Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Регионы. Первый квартал 2025 года

10.06.2025

Версия 1.0

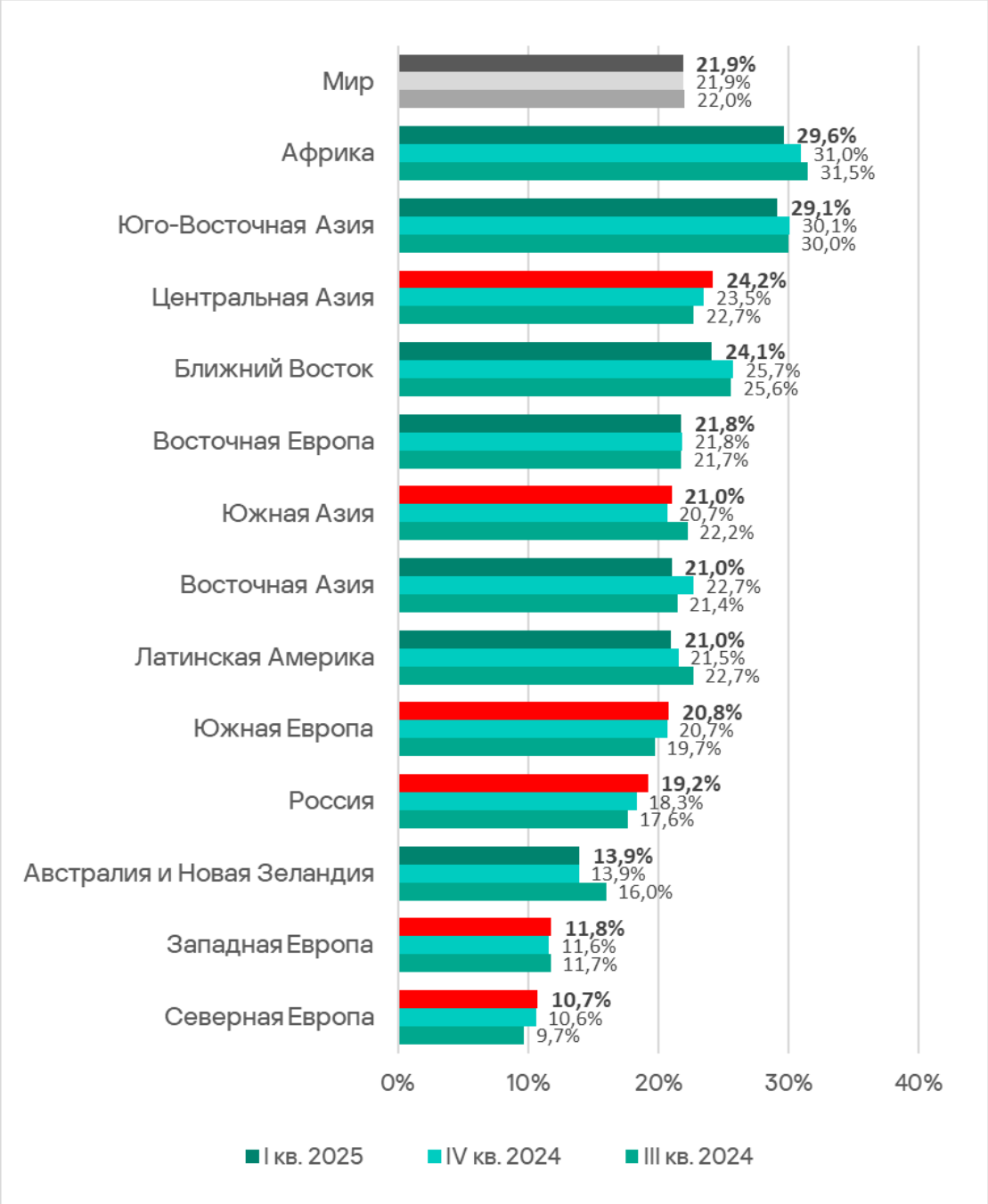
Обзор первого квартала 2025 года

Общая статистика по регионам

В мире в первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, не изменилась и составила 21,9%.

Значение этого параметра в различных регионах варьируется — от 10,7% в Северной Европе до 29,6% в Африке.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2025 года



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

Более 25%

- Африка — 29,6%
- Юго-Восточная Азия — 29,1%

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 — 24,2%
- Ближний Восток — 24,1%
- Восточная Европа — 21,8%
- Южная Азия — 21,0%
- Восточная Азия — 21,0%
- Латинская Америка — 21,0%
- Южная Европа — 20,8%

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

Менее 20%

- Россия — 19,2%
- Австралия и Новая Зеландия — 13,9%
- Западная Европа — 11,8%
- Северная Европа — 10,7%

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

По сравнению с предыдущим кварталом в первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты,

увеличилась в шести регионах, больше всего — в России и Центральной Азии.

Регионы и мир. Изменение доли атакованных компьютеров, I квартал 2025 года

Источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет (обращения ко вредоносным или скомпрометированным интернет-ресурсам, вредоносный контент, распространяемый через мессенджеры, облачные сервисы хранения и обработки данных и CDN), почтовые клиенты (фишинговые рассылки) и съемные носители.

Во всех регионах в рейтинге источников угроз интернет занимает первую позицию, электронная почта — на втором месте, съемные носители — на третьем. Сетевые папки замыкают рейтинг.

Интернет

Обнаружение и блокирование угроз из интернета на компьютерах АСУ, защищенных решением «Лаборатории Касперского», означает, что на момент обнаружения с них был разрешен доступ к внешним сервисам.

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

Топ-3 регионов по показателю этого источника угроз в первом квартале 2025 года:

- Африка — 12,76%;
- Юго-Восточная Азия — 12,32%;
- Южная Азия — 10,83%.

Помимо регионов из топ-3 проблема этого источника угроз особенно актуальна для России (9,34%) и Центральной Азии (9,50).

Наименьший показатель отмечен в Северной Европе — 5,24%.

Больше всего за квартал доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, выросла в России (+1,29 п. п.), Центральной Азии (+1,04 п. п.), Австралии и Новой Зеландии (+0,51 п. п.).

Угрозы, распространяемые через электронную почту

Некоторые из обнаруженных и заблокированных угроз были доставлены на защищенный компьютер системой доставки почты и/или пытались получить доступ через клиентское приложение электронной почты.

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

Топ-3 регионов по уровню угроз из почтовых клиентов в первом квартале 2025 года:

- Южная Европа — 6,76%;
- Ближний Восток — 5,17%;
- Латинская Америка — 4,55%.

Регионы из топ-3 — неизменные лидеры этого рейтинга. Проблема электронной почты как источника угроз характерна также для Восточной Европы (4,00%).

Наименьший показатель в России — 0,88%.

Больше всего за квартал показатель этого источника угроз вырос в Австралии и Новой Зеландии (+0,35 п. п.), Южной Азии (+0,29 п. п.) и Южной Европе (+0,25 п. п.).

Съемные носители

Основными категориями угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ, являются черви, вирусы и шпионское ПО.

Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры. Эти криптомайнеры способны распространяться по локальным сетям, используя кражу учетных данных с зараженных хостов, эксплуатируя уязвимости (известные, но еще не закрытые) и выполняя атаки на сетевые службы методом перебора (брутфорс).

Большинство шпионских программ, обнаруженных на съемных носителях, состояли из универсальных компонентов как современных, так и устаревших червей, таких как стилеры, загрузчики, AV-киллеры.

Первые шесть позиций в рейтинге по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, занимают Африка, Ближний Восток (4-е место в рейтинге) и все регионы Азии.

Топ-3 регионов в первом квартале 2025 года по этому показателю:

- Африка — 2,44%;
- Южная Азия — 1,08%;
- Восточная Азия — 1,01%.

Наименьший показатель — в Австралии и Новой Зеландии (0,06%).

Показатель этого источника угроз за квартал уменьшился во всех регионах.

Сетевые папки

Сетевые папки — это незначительный источник угроз, через который распространяются черви, вирусы и вредоносное ПО для AutoCAD.

Топ-3 регионов по уровню угроз в сетевых папках в первом квартале 2025 года:

- Восточная Азия, безусловный лидер рейтинга, — 0,27%;
- Юго-Восточная Азия — 0,16%;
- Южная Азия — 0,11%.

Наименьший показатель в Австралии и Новой Зеландии — 0,01%.

Как и в случае съемных носителей, проблема угроз в сетевых папках характерна для регионов Азии, Африки и Ближнего Востока.

Категории вредоносного ПО

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, по способу распространения и назначению можно условно разделить на три группы.

1. Вредоносные объекты, используемые для первичного заражения. Чаще всего, это ресурсы в интернете из списка запрещенных; вредоносные скрипты и фишинговые страницы; вредоносные документы.
2. Вредоносное ПО следующего этапа. Как правило, это программы-шпионы, программы-вымогатели, майнеры — исполняемые файлы для ОС Windows и веб-майнеры.
3. Самораспространяющееся вредоносное ПО. Эта категория включает в себя вирусы и черви.

Вредоносные программы для AutoCAD распространяются разными способами, поэтому мы не относим их к конкретной группе по типу распространения.

Вредоносные объекты, используемые для первичного заражения

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

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.

Ресурсы в интернете из списка запрещенных

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

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных:

- Африка — 6,21%;
- Россия — 5,60%;
- Центральная Азия — 5,50%.

Наименьший показатель в Северной Европе — 2,65%.

В первом квартале 2025 года показатель уменьшился во всех регионах, за исключением России (+0,33 п. п.), где он увеличился в связи с очередной волной атак на сайты, использующие устаревшие шаблоны АСПРО для CMS Bitrix.

Вредоносные документы

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы:

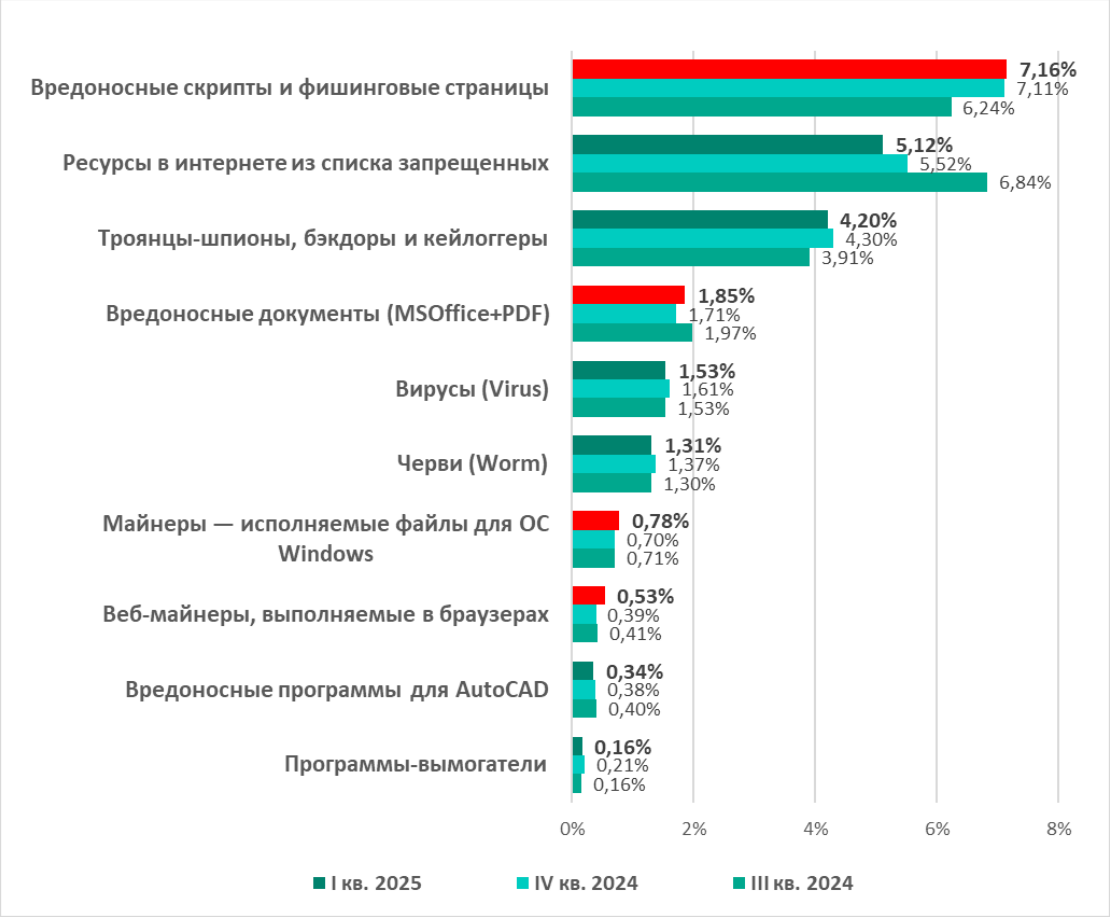
- Южная Европа — 4,02%;
- Латинская Америка — 3,30%;
- Ближний Восток — 2,70%.

Эти же регионы лидирую в рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы из почты.

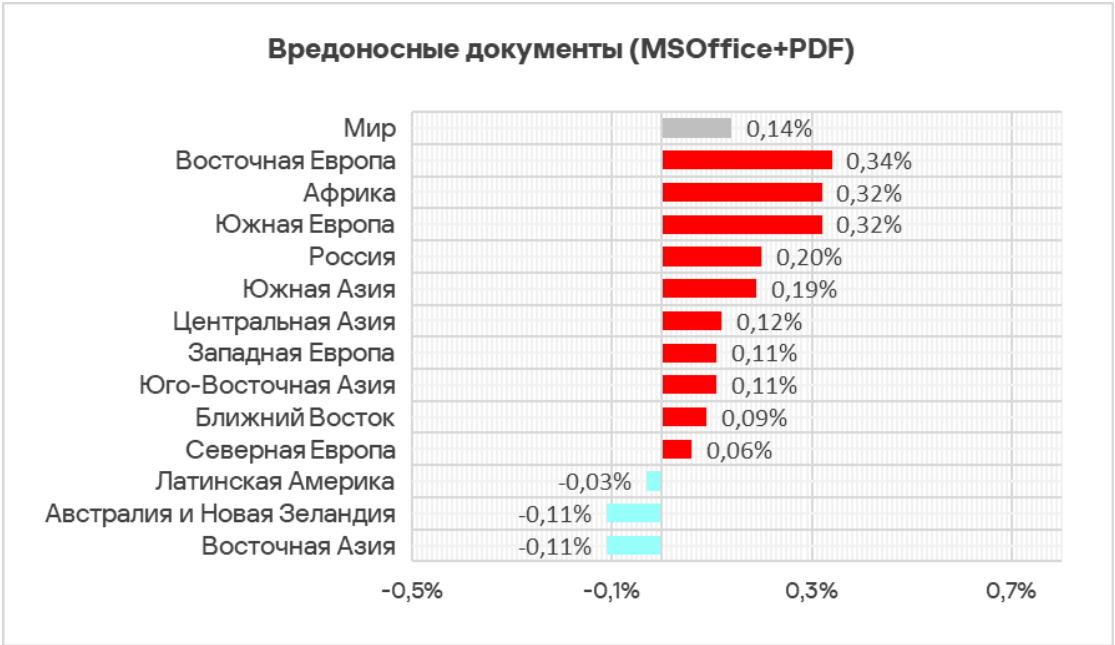
Наименьший показатель вредоносных документов в Северной Европе — 0,60%.

В мире в первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные документы, выросла в 1,1 раза. Показатель увеличился почти во всех регионах, в тройку лидеров по росту вошли: Восточная Европа, Африка и Южная Европа.

Доля компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные документы, I квартал 2025 года



Вредоносные скрипты и фишинговые страницы

Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы:

- Южная Европа — 10,31%;
- Африка — 10,14%;
- Ближний Восток — 9,58%.

Наименьший показатель в Северной Европе — 3,07%.

Тройка лидеров по росту этого показателя: Центральная Азия (+1,16 п. п.), Австралия и Новая Зеландия (+0,85 п. п.), Южная Азия (+0,71 п. п.).

Вредоносное ПО следующего этапа

Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа. Обычно это — шпионское ПО, программы-вымогатели и майнеры. Как правило, чем выше доля компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, тем выше этот показатель и для вредоносного ПО следующего этапа.

Шпионские программы

Шпионское ПО применяется для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

В первом квартале 2025 года в топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, вошли:

- Африка — 7,05%;
- Южная Европа — 6,52%;
- Ближний Восток — 6,25%.

Эти регионы также лидируют по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы.

Проблема шпионских программ весьма актуальна и для Восточной Азии (4,81%) — здесь шпионские программы занимают первое место в рейтинге категорий вредоносного ПО по доле компьютеров АСУ, на которых они были заблокированы.

В регионах из топ-3 в рейтингах категорий блокируемых угроз шпионские программы находятся на втором месте. Такая же ситуация в Восточной Европе (5,15%) и Латинской Америке (4,33%).

Наименьший показатель — в Западной Европе (1,62%).

За квартал доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла в Южной (+0,14 п. п.) и Западной Европе (+0,08 п. п.).

Программы для скрытого майнинга криптовалюты

В мире в первом квартале 2025 года наиболее заметно выросла доля компьютеров АСУ, на которых были заблокированы майнеры:

- веб-майнеры по отношению к показателю предыдущего квартала — в 1,4 раза;
- майнеры — исполняемые файлы для ОС Windows — в 1,1 раза.

Увеличение доли компьютеров АСУ, на которых были заблокированы майнеры обеих категорий, отмечено почти во всех регионах.

Веб-майнеры, выполняемые в браузерах

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах:

- Африка — 0,81%;
- Юго-Восточная Азия — 0,80%;
- Восточная Европа — 0,76%.

Наименьший показатель в Восточной Азии — 0,18%.

В Австралии и Новой Зеландии, а также Западной Европе веб-майнеры занимают более высокую позицию в рейтинге категорий заблокированных угроз, чем в мировом рейтинге — шестое место в регионах против восьмого в мире.

В первом квартале 2025 года рост доли компьютеров АСУ, на которых были заблокированы веб-майнеры, зафиксирован во всех регионах, за исключением Северной Европы и России. Лидируют по этому критерию Юго-Восточная и Южная Азия.

Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, I квартал 2025 года

Майнеры — исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, лидируют среди регионов:

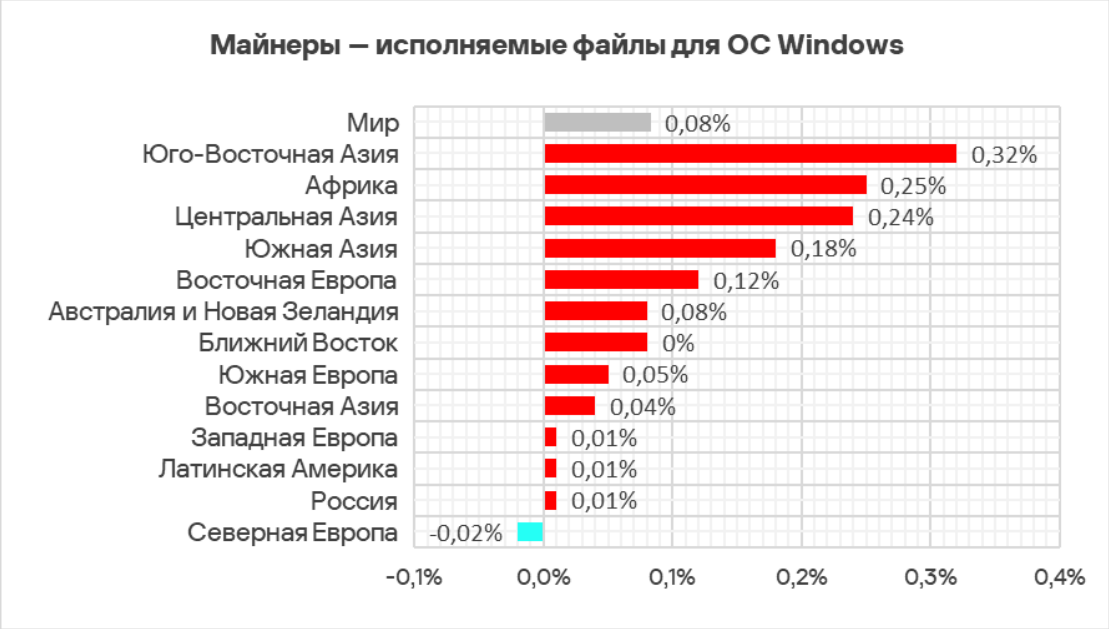
- Центральная Азия — 1,72%;
- Россия — 1,04%;
- Восточная Европа — 0,85%.

Наименьший показатель — в Западной Европе (0,20%).

В мире в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows находятся на седьмом месте. В аналогичном региональном рейтинге в России они занимают четвертое место. Среди регионов это самая высокая позиция для данной категории угроз.

В первом квартале 2025 года этот показатель вырос почти во всех регионах. Лидерами по росту стали Юго-Восточная Азия, Африка и Центральная Азия.

Изменение доли компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2025 года



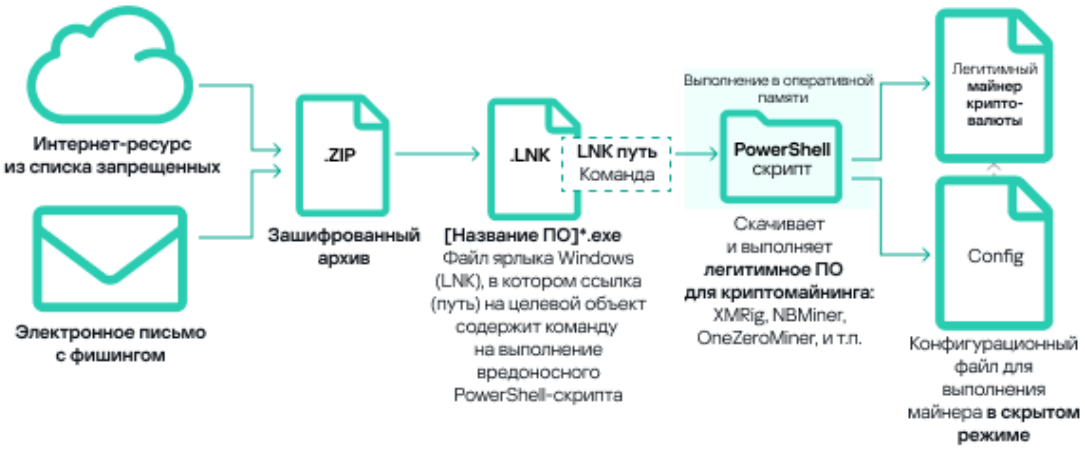
Наряду с «классическими» майнерами — приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют, — появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры криптовалют на компьютеры АСУ.

Значительная часть майнеров для ОС Windows, обнаруженных на компьютерах АСУ, представляет собой архивы, названия которых имитировали легальное программное обеспечение. Эти архивы не содержат реального программного обеспечения, но включают в себя файл формата Windows LNK, более известный как ярлык. Однако целевой объект (или путь), на который указывает LNK-файл, не является обычным приложением, а представляет собой команду, которая может выполнить вредоносный код, например, скрипт PowerShell. Злоумышленники все чаще выбирают PowerShell, с помощью которого код вредоносного ПО (в том числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом. Бесфайловое выполнение майнера делает 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 использованием легитимных криптомайнеров



Программы-вымогатели

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели:

- Восточная Азия — 0,32%;

- Ближний Восток — 0,30%;
- Африка — 0,25%.

Наименьший показатель — в Западной Европе (0,08%).

Тройку лидеров по росту этого показателя составляют Восточная Азия (+0,09 п. п.), Южная Европа (+0,07 п. п.), Россия (+0,06 п. п.).

Самораспространяющееся вредоносное ПО. Черви и вирусы

Самораспространяющееся вредоносное ПО — черви и вирусы — относится к отдельной категории. Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнетов, приобрели черты угроз следующего этапа.

Черви

В сетях АСУ встречаются новые версии червей, используемые злоумышленниками для распространения шпионского ПО, программ-вымогателей и майнеров. Чаще всего эти черви используют эксплойты известных уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы черви:

- Африка — 3,65%;
- Центральная Азия — 2,79%;
- Ближний Восток — 1,99%;

Наименьший показатель — в Австралии и Новой Зеландии (0,28%).

В мире черви находятся на шестом месте в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. При этом в Центральной Азии черви занимают четвертое место в региональном рейтинге категорий угроз — это самая высокая позиция в региональных рейтингах.

Лидирует по росту этого показателя за квартал Южная Европа (+0,14 п. п.).

Вирусы

Топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы вирусы:

- Юго-Восточная Азия, безусловный лидер — 8,68%;
- Африка — 3,87%;
- Восточная Азия — 2,85%.

Юго-Восточная Азия лидирует в этом рейтинге с большим отрывом. В регионе вирусы находятся на втором месте в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы. В рейтингах остальных регионов вирусы не поднимаются выше четвертой позиции.

Два азиатских региона из тройки лидеров входят также в топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.

Наименьший показатель — в Австралии и Новой Зеландии (0,19%).

Лидируют по росту этого показателя Центральная Азия (+0,12 п. п.), Южная Европа (+0,09 п. п.) и Южная Азия (+0,06 п. п.).

Вредоносные программы для AutoCAD

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

- Юго-Восточная Азия — 2,65%;
- Восточная Азия — 1,19%;
- Африка — 0,51%.

Показатели Восточной и особенно Юго-Восточной Азии значительно превышают значения в остальных регионах. Эти же регионы — и тоже с большим отрывом — лидируют в рейтинге по доле угроз из сетевых папок.

Как правило, вредоносные программы для AutoCAD занимают последние места в рейтингах категорий вредоносного ПО по доле компьютеров АСУ, на которых оно было заблокировано. Однако в Восточной и Юго-Восточной Азии вредоносное ПО для AutoCAD оказалось на более высоких позициях:

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

Наименьший показатель в Северной Европе — 0,01%.

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 вредоносные объекты, используемые для первичного заражения компьютеров, и программы-шпионы. 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
10,14% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▼ снижение в I кв. 2025 г. 2-е место в мире 1,4x выше среднего по миру	**7,05%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г. 1-е место в мире 1,7x выше среднего по миру	**6,21%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г. 1-е место в мире 1,2x выше среднего по миру
3,87% **ВИРУСЫ** ▼ снижение в I кв. 2025 г. 2-е место в мире 2,5x выше среднего по миру	**3,65%** **ЧЕРВИ** ▼ снижение в I кв. 2025 г. 1-е место в мире 2,8x выше среднего по миру	**2,36%** **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,2x рост в I кв. 2025 г. 1,3x выше среднего по миру
0,81% **ВЕБ-МАЙНЕРЫ** ▲ 1,6x рост в I кв. 2025 г. 1-е место в мире 1,5x выше среднего по миру	**0,81%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,4x рост в I кв. 2025 г. 2-е место по росту	**0,25%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,6x выше среднего по миру
12,76% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 1-е место в мире 1,3x выше среднего по миру	**3,89%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ рост в I кв. 2025 г. 1,4x выше среднего по миру	**2,44%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 1-е место в мире 4,7x выше среднего по миру

- Африка много лет лидирует в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с показателем,

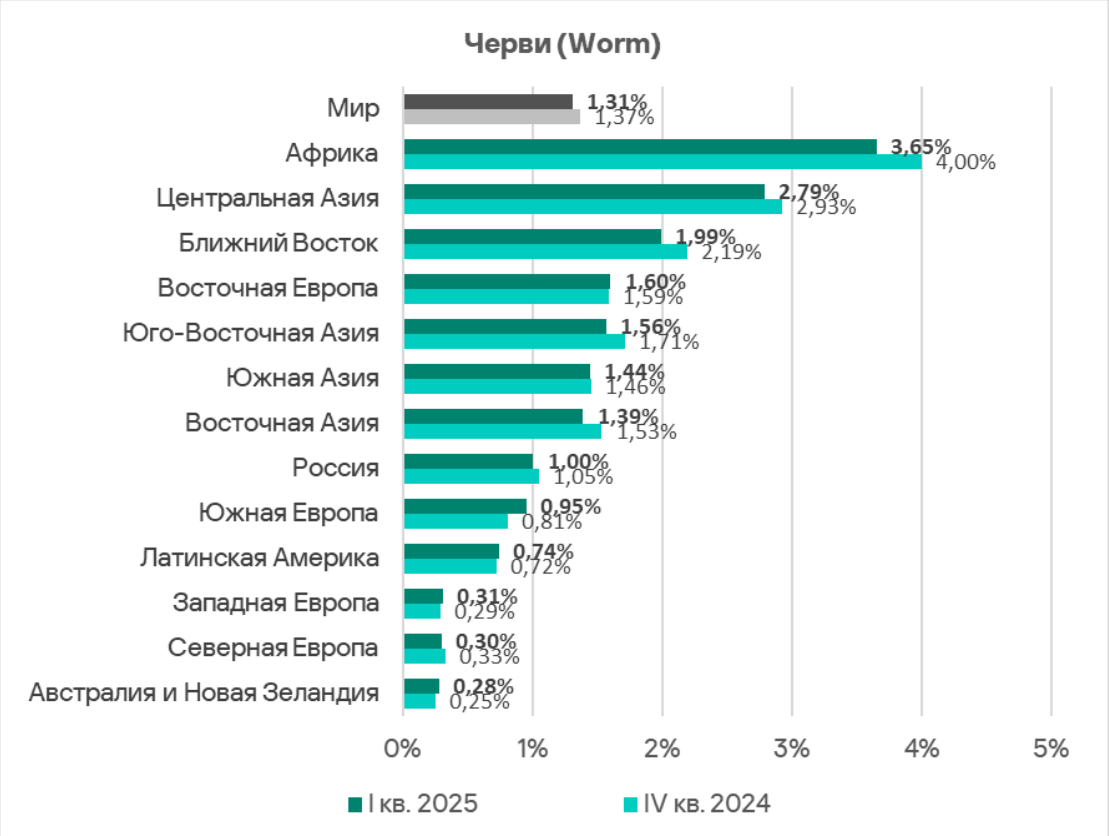
который значительно превышает среднемировое значение — в первом квартале 2025 года в 1,4 раза.

Самораспространяющееся вредоносное ПО

- Одна из характерных проблем региона — самораспространяющееся вредоносное ПО — **черви и вирусы**. Доля компьютеров АСУ, на которых блокируются черви и вирусы, значительно **выше, чем в среднем по миру** (в первом квартале 2025 **в 2,8 раз и в 2,5 раза** соответственно).

  По доле компьютеров АСУ, на которых были заблокированы **черви**, Африка с большим отрывом **лидирует** среди регионов, по показателю **вирусов** занимает **второе** место.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы черви, I квартал 2025 года



Высокие показатели обнаружения самораспространяющегося вредоносного ПО и ПО, которое распространяется через сетевые папки, на уровне отрасли, страны или региона, вероятно, указывают, как правило, на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных устройств. Эти незащищенные компьютеры становятся источниками распространения вредоносного ПО.

Ситуацию могут ухудшать и слабая сегментация сети предприятия, и отсутствие контроля использования съемных носителей информации.

Несмотря на то, что среди распространяющихся вирусов и червей довольно много старых с отключенными командными серверами, они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, — но также могут приводить к сбоям в работе ПО, отказам в обслуживании и т. п.

Черви и вирусы распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

Угрозы со съемных носителей

- Африка, также с большим отрывом, **лидирует** по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении **съемных носителей**. Показатель по этому источнику угроз в регионе превышает среднемировой **в 4,7 раза**.

Рейтинг регионов по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, I квартал 2025 года

Частые попытки заражения защищенных систем при подключении USB-накопителей могут свидетельствовать:

- о низкой связности технологической сети предприятия (большое количество удаленных объектов, не связанных с основной сетью линиями высокоскоростной и надежной связи);
- о низкой степени информатизации предприятия (отсутствии других внутренних штатных систем хранения и передачи файлов);
- о существовании значительной незащищенной части инфраструктуры предприятия, которая становится источником первоначального заражения накопителей;
- об общей низкой культуре информационной безопасности.

Шпионские программы

- Еще одна заметная проблема региона — **шпионские программы**, показатель которых также значительно **превышает среднемировое значение** — в **первом квартале 2025 года в 1,7 раза**.

  По доле компьютеров АСУ, на которых блокируется эта угроза, Африка **лидирует** в соответствующем рейтинге регионов.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, I квартал 2025 года

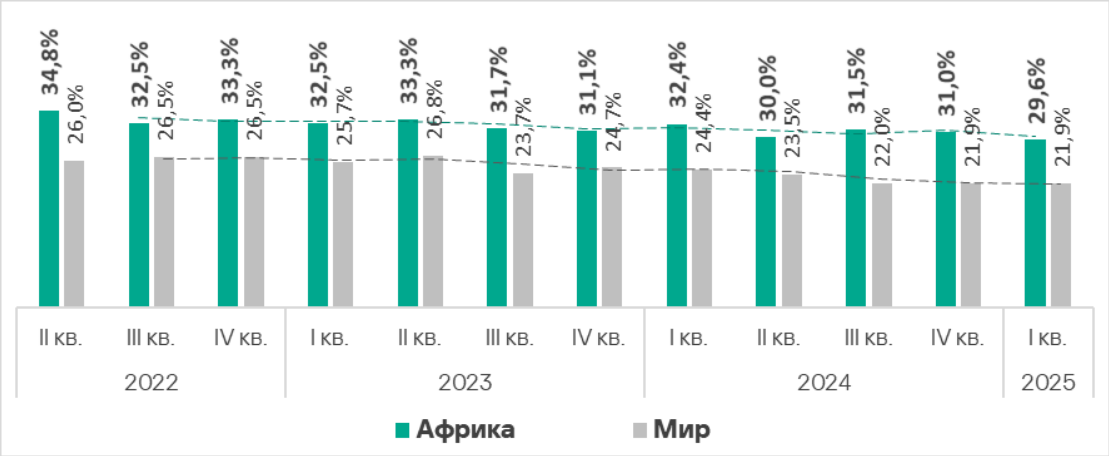
Обнаружение шпионского ПО на компьютере АСУ обычно указывает на то, что вектор первоначального заражения сработал, будь то переход по вредоносной ссылке, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует об отсутствии или о неэффективности мер защиты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

Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

Общая ситуация

Африка традиционно занимает **первое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. В первом квартале 2025 года показатель региона составил **29,6%.** При этом доля компьютеров АСУ, на которых были заблокированы вредоносные

объекты, снизилась. В регионе наблюдается незначительный **нисходящий тренд** с колебаниями.



Сравнительный анализ

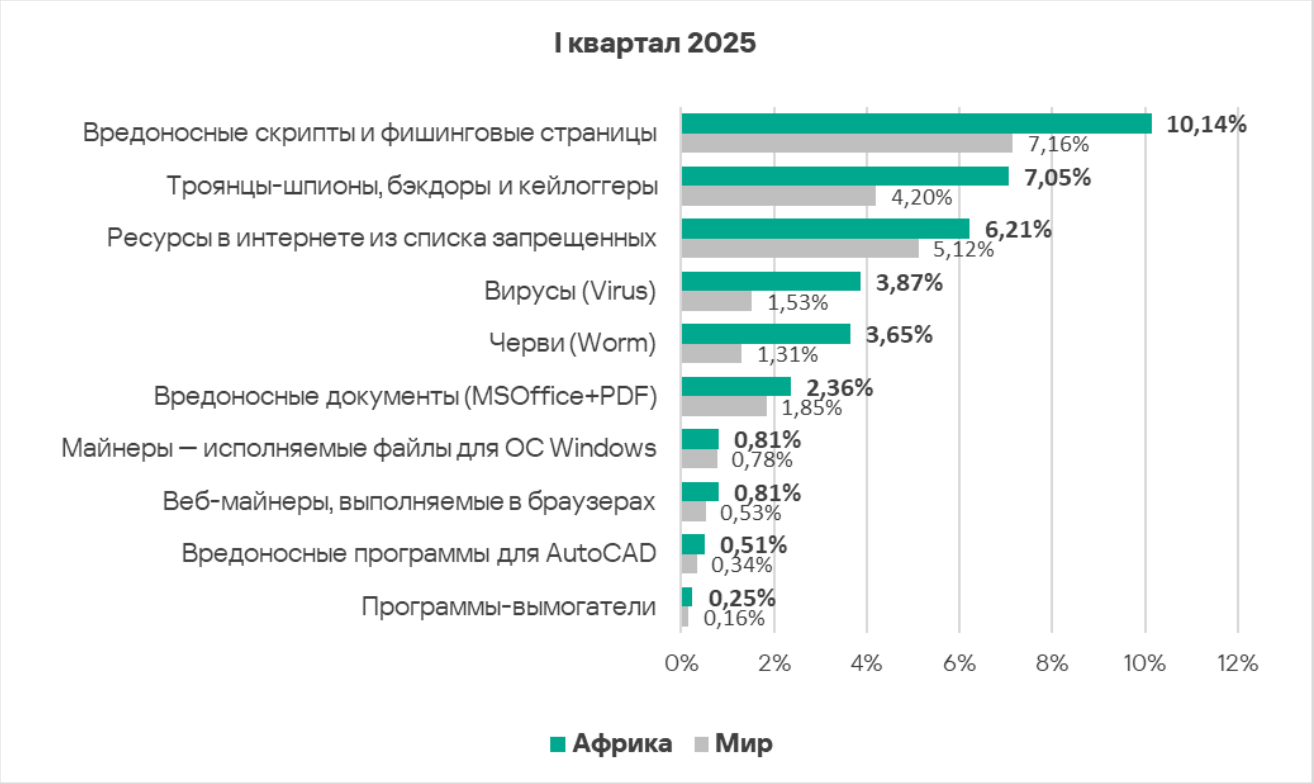
В **первом квартале 2025 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Африке выше **среднемирового значения в 1,4 раза**.

Категории угроз

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

Значительно **выше, чем в среднем по миру,** доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- Черви — в 2,8 раза;
- Вирусы — в 2,5 раза;
- Шпионские программы — в 1,7 раза;
- Программы-вымогатели — в 1,6 раза;
- Веб-майнеры — в 1,5 раза;
- Вредоносные программы для AutoCAD — в 1,5 раза;
- Вредоносные скрипты и фишинговые страницы — в 1,4 раза;
- Вредоносные документы — в 1,3 раза;
- Ресурсы в интернете из списка запрещенных — в 1,2 раза.



Показатели по типам угроз свидетельствуют о признаках низкого уровня зрелости кибербезопасности промышленных предприятий на континенте: доступности интернет-ресурсов на компьютерах OT, слабой защите от фишинга, наличии значительной части незащищенной инфраструктуры и пока еще относительно низком уровне кибергигиены сотрудников.

Среди регионов в первом квартале 2025 года Африка лидирует в рейтингах по доле компьютеров АСУ, на которых были заблокированы

- Ресурсы в интернете из списка запрещенных;
- Шпионские программы;
- Черви;
- Веб-майнеры.

На втором месте среди регионов Африка по показателям категорий

- Вирусы;
- Вредоносные скрипты и фишинговые страницы.

Источники угроз

В первом квартале 2025 года Африка занимает **первое место** среди регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из **интернета** и со **съемных носителей.**

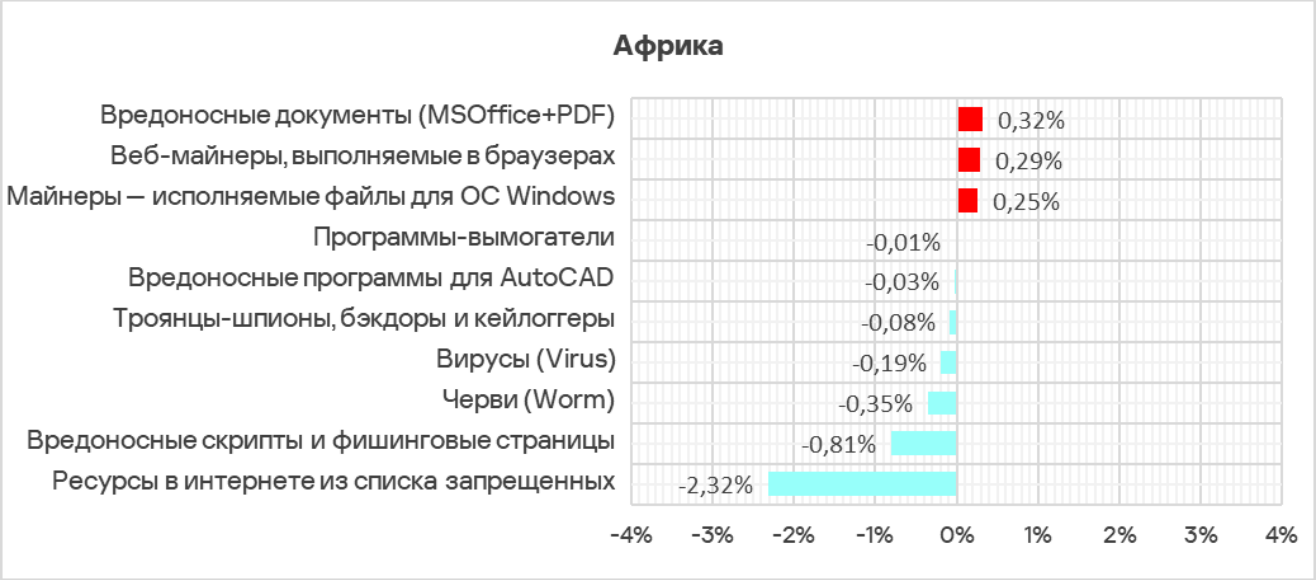
Значения по всем источникам угроз в регионе превышают среднемировые показатели:

- **Угрозы со съемных носителей — в 4,7 раза;**
- Угрозы из почтовых клиентов — в 1,4 раза;
- Угрозы из интернета — в 1,3 раза;
- Угрозы в сетевых папках — в 1,1 раза.

