8,53% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1-е место в мире 1,5x выше среднего по миру</p>	<p>7,13% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p> <p>🌐 1-е место в мире 1,7x выше среднего по миру</p>
<p>4,06% ВИРУСЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p> <p>🌐 1-е место в мире 2,5x выше среднего по миру</p>	<p>4,00% ЧЕРВИ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1-е место в мире 2,9x выше среднего по миру</p>	<p>2,04% ВРЕДНОСНЫЕ ДОКУМЕНТЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,2x выше среднего по миру</p>
<p>0,54% ВРЕДНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,4x выше среднего по миру</p>	<p>0,52% ВЕБ-МАЙНЕРЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 2-е место в мире 1,3x выше среднего по миру</p>	<p>0,26% ПРОГРАММЫ- ВЫМОГАТЕЛИ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 2-е место в мире 1,2x выше среднего по миру</p>
<p>14,44% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>3,73% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>3,09% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>

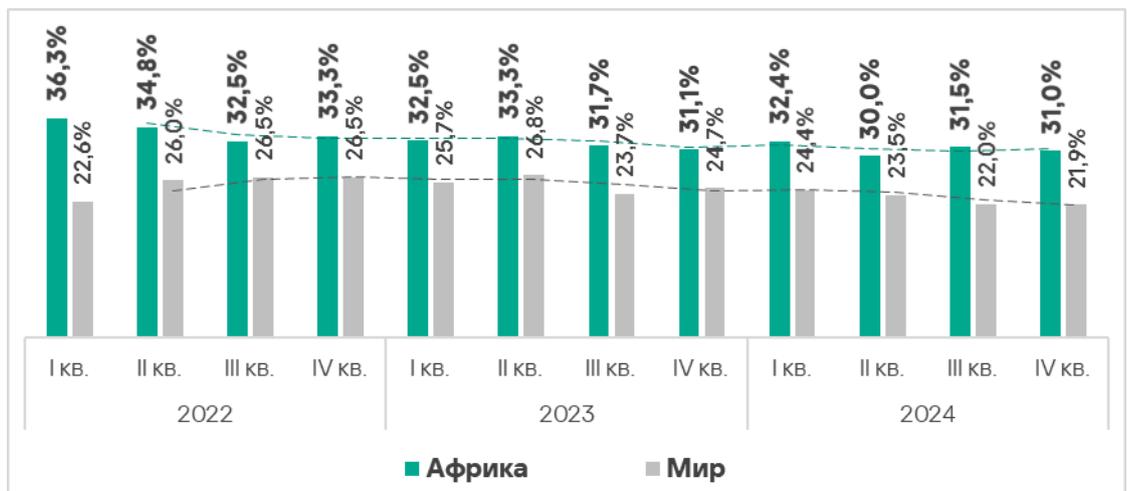
🌐 1-е место в мире
1,4x выше среднего
по миру

🌐 1,4x выше среднего
по миру

🌐 1-е место в мире
4,8x выше среднего
по миру

Общая ситуация

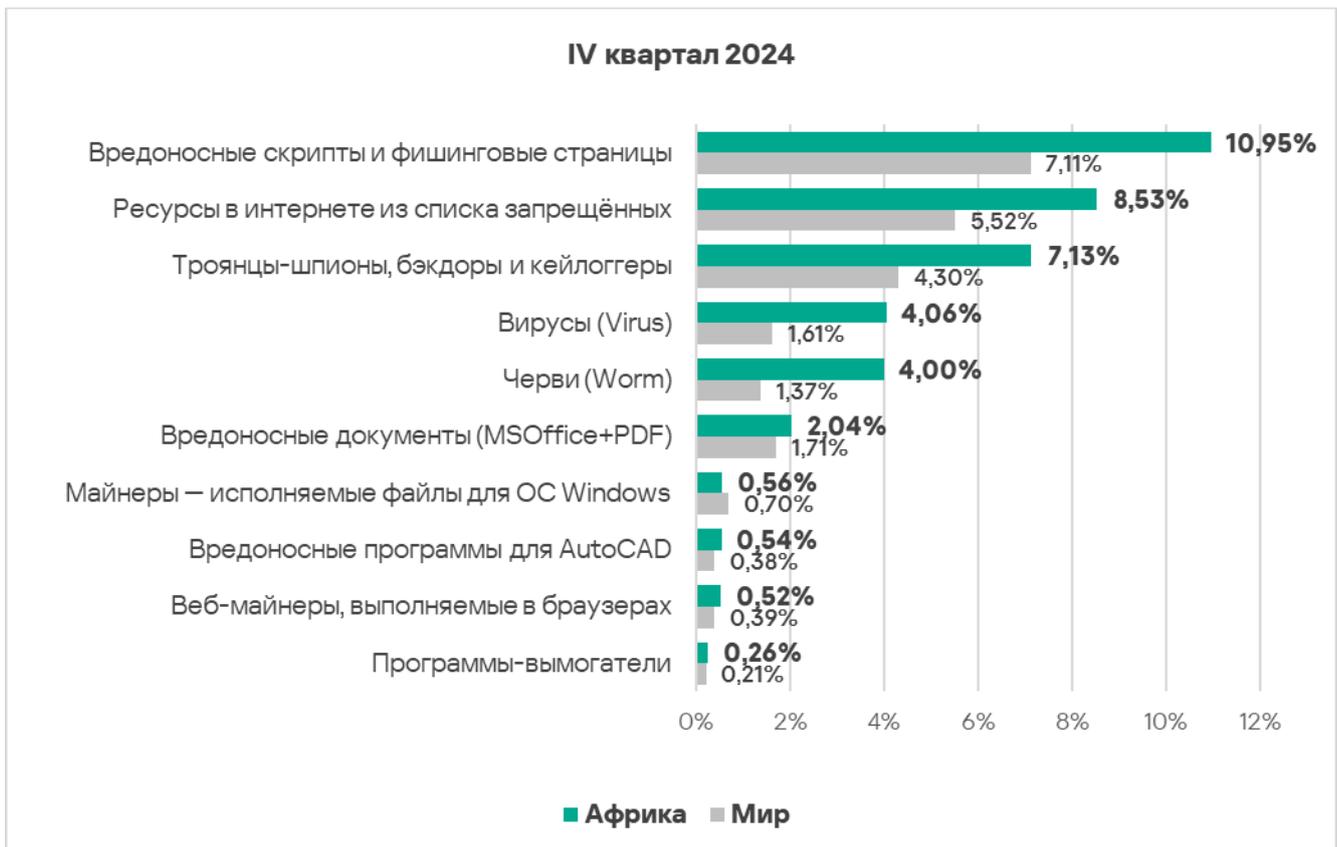
- Африка традиционно занимает **первое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Регион возглавляет многие рейтинги, в некоторых случаях с огромным отрывом.
- Показатель здесь стабильно **превышает среднемировое значение**. В **четвертом квартале 2024 года** он выше среднемирового уровня в 1,4 раза.
- При этом доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, снизилась.
- В регионе наблюдается незначительный **нисходящий тренд** с колебаниями.



Сравнительный анализ

Категории угроз

- В регионе у **всех категорий угроз** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выше среднемирового значения.**



- В регионе значительно **выше, чем в среднем по миру**, доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
 - черви — в 2,9 раза, первое место в мире;
 - вирусы — в 2,5 раза (также выше значения за третий квартал 2024 года), второе место в мире.
- 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, первое место в мире;
- ресурсы в интернете из списка запрещенных — в 1,5 раза, первое место в мире;
- вредоносные скрипты и фишинговые страницы — в 1,5 раза (также выше значения за третий квартал 2024 года), первое место в мире;
- вредоносные программы для AutoCAD — в 1,4 раза, третье место в мире;
- веб-майнеры — в 1,3 раза, второе место в мире;
- программы-вымогатели — в 1,2 раза, второе место в мире;
- вредоносные документы — в 1,2 раза (также выше значения за третий квартал 2024 года).

Источники угроз

- Африка занимает **первое место** по доле компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, а также со **съёмных носителей**. Значения заметно превышают среднемировые показатели:
 - угрозы со съёмных носителей — в 4,8 раза (также выше значения за третий квартал 2024 года);
 - угрозы из интернета — в 1,4 раза.
- Что касается угроз из **почтовых клиентов**, то здесь региональное значение превышает среднемировой уровень в 1,4 раза (также выше значения за третий квартал 2024 года).



Изменения за квартал и тренды

Категории угроз

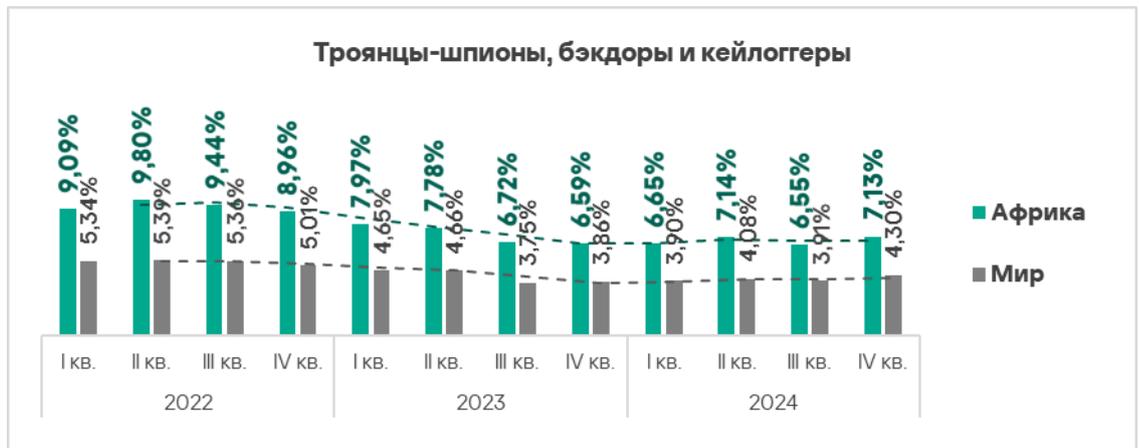


Наиболее существенно в четвертом квартале 2024 года **выросла** доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

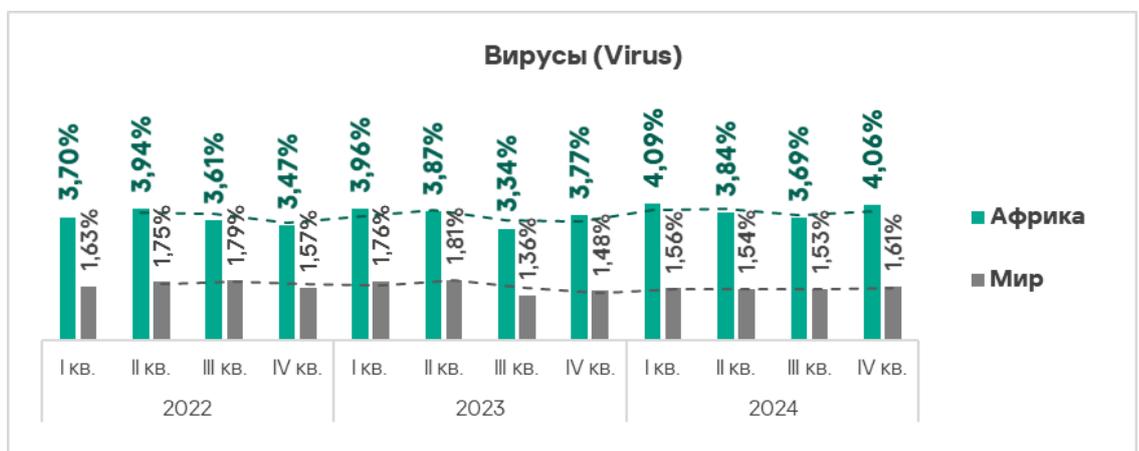
- вредоносные скрипты и фишинговые страницы — в 1,3 раза, первое место по росту показателя в мире;



- шпионское ПО — в 1,1 раза;



➤ вирусы — в 1,1 раза, второе место по росту показателя в мире.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Африке с начала 2022 года. В четвертом квартале 2024 года **вредоносные скрипты и фишинг** вернулись со второго места на первое, а **вирусы** — с пятого на четвертое.

Африка	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	2	2	2	2	2	3	2	1
Ресурсы в интернете из списка запрещенных	2	3	3	2	1	1	1	1	1	1	1	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	2	2	3	3	3	3	3	3	2	3	3
Вирусы (Virus)	6	6	6	6	5	5	5	5	5	5	5	4
Черви (Worm)	4	5	4	4	4	4	4	4	4	4	4	5
Вредоносные документы (MSOffice+PDF)	5	4	5	5	6	6	6	6	6	6	6	6
Майнеры – исполняемые файлы для ОС Windows	7	7	8	8	8	8	8	7	7	7	7	7
Вредоносные программы для AutoCAD	10	9	9	9	9	9	9	9	9	9	9	8
Веб-майнеры, выполняемые в браузерах	8	8	7	7	7	7	7	8	8	8	8	9
Программы-вымогатели	9	10	10	10	10	10	10	10	10	10	10	10

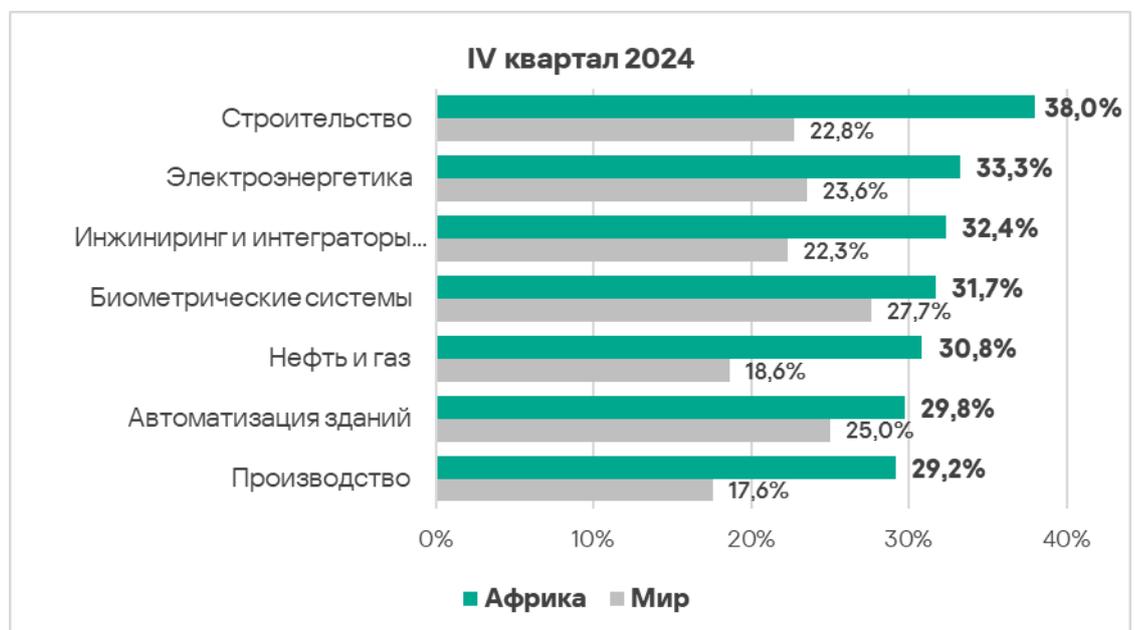
Источники угроз

В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

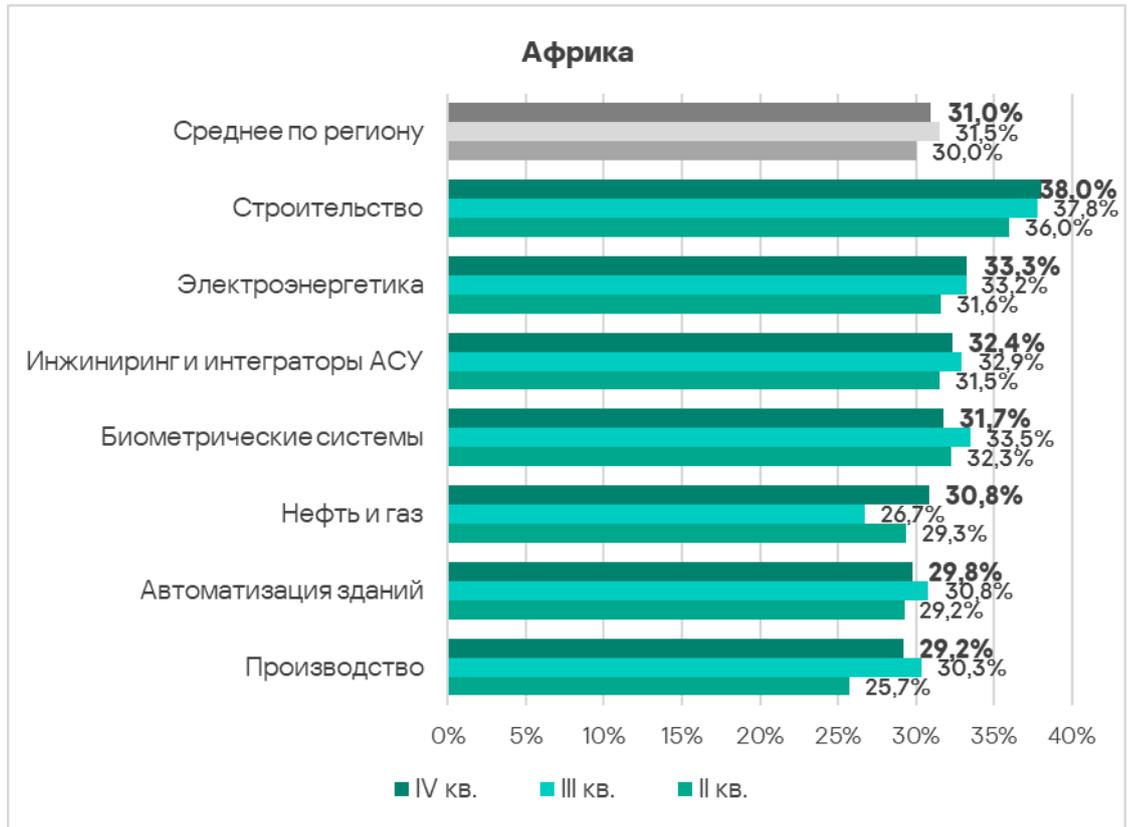


Отрасли

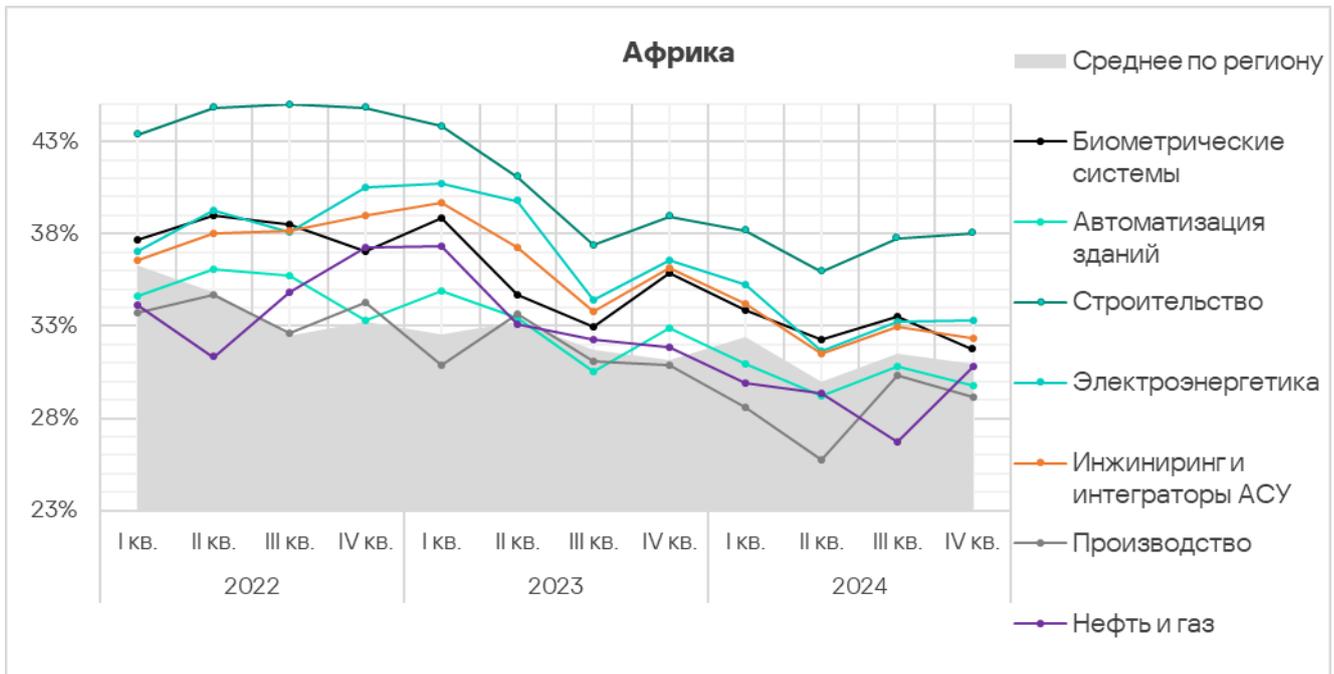
- **Наиболее часто встречающейся с угрозами отраслью** региона среди рассмотренных в отчете по-прежнему является **строительство**.
- По сравнению с соответствующими **среднемировыми показателями** значительно **более высокая доля компьютеров АСУ**, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:
 - строительство — в 1,7 раза;
 - производство — в 1,7 раза;
 - нефть и газ — в 1,7 раза;
 - инжиниринг и интеграторы АСУ — в 1,5 раза;
 - электроэнергетика — в 1,4 раза.



- В **четвертом квартале 2024 года** в нефтегазовой отрасли зафиксировано **заметное увеличение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты — в 1,2 раза по сравнению с предыдущим кварталом.



- Рассмотренные отрасли демонстрируют **положительную динамику долгосрочных трендов** с периодическими значительными колебаниями.



Юго-Восточная Азия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>9,59% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p> <p>▲ 1,3x выше среднего по миру</p>	<p>9,34% ВИРУСЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 1-е место по росту</p> <p>▲ 1-е место в мире 5,8x выше среднего по миру</p>	<p>6,09% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>▲ 2-е место в мире 1,1x выше среднего по миру</p>
<p>5,94% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p> <p>▲ 1,4x выше среднего по миру</p>	<p>2,83% ВРЕДНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD</p> <p>▲ слабый рост в IV кв. 2024 г. 1-е место по росту</p> <p>▲ 1-е место в мире 7,4x выше среднего по миру</p>	<p>1,87% ВРЕДНОСНЫЕ ДОКУМЕНТЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>▲ 1,1x выше среднего по миру</p>
<p>1,71% ЧЕРВИ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>▲ 1,2x выше среднего по миру</p>		
<p>13,01% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>3,92% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>0,23% СЕТЕВЫЕ ПАПКИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>



2-е место в мире
1,3x выше среднего
по миру



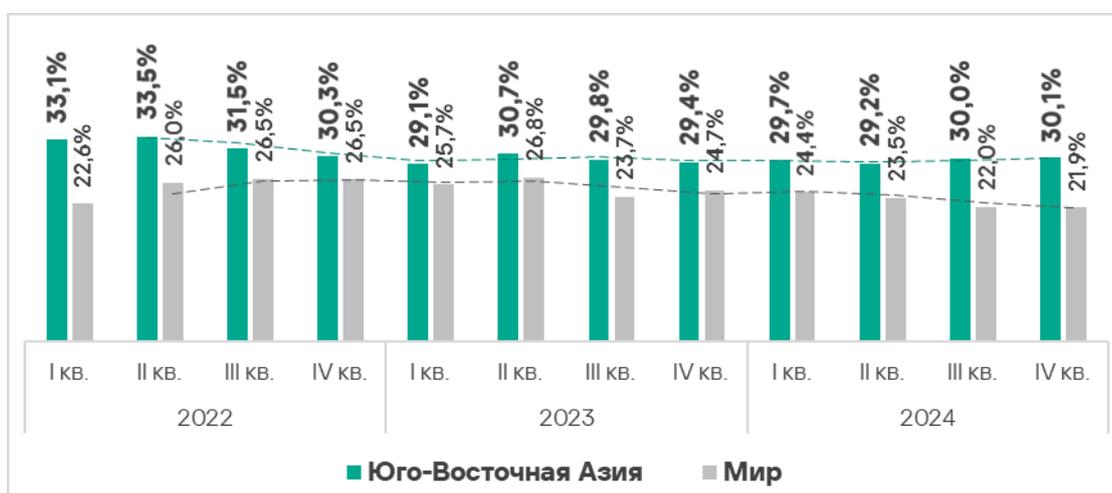
1,7x выше среднего
по миру



2-е место в мире
2,9x выше среднего
по миру

Общая ситуация

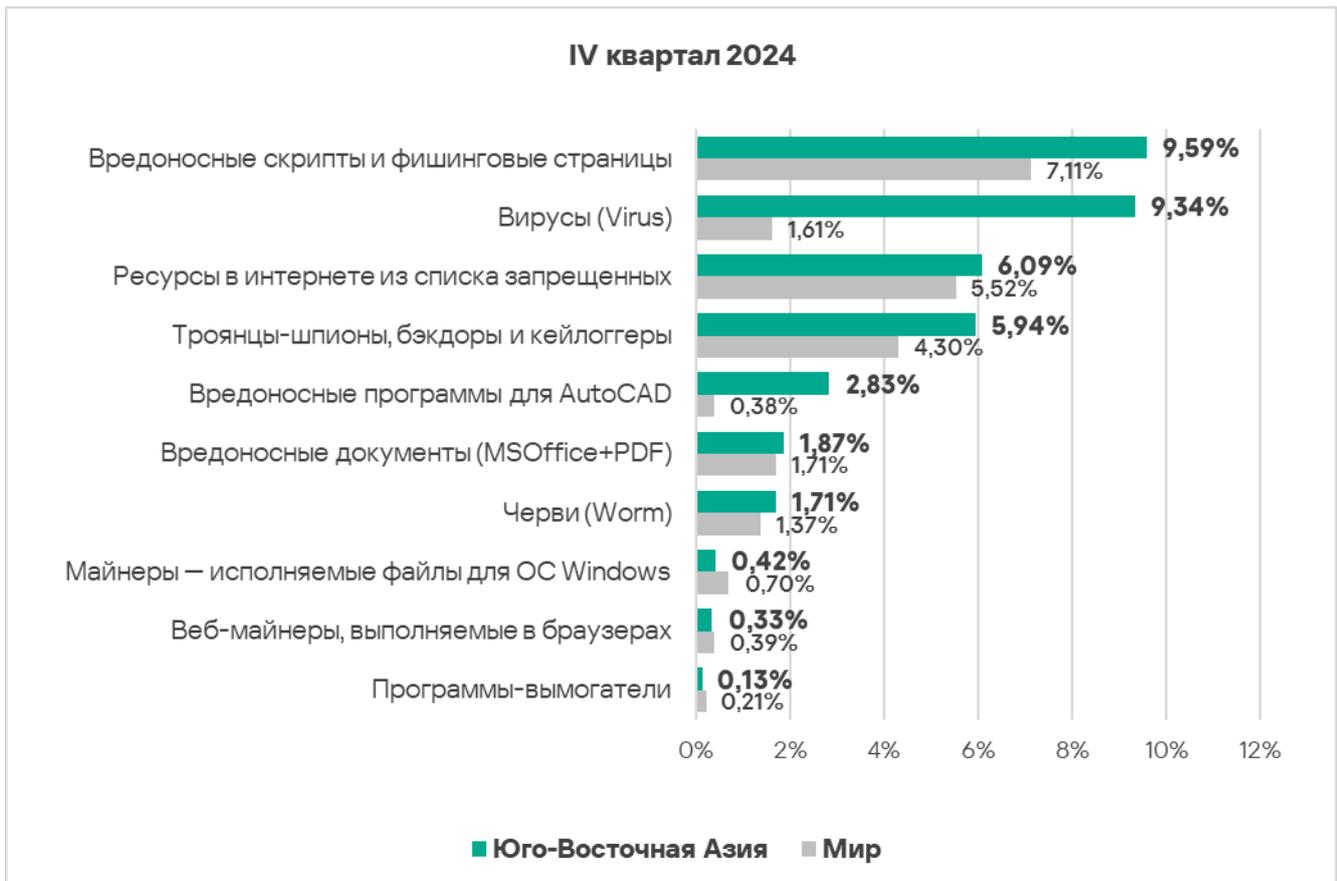
- Юго-Восточная Азия занимает **второе место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Этот показатель стабильно **превышает среднемировое значение**, что отражает долгосрочную тенденцию. В четвертом квартале 2024 года региональное значение выше среднемирового в 1,4 раза.
- В этом квартале года показатель снова **вырос**.



Сравнительный анализ

Категории угроз

- В регионе у **большинства категорий угроз** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выше среднемирового значения**.



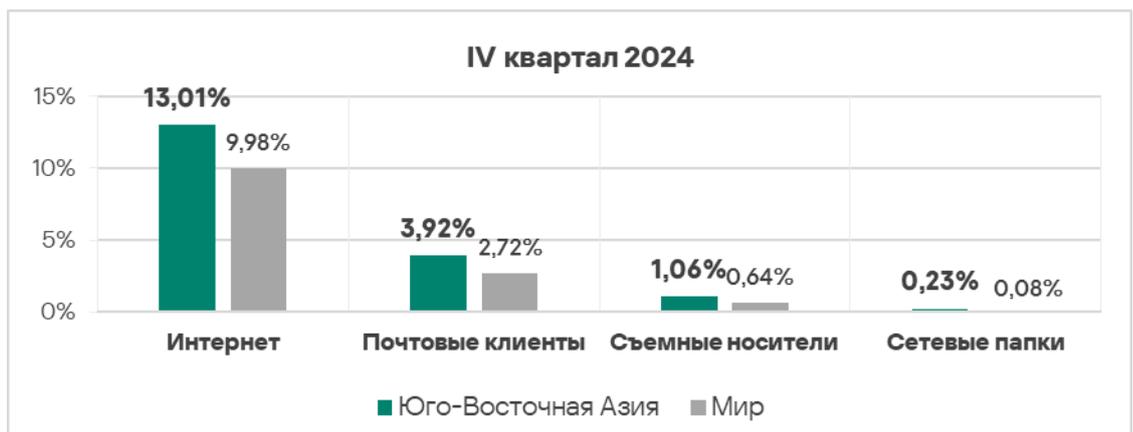
- В Юго-Восточной Азии **вирусы занимают второе место** в рейтинге категорий вредоносных программ по доле компьютеров АСУ, на которых они были заблокированы. Региональный показатель в 5,8 раза превышает среднемировой и является самым высоким значением в мире (также оно выше значения за третий квартал 2024 года).
- **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). Региональный показатель в 7,4 раза превышает среднемировой и тоже является самым высоким значением в мире (также оно выше значения за третий квартал 2024 года).
- **По сравнению с мировыми показателями** в регионе значительно **выше доля компьютеров АСУ**, на которых были заблокированы следующие категории вредоносных объектов:
 - шпионские программы — в 1,4 раза;
 - вредоносные скрипты и фишинговые страницы — в 1,3 раза;
 - черви — в 1,2 раза;
 - интернет-ресурсы из списка запрещенных — в 1,1 раза, второе место в мире;

- вредоносные документы — в 1,1 раза.

Источники угроз

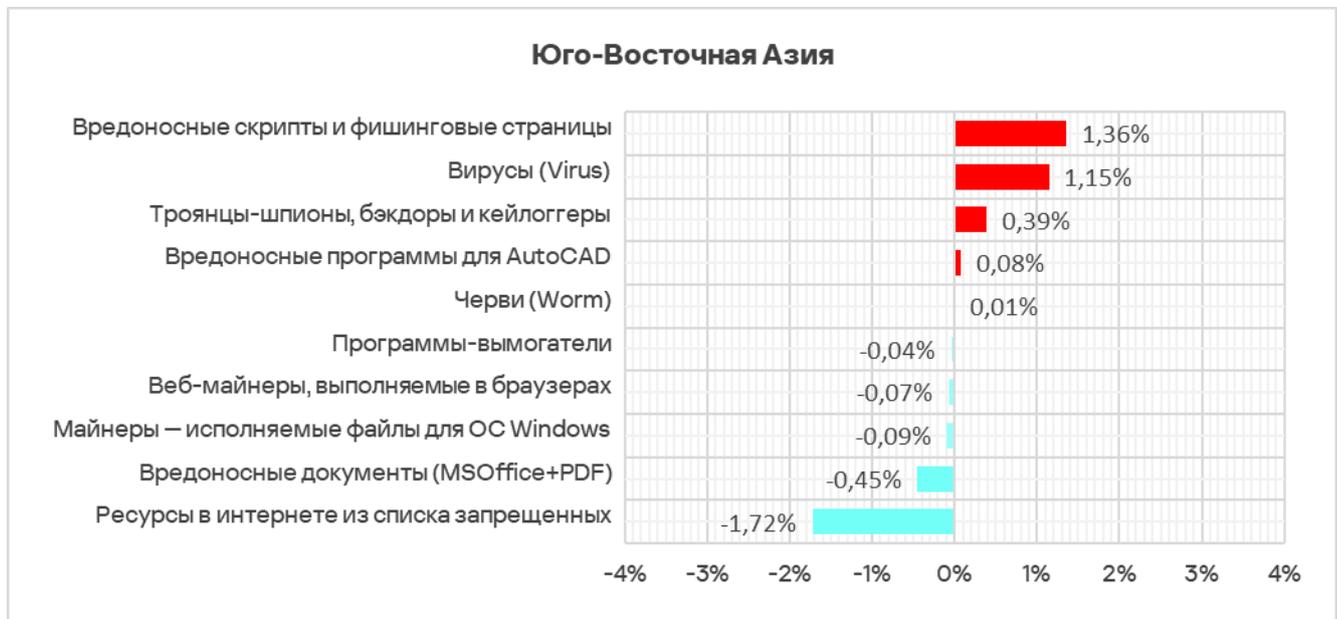
Юго-Восточная Азия занимает **второе место в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках**, с превышением среднемирового значения в 2,9 раза (показатель также выше значения за третий квартал 2024 года).

