Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первый квартал 2025 года

15.05.2025

Версия 1.0

Цифры ... 3
Тенденции ... 4
Статистика по всем угрозам ... 8
Исследуемые отрасли ... 10
Разнообразие обнаруженных вредоносных объектов ... 12
Категории вредоносных объектов ... 14
Вредоносные объекты, используемые для первичного заражения ... 14
Ресурсы в интернете из списка запрещенных ... 14
Вредоносные документы (MSOffice + PDF) ... 17
Вредоносные скрипты и фишинговые страницы (JS и HTML) ... 19
Вредоносное ПО следующего этапа ... 22
Программы-шпионы ... 22
Программы-вымогатели ... 25
Майнеры — исполняемые файлы для ОС Windows ... 27
Веб-майнеры ... 30
Самораспространяющееся вредоносное ПО. Черви и вирусы ... 32
Черви ... 33
Вирусы ... 35
Вредоносные программы для AutoCAD ... 37
Основные источники угроз ... 40
Интернет ... 41
Почтовые клиенты ... 42
Съемные носители ... 44
Сетевые папки ... 46
Методика подготовки статистики ... 49

Цифры

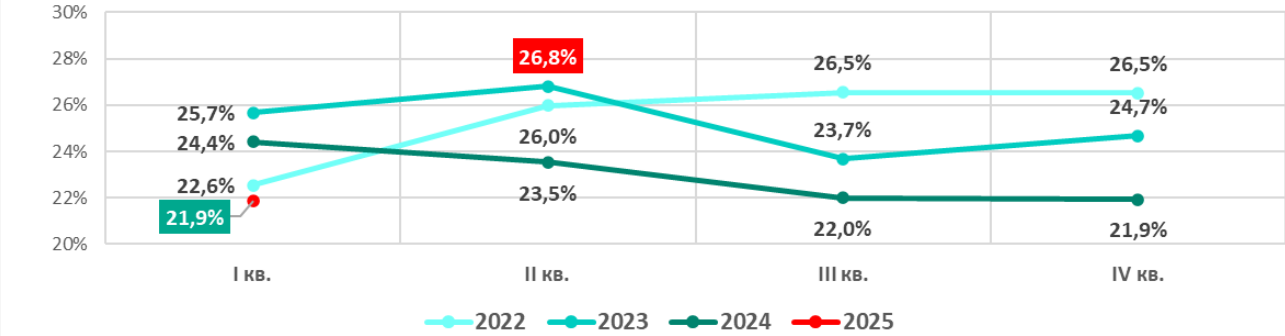
Показатель	IV кв. 2024	I кв. 2025	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	21,9%	21,9%	0 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	7,11%	7,16%	▲0,05 п. п.
Ресурсы в интернете из списка запрещенных	5,52%	5,12%	▼0,40 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	4,30%	4,20%	▼0,10 п. п.
Вредоносные документы (MSOffice + PDF)	1,71%	1,85%	▲0,14 п. п.
Вирусы (Virus)	1,61%	1,53%	▼0,08 п. п.
Черви (Worm)	1,37%	1,31%	▼0,06 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,70%	0,78%	▲0,08 п. п.
Веб-майнеры, выполняемые в браузерах	0,39%	0,53%	▲0,14 п. п.
Вредоносные программы для AutoCAD	0,38%	0,34%	▼0,04 п. п.
Программы-вымогатели	0,21%	0,16%	▼0,05 п. п.
Основные источники угроз			
Интернет	9,98%	10,11%	▲0,13 п. п.
Почтовые клиенты	2,72%	2,81%	▲0,09 п. п.
Съемные носители	0,64%	0,52%	▼0,12 п. п.
Сетевые папки	0,08%	0,07%	▼0,01 п. п.

Тенденции

От квартала к кварталу сохраняется относительная стабильность. Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, за квартал не изменилась и составила 21,9%. В последние три квартала этот показатель попадает в интервал от 22,0 до 21,9%.

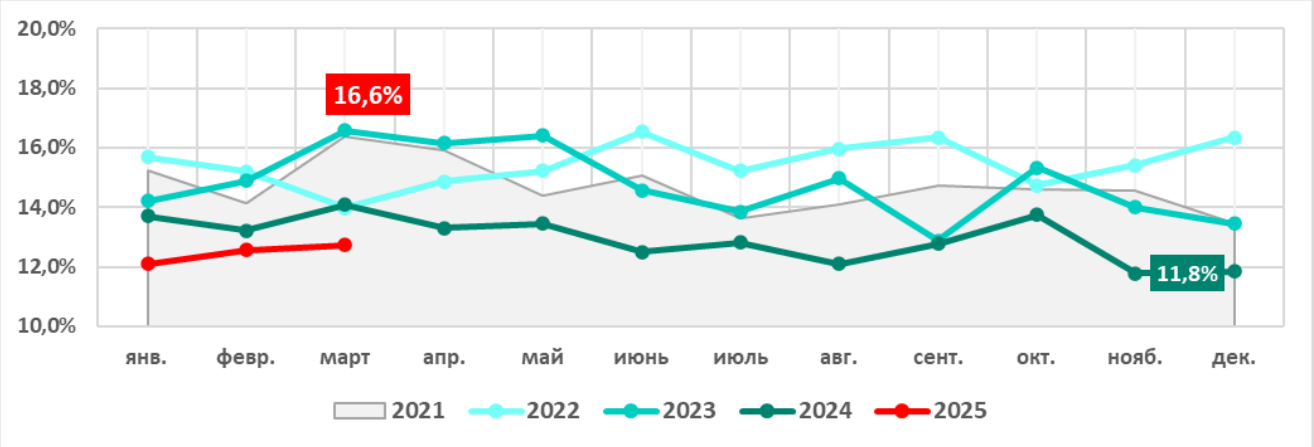
От года к году квартальные показатели уменьшаются. После второго квартала 2023 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты за квартал, была меньше аналогичного показателя предыдущего года.

Доля атакованных компьютеров АСУ в первом квартале 2025 года меньше, чем была в первом квартале 2024 года, на 2,5 п. п.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2022 года — I квартал 2025 года

С января по март 2025 года значения были наименьшими по сравнению со значениями в аналогичные месяцы предыдущих четырех лет.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2021 года — март 2025 года

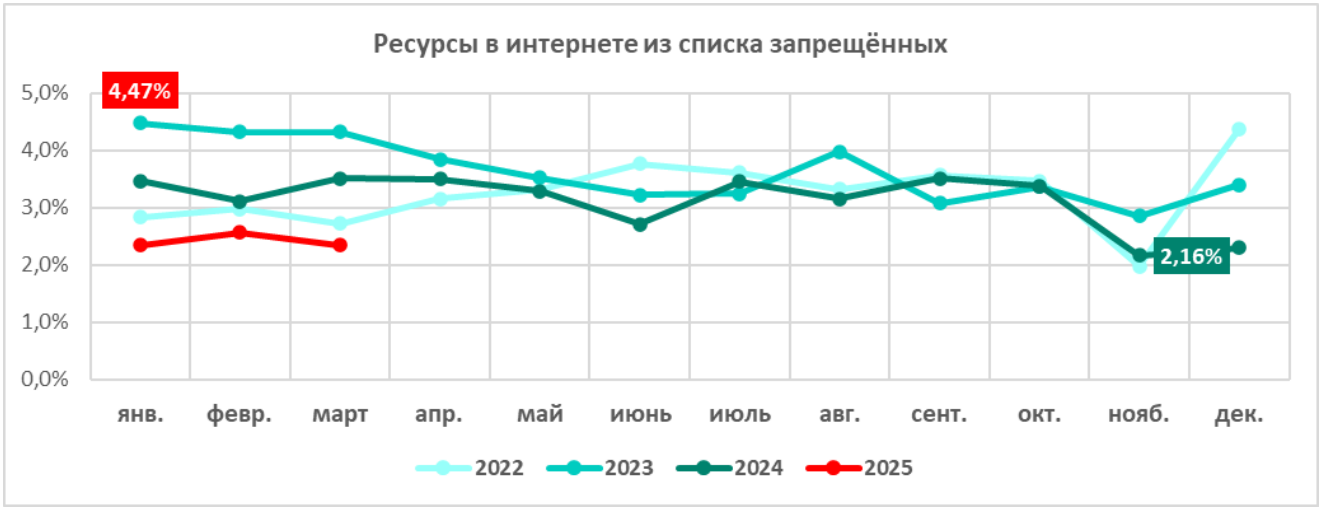
Биометрические системы по-прежнему лидируют среди исследуемых отраслей. Это единственный тип OT-инфраструктур, где доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась за квартал.

Сохраняются различия регионов. В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьировала от 10,7% в Северной Европе до 29,6% в Африке. У восьми регионов показатели попали в диапазон от 19% до 25%.

Уменьшается доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, снизилась в первом квартале 2025 года до наименьшего значения с 2022 года.

В первые три месяца 2025 года показатель был меньше, чем с января по март в предшествующие три года.



Доля компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, январь 2022 года — март 2025 года

Изменение показателей угроз первого этапа влияет на долю компьютеров АСУ, атакованных вредоносным ПО второго этапа

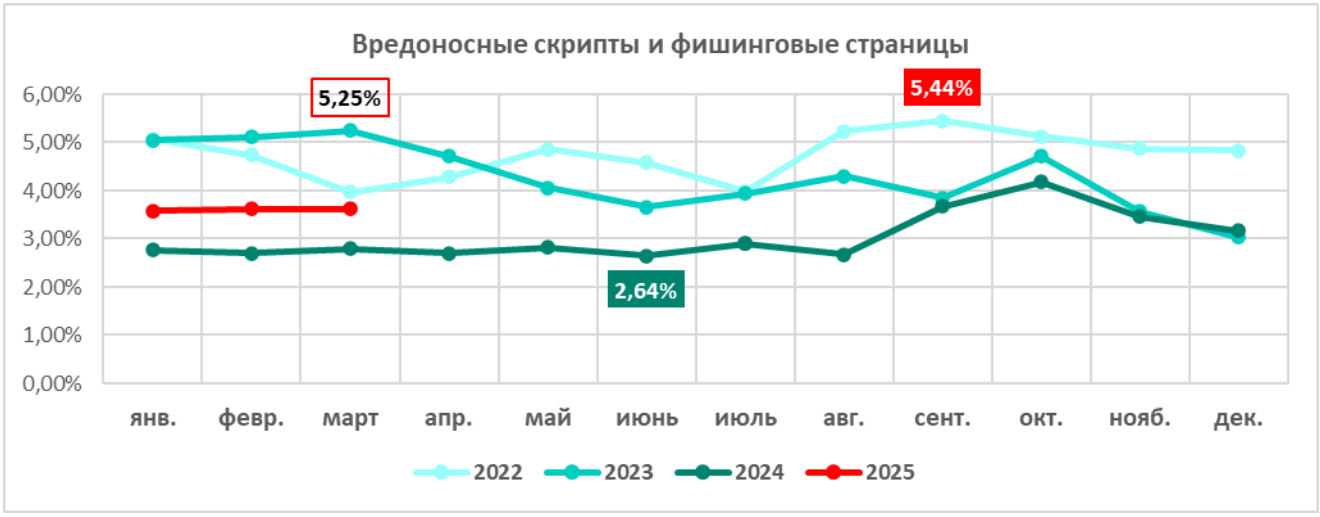
В первом квартале 2025 года впервые с начала 2023 года увеличилась доля компьютеров АСУ, на которых в течение квартала были заблокированы угрозы из интернета и угрозы, распространяемые через почту.

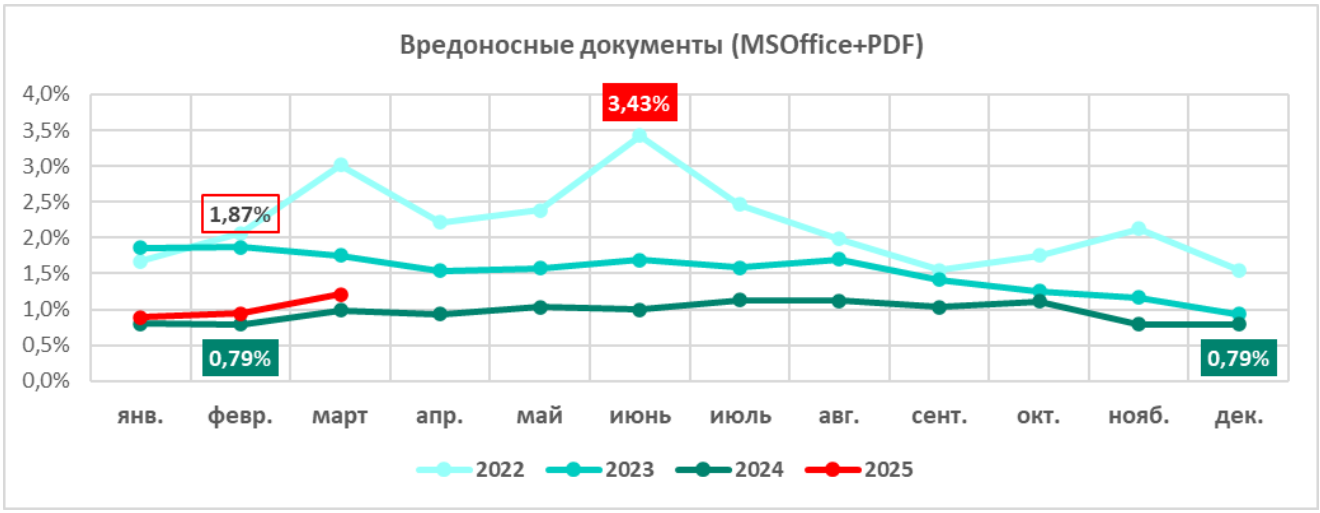
Интернет — главный источник угроз для компьютеров АСУ. Основные категории угроз из интернета, блокируемые на компьютерах АСУ, — это

интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы.

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

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы и вредоносные документы, за квартал увеличилась. С января по март 2025 года месячные значения этих двух категорий угроз оказались выше, чем в аналогичный период 2024 года.