Как мы видим, в случае съемных носителей это превышение весьма значительно. Для остальных источников угроз оно сопоставимо с превышением показателя по всем угрозам (в 1,4 раза).

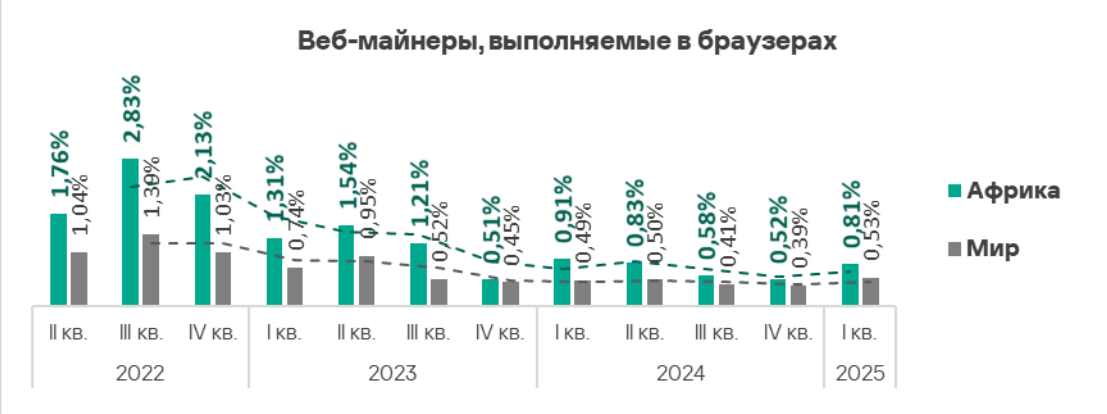
Изменения за квартал и тренды

Категории угроз

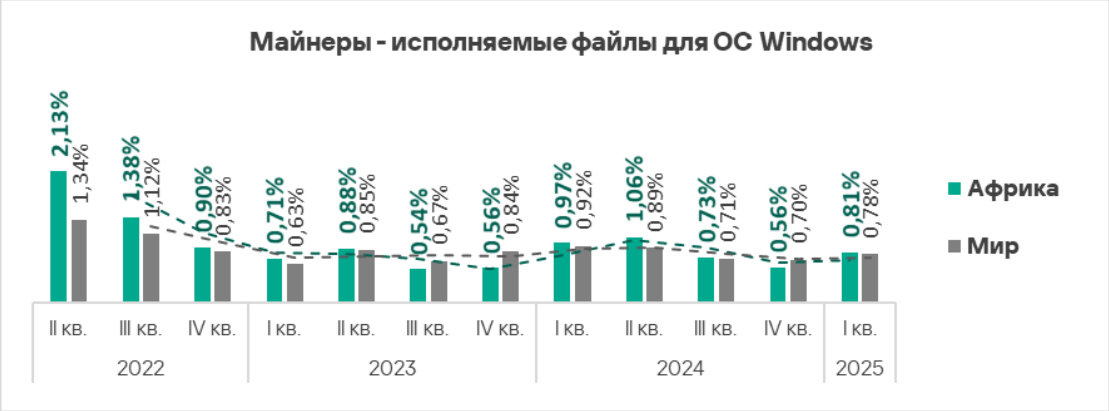


В первом квартале 2025 года **выросла** доля компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

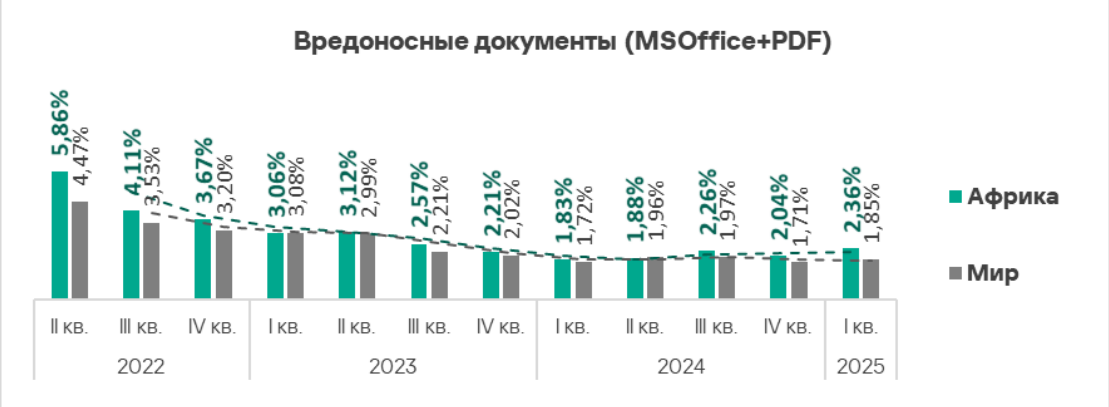
- Веб-майнеры — в 1,6 раз;



- Майнеры — исполняемы файлы — в 1,4 раза;



- Вредоносные документы — в 1,2 раза.



Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Африке со второго квартала 2022 года. В первом квартале 2025 года **шпионские программы** поднялись в третьей позиции в рейтинге на вторую.

Африка	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	2	2	2	2	2	3	2	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	3	3	3	3	3	3	2	3	3	2
Ресурсы в интернете из списка запрещенных	3	3	2	1	1	1	1	1	1	1	2	3
Вирусы (Virus)	6	6	6	5	5	5	5	5	5	5	4	4
Черви (Worm)	5	4	4	4	4	4	4	4	4	4	5	5
Вредоносные документы (MSOffice+PDF)	4	5	5	6	6	6	6	6	6	6	6	6
Майнеры – исполняемые файлы для ОС Windows	7	8	8	8	8	8	7	7	7	7	7	7
Веб-майнеры, выполняемые в браузерах	8	7	7	7	7	7	8	8	8	8	9	7
Вредоносные программы для AutoCAD	9	9	9	9	9	9	9	9	9	9	8	9
Программы-вымогатели	10	10	10	10	10	10	10	10	10	10	10	10

Источники угроз

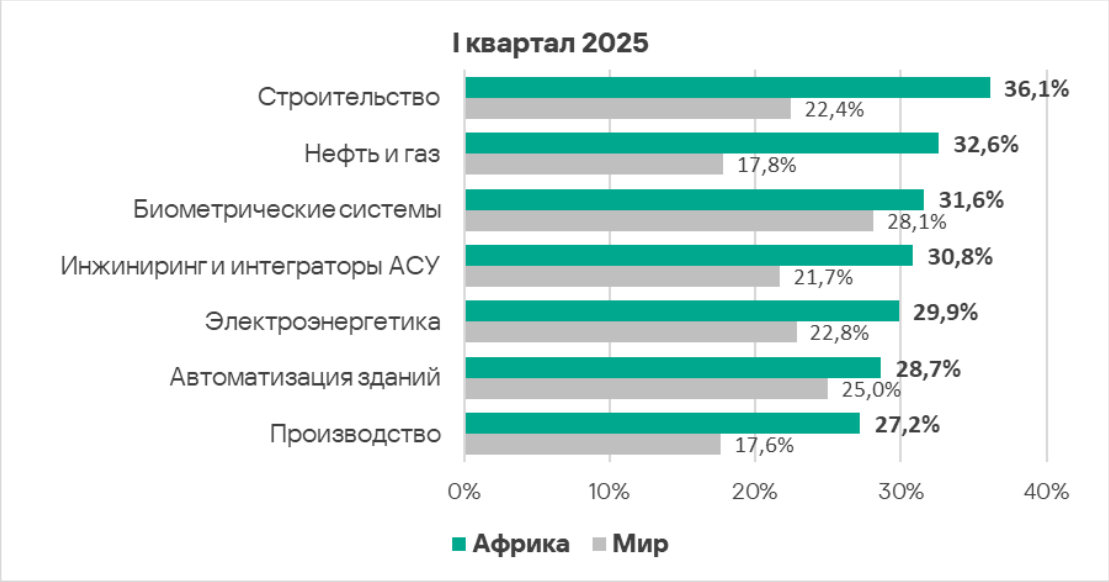
В **первом квартале 2025 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз, **кроме почтовых клиентов**.

Отрасли

Наиболее часто встречающейся с угрозами отраслью региона среди рассмотренных в отчете по-прежнему остается **строительство.**

Во всех рассмотренных отраслях региона зафиксирована **более высокая по сравнению с соответствующими среднемировыми показателями** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты. Наиболее значительная разница:

- Нефть и газ — в 1,8 раза;
- Строительство — в 1,6 раза;
- Производство — в 1,5 раза;
- Инжиниринг и интеграторы АСУ — в 1,4 раза;
- Электроэнергетика — в 1,3 раза.

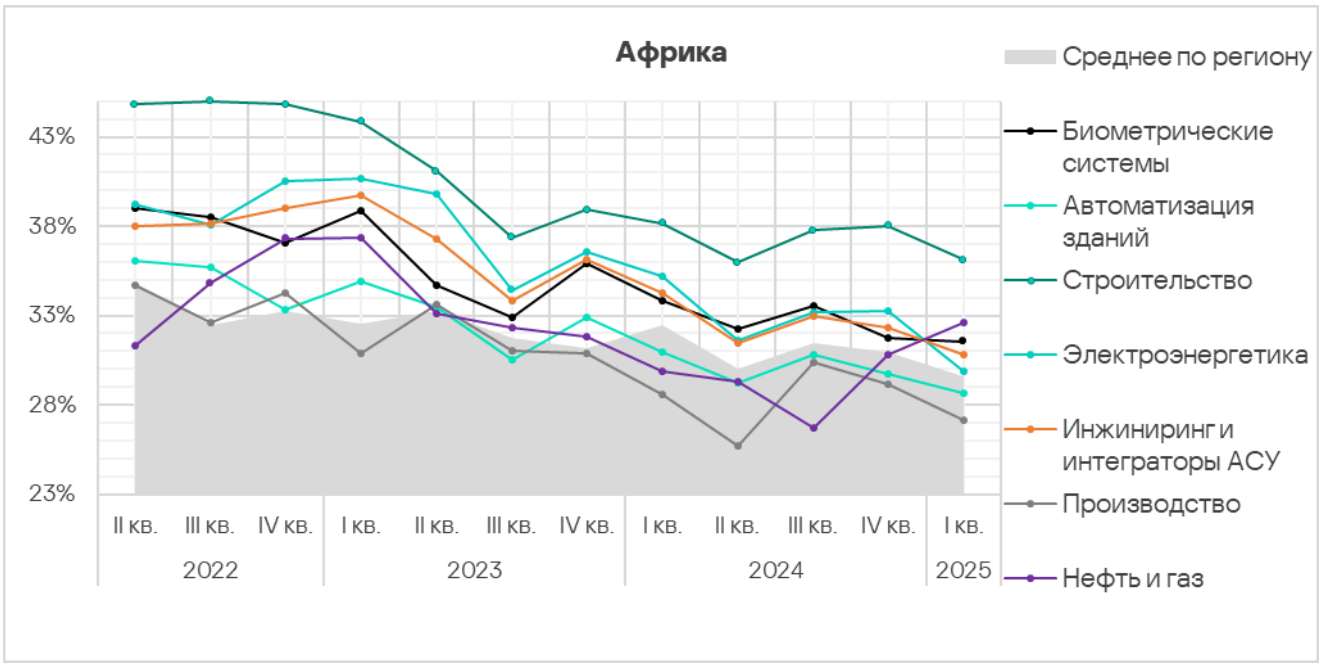


Один из общих выводов, которые можно сделать по итогам многолетних наблюдений за изменением показателей доступности OT-инфраструктур для угроз — скорость внедрения мер и средств кибербезопасности обычно уступает темпам развития отрасли. При введении объекта в эксплуатацию часто о его кибербезопасности думают в последнюю очередь. И средств защиты — недостаточно, и персонал — обучен плохо, и за соблюдением политик ИБ следят спустя рукава.

Эта тенденция хорошо просматривается на статистике по отраслям и типам инфраструктур в Африке. Нефтегазовый сектор, энергетика, промышленное производство, строительство — быстро развивающиеся секторы. Инжиниринг — им сопутствующий.

В **первом квартале 2025 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **увеличилась только в нефтегазовой отрасли**. Этот показатель растет второй квартал подряд, в результате нефтегазовая отрасль поднялась в соответствующем рейтинге исследуемых отраслей с последнего, седьмого, на второе место.

Рассмотренные отрасли демонстрируют **положительную динамику долгосрочных трендов** (показатели снижаются) с периодическими значительными колебаниями.



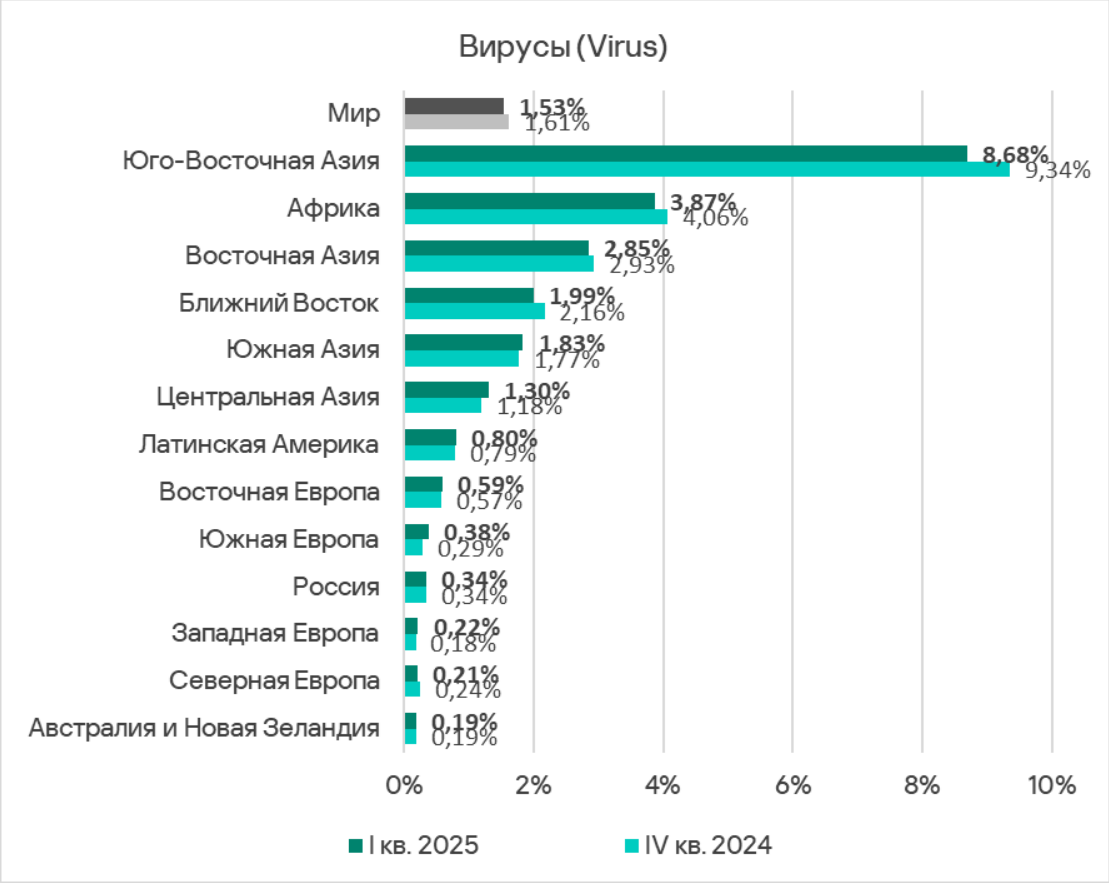
Юго-Восточная Азия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
9,34% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** снижение в I кв. 2025 г. 1,3x выше среднего по миру	**8,68%** **ВИРУСЫ** снижение в I кв. 2025 г. 1-е место в мире 5,7x выше среднего по миру	**5,93%** **ШПИОНСКИЕ ПРОГРАММЫ** снижение в I кв. 2025 г. 1,4x выше среднего по миру
2,65% **ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD** снижение в I кв. 2025 г. 1-е место в мире 7,8x выше среднего по миру	**0,80%** **ВЕБ-МАЙНЕРЫ** 2,4x рост в I кв. 2025 г. 1-е место по росту 2-е место в мире 1,5x выше среднего по миру	**0,74%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** 1,8x рост в I кв. 2025 г. 1-е место по росту
12,32% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ снижение в I кв. 2025 г. 2-е место в мире 1,2x выше среднего по миру	**3,97%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ рост в I кв. 2025 г. 1,4x выше среднего по миру	**0,16%** **СЕТЕВЫЕ ПАПКИ** КАК ИСТОЧНИК УГРОЗ снижение в I кв. 2025 г. 2-е место в мире 2,3x выше среднего по миру

- Юго-Восточная Азия занимает **второе место в мире** по доле компьютеров АСУ, на которых были заблокированы **угрозы в сетевых папках.** Показатель в регионе **выше среднемирового** значения **в 2,3 раза**.
- В Юго-Восточной Азии **вирусы занимают второе место** в региональном рейтинге категорий вредоносных программ по доле компьютеров АСУ, на которых они были заблокированы. Это самая высокая позиция вирусов в региональных рейтингах. Региональный показатель **в 5,7 раза превышает среднемировой** и является самым высоким значением в мире.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, I квартал 2025 года



Высокие показатели для самораспространяющегося ПО и сетевых папок свидетельствуют, вероятно, о наличии значительной части незащищенной инфраструктуры, которая становится источником вторичного заражения (распространения) вредоносного ПО, и недостатках сегментации сети предприятий в регионе.

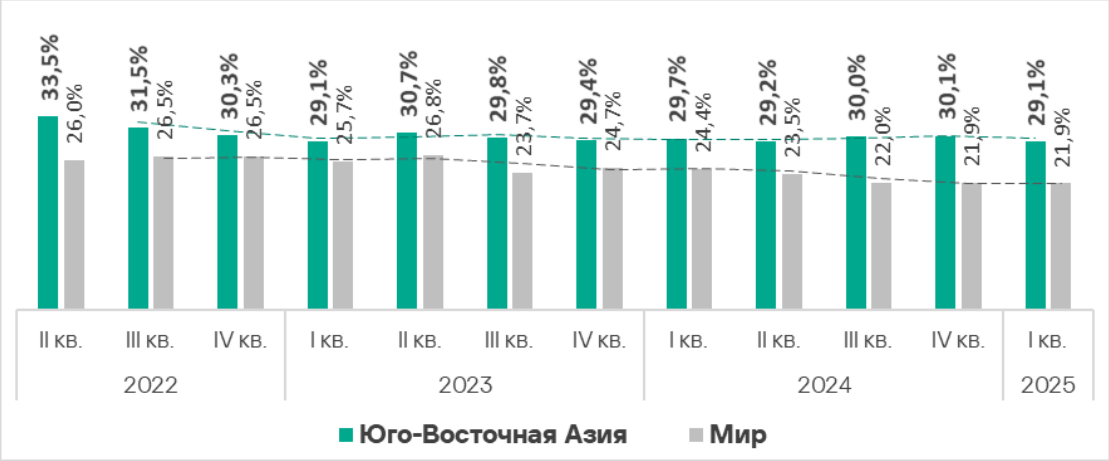
- Необычно высок в регионе показатель **вредоносных программ для AutoCAD.** В мире доля компьютеров АСУ, на которых было заблокировано такое вредоносное ПО, одна из самых низких среди всех категорий. А в региональном рейтинге они находятся **на пятом месте** с показателем, который **в 7,8 раза** превышает среднемировой и является самым высоким в мире.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, I квартал 2025 года

Вредоносные программы для AutoCAD в большинстве случаев распространяются так же, как и вирусы. Эта особенность объясняет столь высокий процент для этой категории вредоносного ПО.

Общая ситуация

Юго-Восточная Азия занимает **второе место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты с показателем **29,1%.** Этот показатель стабильно **превышает среднемировое значение**.



Сравнительный анализ

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Юго-Восточной Азии в первом квартале 2025 года превысила **среднемировое значение в 1,3 раза**.

Категории угроз

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

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

- Вредоносные программы для AutoCAD — в 7,8 раза.
- Вирусы — в 5,7 раза;
- Веб-майнеры — в 1,5 раза;
- Шпионские программы — в 1,4 раза.

Среди регионов в первом квартале 2025 года Юго-Восточная Азия лидирует в рейтингах по доле компьютеров АСУ, на которых были заблокированы:

- Вирусы;
- Вредоносные программы для AutoCAD.

Источники угроз

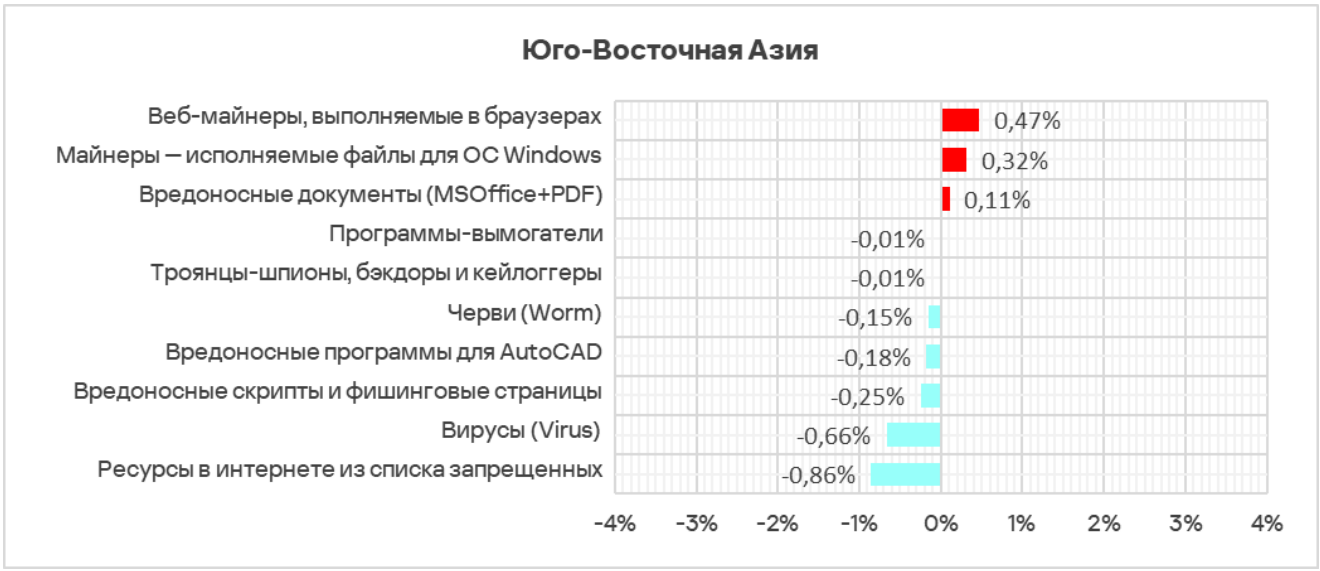
Значения доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, по всем источникам угроз в регионе превышают среднемировые показатели.

- **Угрозы в сетевых папках — в 2,3 раза;**

- Угрозы из почтовых клиентов — в 1,4 раза.
- Угрозы со съемных носителей — в 1,4 раза
- Угрозы из интернета — в 1,2 раза.

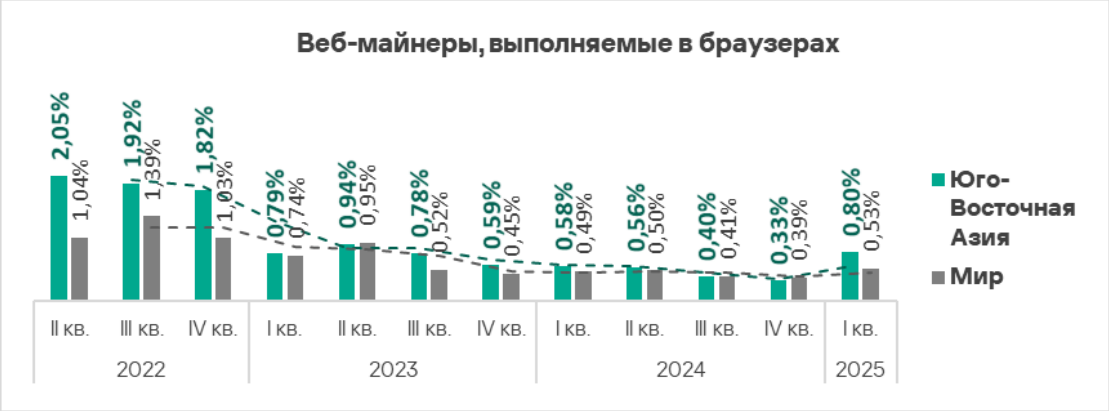
Изменения за квартал и тренды

Категории угроз

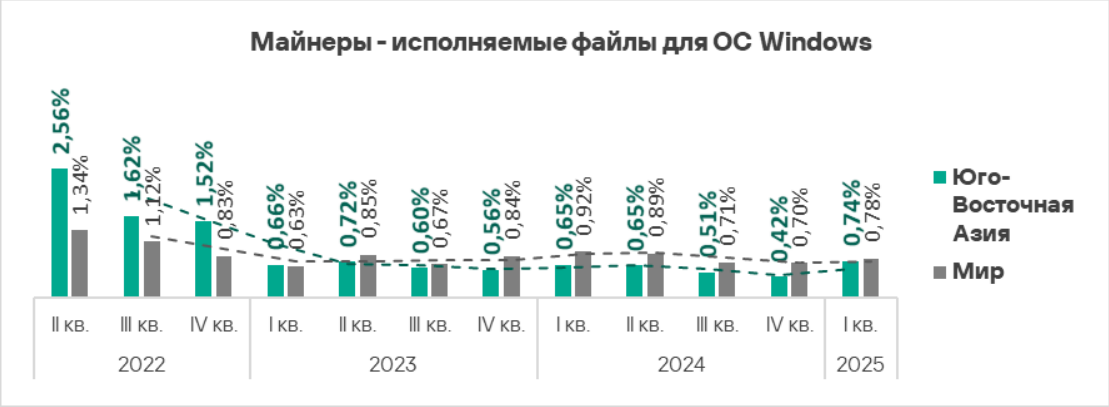


Наибольший рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- Веб-майнеры — в 2,4 раза, по росту этого показателя регион занял первое место в мире;



- Майнеры — исполняемые файлы для ОС Windows — в 1,8 раза; по росту этого показателя регион занял первое место в мире.

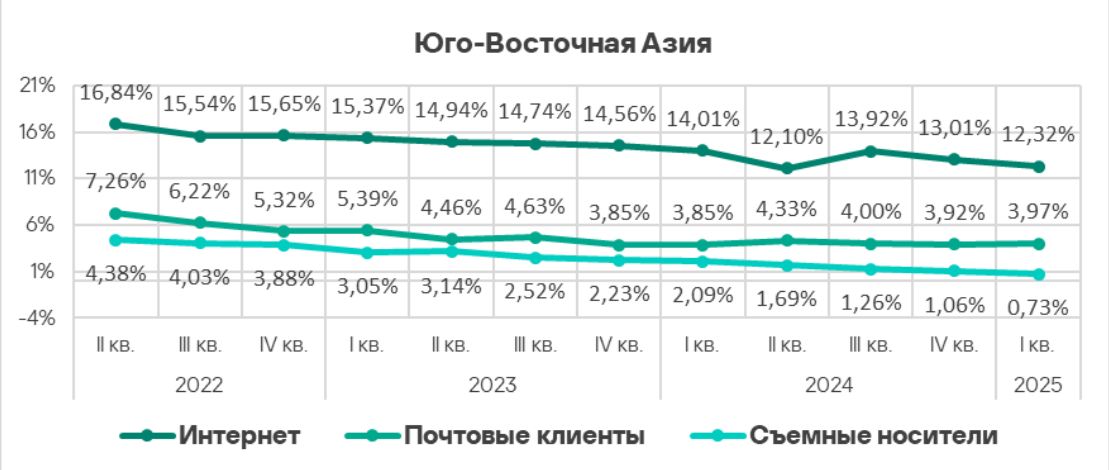


Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Юго-Восточной Азии со второго квартала 2022 года. В первом квартале 2025 года в этом рейтинге **программы-шпионы** поднялись с четвертого на третье место, а веб-майнеры — с девятого на восьмое.

Юго=Восточная Азия	2022 Q2	Q3	Q4	2023 Q1	Q2	Q3	Q4	2024 Q1	Q2	Q3	Q4	2025 Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	2	2	1	1	3	2	1	1	1
Вирусы (Virus)	5	4	4	4	3	4	3	1	1	2	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	2	3	3	4	3	4	4	4	4	4	3
Ресурсы в интернете из списка запрещенных	3	3	2	1	1	2	2	2	3	3	3	4
Вредоносные программы для AutoCAD	9	9	9	7	6	7	6	5	5	5	5	5
Вредоносные документы (MSOffice+PDF)	4	5	5	5	5	5	5	6	6	6	6	6
Черви (Worm)	7	6	6	6	7	6	7	7	7	7	7	7
Веб-майнеры, выполняемые в браузерах	8	7	7	8	8	8	8	9	9	9	9	8
Майнеры – исполняемые файлы для ОС Windows	6	8	8	9	9	9	9	8	8	8	8	9
Программы-вымогатели	10	10	10	10	10	10	10	10	10	10	10	10

Источники угроз

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз, **кроме угроз из почты**.

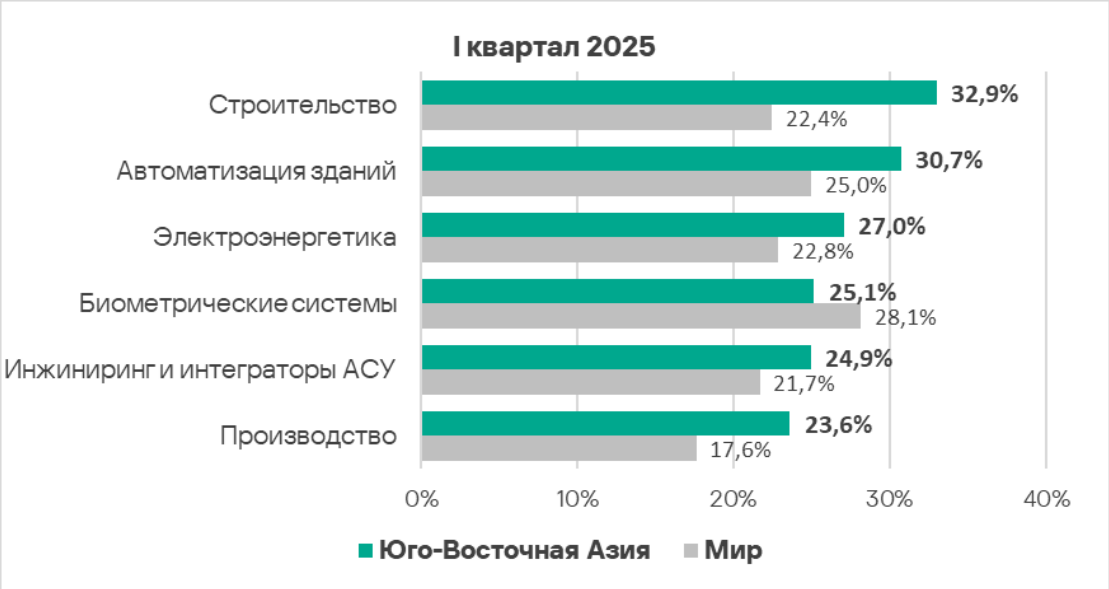


Отрасли

Наиболее часто встречающиеся с угрозами отрасли региона среди рассмотренных в отчете — **строительство и автоматизация зданий**, что также, судя по всему, отражает динамику развития промышленных секторов региональной экономики (скорость внедрения мер и средств кибербезопасности обычно уступает темпам развития отрасли).

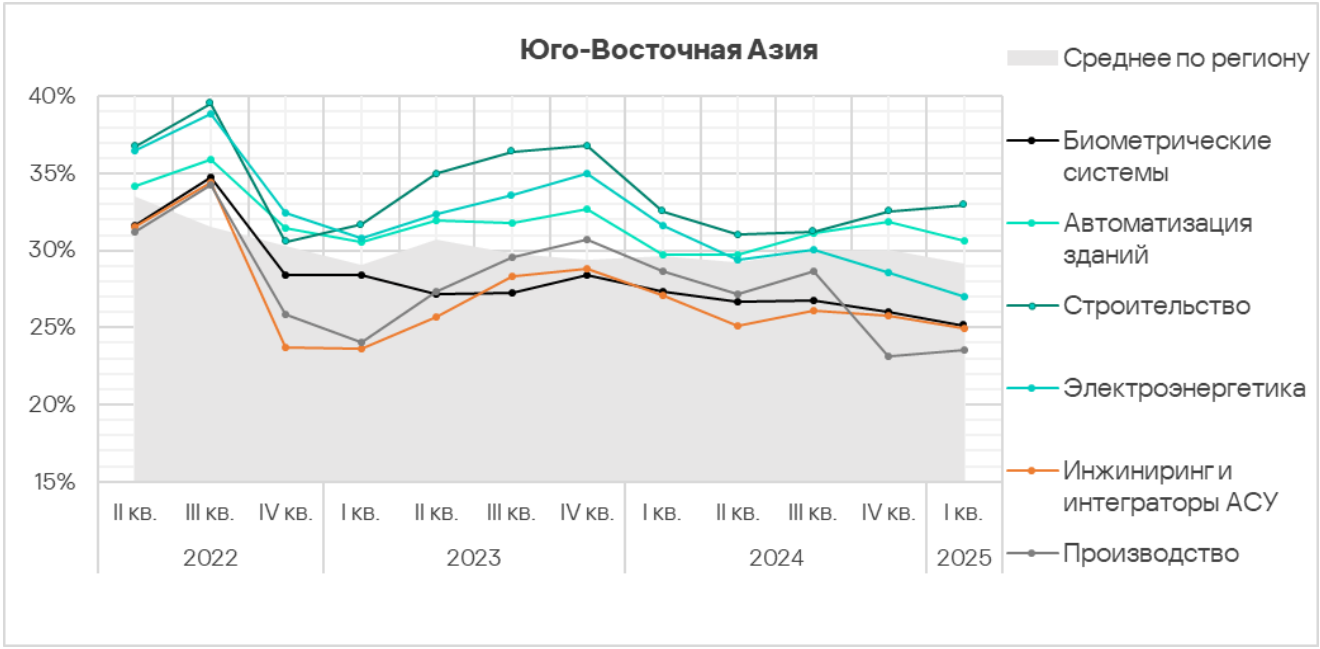
По сравнению с соответствующими **среднемировыми показателями более высокая доля компьютеров АСУ,** на которых были заблокированы вредоносные объекты, наблюдалась в следующих отраслях:

- Строительство — в 1,5 раза;
- Производство — в 1,3 раза;
- Автоматизация зданий — в 1,2 раза;
- Электроэнергетика — в 1,2 раза;
- Инжиниринг и интеграторы АСУ — в 1,2 раза.



В первом квартале 2025 года **рост** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался только в отраслях **строительство** и **производство.**

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



Центральная Азия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
5,50% **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,1x выше среднего по миру	**5,40%** **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ 1,3x рост в I кв. 2025 г. 1-е место по росту	**4,70%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г. 1,1x выше среднего по миру
2,79% **ЧЕРВИ** ▼ снижение в I кв. 2025 г. 2-е место в мире 2,1x выше среднего по миру	**1,72%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,2x рост в I кв. 2025 г. 1-е место в мире 2,2x выше среднего по миру	**1,30%** **ВИРУСЫ** ▲ 1,1x рост в I кв. 2025 г. 2-е место по росту
0,41% **ВЕБ-МАЙНЕРЫ** ▲ 1,4x рост в I кв. 2025 г.		
9,50% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г.	**1,42%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г.	**0,78%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 1,5x выше среднего по миру

- В Центральной Азии традиционно высока доля компьютеров АСУ, на которых угрозы блокируются при подключении **съемных носителей**. В первом квартале 2025 года соответствующий показатель в регионе был в 1,5 раза выше, чем в среднем по миру.
- В регионе также выше, чем среднемировой, показатель **сетевых папок**.

  Обе эти проблемы приводят, как правило к высоким показателям для самораспространяющихся угроз.

- В первом квартале 2025 года доля компьютеров АСУ, на которых блокируются **черви,** в регионе **в 2,1** раза выше, чем в среднем по миру.

  В рейтинге регионов по этому показателю Центральная Азия занимает **второе** (после Африки) место.

- **По росту** доли компьютеров АСУ, на которых блокируются **вирусы**, Центральная Азия в первом квартале 2025 года **лидирует среди регионов.**

- Еще одна угроза, характерная для региона, — **майнеры — исполняемые файлы для ОС Windows.** В первом квартале 2025 года доля компьютеров АСУ, на которых блокируются такие майнеры, в регионе **в 2,2** раза выше, чем в среднем по миру.

  В рейтинге регионов по этому показателю Центральная Азия занимает **первое место**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2025 года

Небольшое исследование показало, что программы для майнинга криптовалют, по всей видимости, нередко устанавливаются на компьютеры АСУ в регионе их легитимными пользователями. Однако зачастую, скачивая из сети такое ПО, сотрудники предприятия не подозревают, что его

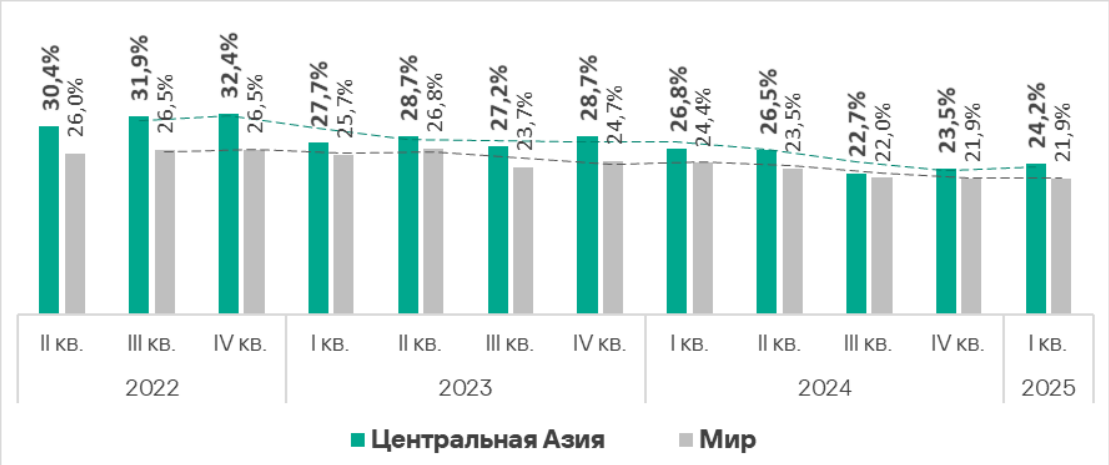
конфигурация была модифицирована злоумышленниками — в результате добытые майнингом средства уходят совсем не тем, кто это ПО для майнинга установил.

Также следует иметь в виду, что многие семейства такого вредоносного ПО обладают функциональностью кражи данных аутентификации и самостоятельного распространения по сети (см. выше) — так что его присутствие в технологической сети организации вовсе не стоит считать незначительной угрозой.

Общая ситуация

Центральная Азия занимает **третье место** в мире по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. В предыдущем квартале регион был на четвертом месте.

В первом квартале 2025 года региональный показатель незначительно **вырос — до 24,2%.**



Сравнительный анализ

Показатель региона все еще **превышает среднемировой,** хотя наблюдается тенденция к сокращению разрыва.

Категории угроз

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

- **Черви — в 2,1** раза. В Центральной Азии черви занимают четвертое место в региональном рейтинге категорий угроз — это самая высокая позиция червей в региональных рейтингах;
- **Майнеры — исполняемые файлы для Windows — в 2,2** раза;
- Программы-вымогатели — в 1,3 раза;
- Интернет-ресурсы из списка запрещенных — в 1,1 раза;
- Шпионские программы — в 1,1 раза.