- По угрозам из **интернета** регион также находится **на втором месте в мире**. Этот показатель превышает среднемировое значение в 1,3 раза.
- Что касается доли компьютеров, на которых были заблокированы вредоносные объекты на **съёмных носителях**, то она превышает среднемировое значение в 1,7 раза.
- Доля компьютеров, на которых были заблокированы угрозы из **почтовых клиентов**, превышает среднемировой уровень в 1,4 раза.



Изменения за квартал и тренды

Категории угроз

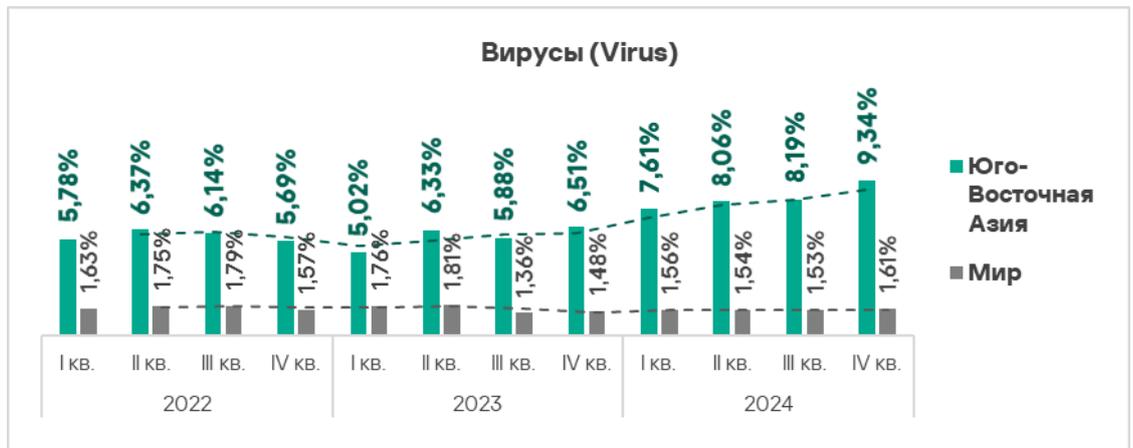


- **Наибольший рост за квартал** отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

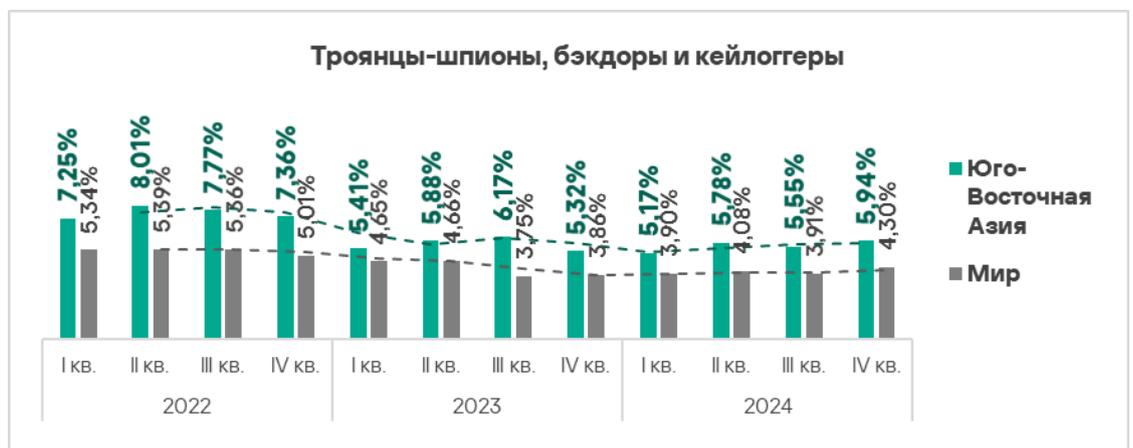
➤ вредоносные скрипты и фишинговые страницы — в 1,2 раза;



➤ вирусы — в 1,1 раза, первое место по росту показателя в мире;



➤ шпионские программы – в 1,1 раза.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Юго-Восточной Азии с начала 2022 года.

Юго-Восточная Азия	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	2	2	1	1	3	2	1	1
Вирусы (Virus)	5	5	4	4	4	3	4	3	1	1	2	2
Ресурсы в интернете из списка запрещенных	4	3	3	2	1	1	2	2	2	3	3	3
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	2	3	3	4	3	4	4	4	4	4
Вредоносные программы для AutoCAD	9	9	9	9	7	6	7	6	5	5	5	5
Вредоносные документы (MSOffice+PDF)	3	4	5	5	5	5	5	5	6	6	6	6
Черви (Worm)	7	7	6	6	6	7	6	7	7	7	7	7
Майнеры – исполняемые файлы для ОС Windows	6	6	8	8	9	9	9	9	8	8	8	8
Веб-майнеры, выполняемые в браузерах	8	8	7	7	8	8	8	8	9	9	9	9
Программы-вымогатели	10	10	10	10	10	10	10	10	10	10	10	10

Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

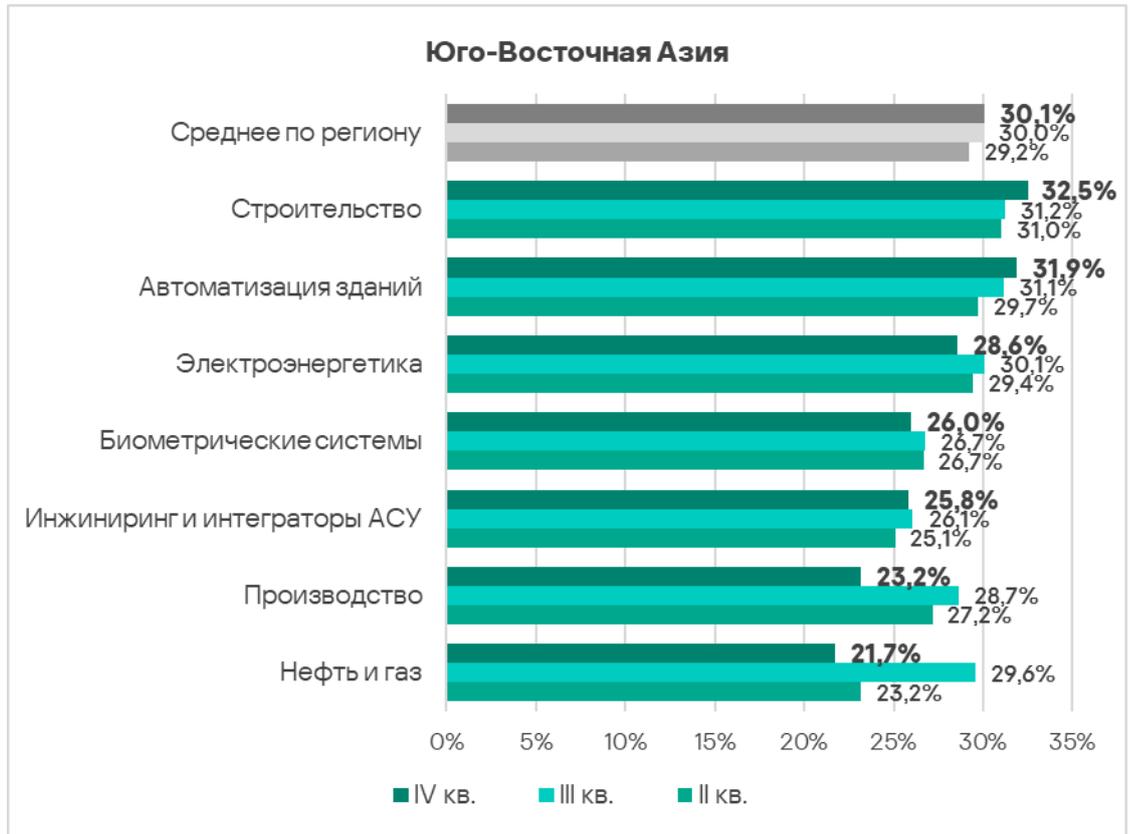


Отрасли

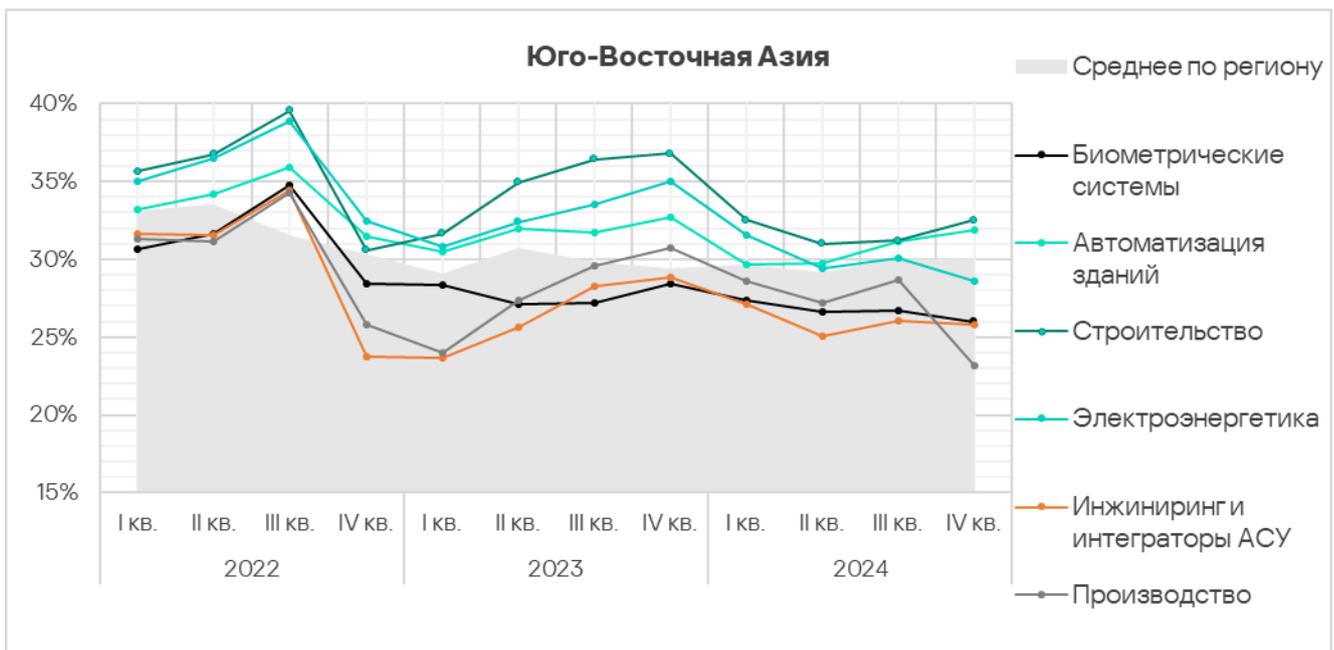
- **Наиболее часто встречающиеся с угрозами отрасли** региона среди рассмотренных в отчете:
 - строительство;
 - автоматизация зданий.
- По сравнению с соответствующими **среднемировыми показателями** значительно **более высокая доля компьютеров АСУ**, на которых были заблокированы вредоносные объекты, наблюдалась в следующих отраслях:
 - строительство — в 1,4 раза;
 - производство — в 1,3 раза;
 - автоматизация зданий — в 1,3 раза;
 - электроэнергетика — в 1,2 раза;
 - инжиниринг и интеграторы АСУ — в 1,2 раза.



В четвертом квартале 2024 года **рост** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался только в **строительстве** и **автоматизации зданий**.



- **Тренды** в рассмотренных отраслях демонстрируют в целом **положительную динамику**, хотя и сопровождаются резкими скачками и продолжительными периодами медленного роста и снижения значений.



Ближний Восток

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>9,68% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 3-е место по росту</p> <p>▲ 1,4x выше среднего по миру</p>	<p>6,62% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p> <p>▲ 2-е место в мире 1,5x выше среднего по миру</p>	<p>5,79% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>
<p>2,61% ВРЕДОНОСНЫЕ ДОКУМЕНТЫ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>▲ 3-е место в мире 1,5x выше среднего по миру</p>	<p>2,19% ЧЕРВИ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>▲ 3-е место в мире 1,6x выше среднего по миру</p>	<p>2,16% ВИРУСЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 3-е место по росту</p> <p>▲ 1,3x выше среднего по миру</p>
<p>0,62% ВЕБ-МАЙНЕРЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>▲ 1-е место в мире 1,6x выше среднего по миру</p>	<p>0,27% ПРОГРАММЫ- ВЫМОГАТЕЛИ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>▲ 1-е место в мире 1,3x выше среднего по миру</p>	
<p>11,77% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>5,30% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 2-е место по росту</p>	<p>1,04% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>

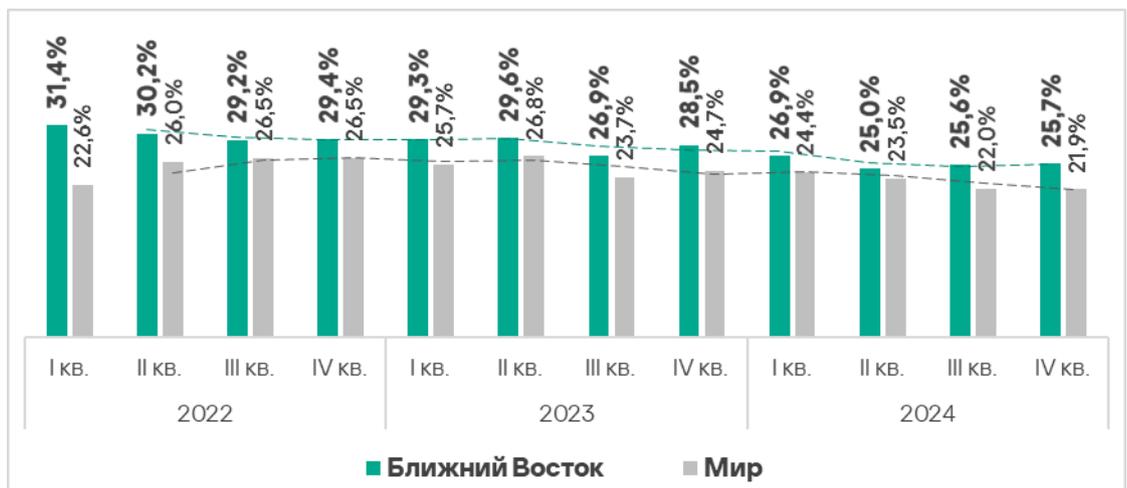
🌐 3-е место в мире
1,2x выше среднего
по миру

🌐 2-е место в мире
1,9x выше среднего
по миру

🌐 1,6x выше среднего
по миру

Общая ситуация

- Ближний Восток занимает **третье место** в мире по доле компьютеров АСУ, на которых заблокированы вредоносные объекты.
- Этот показатель **превышает среднемировое значение** на протяжении всего рассматриваемого периода. В четвертом квартале 2024 года региональное значение выше среднемирового в 1,2 раза.
- По сравнению с предыдущим кварталом показатель **незначительно вырос**.



Сравнительный анализ

Категории угроз

- В регионе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выше среднемирового значения** у всех категорий, кроме майнеров — исполняемых файлов, а также вредоносных программ для AutoCAD.



- Наиболее существенно **по сравнению со среднемировыми значениями выросли** показатели следующих категорий угроз:
 - черви — в 1,6 раза, третье место в мире;
 - веб-майнеры — в 1,6 раза, первое место в мире;
 - шпионские программы — в 1,5 раза, второе место в мире;
 - вредоносные документы — в 1,5 раза (также выше значения за третий квартал 2024 года), третье место в мире;
 - вредоносные скрипты и фишинговые страницы — в 1,4 раза, (также выше значения за третий квартал 2024 года);
 - вирусы — в 1,3 раза;
 - программы-вымогатели — в 1,3 раза, первое место в мире.

Источники угроз

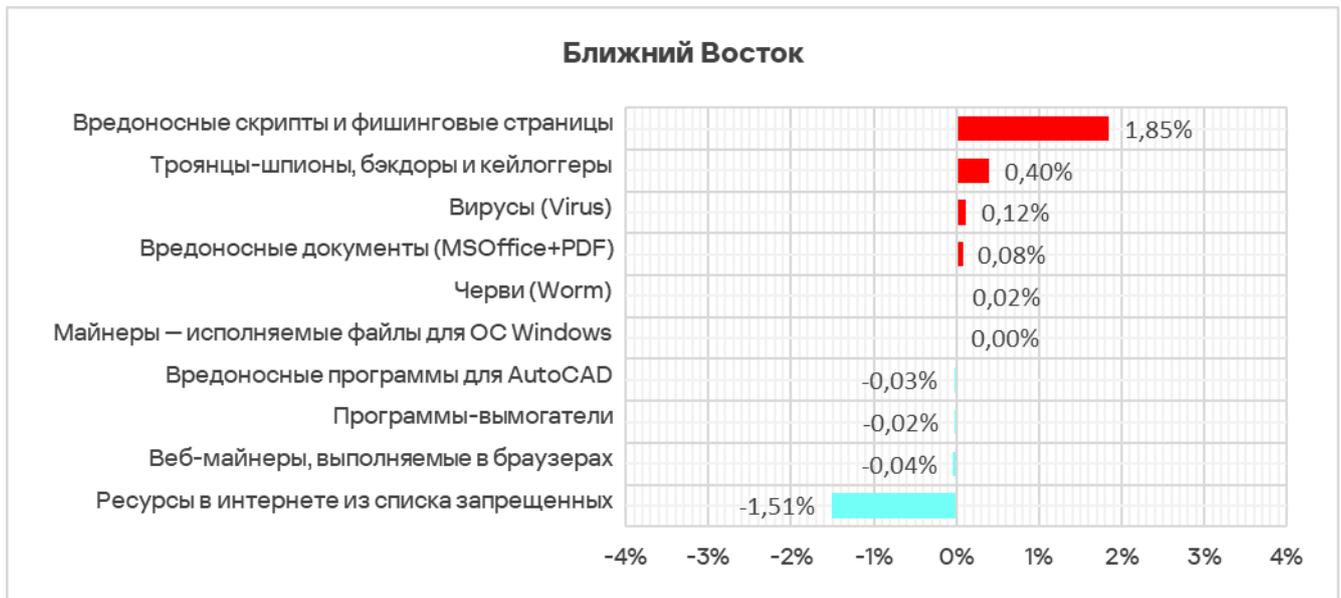
- Ближний Восток занимает **второе место в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, с превышением среднемирового значения в 1,9 раза (это также выше значения за третий квартал 2024 года).
- Также регион занимает **третье место в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, с превышением среднемирового значения в 1,2 раза (это также выше значения за третий квартал 2024 года).
- Доля компьютеров АСУ, на которых были заблокированы угрозы на **съёмных носителях**, превышает среднемировое значение в 1,6 раза.



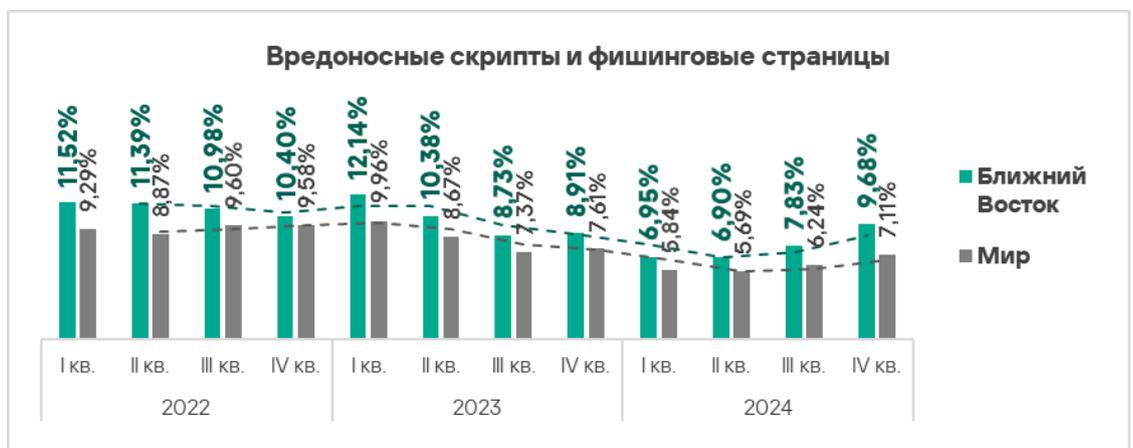
Изменения за квартал и тренды

Категории угроз

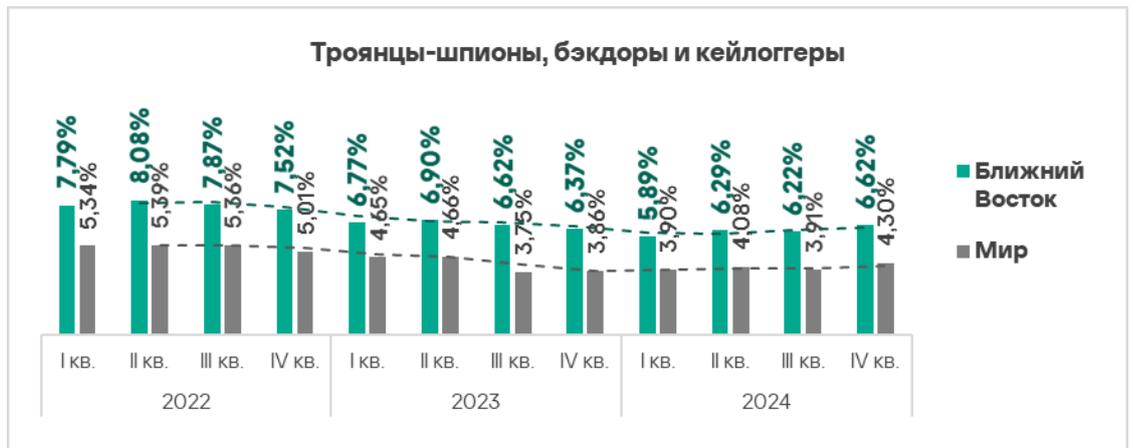
- В течение четвертого квартала доля компьютеров АСУ, на которых были заблокированы вредоносных объектов, выросла у пяти из 10 категорий угроз.



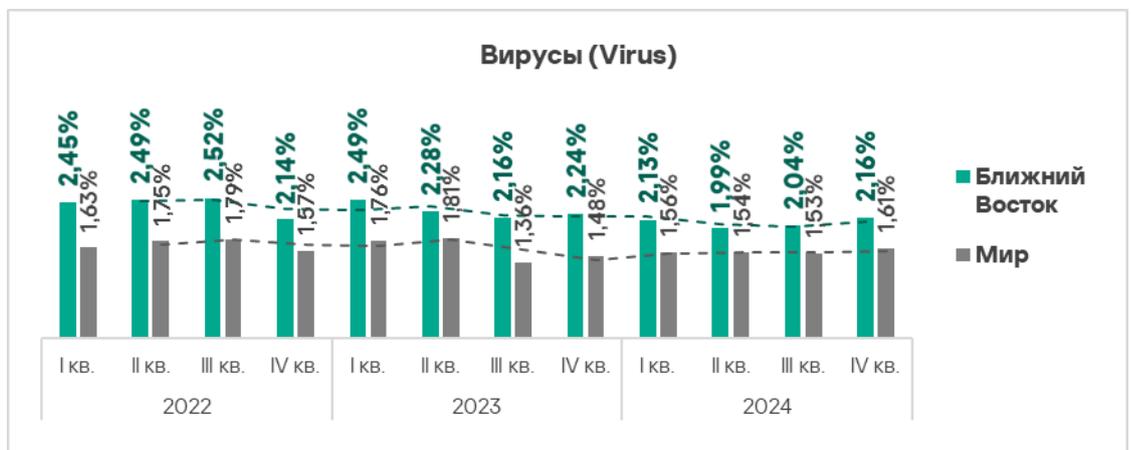
- Наибольший рост за квартал** зафиксирован у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
 - вредоносные скрипты и фишинговые страницы – в 1,2 раза, третье место по росту показателя в мире;



- шпионские программы – в 1,1 раза;



➤ Вирусы — в 1,1 раза, третье место по росту показателя в мире.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз на Ближнем Востоке с начала 2022 года. **Вредоносные скрипты и фишинговые страницы** возглавляют рейтинг категорий угроз в регионе на протяжении всего этого времени. **Шпионские программы** в четвертом квартале 2024 года вернулись на второе место.

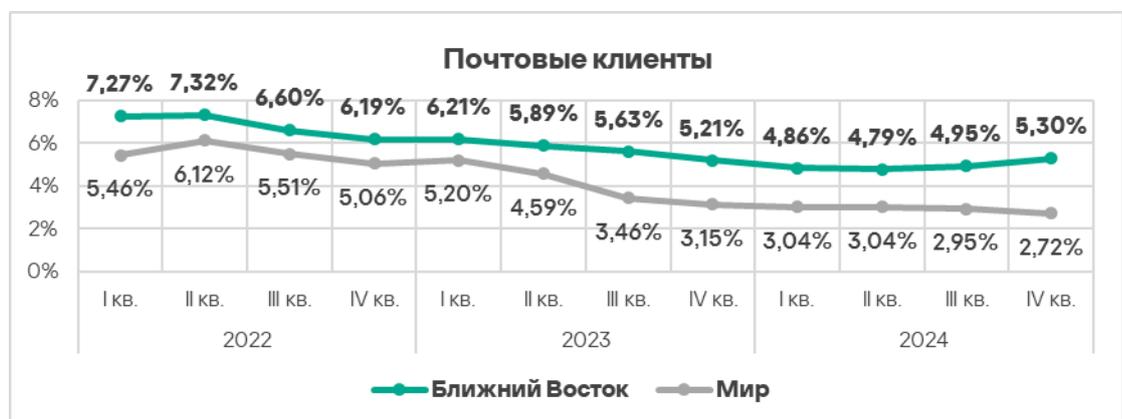
Ближний Восток	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	1	1	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	2	2	3	3	2	3	3	2	3	2
Ресурсы в интернете из списка запрещенных	3	3	3	3	2	2	3	2	2	3	2	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	4	5	4	4	4
Черви (Worm)	5	5	5	5	5	5	5	5	4	5	5	5
Вирусы (Virus)	6	6	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	7	7
Майнеры – исполняемые файлы для ОС Windows	7	7	8	8	8	8	8	8	8	8	8	8
Вредоносные программы для AutoCAD	10	10	9	10	9	9	9	9	9	10	9	9
Программы-вымогатели	9	9	10	9	10	10	10	10	10	9	10	10

Источники угроз

- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз, кроме почтовых клиентов.



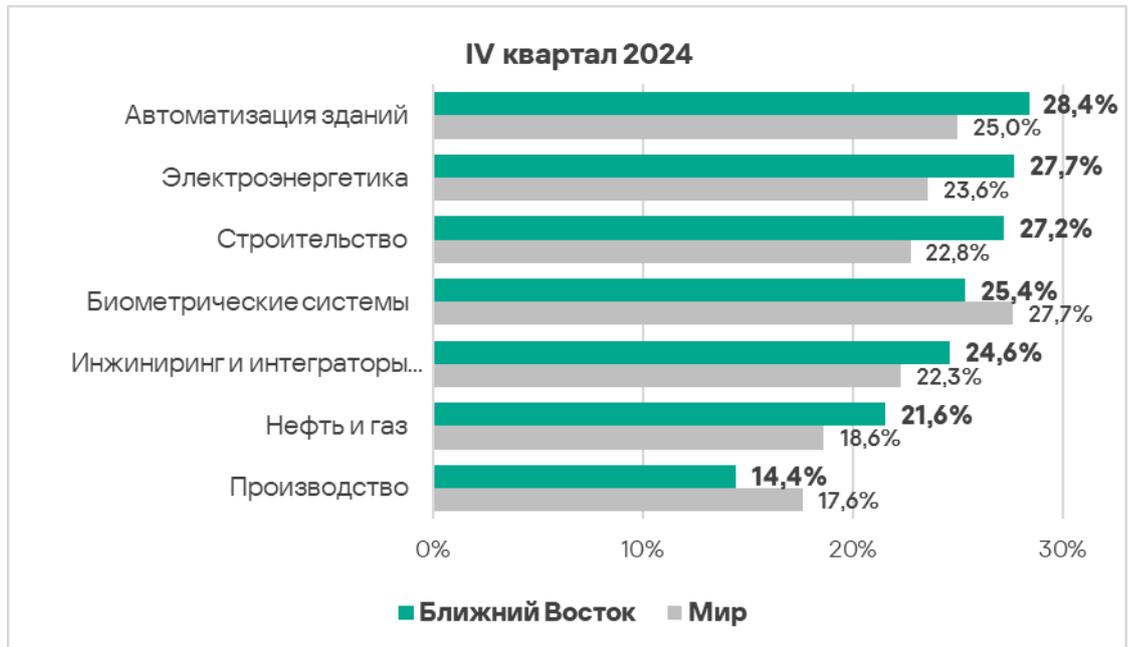
- Показатель угроз из **почтовых клиентов** вырос по сравнению с предыдущим кварталом в 1,1 раза, что еще более увеличило разрыв между региональным и среднемировым значениями, последнее из которых снова уменьшилось.
- Регион занимает **второе место** по росту доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в мире.



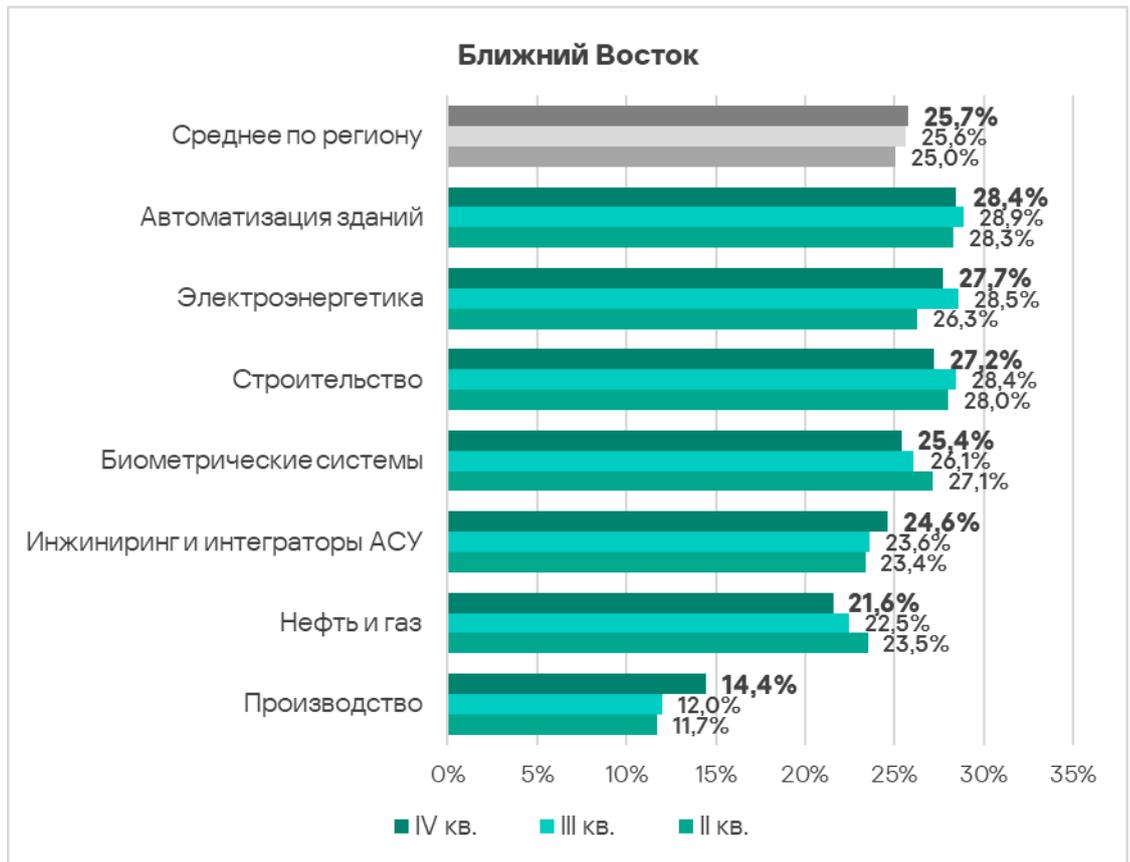
Отрасли

- **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:
 - строительство — в 1,2 раза;
 - электроэнергетика — в 1,2 раза;
 - нефть и газ — в 1,2 раза;
 - автоматизация зданий — в 1,1 раза;

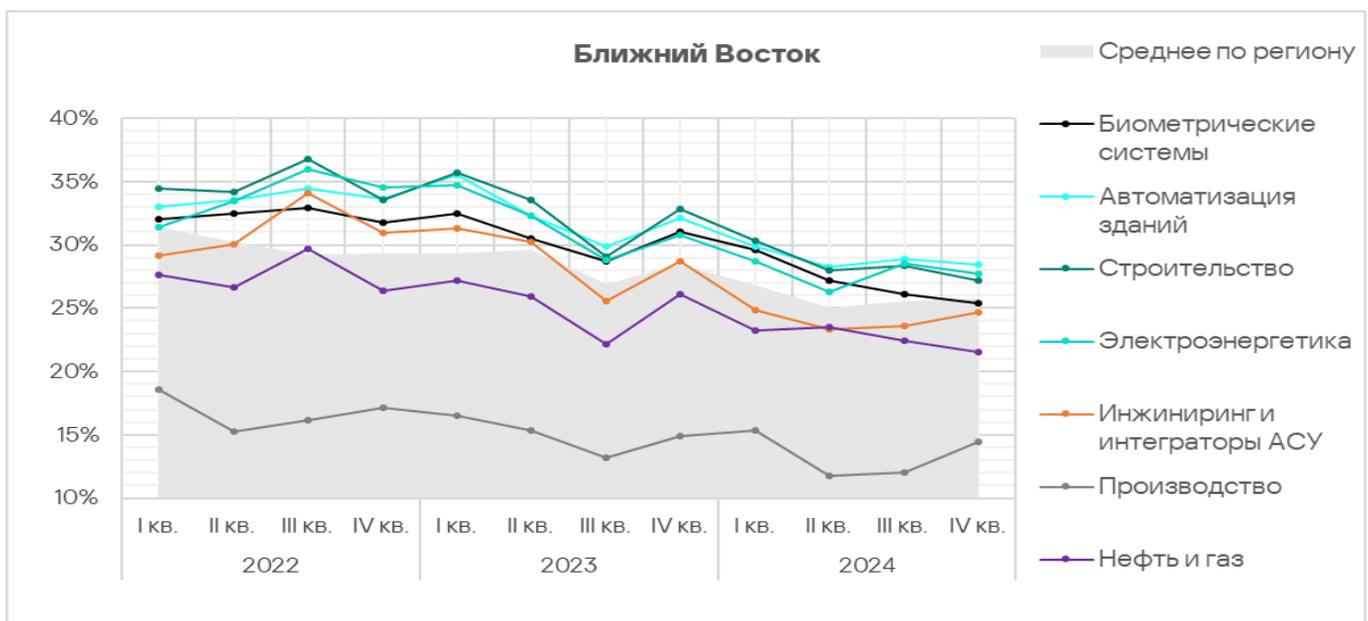
➤ инжиниринг и интеграторы АСУ – в 1,1 раза.