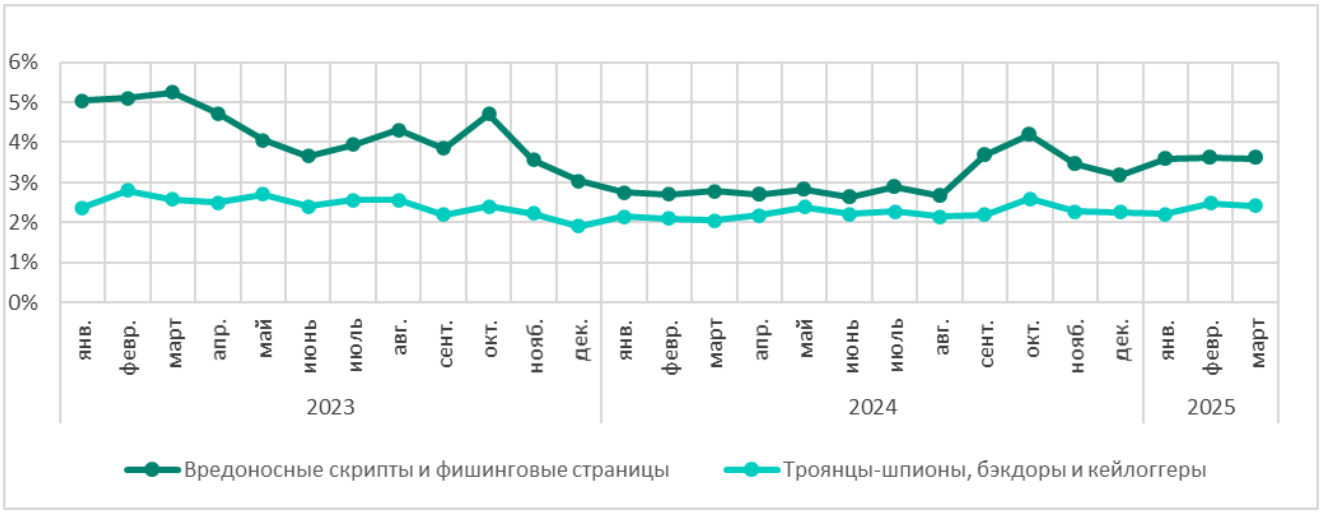




Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2022 года — март 2025 года

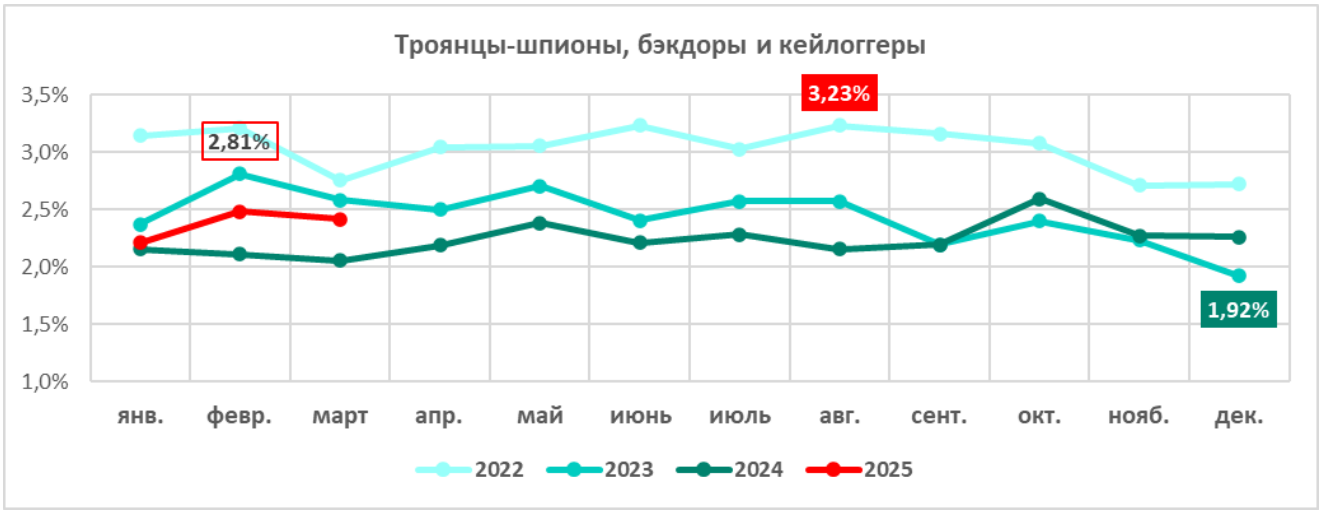
Лидирующая категория вредоносного ПО, используемого для первичного заражения компьютеров АСУ (см. ниже), — вредоносные скрипты и фишинговые страницы.

Большинство вредоносных скриптов и фишинговых страниц действуют как дропперы или загрузчики вредоносного ПО следующего этапа — шпионского ПО, криптомайнеров и программ-вымогателей. Сильная корреляция (r=0,705, p<0,001) между показателями для скриптов и фишинговых страниц и программ-шпионов хорошо видна на графике ниже.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года — март 2025 года

Показатели первых трех месяцев 2025 года у шпионских программ также, как и у вредоносных скриптов и фишинговых страниц, выше, чем с января по март 2024 года.



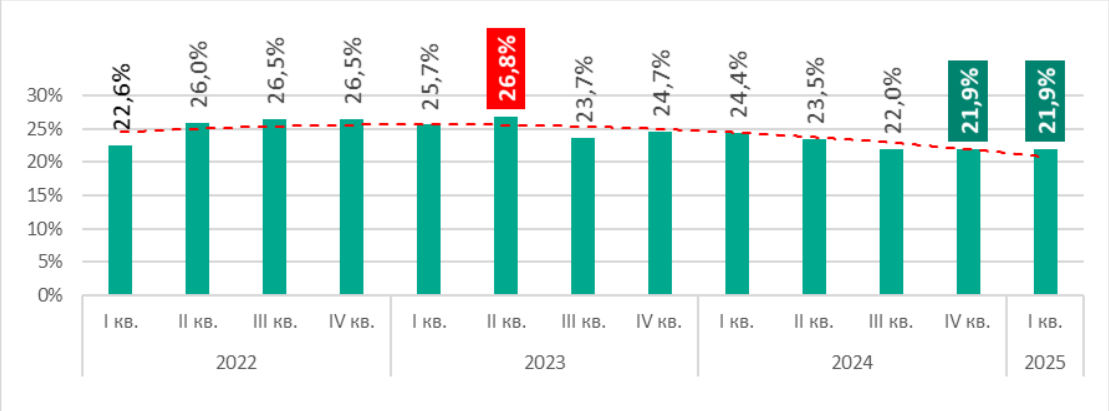
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2022 года — март 2025 года

Доля компьютеров АСУ, на которых были заблокированы майнеры (как веб-майнеры, так и майнеры — исполняемые файлы для ОС Windows), в первом квартале 2025 года также выросла.

Статистика по всем угрозам

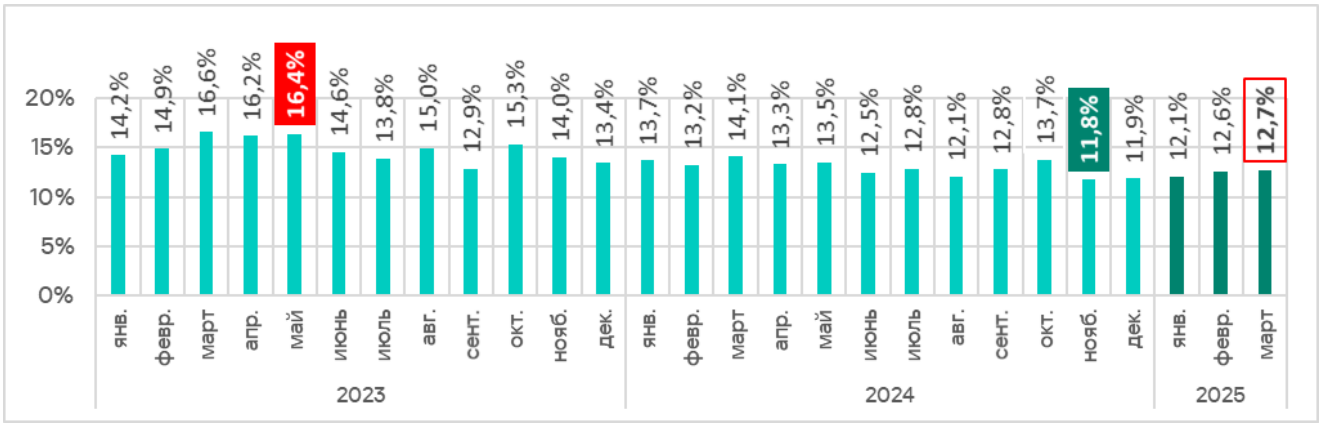
В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, не изменилась по сравнению с предыдущим кварталом и составила 21,9%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2022 года — I квартал 2025 года



В первом квартале 2025 года по сравнению с первым кварталом 2024 года доля атакованных компьютеров АСУ уменьшилась на 2,5 п. п.

От месяца к месяцу в течение первого квартала 2025 года этот показатель понемногу увеличивался и в марте достиг наибольшего значения за квартал.

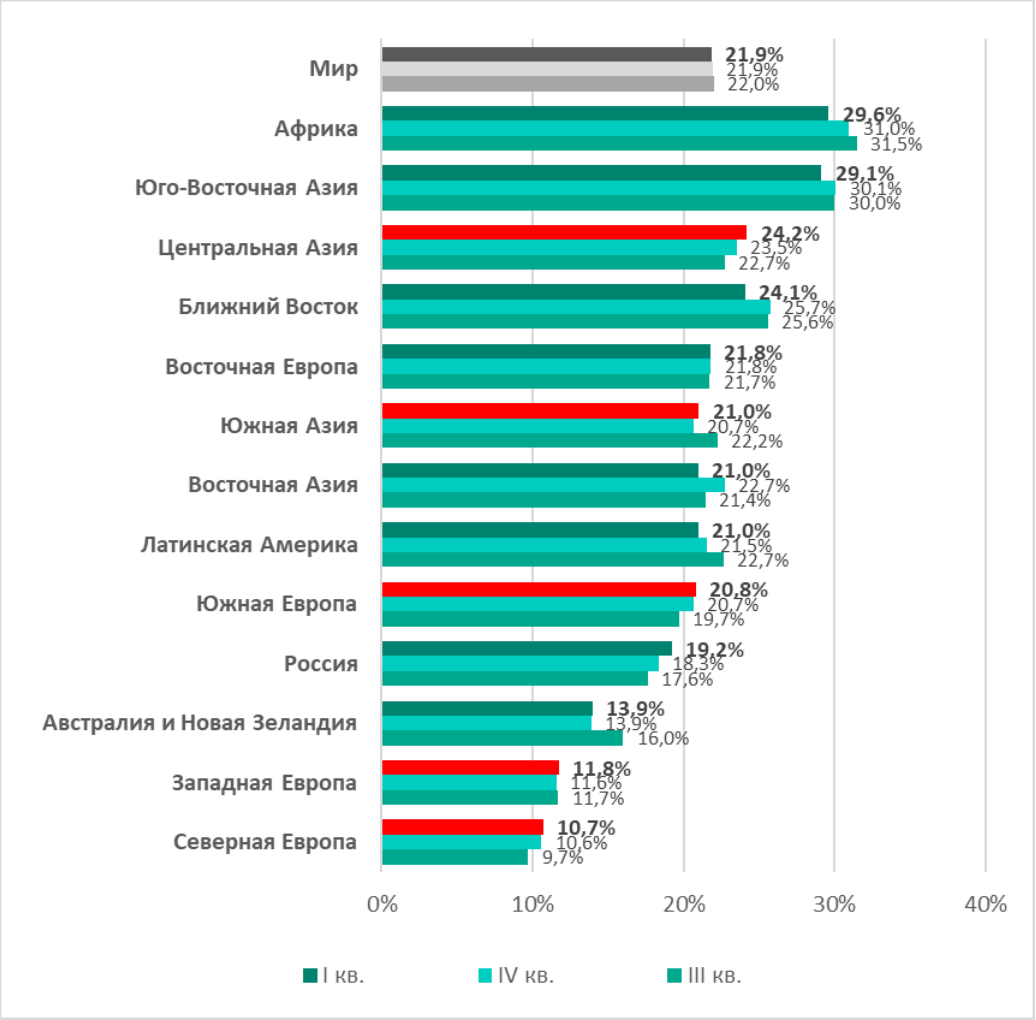


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года — март 2025 года

В регионах доля компьютеров АСУ, на которых в течение первого квартала 2025 года были заблокированы вредоносные объекты, варьирует от 10,7% в Северной Европе до 29,6% в Африке.

В шести из 13 регионов, рассматриваемых в этом отчете, показатели увеличились по сравнению с предыдущим кварталом, больше всего эта разница — в России.