Среди регионов в первом квартале 2025 года Центральная Азия находится:

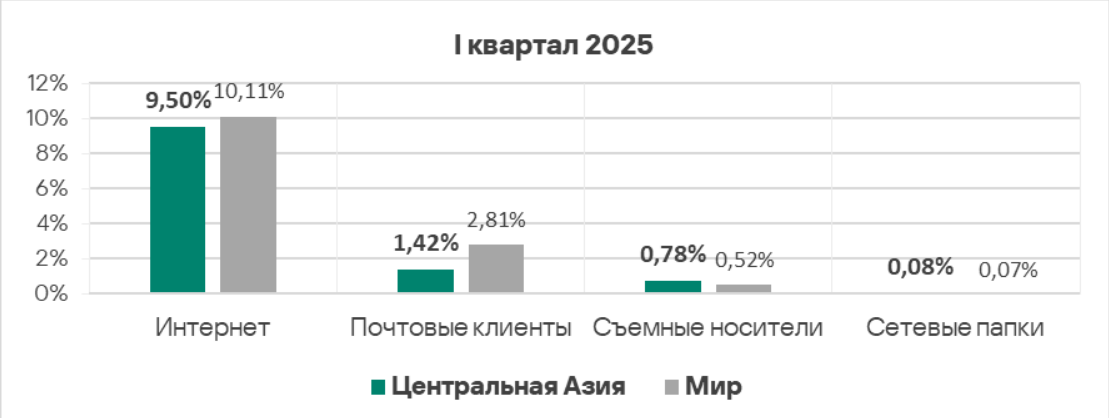
- **На первом** месте по доле компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для Windows**;
- **На втором** месте по доле компьютеров АСУ, на которых были заблокированы **черви**;

- **На третьем** месте по доле компьютеров АСУ, на которых были заблокированы **интернет-ресурсы из списка запрещенных.**

Источники угроз

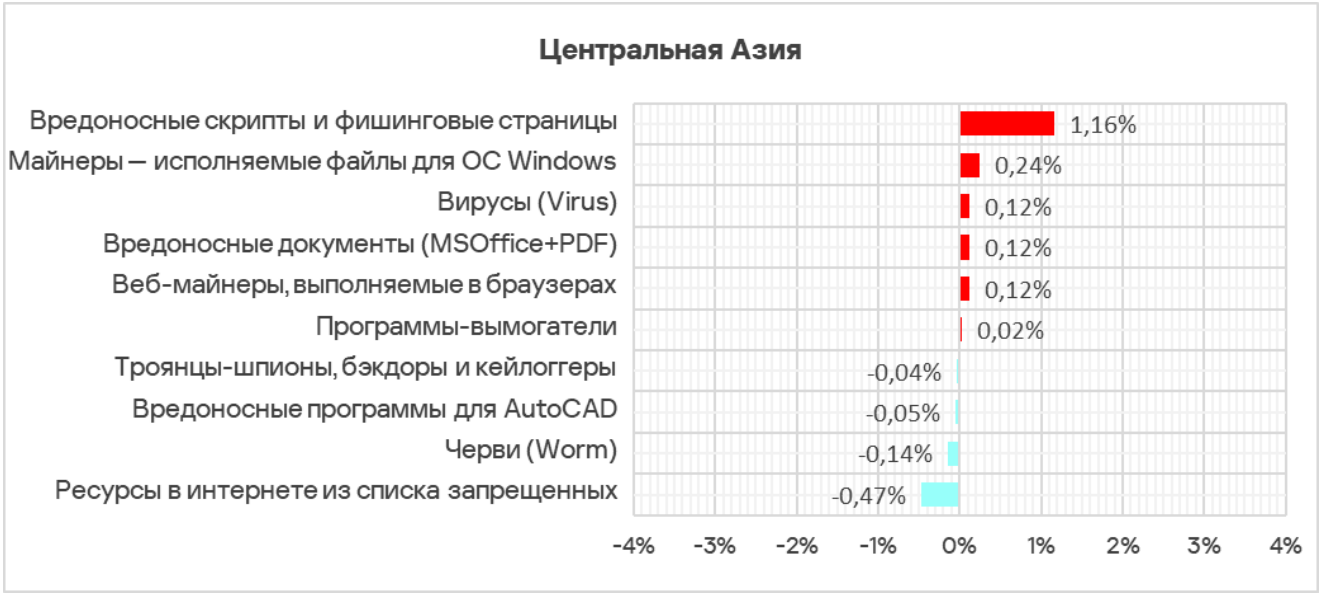
В первом квартале 2025 года в Центральной Азии **превышает среднемировые значения** доля компьютеров АСУ, на которых были заблокированы:

- Угрозы на **съемных носителях** — в 1,5 раза;
- Угрозы **в сетевых папках** — в 1,1 раза.



Изменения за квартал и тренды

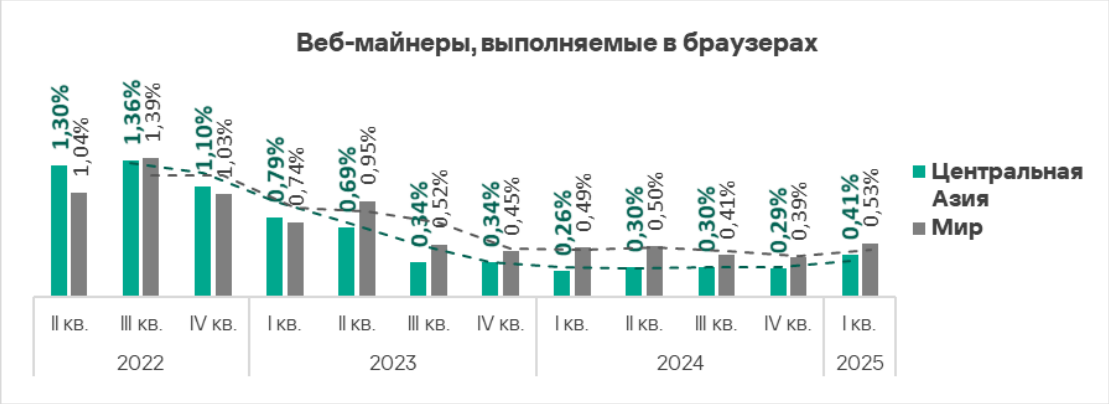
Категории угроз



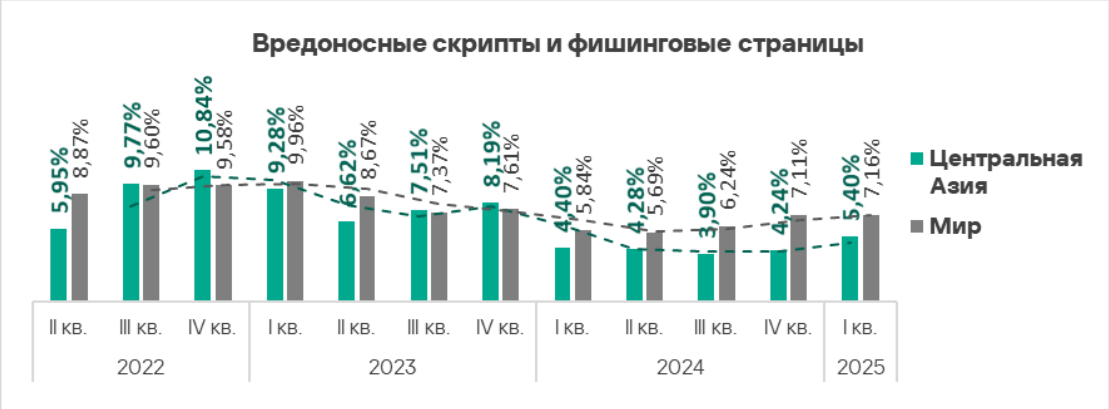
Центральная Азия находится **на первом месте среди регионов по росту** доли компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы**, и **на втором месте** — по **вирусам**.

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

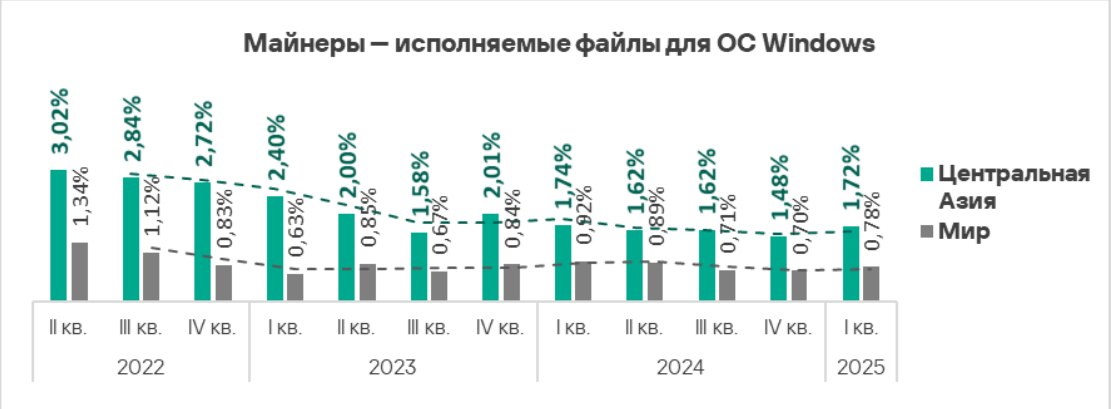
- Веб-майнеры — в 1,4 раза;



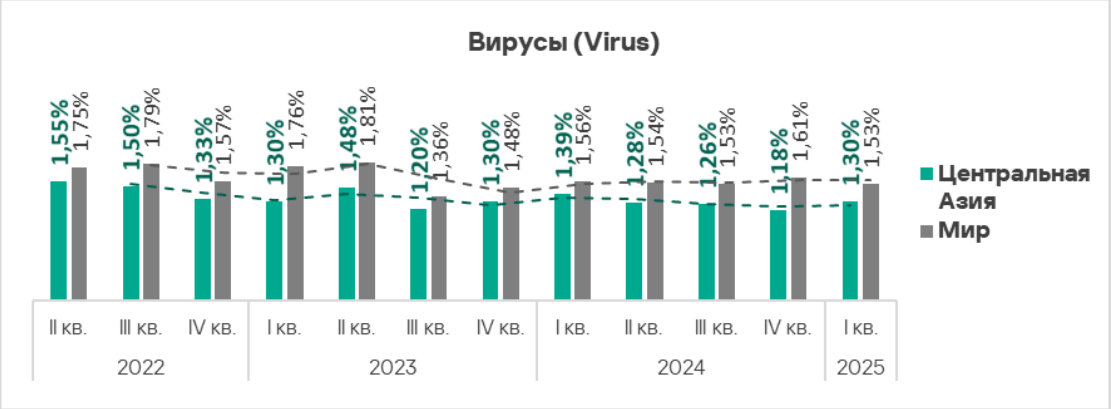
- Вредоносные скрипты и фишинговые страницы — в 1,3 раза;



- Майнеры — исполняемые файлы для ОС Windows — в 1,2 раза;



- Вирусы — в 1,1 раза.



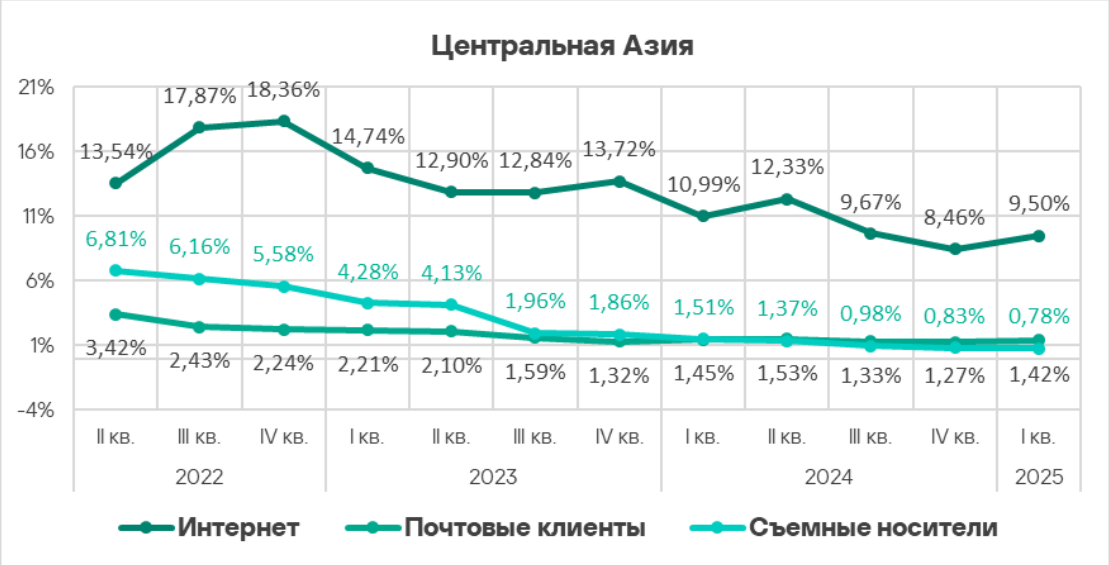
Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Центральной Азии со второго квартала 2022 года. **Вредоносные скрипты и фишинговые страницы** в первом квартале 2025 года поднялись с третьего места на второе.

Центральная Азия	2022 Q2	Q3	Q4	2023 Q1	Q2	Q3	Q4	2024 Q1	Q2	Q3	Q4	2025 Q1
Ресурсы в интернете из списка запрещенных	1	1	2	1	1	1	2	1	1	1	1	1
Вредоносные скрипты и фишинговые страницы	3	2	1	2	2	2	1	3	3	3	3	2
Троянцы-шпионы, бэкдоры и кейлоггеры	2	3	3	3	3	3	3	2	2	2	2	3
Черви (Worm)	4	4	4	4	4	4	4	4	4	4	4	4
Майнеры – исполняемые файлы	5	5	5	5	5	5	5	5	5	5	5	5
Вирусы (Virus)	7	7	7	7	7	6	6	6	6	6	6	6
Вредоносные документы (MSOffice+PDF)	6	6	6	6	6	7	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 первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **увеличилась** у двух источников угроз:

- Угрозы из интернета — в **1,1** раза;
- Угрозы из почтовых клиентов — в **1,1** раза.



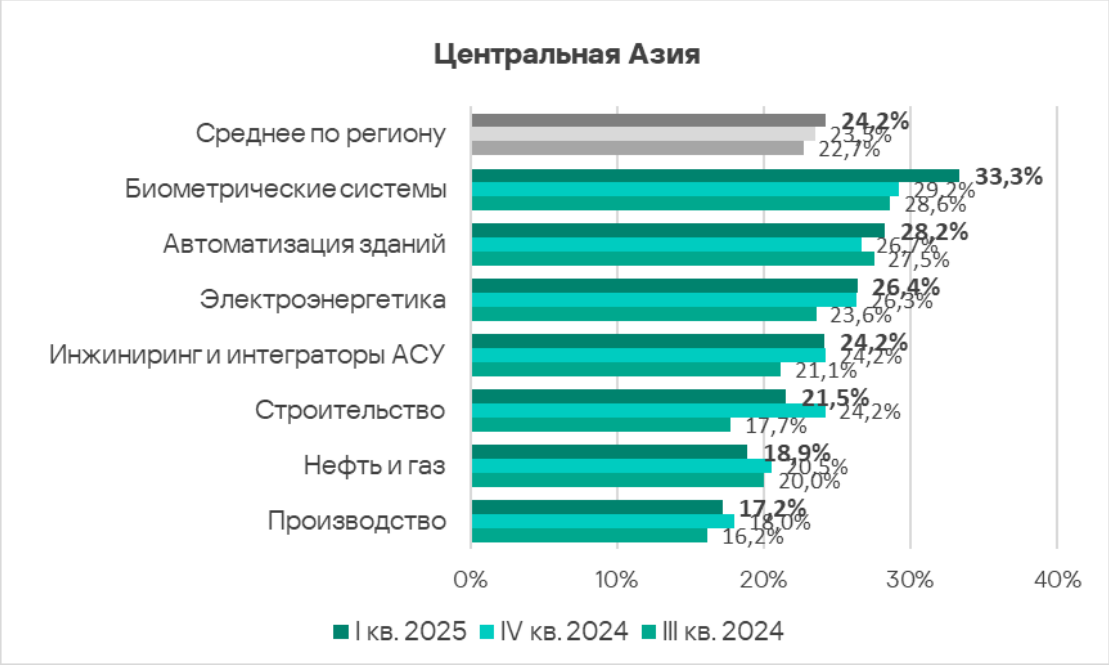
Отрасли

Из отраслей региона, рассмотренных в отчете, чаще встречаются с угрозами OT-инфраструктура биометрические системы и автоматизация зданий.

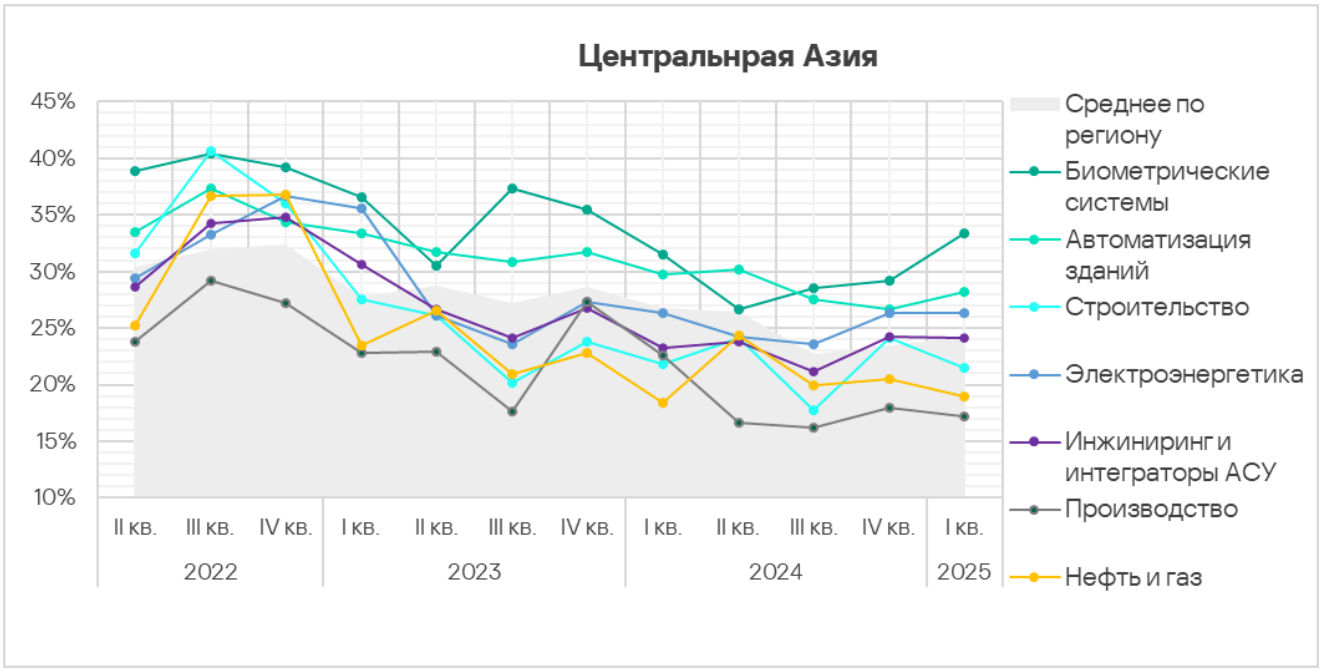
Региональный показатель **превышает среднемировое значение** у следующих отраслей:

- Биометрические системы и электроэнергетика — в 1,2 раза;
- Автоматизация зданий, а также инжиниринг и интеграторы АСУ — в 1,1 раза.

Больше всего за квартал вырос показатель OT-инфраструктуры биометрические системы — в 1,1 раза.



Тренды во всех отраслях демонстрируют в целом **положительную динамику** (показатели снижаются). Исключение — биометрические системы, где показатель растет с третьего квартала 2024 года.



Ближний Восток

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
9,58% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,3x выше среднего по миру	**6,25%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,5x выше среднего по миру	**4,62%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.
2,70% **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ рост в I кв. 2025 г. 3-е место в мире 1,5x выше среднего по миру	**1,99%** **ВИРУСЫ** ▼ снижение в I кв. 2025 г. 1,3x выше среднего по миру	**1,99%** **ЧЕРВИ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,5x выше среднего по миру
0,66% **ВЕБ-МАЙНЕРЫ** ▲ 1,1x рост в I кв. 2025 г. 1,2x выше среднего по миру	**0,61%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,2x рост в I кв. 2025 г.	**0,30%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 1,1x рост в I кв. 2025 г. 2-е место в мире 1,9x выше среднего по миру
10,56% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.	**5,17%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 2-е место в мире 1,8x выше среднего по миру	**0,89%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 1,7x выше среднего по миру

- На Ближнем Востоке значительно **выше среднемировых значений** доля компьютеров АСУ, на которых были заблокированы
  - **Угрозы из почтовых клиентов** — в 1,8 раза;
  - **Угрозы на съемных носителях** — в 1,7 раза.

- По доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов,** Ближний Восток занимает **второе место** среди регионов, а показатель категории **вредоносные документы** на Ближнем Востоке — в **1,5** раза выше, чем в среднем в мире.
- Одна из основных угроз, которые распространяются с использованием вредоносных документов, — **шпионское ПО**. Доля компьютеров АСУ, на которых блокируются шпионские программы, на Ближнем Востоке, как и у вредоносных документов, в **1,5** раза выше, чем в среднем в мире.

  Такая схема распространения отражается в нашей статистике.

> Шпионские программы используются злоумышленниками для кражи конфиденциальных данных. А в целевых атаках — и для распространения по сети атакованной организации и загрузки вредоносного ПО финального этапа. В ряде случаев попадание на компьютер шпионского ПО заканчивается установкой программ-вымогателей.

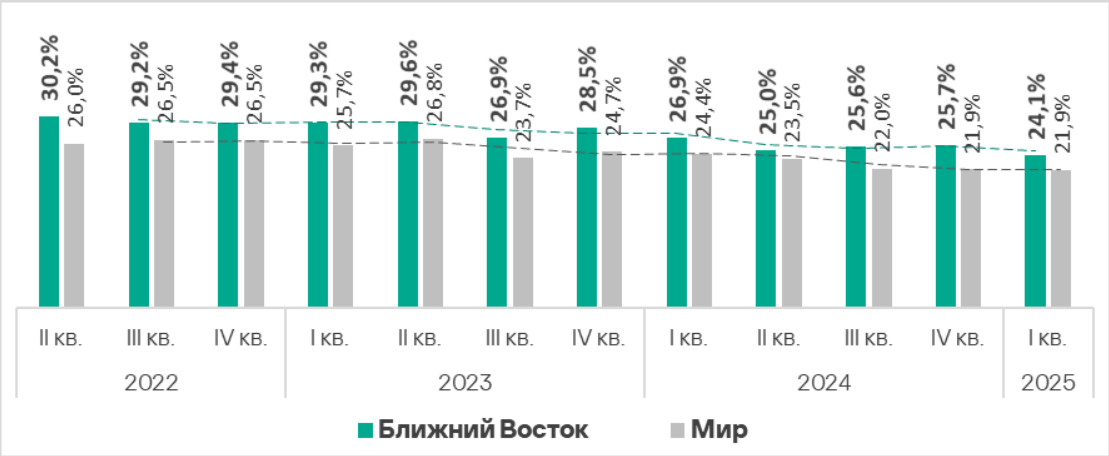
- На Ближнем Востоке доля компьютеров АСУ, на которых были заблокированы **программы-вымогатели,** стабильно высока. Показатель программ-вымогателей в регионе почти **вдвое превышает среднемировой**.

  В первом квартале 2025 года Ближний Восток занял **второе место** среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели (отметим, что в 2024 году регион лидировал в этом рейтинге).

Общая ситуация

Ближний Восток занимает **четвертое место** в мире по доле компьютеров АСУ, на которых заблокированы вредоносные объекты. Этот показатель в регионе стабильно **превышает среднемировое значение.**

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, на Ближнем Востоке уменьшилась и составила **24,1%.**



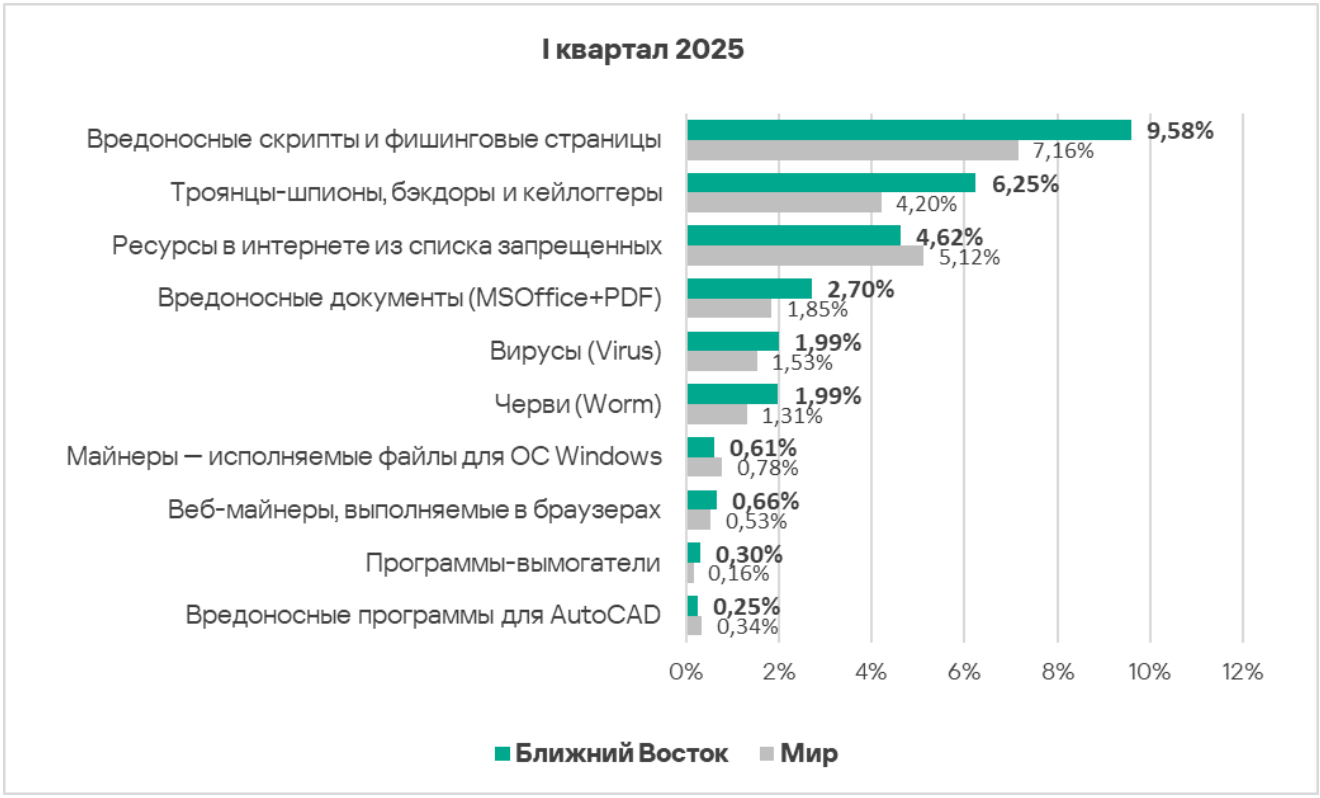
Общий анализ показывает высокий риск целевых атак. Высокие показатели для угроз, распространяющихся через почтовые клиенты (фишинг), шпионского ПО и программ вымогателей — явные признаки высокой доступности технологических систем в регионе для продвинутых категорий злоумышленников.

Сравнительный анализ

В первом квартале 2025 года региональное значение **выше среднемирового в 1,1 раза.**

Категории угроз

В регионе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выше среднемирового значения** у всех категорий, кроме ресурсов в интернете из списка запрещенных, майнеров — исполняемых файлов для Windows, а также вредоносных программ для AutoCAD.



О высоком риске целевых атак на технологические инфраструктуры промышленных предприятий в регионе (см. выше) свидетельствует, в том числе и высокий показатель для вредоносных скриптов и фишинговых страниц, многие из которых нацелены напрямую на кражу данных аутентификации сотрудников в корпоративных сервисах.

При этом относительно высокие показатели самораспространяющегося ПО свидетельствуют о наличии значительной части инфраструктуры, незащищенной от вредоносного ПО, и недостаточной сегментации сети.

Наибольшая разница **по сравнению со среднемировыми** у региональных показателей следующих категорий угроз:

- Программы-вымогатели — в 1,9 раза, второе место среди регионов;
- Черви — в 1,5 раза, третье место среди регионов;
- Шпионские программы — в 1,5 раза, третье место среди регионов;
- Вредоносные документы — в 1,5 раза, третье место среди регионов;
- Вредоносные скрипты и фишинговые страницы — в 1,3 раза, третье место среди регионов;
- Вирусы — в 1,3 раза.

Источники угроз

На Ближнем Востоке значительно превышает среднемировые значения доля компьютеров АСУ, на которых были заблокированы:

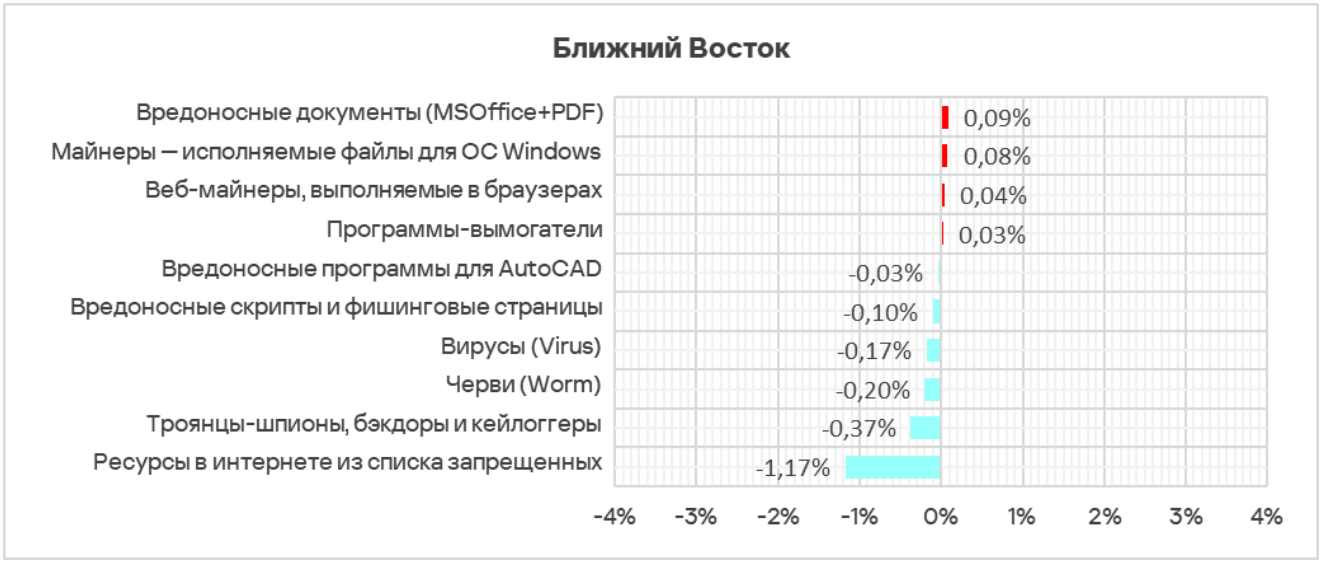
- Угрозы из **почтовых клиентов — в 1,8** раза;
- Угрозы на **съемных носителях** — в **1,7** раза.

По показателю **угроз из почты** в первом квартале 2025 года Ближний Восток занимает **второе место** среди регионов.

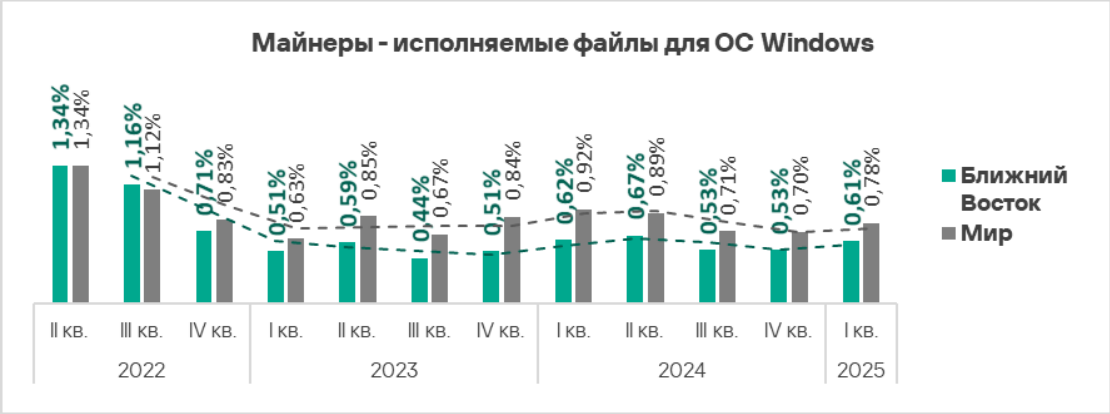
Изменения за квартал и тренды

Категории угроз

В течение первого квартала 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла у четырех категорий угроз.

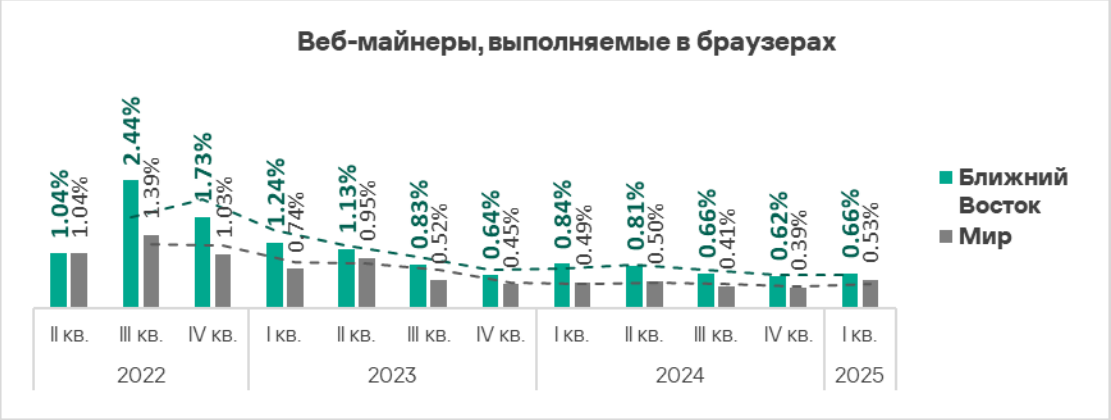


Наибольший рост за квартал зафиксирован у доли компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows — в 1,2 раза.

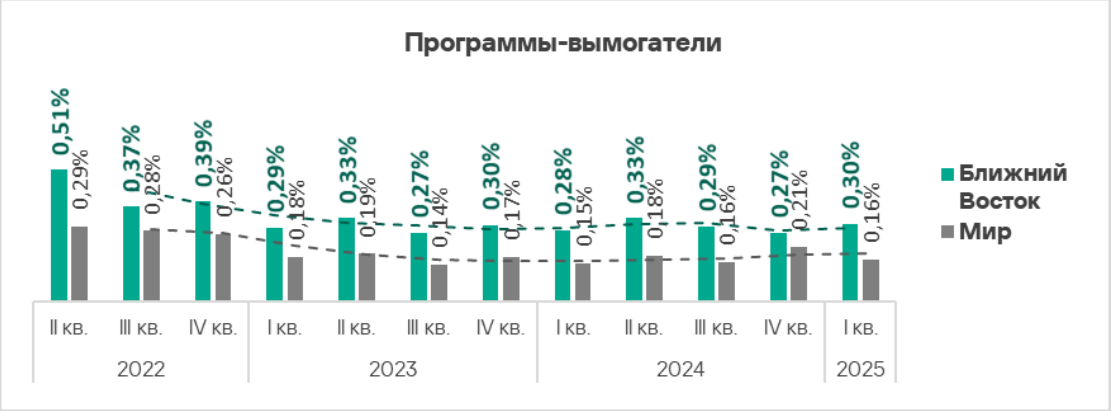


Выросли также показатели категорий:

- Веб-майнеры — в 1,1 раза;



- Программы-вымогатели — в 1,1 раза;



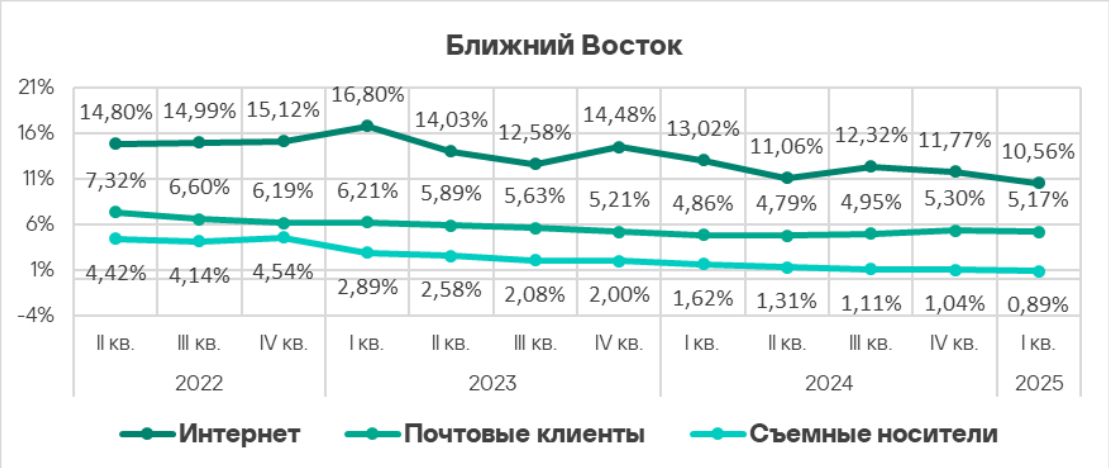
- Вредоносные документы.

Тепловая карта иллюстрирует изменения в рейтингах категорий угроз на Ближнем Востоке со второго квартала 2022 года. **Вирусы** в первом квартале 2025 года поднялись с шестого на пятое место, **программы-вымогатели** — с последнего десятого на девятое место.

Ближний Восток	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
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	3	3	2	3	3	2	3	2	2
Ресурсы в интернете из списка запрещенных	3	3	3	2	2	3	2	2	3	2	3	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	5	4	4	4	4
Вирусы (Virus)	6	6	6	6	6	6	6	6	6	6	6	5
Черви (Worm)	5	5	5	5	5	5	5	4	5	5	5	6
Веб-майнеры, выполняемые в браузерах	8	7	7	7	7	7	7	7	7	7	7	7
Майнеры – исполняемые файлы для ОС Windows	7	8	8	8	8	8	8	8	8	8	8	8
Программы-вымогатели	9	10	9	10	10	10	10	10	9	10	10	9
Вредоносные программы для AutoCAD	10	9	10	9	9	9	9	9	10	9	9	10

Источники угроз

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** у всех источников угроз.