- В **четвертом квартале 2024 года** наиболее существенный, по сравнению с предыдущим кварталом, **рост** (в 1,2 раза) доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, отмечен в **производстве**.



- Несмотря на периодические колебания, **тренды** в исследуемых отраслях демонстрируют в целом **положительную динамику**.



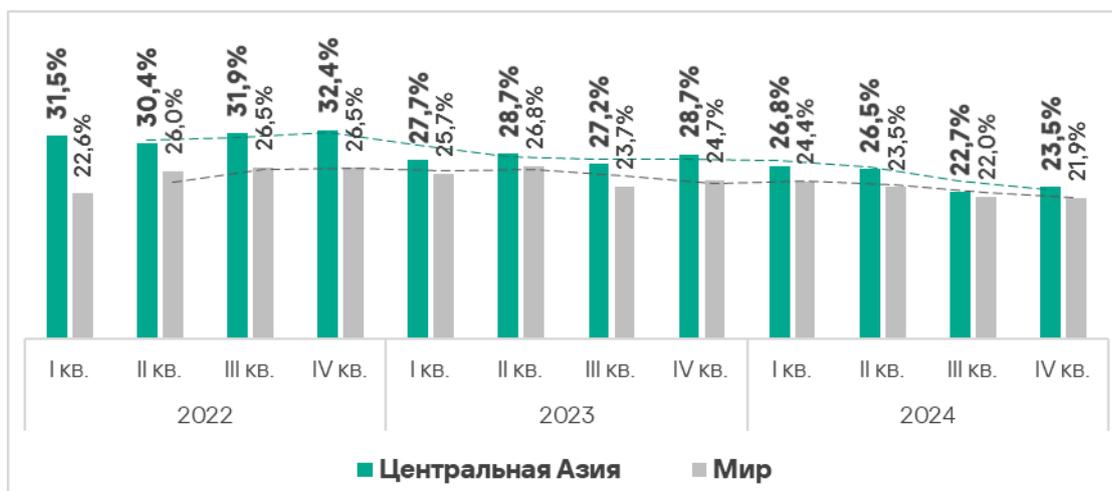
Центральная Азия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>5,97% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,1x выше среднего по миру</p>	<p>4,74% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 3-е место по росту</p> <p>🌐 3-е место в мире 1,1x выше среднего по миру</p>	<p>4,24% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▼ снижение в IV кв. 2024 г.</p>
<p>2,93% ЧЕРВИ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>🌐 2-е место в мире 2,1x выше среднего по миру</p>	<p>1,48% МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1-е место в мире 2,1x выше среднего по миру</p>	
<p>8,46% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>0,83% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,3x выше среднего по миру</p>	

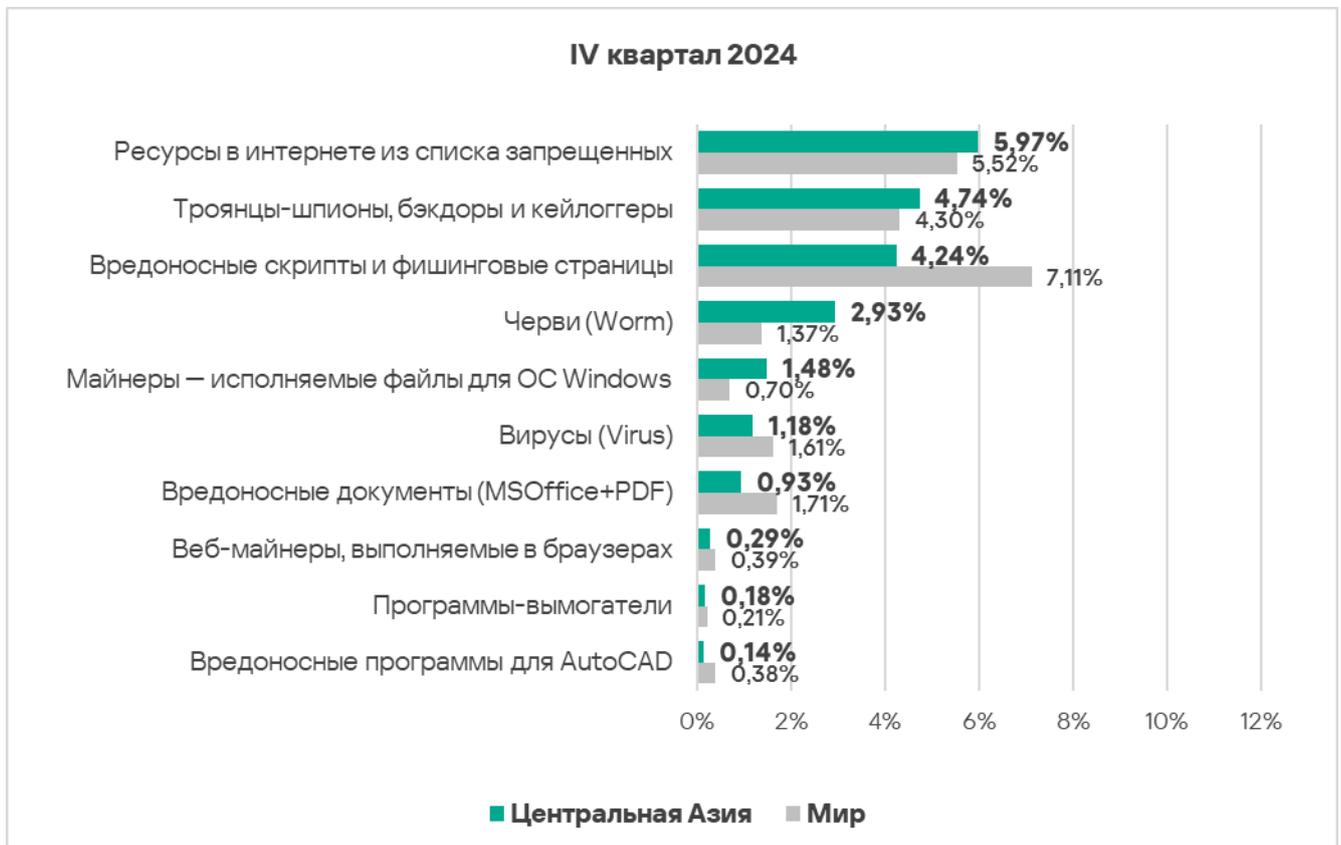
Общая ситуация

- Центральная Азия занимает **четвертое место** в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Показатель все еще **превышает среднемировое значение**, хотя наблюдается тенденция к сокращению разрыва.
- В **четвертом квартале 2024 года** региональный показатель незначительно **вырос**.



Сравнительный анализ

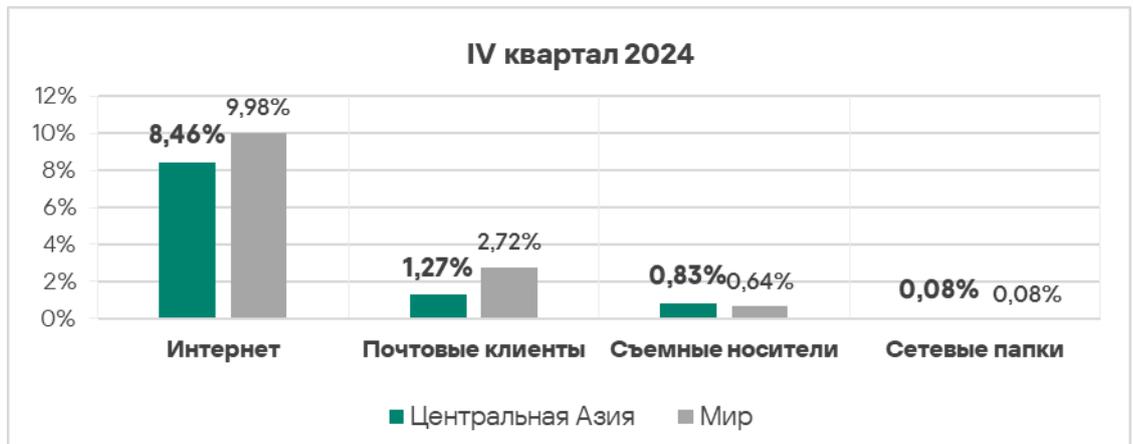
Категории угроз



- По сравнению со среднемировыми показателями в регионе **выше** доля компьютеров АСУ, на которых заблокированы следующие категории угроз:
 - майнеры — исполняемые файлы для Windows — в 2,1 раза, первое место в мире;
 - черви — в 2,1 раза, второе место в мире;
 - интернет-ресурсы из списка запрещенных — в 1,1 раза, третье место в мире;
 - шпионские программы — в 1,1 раза.

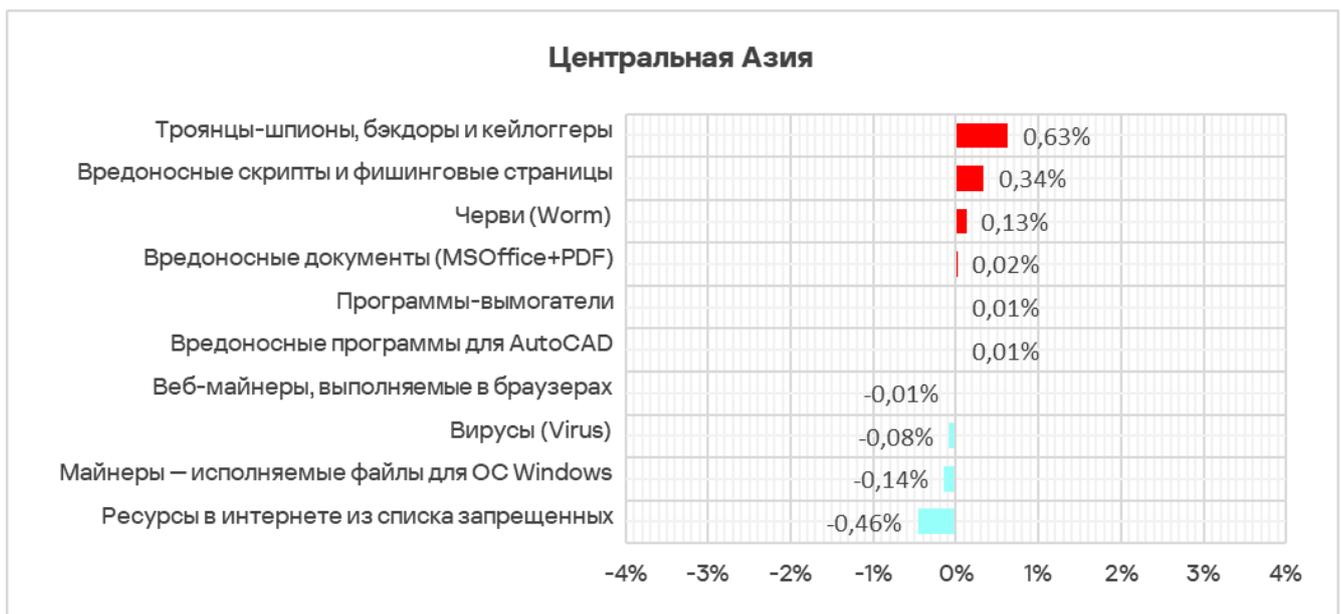
Источники угроз

- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы на **съёмных носителях, превысила среднемировое значение** в 1,3 раза.

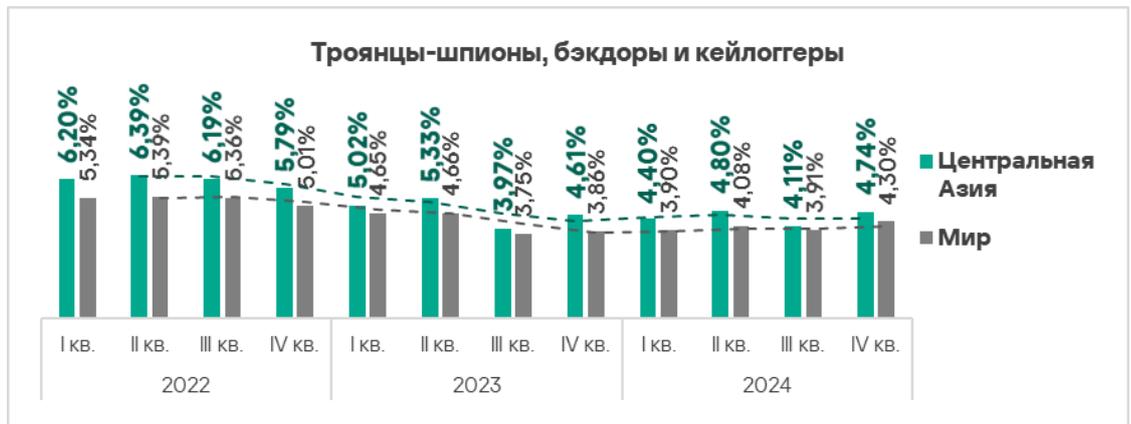


Изменения за квартал и тренды

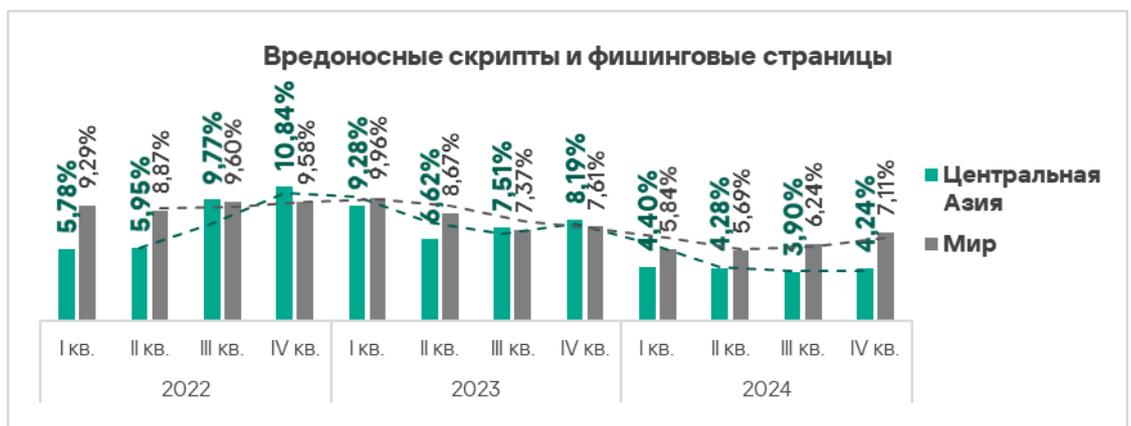
Категории угроз



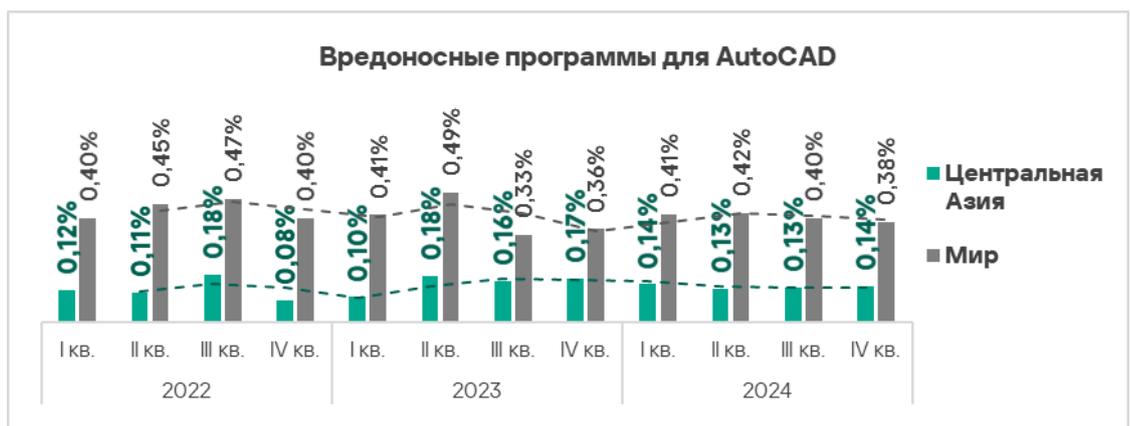
- **Наибольший рост** за квартал зафиксирован у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
 - шпионские программы – в 1,2 раза;



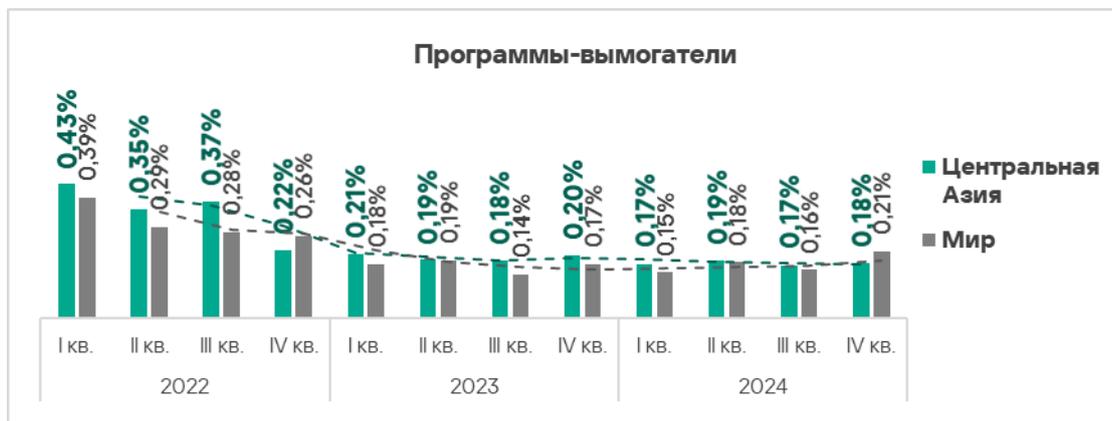
➤ вредоносные скрипты и фишинговые страницы — в 1,1 раза;



➤ вредоносные программы для AutoCAD — в 1,1 раза;



➤ программы-вымогатели — в 1,1 раза.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Центральной Азии с начала 2022 года. **Ресурсы в интернете из списка запрещенных** остаются ведущей категорией угроз в регионе на протяжении всего этого времени, за исключением четвертого квартала 2022 года и четвертого квартала 2023 года.

Центральная Азия	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Ресурсы в интернете из списка запрещенных	1	1	1	2	1	1	1	2	1	1	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	3	3	3	3	3	3	2	2	2	2
Вредоносные скрипты и фишинговые страницы	3	3	2	1	2	2	2	1	3	3	3	3
Черви (Worm)	4	4	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	5	5
Вирусы (Virus)	7	7	7	7	7	7	6	6	6	6	6	6
Вредоносные документы (MSOffice+PDF)	6	6	6	6	6	6	7	7	7	7	7	7
Веб-майнеры, выполняемые в браузерах	8	8	8	8	8	8	8	8	8	8	8	8
Программы-вымогатели	9	9	9	9	9	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	10	10	10

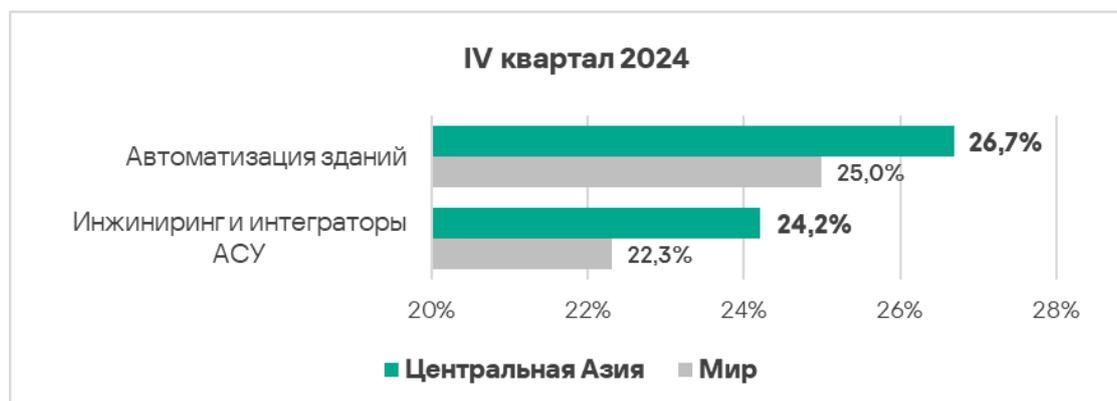
Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

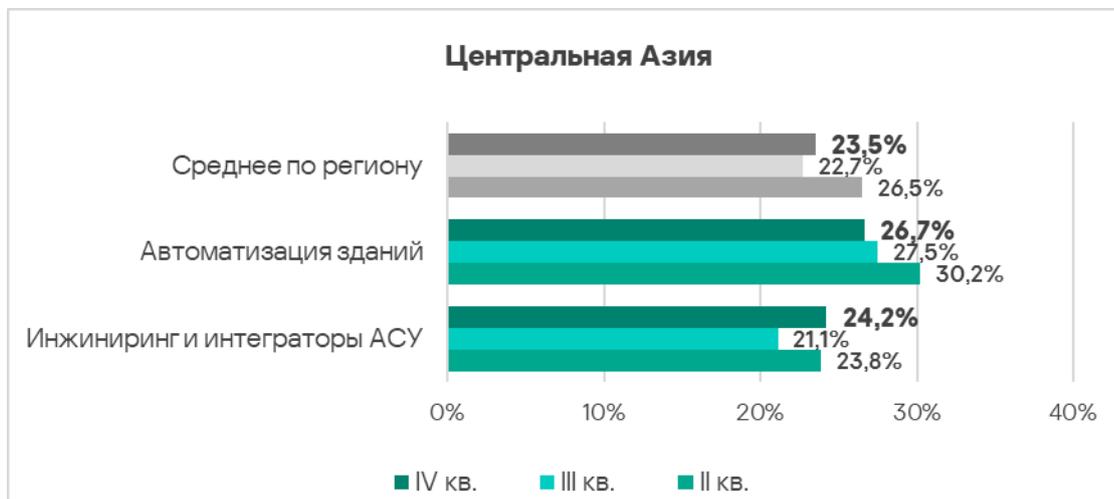


Отрасли

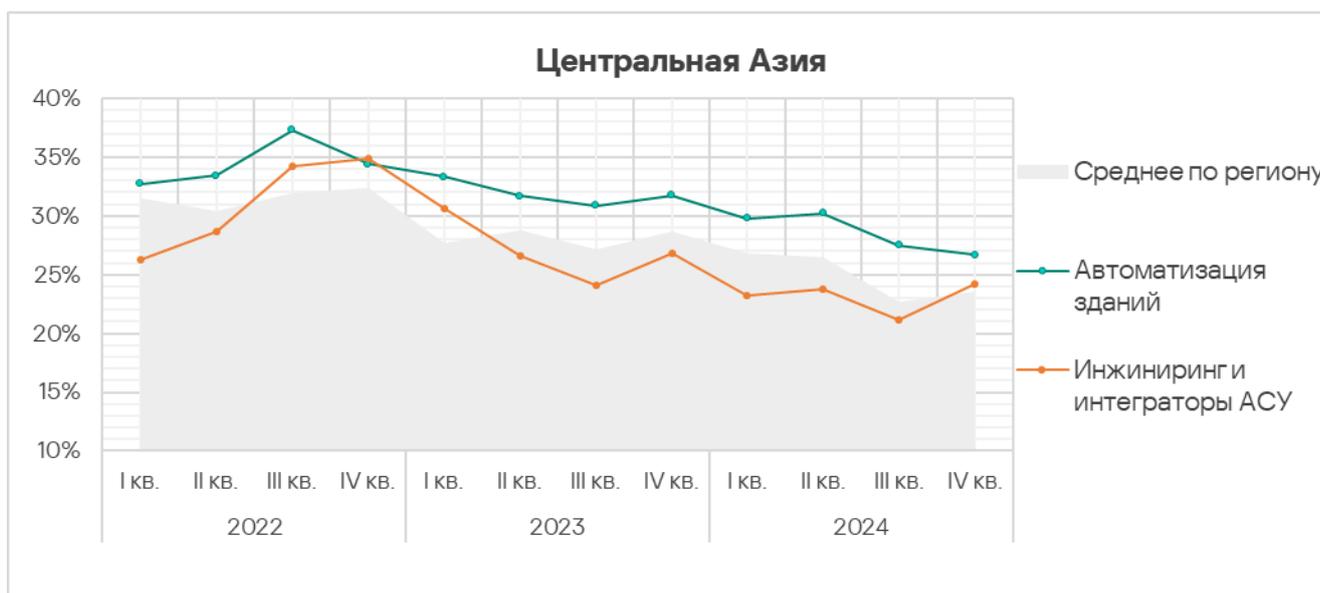
- **Наиболее часто встречающейся с угрозами отраслью** региона среди рассмотренных в отчете оказалась **автоматизация зданий**.
- Отрасли, в которых доля компьютеров АСУ с заблокированными на них вредоносными объектами **превышает среднемировое значение:** автоматизация зданий и инжиниринг и интеграторы АСУ. В каждом случае региональный показатель выше 1,1 раза.



- Инжиниринг и интеграторы АСУ – отрасль, где показатель по сравнению с предыдущим кварталом вырос в 1,1 раза.



Тренды в этих отраслях демонстрируют в целом **положительную динамику**.



Восточная Азия

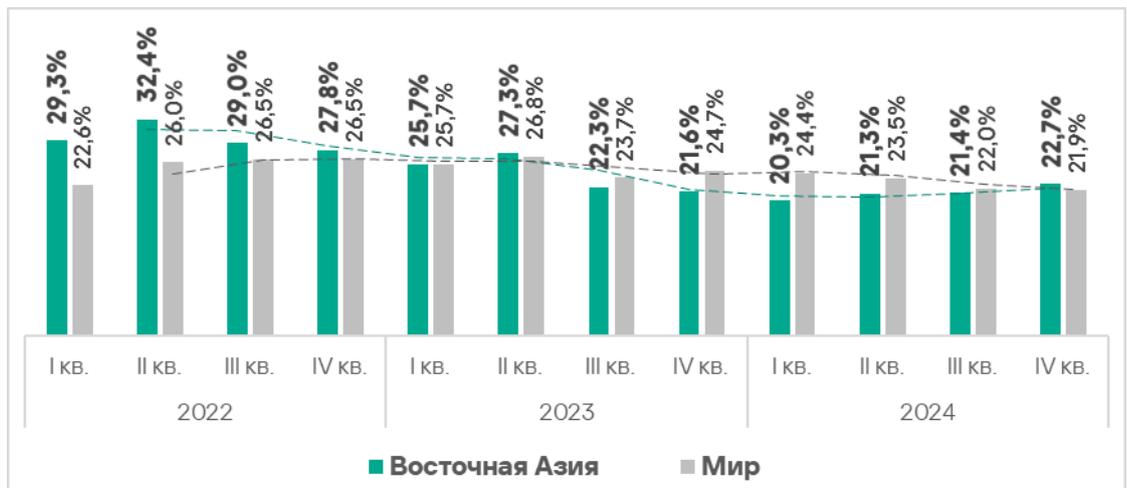
Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>4,89% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>4,38% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>3,56% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▲ слабый рост в IV кв. 2024 г. (единственный регион, где показатель вырос)</p>
<p>2,93% ВИРУСЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,8x выше среднего по миру</p>	<p>1,53% ЧЕРВИ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>1,44% ВРЕДНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 2-е место в мире 3,8x выше среднего по миру</p>
<p>0,23% ПРОГРАММЫ-ВЫМОГАТЕЛИ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 2-е место по росту</p> <p>🌐 1,1x выше среднего по миру</p>		
<p>7,33% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 1-е место по росту</p>	<p>1,30% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ слабый рост в IV кв. 2024 г.</p>	<p>0,27% СЕТЕВЫЕ ПАПКИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>

	<p>2-е место по росту</p> <p>🌐 2-е место в мире 2x выше среднего по миру</p>	<p>🌐 1-е место в мире 3,4x выше среднего по миру</p>
--	--	--

Общая ситуация

- Восточная Азия занимает **пятое место** в мировом рейтинге по доле компьютеров АСУ, на которых заблокированы вредоносные объекты. В предыдущем квартале регион занимал **восьмое место**.
- В регионе наблюдается **нисходящий** колебательный **тренд**.
- **В четвертом квартале 2024 года** в Восточной Азии доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла в 1,1 раза. Регион занимает первое место по росту этого показателя в мире.
- В этом квартале показатель **превысил среднемировое значение** впервые со второго квартала 2023 года.



Сравнительный анализ

Категории угроз



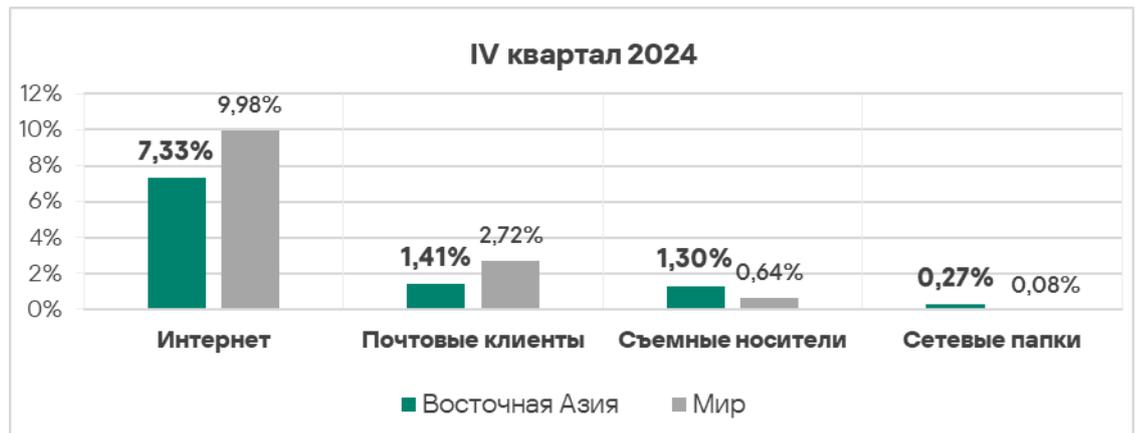
- По сравнению со среднемировыми показателями в регионе заметно выше доля компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
 - вредоносные программы для AutoCAD — в 3,8 раза, второе место в мире;
 - вирусы — в 1,8 раза (также выше значения за третий квартал 2024 года), третье место в мире;
 - черви — в 1,1 раза;
 - программы-вымогатели — в 1,1 раза;
 - шпионские программы — в 1,1 раза.

Источники угроз

- Восточная Азия по-прежнему занимает **первое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в

сетевых папках, с показателем, превышающим среднемировой в 3,4 раза (он также выше значения за третий квартал 2024 года).

- Доля компьютеров АСУ, на которых были заблокированы угрозы на **съемных носителях**, здесь в два раза **выше, чем в среднем по миру** (показатель также выше значения за третий квартал 2024 года).