Рейтинг регионов по доле атакованных компьютеров АСУ, I квартал 2025 года

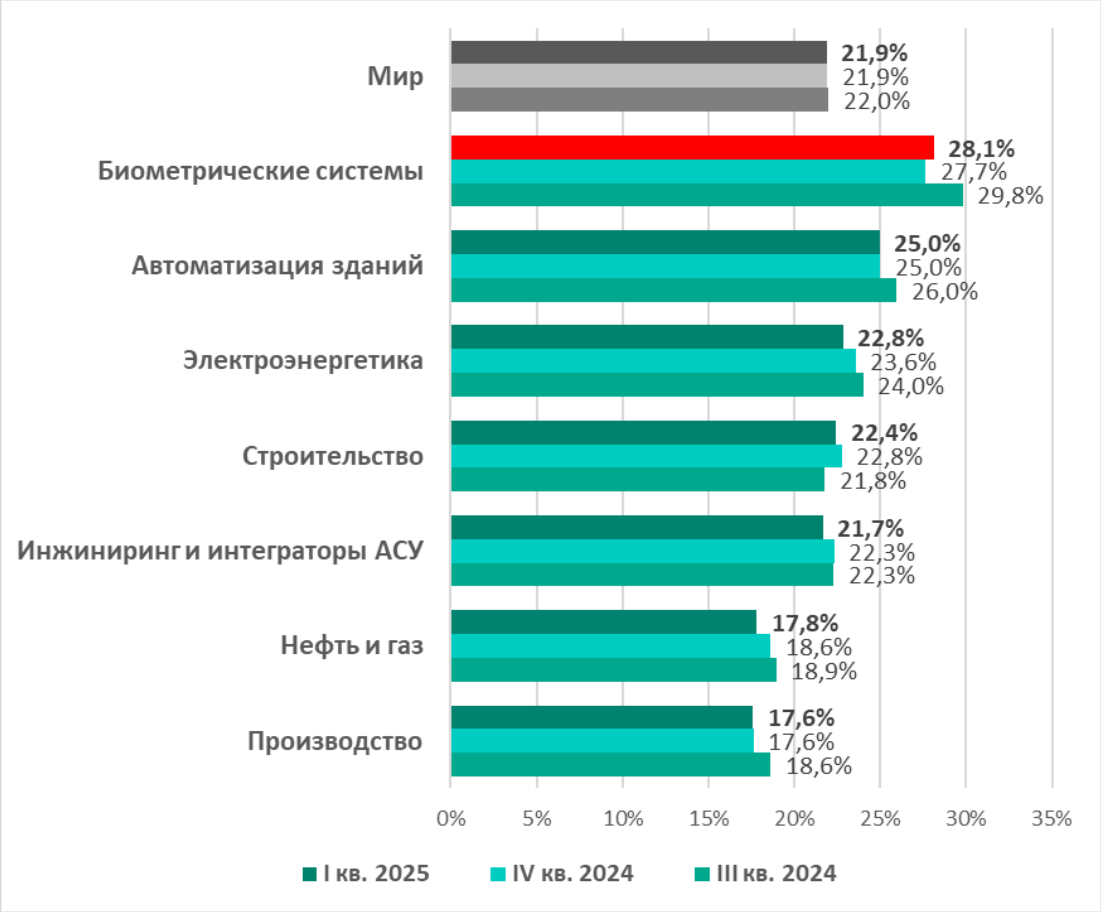


Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2025 года

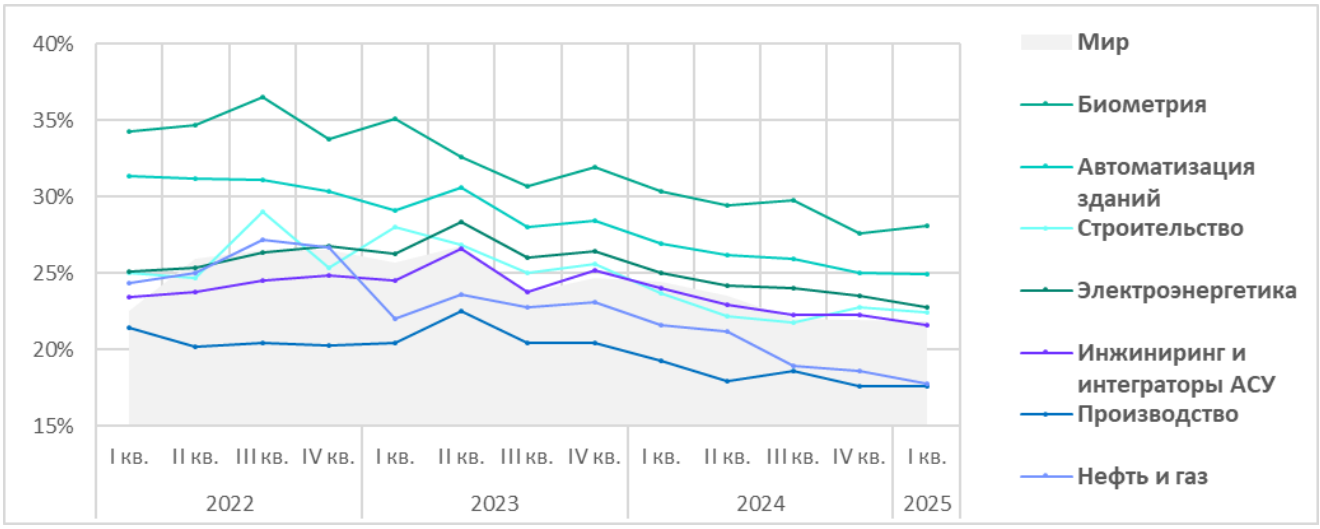
Исследуемые отрасли

В первом квартале 2025 года рейтинг исследуемых отраслей и типов OT-инфраструктур по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, снова возглавили биометрические системы.

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



Также биометрические системы оказались единственным из исследуемых типов инфраструктур, где доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, незначительно увеличилась, тем не менее демонстрируя в долгосрочной перспективе очевидный спад.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в исследуемых отраслях

Разнообразие обнаруженных вредоносных объектов

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

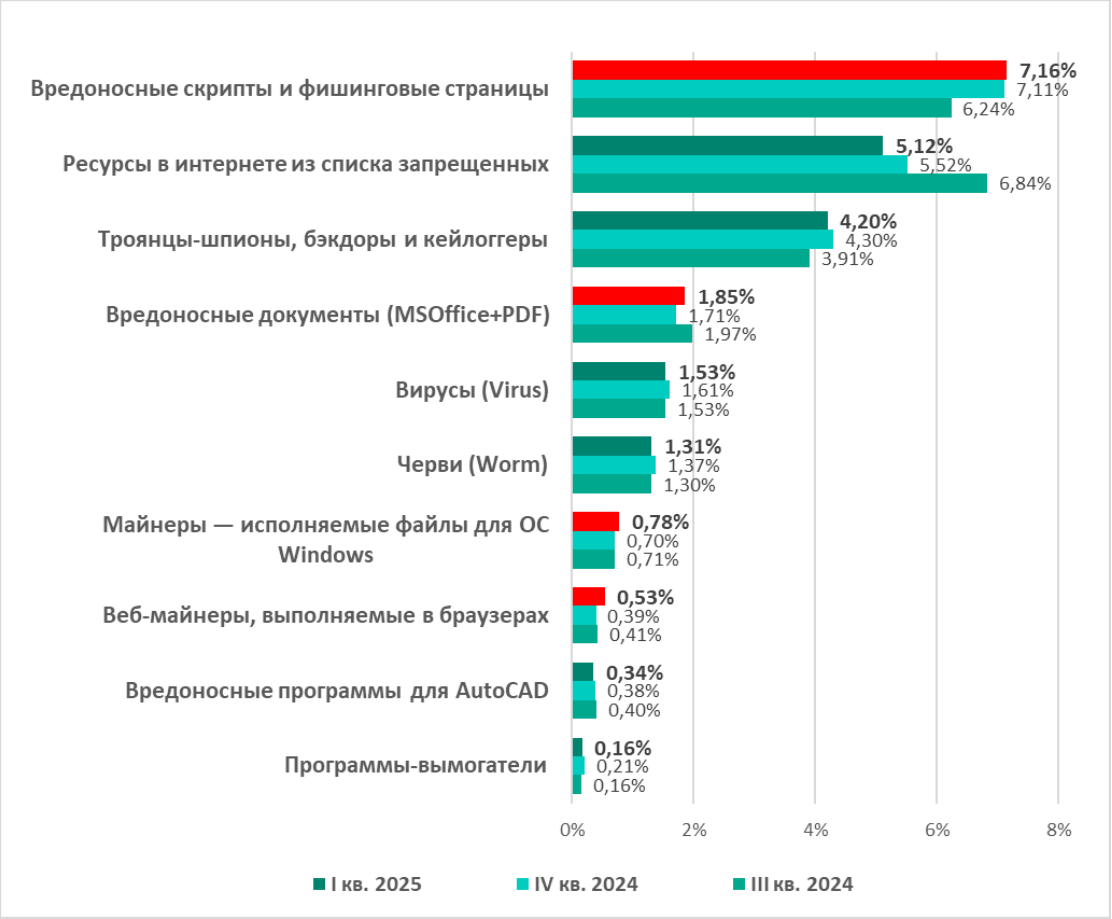
1. Вредоносные объекты, используемые для первичного заражения.
   Чаще всего, это ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вредоносные документы.
2. Вредоносное ПО следующего этапа.
   Как правило, это программы-шпионы, программы-вымогатели, майнеры — исполняемые 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.

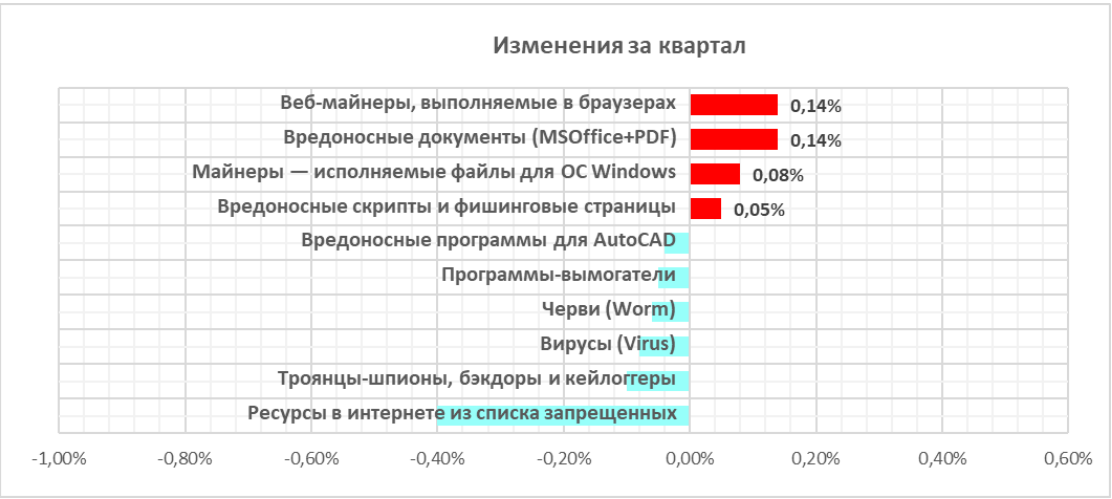
В первом квартале 2025 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 11 679 семейств, относящихся к различным категориям.

Вредоносные объекты для первичного заражения компьютеров АСУ активно используются злоумышленниками, в результате они чаще остальных блокируются защитными решениями. Это отражается и в нашей статистике: в мире и почти во всех регионах вредоносные скрипты и фишинговые страницы, а также интернет-ресурсы из списка запрещенных занимают первые места в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

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



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, I квартал 2025 года



Наиболее заметно в первом квартале 2025 года выросла доля компьютеров АСУ, на которых были заблокированы веб-майнеры (по отношению к показателю предыдущего квартала в 1,4 раза) и вредоносные документы (в 1,1 раза).

Категории вредоносных объектов

Типовые атаки, блокируемые в сети АСУ, представляют собой многоступенчатый процесс, где каждый последующий шаг злоумышленников направлен на повышение привилегий и получение доступа к другим системам путем эксплуатации проблем безопасности промышленных предприятий, в том числе технологических инфраструктур.

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

Вредоносные объекты, используемые для первичного заражения

Ресурсы в интернете из списка запрещенных

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 и фишинговых атак, а также 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), недостатках защиты от фишинга (многие вредоносные

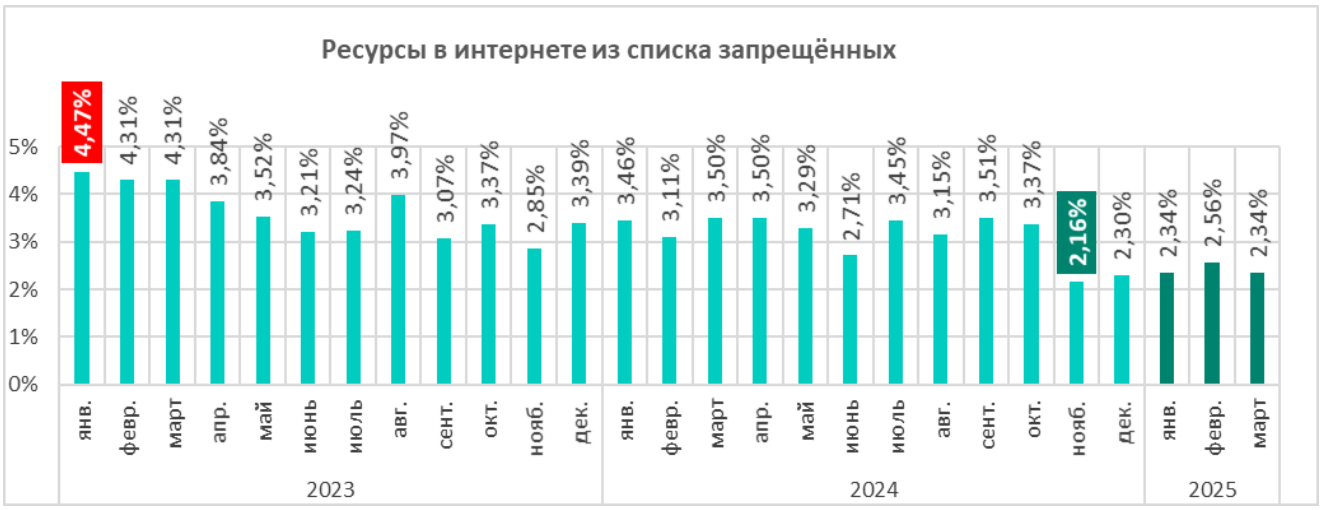
ссылки доставляются в фишинговых сообщениях) и недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным интернет-ресурсам и ссылкам из подозрительных писем и сообщений мессенджеров).

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, снизилась до наименьшего значения с 2022 года.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, I квартал 2022 года — I квартал 2025 года

В первые три месяца 2025 года доля компьютеров АСУ, на которых была заблокирована эта категория угроз, была меньше, чем с января по март в предшествующие три года.

На диаграмме ниже показано ежемесячное значение этого показателя за рассматриваемый период.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года — март 2025 года

На снижение доли вредоносных и потенциально опасных веб-ресурсов, которое мы наблюдаем с ноября 2024 года, вероятно, повлияли не только решительные меры по противодействию угрозам, реализуемые на различных уровнях, но и используемые злоумышленниками техники обхода блокировки по репутации ресурса — нагрузка по защите таким образом перераспределяется на другие технологии детектирования.