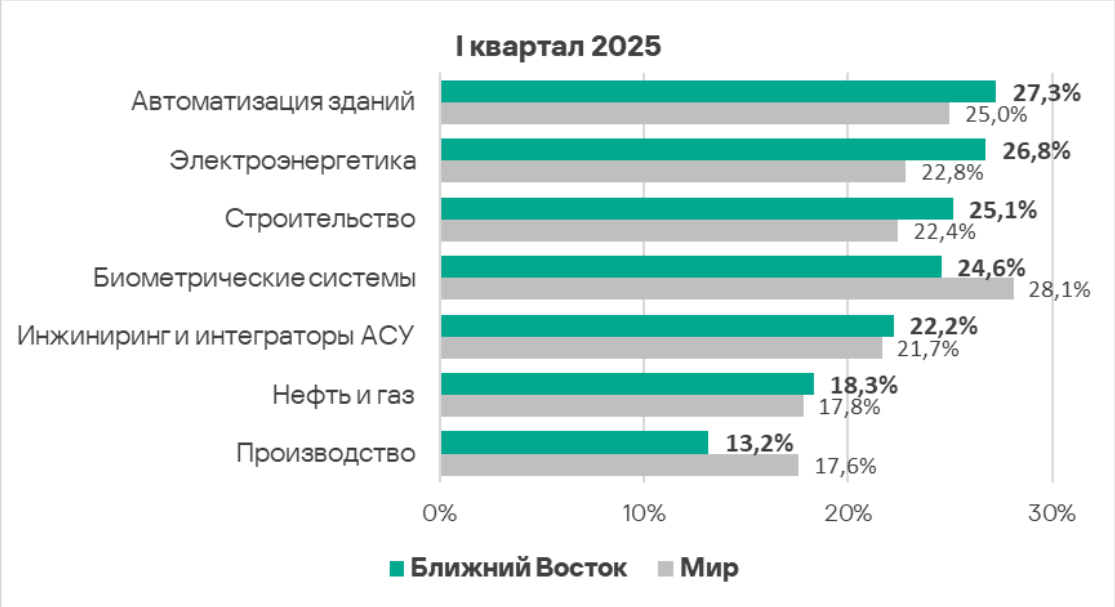


Отрасли

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

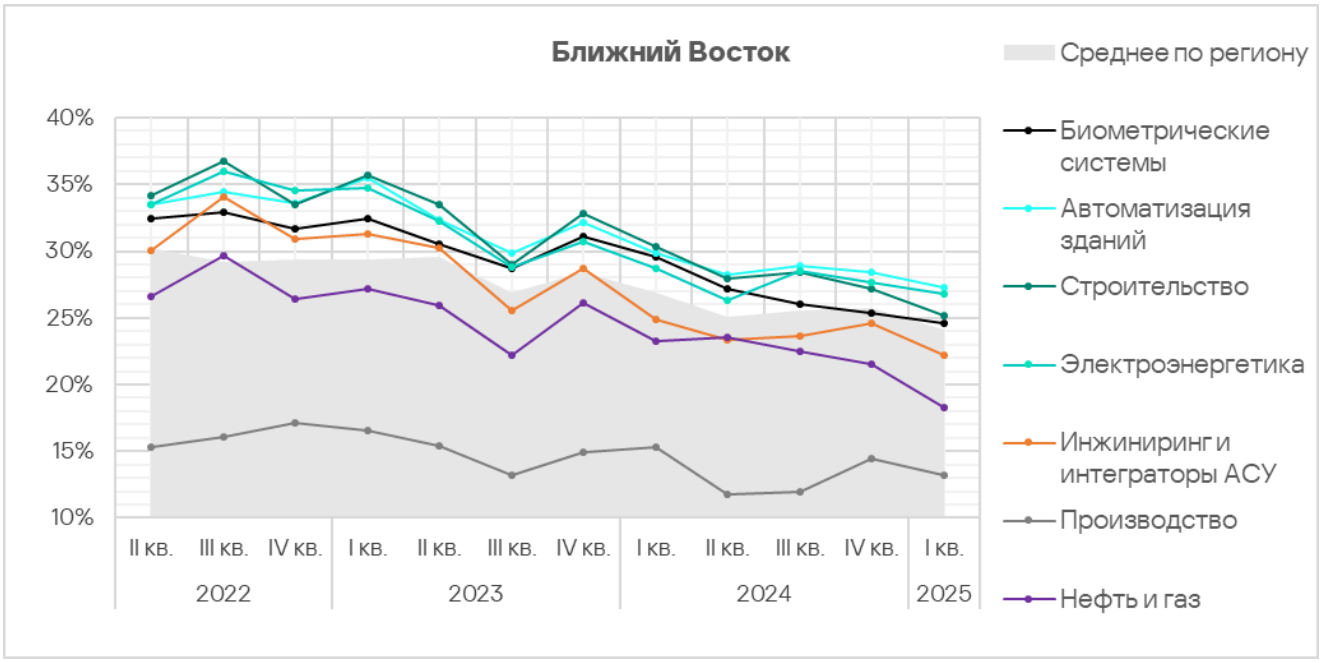
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, больше всего **превышает среднемировые значения** в следующих отраслях:

- Электроэнергетика — в 1,2 раза;
- Строительство — в 1,1 раза;
- Автоматизация зданий — в 1,1 раза.



В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **уменьшилась** во всех исследуемых отраслях.

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



Восточная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
7,68% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ слабый рост в I кв. 2025 г. 1,1x выше среднего по миру	**5,15%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г. 1,2x выше среднего по миру	**5,11%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.
2,43% **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,2x рост в I кв. 2025 г. 1-е место по росту 1,3x выше среднего по миру	**0,85%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,2x рост в I кв. 2025 г. 3-е место в мире 1,1x выше среднего по миру	**0,76%** **ВЕБ-МАЙНЕРЫ** ▲ 1,7x рост в I кв. 2025 г. 3-е место в мире 1,4x выше среднего по миру
0,15% **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 1,3x рост в I кв. 2025 г.	**9,78%** **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ рост в I кв. 2025 г.	**4,00%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 4-е место в мире 1,4x выше среднего по миру

- В Восточной Европе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты из **почтовых клиентов**, значительно **превышает среднемировой** показатель. В первом квартале 2025 года — **в 1,4 раза**. По этому показателю Восточная Европа занимает четвертое место среди регионов.
- Почтовые клиенты — основной источник, через который распространяются **вредоносные документы**. В регионе показатель этой категории угроз **в 1,3 раза превышает среднемировой**. По этому показателю Восточная Европа также (как и по почтовым клиентам) занимает четвертое место среди регионов.

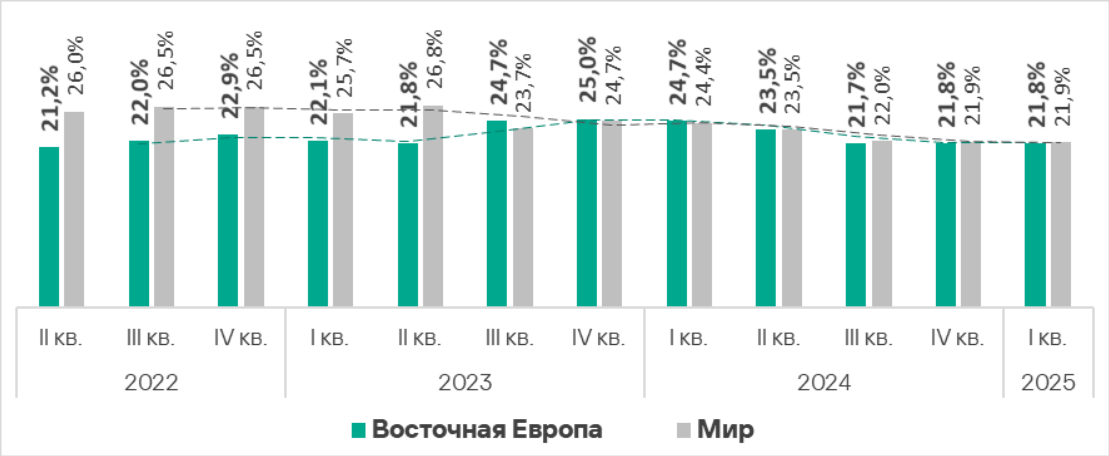
В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные документы, **увеличилась в 1,2 раза** — **по росту** этого показателя Восточная Европа **лидирует среди регионов**.

- Вредоносные документы используются злоумышленниками для распространения целевого вредоносного ПО — такого как **шпионские программы** и программы-вымогатели. Доля компьютеров АСУ, на которых были заблокированы **программы-вымогатели**, в первом квартале 2025 года **выросла** в регионе в **1,3 раза**.

Общая ситуация

В первом квартале 2025 года Восточная Европа поднялась с шестого на **пятое место** в мировом рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. До второго квартала 2023 года регион не поднимался в рейтинге выше девятого места.

В первом квартале 2025 года показатель **не изменился (21,8%)** и незначительно отличается от среднемирового значения.



Сравнительный анализ

Категории угроз

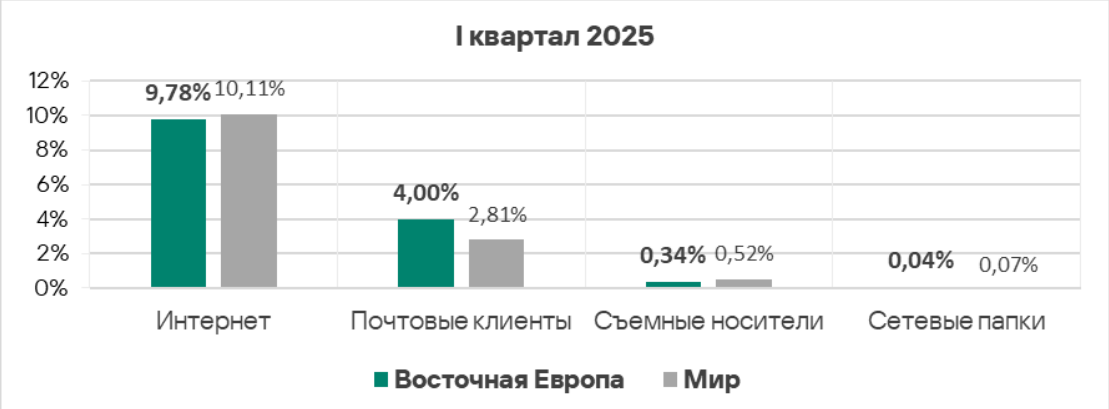
По сравнению со среднемировыми показателями в регионе заметно **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- Веб-майнеры — в 1,4 раза;
- Вредоносные документы — в 1,3 раза;
- Шпионские программы — в 1,2 раза;
- Черви — в 1,2 раза;
- Вредоносные скрипты и фишинговые страницы — в 1,1 раза;
- Майнеры — исполняемые файлы для ОС Windows — в 1,1 раза.

По показателям **майнеров** обеих категорий Восточная Европа **на третьем месте среди регионов.**

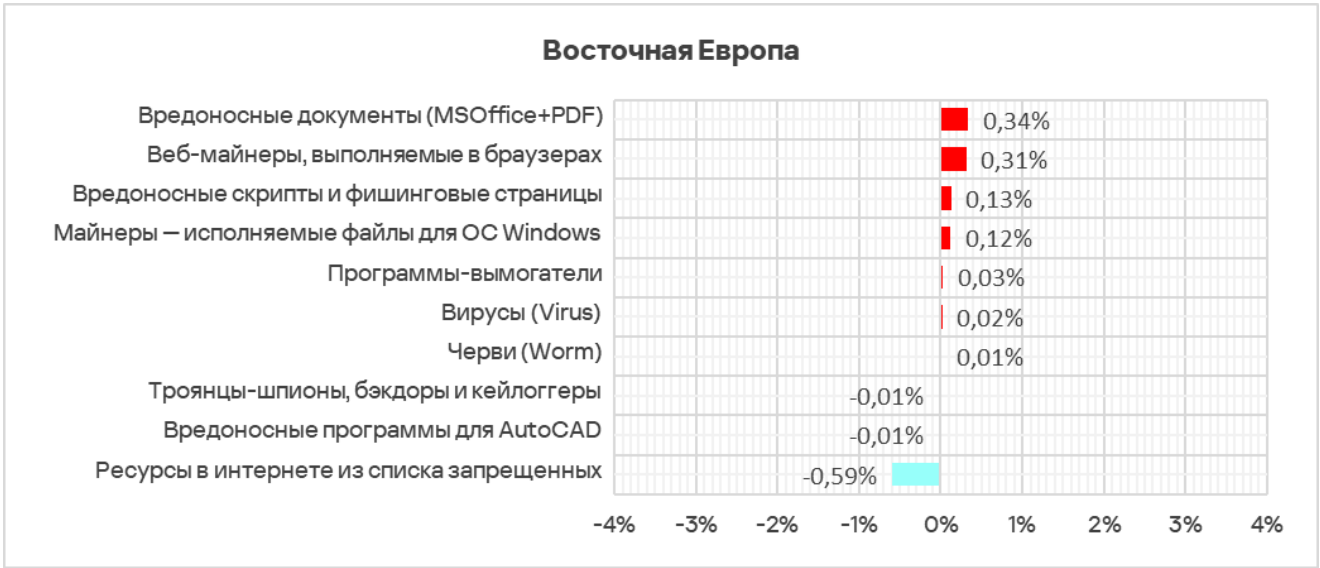
Источники угроз

Как и в предыдущем квартале, уровень угроз из **почтовых клиентов** в регионе **превышает среднемировой,** в этом квартале — **в 1,4 раза**. По этому показателю Восточная Европа занимает четвертое место среди регионов.



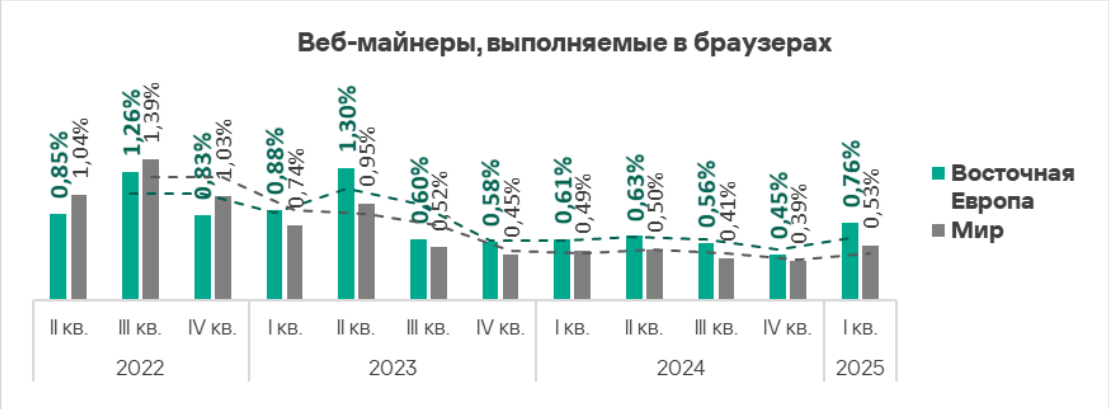
Изменения за квартал и тренды

Категории угроз

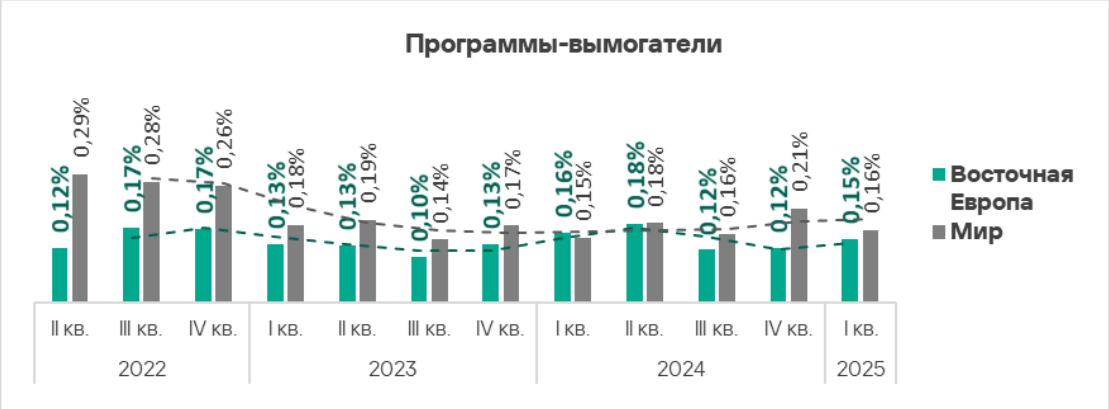


Наибольший рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

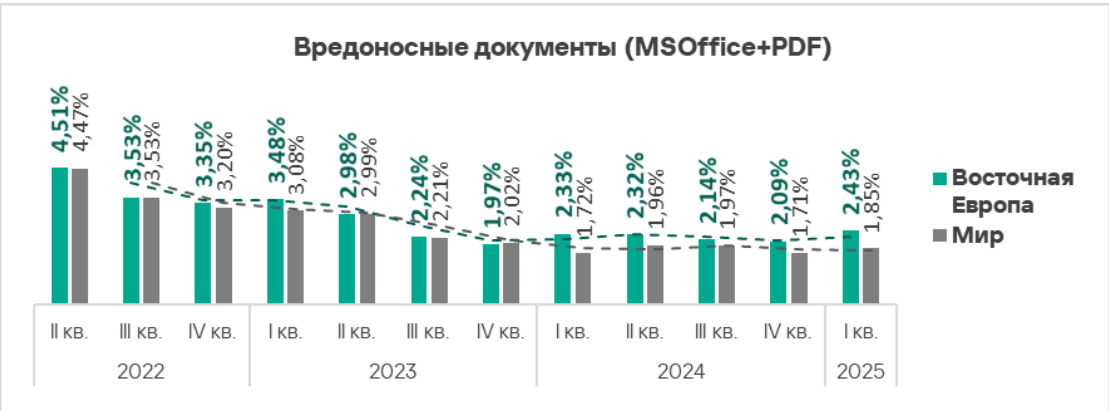
- Веб-майнеры — в 1,7 раз, регион занял **третье место в мире** по этому показателю;



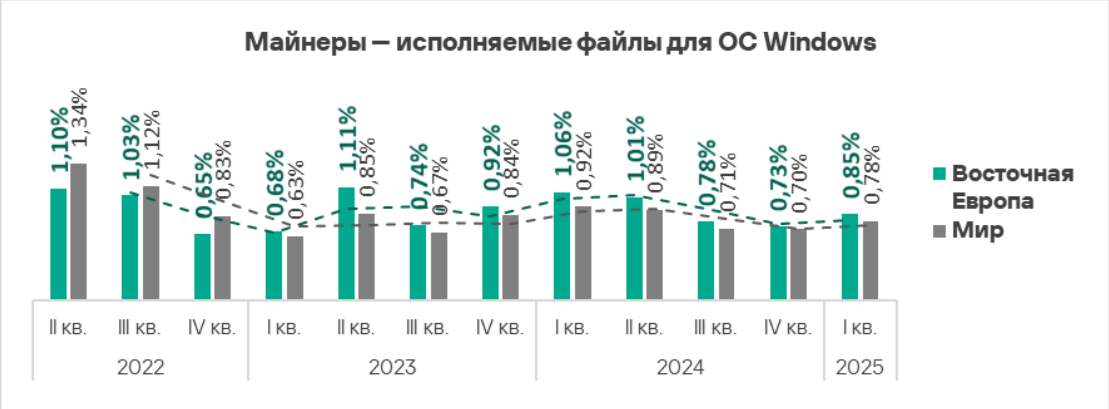
- Программы-вымогатели — в 1,3 раза;



- Вредоносные документы — в 1,2 раза. **По росту** этого показателя Восточная Европа заняла **первое место среди регионов**.



- Майнеры — исполняемые файлы для ОС Windows — в 1,2 раза; регион занял **третье место в мире по этому показателю**.

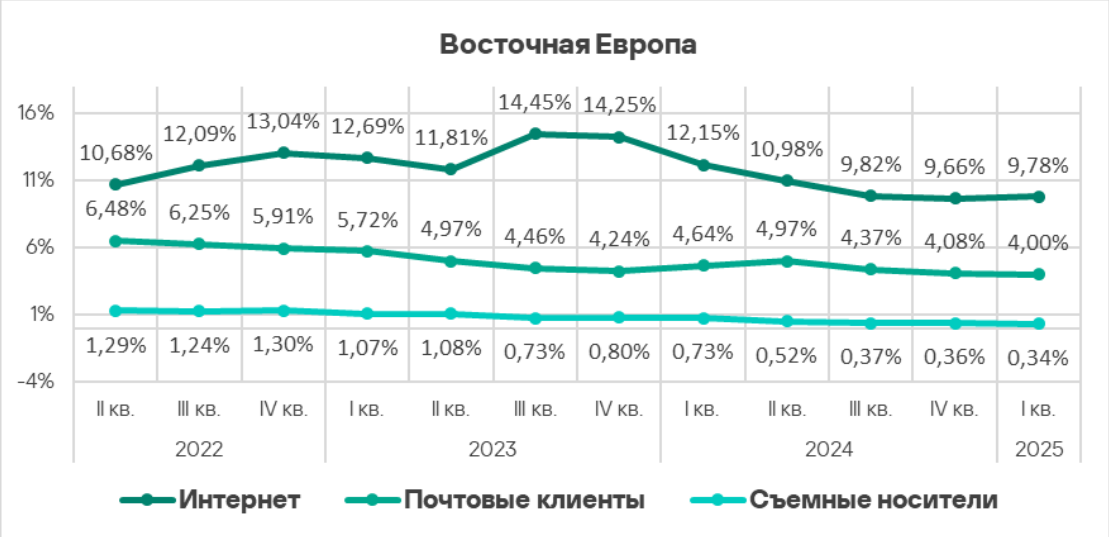


Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Европе с начала 2022 года. В первом квартале 2025 года **шпионские программы поднялись с третьего на второе место**.

Восточная Европа	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	2	2	1	1	2	2	2	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	3	3	3	3	3	2
Ресурсы в интернете из списка запрещенных	2	2	2	1	1	2	2	1	1	1	2	3
Вредоносные документы (MSOffice+PDF)	4	4	4	4	4	4	4	4	4	4	4	4
Черви (Worm)	6	7	6	5	6	5	5	5	5	5	5	5
Майнеры – исполняемые файлы для ОС Windows	5	6	7	7	7	6	6	6	6	6	6	6
Веб-майнеры, выполняемые в браузерах	7	5	5	6	5	7	7	7	7	7	8	7
Вирусы (Virus)	8	8	8	8	8	8	8	8	8	8	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

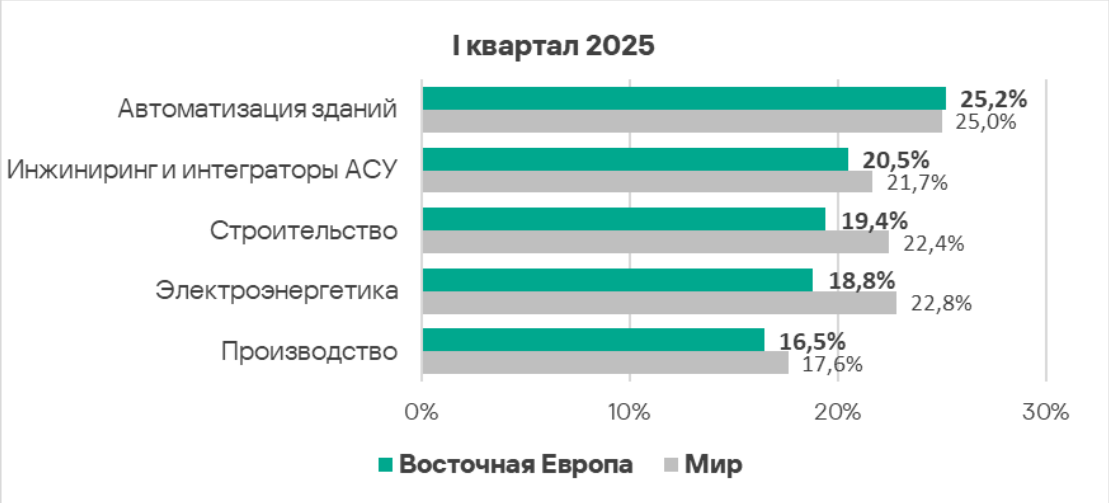
В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, из всех источников угроз немного увеличилась только у интернета.



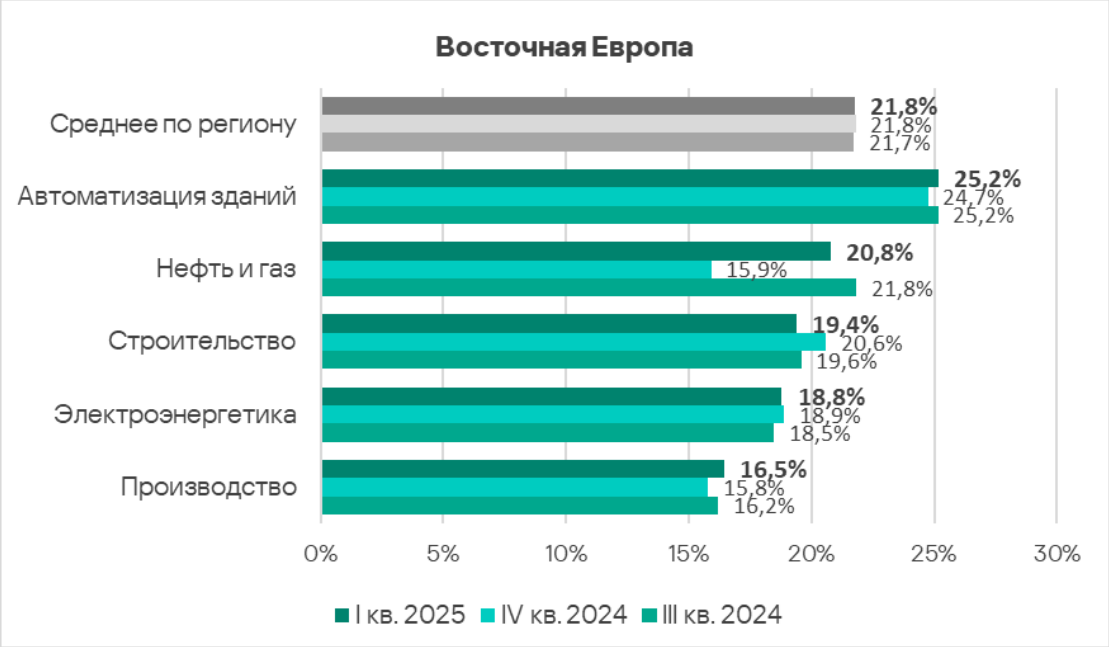
Хотя доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов,** снизилась, ее значение все равно осталось существенно выше среднемирового уровня — в первом квартале 2025 года в 1,4 раза.

Отрасли

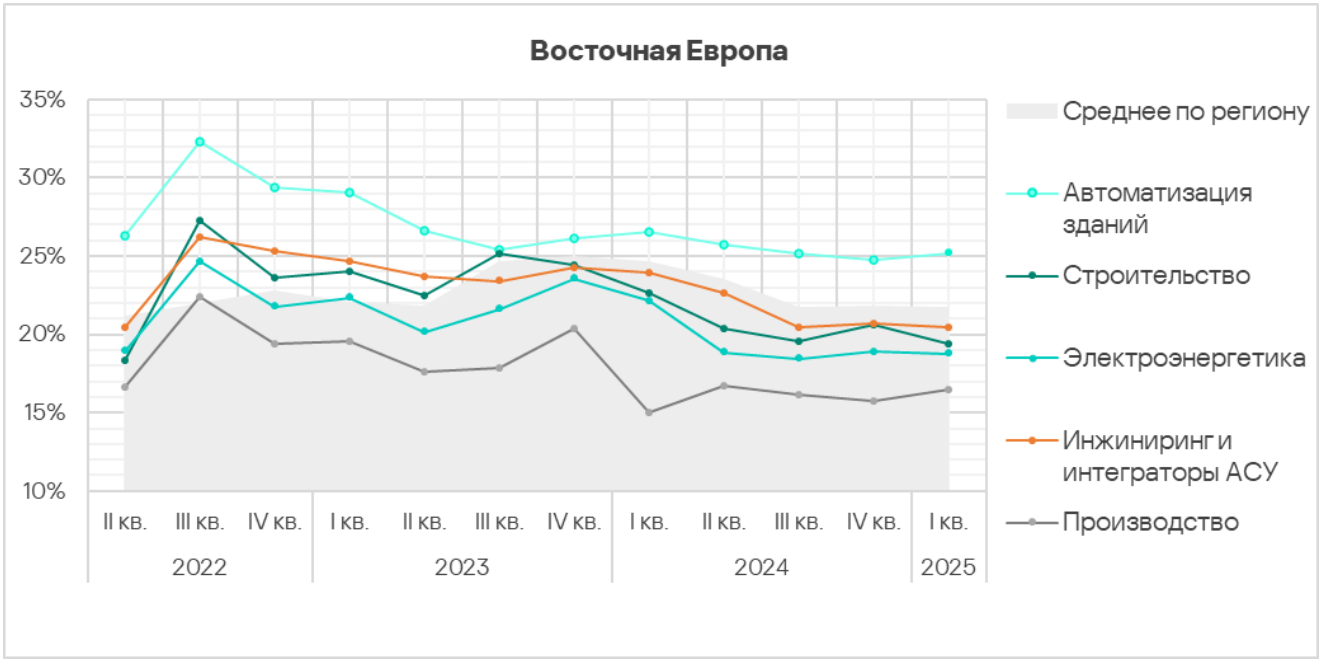
Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является **автоматизация зданий.** Только у этой отрасли из всех рассмотренных показатель **немного превышает среднемировой**.



В первом квартале 2025 наибольшее **увеличение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, зафиксировано **в нефтегазовой отрасли** — в 1,3 раза.



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



Южная Азия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
7,77% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ 1,1x рост в I кв. 2025 г. 1,1x выше среднего по миру	**4,66%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.	**2,90%** **ШПИОНСКИЕ ПРОГРАММЫ**
1,83% **ВИРУСЫ** ▲ слабый рост в I кв. 2025 г. 1,2x выше среднего по миру	**0,71%** **ВЕБ-МАЙНЕРЫ** ▲ 2,6x рост в I кв. 2025 г. 2-е место по росту 1,3x выше среднего по миру	**0,66%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,4x рост в I кв. 2025 г.
10,83% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ слабый рост в I кв. 2025 г. 3-е место в мире 1,1x выше среднего по миру	**2,08%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ 1,2x рост в I кв. 2025 г.	**1,08%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 2-е место в мире 2,1x выше среднего по миру
0,11% **СЕТЕВЫЕ ПАПКИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 3-е место в мире 1,6x выше среднего по миру		

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

- Южная Азия находится **на третьем месте** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках. Показатель по этому источнику угроз** превышает среднемировое значение в **1,6** раза.

  Съемные носители и сетевые папки часто становятся средством распространения самораспространяющегося вредоносного ПО.

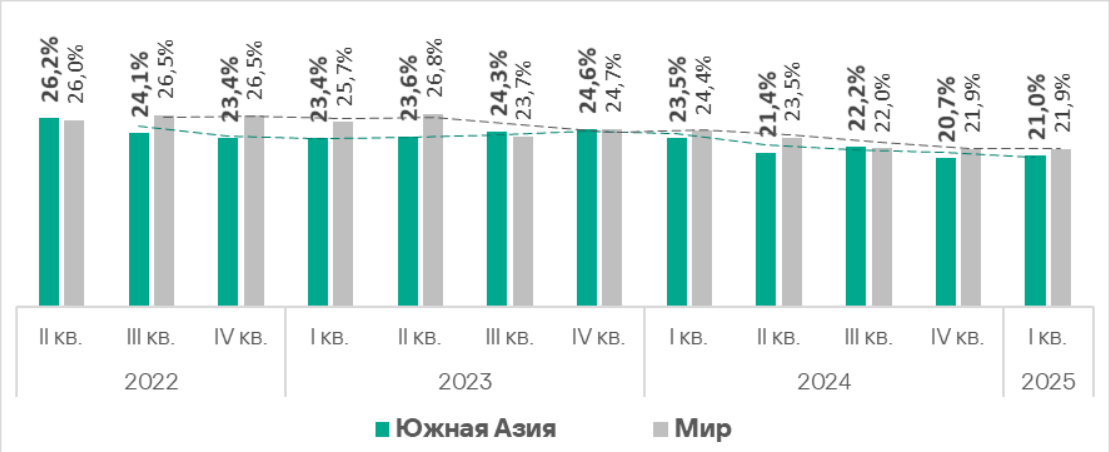
- **Вирусы** занимают **в регионе четвертое место** в рейтинге категорий блокируемых вредоносных объектов. У остальных регионов, за исключением Африки, Восточной и Юго-Восточной Азии, вирусы в аналогичном рейтинге не поднимаются выше пятой позиции.

Общая ситуация

В первом квартале 2025 года Южная Азия поднялась с восьмого на **шестое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

При этом показатель региона **уменьшился и составил 21,0%.**

Регион демонстрирует плавный **нисходящий тренд** с некоторыми колебаниями. С предыдущего квартала показатель региона **ниже среднемирового значения**.



Сравнительный анализ

Категории угроз

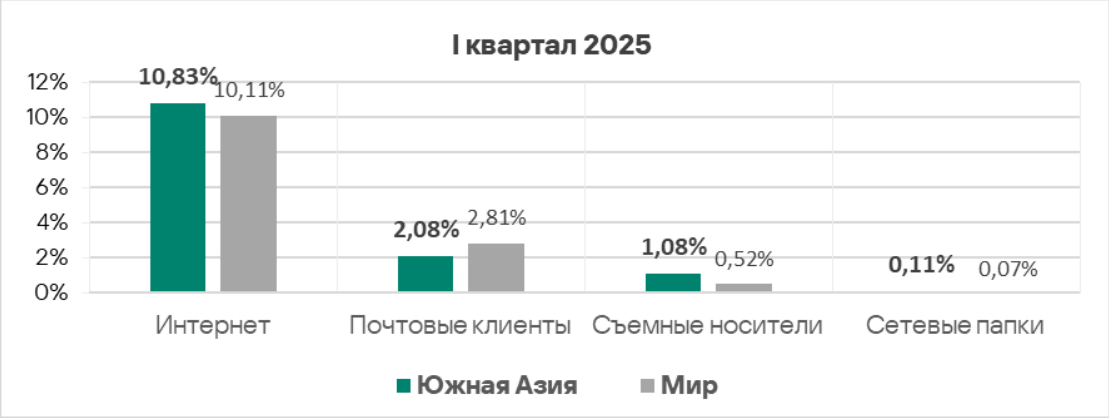
По сравнению со среднемировыми показателями в регионе заметно **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- Веб-майнеры — в 1,3 раза;
- Вирусы — в 1,2 раза;
- Вредоносные скрипты и фишинговые страницы — в 1,1 раза;
- Черви — в 1,1 раза.

Источники угроз

Южная Азия занимает **второе место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы угрозы **на съемных носителях,** с превышением среднемирового показателя в **2,1** раза. В прошлом квартале регион был на третьем месте в этом рейтинге.

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

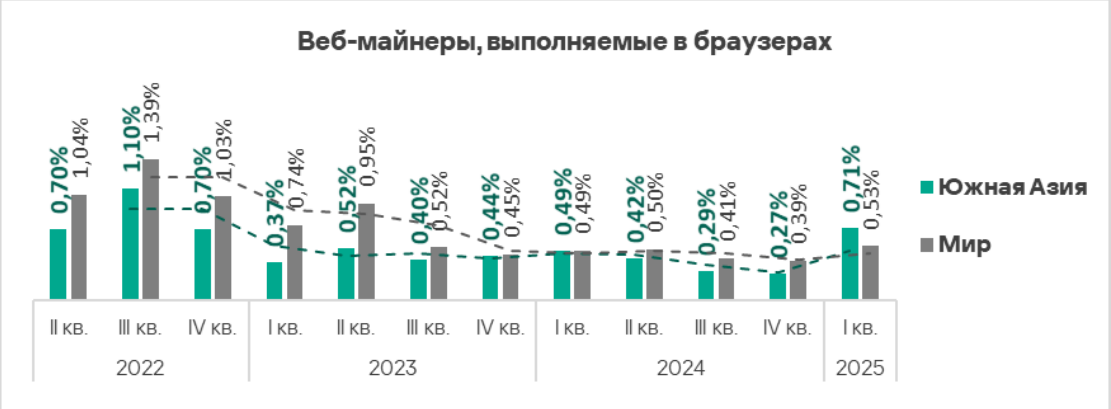


Изменения за квартал и тренды

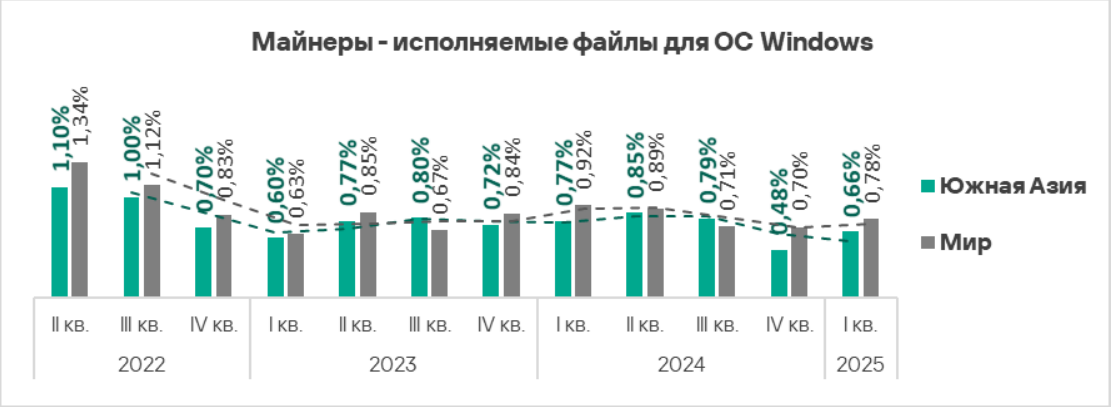
Категории угроз

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

- Веб-майнеры — в 2,6 раза, по росту показателя этой категории угроз регион занял второе место в мире;

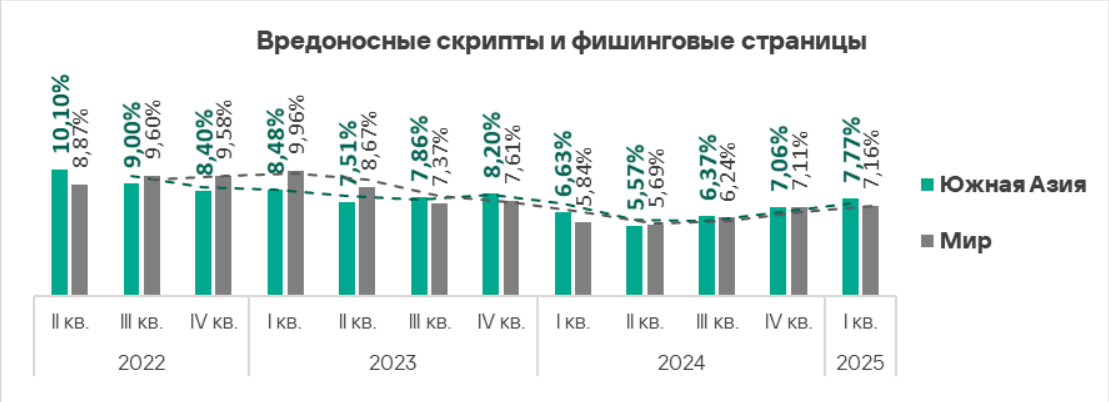


- Майнеры — исполняемые файлы для ОС Windows — в 1,4 раза;



- Вредоносные документы — в 1,2 раза;

- Вредоносные скрипты и фишинговые страницы — в 1,1 раз.



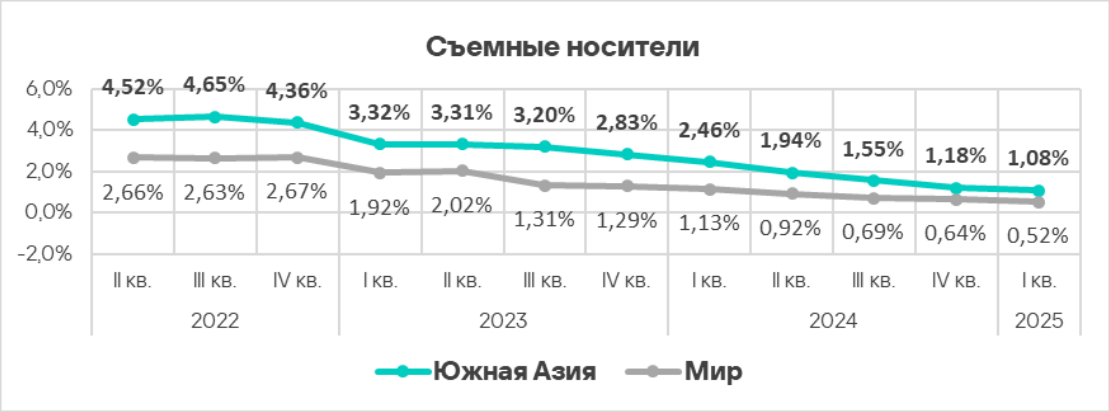
Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Азии со второго квартала 2022 года. В первом квартале 2025 года **веб-майнеры** поднялись с девятой на седьмую позицию в рейтинге.

Южная Азия	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	2	2	2	1	2	2	2	1	1
Ресурсы в интернете из списка запрещенных	2	2	2	1	1	1	2	1	1	1	2	2
Троянцы-шпионы, бэкдоры и кейлогтеры	3	3	3	3	3	3	3	3	3	3	3	3
Вирусы (Virus)	6	4	6	4	4	5	4	5	5	5	4	4
Черви (Worm)	5	5	4	5	5	4	5	4	4	4	5	5
Вредоносные документы (MSOffice+PDF)	4	5	5	6	6	6	6	6	6	6	6	6
Веб-майнеры, выполняемые в браузерах	8	7	7	9	8	8	8	8	8	8	9	7
Майнеры – исполняемые файлы для ОС Windows	7	8	7	7	7	7	7	7	7	7	7	8
Вредоносные программы для	9	9	9	8	9	10	10	9	9	9	8	9
Программы-вымогатели	9	10	9	10	10	9	9	10	10	10	10	10

Источники угроз

Из источников угроз в первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного **увеличилась** у **интернета** и в **1,2 раза — у почтовых клиентов**.