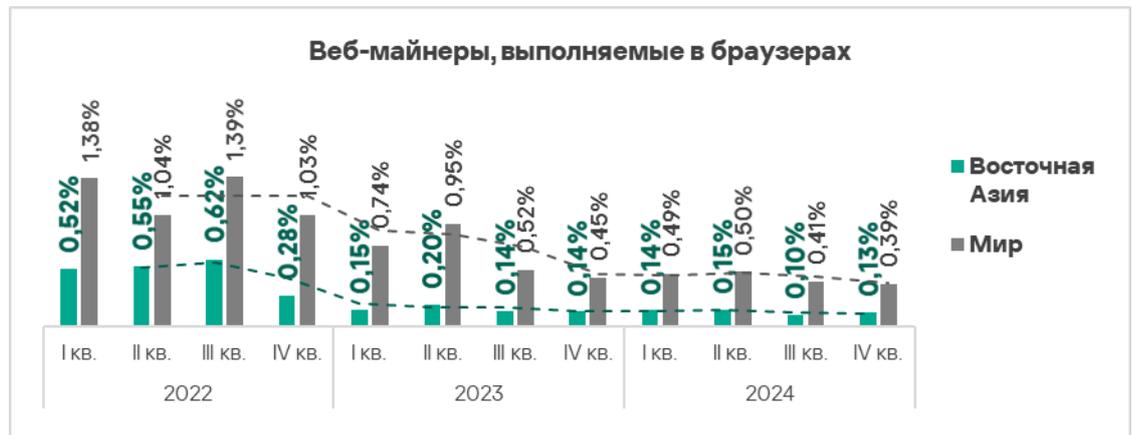
Изменения за квартал и тренды

Категории угроз

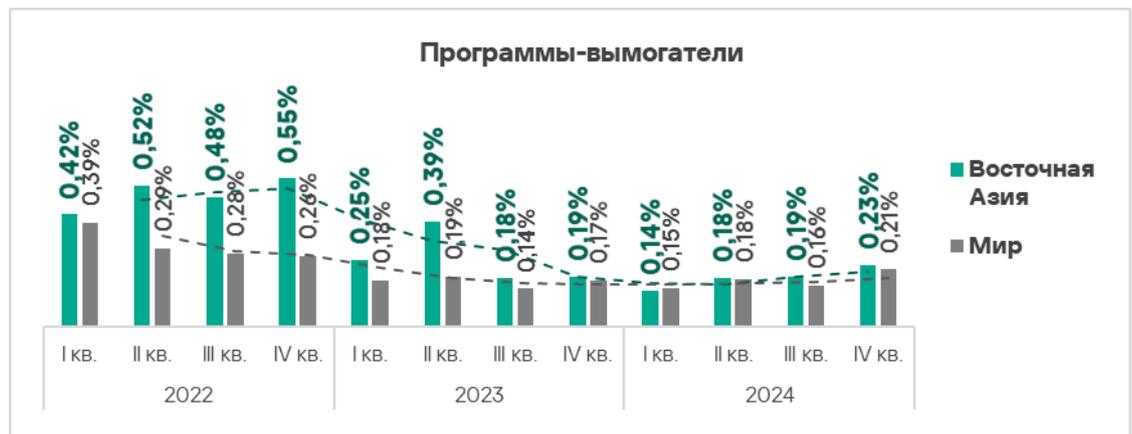


Наибольший рост за квартал зафиксирован у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

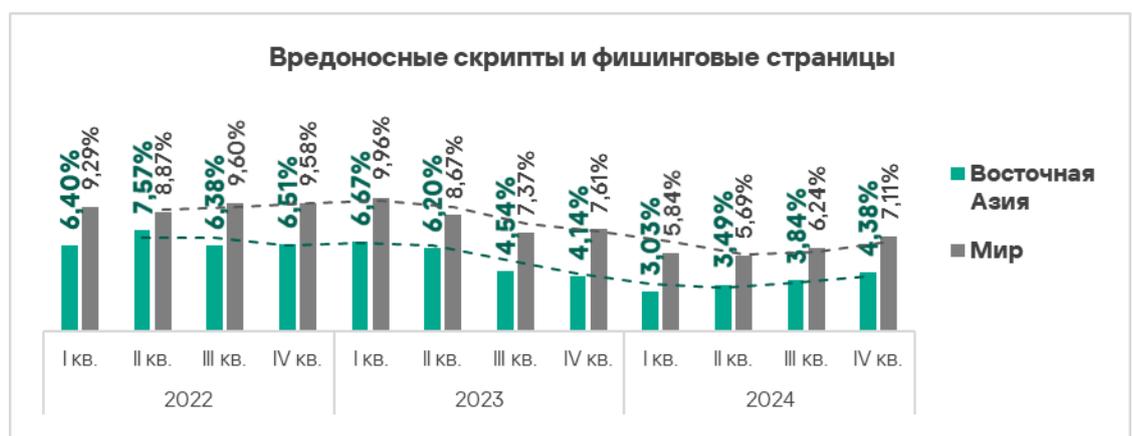
- веб-майнеры — в 1,3 раза, третье место по росту показателя в мире;



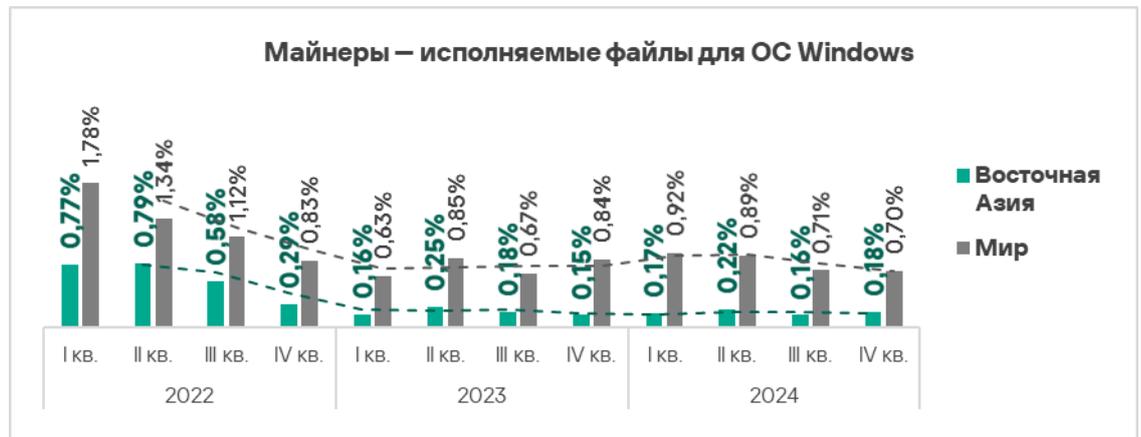
- программы-вымогатели — в 1,2 раза, второе место по росту показателя в мире;



- вредоносные скрипты и фишинговые страницы — в 1,1 раза;



- майнеры — исполняемые файлы для ОС Windows — в 1,1 раза;



➤ шпионские программы – в 1,1 раза.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Азии с начала 2022 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**.

Восточная Азия	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	1	1	1	1	1
Вредоносные скрипты и фишинговые страницы	2	2	1	1	1	1	1	2	3	2	2	2
Ресурсы в интернете из списка запрещенных	1	1	2	2	2	2	1	3	2	3	3	3
Вирусы (Virus)	4	4	4	4	4	4	4	4	4	4	4	4
Вредоносные документы (MSOffice+PDF)	5	5	5	5	6	5	7	7	7	6	5	5
Черви (Worm)	6	6	6	7	5	6	5	5	5	5	6	6
Вредоносные программы для AutoCAD	7	7	7	6	7	7	6	6	6	7	7	7
Программы-вымогатели	10	10	10	8	8	8	9	8	10	9	8	8
Майнеры – исполняемые файлы для ОС Windows	8	8	9	9	9	9	8	9	8	8	9	9
Веб-майнеры, выполняемые в браузерах	9	9	8	10	10	10	10	10	9	10	10	10

Источники угроз

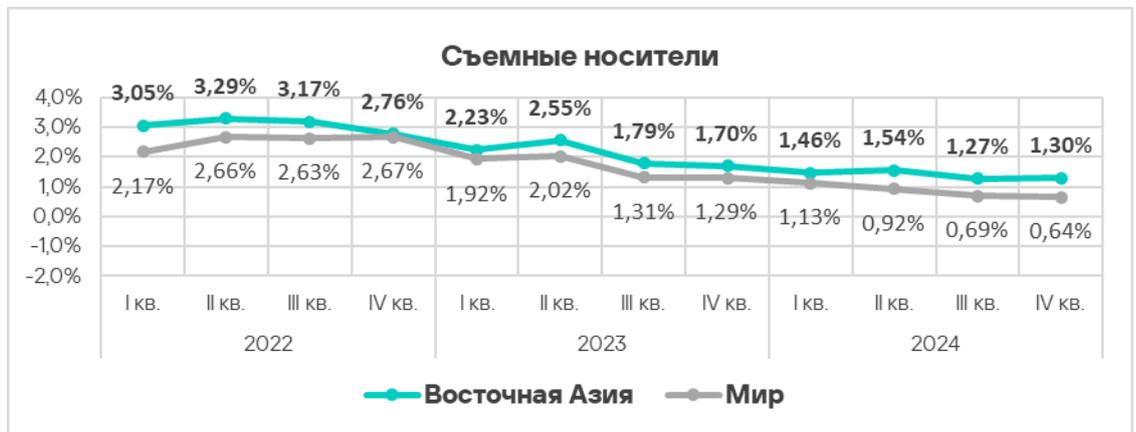
- Уровень угроз из **интернета** в Восточной Азии в четвертом квартале 2024 года **вырос** (в 1,1 раза), в отличие от среднемирового показателя.



- Уровень угроз в **сетевых папках**, заблокированных на компьютерах АСУ в Восточной Азии, продолжает демонстрировать **нисходящий тренд**, который сформировался во второй половине 2022 года. При этом показатель остается значительно **выше среднемирового значения**.



Уровень угроз, распространяемых на **съёмных носителях, вырос.**

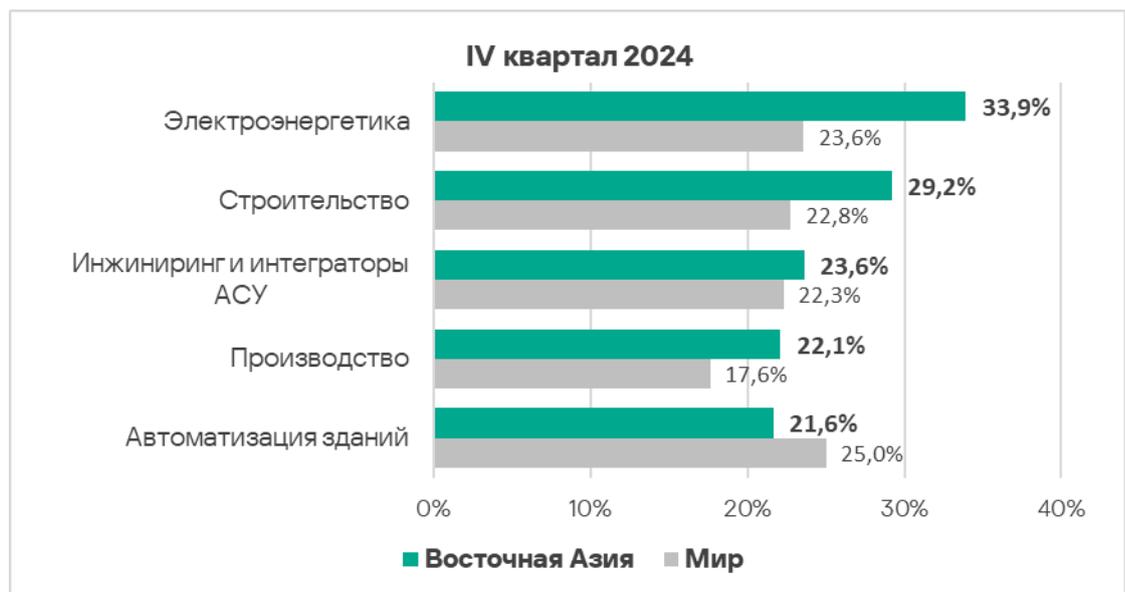


В целом, все основные источники угроз в рамках долгосрочных **трендов** демонстрируют **тенденцию к снижению.**



Отрасли

- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **электроэнергетика**.
- По сравнению с соответствующими **среднемировыми значениями** более **высокая доля компьютеров АСУ**, на которых были заблокированы вредоносные объекты, зафиксирована в следующих отраслях:
 - электроэнергетика — в 1,4 раза;
 - строительство — в 1,3 раза (также выше значения за третий квартал 2024 года);
 - производство — в 1,3 раза (также выше значения за третий квартал 2024 года);
 - инжиниринг и интеграторы АСУ — в 1,1 раза (также выше значения за третий квартал 2024 года).

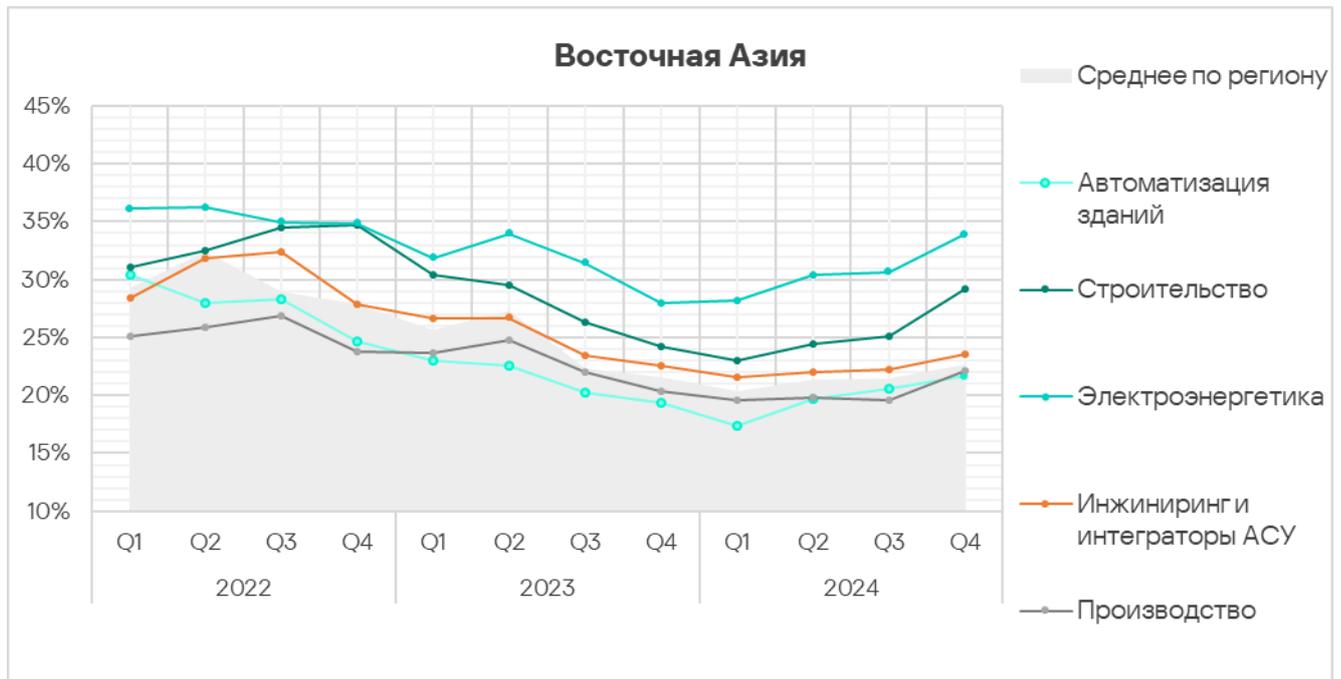


- В **четвертом квартале 2024 года** во всех отраслях зафиксирован **рост** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



- В **электроэнергетике** на протяжении всего рассматриваемого периода сохраняется **самая высокая доля компьютеров АСУ**, на которых были заблокированы вредоносные объекты, причем этот показатель **значительно превышает среднемировое значение**.

Начиная со второго квартала 2024 года уровень угроз **растет во всех отраслях**.



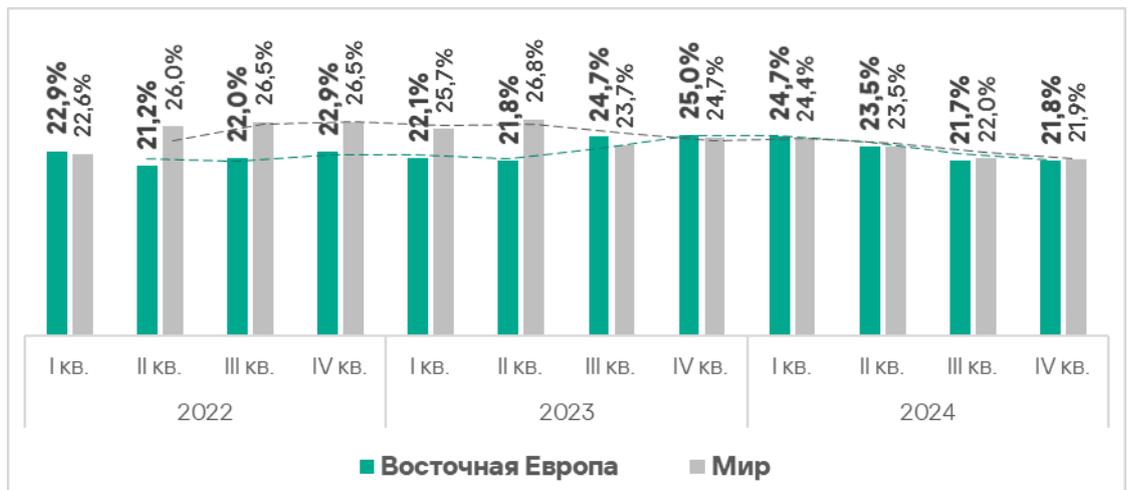
Восточная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>7,55% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>5,70% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>5,16% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,2x выше среднего по миру</p>
<p>2,09% ВРЕДНОСНЫЕ ДОКУМЕНТЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,2x выше среднего по миру</p>	<p>1,59% ЧЕРВИ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 1-е место по росту</p> <p>🌐 1,2x выше среднего по миру</p>	<p>0,45% ВЕБ-МАЙНЕРЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,2x выше среднего по миру</p>
<p>9,66% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>4,08% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,5x выше среднего по миру</p>	

Общая ситуация

- Восточная Европа занимает **шестое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. В прошлом квартале регион находился на седьмом месте. При этом до второго квартала 2023 года он не поднимался в рейтинге выше девятого места.
- **В четвертом квартале 2024 года** показатель **незначительно вырос** и практически сравнялся со среднемировым значением.



Сравнительный анализ

Категории угроз



- По сравнению со среднемировыми показателями в регионе заметно **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
 - вредоносные документы – в 1,2 раза (также выше значения за третий квартал 2024 года);
 - шпионские программы – в 1,2 раза;
 - черви – в 1,2 раза (также выше значения за третий квартал 2024 года);
 - веб-майнеры – в 1,2 раза;
 - вредоносные скрипты и фишинговые страницы – в 1,1 раза (также выше значения за третий квартал 2024 года);

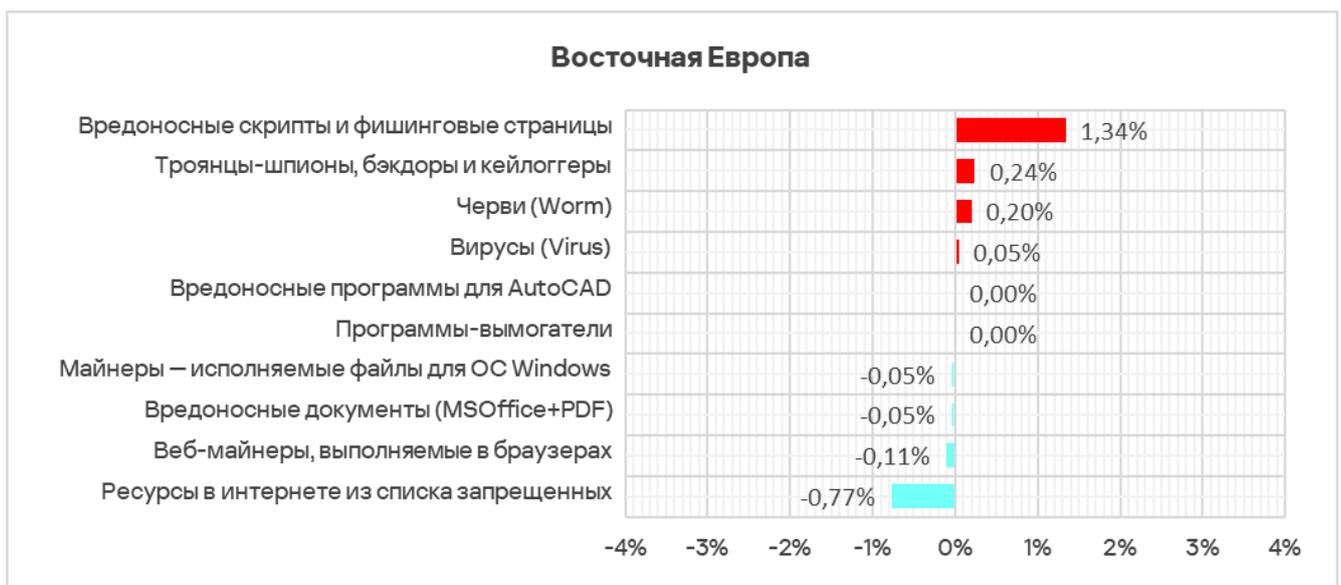
Источники угроз

Как и в предыдущем квартале, уровень угроз из **почтовых клиентов** в регионе **превышает среднемировой** в 1,5 раза.



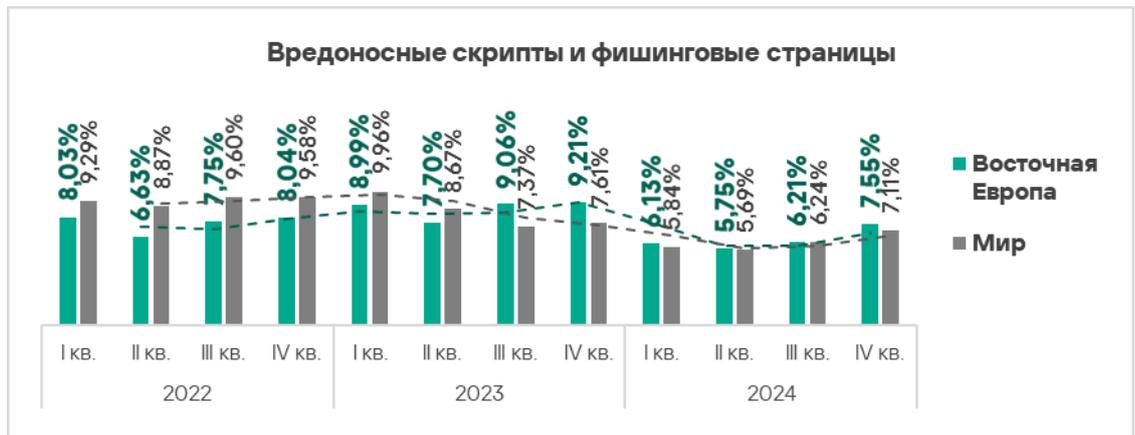
Изменения за квартал и тренды

Категории угроз

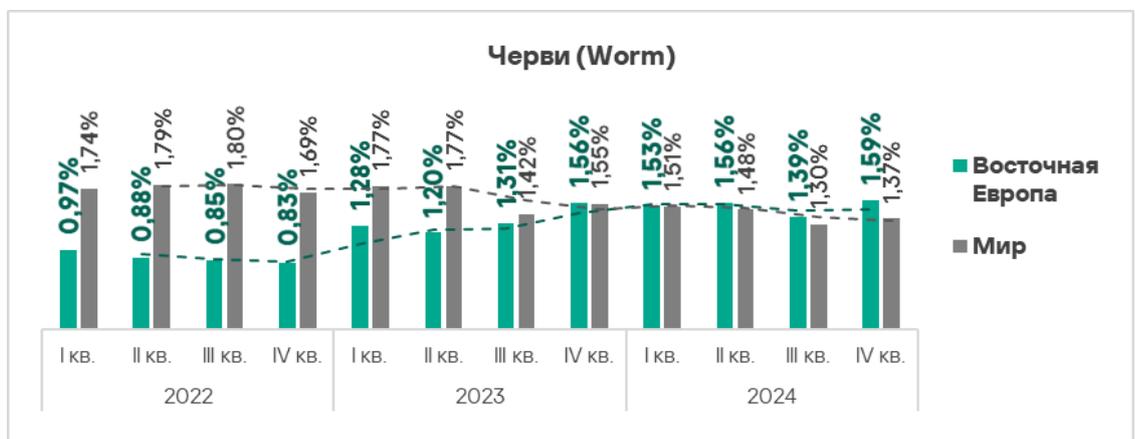


Наибольший рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

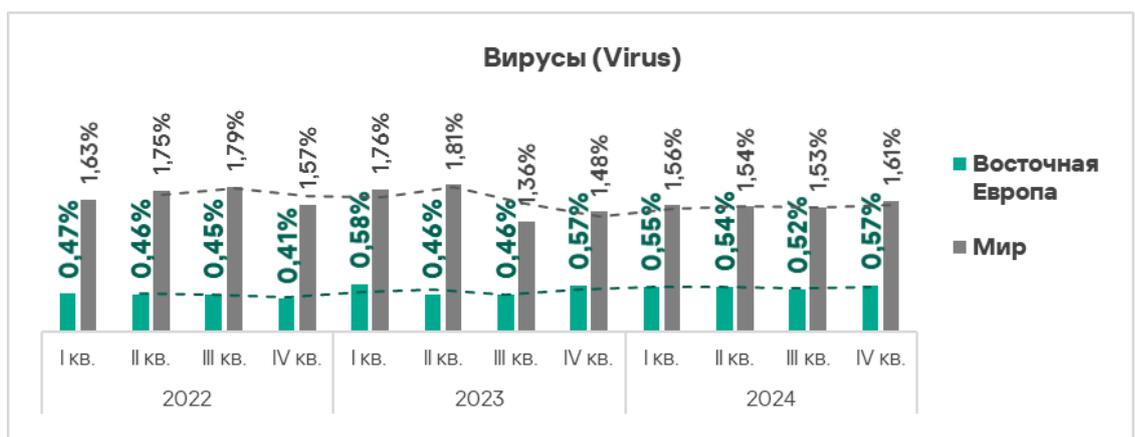
- вредоносные скрипты и фишинговые страницы – в 1,2 раза;



➤ черви – в 1,1 раза;



➤ вирусы – в 1,1 раза.

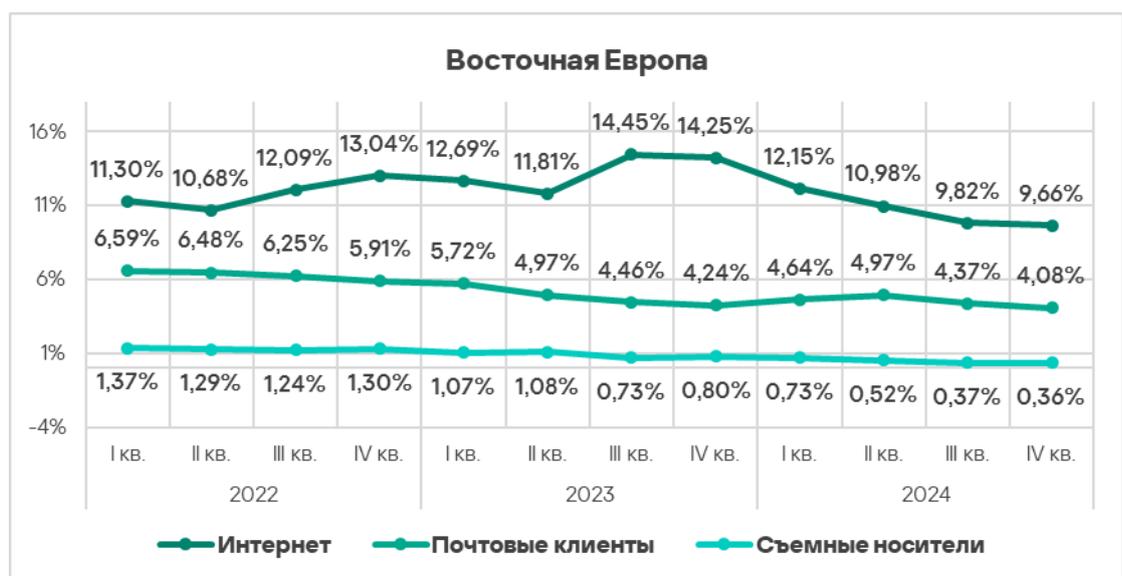


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Европе с начала 2022 года. В четвертом квартале 2024 года **вредоносные скрипты и фишинговые страницы** вернулись на первое место, а **вирусы** поднялись на седьмое.

Восточная Европа	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	2	2	1	1	2	2	2	1
Ресурсы в интернете из списка запрещенных	3	2	2	2	1	1	2	2	1	1	1	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	3	3	3	3	3	3	3	3	3	3	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	4	4	4	4	4
Черви (Worm)	7	6	7	6	5	6	5	5	5	5	5	5
Майнеры – исполняемые файлы для ОС Windows	5	5	6	7	7	7	6	6	6	6	6	6
Вирусы (Virus)	8	8	8	8	8	8	8	8	8	8	8	7
Веб-майнеры, выполняемые в браузерах	6	7	5	5	6	5	7	7	7	7	7	8
Программы-вымогатели	9	9	9	9	9	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	10	10	10

Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

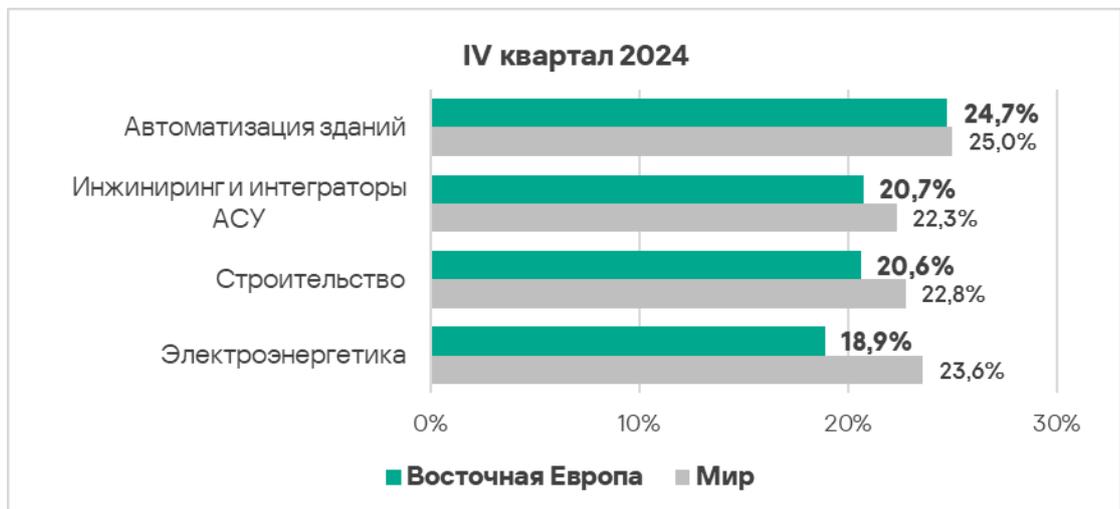


- Хотя доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**, снизилась, ее значение все равно осталось существенно выше среднемирового уровня.

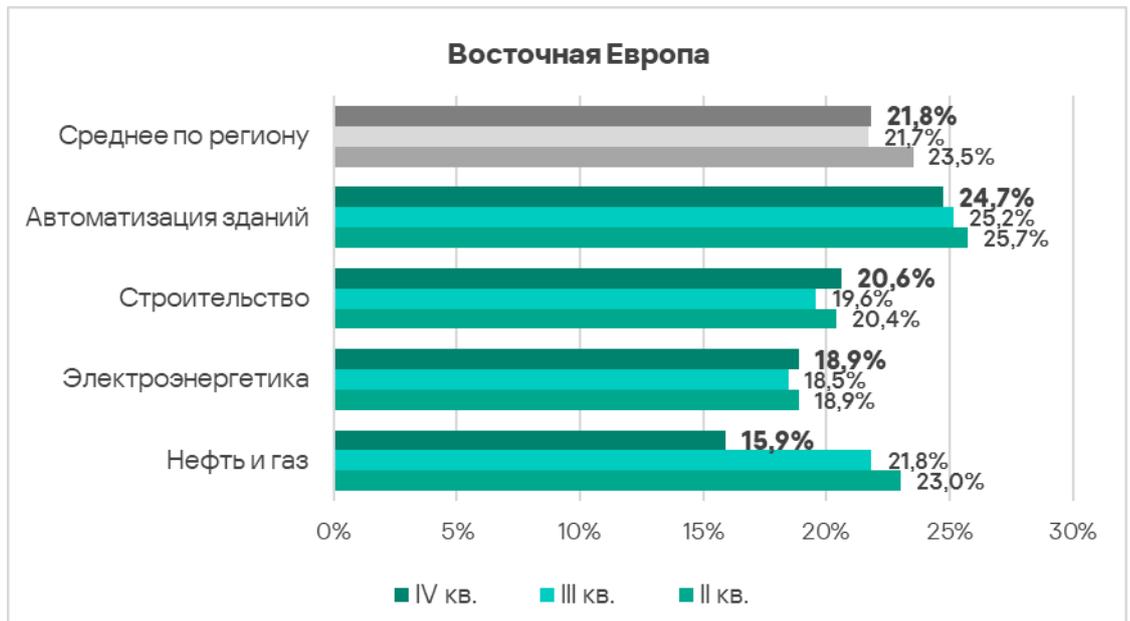


Отрасли

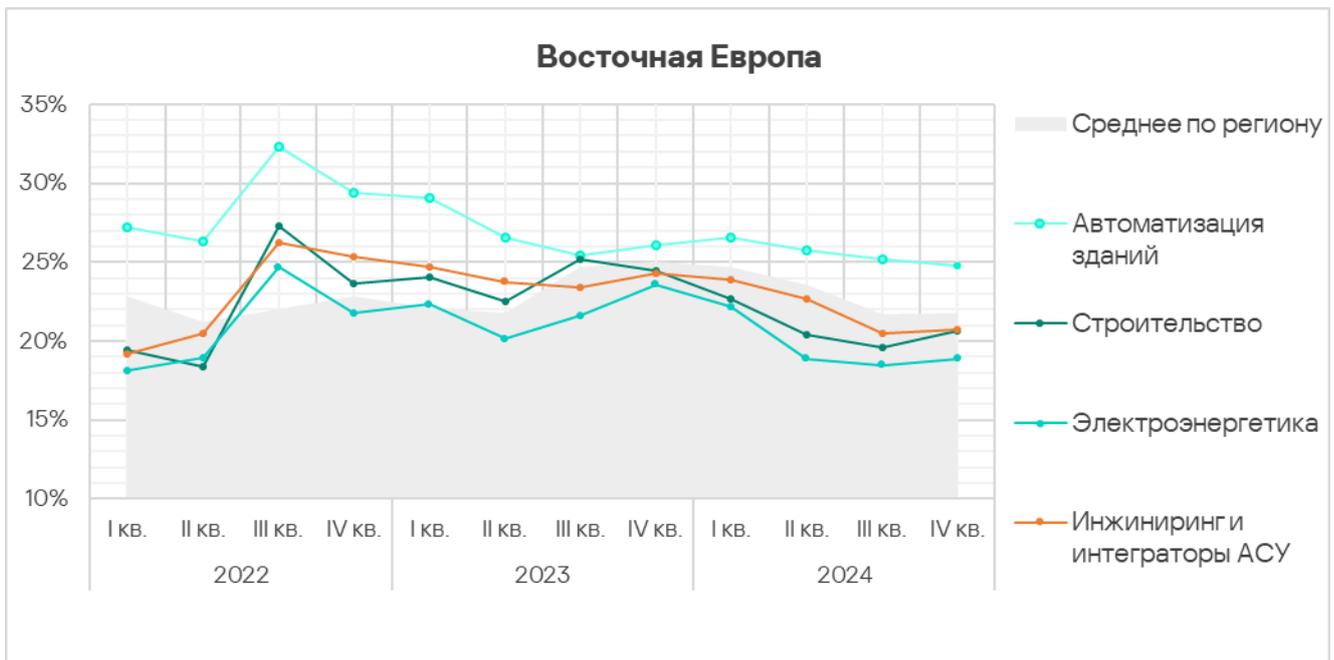
- **Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий**.
- По сравнению со **среднемировыми показателями** во всех рассмотренных отраслях зафиксирована более **низкая доля компьютеров АСУ**, на которых были заблокированы вредоносные объекты.