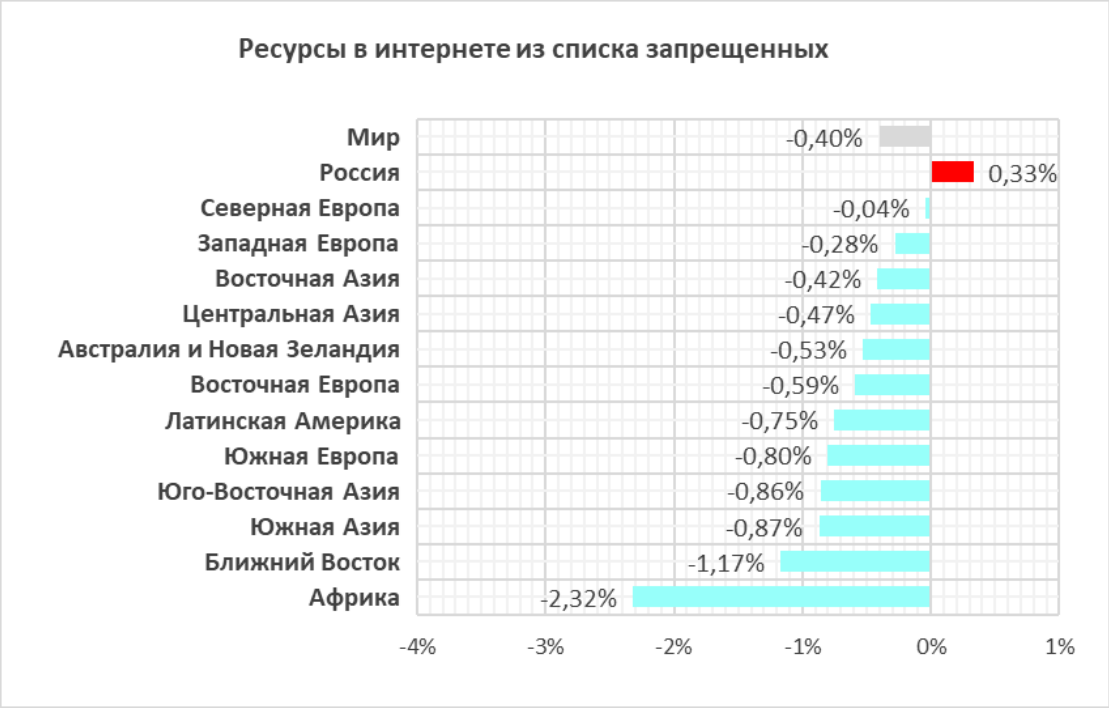
Обнаруженный опасный интернет-ресурс не всегда может быть добавлен в список запрещенных, поскольку злоумышленники все чаще используют легитимные интернет-ресурсы и сервисы, например платформы доставки контента (CDN), мессенджеры и облачные хранилища. Подобные сервисы позволяют распространять вредоносный код по уникальным ссылкам на уникальный контент, затрудняя таким образом тактики блокировки по репутации. Настоятельно рекомендуем промышленным организациям предусмотреть блокировку подобных сервисов политикой, как минимум, для технологических сетей, где необходимость в таких сервисах крайне редко бывает обусловлена объективными причинами.

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

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, I квартал 2025 года

Показатель уменьшился во всех регионах, за исключением России.

Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, I квартал 2025 года

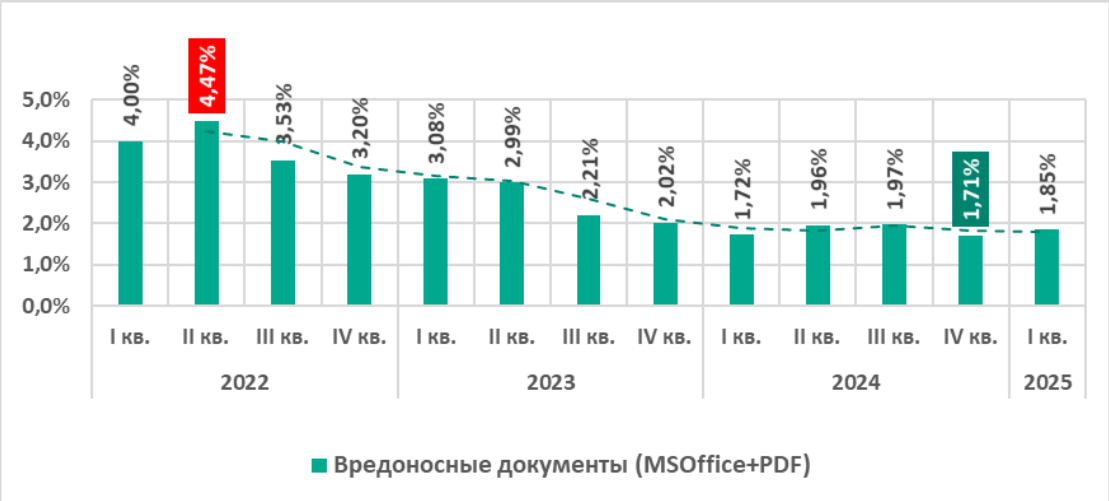


Вредоносные документы (MSOffice + PDF)

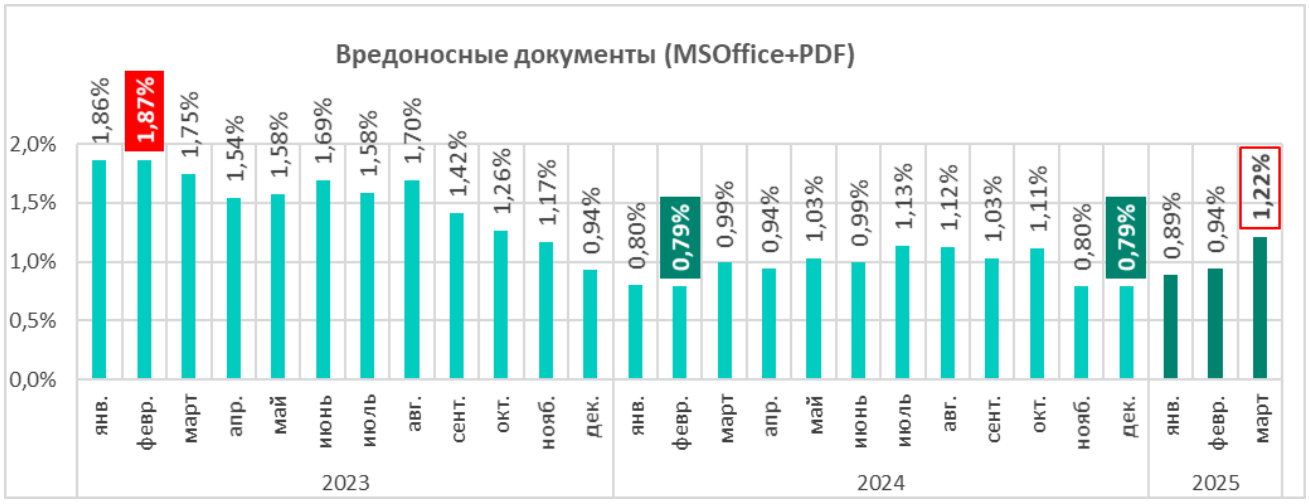
Вредоносные документы злоумышленники преимущественно рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

В первом квартале 2025 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, увеличилась по сравнению с предыдущим кварталом.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, I квартал 2022 года — I квартал 2025 года



В конце 2024 года показатели по этой категории угроз были наименьшими за два года — и за квартал, и за месяц (за исключением февраля 2024 года). В марте 2025 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, оказалась максимальной с ноября 2023 года.



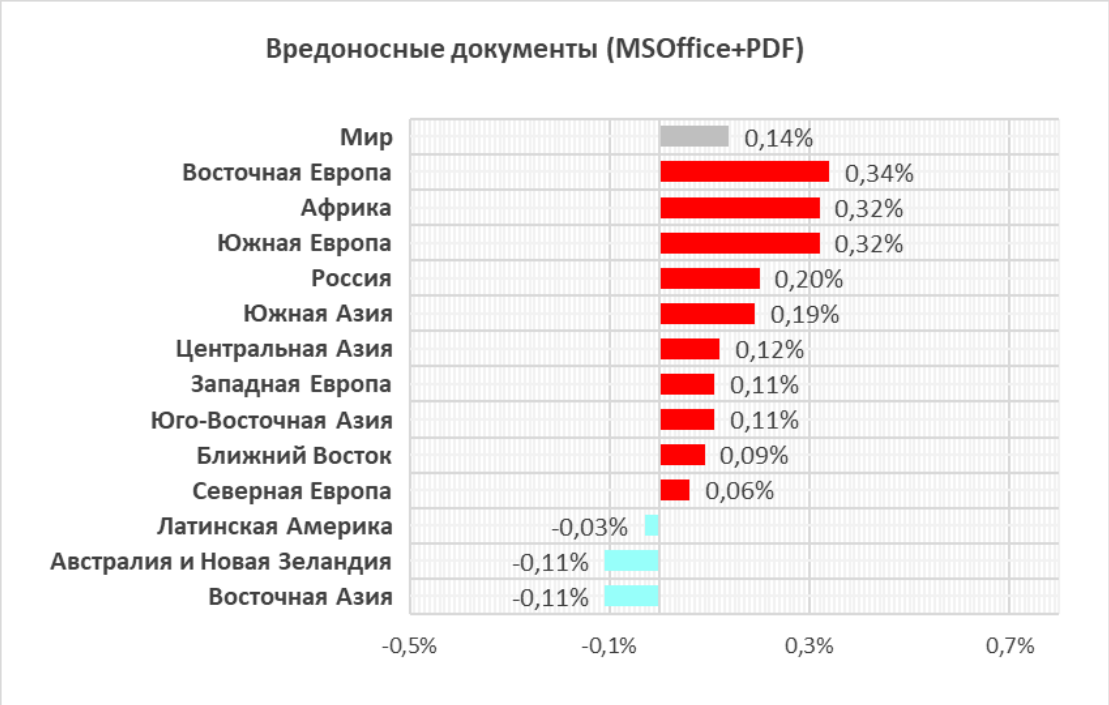
Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, январь 2023 года — март 2025 года

В тройку лидеров по этому показателю вошли: Южная Европа, Латинская Америка и Ближний Восток.

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

В тройку лидеров по росту доли компьютеров АСУ, на которых были обнаружены вредоносные документы, вошли: Восточная Европа, Африка и Южная Европа.

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

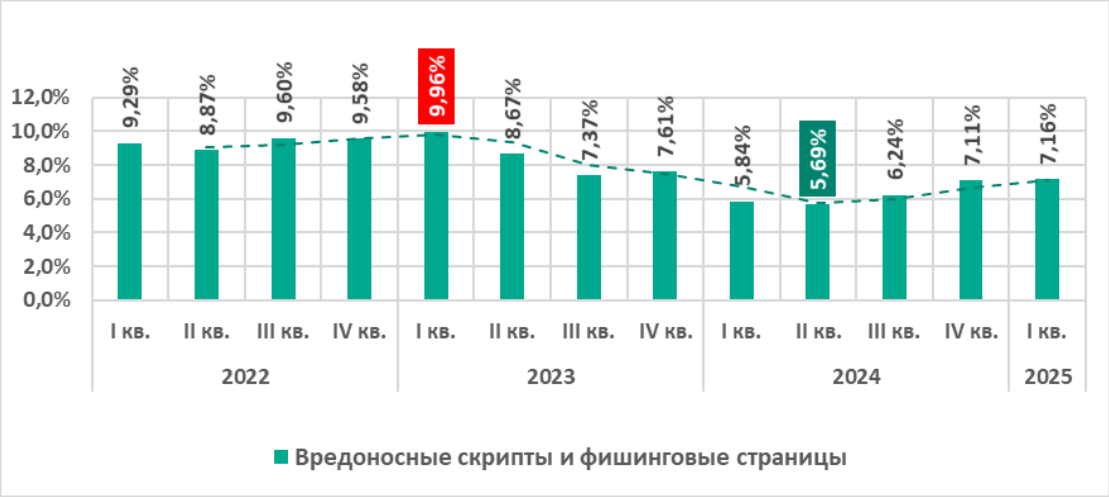


Вредоносные скрипты и фишинговые страницы (JS и HTML)

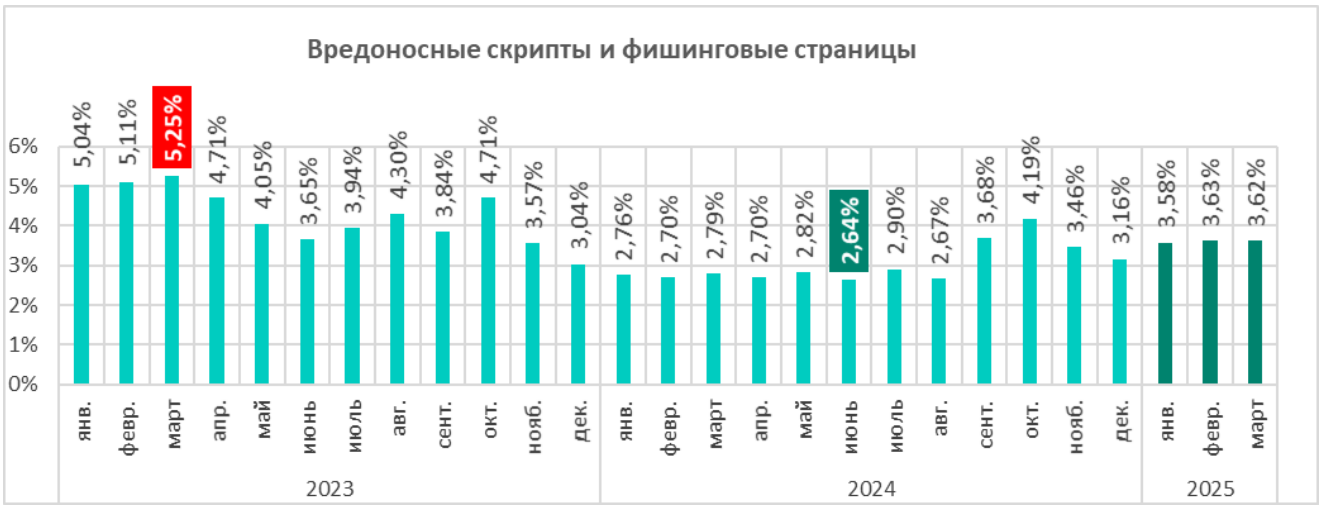
Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для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

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, немного увеличилась.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, I квартал 2022 года — I квартал 2025 года



Ежемесячное значение этого показателя с января по март 2025 года колебалось в пределах 3,58–3,62%. Эти значения оказались выше, чем в аналогичный период 2024 года.