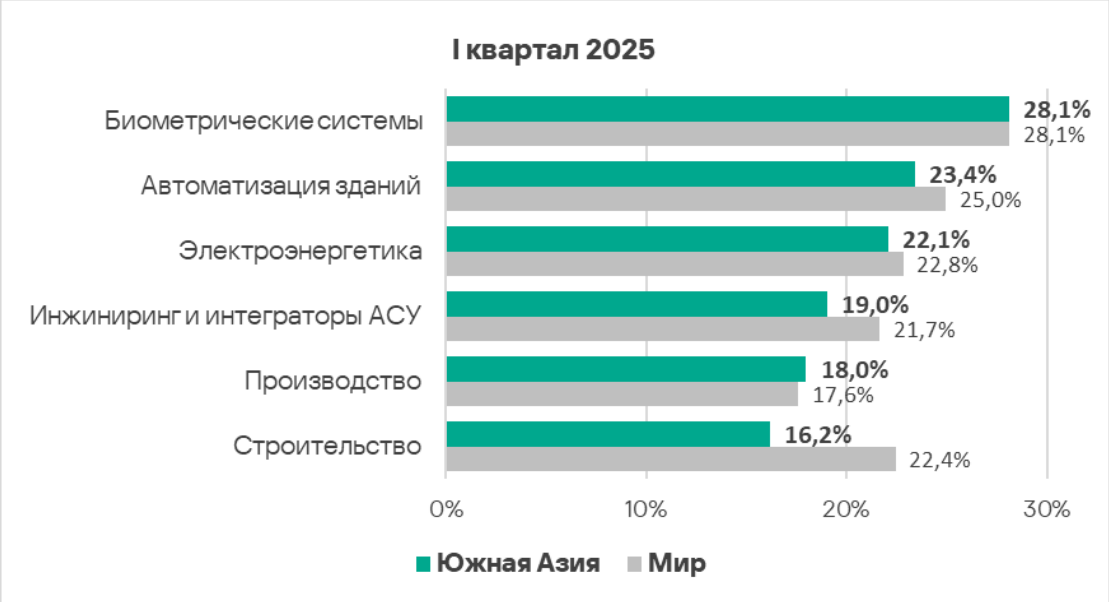
Уровень угроз на **съемных носителях** продолжает демонстрировать **нисходящий тренд,** однако все еще остается выше соответствующего среднемирового значения.



Отрасли

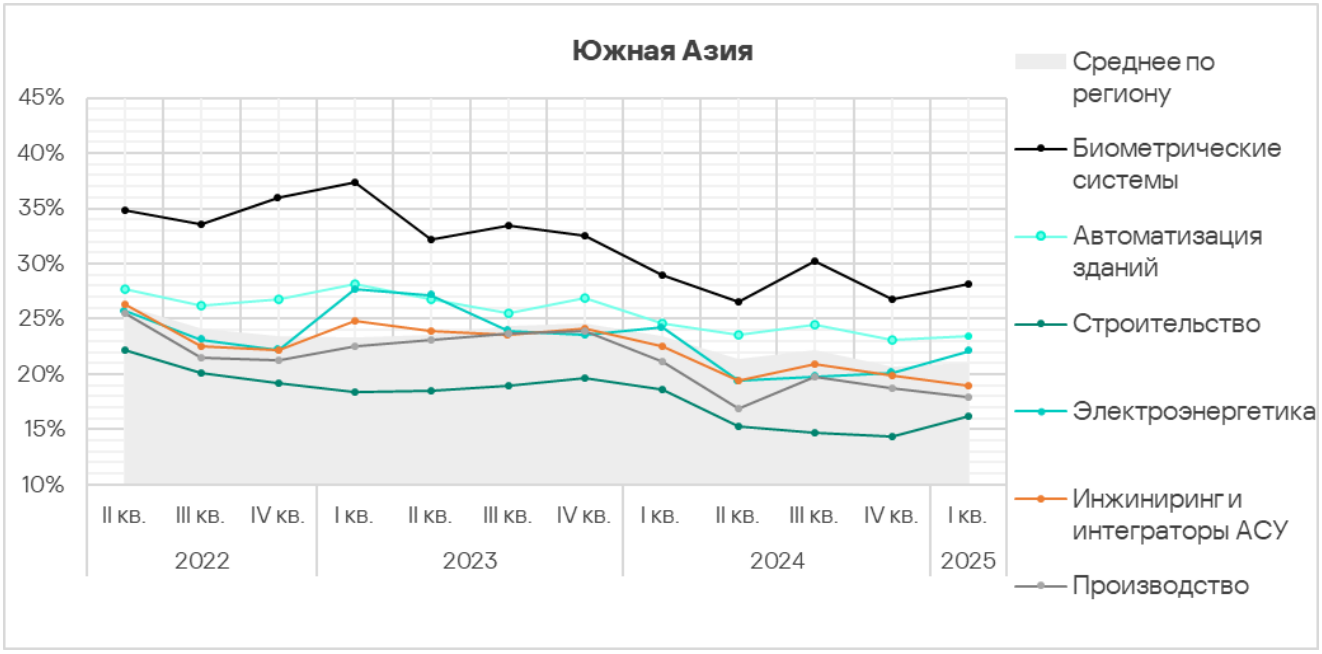
Биометрические системы по-прежнему **лидируют** среди исследуемых отраслей и OT-инфраструктур.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, во всех рассматриваемых областях, кроме производства, **ниже среднемирового значения.**



В первом квартале 2025 года во всех рассмотренных отраслях региона, кроме отраслей инжиниринг и интеграторы АСУ, а также производство, зафиксировано **увеличение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.

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



Восточная Азия

Актуальные угрозы

1-е место в регионе **4,81%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г. 1,1x выше среднего по миру	2-е место в регионе **4,34%** **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▼ снижение в I кв. 2025 г.	3-е место в регионе **3,14%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.
2,85% **ВИРУСЫ** ▼ снижение в I кв. 2025 г. 3-е место в мире 1,9x выше среднего по миру	**1,19%** **ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD** ▼ снижение в I кв. 2025 г. 2-е место в мире 3,5x выше среднего по миру	**0,32%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 1,4x рост в I кв. 2025 г. 1-е место по росту 1-е место в мире 2x выше среднего по миру
0,18% **ВЕБ-МАЙНЕРЫ** ▲ 1,4x рост в I кв. 2025 г.		
1,55% **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г.	**1,01%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г. 3-е место в мире 1,9x выше среднего по миру	**0,27%** **СЕТЕВЫЕ ПАПКИ** КАК ИСТОЧНИК УГРОЗ 1-е место в мире 3,9x выше среднего по миру

- Восточная Азия — единственный регион, где **шпионские программы занимают первое место в рейтинге категорий** вредоносного ПО по доле компьютеров АСУ, на которых они были заблокированы.

> 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).

Шпионское ПО применяется для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

Шпионские программы используются в том числе для установки на зараженные компьютеры **программ-вымогателей**.

- Восточная Азия **лидирует среди регионов** по доле компьютеров АСУ, на которых были заблокированы **программы-вымогатели** со значением, которое **вдвое превышает среднемировое**. В первом квартале 2025 года регион лидирует и **по росту** этого показателя.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, I квартал 2025 года

- По доле компьютеров АСУ, на которых угрозы были заблокированы при подключении **съемных носителей**, регион занимает **третье место в мире**. Для сравнения: по угрозам из интернета Восточная Азия находится на 11-м

месте, по угрозам из почтовых клиентов — на 10-м месте в соответствующих рейтингах регионов.

- Еще по одному источнику угроз — **сетевые папки** — Восточная Азия **лидирует.**

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, I квартал 2025 года

- Через сетевые папки, как правило, распространяются **вирусы** и **вредоносное ПО для AutoCAD**. Показатели обеих категорий заметно **превышают среднемировые — в 1,9 и 3,5 раза** соответственно.

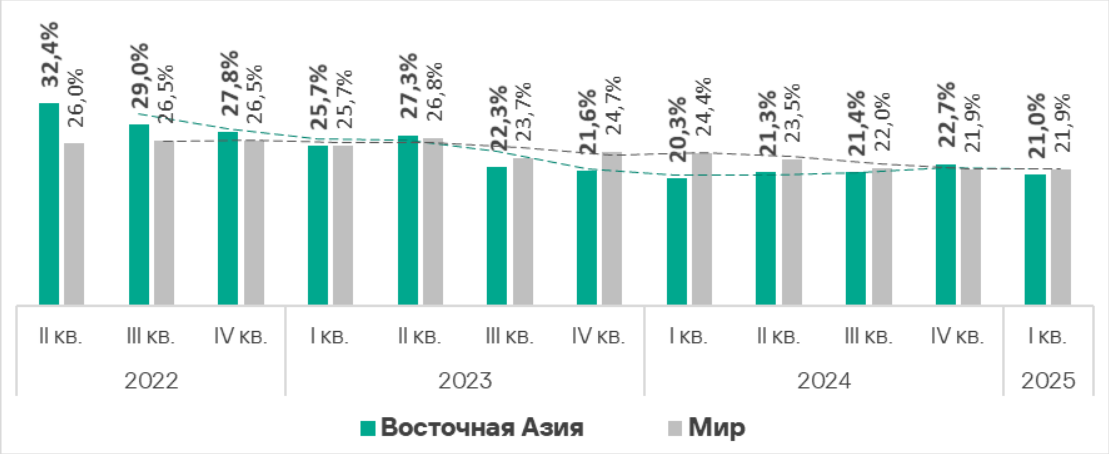
  В рейтинге регионов по доле компьютеров АСУ, на которых блокируются **вирусы**, Восточная Азия занимает **третье место**, по показателю **вредоносного ПО для AutoCAD — второе**.

Общая ситуация

Восточная Азия занимает **седьмое место** в мировом рейтинге по доле компьютеров АСУ, на которых заблокированы вредоносные объекты.

В регионе наблюдается **нисходящий** колебательный **тренд.**

В первом квартале 2025 года в Восточной Азии после заметного роста в предыдущем квартале доля компьютеров АСУ, на которых были заблокированы вредоносные объекты уменьшилась до **21,0%.**



Сравнительный анализ

Категории угроз

Восточная Азия — единственный регион, где шпионские программы занимают первое место в рейтинге категорий угроз.

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

- Вредоносное ПО для AutoCAD — в 3,5 раза;
- Программы-вымогатели — в 2 раза;
- Вирусы — в 1,9 раза;
- Черви — в 1,1 раза;
- Шпионские программы — в 1,1 раза.

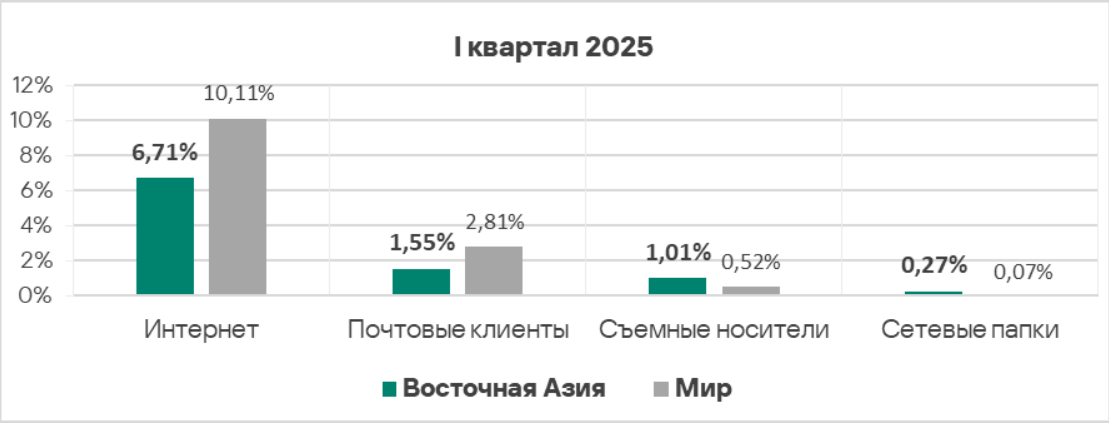
Среди регионов в первом квартале 2025 года Восточная Азия занимает:

- **Первое место** по доле компьютеров АСУ, на которых были заблокированы **программы-вымогатели**;
- **Второе место** по доле компьютеров АСУ, на которых были заблокированы вредоносные **программы для AutoCAD**;
- **Третье место** по доле компьютеров АСУ, на которых были заблокированы **вирусы.**

Источники угроз

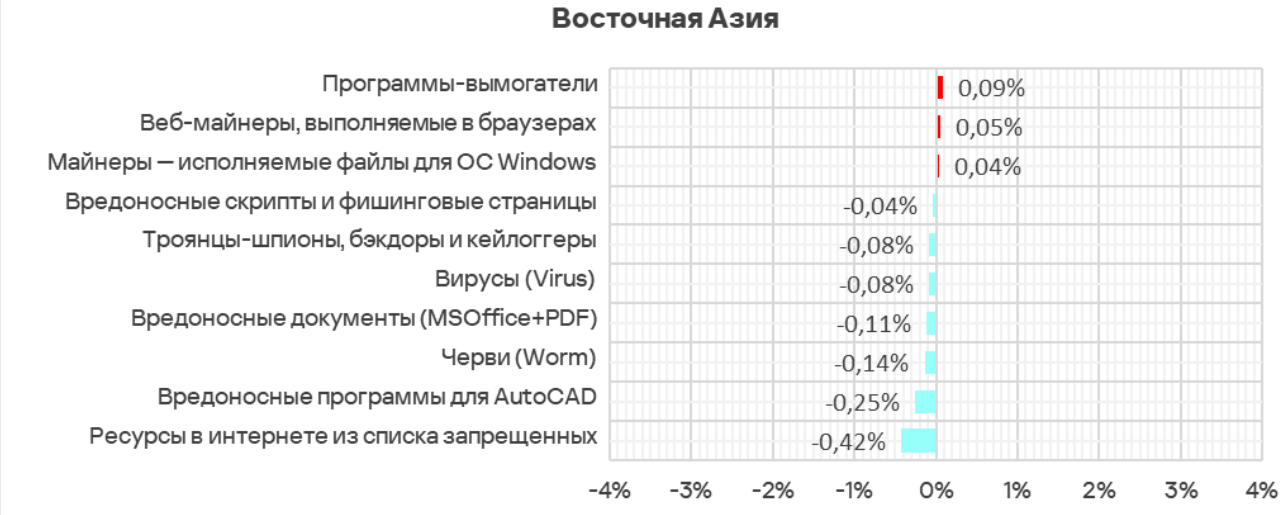
Восточная Азия по-прежнему занимает **первое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в **сетевых папках.** В первом квартале 2025 года показатель **региона превышает среднемировой в 3,9 раза**.

Доля компьютеров АСУ, на которых были заблокированы угрозы на **съемных носителях,** в регионе **в 1,9 раз выше, чем в среднем по миру.** По этому показателю регион — **на третьем месте** в мире.



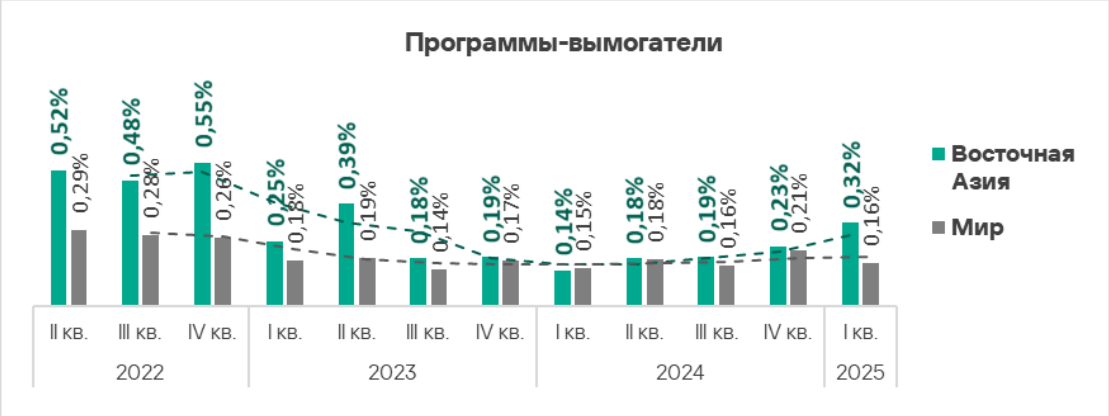
Изменения за квартал и тренды

Категории угроз

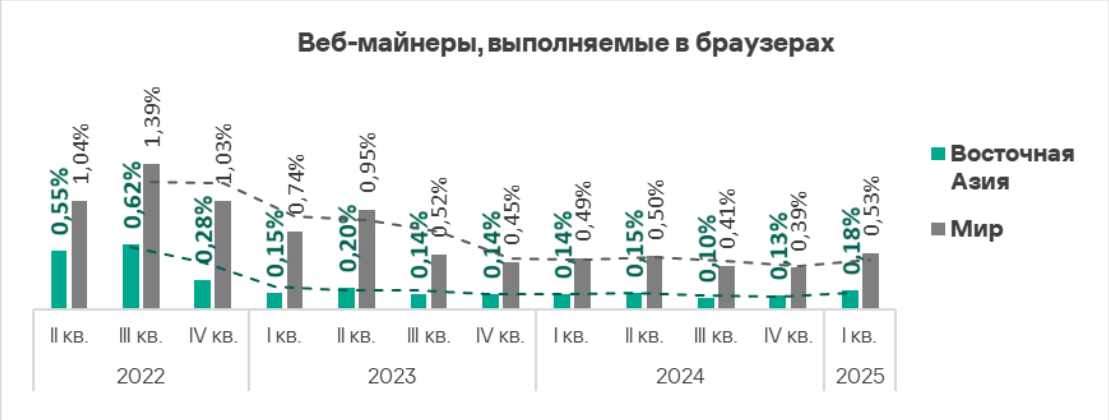


Наибольший рост за квартал зафиксирован у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

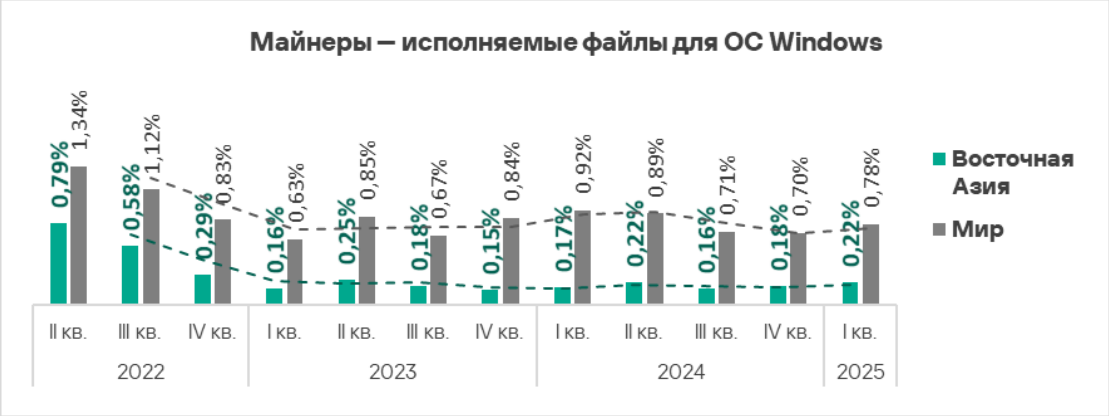
- Программы-вымогатели — в 1,4 раза, **первое место** среди регионов **по росту** показателя;



- Веб-майнеры — в 1,4 раза;



- Майнеры — исполняемые файлы для ОС Windows — в 1,2 раза.

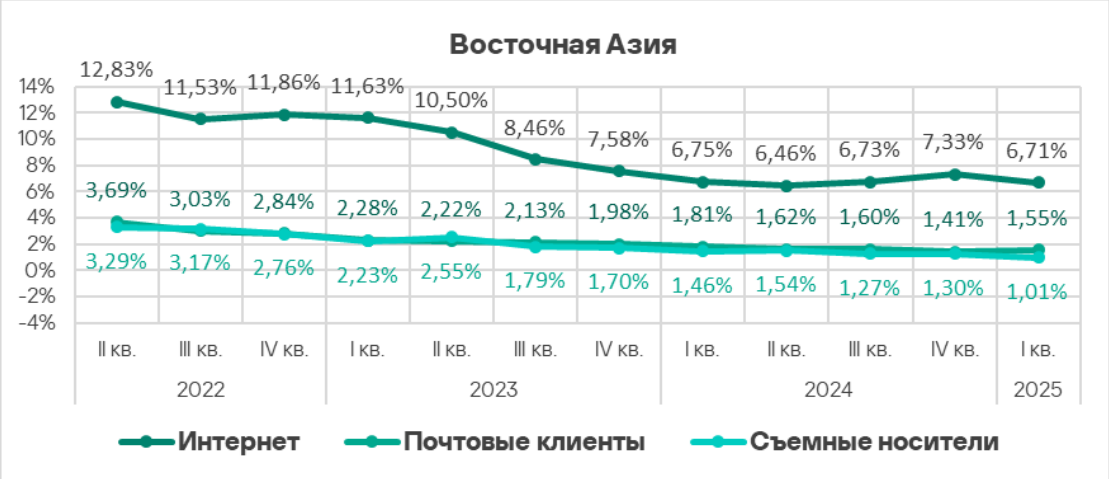


Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Восточной Азии со второго квартала 2022 года. В первом квартале 2025 все категории угроз остались на прежних позициях.

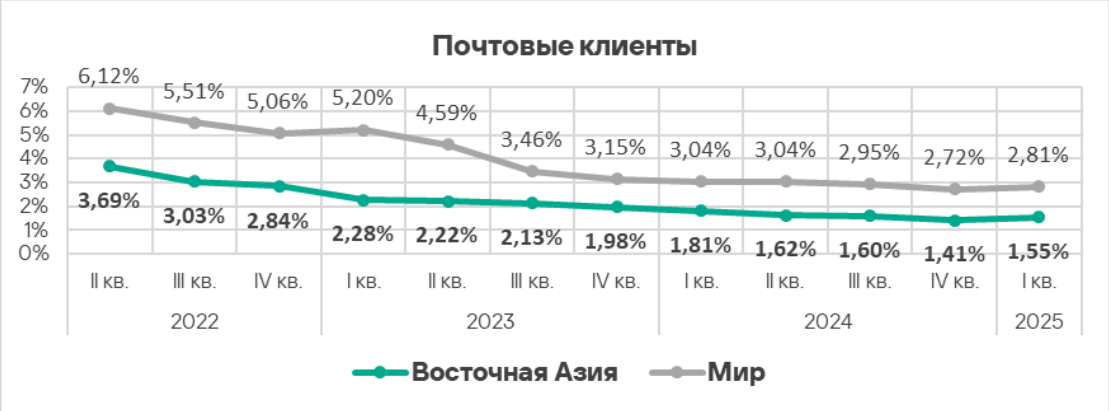
Восточная Азия	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	3	3	3	3	1	1	1	1	1	1
Вредоносные скрипты и фишинговые страницы	2	1	1	1	1	1	2	3	2	2	2	2
Ресурсы в интернете из списка запрещенных	1	2	2	2	2	1	3	2	3	3	3	3
Вирусы (Virus)	4	4	4	4	4	4	4	4	4	4	4	4
Вредоносные документы (MSC	5	5	5	6	5	7	7	7	6	5	5	5
Черви (Worm)	6	6	7	5	6	5	5	5	5	6	6	6
Вредоносные программы для AutoCAD	7	7	6	7	7	6	6	6	7	7	7	7
Программы-вымогатели	10	10	8	8	8	9	8	10	9	8	8	8
Майнеры – исполняемые файл	8	9	9	9	9	8	9	8	8	9	9	9
Веб-майнеры, выполняемые в браузерах	9	8	10	10	10	10	10	9	10	10	10	10

Источники угроз

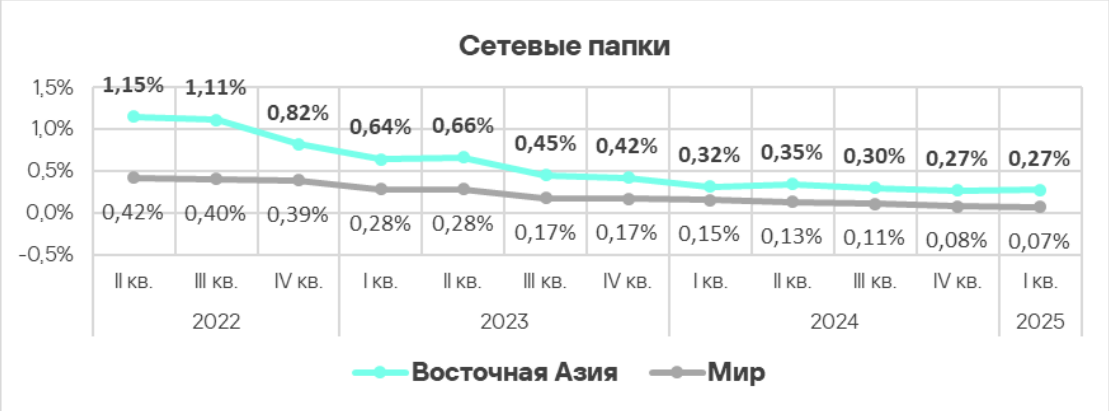
В целом, все основные источники угроз в рамках долгосрочных **трендов** демонстрируют **тенденцию к снижению.**



При этом уровень угроз из **почтовых клиентов** в Восточной Азии в первом квартале 2025 года **вырос** в 1,1 раза.



Доля компьютеров АСУ, на которых угрозы были заблокированы в **сетевых папках,** в Восточной Азии демонстрирует **нисходящий тренд**. Однако показатель остается значительно **выше среднемирового** и самым высоким среди регионов.

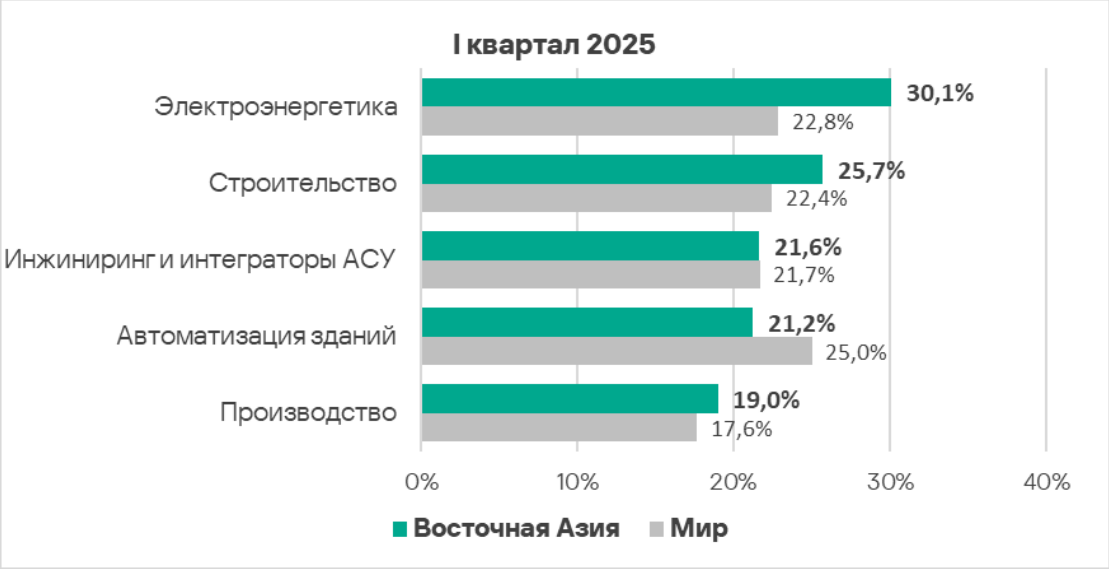


Отрасли

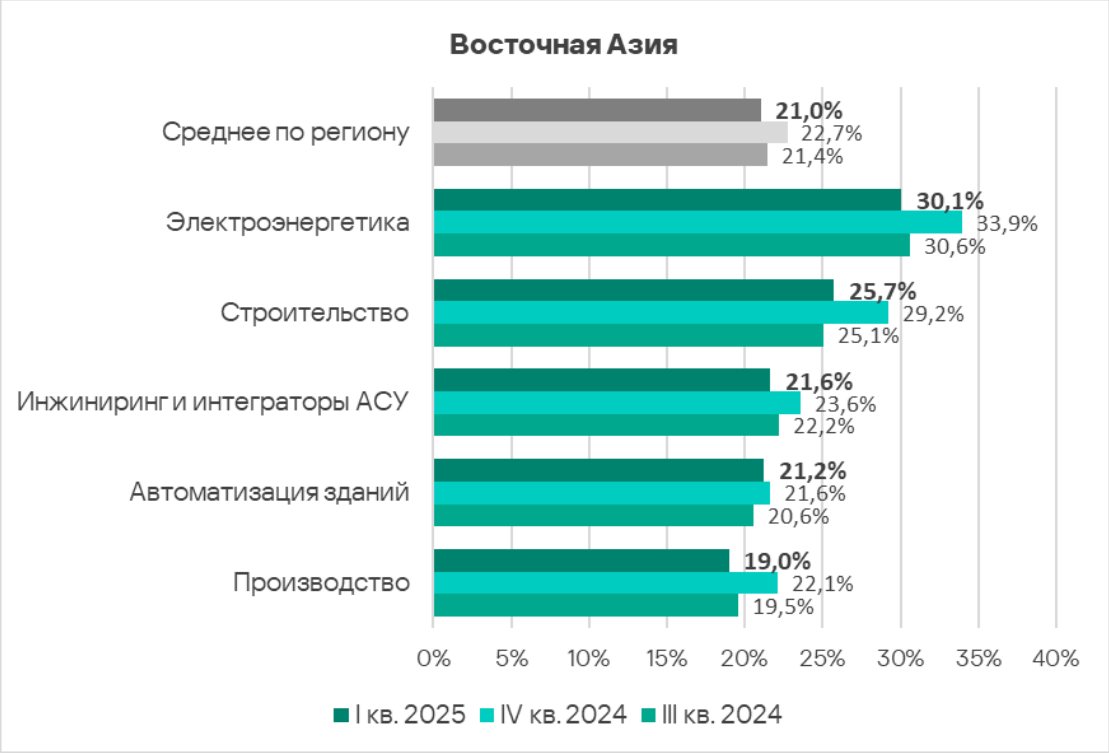
Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является **электроэнергетика.**

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

- Электроэнергетика — в 1,3 раза;
- Строительство — в 1,1;
- Производство — в 1,1 раза.

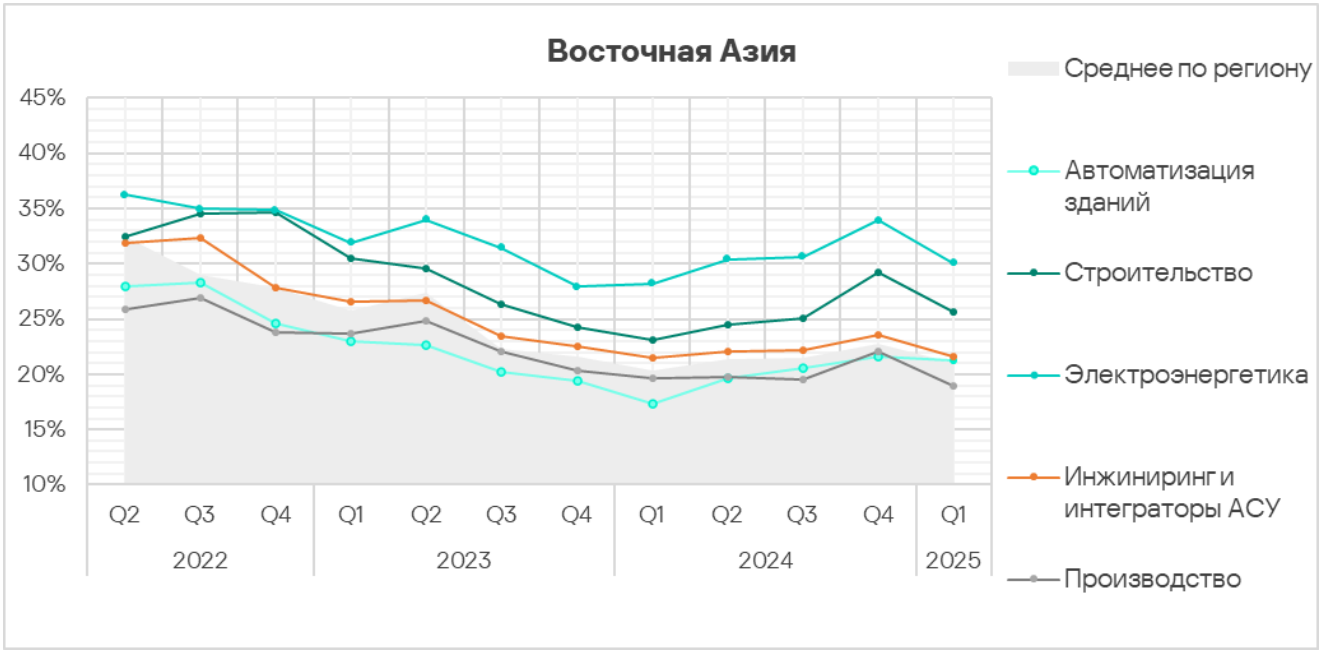


В первом квартале 2025 года во всех отраслях зафиксировано **уменьшение** доли компьютеров АСУ, на которых были заблокированы вредоносные объекты.



Восточная Азия — крупнейший мировой потребитель электроэнергии. Потребление и, соответственно, генерация в регионе почти непрерывно растет. Соответственно, неудивительны высокие значения показателя доступности OT-систем сектора для киберугроз. Как мы писали выше, при вводе в эксплуатацию новых объектов адекватные меры киберзащиты обычно применяются с заметным запозданием.

Самая высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, сохраняется в **электроэнергетике** на протяжении всего рассматриваемого периода. При этом ее значение **значительно превышает не только среднее по региону, но и среднемировое.**



Латинская Америка

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
9,33% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▼ снижение в I кв. 2025 г. 1,3x выше среднего по миру	**4,33%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г.	**4,19%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.
3,30% **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▼ снижение в I кв. 2025 г. 2-е место в мире 1,8x выше среднего по миру	**0,71%** **ВЕБ-МАЙНЕРЫ** ▲ 1,7x рост в I кв. 2025 г. 1,3x выше среднего по миру	
9,99% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.	**4,55%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ слабый рост в I кв. 2025 г. 3-е место в мире 1,6x выше среднего по миру	

- Латинская Америка занимает **второе место среди регионов** по доле компьютеров АСУ, на которых блокируются **вредоносные документы,** с показателем, который превышает среднемировой **в 1,8 раза**.

> Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

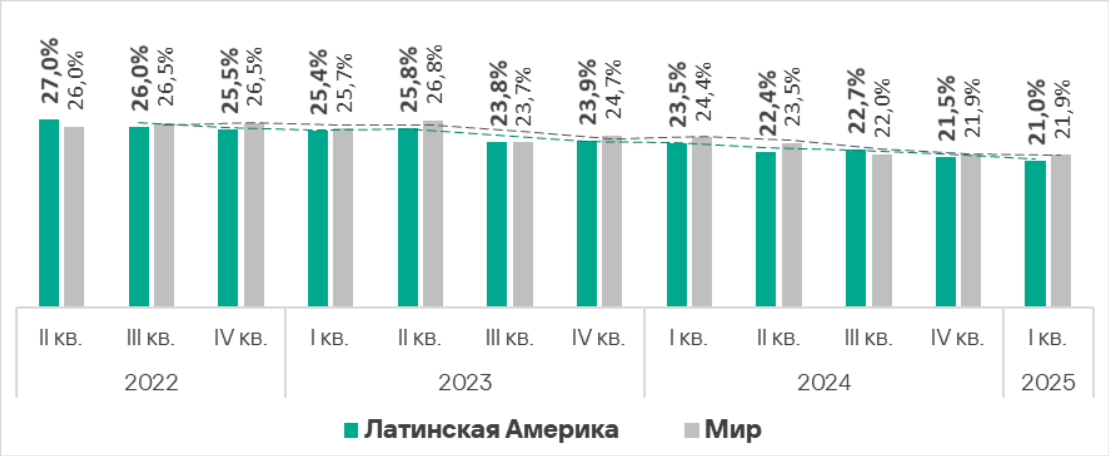
- Источником угрозы служат в основном почтовые клиенты. Доля компьютеров АСУ, на которых были заблокированы **угрозы из почтовых клиентов**, в регионе **в 1,6 раза выше, чем в среднем по миру**. По этому показателю Латинская Америка занимает **третье место** среди регионов.

Общая ситуация

Латинская Америка занимает **восьмое место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

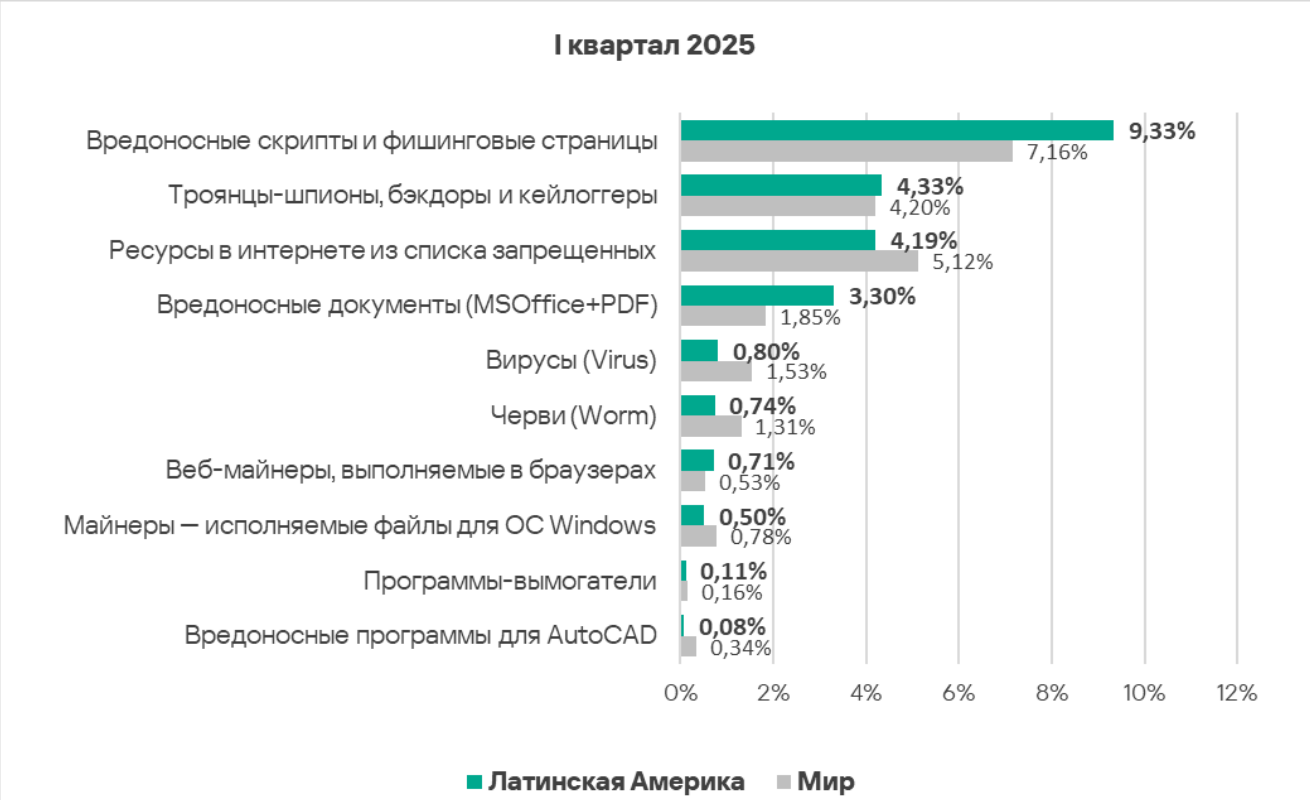
В **первом квартале 2025 года** показатель **уменьшился** до **21,0%** — это ниже среднемирового значения.

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 1,8 раза;
- Вредоносные скрипты и фишинговые страницы — в 1,3 раза;
- Веб-майнеры — в 1,3 раза.

Среди регионов Латинская Америка занимает **второе место** по доле компьютеров АСУ, на которых блокируются **вредоносные документы**.