- В **четвертом квартале 2024 года** во всех рассматриваемых отраслях, кроме автоматизации зданий, наблюдалось **увеличение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Наибольший рост зафиксирован в строительстве — в 1,1 раза.



- **Тренды** в рассмотренных отраслях указывают на **стабилизацию** после значительного роста в 2022 году.



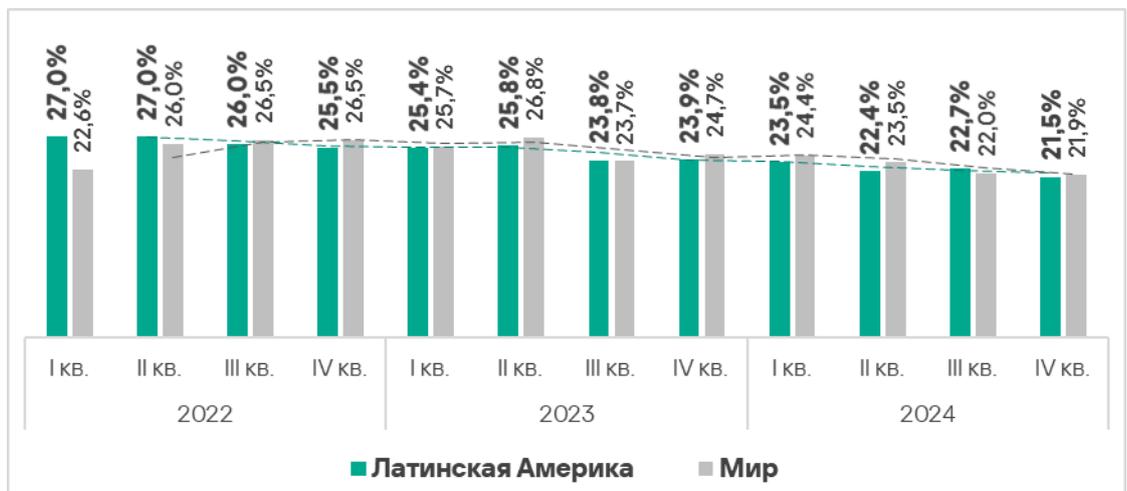
Латинская Америка

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>9,86% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,4x выше среднего по миру</p>	<p>4,94% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>4,37% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▼ снижение в IV кв. 2024 г.</p>
<p>2,09% ВРЕДНОСНЫЕ ДОКУМЕНТЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 2-е место в мире 1,9x выше среднего по миру</p>	<p>1,59% ВЕБ-МАЙНЕРЫ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	
<p>11,09% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>4,52% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,7x выше среднего по миру</p>	

Общая ситуация

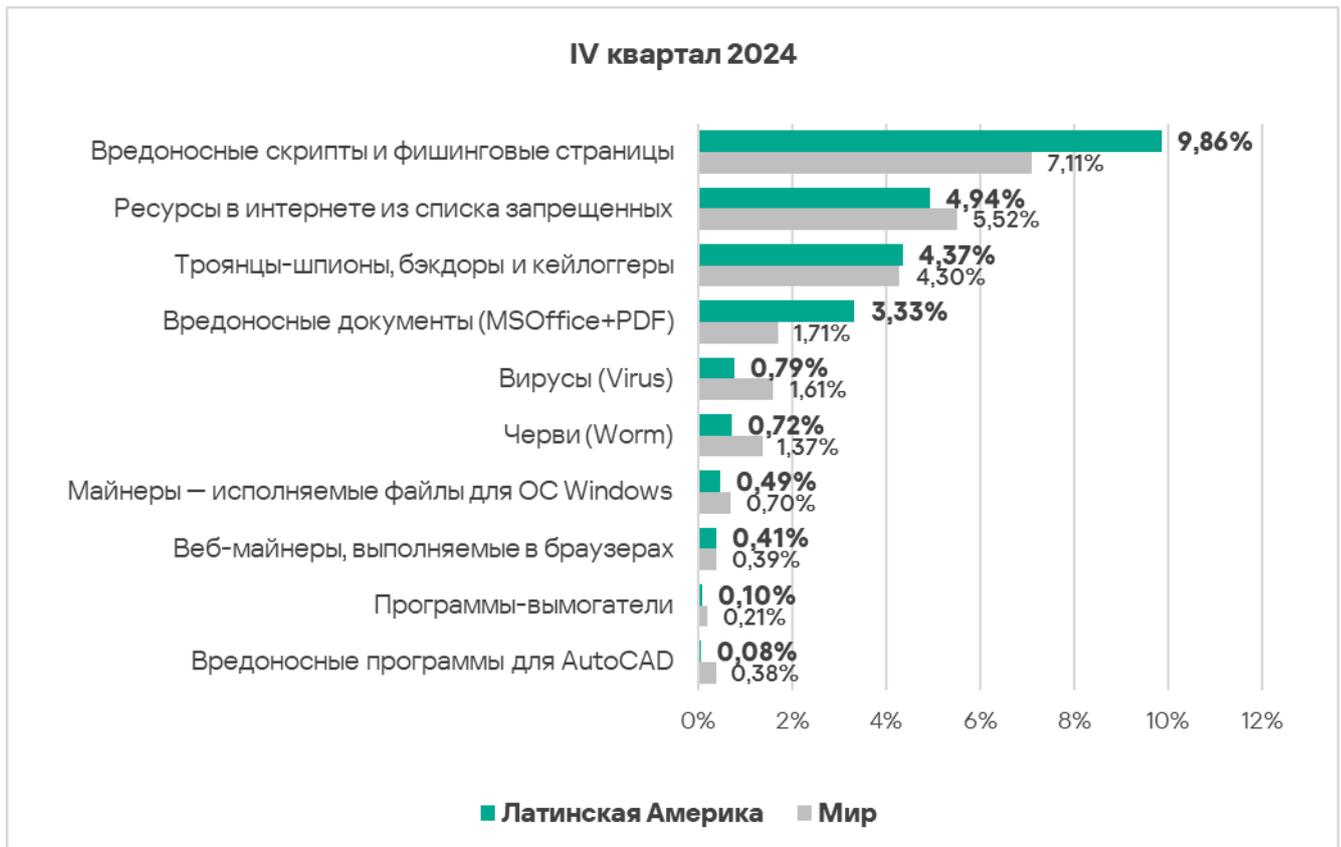
- Латинская Америка занимает **седьмое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. В прошлом квартале регион занимал пятое место.
- В **четвертом квартале 2024 года** показатель **уменьшился** и стал ниже среднемирового значения.
- В целом, в регионе наблюдается **нисходящий тренд**.



Сравнительный анализ

Категории угроз

- По сравнению с мировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
 - вредоносные документы — в 1,9 раза, второе место в мире;
 - вредоносные скрипты и фишинговые страницы — в 1,4 раза, второе место в мире;
 - веб-майнеры — в 1,1 раза.



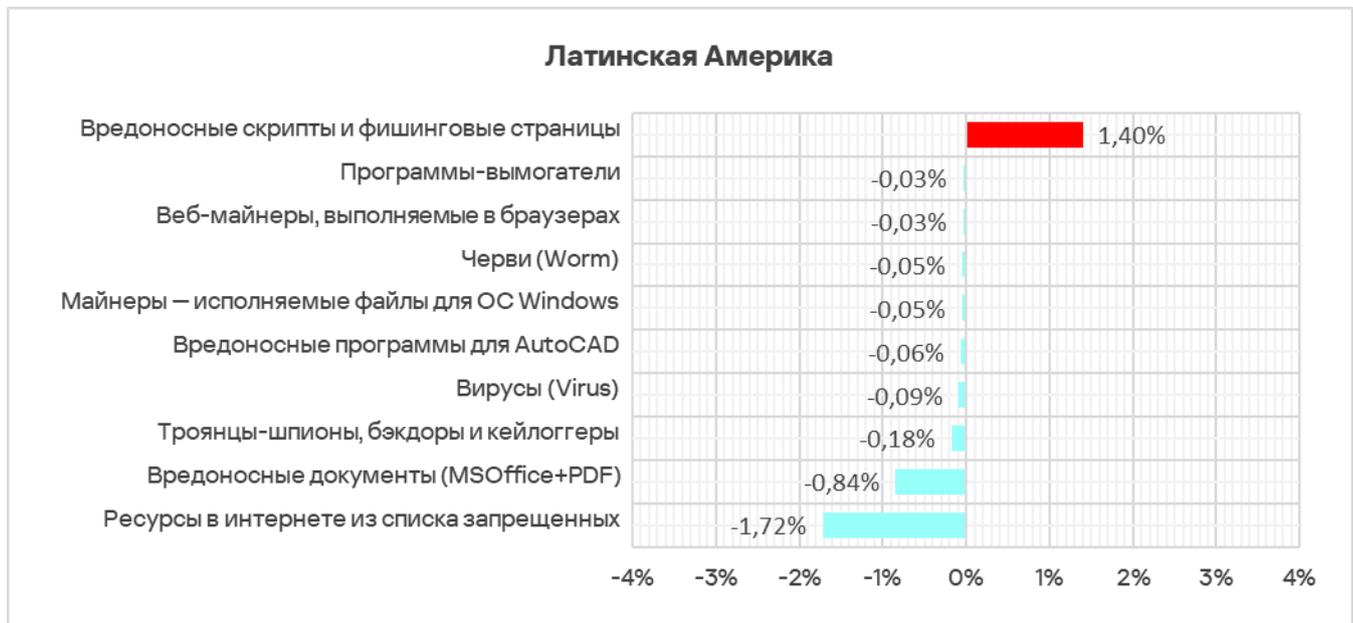
Источники угроз

- Латинская Америка занимает **третье место** в мировом рейтинге по доле компьютеров АСУ, на которых заблокированы угрозы из **почтовых клиентов**, с превышением среднемирового значения в 1,7 раза.
- Уровень угроз из **интернета** выше среднемирового значения в 1,1 раза.

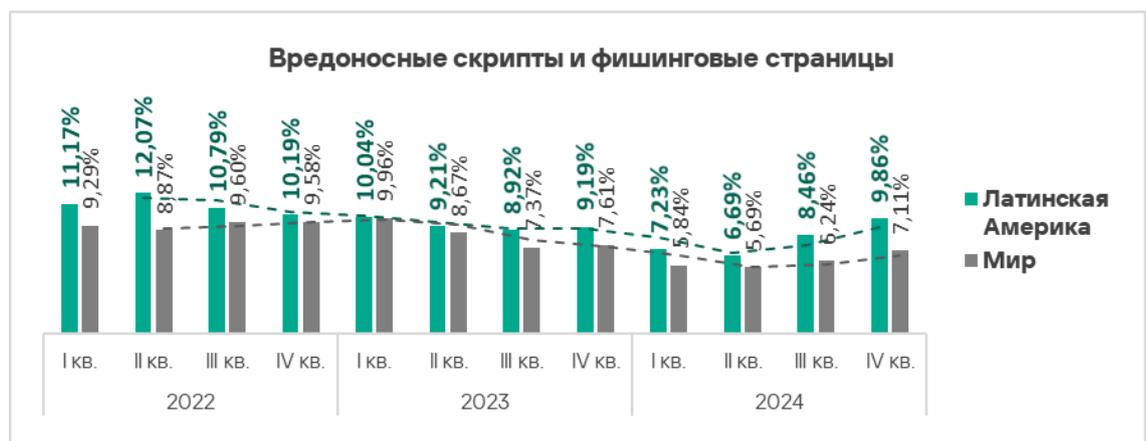


Изменения за квартал и тренды

Категории угроз



- **Наибольший прирост в процентах** за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
 - вредоносные скрипты и фишинговые страницы — в 1,2 раза.

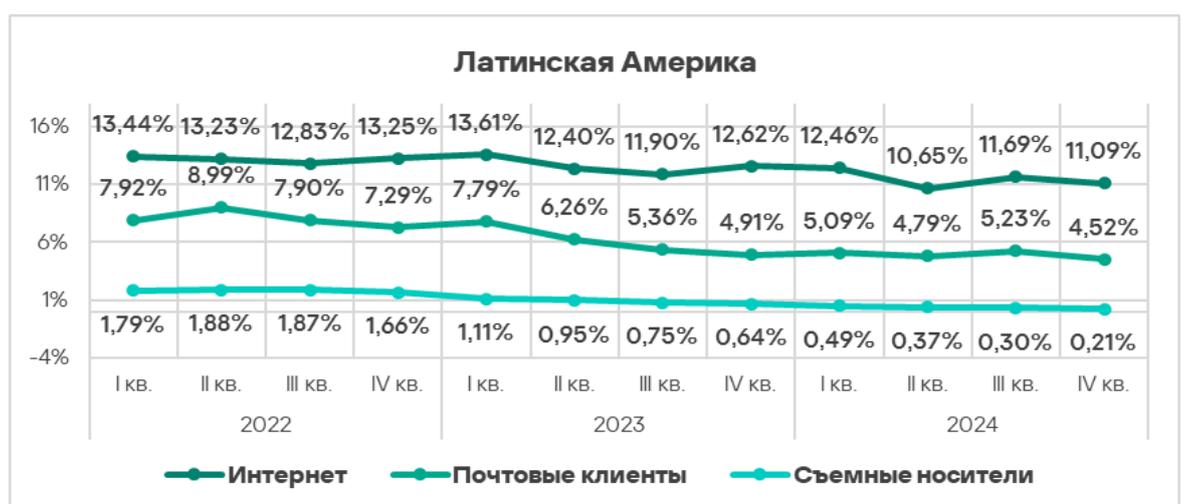


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Латинской Америке с начала 2022 года. На протяжении всего этого времени **вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе. В четвертом квартале 2024 года **программы-вымогатели** переместились на одну позицию вверх.

Латинская Америка	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	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	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	4	3	4	4	4	4	3	3	3	3	3
Вредоносные документы (MSOffice+PDF)	4	3	4	3	3	3	3	4	4	4	4	4
Вирусы (Virus)	8	8	8	7	6	6	6	6	5	6	5	5
Черви (Worm)	7	6	6	6	5	5	5	5	6	5	6	6
Майнеры – исполняемые файлы для ОС Windows	5	5	7	8	8	8	8	7	7	7	7	7
Веб-майнеры, выполняемые в браузерах	6	7	5	5	7	7	7	8	8	8	8	8
Программы-вымогатели	9	9	9	9	9	9	9	9	9	9	10	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	10	9	10

Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

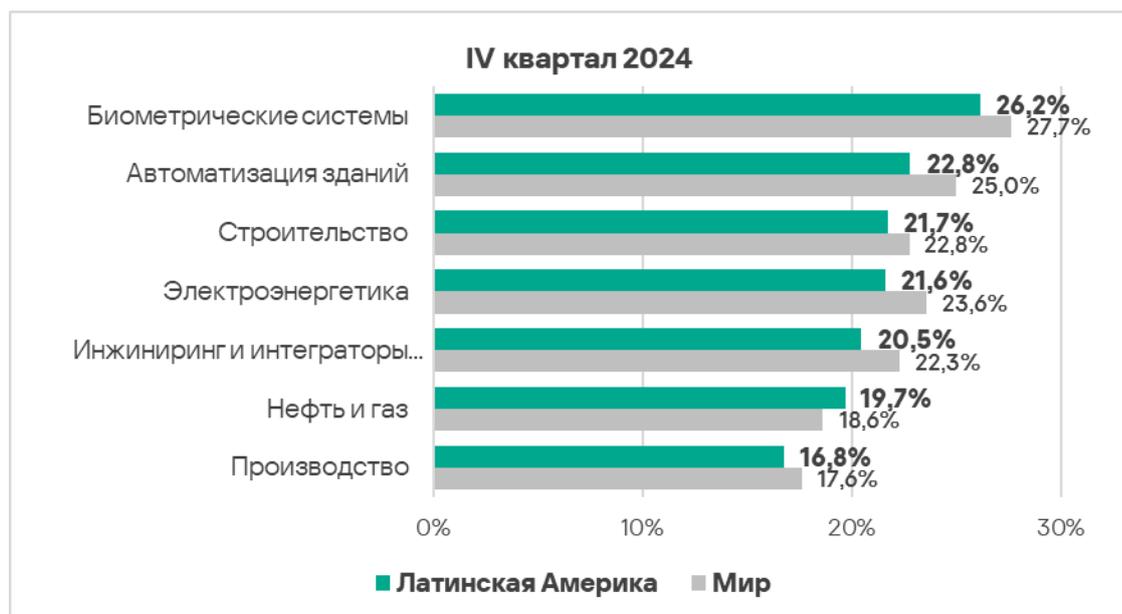


- Уровень угроз из **почтовых клиентов** (с точки зрения доли компьютеров АСУ, на которых они были заблокированы) демонстрирует плавно **нисходящий тренд**, что соответствует общемировому тренду, однако региональный показатель значительно превышает среднемировой.



Отрасли

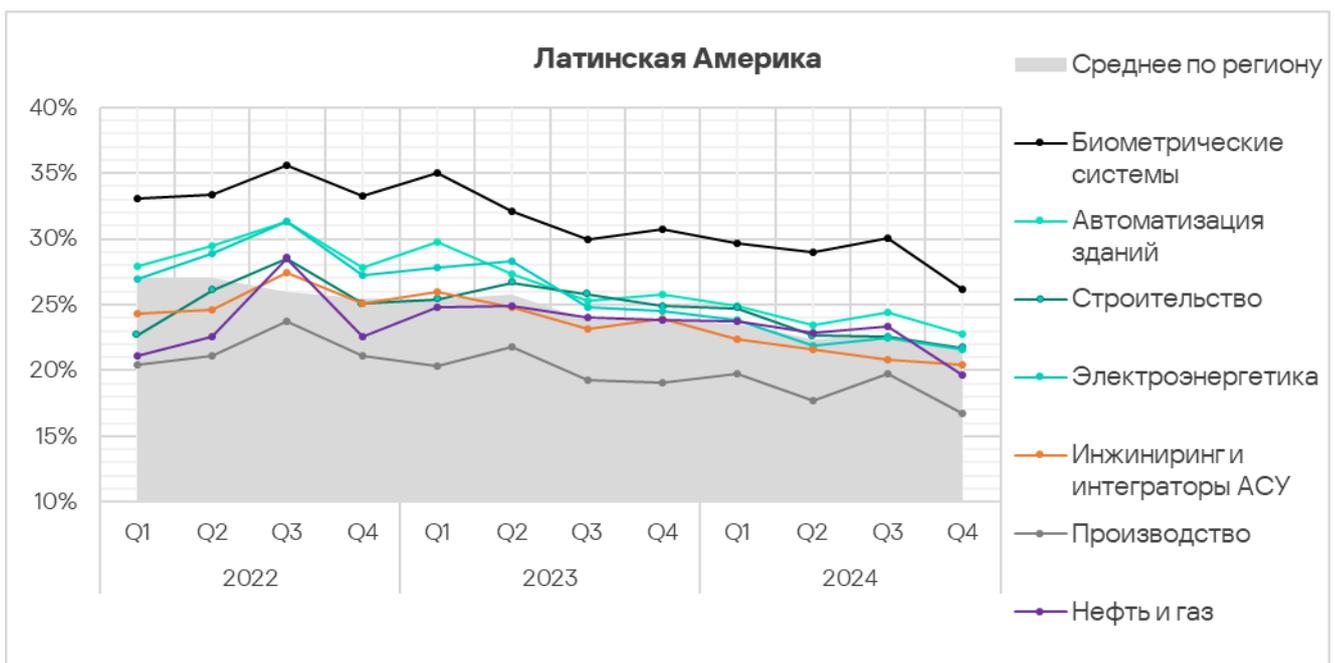
- Наиболее часто встречающаяся с угрозами отрасль** в регионе из рассмотренных в отчете — **биометрические системы**.
- В **нефтегазовой отрасли** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **превышает среднемировое значение** в 1,1 раза.



- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех рассматриваемых отраслях.



- Рассмотренные отрасли, несмотря на колебания, демонстрируют преимущественно **позитивную динамику** долгосрочных **трендов** начиная с первого квартала 2023 года.



Южная Азия

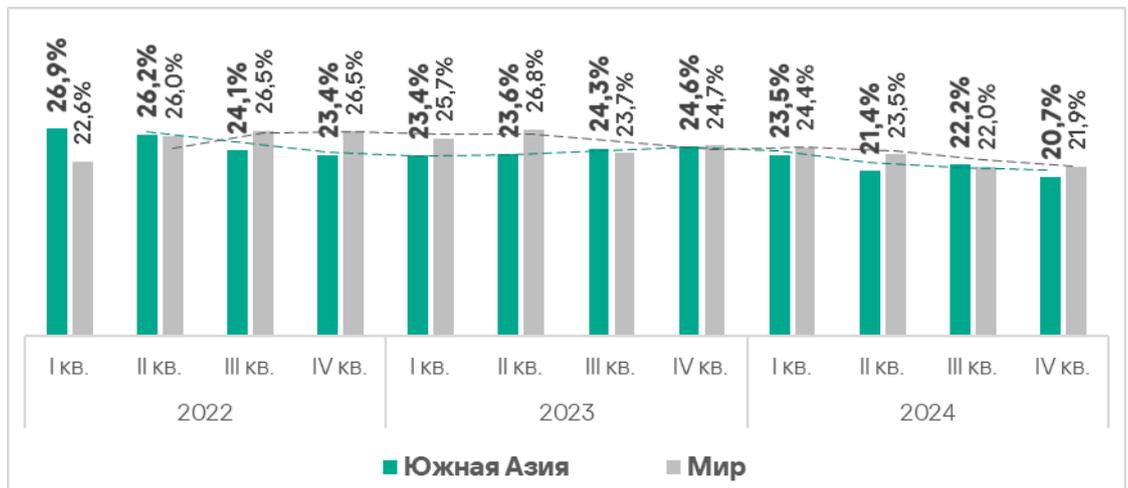
Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>7,06% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>5,53% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>2,90% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ слабый рост в IV кв. 2024 г.</p>
<p>1,77% ВИРУСЫ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>1,46% ЧЕРВИ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 1,1x выше среднего по миру</p>	<p>0,35% ВРЕДНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD</p> <p>▲ 1,3x рост в IV кв. 2024 г. 2-е место по росту</p>
<p>0,23% ПРОГРАММЫ- ВЫМОГАТЕЛИ</p> <p>▲ слабый рост в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,1x выше среднего по миру</p>		
<p>10,45% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>1,18% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p> <p>🌐 3-е место в мире 1,8x выше среднего по миру</p>	<p>0,18% СЕТЕВЫЕ ПАПКИ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ 1,1x рост в IV кв. 2024 г. (единственный регион, где показатель вырос)</p> <p>🌐 3-е место в мире</p>

2,3x выше среднего
по миру

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.
- В **четвертом квартале 2024 года** показатель **уменьшился** и стал ниже среднемирового значения.



Сравнительный анализ

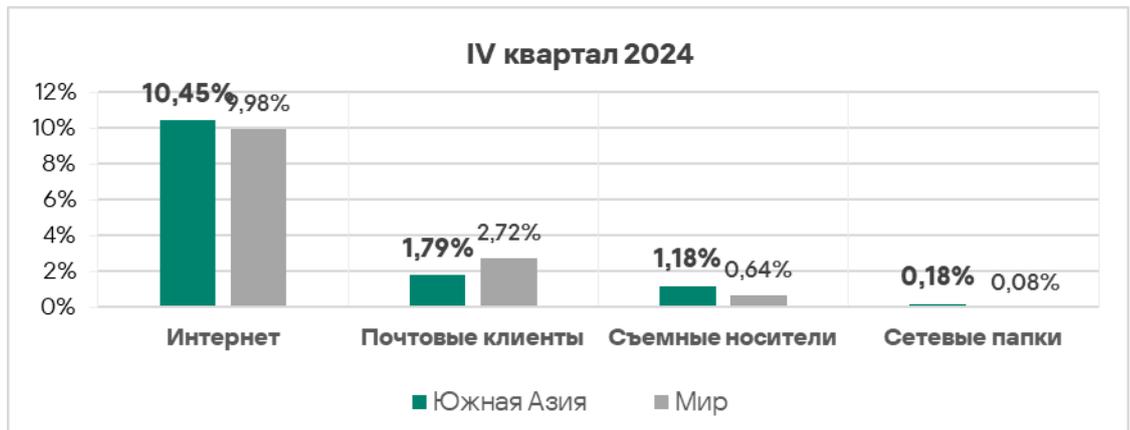
Категории угроз



- По сравнению со среднемировыми показателями в регионе заметно **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
 - черви – в 1,1 раза;
 - вирусы – в 1,1 раза;
 - программы-вымогатели – в 1,1 раза.

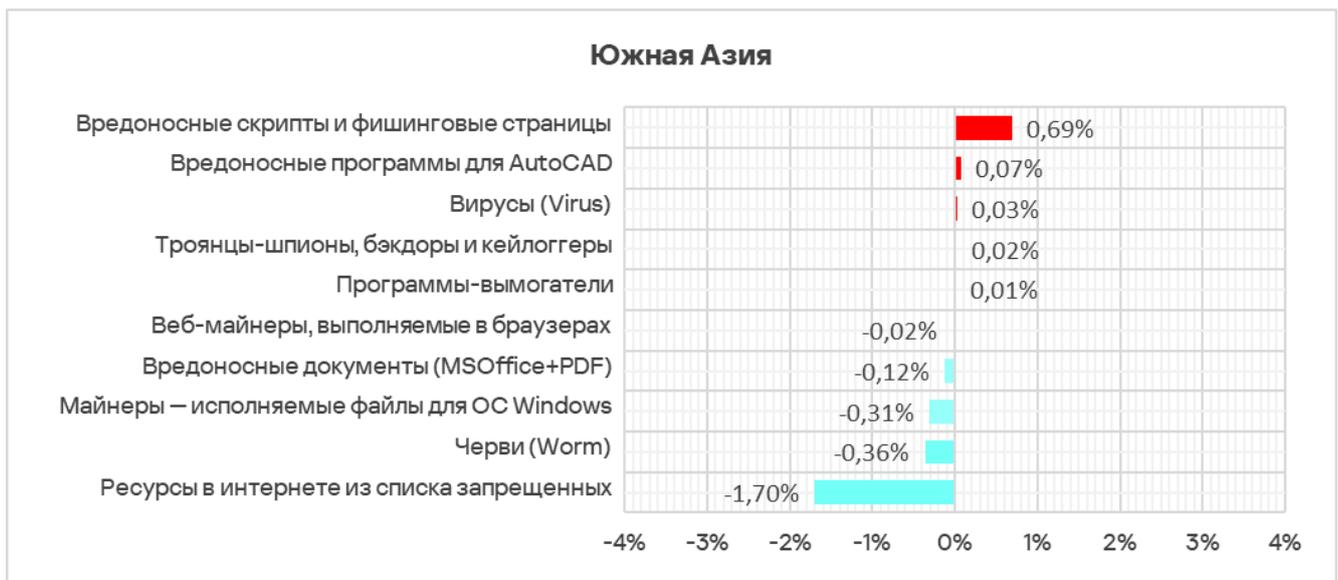
Источники угроз

- Южная Азия занимает **третье место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы **на съемных носителях**, с превышением среднемирового показателя в 1,8 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 2,3 раза.

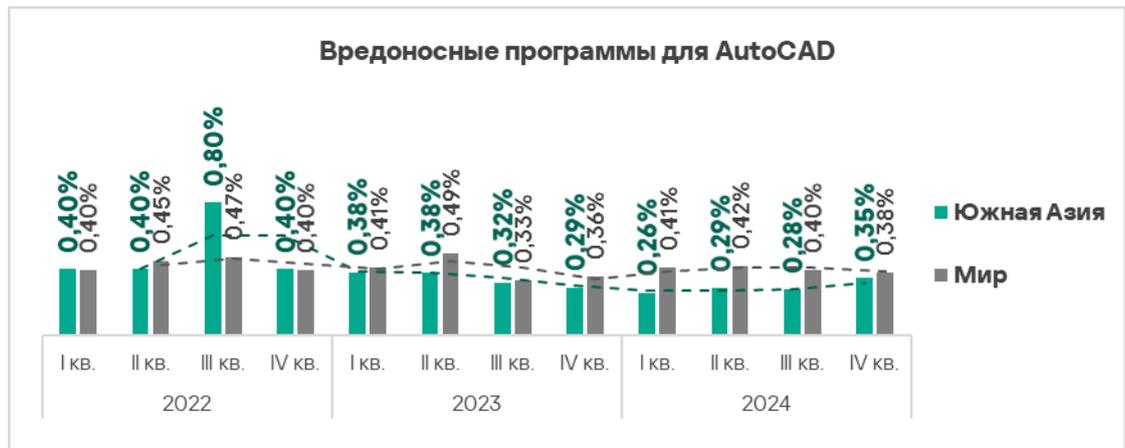


Изменения за квартал и тренды

Категории угроз



- **Наибольший прирост в процентах** за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
 - вредоносные программы для AutoCAD – в 1,3 раза;



➤ вредоносные скрипты и фишинговые страницы — в 1,1 раза.



- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Азии с начала 2022 года. В четвертом квартале 2024 года **вредоносные скрипты и фишинговые страницы** заняли верхнюю строчку. **Вирусы** поднялись на четвертую позицию (вирусы и черви стабильно удерживают высокие места на протяжении рассматриваемого периода), а **вредоносные программы для AutoCAD** — на восьмую.

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

Источники угроз

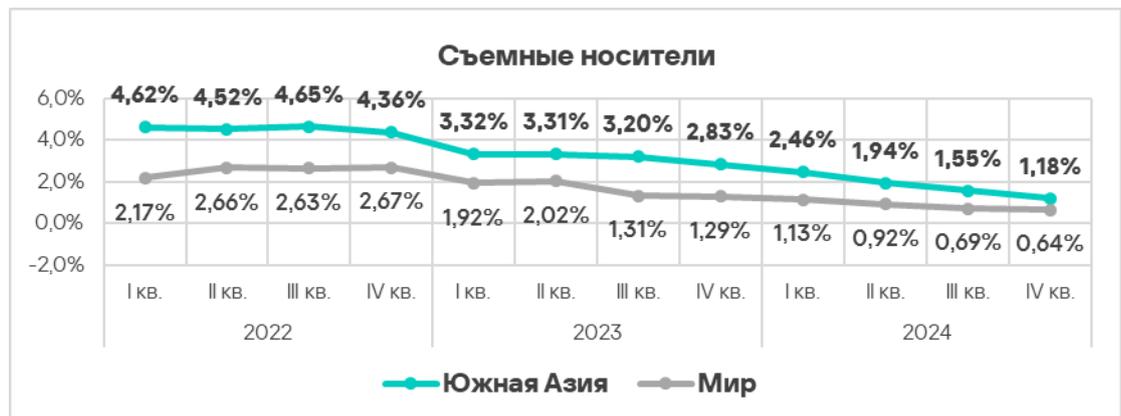
- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у большинства источников угроз.



- Уровень угроз из **сетевых папок** вырос и тем самым увеличил разрыв между региональным и среднемировым значениями.

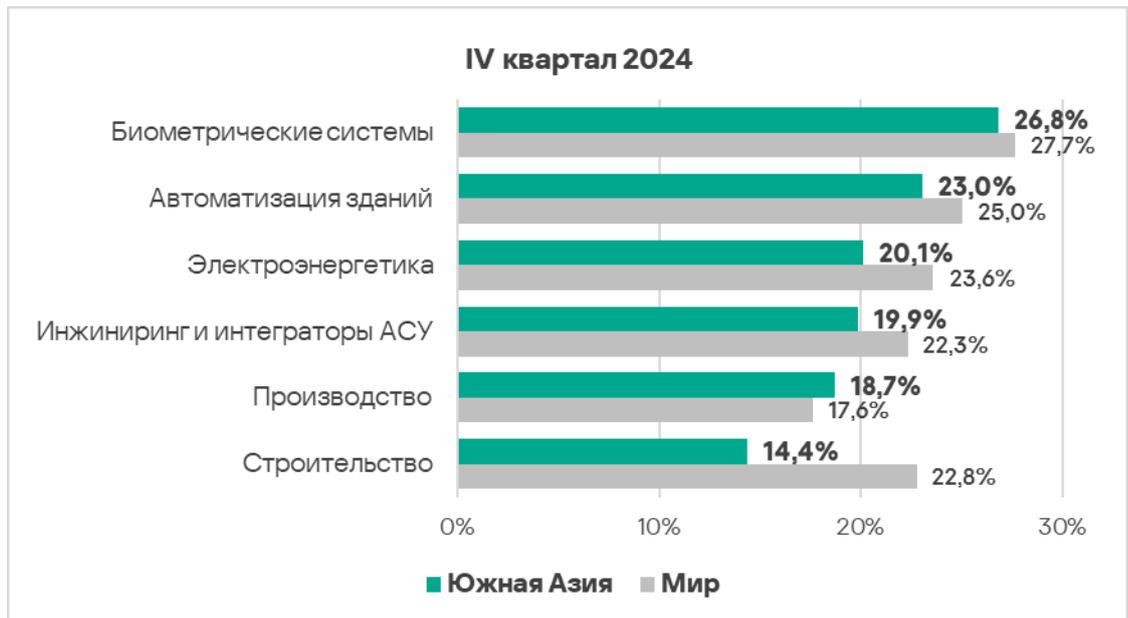


- Уровень угроз на **съемных носителях** продолжает демонстрировать **нисходящий тренд**, однако все еще остается значительно выше соответствующего среднемирового значения.