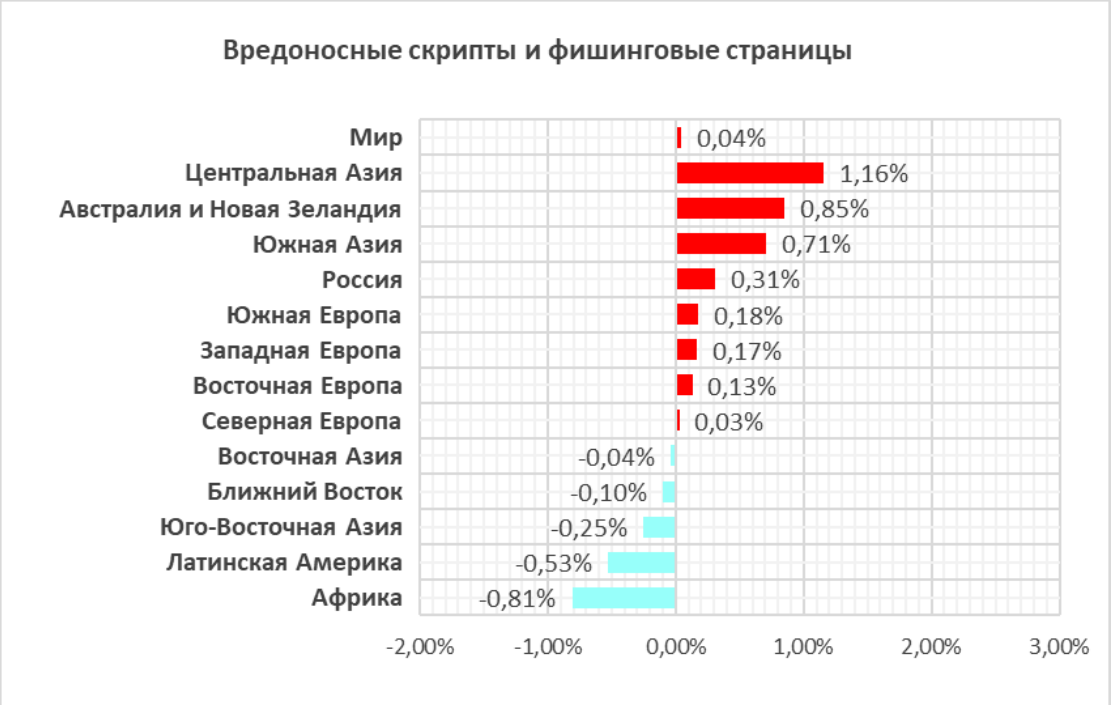
Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, январь 2023 года — март 2025 года

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

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

Тройку лидеров по росту этого показателя составляют Центральная Азия, Австралия и Новая Зеландия, Южная Азия.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, I квартал 2025 года



Вредоносное ПО следующего этапа

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

Программы-шпионы

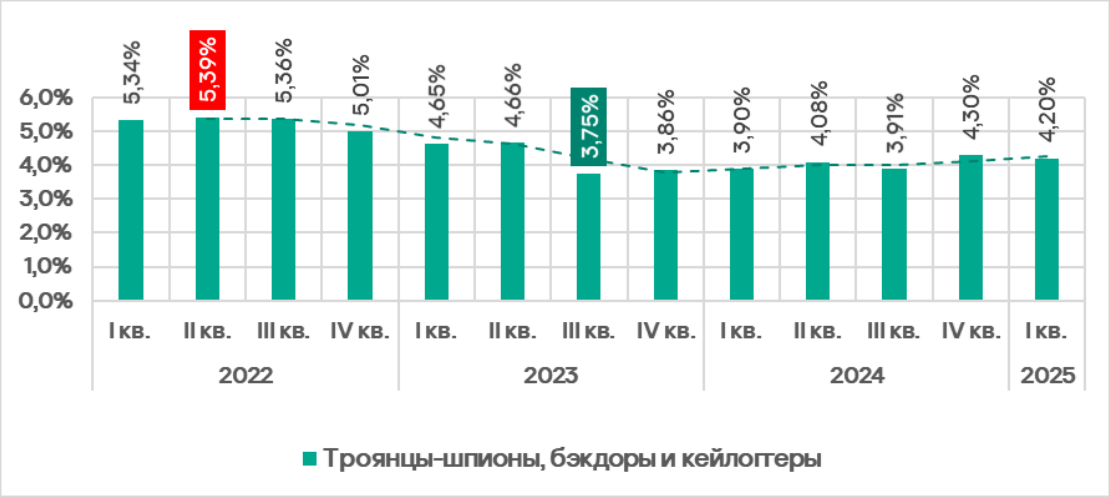
Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО (троянцы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструментарий промежуточных этапов кибератаки (например, разведки и распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных. В большинстве случаев конечная цель атак с применением такого ПО — кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

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.

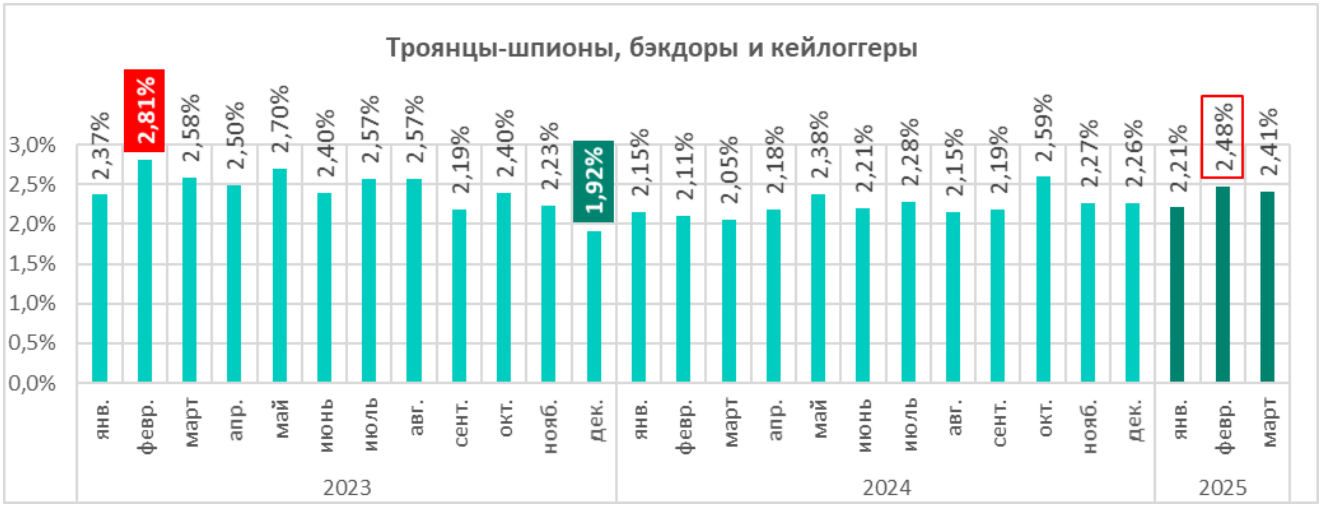
Обнаружение шпионского ПО на компьютере АСУ обычно указывает на то, что вектор первоначального заражения сработал, будь то переход по вредоносной ссылке, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует об отсутствии или о неэффективности мер защиты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

В первом квартале 2025 года доля компьютеров АСУ, на которых было заблокировано шпионское ПО, уменьшилась по сравнению с предыдущим кварталом.

Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, I квартал 2022 года — I квартал 2025 года



Наибольшее месячное значение за первый квартал 2025 года было отмечено в феврале.



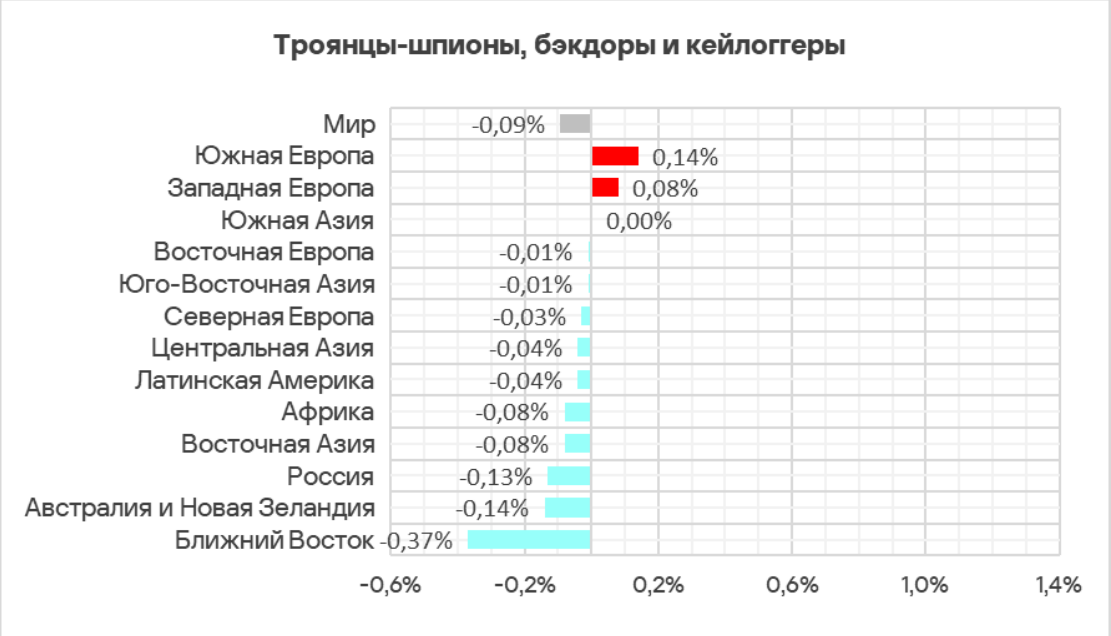
Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, январь 2023 года — март 2025 года

В первом квартале 2025 года в топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, вошли Африка, Южная Европа и Ближний Восток. Эти регионы также лидируют по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы.

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

За квартал доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла в Южной и в Западной Европе.

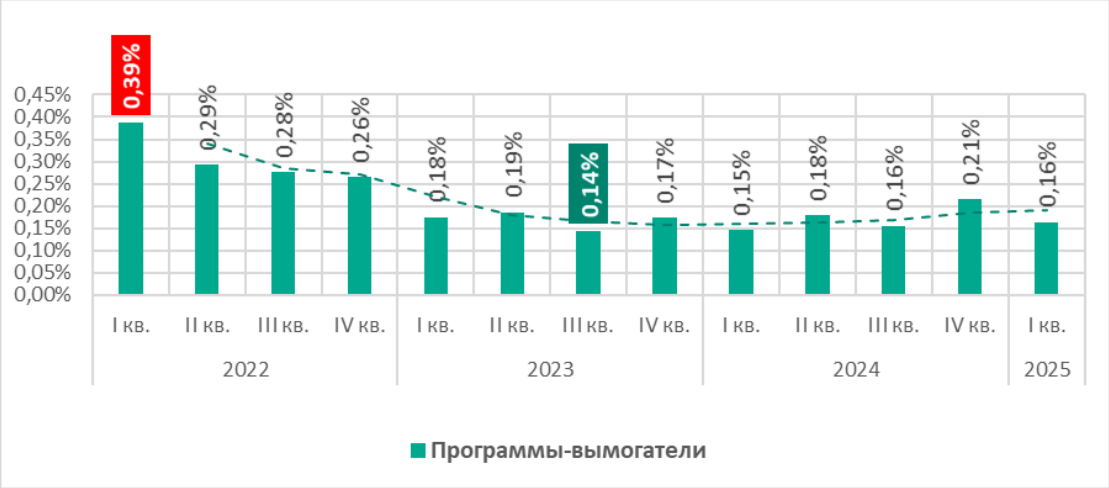
Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, I квартал 2025 года



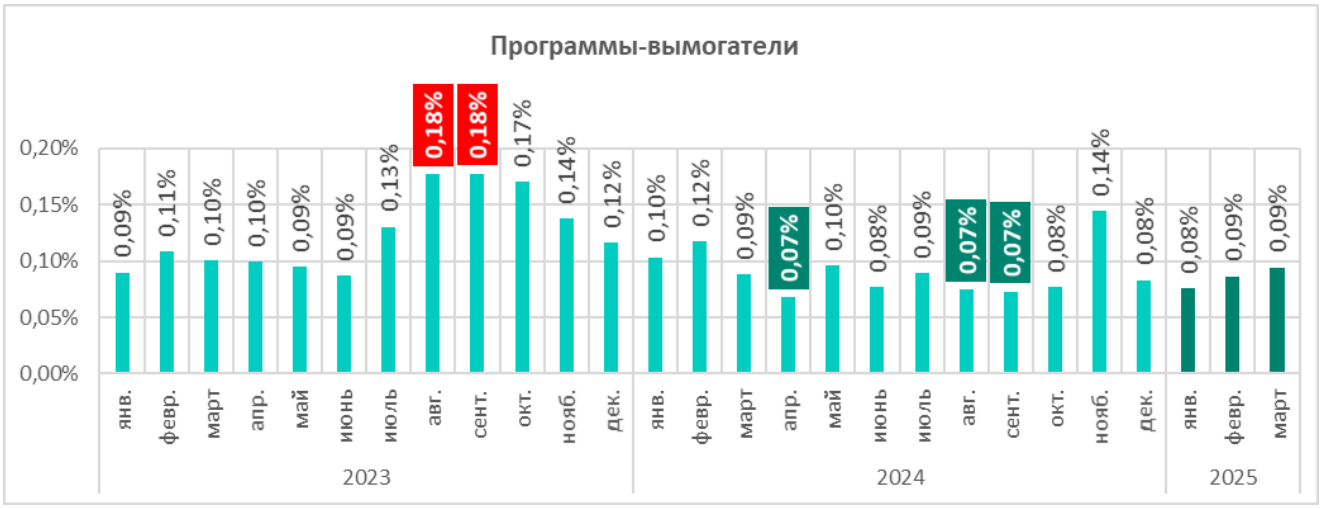
Программы-вымогатели

После роста в конце 2024 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, уменьшилась.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, I квартал 2022 года — I квартал 2025 года