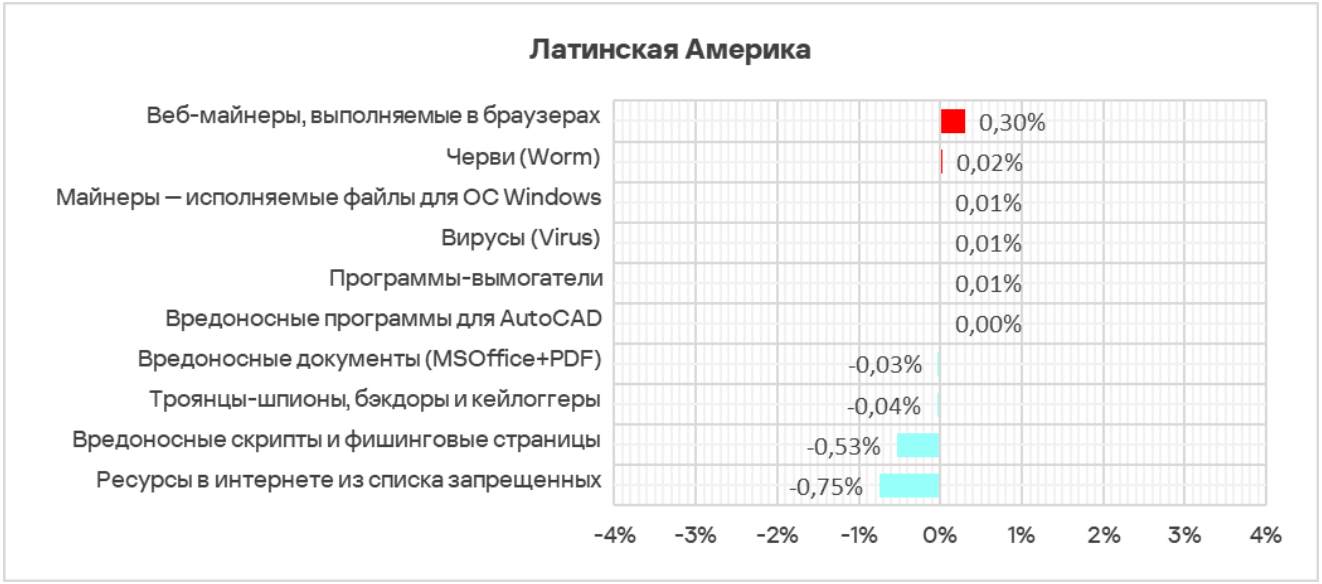
Источники угроз

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

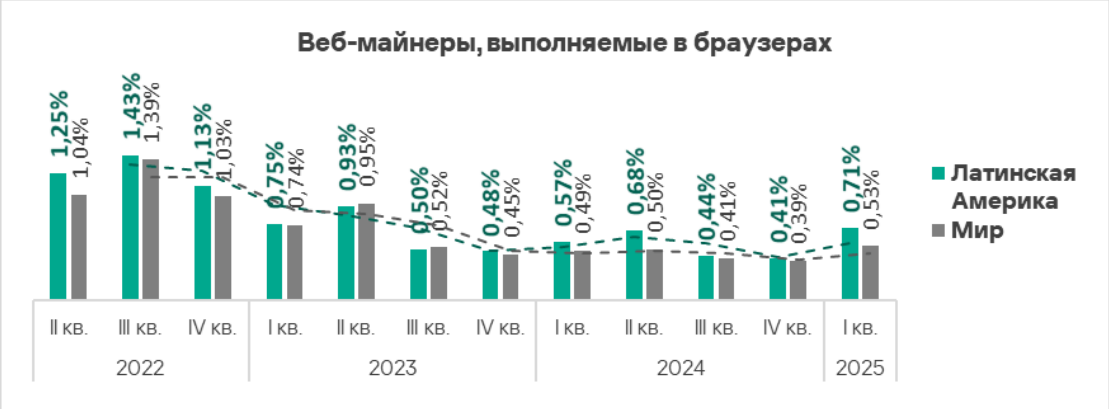
Совместно с высокими показателями для скриптов и фишинговых страниц (см. выше) это говорит о высокой доступности систем, относящихся к OT-инфраструктуре, для целевых атак.

Изменения за квартал и тренды

Категории угроз



Наибольший прирост в процентах за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы веб-майнеры, — в 1,7 раза.



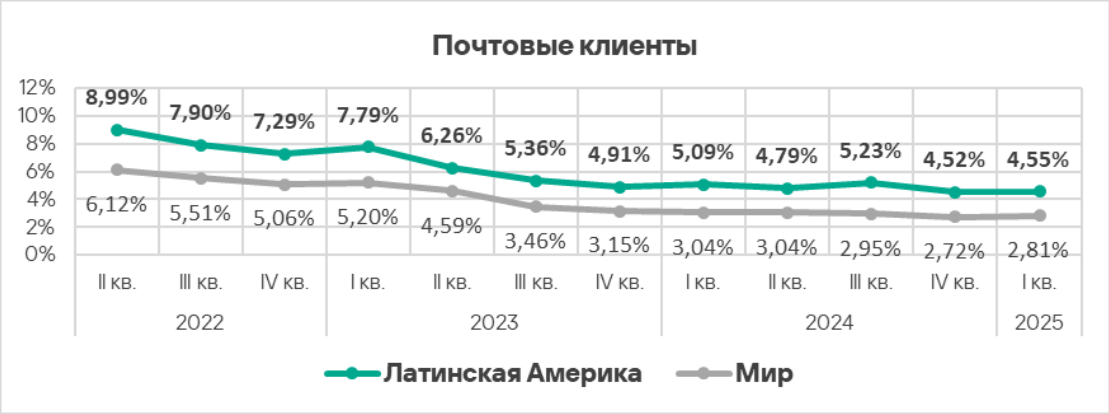
Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Латинской Америке со второго квартала 2022 года. На протяжении всего этого времени **вредоносные скрипты и фишинговые страницы** остаются ведущей категорией угроз в регионе. В первом квартале 2025 года **шпионские программы** и **веб-майнеры** переместились на одну позицию вверх.

Латинская Америка	2022 Q2	Q3	Q4	2023 Q1	Q2	Q3	Q4	2024 Q1	Q2	Q3	Q4	2025 Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	1	1	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	4	3	4	4	4	4	3	3	3	3	3	2
Ресурсы в интернете из списка запрещенных	2	2	2	2	2	2	2	2	2	2	2	3
Вредоносные документы (MSOffice+PDF)	3	4	3	3	3	3	4	4	4	4	4	4
Вирусы (Virus)	8	8	7	6	6	6	6	5	6	5	5	5
Черви (Worm)	6	6	6	5	5	5	5	6	5	6	6	6
Веб-майнеры, выполняемые в браузерах	7	5	5	7	7	7	8	8	8	8	8	7
Майнеры – исполняемые файлы для ОС Windows	5	7	8	8	8	8	7	7	7	7	7	8
Программы-вымогатели	9	9	9	9	9	9	9	9	9	10	9	9
Вредоносные программы для AutoCAD	10	10	10	10	10	10	10	10	10	9	10	10

Источники угроз

В первом квартале 2025 года из всех источников угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного увеличилась только у **почтовых клиентов**. Региональный показатель **превышает среднемировой в 1,6 раза.**

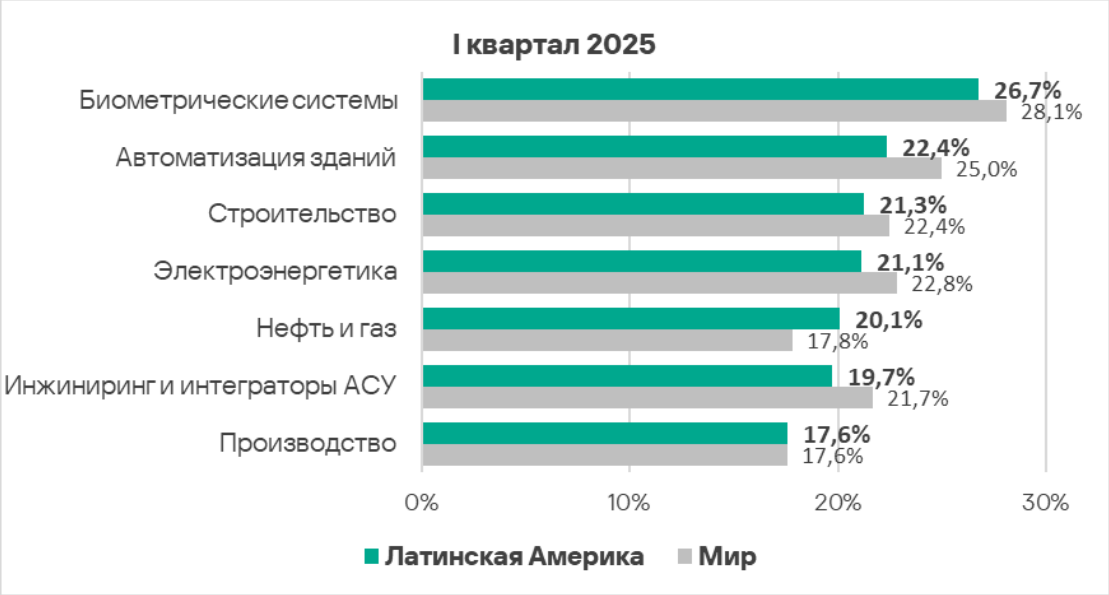
Уровень угроз из **почтовых клиентов** демонстрирует плавно **нисходящий тренд,** что соответствует общемировому тренду, однако региональный показатель значительно превышает среднемировой.



Отрасли

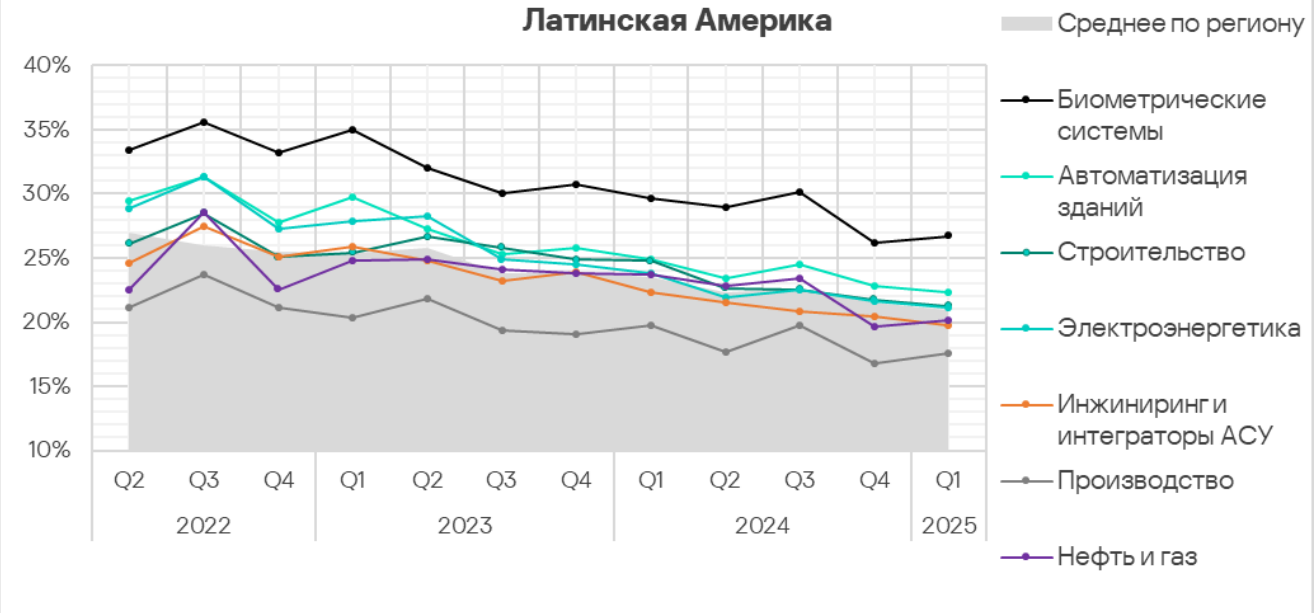
В регионе из всех рассмотренных в отчете отраслей **чаще всего** вредоносные объекты блокируются в OT-инфраструктуре **биометрические системы.**

Единственная отрасль, где доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **превышает** (в 1,1 раза) **среднемировое значение** — **нефтегазовая**.



В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного **увеличилась в ОТ-инфраструктуре биометрические системы, нефтегазовой отрасли и производстве**.

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



Южная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
10,31% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ слабый рост в I кв. 2025 г. 1-е место в мире 1,4x выше среднего по миру	**6,52%** **ШПИОНСКИЕ ПРОГРАММЫ** ▲ слабый рост в I кв. 2025 г. 1-е место по росту 2-е место в мире 1,6x выше среднего по миру	**4,02%** **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,1x рост в I кв. 2025 г. 2-е место по росту 1-е место в мире 2,2x выше среднего по миру
0,95% **ЧЕРВИ** ▲ 1,2x рост в I кв. 2025 г. 1-е место по росту	**0,41%** **ВЕБ-МАЙНЕРЫ** ▲ 1,4x рост в I кв. 2025 г.	**0,38%** **ВИРУСЫ** ▲ 1,3x рост в I кв. 2025 г. 3-е место по росту
0,31% **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,2x рост в I кв. 2025 г.	**0,24%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 1,4x рост в I кв. 2025 г. 2-е место по росту 1,5x выше среднего по миру	**0,08%** **ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD** ▲ 1,3x рост в I кв. 2025 г. 1-е место по росту
9,24% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.	**6,76%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ слабый рост в I кв. 2025 г. 1-е место в мире 2,4x выше среднего по миру	**0,17%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.

Несмотря на то, что Южная Европа занимает **девятое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, по некоторым позициям ситуация в регионе не кажется благополучной.

- Южная Европа находится **на первом месте в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов.** Значение показателя **превышает среднемировое** в 2,4 раза.

  Электронная почта играет значительную роль в распространении угроз в регионе.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, I квартал 2025 года

- В первом квартале 2025 года Южная Европа занимает **первое место среди регионов** по доле компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы**. Этот показатель в регионе **превышает среднемировой в 1,4 раза**.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, I квартал 2025 года

Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

- Южная Европа занимает **первое место среди регионов** по доле компьютеров АСУ, на которых были заблокированы **вредоносные документы**, с показателем, который **превышает среднемировой в 2,2 раза**.

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, I квартал 2025 года

По совокупности этих факторов можно считать риск успешных целевых атак на системы, относящиеся к OT-инфраструктуре региона, одним из самых высоких в мире.

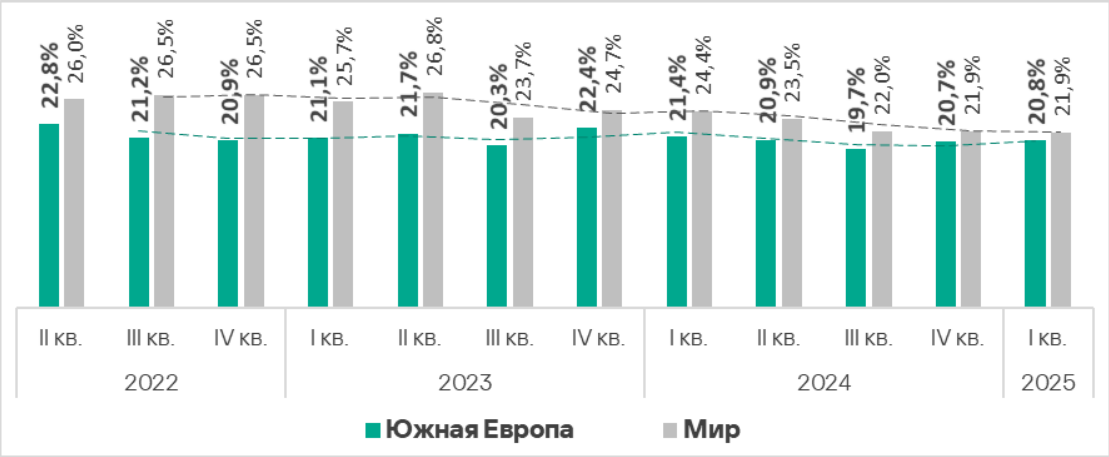
- **Второе место** у Южной Европы — по доле компьютеров АСУ, на которых были заблокированы **шпионские программы.** Показатель региона **превышает среднемировой в 1,6 раза.** В первом квартале 2025 года регион занял **первое место по росту** этого показателя.
- Еще один высокий показатель в регионе — доля компьютеров АСУ, на которых блокируются **программы-вымогатели**. Он **выше среднемирового в 1,5 раза**. Эта категория вредоносного ПО распространяется в том числе с использованием шпионских программ. В первом квартале 2025 года регион занял **второе место по росту** этого показателя.
- В первом квартале 2025 года Южная Европа занимает **первое место среди регионов по росту** доли компьютеров АСУ, на которых были заблокированы

черви и вредоносные программы для AutoCAD. **Третье место** — по **росту** показателей **вирусов**.

Общая ситуация

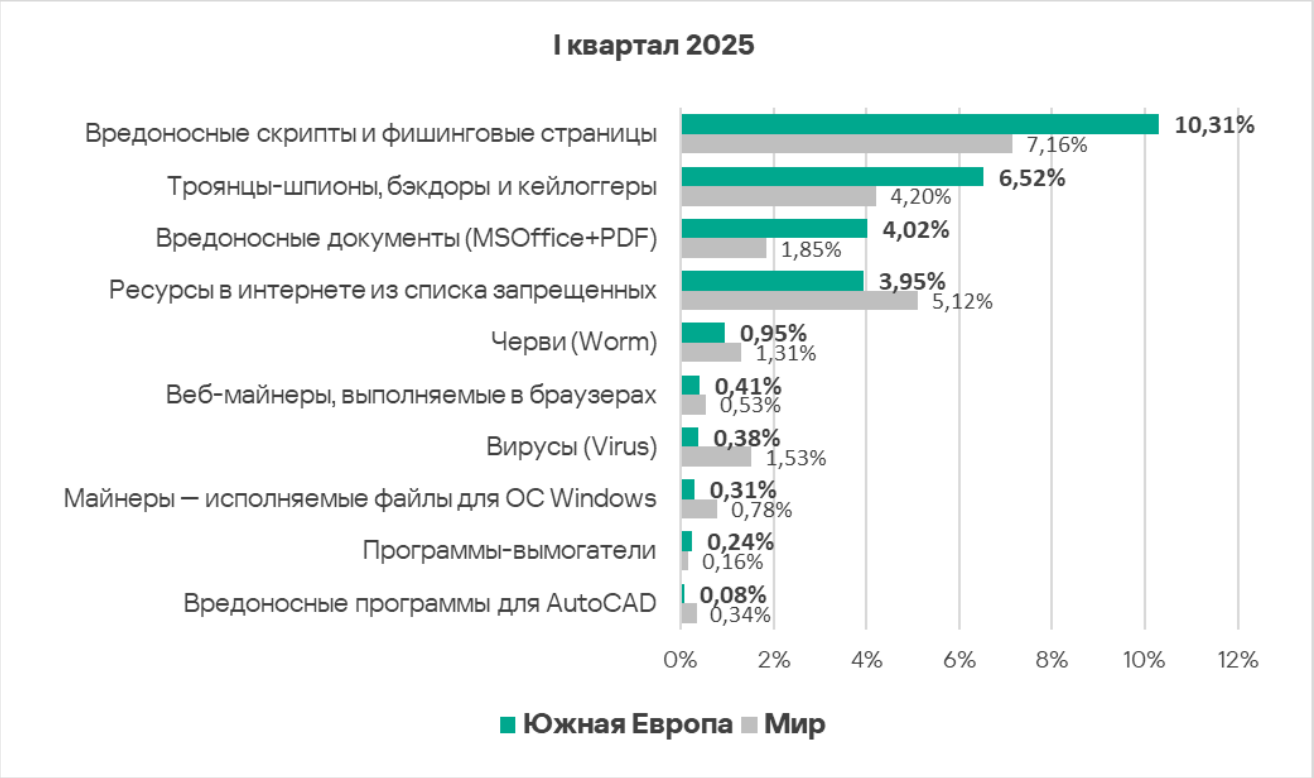
Южная Европа занимает **девятое место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Показатель региона — **20,8%** — **ниже среднемирового значения.**



Сравнительный анализ

Категории угроз

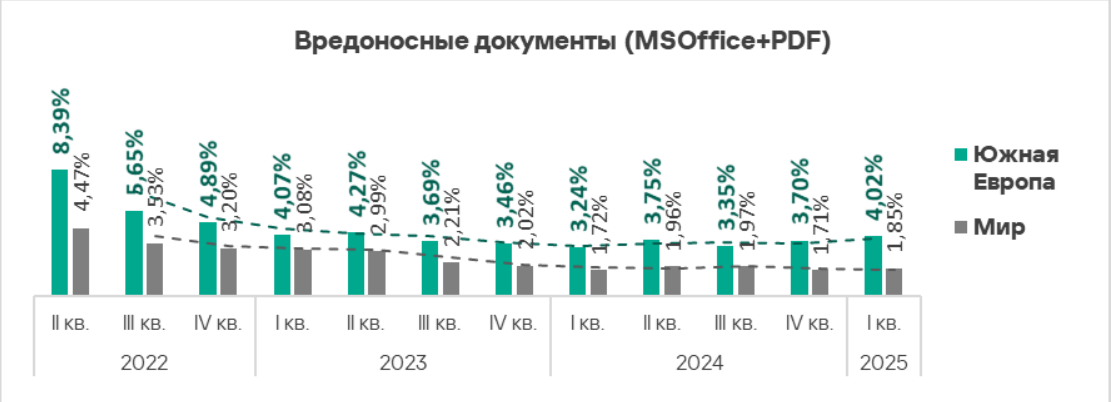


По сравнению со среднемировыми показателями в регионе **выше** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

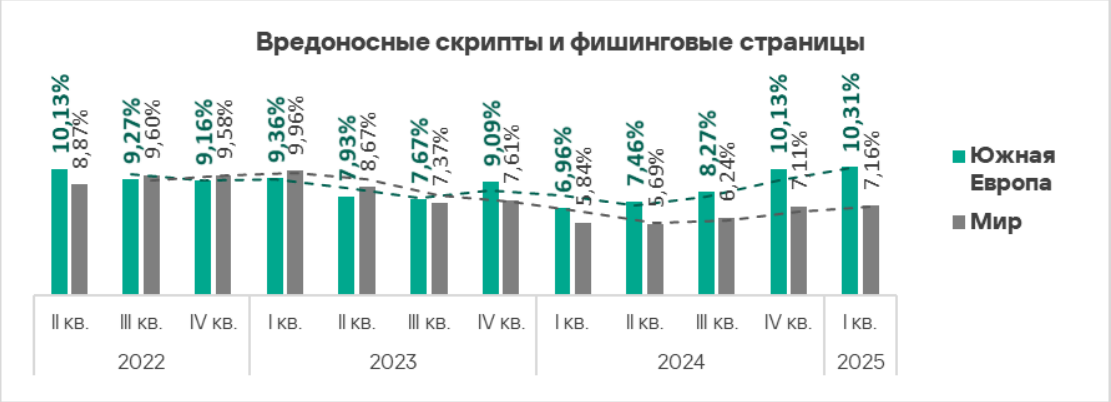
- Вредоносные документы — в 2,2 раза;
- Шпионские программы — в 1,6 раза;
- Программы-вымогатели — в 1,5 раза;
- Вредоносные скрипты и фишинговые страницы — в 1,4 раза.

Среди регионов в первом квартале 2025 года Южная Европа занимает **первое место** по доле компьютеров АСУ, на которых были заблокированы:

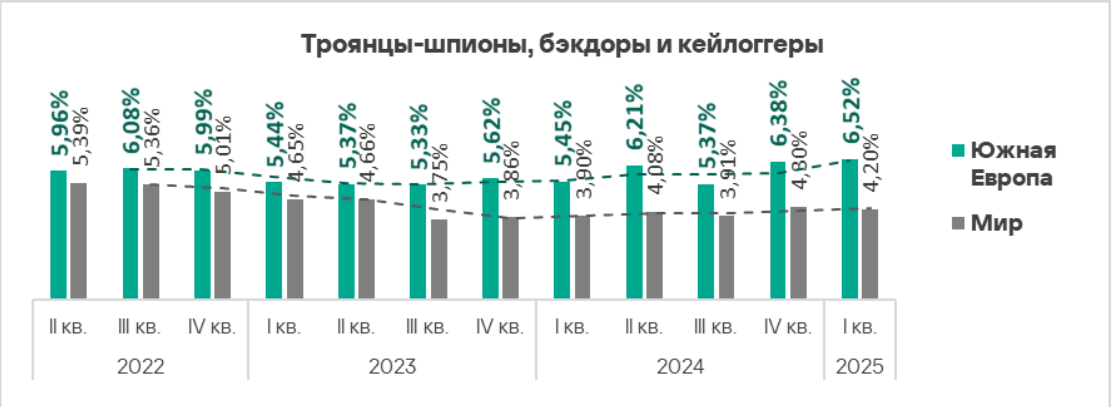
- Вредоносные документы;



- Вредоносные скрипты и фишинговые страницы.



Второе место у Южной Европы — по доле компьютеров АСУ, на которых были заблокированы **шпионские программы**.

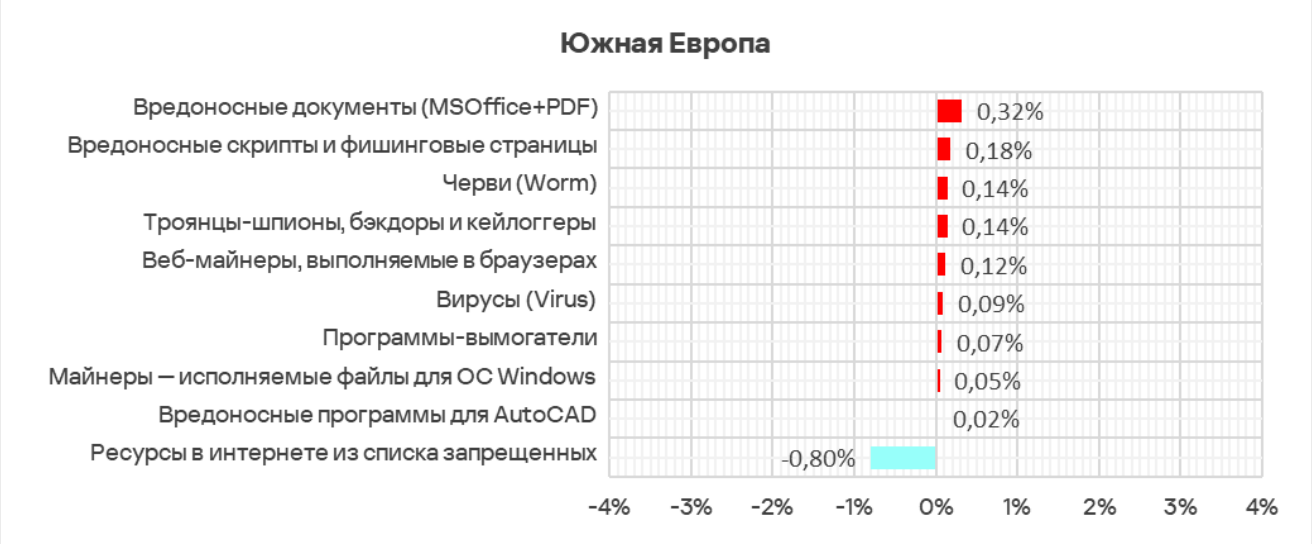


Источники угроз

Южная Европа находится **на первом месте в мире** по доле компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов.** Значение показателя **превышает среднемировое** в 2,4 раза.

Изменения за квартал и тренды

Категории угроз



В первом квартале 2025 года Южная Европа занимает **первое место среди регионов по росту** доли компьютеров АСУ, на которых были заблокированы

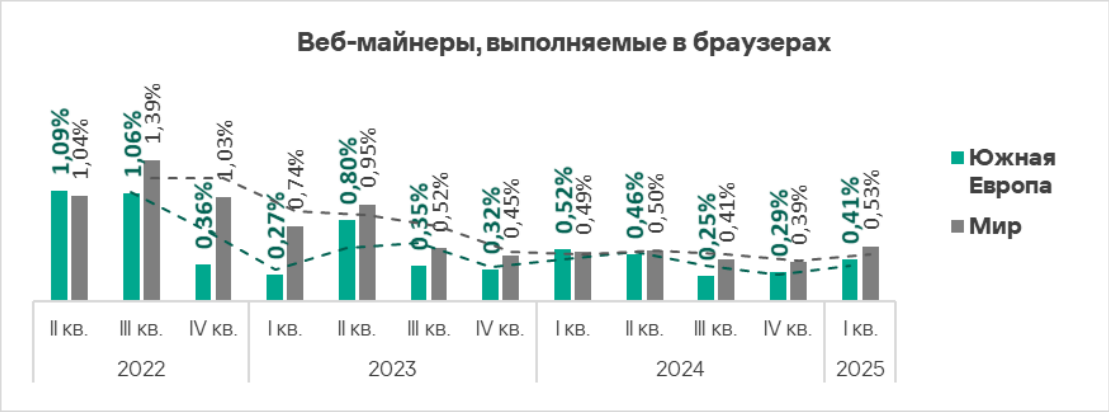
- Шпионские программы;
- Черви;
- Вредоносные программы для AutoCAD.

Регион **на втором месте** по росту доли компьютеров АСУ, на которых были заблокированы:

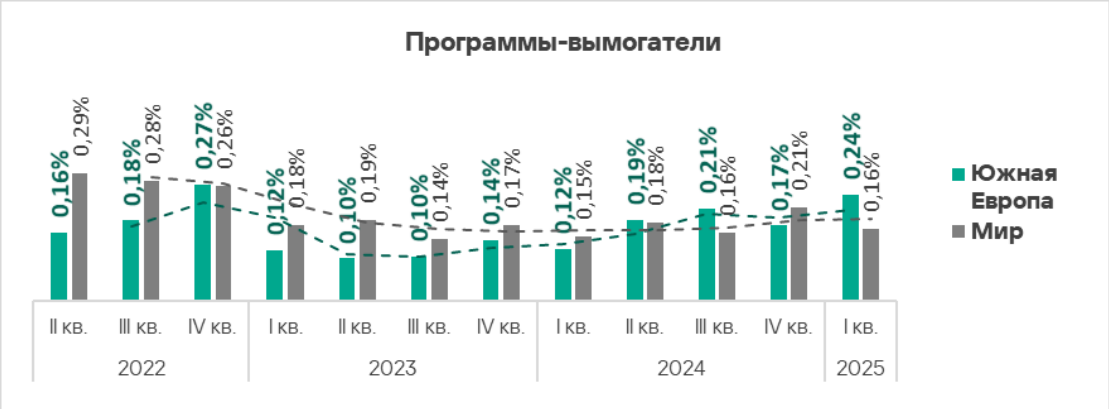
- Вредоносные документы;
- Программы-вымогатели.

В Южной Европе **больше всего за квартал выросла** доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

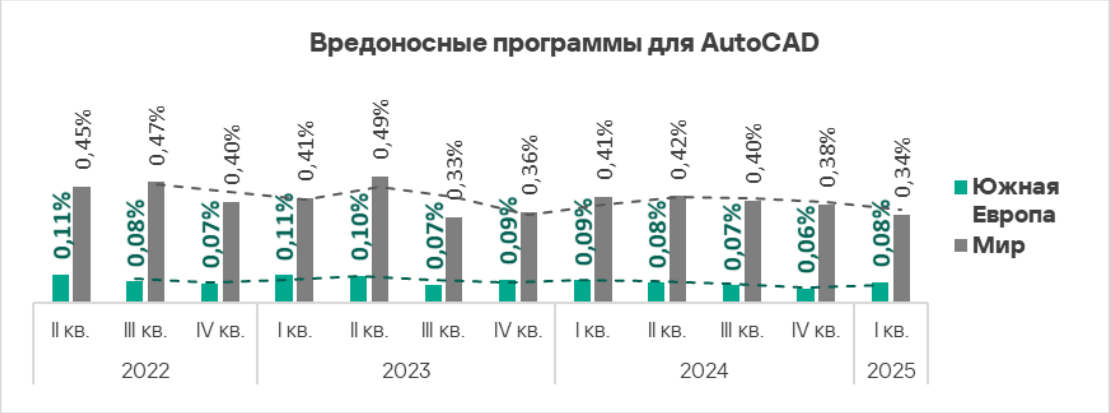
- Веб-майнеры — в 1,4 раза;



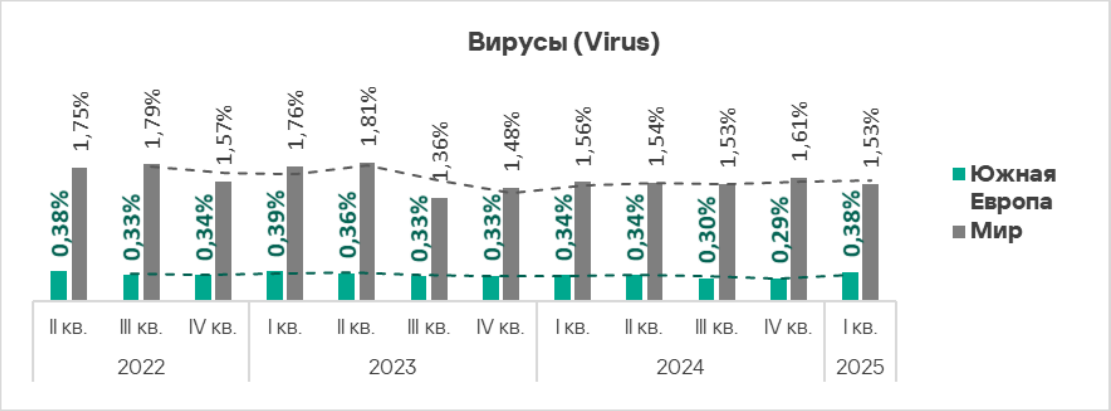
- Программы-вымогатели — в 1,4 раза;



- Вредоносные программы для AutoCAD — в 1,3 раза;



- Вирусы — в 1,3 раза;



Увеличилась также доля компьютеров АСУ, на которых были заблокированы:

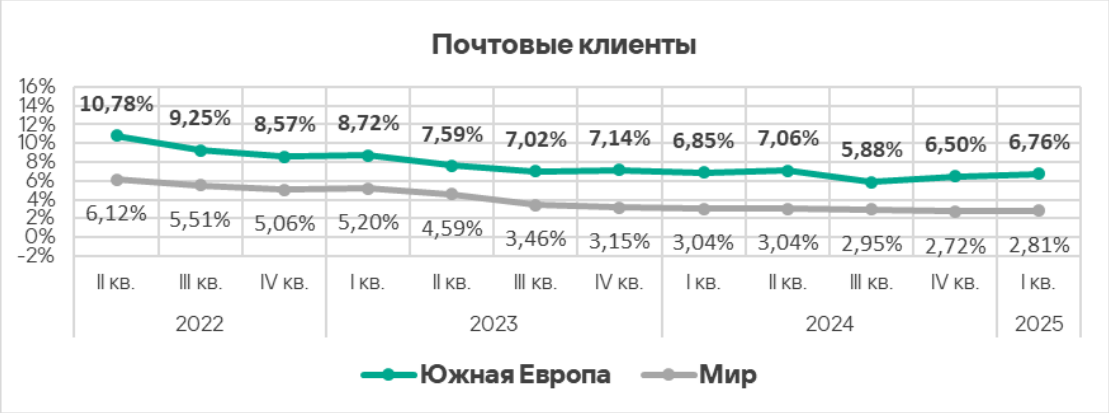
- Черви — в 1,2 раза;
- Майнеры — исполняемые файлы для ОС Windows — в 1,2 раза;
- Вредоносные документы — в 1,1 раза.

Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Южной Европе со второго квартала 2022 года. В первом квартале 2025 года **вредоносные документы поднялись** с четвертого на **третье** место, а **веб-майнеры** — с седьмого на **шестое**.

Южная Европа	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	1	1	1	1
Троянцы-шпионы, бэкдоры и кейлоггеры	3	2	2	3	3	2	3	3	2	3	2	2
Вредоносные документы (MSOffice+PDF)	2	3	3	4	4	4	4	4	4	4	4	3
Ресурсы в интернете из списка запрещенных	4	4	4	2	2	3	2	2	3	2	3	4
Черви (Worm)	7	6	5	5	5	5	5	5	5	5	5	5
Веб-майнеры, выполняемые в браузерах	6	5	6	7	6	7	8	7	7	7	7	6
Вирусы (Virus)	8	8	8	6	8	8	6	8	8	6	6	7
Майнеры – исполняемые файлы для ОС Windows	5	7	7	8	7	6	7	6	6	8	8	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

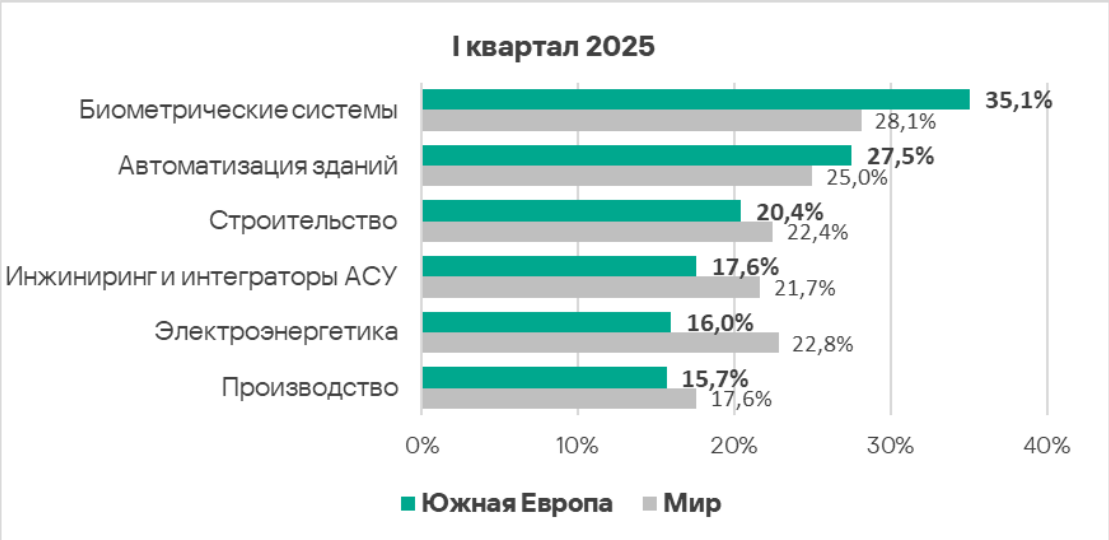
В первом квартале 2025 года в регионе из всех источников угроз **выросла** только доля компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов**. Региональный показатель значительно превышает среднемировой.



Отрасли

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

В **биометрических системах** и **автоматизации зданий** зафиксирована наиболее высокая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышающая **среднемировое значение** в 1,2 и 1,1 раза соответственно.

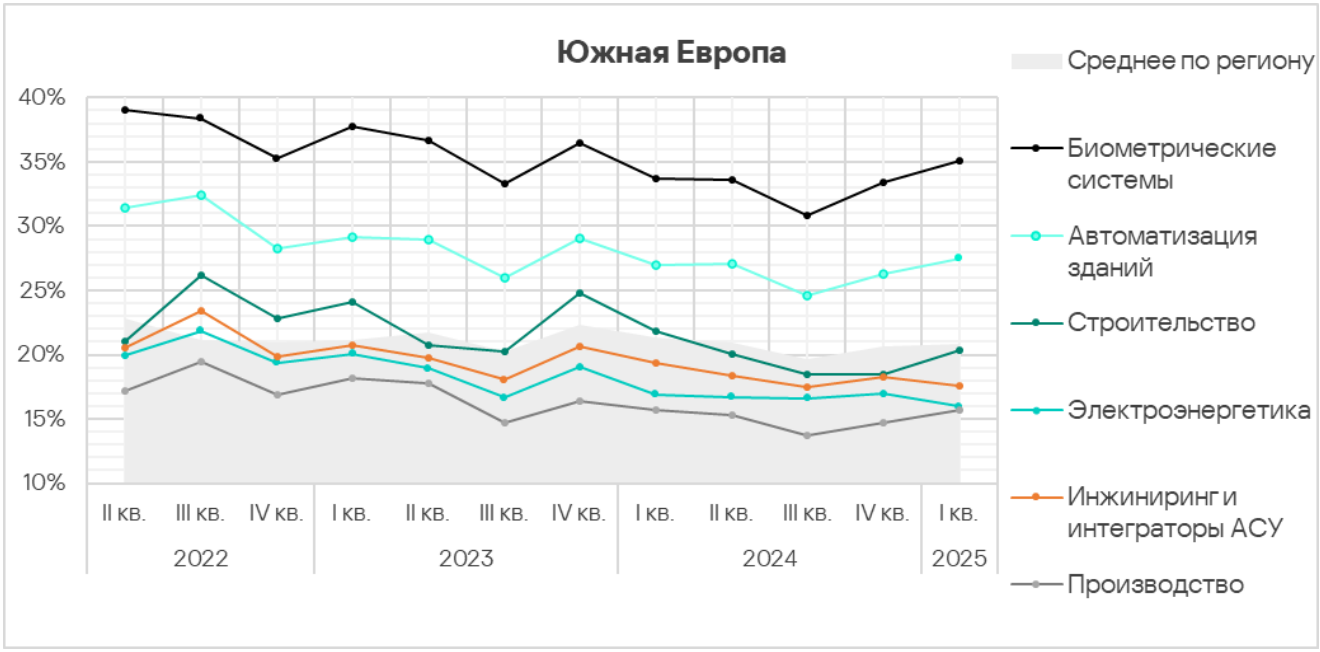


В **первом квартале 2025 года** доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла** в следующих отраслях и OT-инфраструктурах:

- Биометрические системы — в 1,1 раза;
- Строительство — в 1,1 раза;

- Производство — в 1,1 раза;
- Автоматизация зданий.

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



Россия

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
5,60% **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▲ 1,1x рост в I кв. 2025 г. 1-е место по росту 1,1x выше среднего по миру 2-е место в мире	**4,56%** **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ 1,1x рост в I кв. 2025 г.	**2,65%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г.
1,04% **МАЙНЕРЫ — ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ слабый рост в I кв. 2025 г. 1,3x выше среднего по миру 2-е место в мире	**0,77%** **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,4x рост в I кв. 2025 г.	**0,11%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 2,2x рост в I кв. 2025 г. 3-е место по росту
9,34% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ 1,2x рост в I кв. 2025 г. 1-е место по росту	**0,88%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ 1,2x рост в I кв. 2025 г.	**0,24%** **СЪЕМНЫЕ НОСИТЕЛИ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.