Отрасли

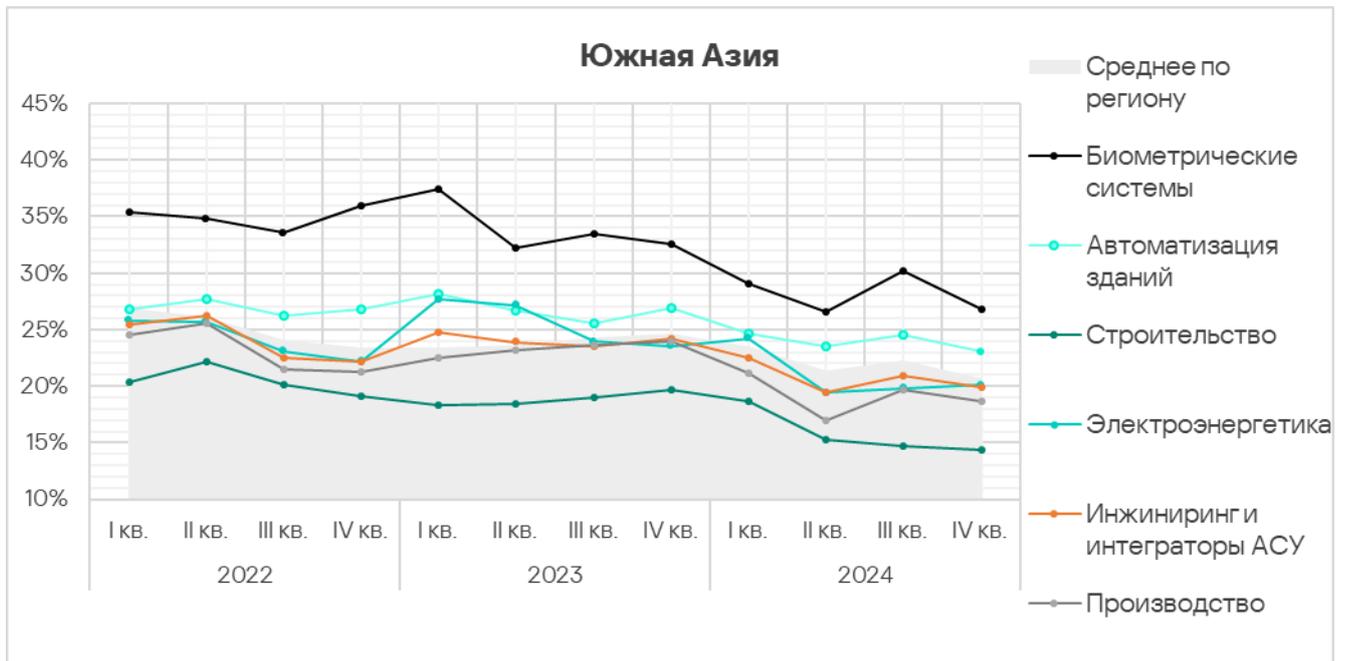
- **Наиболее часто встречающаяся с угрозами отрасль** региона из рассмотренных в отчете — **биометрические системы**.
- **По сравнению с данными по миру** во всех рассматриваемых отраслях, кроме производства, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **ниже соответствующих среднемировых значений**.



- В **четвертом квартале 2024 года** во всех рассмотренных отраслях региона, кроме электроэнергетики, зафиксировано **снижение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



- Рассмотренные отрасли по большей части демонстрируют **положительную динамику** долгосрочных **трендов**, но с существенными колебаниями.



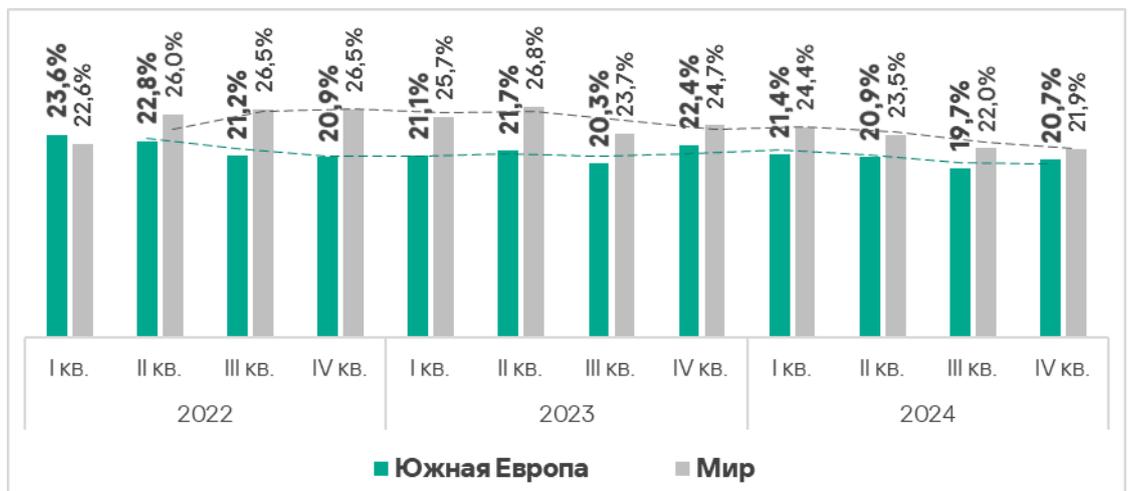
Южная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>10,13% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 2-е место по росту</p> <p>🌐 2-е место в мире 1,4x выше среднего по миру</p>	<p>6,38% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 1-е место по росту</p> <p>🌐 3-е место в мире 1,5x выше среднего по миру</p>	<p>4,75% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>
<p>3,70% ВРЕДОНОСНЫЕ ДОКУМЕНТЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 1-е место по росту</p> <p>🌐 1-е место в мире 2,2x выше среднего по миру</p>	<p>0,81% ЧЕРВИ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p>	<p>0,29% ВЕБ-МАЙНЕРЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 2-е место по росту</p>
<p>0,26% МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>9,74% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ слабый рост в IV кв. 2024 г. 3-е место по росту</p>	<p>6,50% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ 1,1x рост в IV кв. 2024 г. 1-е место по росту</p> <p>🌐 1-е место в мире 2,4x выше среднего по миру</p>

Общая ситуация

- Южная Европа делит с Южной Азией **восьмое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Показатель, как правило, **ниже среднемирового значения**.
- В **четвертом квартале 2024 года** он **вырос** в 1,1 раза. Регион занимает второе место по росту этого показателя.



Сравнительный анализ

Категории угроз



- По сравнению со среднемировыми показателями в регионе **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:
 - вредоносные документы — в 2,2 раза (также выше значения за третий квартал 2024 года), первое место в мире;
 - шпионские программы — в 1,5 раза (также выше значения за третий квартал 2024 года), третье место в мире;
 - вредоносные скрипты и фишинговые страницы — в 1,4 раза (также выше значения за третий квартал 2024 года), второе место в мире.

Источники угроз

- Южная Европа находится **на первом месте в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**. По сравнению с предыдущим кварталом значение показателя выросло и теперь превышает среднемировое в 2,4 раза.



Изменения за квартал и тренды

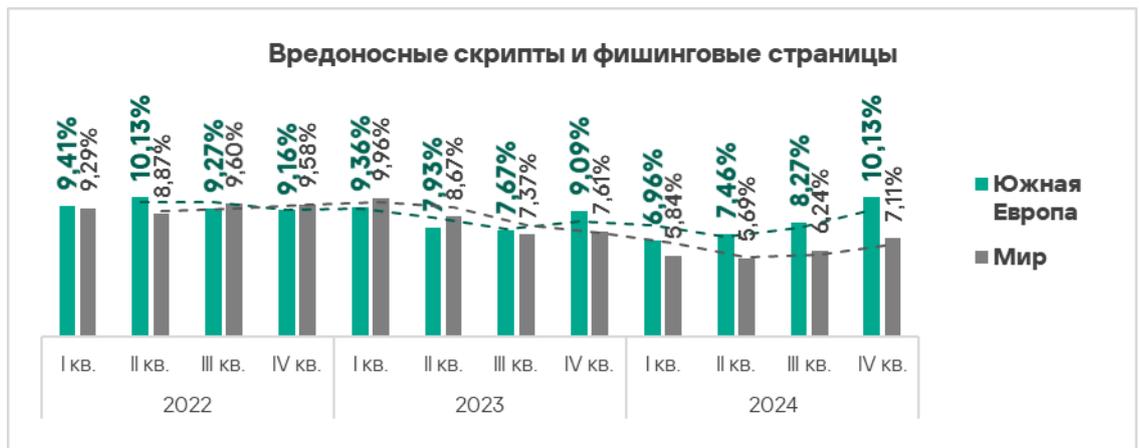
Категории угроз



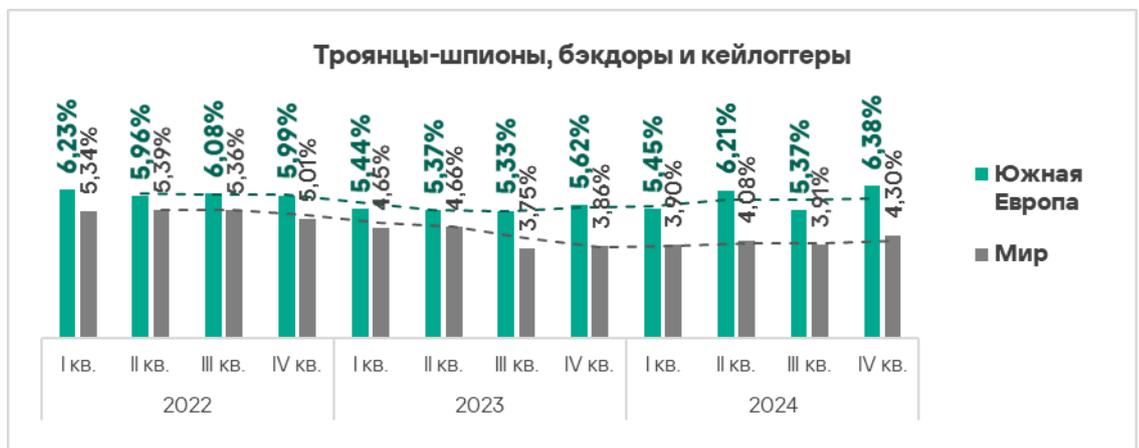
- В октябре 2024 года на промышленные организации Южной Европы обрушилась волна фишинговых электронных писем. По данным Kaspersky Security Network, большинство атак было направлено на компании в Испании и Португалии. Среди проанализированных нами образцов вредоносного ПО, которые распространялись в этих электронных письмах, были обнаружены фишинговые PDF-документы, содержащие ссылки на вредоносные веб-ресурсы, исполняемые файлы и установочные файлы с вредоносным кодом в виде скриптов и шелл-кода, предназначенных для загрузки шпионских программ. Резкий рост в регионе доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты, вредоносные документы и шпионские

программы, отражает масштаб этой волны. Дополнительная информация: [GuLoader: Evolving Tactics in Latest Campaign Targeting European Industry.](#)

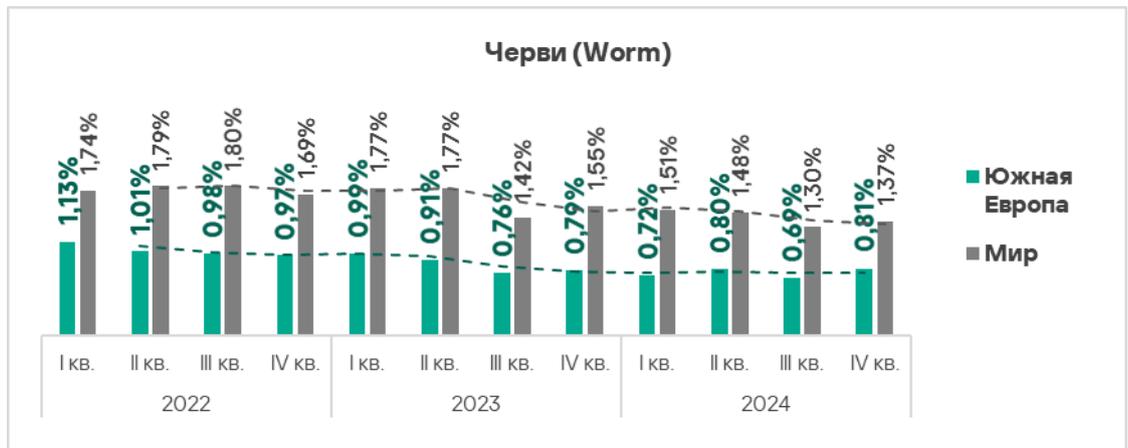
- **Наибольший прирост в процентах за квартал** произошел у доли компьютеров АСУ, на которых были заблокированы следующие категории угроз:
 - вредоносные скрипты и фишинговые страницы — в 1,2 раза, второе место по росту показателя в мире;



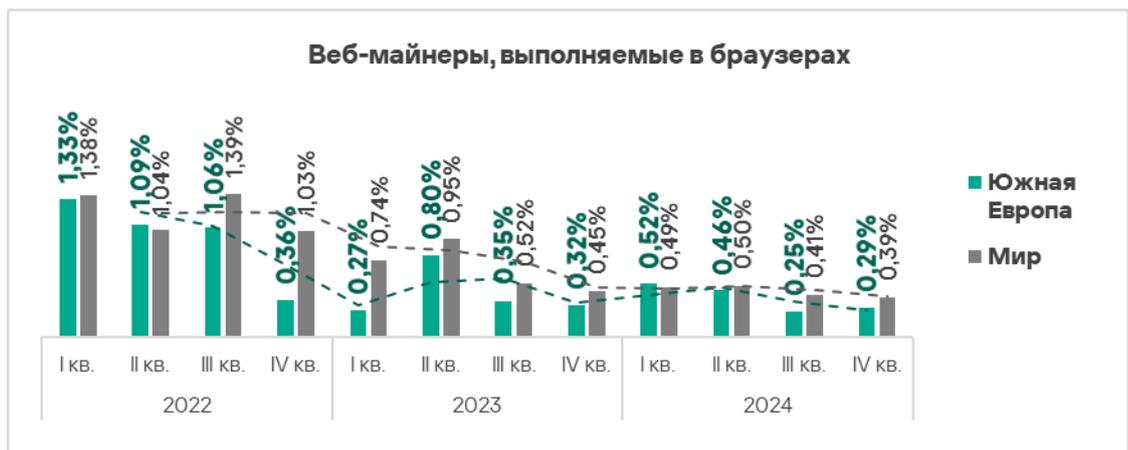
- шпионские программы — в 1,2 раза, первое место по росту показателя в мире;



- черви — в 1,2 раза;



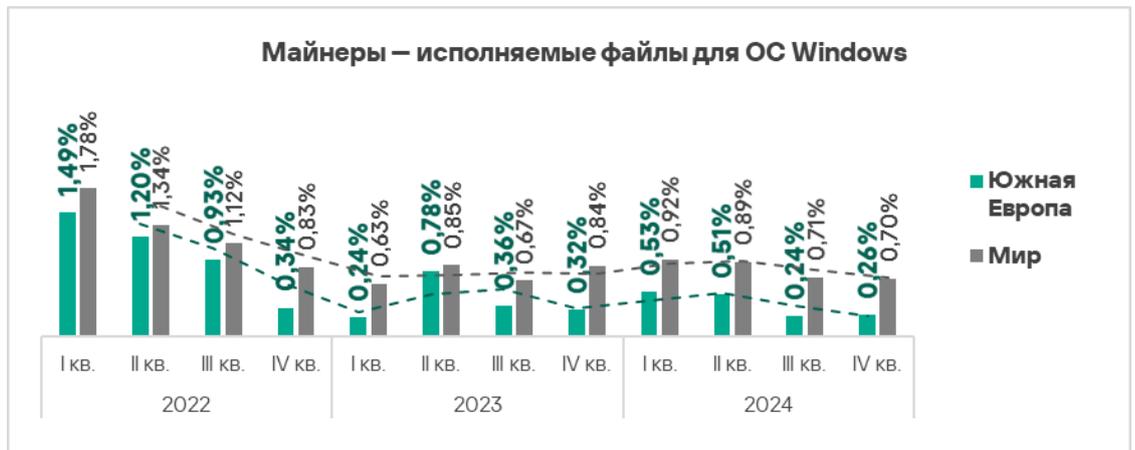
- веб-майнеры — в 1,2 раза, второе место по росту показателя в мире;



- вредоносные документы — в 1,1 раза, первое место по росту показателя в мире;



- майнеры — исполняемые файлы для ОС Windows — в 1,1 раза.

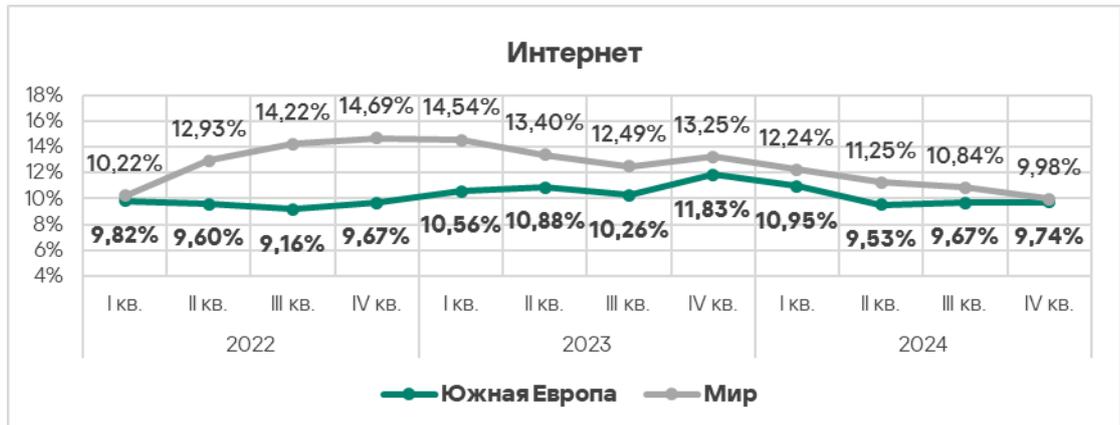


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Европе с начала 2022 года. **Вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе на протяжении всего рассматриваемого периода. В четвертом квартале 2024 года **шпионские программы** вернулись с третьего места на второе.

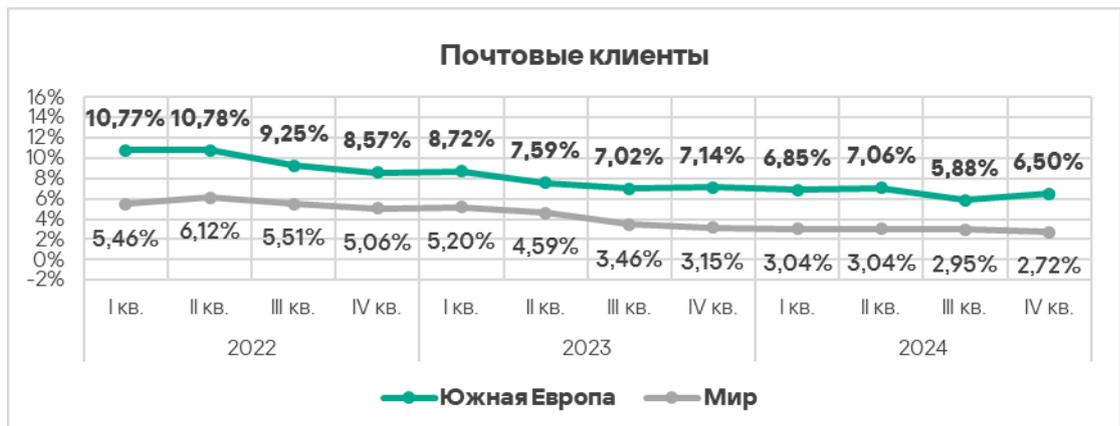
Южная Европа	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	1	1	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	2	2	3	3	2	3	3	2	3	2
Ресурсы в интернете из списка запрещенных	4	4	4	4	2	2	3	2	2	3	2	3
Вредоносные документы (MSOffice+PDF)	2	2	3	3	4	4	4	4	4	4	4	4
Черви (Worm)	7	7	6	5	5	5	5	5	5	5	5	5
Вирусы (Virus)	8	8	8	8	6	8	8	6	8	8	6	6
Веб-майнеры, выполняемые в браузерах	6	6	5	6	7	6	7	8	7	7	7	7
Майнеры – исполняемые файлы для ОС Windows	5	5	7	7	8	7	6	7	6	6	8	8
Программы-вымогатели	9	9	9	9	9	10	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	9	10	10	10	10	10	10

Источники угроз

- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета, выросла** и таким образом разошлась с общемировым трендом.



- Уровень угроз из **почтовых клиентов** по сравнению с предыдущим кварталом **вырос** в 1,1 раза.



Отрасли

- Наиболее часто встречающаяся с угрозами отрасль региона из рассмотренных в отчете — **биометрические системы**.
- В **биометрических системах** и **автоматизации зданий** зафиксирована наиболее высокая доля компьютеров АСУ, на которых были заблокированы угрозы.

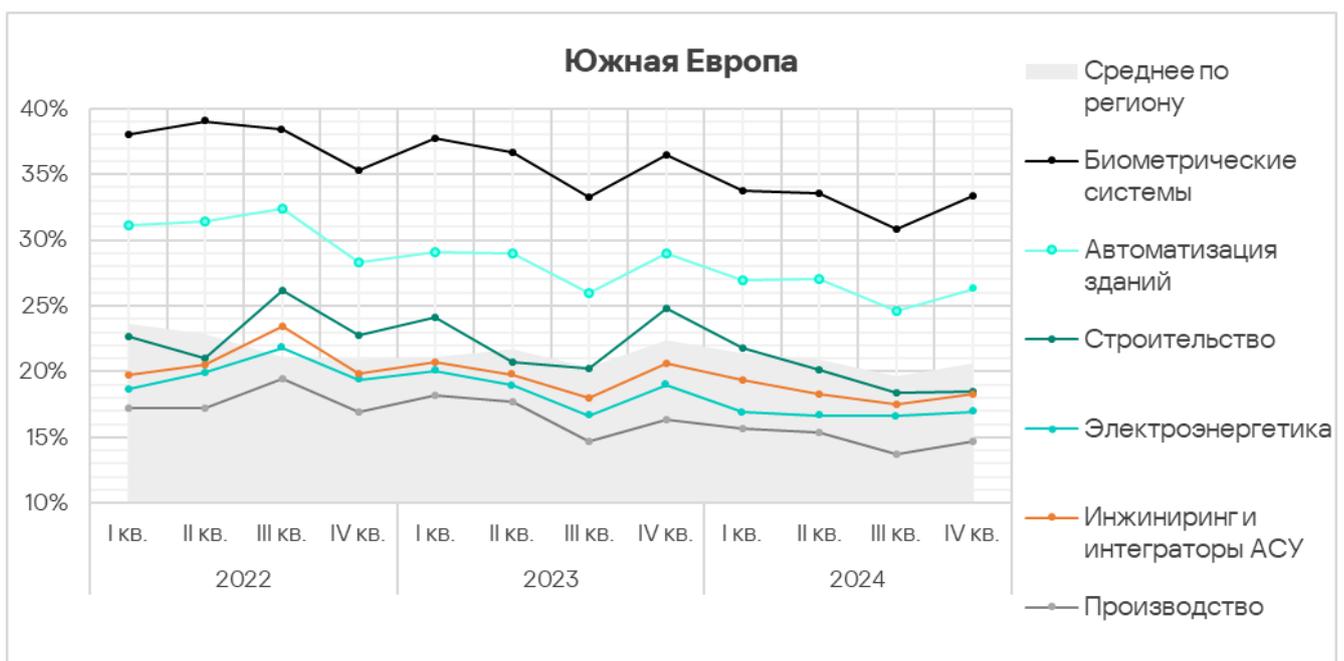
вредоносные объекты — в 1,2 и 1,1 раза **выше среднемирового значения** соответственно.



- В **четвертом квартале 2024 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла** во всех рассмотренных отраслях региона. Наибольший прирост за квартал отмечен в следующих отраслях:
 - биометрические системы — в 1,1 раза;
 - автоматизация зданий — в 1,1 раза;
 - производство — в 1,1 раза.



- Все рассмотренные отрасли демонстрируют **колебательные тренды** изменения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Что касается **биометрических систем** и **автоматизации зданий**, то в этих отраслях показатель все еще значительно **превышает** среднее значение для региона.



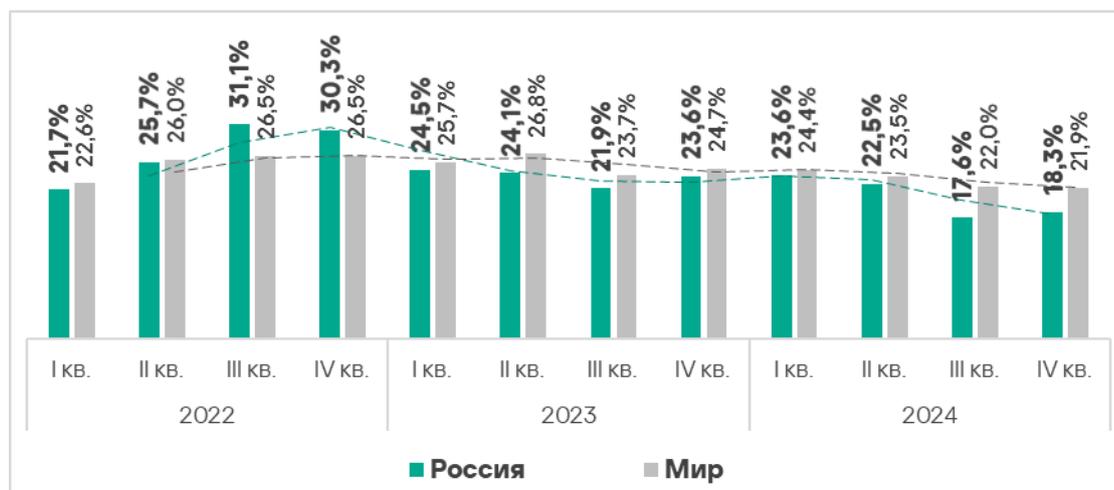
Россия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>5,27% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>4,25% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>2,78% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,3x рост в IV кв. 2024 г. 2-е место по росту</p>
<p>1,05% ЧЕРВИ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 2-е место по росту</p>	<p>1,03% МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 2-е место по росту</p> <p>🌐 2-е место в мире 1,5x выше среднего по миру</p>	
<p>8,04% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>0,29% СЪЕМНЫЕ НОСИТЕЛИ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 1-е место по росту</p>	

Общая ситуация

- Россия занимает **девятое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Показатель остается ниже среднемирового значения с начала 2023 года.
- **В четвертом квартале 2024 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла.



Сравнительный анализ

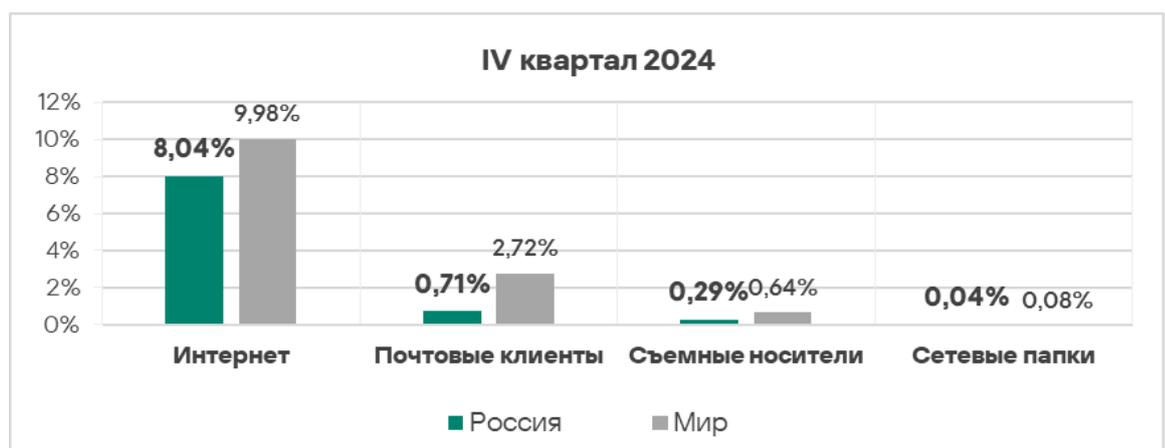
Категории угроз

- По сравнению со среднемировыми показателями в регионе **выше** доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows. Это значение превышает среднемировое в 1,5 раза (также оно выше значения за третий квартал 2024 года), это второе место в мире.



Источники угроз

- Показатели всех источников угроз в России **ниже** соответствующих **среднемировых значений**.

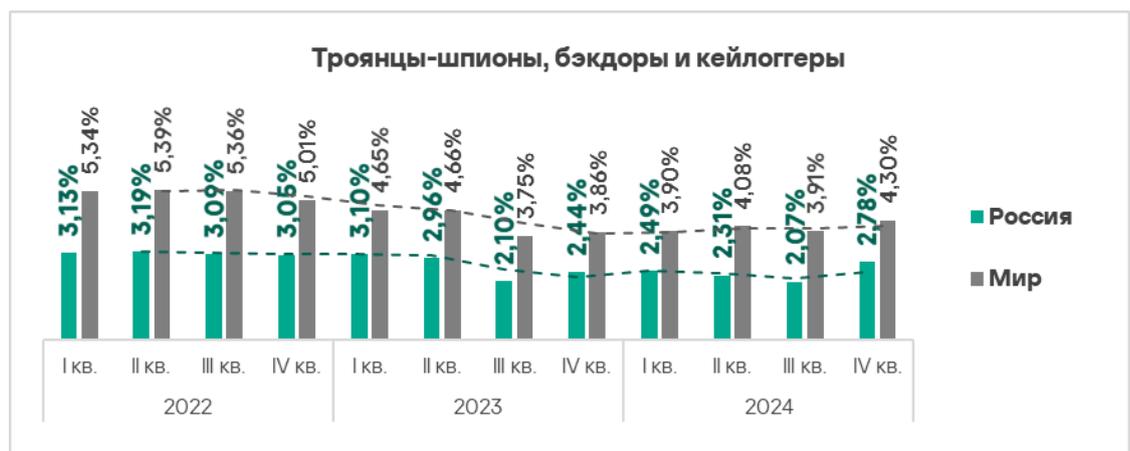


Изменения за квартал и тренды

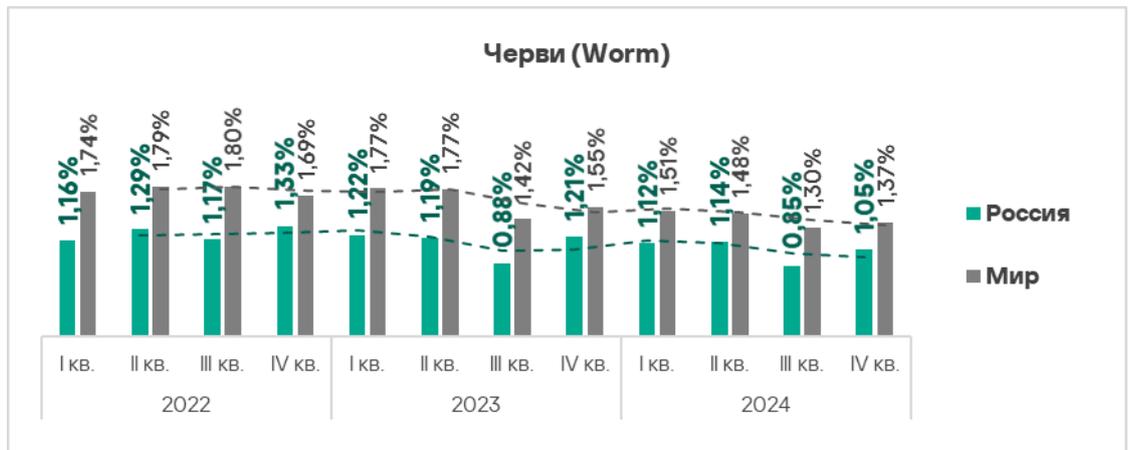
Категории угроз



- **Наибольший прирост в процентах за квартал** отмечен у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:
 - шпионские программы – в 1,3 раза, второе место по росту показателя в мире;



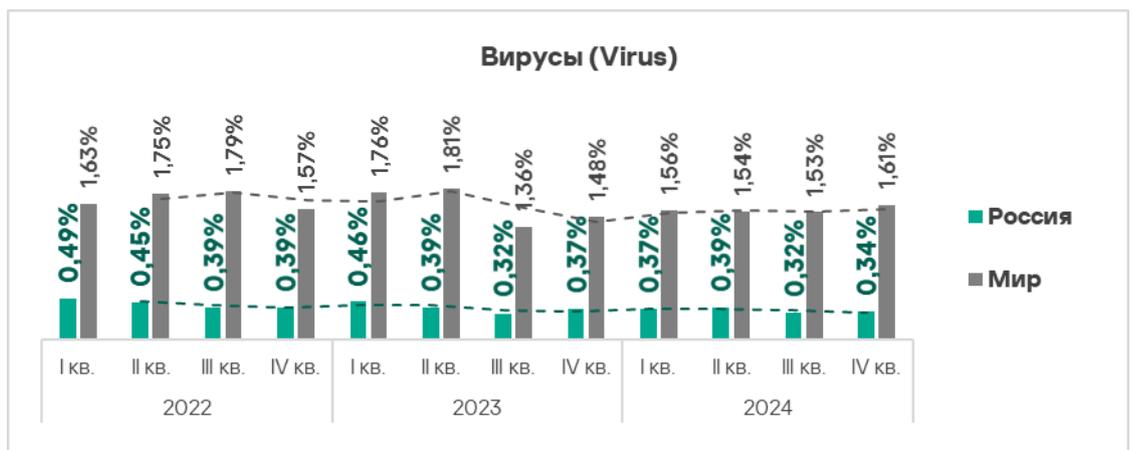
- черви – в 1,2 раза, второе место по росту показателя в мире;



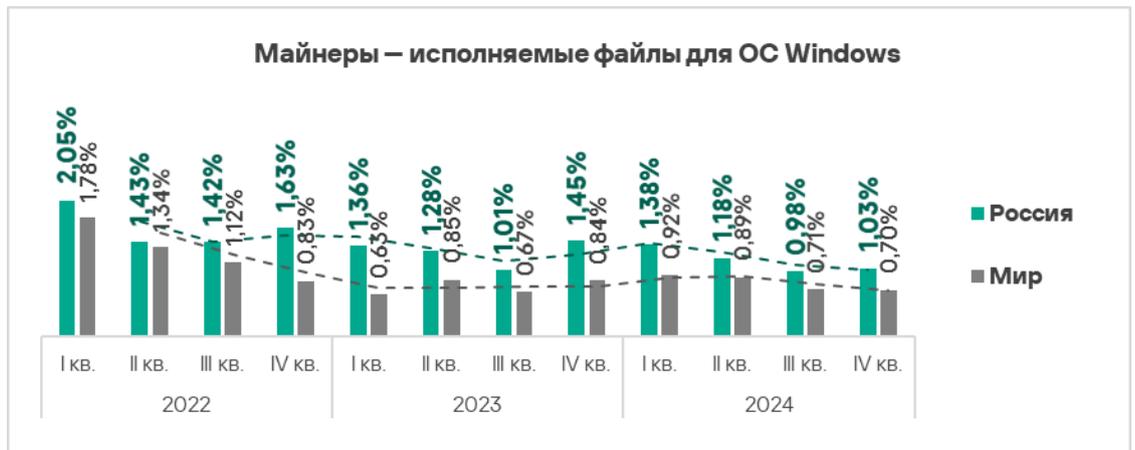
➤ вредоносные скрипты и фишинговые страницы — в 1,1 раза;



➤ вирусы — в 1,1 раза;



➤ майнеры — исполняемые файлы для ОС Windows — в 1,2 раза (в противовес мировой тенденции), второе место по росту показателя в мире.