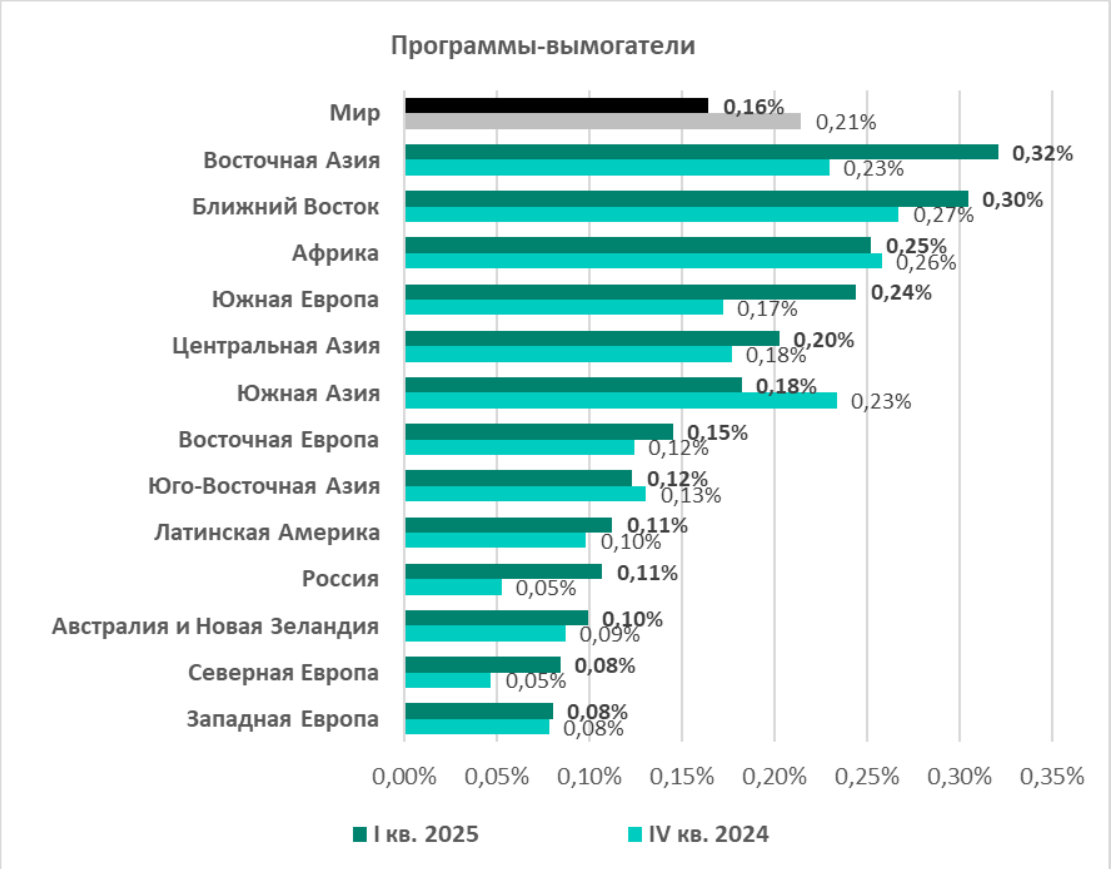
Показатели в первые три месяца 2025 года незначительно увеличивались.



Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь 2023 года — март 2025 года

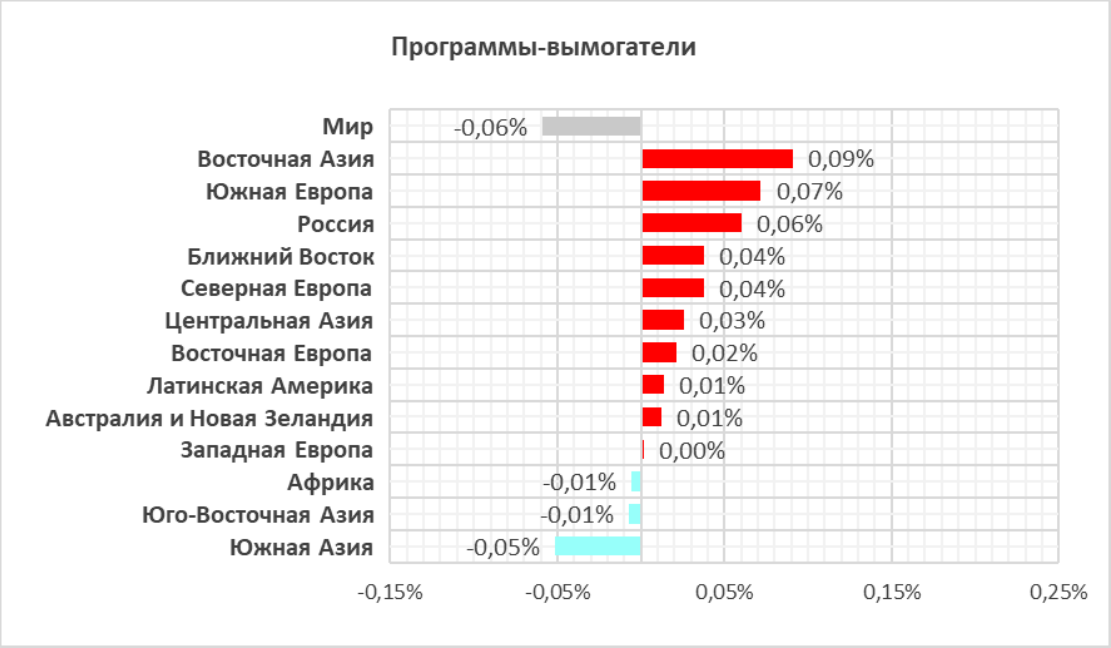
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели: Восточная Азия, Ближний Восток, Африка.

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



Тройку лидеров по росту этого показателя составляют Восточная Азия, Южная Европа, Россия.

Изменение доли компьютеров АСУ, на которых были заблокированы программы-вымогатели, I квартал 2025 года



Майнеры — исполняемые файлы для ОС Windows

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.

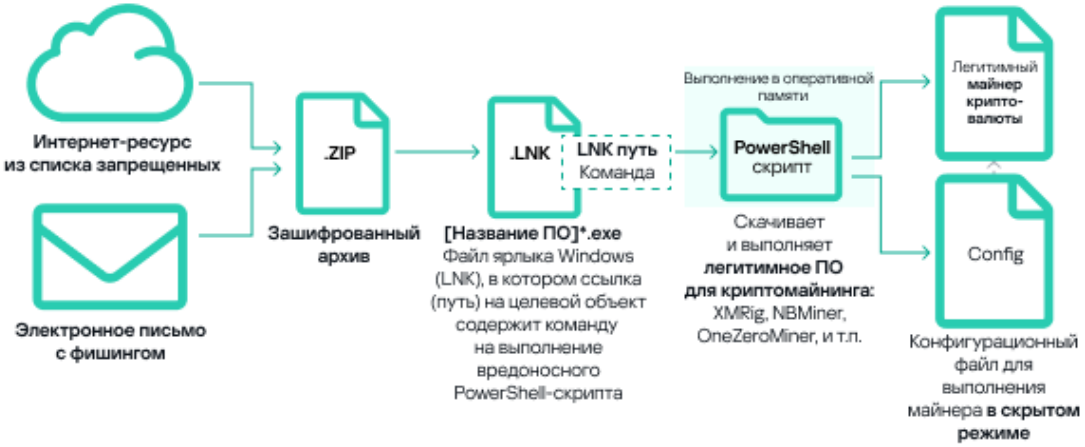
Значительная часть майнеров для ОС Windows, обнаруженных на компьютерах АСУ, представляет собой архивы, названия которых имитировали легальное программное обеспечение. Эти архивы не содержат реального программного обеспечения, но включают в себя файл формата Windows LNK, более известный как ярлык. Однако 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

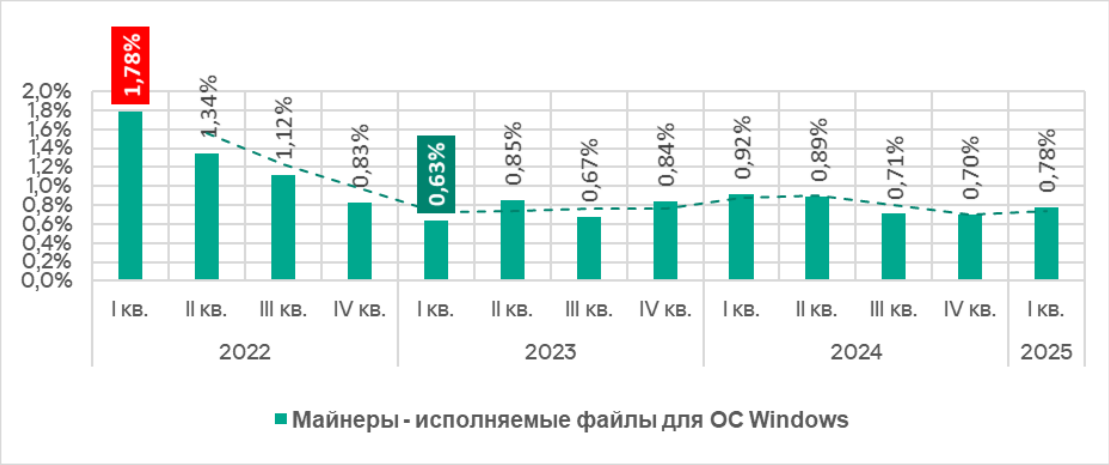
со специфическими файлами конфигурации, позволяющими скрыть активность майнера от пользователя.

Цепочка атаки: пример с использованием легитимных крипто-майнеров

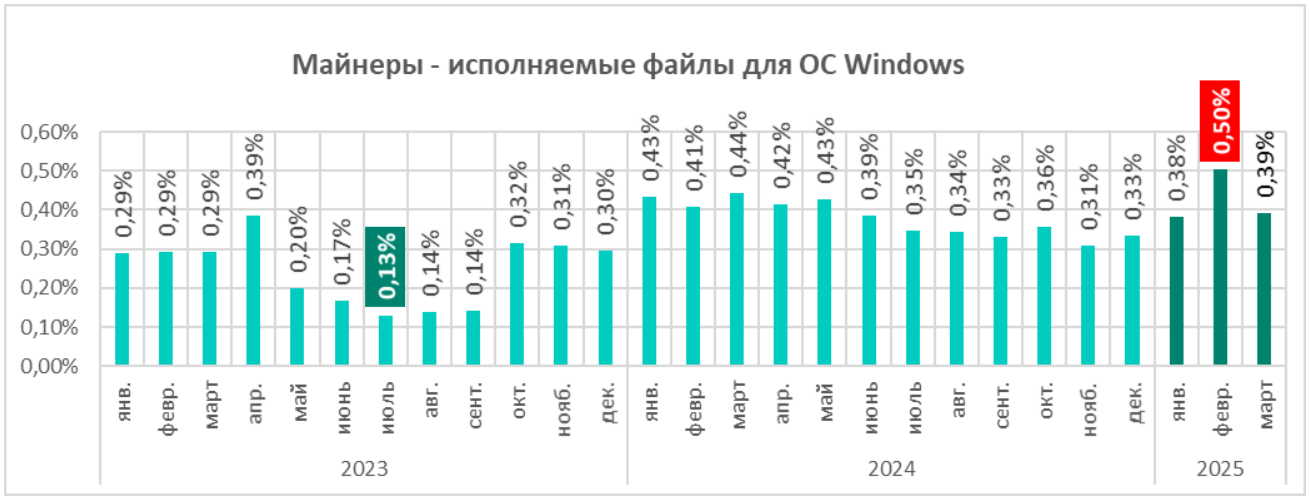


В первом квартале 2025 года доля компьютеров АСУ, на которых были выявлены майнеры в формате исполняемых файлов для Windows, увеличилась.

Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2022 года — I квартал 2025 года



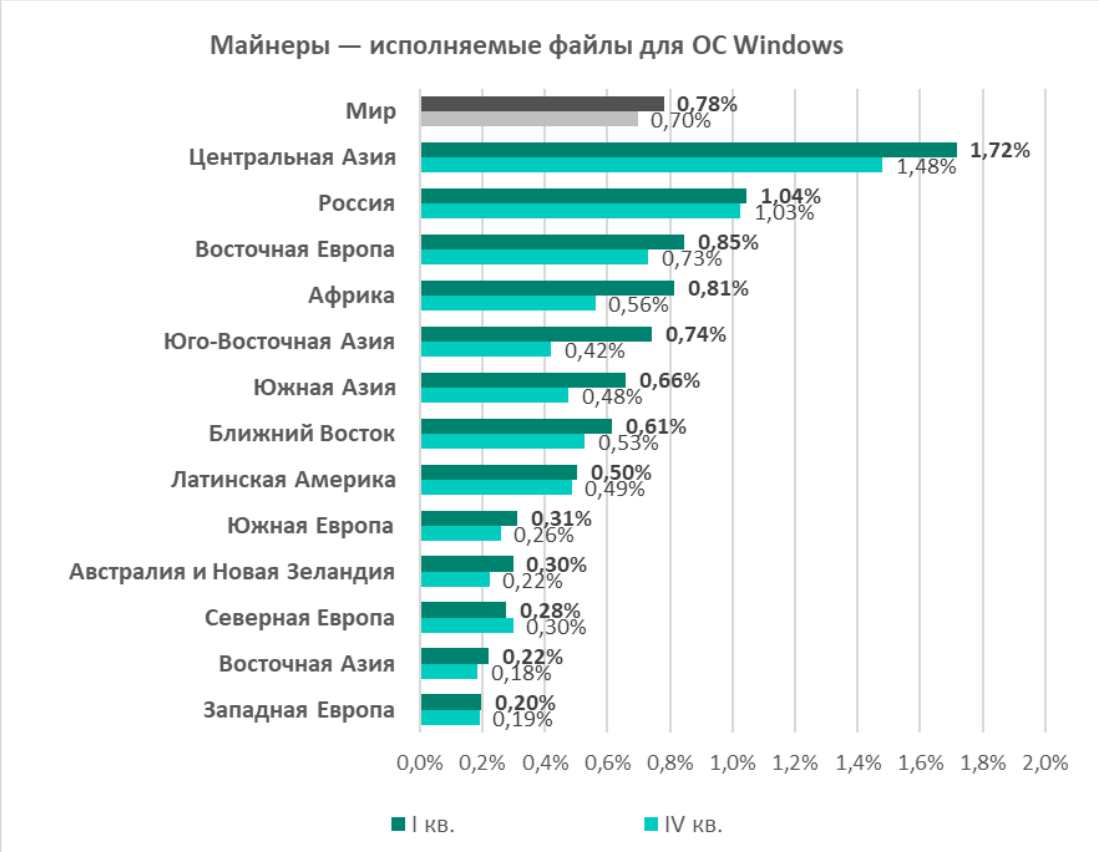
В феврале 2025 года показатель вырос до максимального с января 2023 года месячного значения.