- **Основной источник угроз в России — интернет.**

  Уровень угроз из **интернета** в первом квартале 2025 года **вырос** в России в **1,2** раза. По **росту** доли компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, Россия занимает **первое место** в мире.

- По доле компьютеров АСУ, на которых были заблокированы **ресурсы в интернете из списка запрещенных**, Россия занимает **второе место** среди регионов (после Африки). Россия — единственный регион, где этот показатель вырос за квартал. Региональный показатель выше, чем среднемировой, в 1,1 раза.

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

- Известные вредоносные URL-адреса и IP-адреса, используемые злоумышленниками для размещения вредоносных нагрузок и конфигураций;
- Подозрительные (ненадежные) веб-ресурсы с развлекательным и игровым контентом, часто используемые для доставки нежелательного программного обеспечения, криптомайнеров и вредоносных скриптов;
- Узлы CDN, используемые злоумышленниками для распространения вредоносных скриптов на популярных веб-сайтах;
- Сервисы обмена файлами и данными, включая репозитории, часто используемые злоумышленниками для размещения полезных нагрузок и конфигураций следующего этапа.

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

Высокие значения параметра, как правило, свидетельствуют:

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

- В первом квартале 2025 года Россия находится также на **втором месте среди регионов** по доле компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows**.

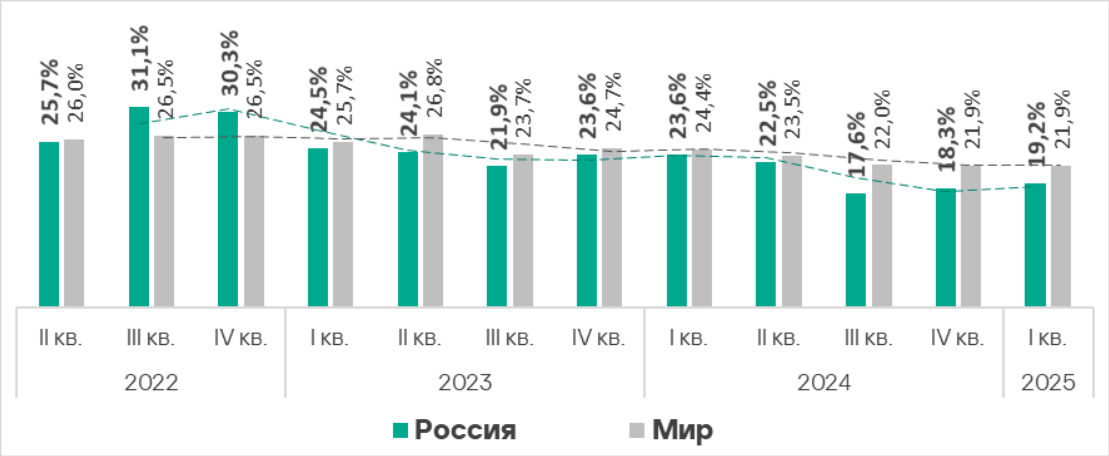
  В России в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows занимают четвертое место. Среди регионов это самая высокая позиция для данной категории угроз. В аналогичном мировом рейтинге она находится на седьмом месте.

Общая ситуация

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

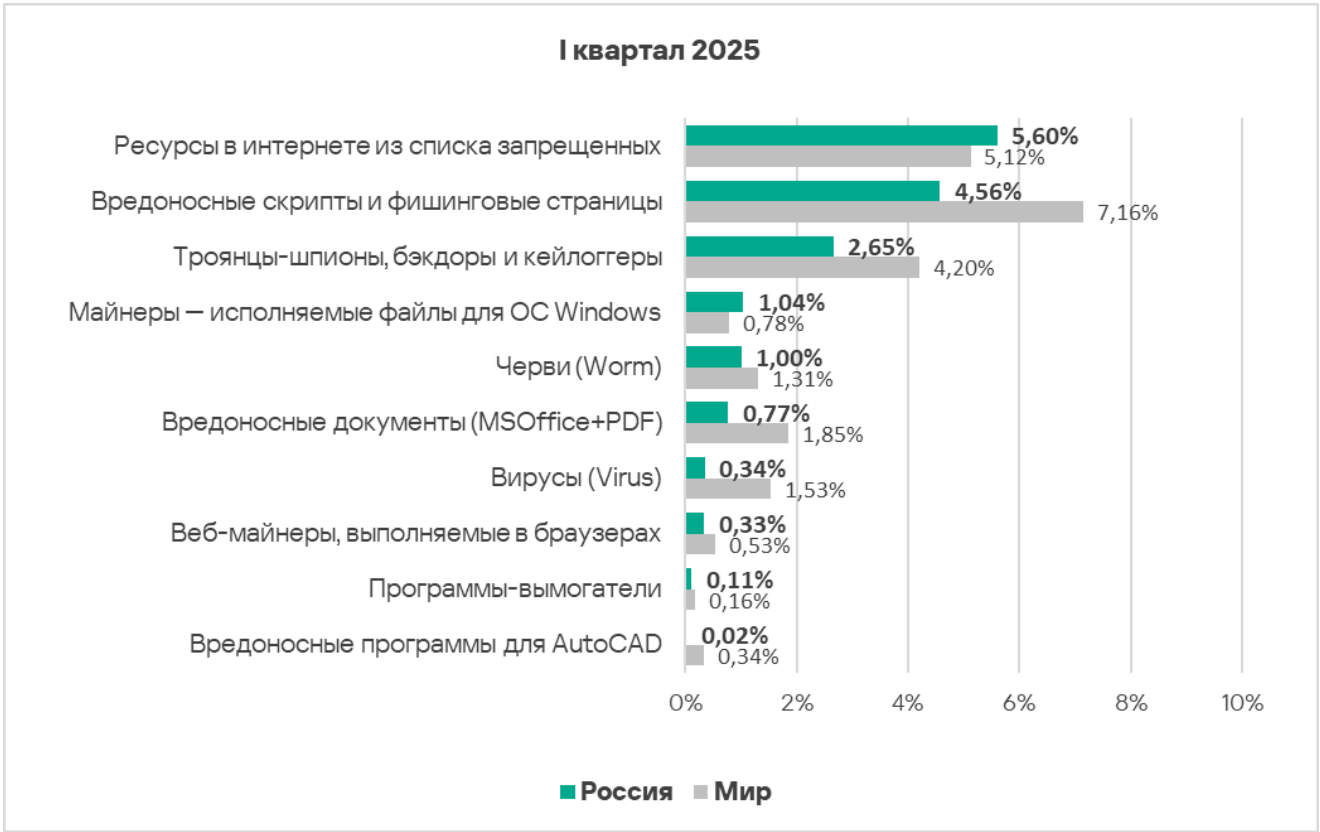
Значение этого показателя остается ниже среднемирового с начала 2023 года.

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла до **19,2%**.



Сравнительный анализ

Категории угроз



По сравнению со среднемировыми показателями в регионе **выше** доля компьютеров АСУ, на которых были заблокированы:

- Ресурсы в интернете из списка запрещенных — в 1,1 раза;
- Майнеры — исполняемые файлы для ОС Windows.

Среди регионов по обоим этим показателям Россия находится на **втором месте**.

Источники угроз

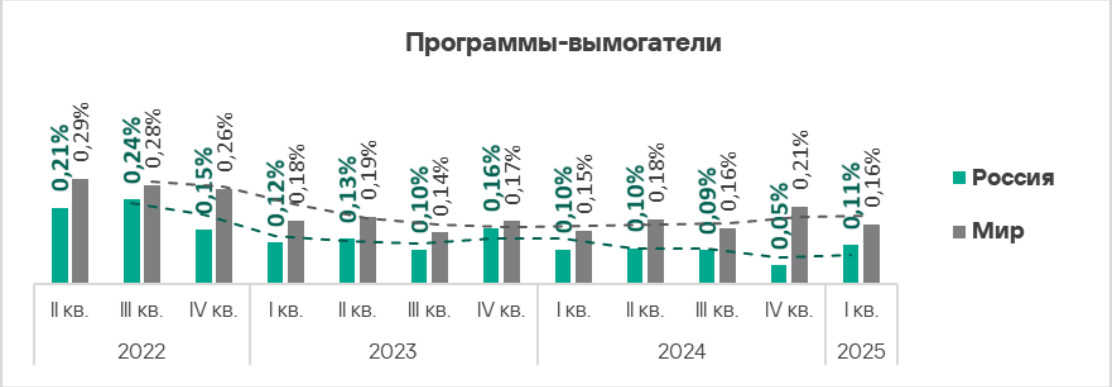
Показатели всех источников угроз в России **ниже** соответствующих **среднемировых значений.** Показатель почтовых клиентов в России — самый маленький среди регионов.

Изменения за квартал и тренды

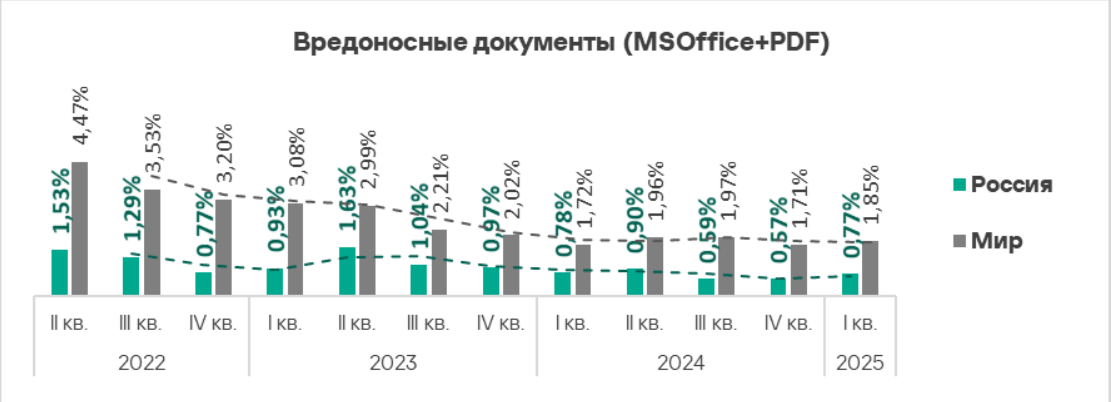
Категории угроз

Наибольший рост за квартал **в регионе** отмечен у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

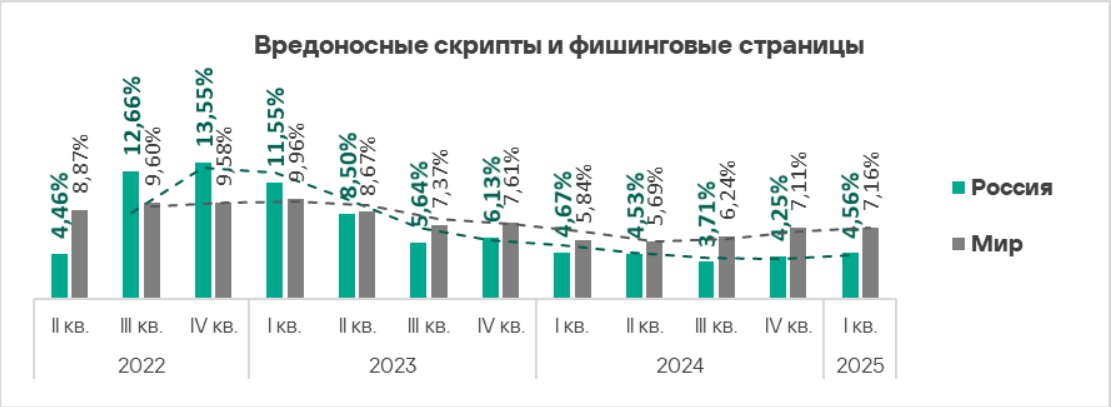
- Программы-вымогатели — в 2,2 раза;



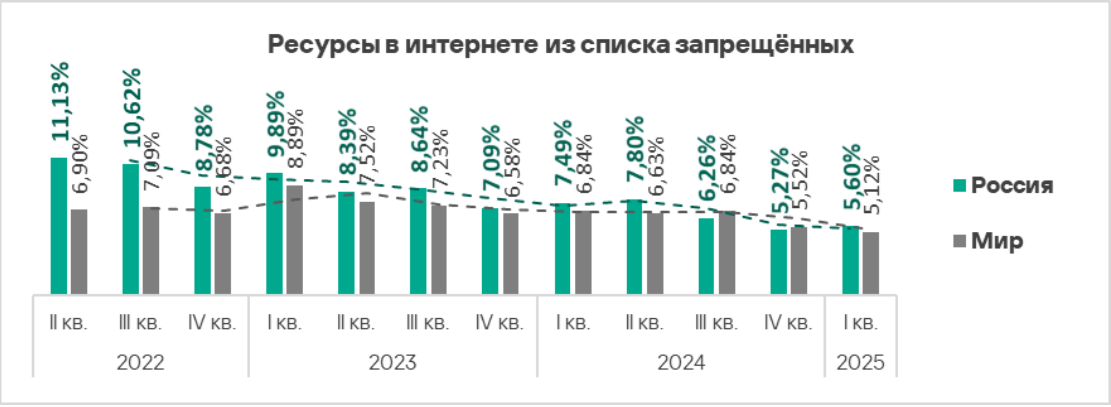
- Вредоносные документы — в 1,4 раза;



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



- Ресурсы в интернете из списка запрещенных — в 1,1 раза. Россия — единственный регион, где этот показатель вырос.



Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в России со второго квартала 2022 года. Ведущей категорией угроз в регионе, начиная с третьего квартала 2023 года, являются **ресурсы в интернете из списка запрещенных.** В первом квартале 2025 года **майнеры —**

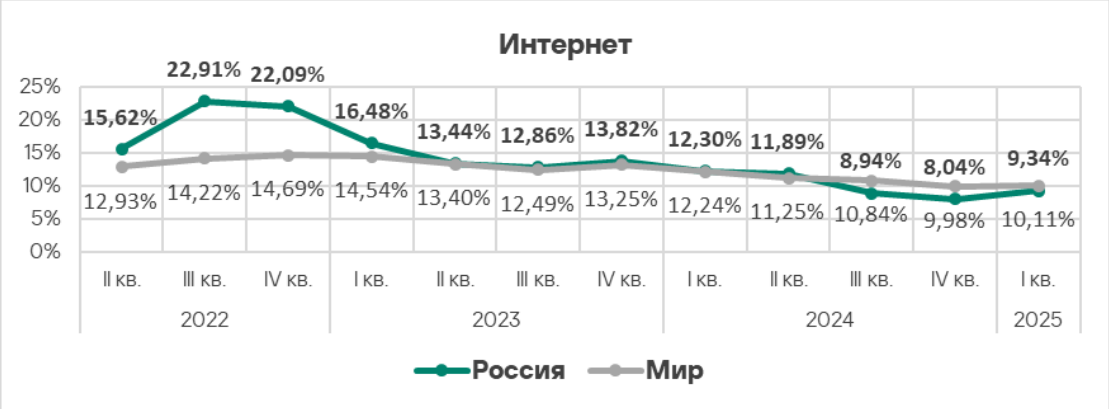
исполняемые файлы для ОС Windows поднялись с пятого места на четвертое, а **вирусы** — с восьмого на седьмое место.

Россия	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Ресурсы в интернете из списка запрещенных	1	2	2	2	2	1	1	1	1	1	1	1
Вредоносные скрипты и фишинговые страницы	2	1	1	1	1	2	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	4	4	4	5	5	4	4	4	4	5	4
Черви (Worm)	6	6	5	5	7	6	5	5	5	5	4	5
Вредоносные документы (MSOffice+PDF)	4	5	7	7	4	4	6	6	6	6	6	6
Вирусы (Virus)	8	8	8	8	8	8	8	7	7	8	8	7
Веб-майнеры, выполняемые в браузерах	7	7	6	6	6	7	7	8	8	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

Уровень угроз из **интернета** и **почтовых клиентов** в первом квартале 2025 года **вырос** в 1,2 раза по каждому источнику.

По **росту** доли компьютеров АСУ, на которых были заблокированы угрозы из **интернета**, Россия занимает **первое** место в мире.



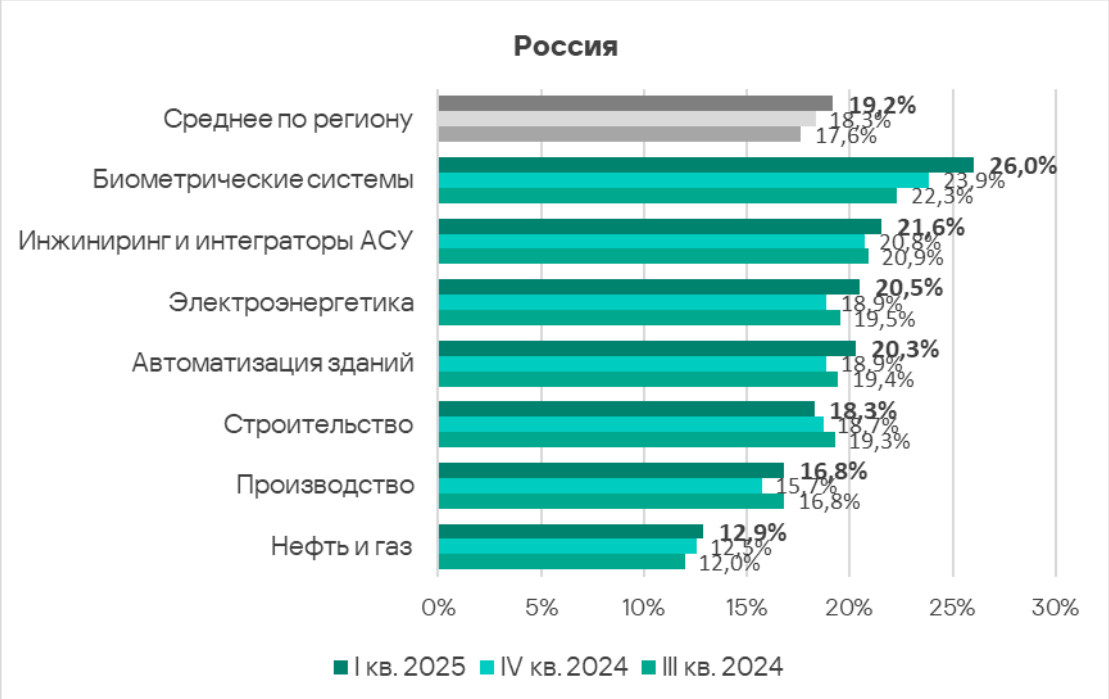
Несмотря на рост доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, Россия находится на последнем месте в рейтинге регионов по этому показателю.

Отрасли

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

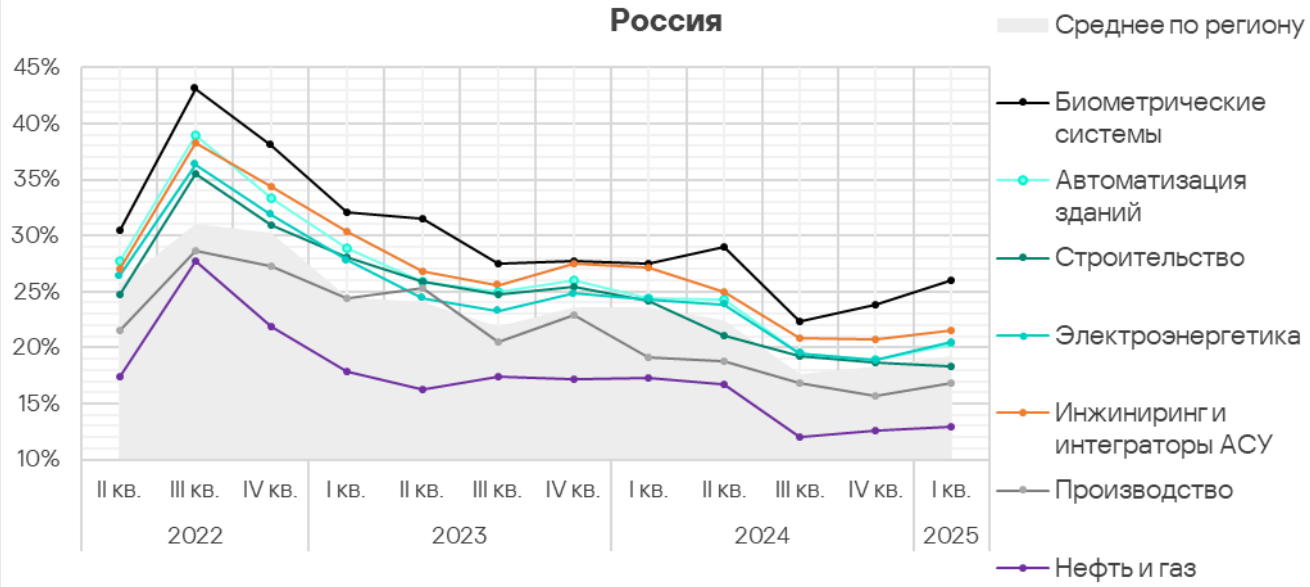
Во всех отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **ниже** соответствующих **среднемировых показателей.**

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **увеличилась** во всех рассмотренных отраслях региона, кроме строительства.



Несмотря на рост в первом квартале 2025 года показателей у всех отраслей, кроме строительства, с четвертого квартала 2022 года **тренды**

рассмотренных отраслей демонстрируют преимущественно **положительную динамику (показатели постепенно снижаются).**



Австралия и Новая Зеландия

Актуальные угрозы

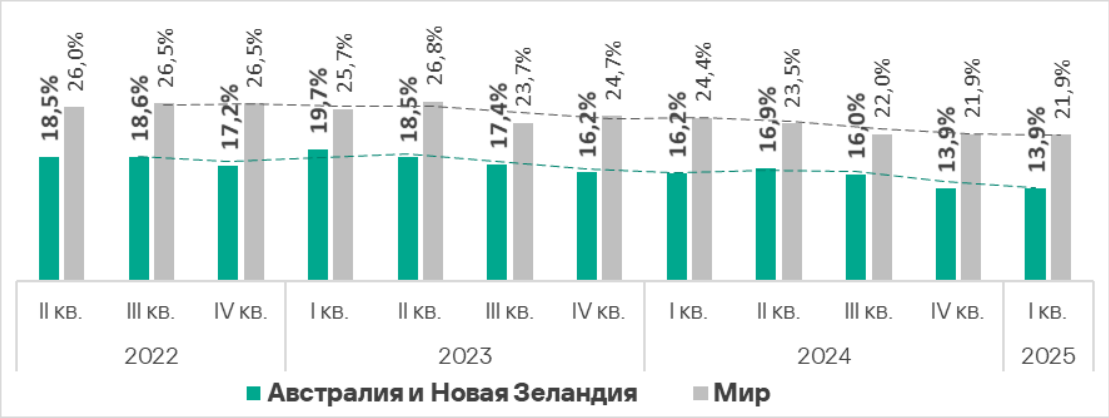
1-е место в регионе	2-е место в регионе	3-е место в регионе
7,19% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ 1,1x рост в I кв. 2025 г. 2-е место по росту	**2,78%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.	**1,72%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г.
0,48% **ВЕБ-МАЙНЕРЫ** ▲ 2,2x рост в I кв. 2025 г.	**0,30%** **МАЙНЕРЫ – ИСПОЛНЯЕМЫЕ ФАЙЛЫ ДЛЯ WINDOWS** ▲ 1,4x рост в I кв. 2025 г.	**0,28%** **ЧЕРВИ** ▲ 1,1x рост в I кв. 2025 г. 2-е место по росту
0,06% **ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ AUTOCAD** ▲ 1,5x рост в I кв. 2025 г. 2-е место по росту	**8,06%** **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г. 3-е место по росту	**2,80%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г. 1-е место по росту

Один из самых благополучных по кибербезопасности регионов.

Общая ситуация

Австралия и Новая Зеландия занимают **11-е место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Значение показателя существенно **ниже среднемирового (13,9%).**



Сравнительный анализ

Категории угроз

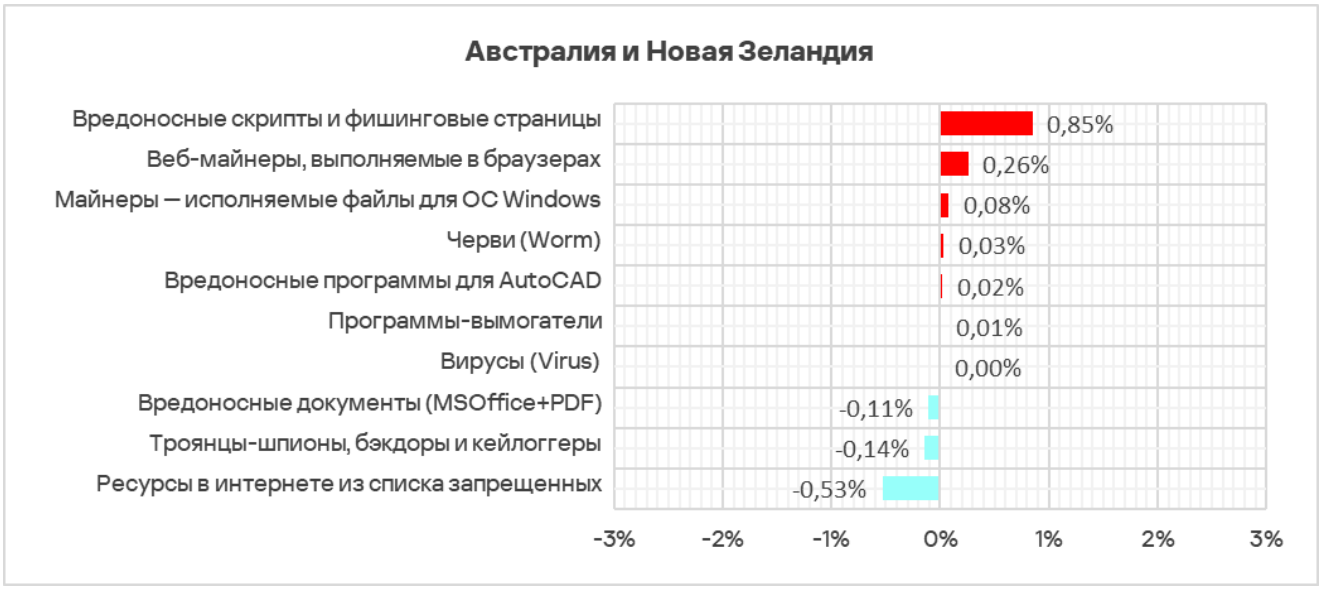
Доля компьютеров АСУ, на которых заблокированы вредоносные объекты, **ниже среднемирового значения** у всех категорий угроз, кроме вредоносных скриптов и фишинговых страниц, показатель которых практически соответствует среднемировому.

Источники угроз

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

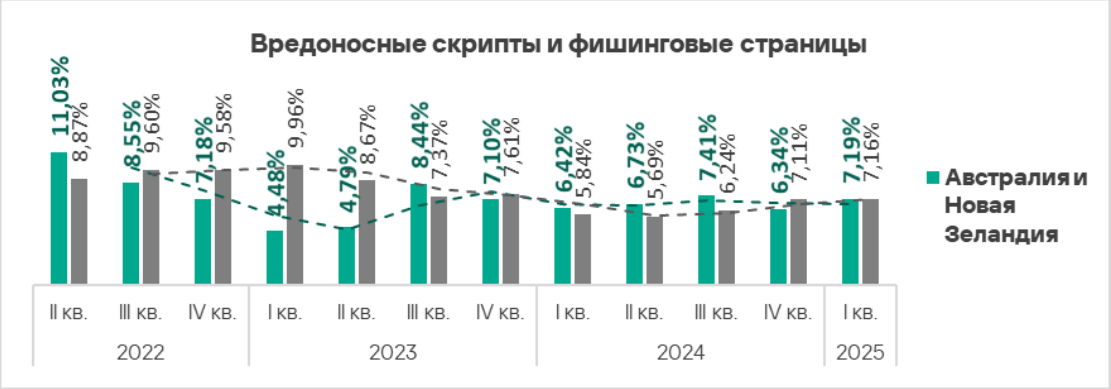
Изменения за квартал и тренды

Категории угроз

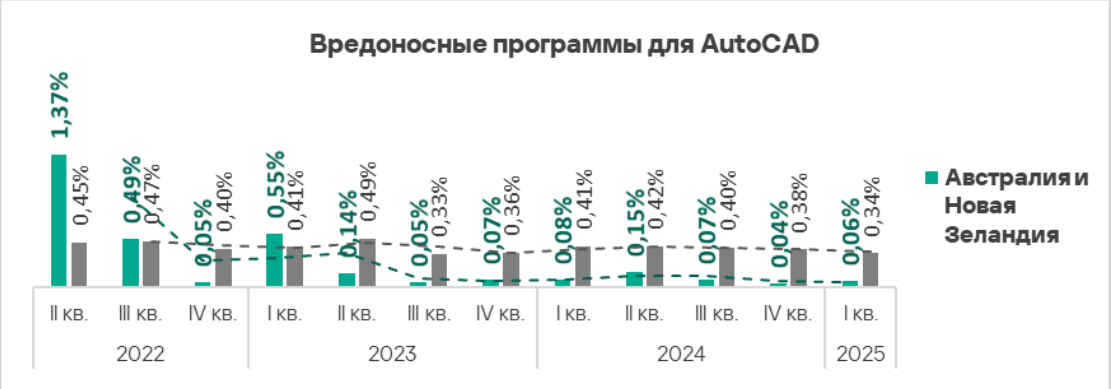


Наибольший рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы:

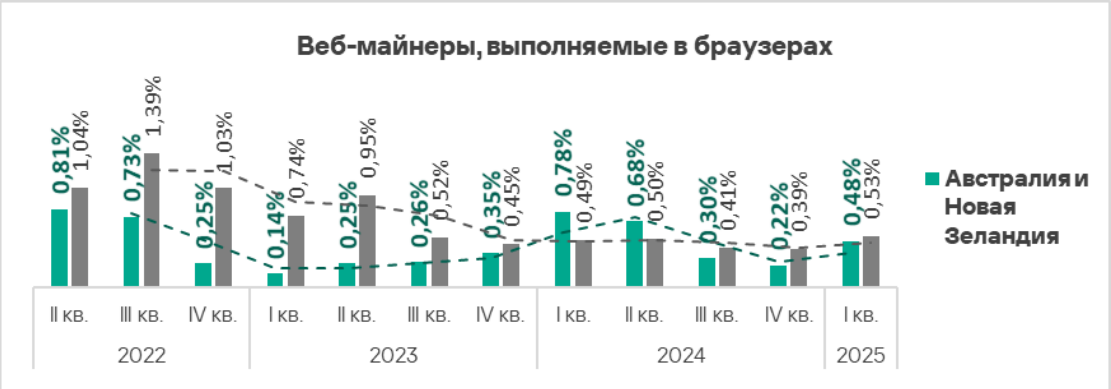
- Вредоносные скрипты и фишинговые страницы — в 1,1 раза, среди регионов — **второе место по росту** этого показателя;



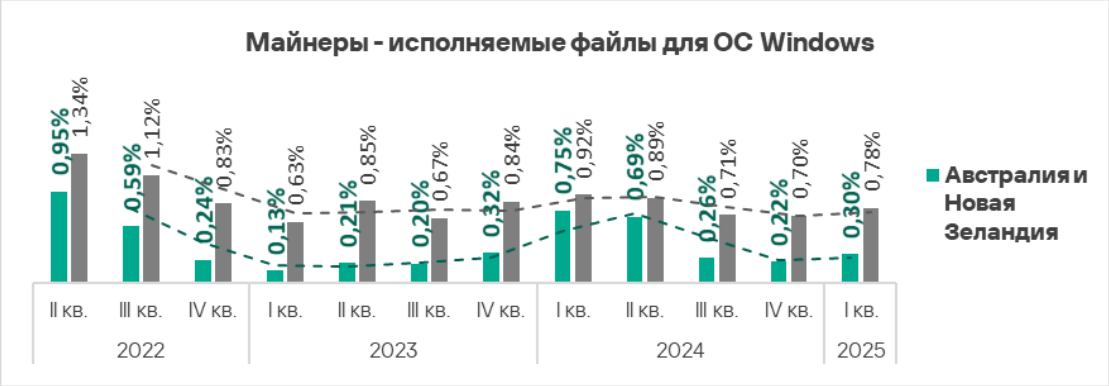
- Вредоносные программы для AutoCAD — в 1,5 раза. Среди регионов — **второе место по росту** этого показателя;



- Веб-майнеры — в 2,2 раза;



- Майнеры — исполняемые файлы для ОС Windows — в 1,4 раза.



В регионе также выросла доля компьютеров АСУ, на которых были заблокированы:

- Черви — в 1,1 раза. Среди регионов Австралия и Новая Зеландия находится на последнем месте по доле компьютеров АСУ, на которых блокируются черви, и на **третьем месте по росту** этого показателя;
- Программы-вымогатели — в 1,1 раза.

Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Австралии и Новой Зеландии со второго квартала 2022 года. В первом квартале 2025 года **веб-майнеры** поднялись с шестой на **пятую** позицию.

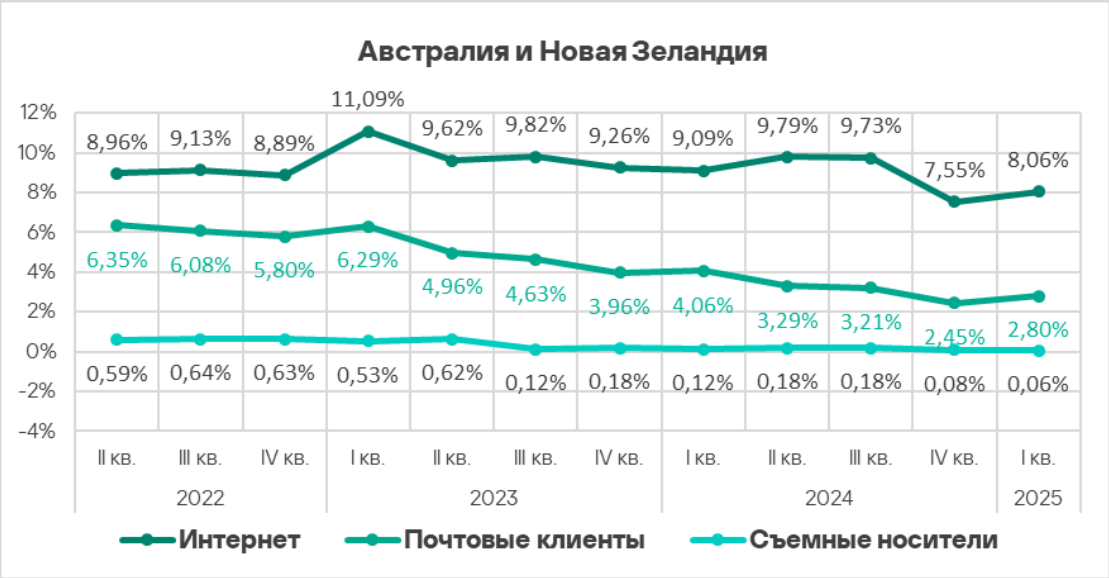
Австралия и Новая Зеландия	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	1	1	1	1	1
Ресурсы в интернете из списка запрещенных	2	2	2	2	2	2	2	2	2	2	2	2
Троянцы-шпионы, бэкдоры и кейлоггеры	3	3	4	3	3	4	4	3	3	4	3	3
Вредоносные документы (MSOffice+PDF)	4	4	3	5	4	3	3	4	4	3	4	4
Веб-майнеры, выполняемые в браузерах	9	6	5	8	6	5	5	5	6	5	6	5
Майнеры – исполняемые файлы для ОС Windows	8	7	6	9	8	6	6	6	5	7	6	6
Черви (Worm)	6	8	8	6	6	7	8	7	7	6	5	7
Вирусы (Virus)	5	5	7	4	5	8	7	8	8	8	8	8
Программы-вымогатели	10	10	10	10	10	9	9	9	9	10	9	9
Вредоносные программы для AutoCAD	7	9	9	7	9	10	10	10	10	9	10	10

Источники угроз

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **увеличилась** у всех источников угроз,

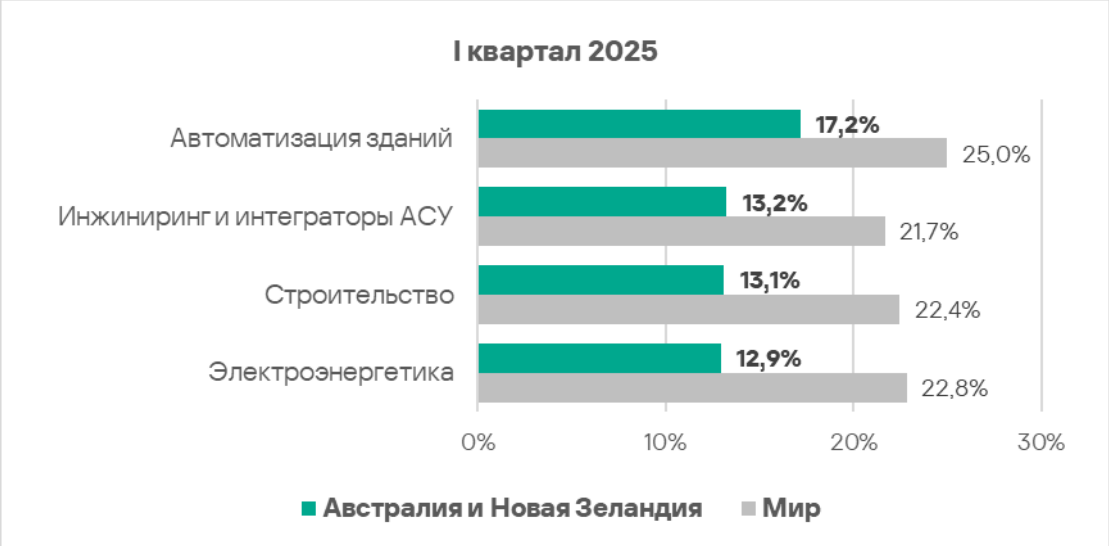
кроме съемных носителей. Показатель **интернета и почтовых клиентов** вырос в **1,1 раза** у каждого источника.

В рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, регион находится на седьмом месте. По **росту** доли компьютеров АСУ, на которых были заблокированы угрозы из **почтовых клиентов,** Австралия и Новая Зеландия занимает **первое** место среди регионов, по росту показателя угроз из интернета — третье место.

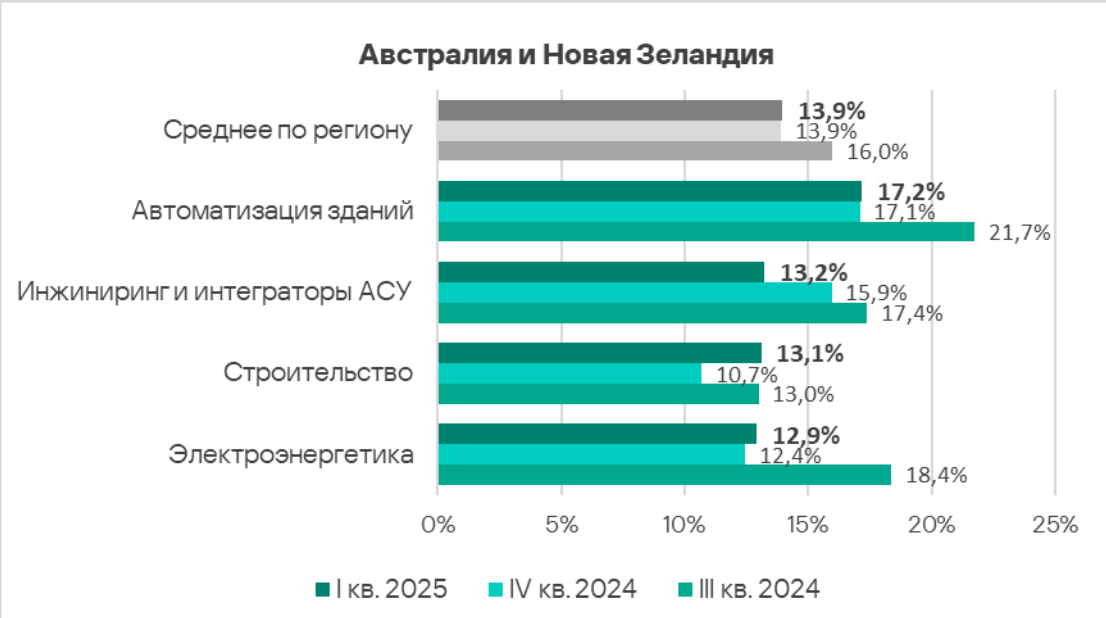


Отрасли

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

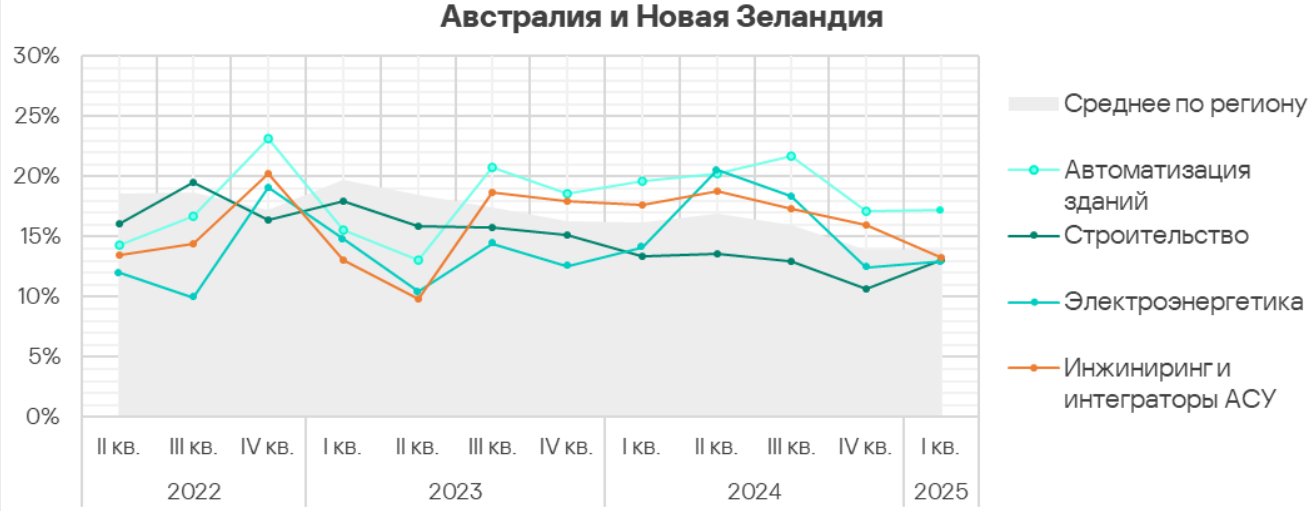


В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **увеличилась** во всех рассматриваемых отраслях, кроме отрасли инжиниринг и интеграторы АСУ. В **строительстве** показатель вырос в **1,2** раза.