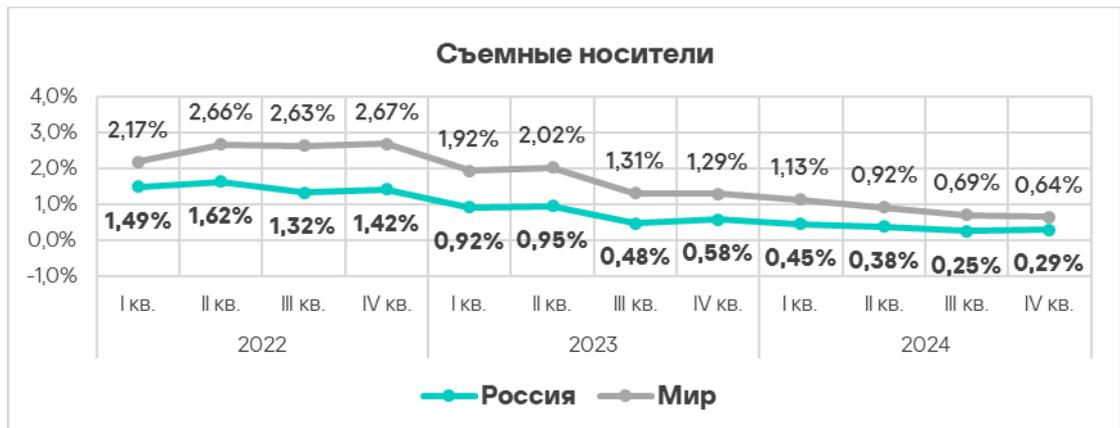


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в России с начала 2022 года. Ведущей категорией угроз в регионе, начиная с третьего квартала 2023 года, являются **ресурсы в интернете из списка запрещенных**. В четвертом квартале 2024 года **черви** поднялись с пятого места на четвертое.

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

Источники угроз

- Уровень угроз со **съемных носителей** в четвертом квартале 2024 года вырос в 1,2 раза. По росту этого показателя Россия занимает первое место в мире.



- Уровень угроз из **интернета, почтовых клиентов** и на **сетевых папках** снизился.





Отрасли

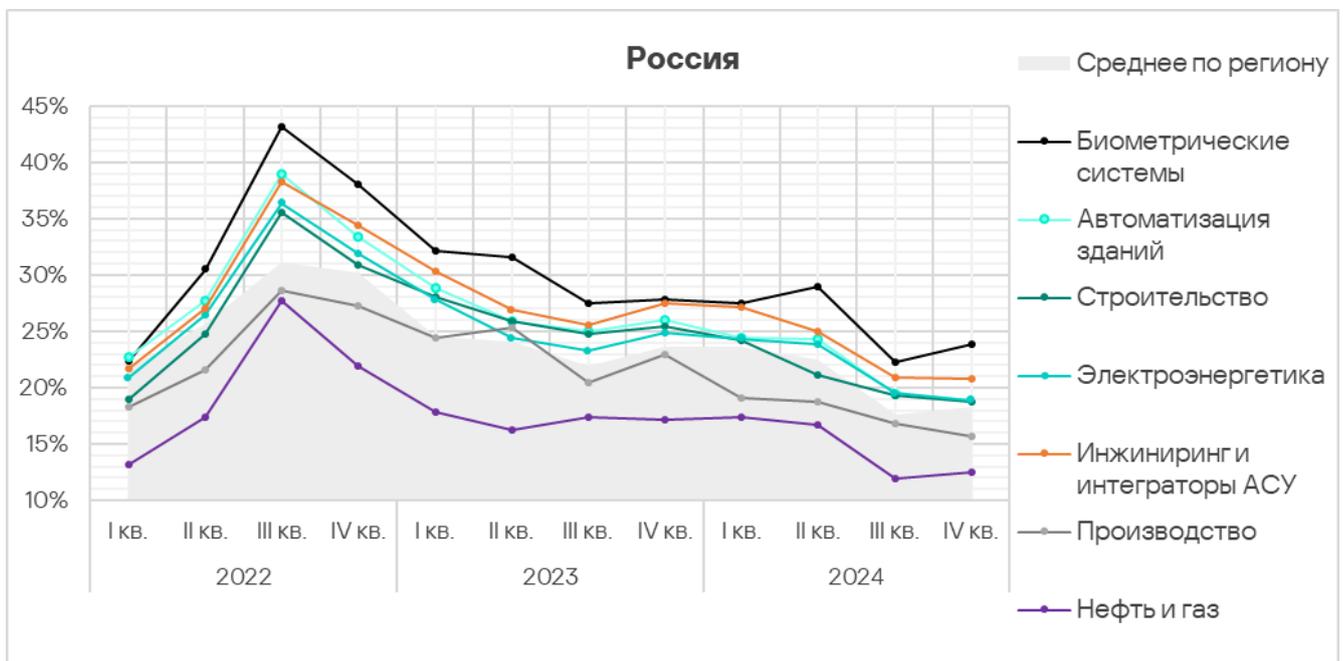
- **Наиболее часто встречающаяся с угрозами отрасль** региона среди рассмотренных в отчете — **биометрические системы**.
- Во всех отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **ниже** соответствующих **среднемировых показателей**.



- **В четвертом квартале 2024 года** в большинстве рассмотренных отраслей региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **снизилась**. Рост показателя наблюдался в нефтегазовой отрасли, а также секторе биометрических систем — здесь он увеличился в 1,1 раза.



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



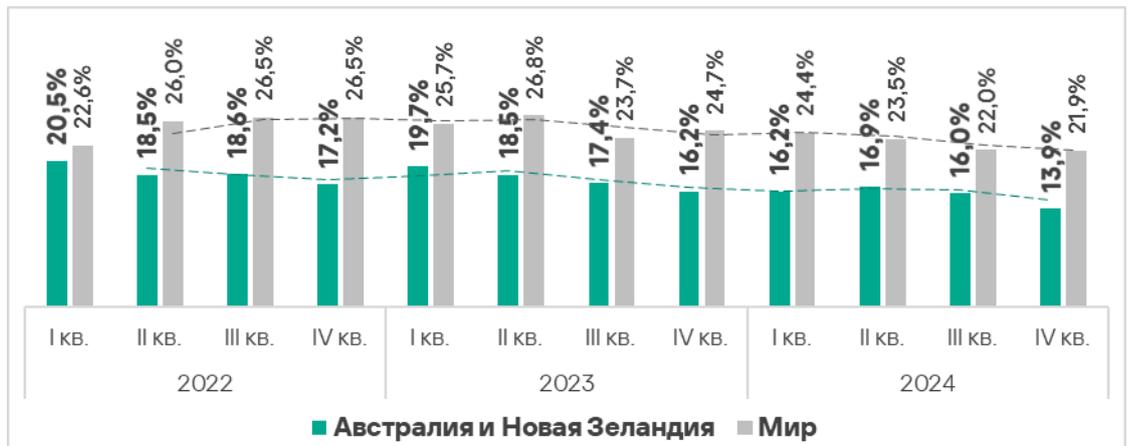
Австралия и Новая Зеландия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>6,34% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>3,31% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>1,86% ШПИОНСКИЕ ПРОГРАММЫ</p>
<p>1,46% ВРЕДНОСНЫЕ ДОКУМЕНТЫ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>0,09% ПРОГРАММЫ- ВЫМОГАТЕЛИ</p> <p>▲ 2,3x рост в IV кв. 2024 г. 1-е место по росту</p>	
<p>7,55% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>2,45% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	

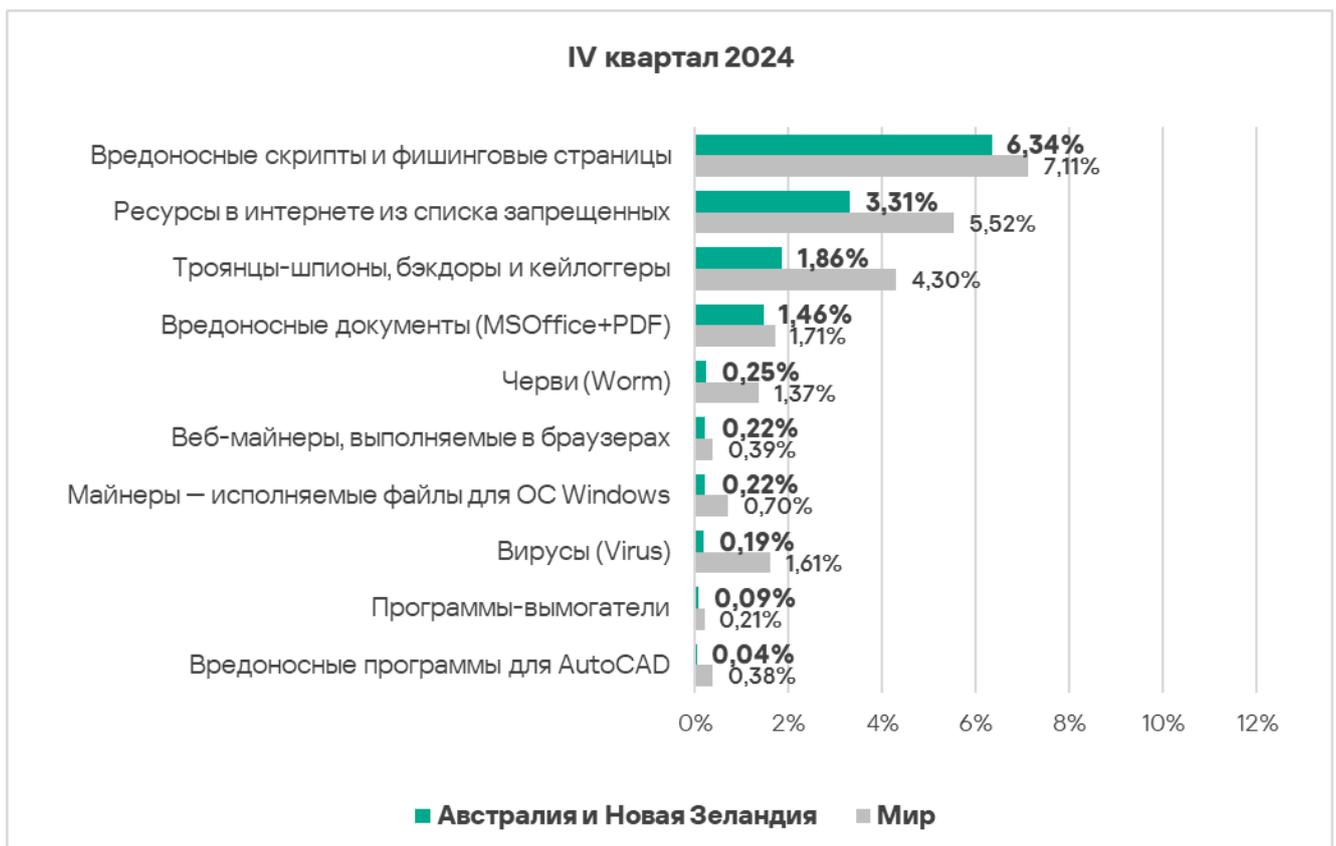
Общая ситуация

- Австралия и Новая Зеландия занимают **десятое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- **В четвертом квартале 2024** года этот показатель **снизился** примерно в 1,2 раза.
- Показатель существенно **ниже среднемирового значения**.



Сравнительный анализ

Категории угроз



- Доля компьютеров АСУ, на которых заблокированы вредоносные объекты, **ниже среднемирового значения** у всех категорий угроз.

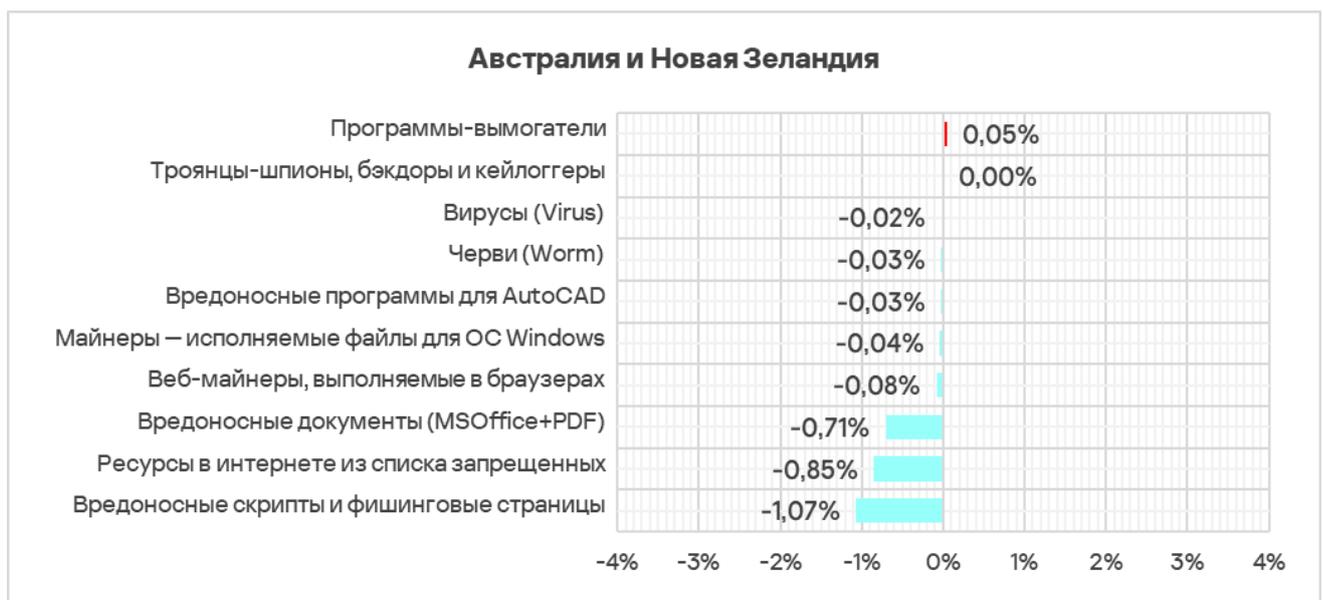
Источники угроз

- Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **ниже среднемирового значения** у всех источников угроз.

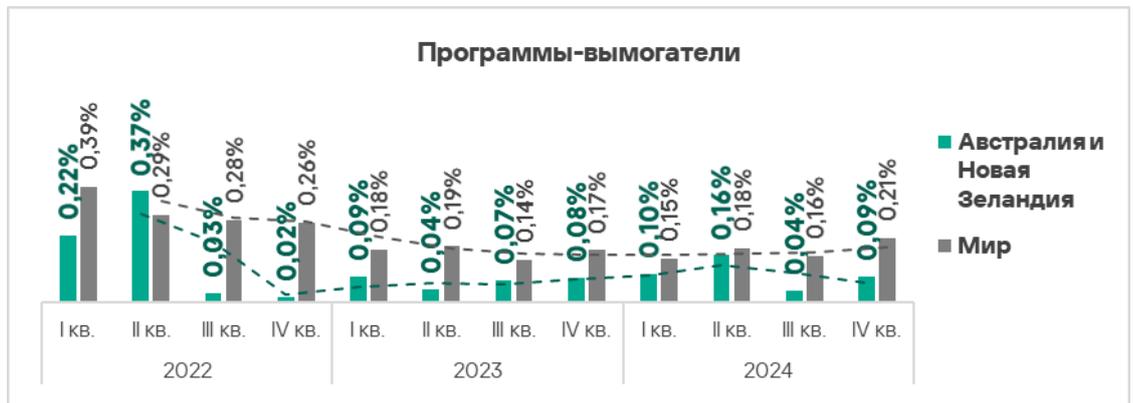


Изменения за квартал и тренды

Категории угроз



- Наибольший прирост в процентах за квартал** отмечен у доли компьютеров АСУ, на которых были заблокированы программы-вымогатели – в 2,3 раза. По росту этого показателя регион занимает первое место в мире.

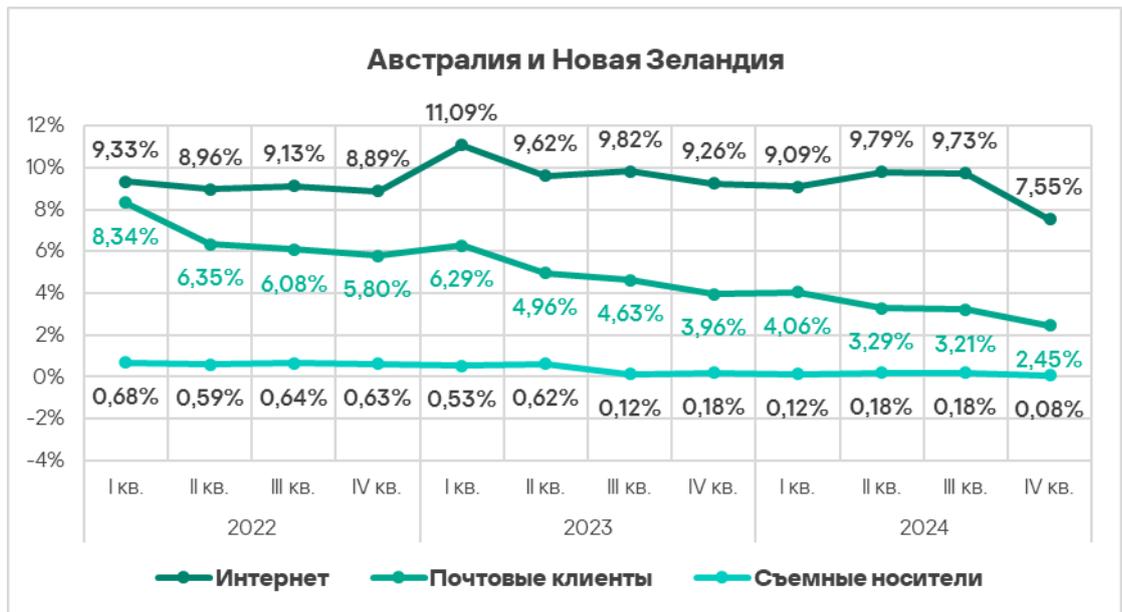


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Австралии и Новой Зеландии с начала 2022 года. Все это время **вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе, а ресурсы в интернете из списка запрещенных занимают второе место. В четвертом квартале 2024 года **шпионские программы** поднялись на третью строчку, сместив вредоносные документы, а **черви** — с шестой на пятую.

Австралия и Новая Зеландия	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	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	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	4	3	3	4	4	3	3	4	3
Вредоносные документы (MSOffice+PDF)	4	4	4	3	5	4	3	3	4	4	3	4
Черви (Worm)	8	6	8	8	6	6	7	8	7	7	6	5
Веб-майнеры, выполняемые в браузерах	6	9	6	5	8	6	5	5	5	6	5	6
Майнеры – исполняемые файлы для ОС Windows	5	8	7	6	9	8	6	6	6	5	7	6
Вирусы (Virus)	7	5	5	7	4	5	8	7	8	8	8	7
Программы-вымогатели	9	10	10	10	10	10	9	9	9	9	10	8
Вредоносные программы для AutoCAD	10	7	9	9	7	9	10	10	10	10	9	9

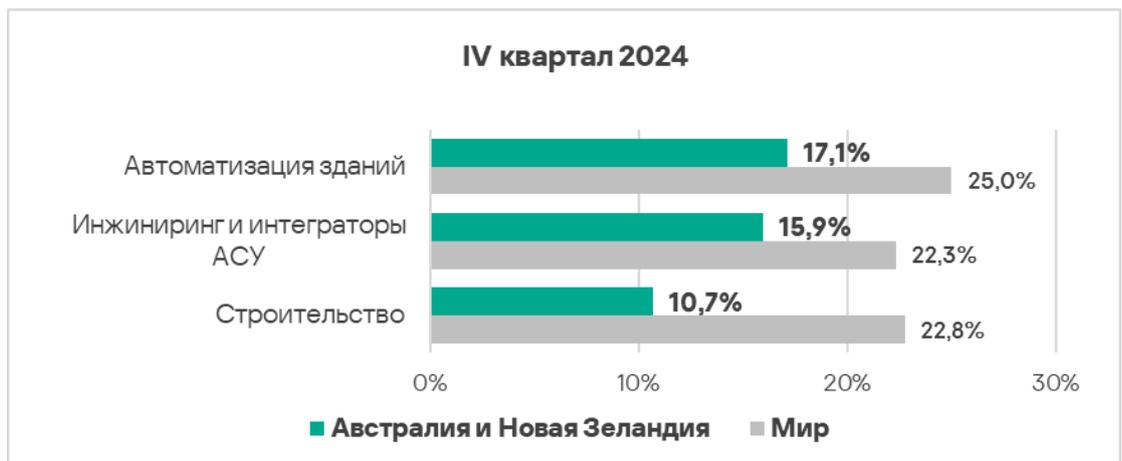
Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

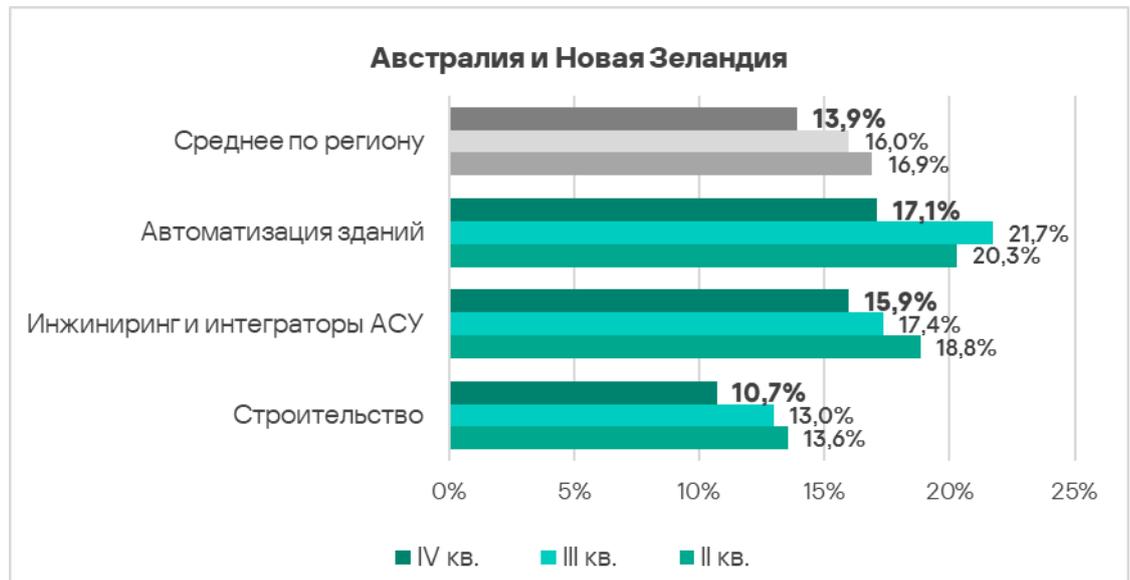


Отрасли

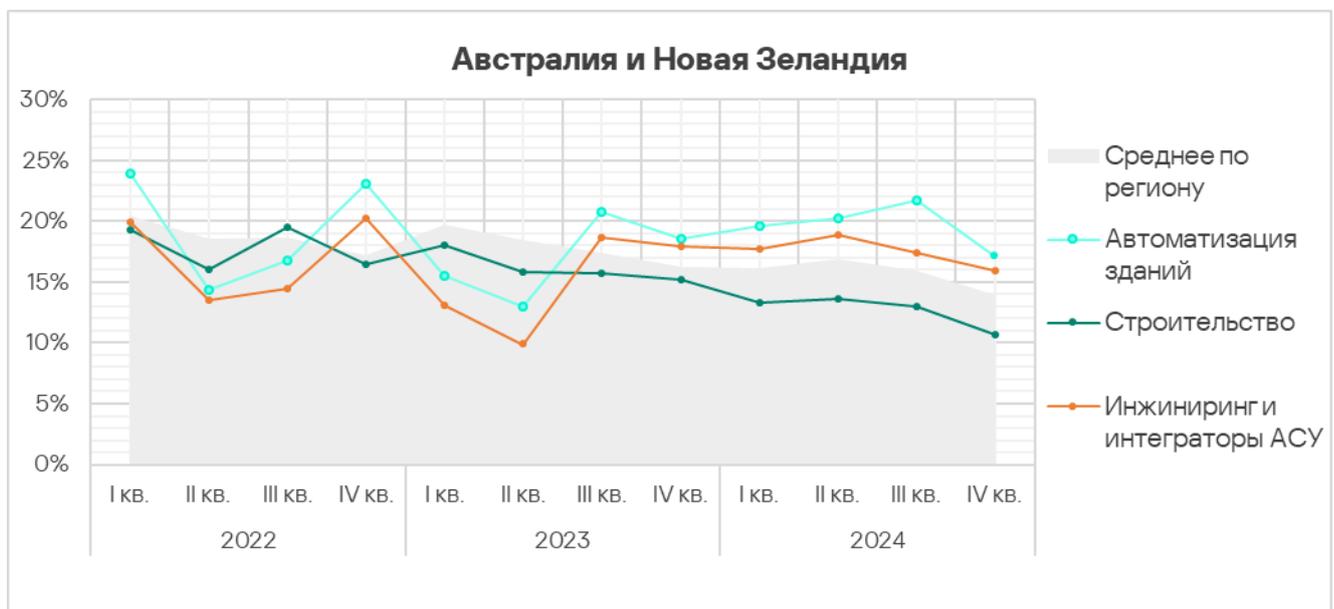
- Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий**.



- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** во всех рассматриваемых отраслях.



- 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. **Строительная** отрасль все еще демонстрирует преимущественно **нисходящий тренд**, оставаясь ниже среднего значения по региону.



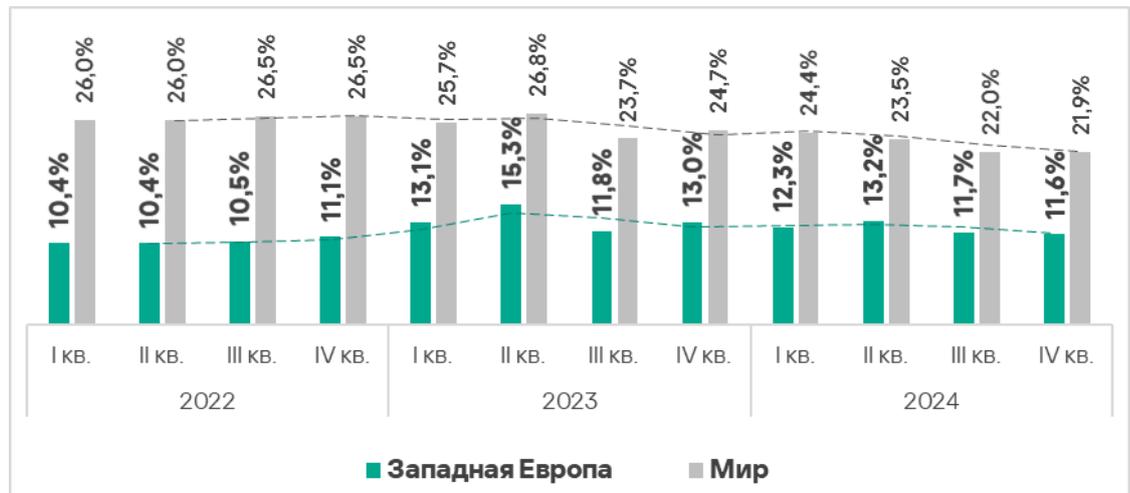
Западная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>4,43% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>3,59% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>1,54% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▼ снижение в IV кв. 2024 г.</p>
<p>0,29% ЧЕРВИ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	<p>0,21% ВЕБ-МАЙНЕРЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г. 3-е место по росту</p>	<p>0,08% ПРОГРАММЫ- ВЫМОГАТЕЛИ</p> <p>▲ 1,3x рост в IV кв. 2024 г.</p>
<p>6,37% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>1,68% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	

Общая ситуация

- Западная Европа занимает **одиннадцатое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Показатель в регионе — **один из самых низких**, он существенно ниже среднемирового значения.
- В **четвертом квартале 2024** года показатель снова **сократился**.



Сравнительный анализ

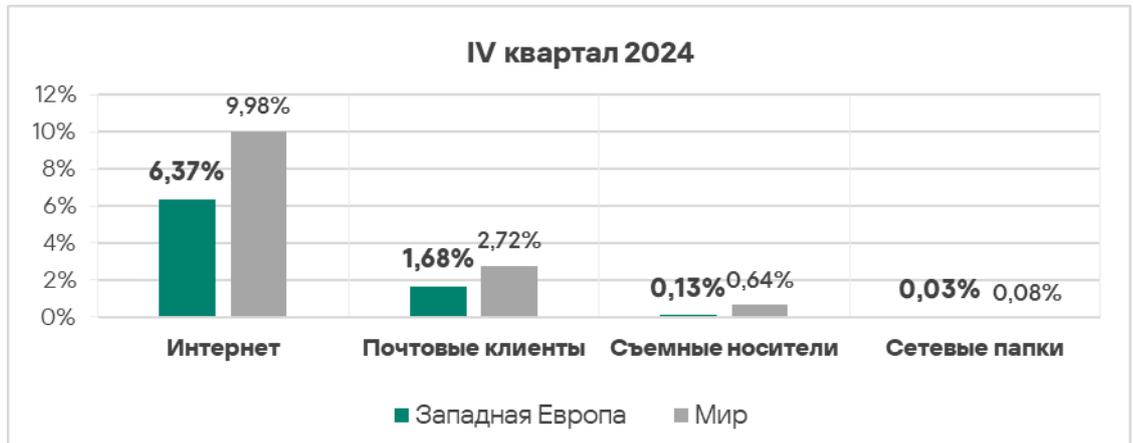
Категории угроз



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

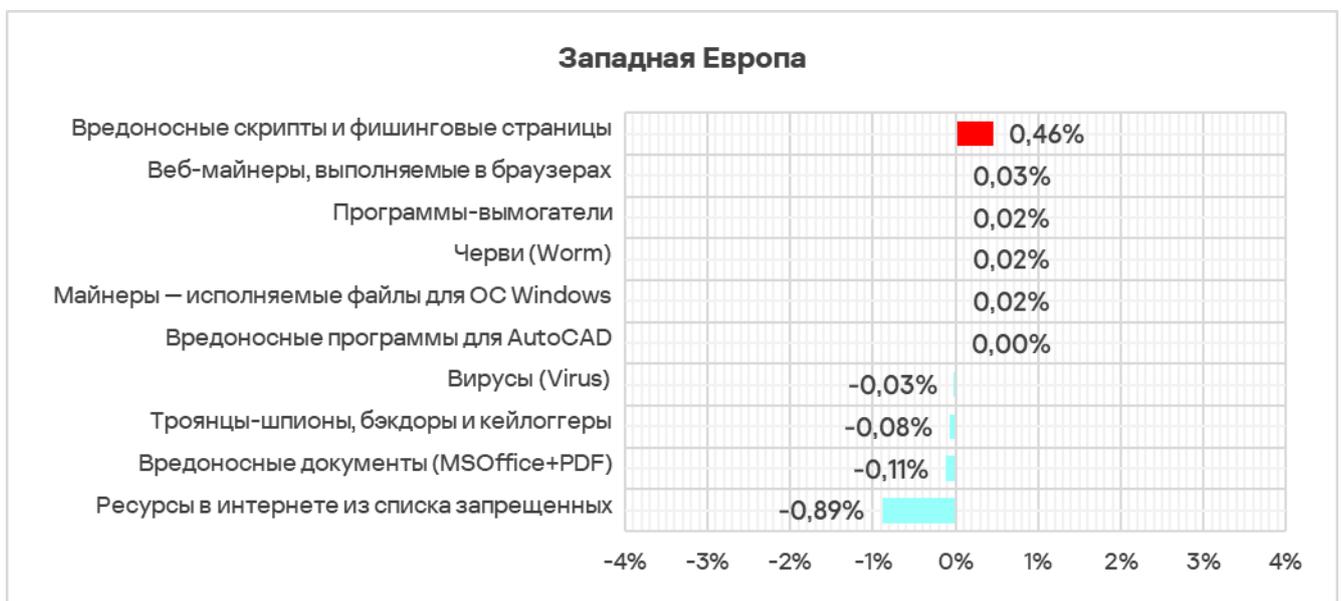
Источники угроз

- Показатели всех источников угроз заметно **ниже** соответствующих **среднемировых значений**.