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, январь 2023 года — март 2025 года

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

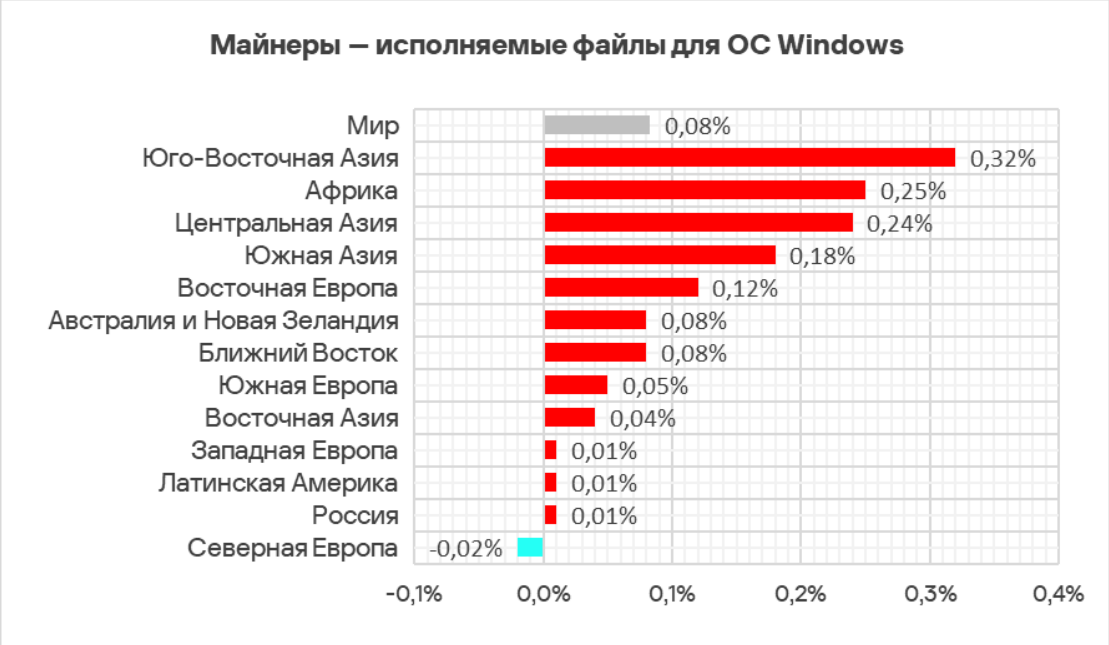
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2025 года



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, в первом квартале 2025 года выросла

почти во всех регионах. Лидерами по росту этого показателя стали Юго-Восточная Азия, Африка и Центральная Азия.

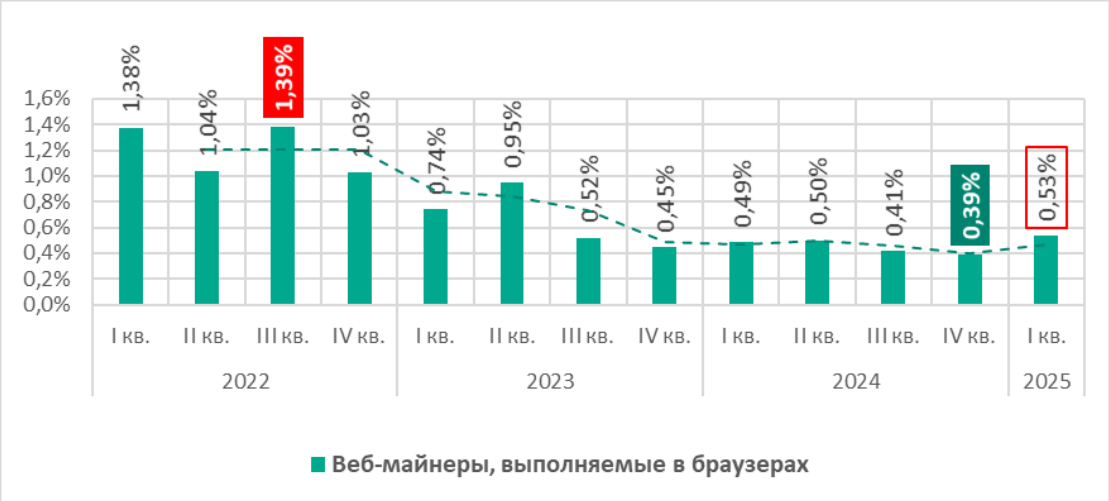
Изменение доли компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2025 года



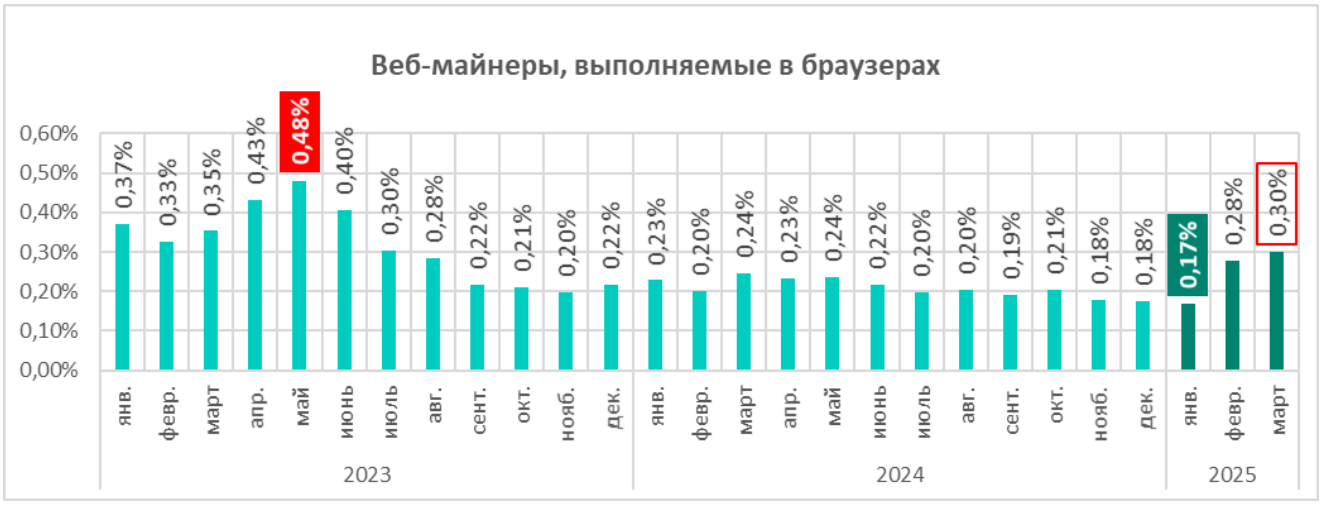
Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, в первом квартале 2025 года увеличилась до значения, максимального с третьего квартала 2023 года.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, I квартал 2022 года — I квартал 2025 года



Месячный показатель, уменьшившись в январе до минимума с 2023 года, за два месяца вырос и достиг максимального с июля 2023 года значения.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года — март 2025 года

Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах: Африка, Юго-Восточная Азия, Восточная Европа.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, I квартал 2025 года

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, выполняемые в браузерах, I квартал 2025 года

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.

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

Среди распространяющихся вирусов и червей довольно много старых, их командные серверы уже отключены. Тем не менее, 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.

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

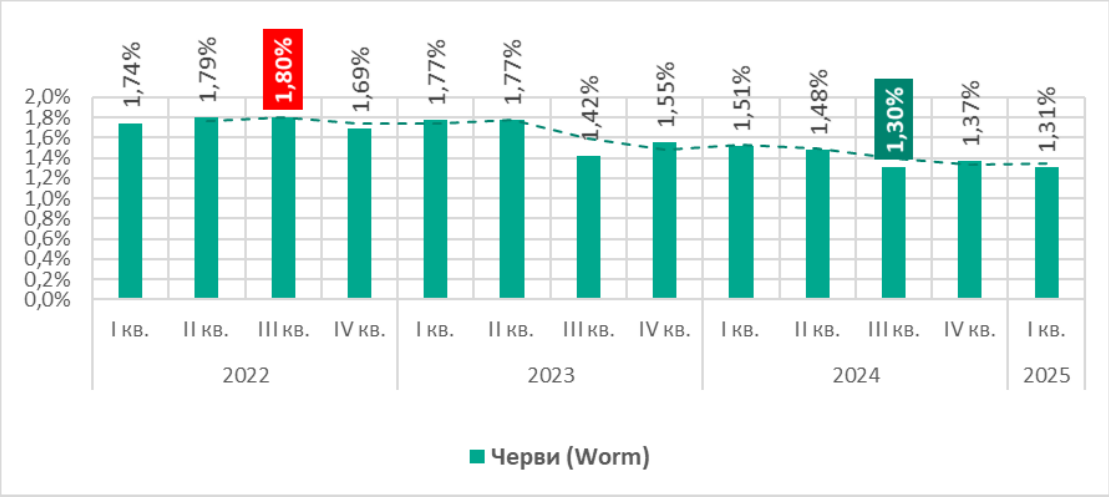
становятся источниками распространения вредоносного ПО. Ситуацию может ухудшать и слабая сегментация сети предприятия, и отсутствие контроля использования съемных носителей информации.

Черви

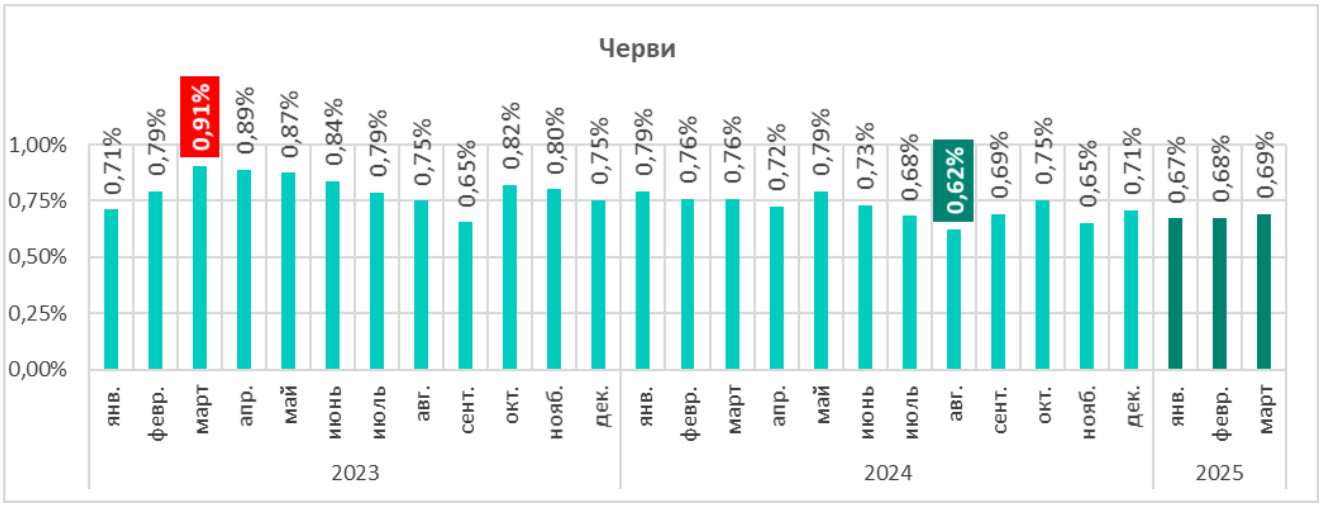
В сетях АСУ встречаются новые версии червей, используемые злоумышленниками для распространения шпионского ПО, программ-вымогателей и майнеров. Чаще всего эти черви используют эксплойты известных уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

Доля компьютеров АСУ, на которых были заблокированы черви, уменьшилась в первом квартале 2025 года.

Доля компьютеров АСУ, на которых были заблокированы черви, I квартал 2022 года — I квартал 2025 года



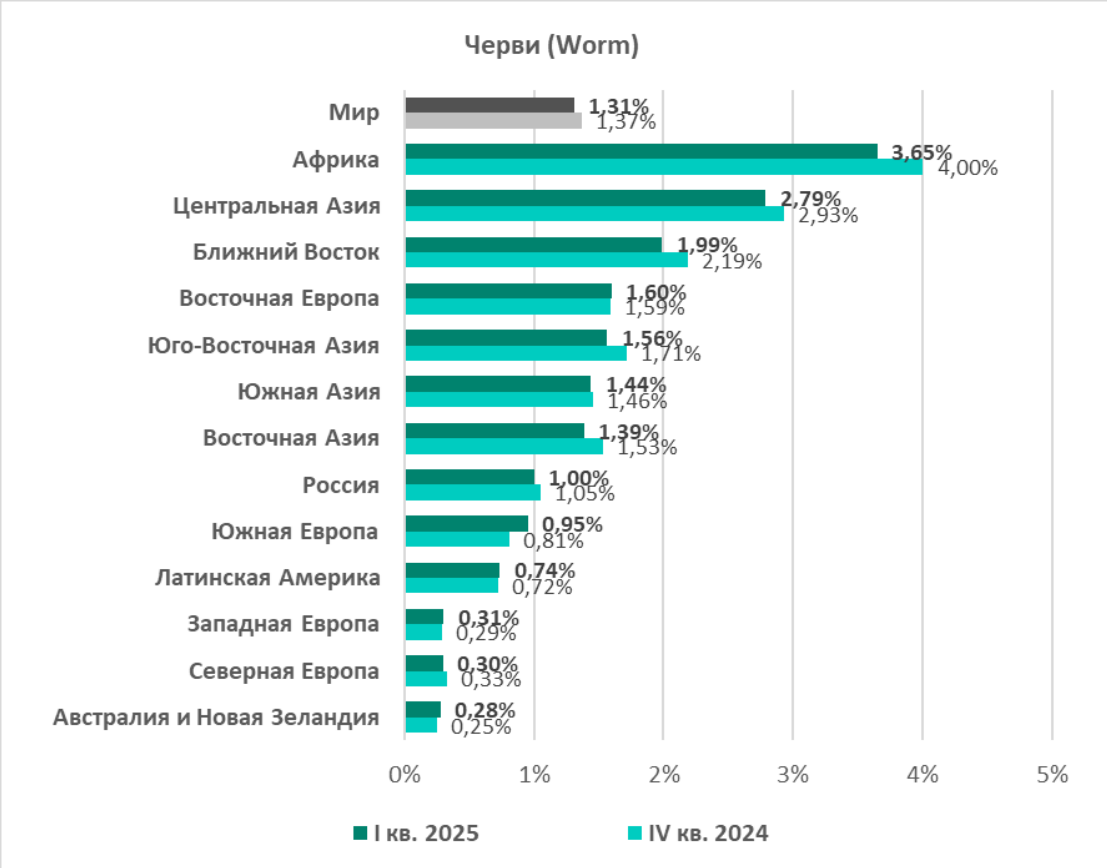
При этом в течение квартала показатель немного увеличивался от месяца к месяцу.