Автоматизация зданий, электроэнергетика, 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. Это тренд продолжается у

электроэнергетики, показатели остальных отраслей стали более стабильными. **Строительная** отрасль все еще демонстрирует преимущественно **нисходящий тренд**, оставаясь ниже среднего значения по региону, но показатель отрасли за отчетный период вырос.



Западная Европа

Актуальные угрозы

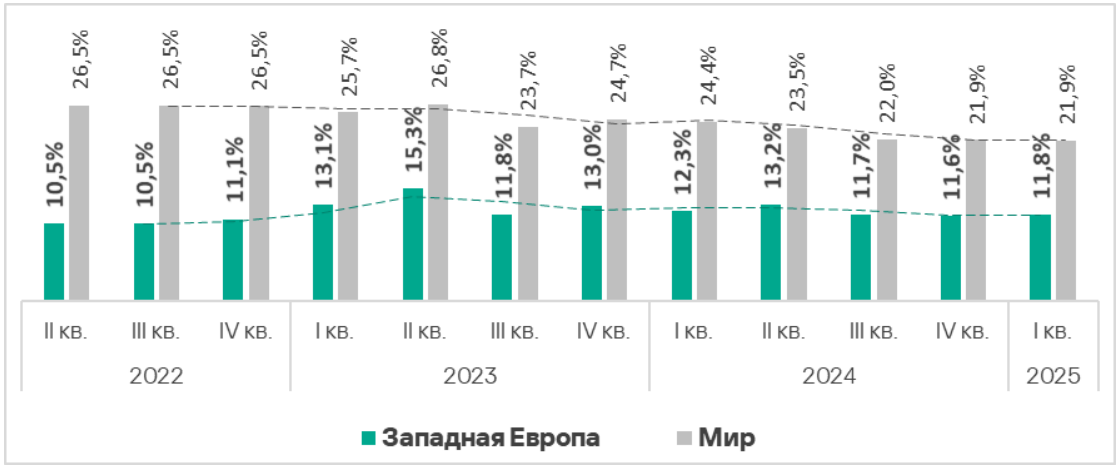
1-е место в регионе	2-е место в регионе	3-е место в регионе
4,60% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ слабый рост в I кв. 2025 г.	**3,31%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.	**1,62%** **ШПИОНСКИЕ ПРОГРАММЫ** ▲ 1,1x рост в I кв. 2025 г. 2-е место по росту
0,90% **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,1x рост в I кв. 2025 г.	**0,50%** **ВЕБ-МАЙНЕРЫ** ▲ 2,4x рост в I кв. 2025 г.	**0,22%** **ВИРУСЫ** ▲ 1,2x рост в I кв. 2025 г.
6,60% **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ рост в I кв. 2025 г.	**1,65%** **ПОЧТОВЫЕ КЛИЕНТЫ** КАК ИСТОЧНИК УГРОЗ ▼ снижение в I кв. 2025 г.	**0,03%** **СЕТЕВЫЕ ПАПКИ** КАК ИСТОЧНИК УГРОЗ ▲ 1,1x рост в I кв. 2025 г.

Один из самых благополучных по кибербезопасности регионов.

Общая ситуация

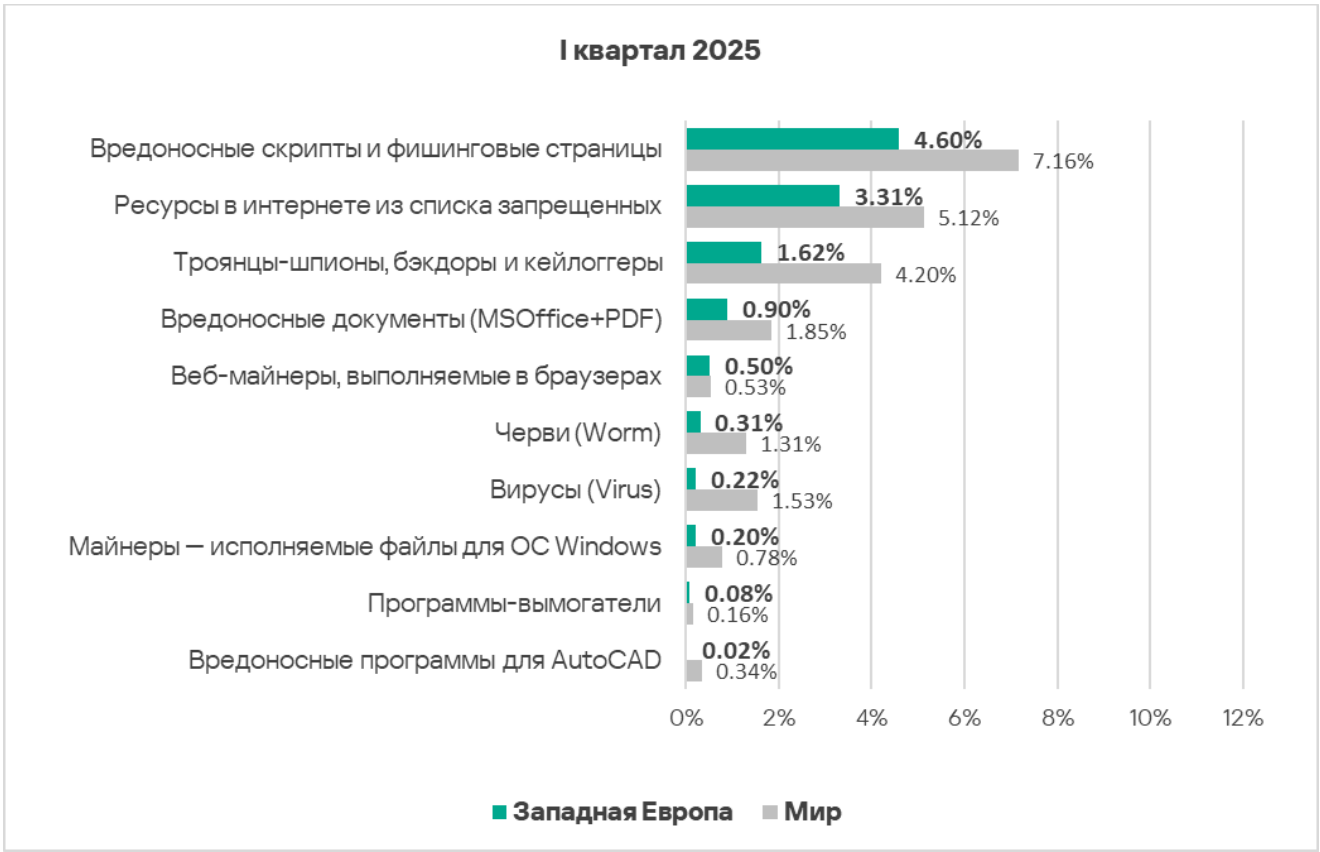
Западная Европа занимает **12-е место** в мировом рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Значение этого показателя в регионе — **одно из самых низких,** оно существенно ниже среднемирового. В первом квартале 2025 года оно **увеличилось на 0,2 п. п.**



Сравнительный анализ

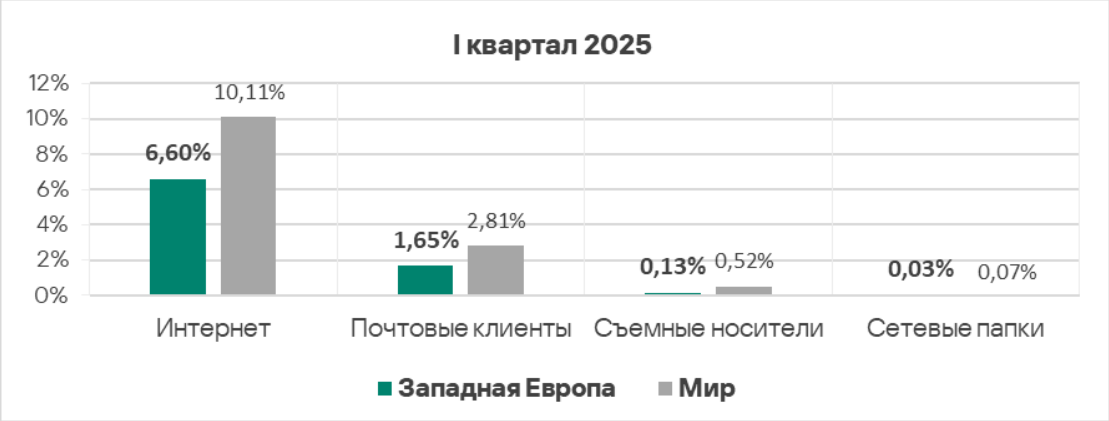
Категории угроз



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

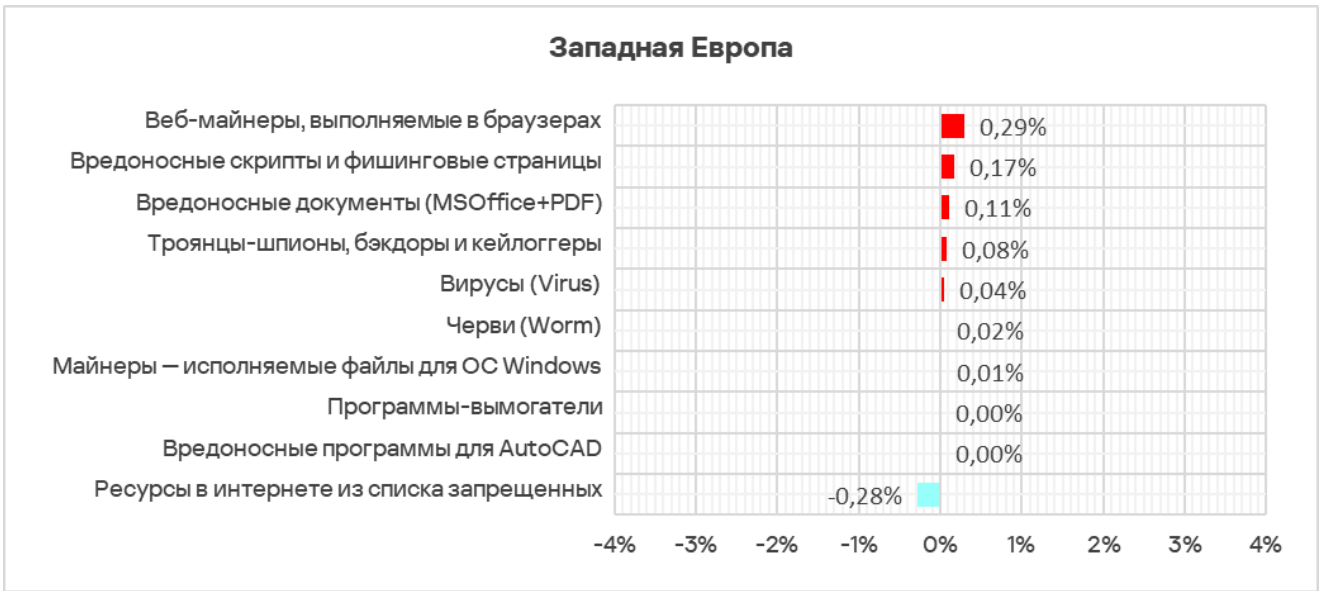
Источники угроз

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



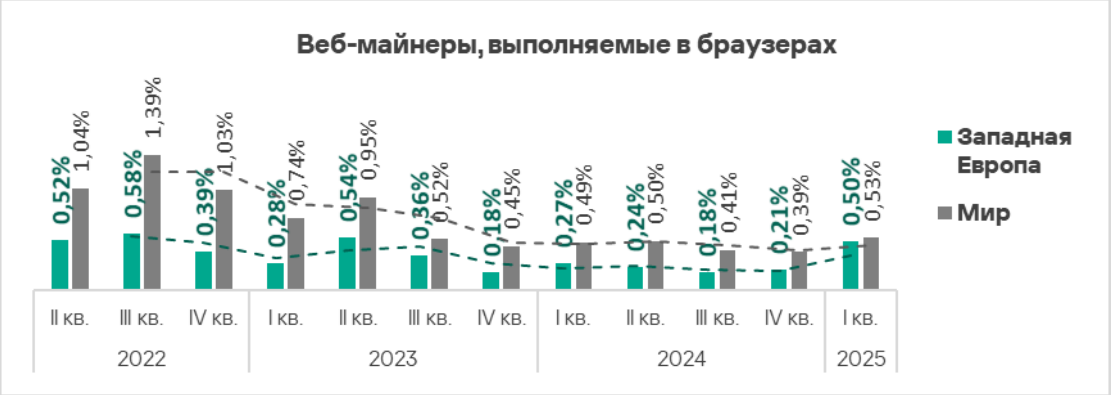
Изменения за квартал и тренды

Категории угроз

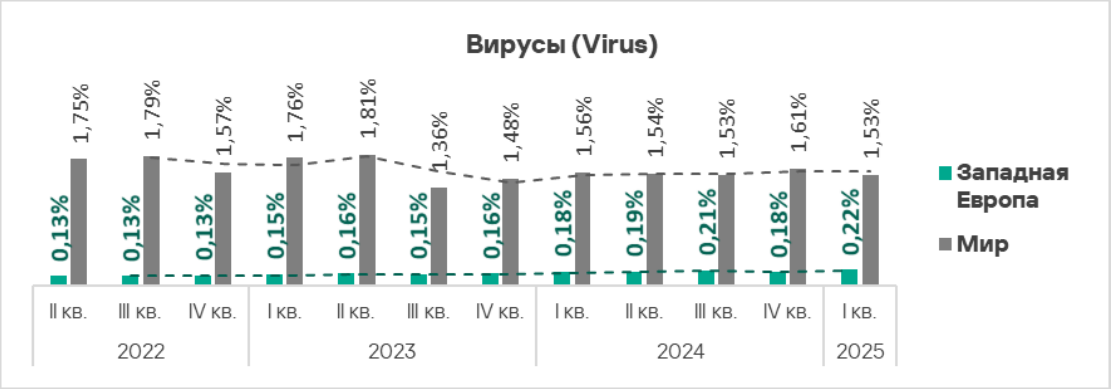


Наибольший рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие вредоносные объекты:

- Веб-майнеры — в 2,4 раза;



- Вирусы — в 1,2 раза;



- Шпионские программы, вредоносные документы, черви, майнеры — исполняемые файлы для ОС Windows — в 1,1 раза каждая из категорий.

По **росту** показателя **шпионских программ** Западная Европа занимает **второе** место среди регионов.

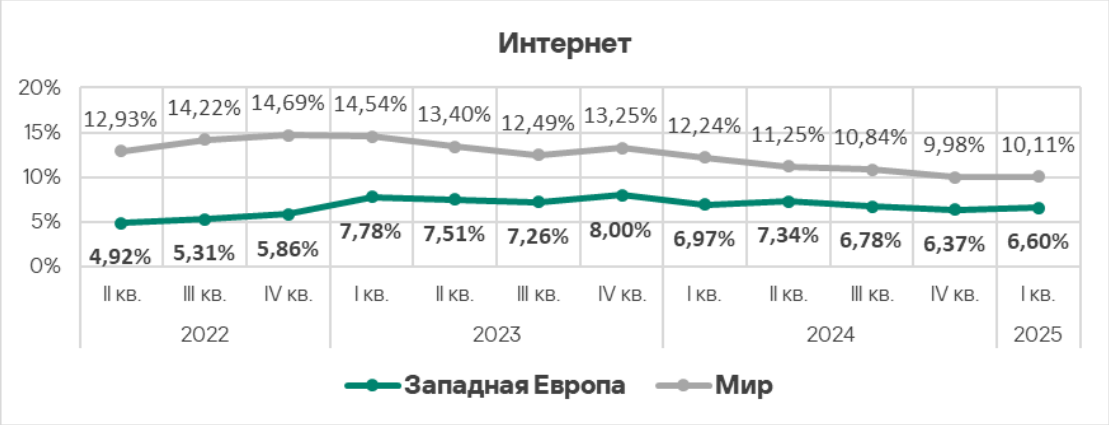
Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Западной Европе со второго квартала 2022 года. В первом квартале 2025 года **вирусы** поднялись с восьмого на седьмое место.

Западная Европа	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	1	1	1	1	2	2	2	1	1
Ресурсы в интернете из списка запрещенных	2	2	2	2	2	2	2	1	1	1	2	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
Веб-майнеры, выполняемые в браузерах	6	5	5	6	5	5	6	6	7	7	6	5
Черви (Worm)	7	7	6	5	7	6	5	5	5	5	5	6
Вирусы (Virus)	9	9	9	7	8	8	7	8	8	6	8	7
Майнеры – исполняемые файлы для ОС Windows	5	6	7	8	6	7	8	7	6	8	7	8
Программы-вымогатели	8	8	8	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 первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты из интернета, **увеличилась**.

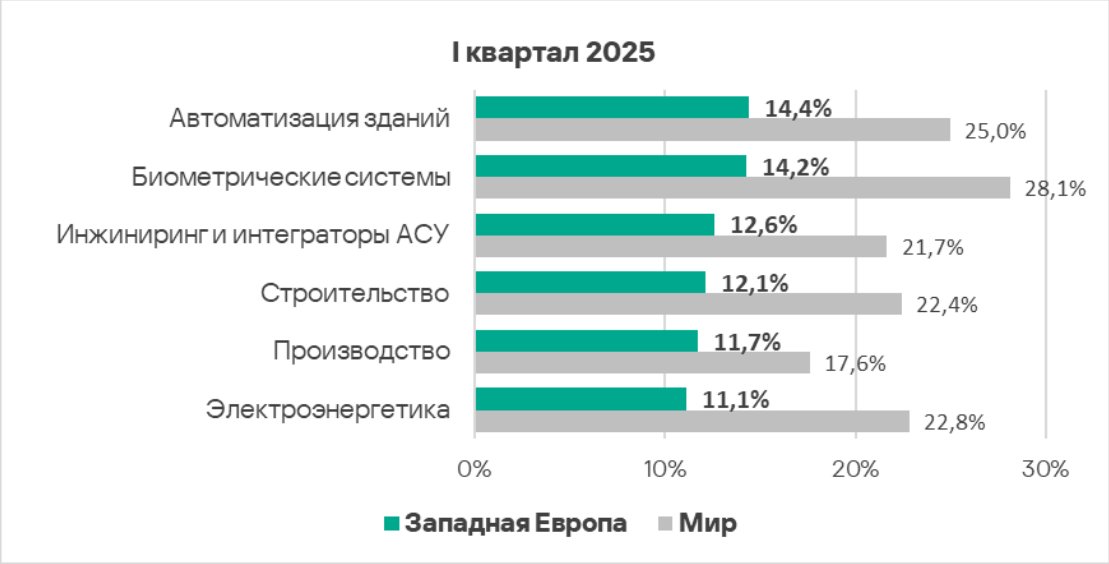
Показатель интернета как источника угроз в регионе значительно ниже среднемирового значения.



Отрасли

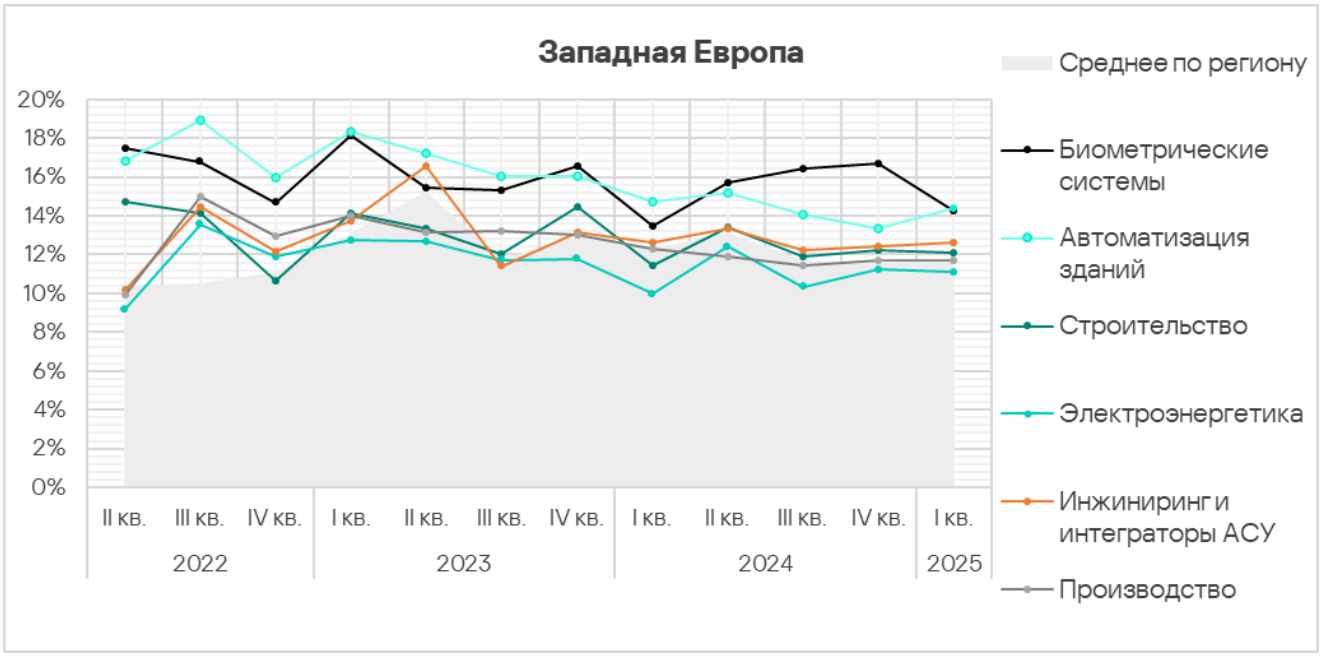
Наиболее часто встречающейся с угрозами отраслью из рассмотренных в отчете является **автоматизация зданий.**

Показатели во всех отраслях региона значительно **ниже** соответствующих **среднемировых значений.**



В первом квартале 2025 года из всех рассмотренных отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла** в двух отраслях — **автоматизация зданий, инжиниринг и интеграторы АСУ**.

Автоматизация зданий и **биометрические системы** по-прежнему демонстрируют **тренды,** заметно превышающие среднее для региона значение.



Северная Европа

Актуальные угрозы

1-е место в регионе	2-е место в регионе	3-е место в регионе
3,07% **ВРЕДОНОСНЫЕ СКРИПТЫ И ФИШИНГОВЫЕ СТРАНИЦЫ** ▲ слабый рост в I кв. 2025 г.	**2,65%** **ИНТЕРНЕТ-РЕСУРСЫ ИЗ СПИСКА ЗАПРЕЩЕННЫХ** ▼ снижение в I кв. 2025 г.	**1,71%** **ШПИОНСКИЕ ПРОГРАММЫ** ▼ снижение в I кв. 2025 г.
0,60% **ВРЕДОНОСНЫЕ ДОКУМЕНТЫ** ▲ 1,1x рост в I кв. 2025 г.	**0,08%** **ПРОГРАММЫ-ВЫМОГАТЕЛИ** ▲ 1,6x рост в I кв. 2025 г.	**5,24%** **ИНТЕРНЕТ** КАК ИСТОЧНИК УГРОЗ ▲ рост в I кв. 2025 г.

Самый благополучный по кибербезопасности регион, традиционно занимает последнее место в рейтинге по доле компьютеров АСУ, на которых блокируются вредоносные объекты.

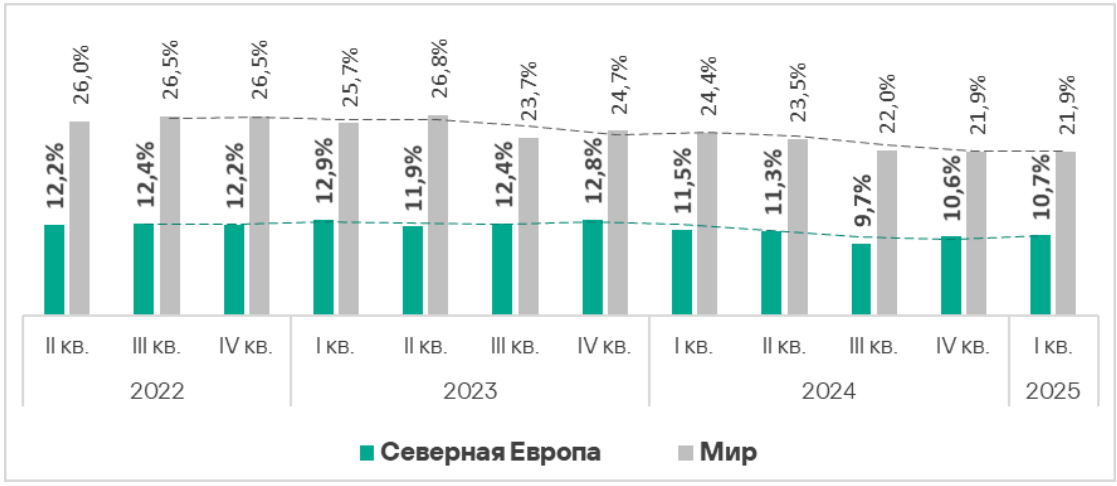
Тем не менее, регион занял пятое место в мире по росту показателя программ-вымогателей (в 1,6 раза).

Общая ситуация

Северная Европа занимает **13-е место** в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Показатель значительно ниже среднемирового.

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Северной Европе выросла до **10,7%.** Это наименьшее значение из всех регионов.



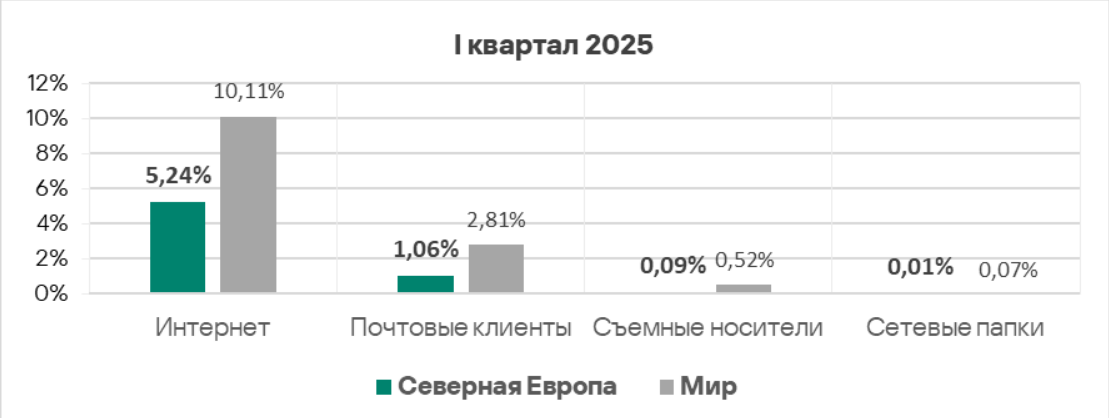
Сравнительный анализ

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.**



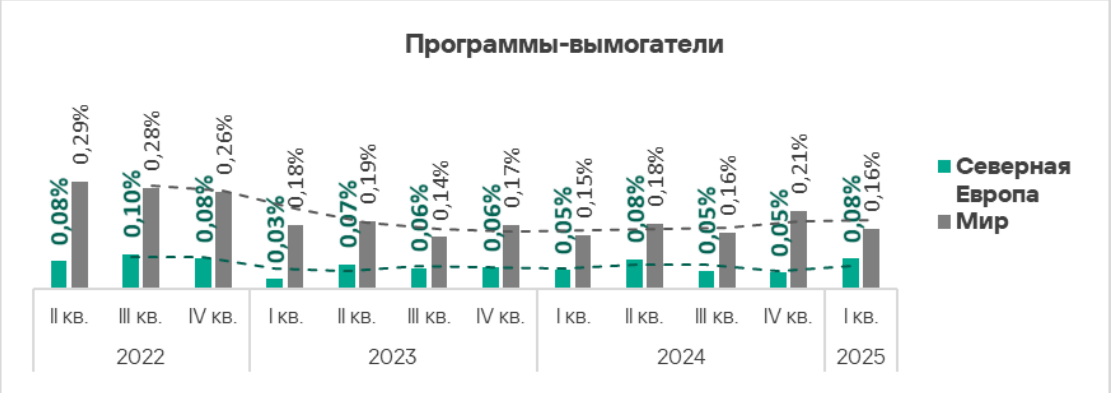
Изменения за квартал и тренды

Категории угроз

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

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

- Программы-вымогатели — в 1,6 раза;



- Вредоносные документы — в 1,1 раза.

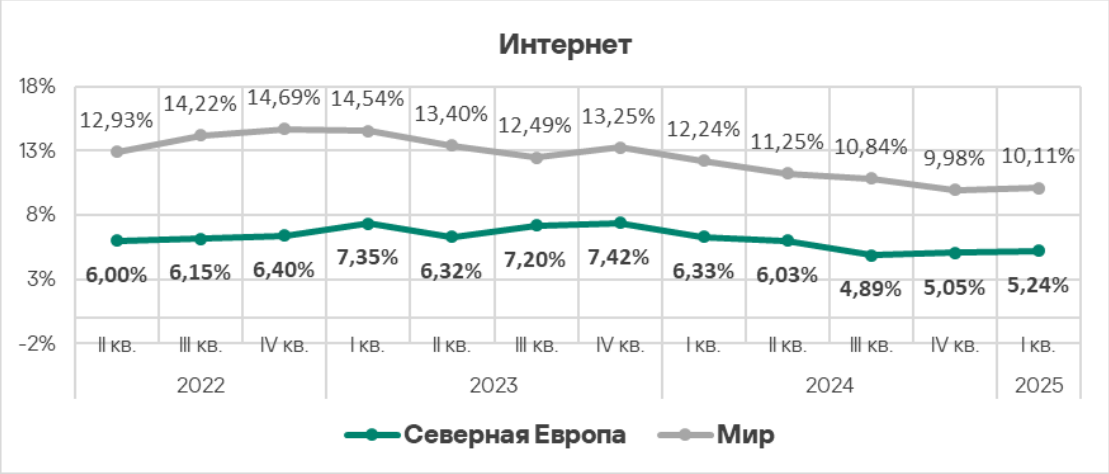
Тепловая карта иллюстрирует изменения в рейтингах категорий угроз в Северной Европе со второго квартала 2022 года. В первом квартале 2025 года изменений в позициях категорий угроз нет.

Северная Европа	2022			2023				2024				2025
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Вредоносные скрипты и фишинговые страницы	1	1	1	2	2	2	1	2	2	2	1	1
Ресурсы в интернете из списка запрещенных	2	2	2	1	1	1	2	1	1	1	2	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	6	5	6	6	5	7	7	7	5	5
Майнеры – исполняемые файлы для ОС Windows	5	6	7	8	7	6	8	6	5	6	6	6
Веб-майнеры, выполняемые в браузерах	6	5	5	7	5	5	7	5	6	8	7	7
Вирусы (Virus)	8	8	8	6	8	8	6	8	8	5	8	8
Программы-вымогатели	9	9	9	10	9	9	9	9	9	9	9	9
Вредоносные программы для AutoCAD	10	10	10	9	10	10	10	10	10	10	10	10

Источники угроз

В первом квартале 2025 года выросла доля компьютеров АСУ, на которых были заблокированы угрозы из **интернета**.

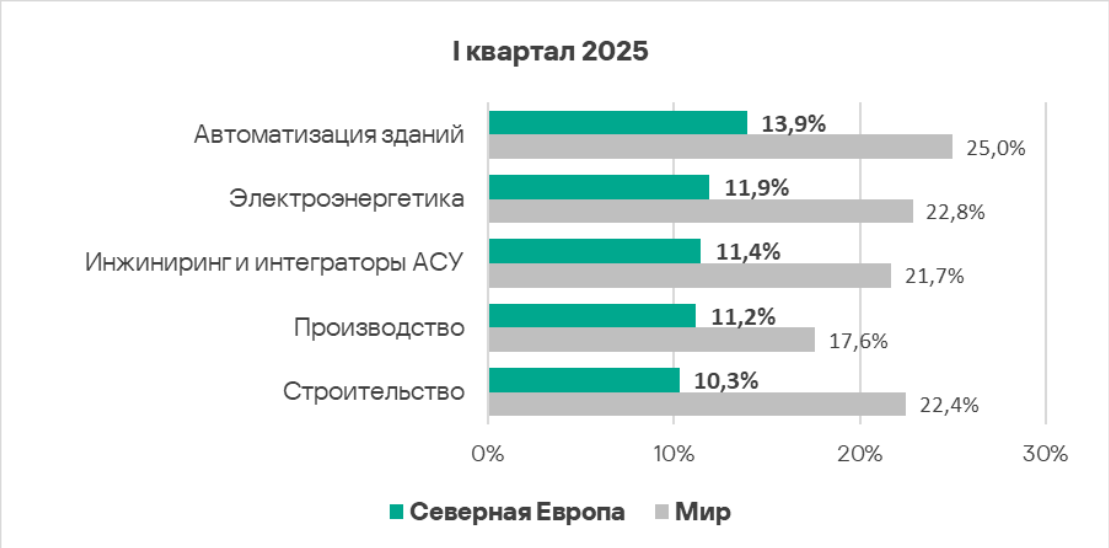
Показатель интернета как источника угроз в регионе значительно меньше, чем среднемировой.



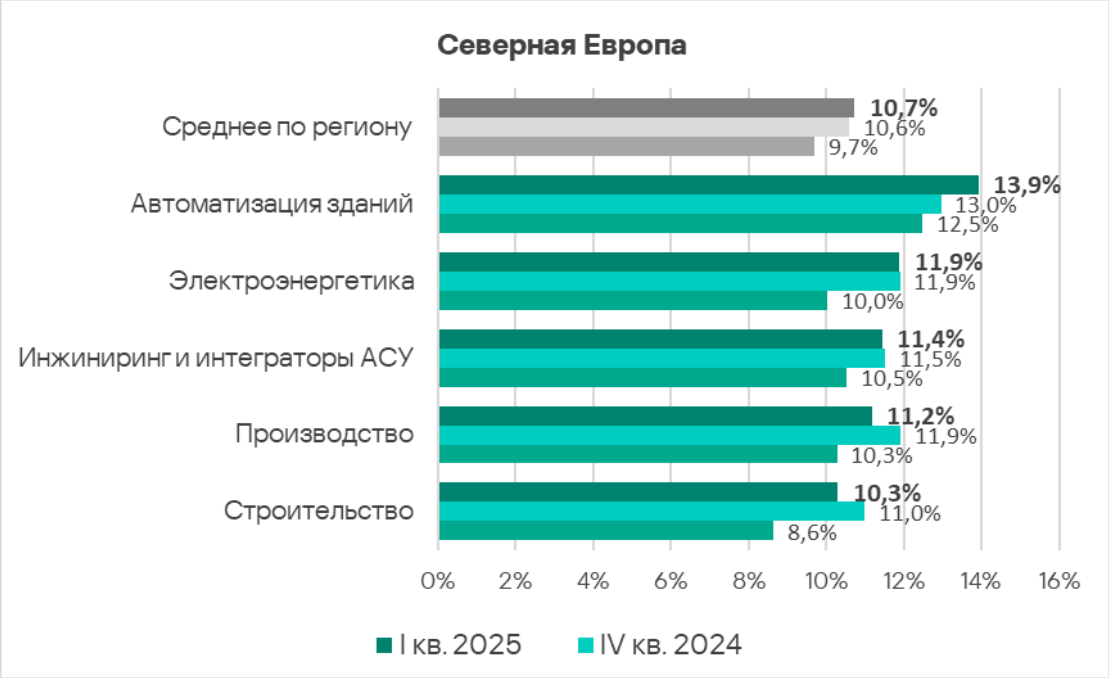
Отрасли

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

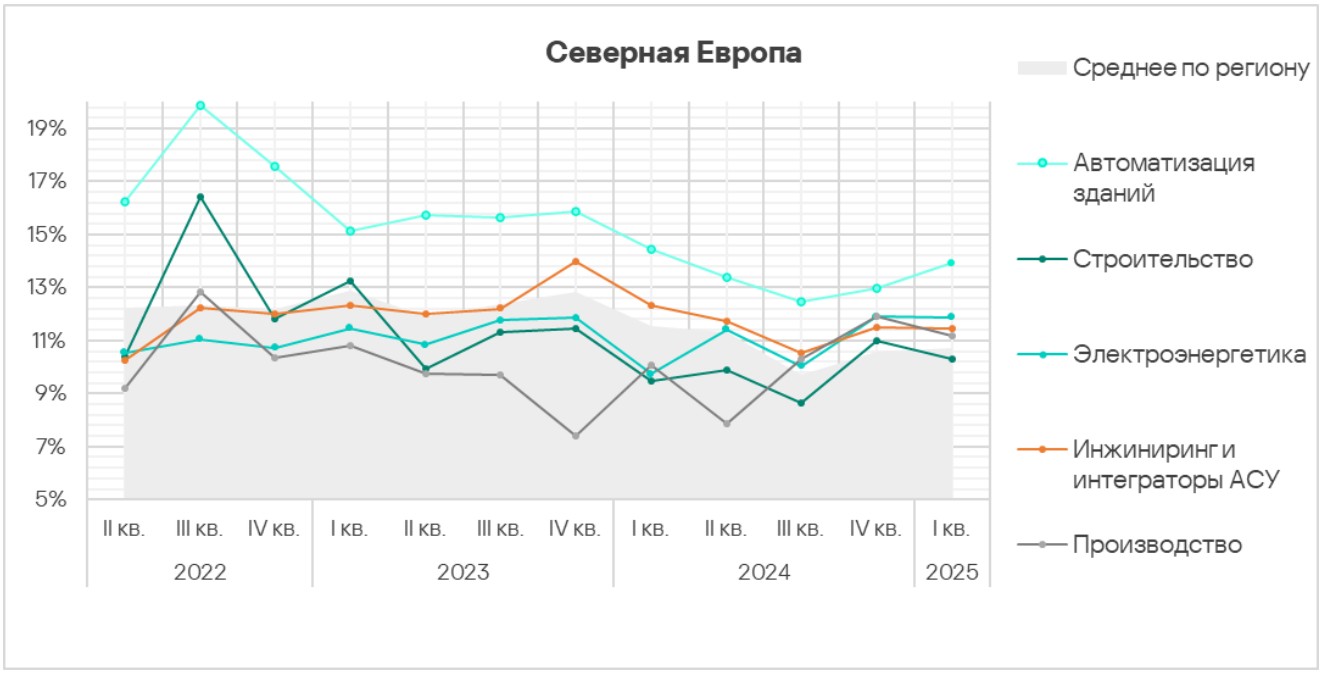
Показатели во всех отраслях региона по-прежнему остаются значительно ниже соответствующих **среднемировых значений.**



В первом квартале 2025 года из всех рассмотренных отраслей региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, **выросла** только у **автоматизации зданий** — в 1,1 раза.



Тренд **автоматизации зданий** остается заметно выше среднего регионального.



Методика подготовки статистики

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

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

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[1].

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

- серверы управления и сбора данных (SCADA);
- серверы автоматизации зданий;
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human machine interface (HMI);

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

- компьютеры, используемые для администрирования технологических сетей и сетей автоматизации зданий;
- компьютеры программистов АСУ/ПЛК.

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

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

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com