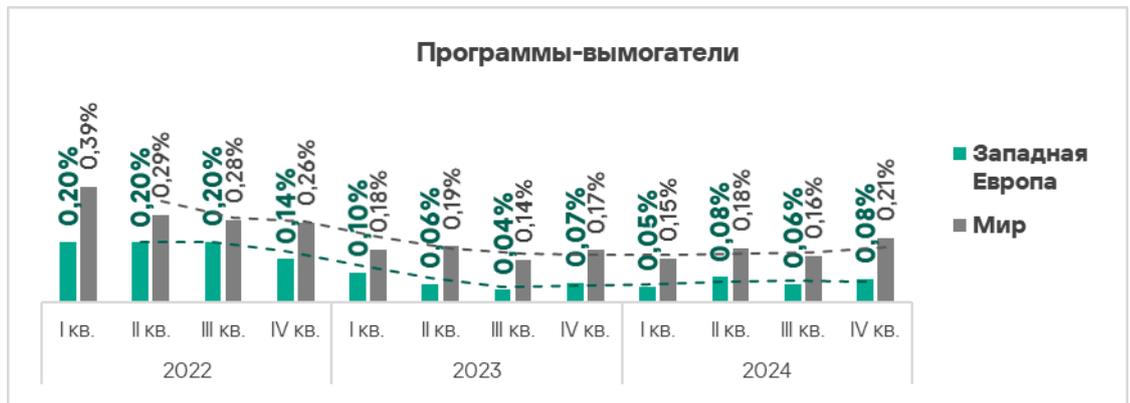


Изменения за квартал и тренды

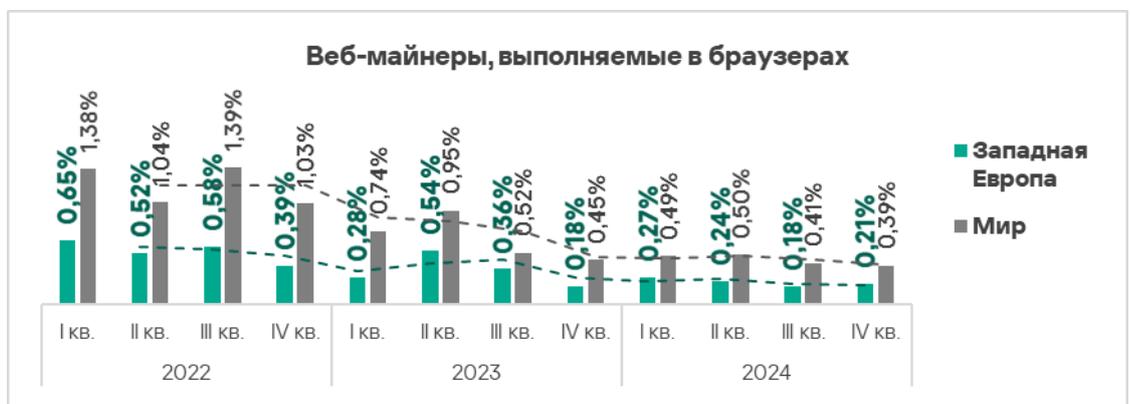
Категории угроз



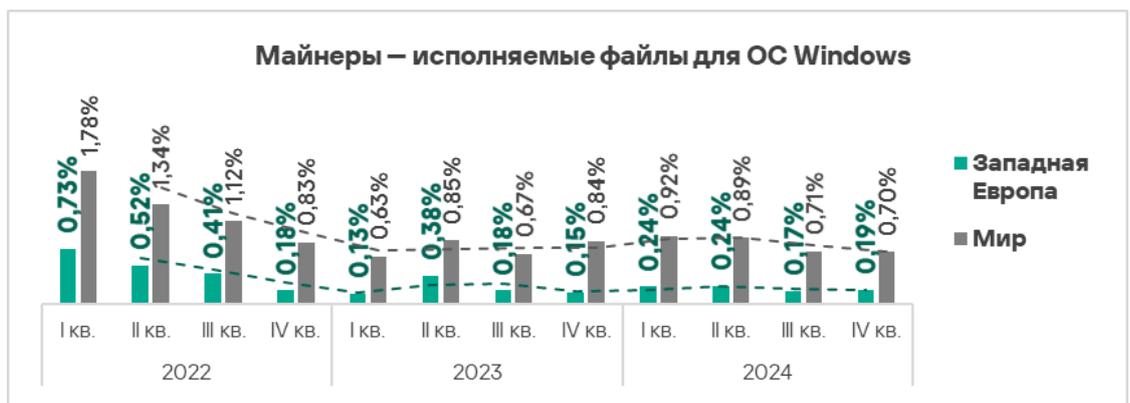
- Наибольший прирост в процентах** за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
 - программы-вымогатели — в 1,3 раза;



➤ веб-майнеры — в 1,2 раза, третье место по росту показателя в мире;



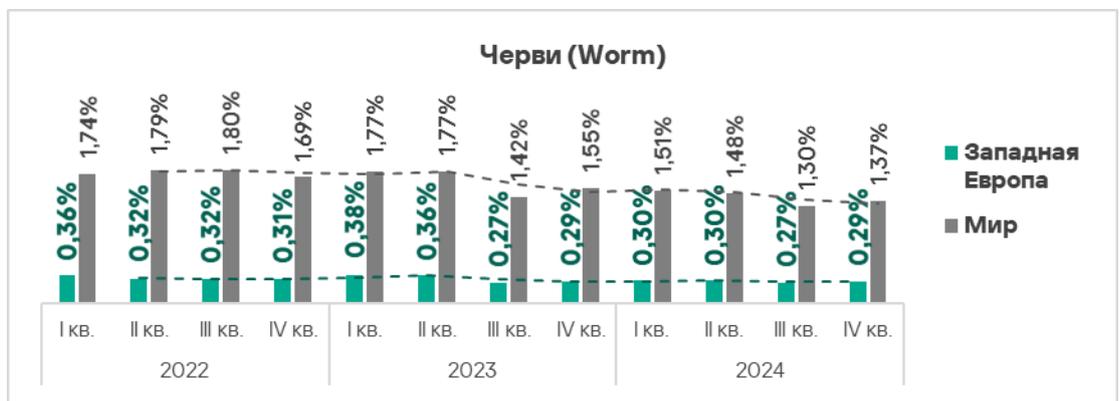
➤ майнеры — исполняемые файлы для ОС Windows — в 1,1 раза;



➤ вредоносные скрипты и фишинговые страницы — в 1,1 раза;



➤ черви — в 1,1 раза.

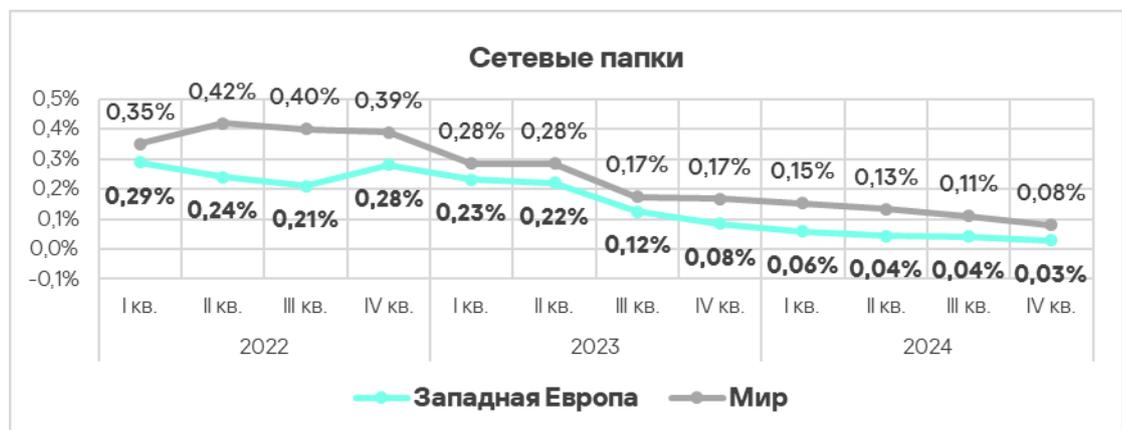


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Западной Европе с начала 2022 года. В четвертом квартале 2024 года **вредоносные скрипты и фишинговые страницы** вернулись на вершину рейтинга, а **вирусы** упали на восьмую строчку.

Западная Европа	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	2	2	2	1
Ресурсы в интернете из списка запрещенных	2	2	2	2	2	2	2	2	1	1	1	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	3	3	3	3	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	4	4	4	4	4
Черви (Worm)	7	7	7	6	5	7	6	5	5	5	5	5
Веб-майнеры, выполняемые в браузерах	6	6	5	5	6	5	5	6	6	7	7	6
Майнеры – исполняемые файлы для ОС Windows	5	5	6	7	8	6	7	8	7	6	8	7
Вирусы (Virus)	9	9	9	9	7	8	8	7	8	8	6	8
Программы-вымогатели	8	8	8	8	9	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	10	10	10

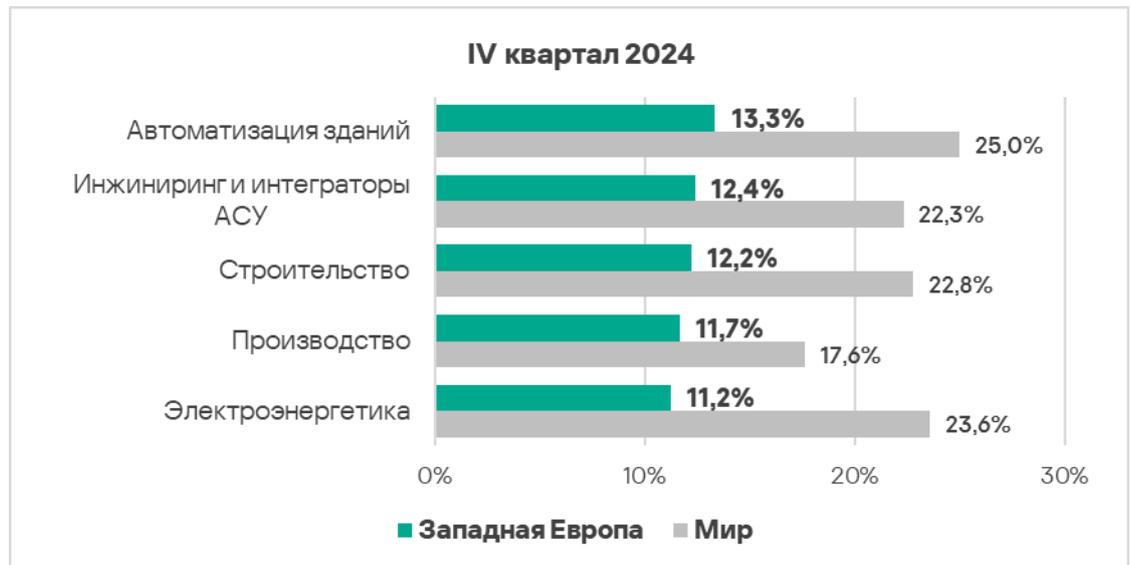
Источники угроз

- В четвертом квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.



Отрасли

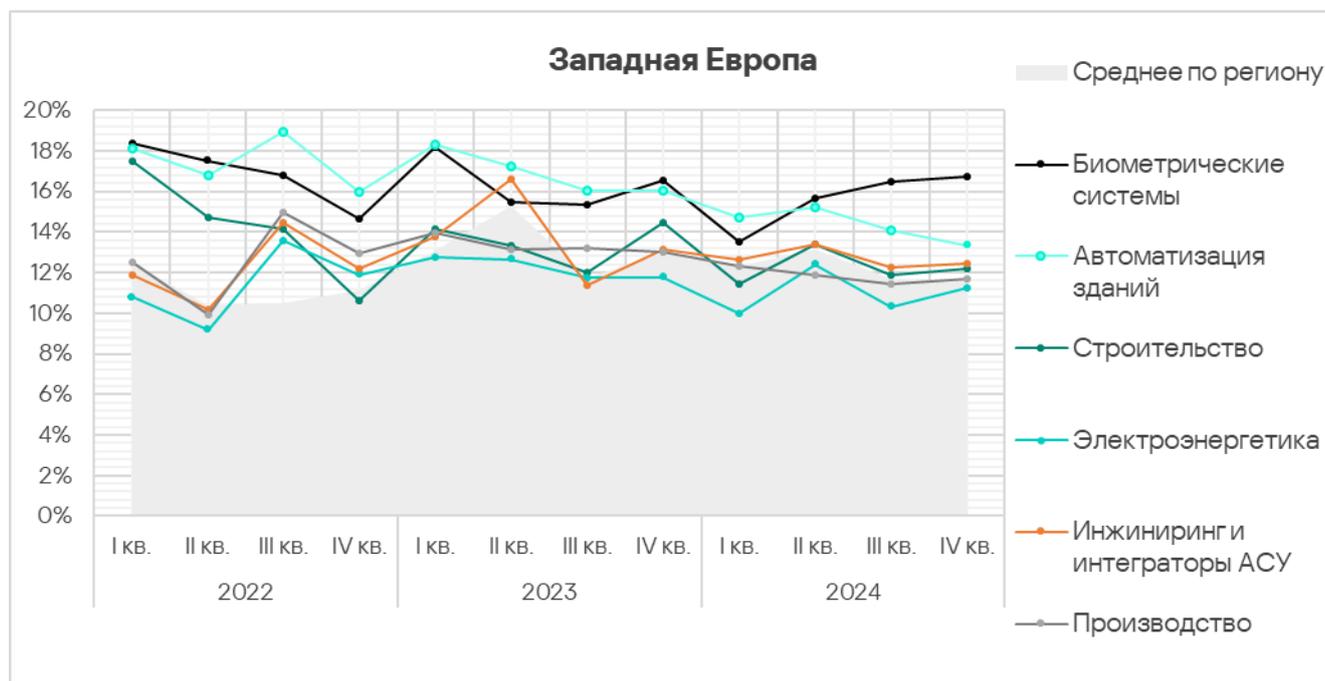
- **Наиболее часто встречающейся с угрозами отрасли** из рассмотренных в отчете является **автоматизация зданий**.
- Показатели во всех отраслях региона значительно **ниже** соответствующих **среднемировых значений**.



- **В четвертом квартале 2024 года** во всех рассмотренных отраслях региона, кроме автоматизации зданий, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла**, причем в электроэнергетике — в 1,1 раза.



- **Автоматизация зданий и биометрические системы** по-прежнему демонстрируют **тренды**, заметно превышающие среднее для региона значение. Более того, биометрические системы демонстрируют восходящий тренд начиная со второго квартала 2024 года.



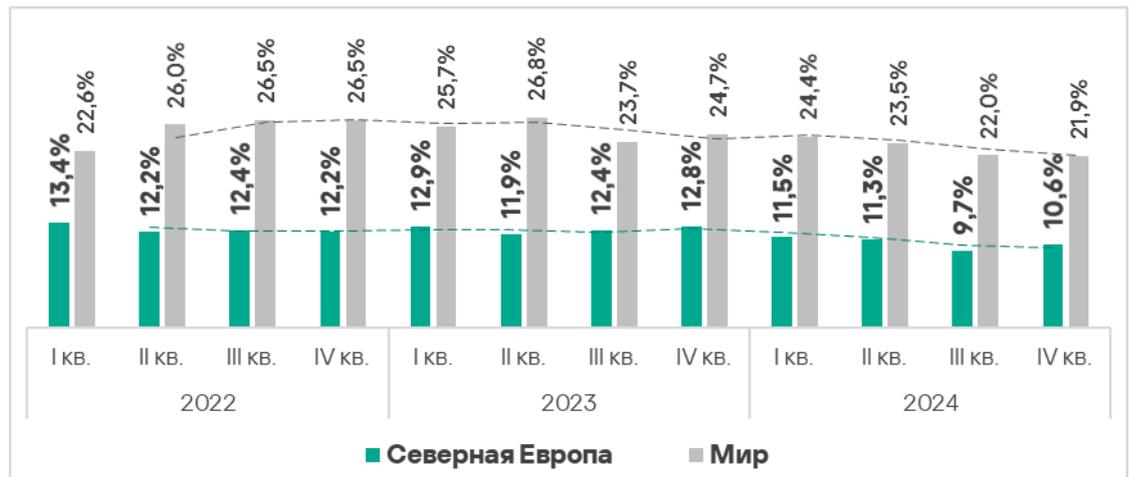
Северная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
<p>3,04% СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p>	<p>2,69% ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ</p> <p>▼ снижение в IV кв. 2024 г.</p>	<p>1,74% ШПИОНСКИЕ ПРОГРАММЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>
<p>0,33% ЧЕРВИ</p> <p>▲ 1,2x рост в IV кв. 2024 г.</p>	<p>0,28% ВЕБ-МАЙНЕРЫ</p> <p>▲ 1,1x рост в IV кв. 2024 г.</p>	
<p>5,05% ИНТЕРНЕТ КАК ИСТОЧНИК УГРОЗ</p> <p>▲ слабый рост в IV кв. 2024 г. 2-е место по росту</p>	<p>1,10% ПОЧТОВЫЕ КЛИЕНТЫ КАК ИСТОЧНИК УГРОЗ</p> <p>▼ снижение в IV кв. 2024 г.</p>	

Общая ситуация

- Северная Европа занимает **двенадцатое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.
- Показатель значительно **ниже среднемирового значения**.
- В **четвертом квартале 2024 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Северной Европе вырос в 1,1 раза. Регион занимает третье место по росту этого показателя в мире.



Сравнительный анализ

Категории угроз



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

Источники угроз

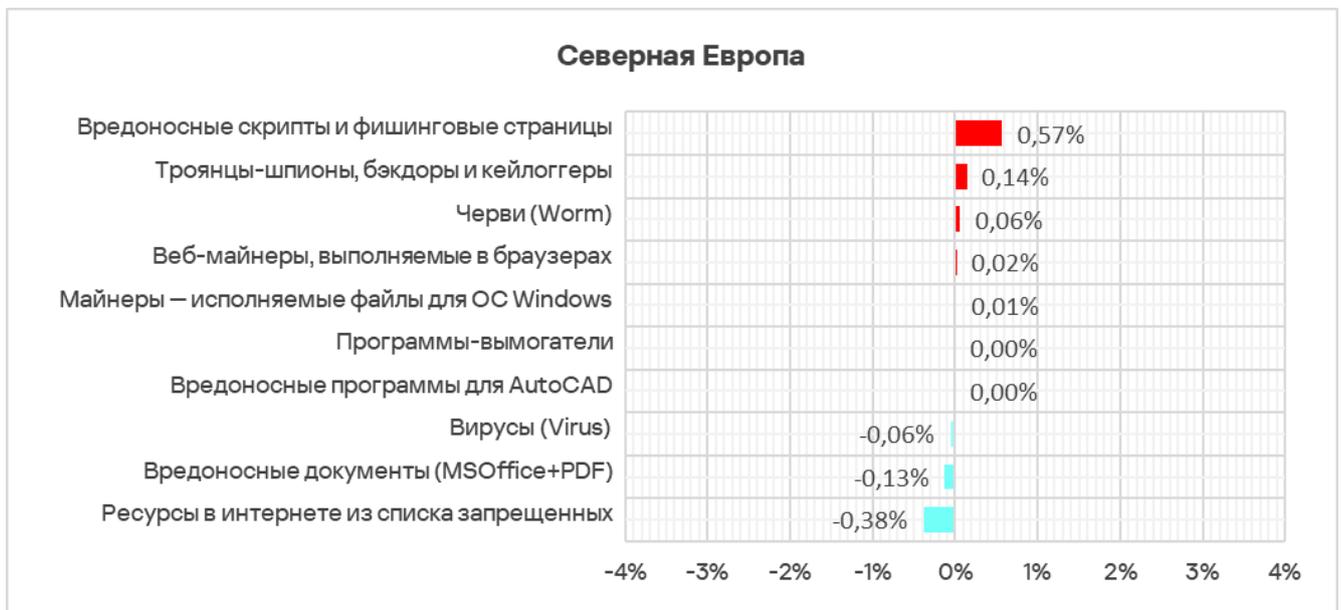
- Показатели всех источников угроз заметно **ниже** соответствующих **среднемировых значений**.



Изменения за квартал и тренды

Категории угроз

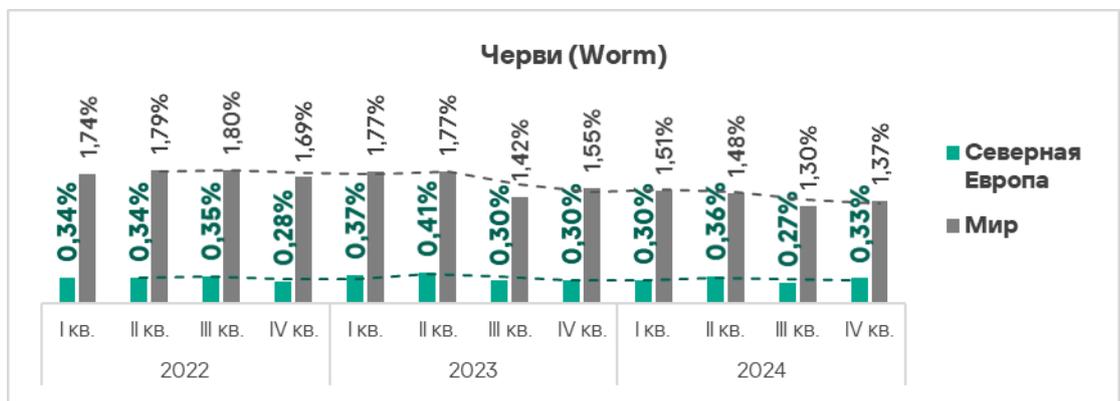
- Большинство категорий угроз демонстрирует **снижение доли компьютеров АСУ**, на которых вредоносные объекты из данных категорий были заблокированы.



- Наибольший прирост в процентах** за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:
 - вредоносные скрипты и фишинговые страницы — в 1,2 раза;



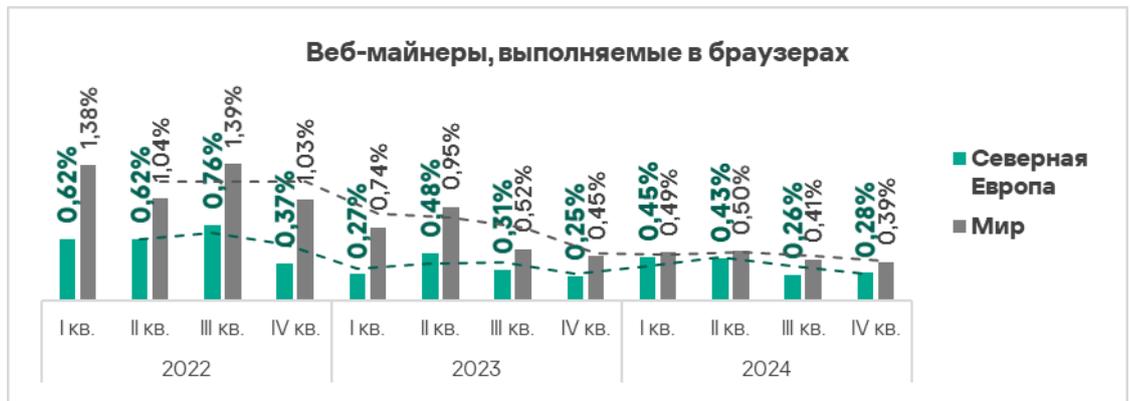
➤ черви — в 1,2 раза;



➤ шпионские программы — в 1,1 раза;



➤ веб-майнеры — в 1,1 раза.

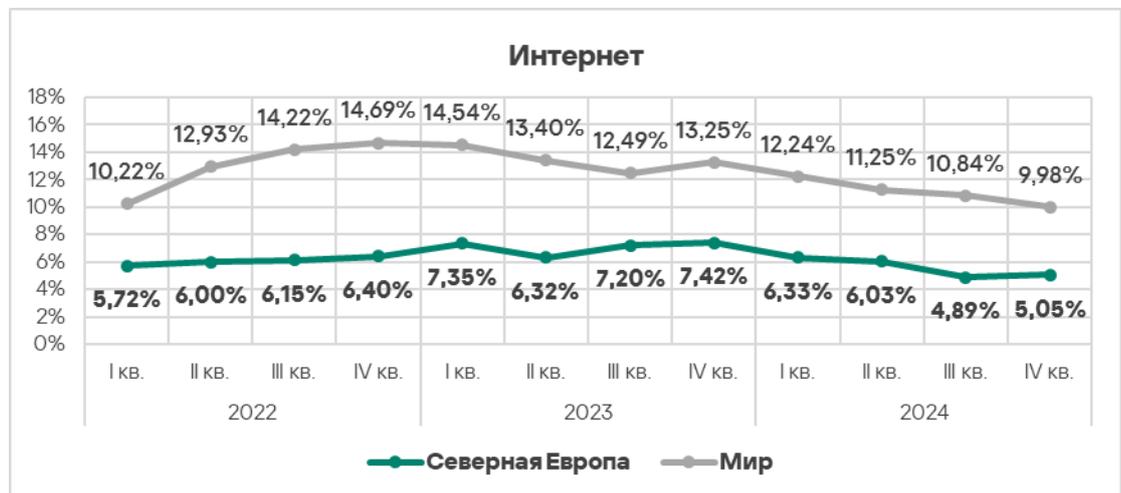


- Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Северной Европе с начала 2022 года. В четвертом квартале 2024 года **вредоносные скрипты и фишинговые страницы** вернулись на верхнюю строчку рейтинга.

Северная Европа	2022				2023				2024			
	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.	I кв.	II кв.	III кв.	IV кв.
Вредоносные скрипты и фишинговые страницы	1	1	1	1	2	2	2	1	2	2	2	1
Ресурсы в интернете из списка запрещенных	2	2	2	2	1	1	1	2	1	1	1	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	3	3	3	3	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	4	4	4	4	4
Черви (Worm)	7	7	7	6	5	6	6	5	7	7	7	5
Майнеры – исполняемые файлы для ОС Windows	5	5	6	7	8	7	6	8	6	5	6	6
Веб-майнеры, выполняемые в браузерах	6	6	5	5	7	5	5	7	5	6	8	7
Вирусы (Virus)	8	8	8	8	6	8	8	6	8	8	5	8
Программы-вымогатели	9	9	9	9	10	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	10	9	10	10	10	10	10	10	10

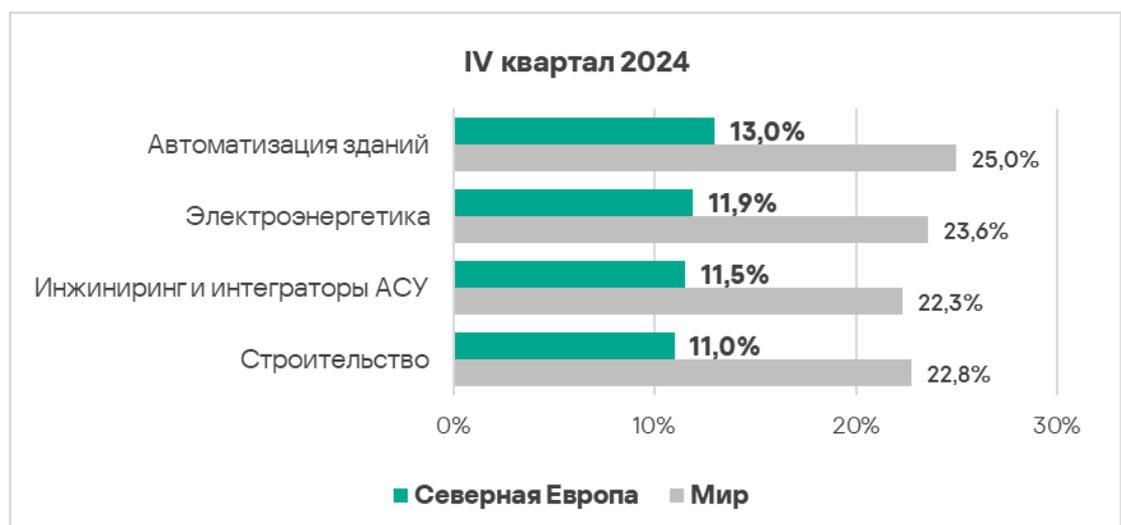
Источники угроз

- В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, выросла.

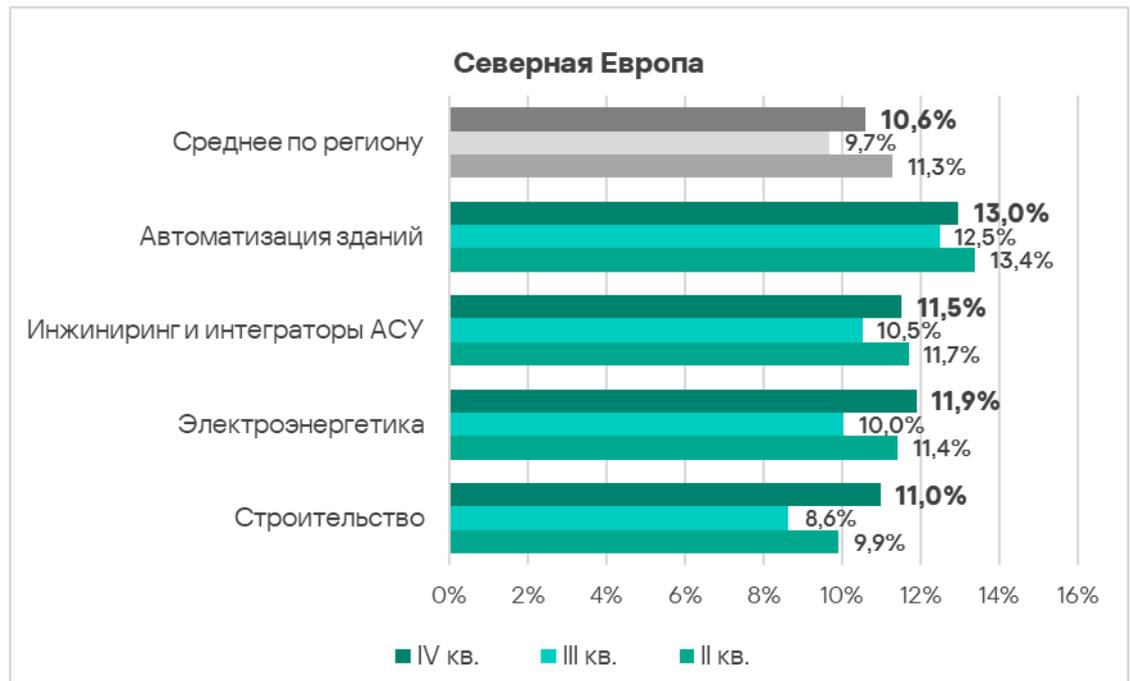


Отрасли

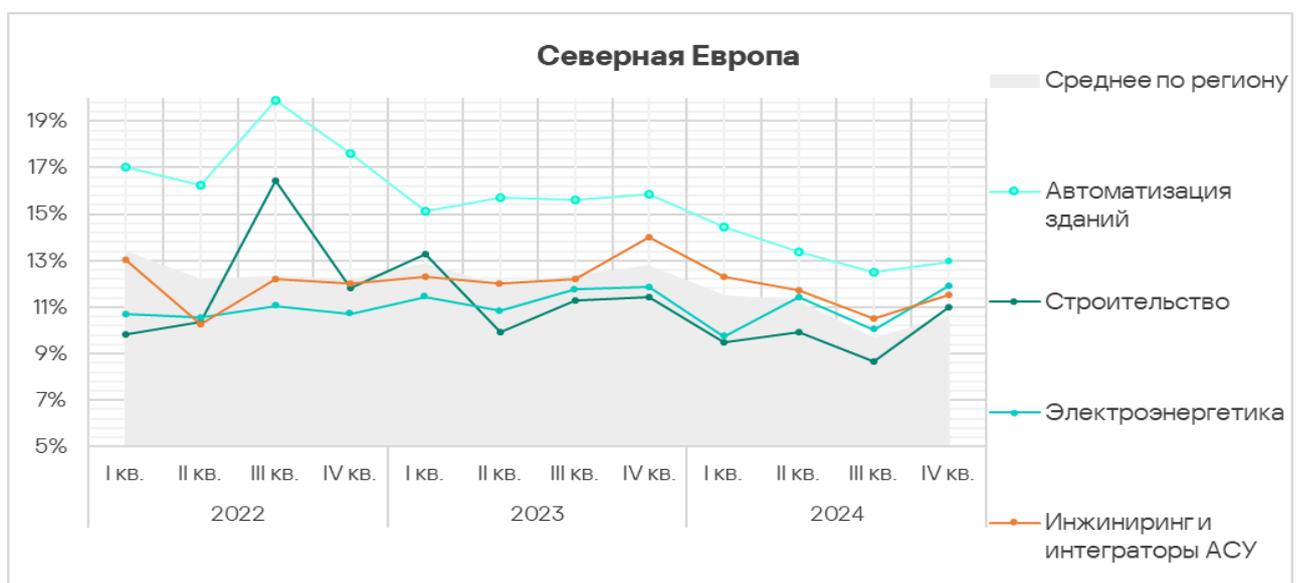
- Наиболее часто встречающейся с угрозами отраслью** региона из рассмотренных в отчете является **автоматизация зданий**. В мировом рейтинге она находится на пятом месте среди рассмотренных отраслей.
- Показатели во всех отраслях региона по-прежнему остаются значительно ниже соответствующих **среднемировых значений**.



- В четвертом квартале 2024 года** во всех рассмотренных отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла**.



- **Наиболее заметный рост** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал зафиксирован в следующих отраслях:
 - строительство – в 1,3 раза;
 - электроэнергетика – в 1,2 раза;
 - производство – в 1,2 раза;
 - инжиниринг и интеграторы АСУ – в 1,1 раза.
- Тренд **автоматизации зданий** остается заметно выше среднего регионального тренда, хотя и демонстрирует постепенное снижение.



Методика подготовки статистики

В отчете представлены результаты анализа статистических данных, полученных с помощью распределенной антивирусной сети [Kaspersky Security Network \(KSN\)](#). Данные получены от тех пользователей KSN, которые добровольно подтвердили свое согласие на их анонимную передачу и обработку с целью, описанной в Соглашении KSN для установленного на их компьютере продукта «Лаборатории Касперского».

Подключение к сети KSN дает нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счет обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за ее объема и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и АРТ¹.

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

- серверы управления и сбора данных (SCADA);
- серверы автоматизации зданий;
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human machine interface (HMI);
- компьютеры, используемые для администрирования технологических сетей и сетей автоматизации зданий;
- компьютеры программистов АСУ/ПЛК.

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

Компьютеры, передающие нам статистику, принадлежат организациям из разных отраслей. Наиболее широко представлены химическая промышленность, металлургия, инжиниринг и интеграторы АСУ, нефтегазовая отрасль, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность и фармацевтическая отрасль. Сюда же входят системы инжиниринговых компаний и интеграторов АСУ, работающих с предприятиями в самых разных отраслях, а также системы управления зданиями, физической безопасности и обработки биометрических данных.

Атакowanными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете доли машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение исследуемого периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение исследуемого периода мы получали обезличенную информацию.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», 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