Доля компьютеров АСУ, на которых были заблокированы черви, январь 2023 года — март 2025 года

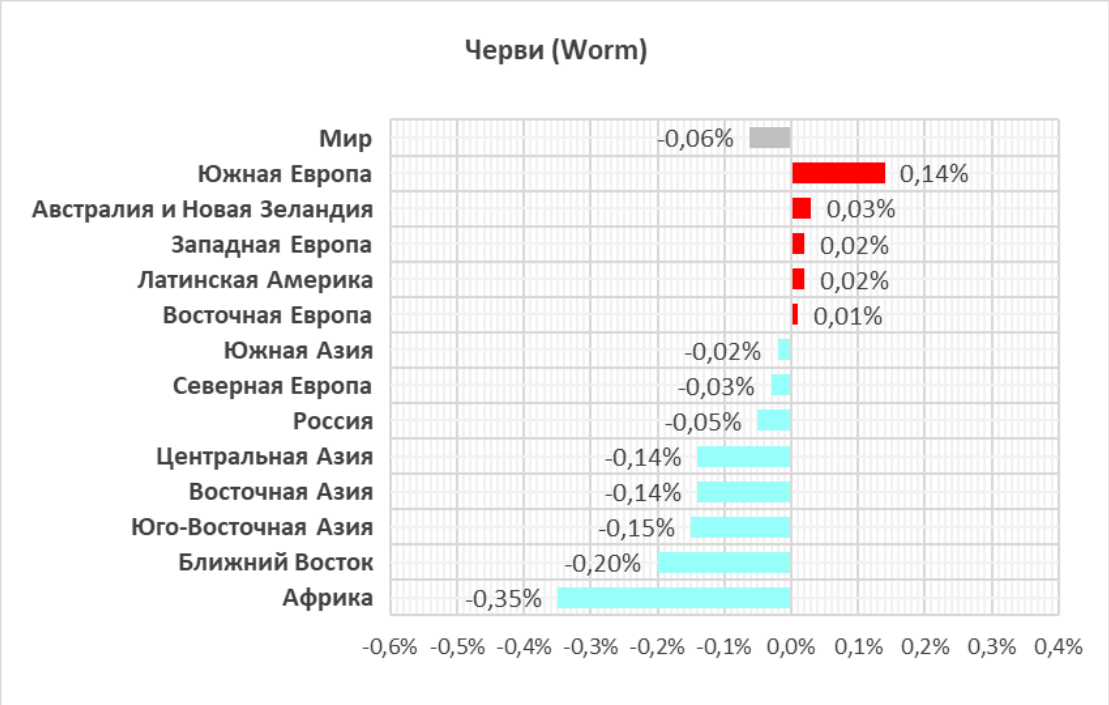
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы черви: Африка, Центральная Азия и Ближний Восток.

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



Лидирует по росту этого показателя Южная Европа.

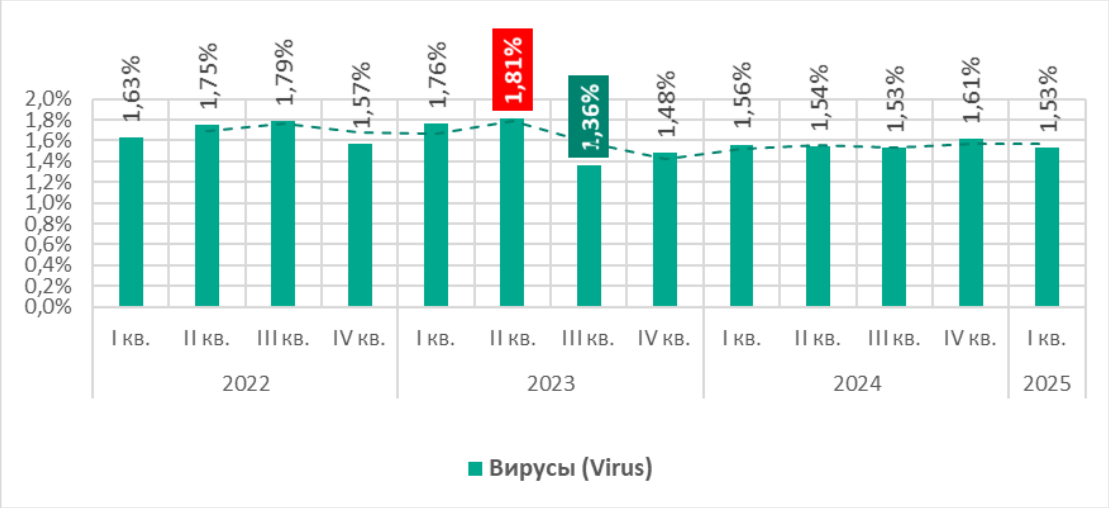
Изменение доли компьютеров АСУ, на которых были заблокированы черви, I квартал 2025 года



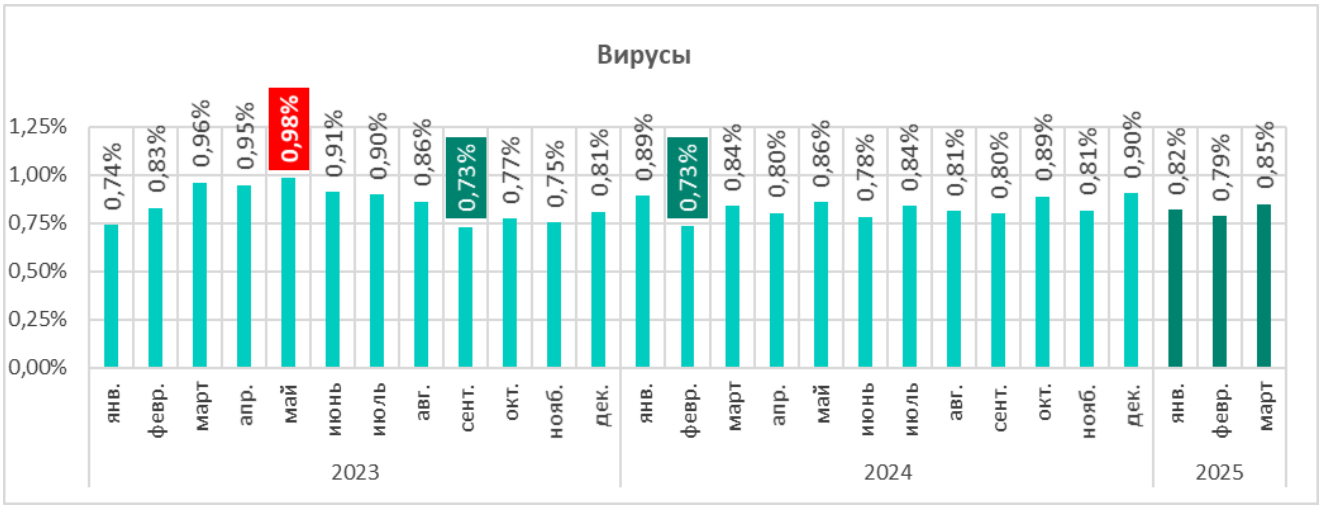
Вирусы

Доля компьютеров АСУ, на которых были заблокированы вирусы, в первом квартале 2025 года уменьшилась.

Доля компьютеров АСУ, на которых были заблокированы вирусы, I квартал 2022 года — I квартал 2025 года



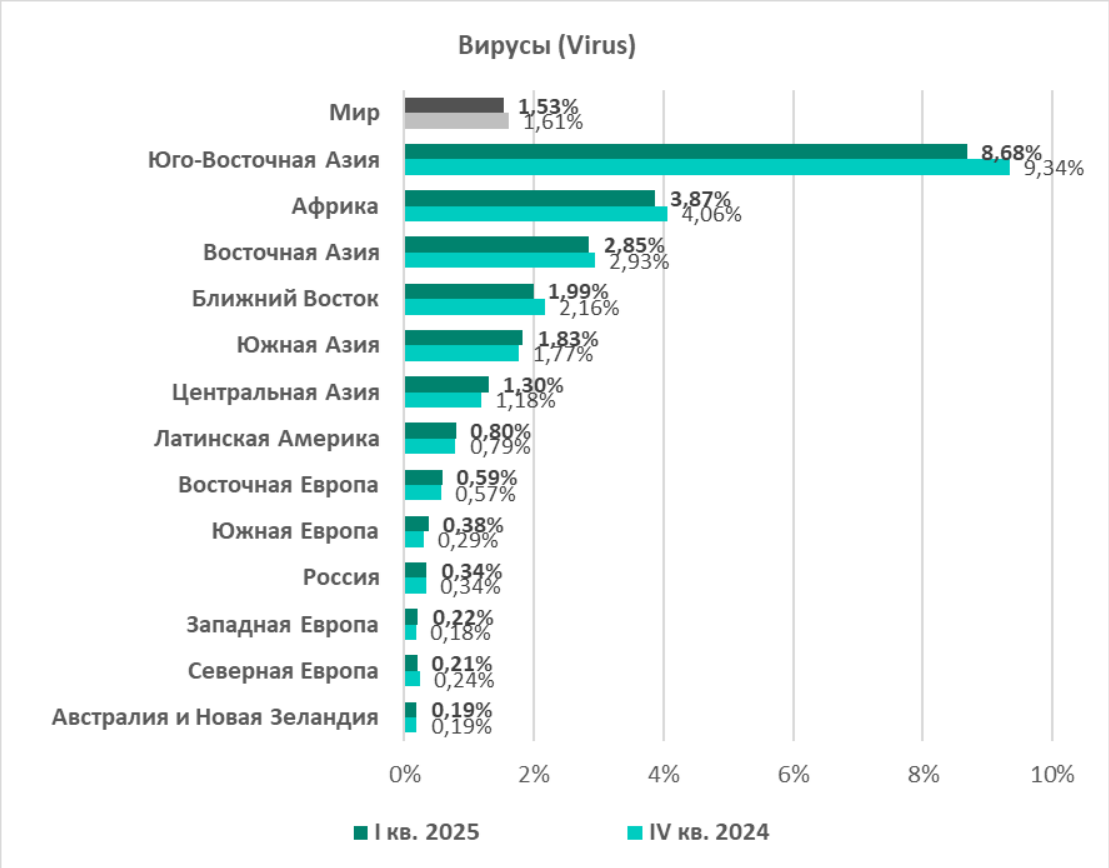
Ежемесячное значение показателя колебалось в течение первого квартала.



Доля компьютеров АСУ, на которых были заблокированы вирусы, январь 2023 года — март 2025 года

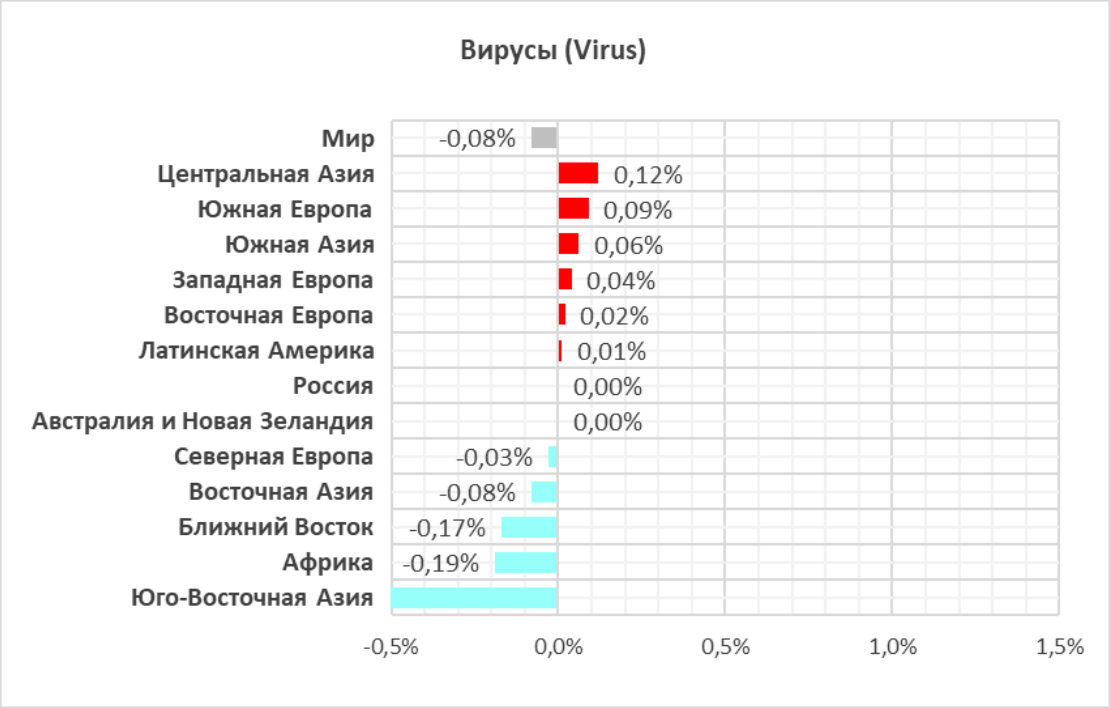
Топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, не изменилась: Юго-Восточная Азия, Африка и Восточная Азия.

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



Лидирует по росту этого показателя Центральная Азия.

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



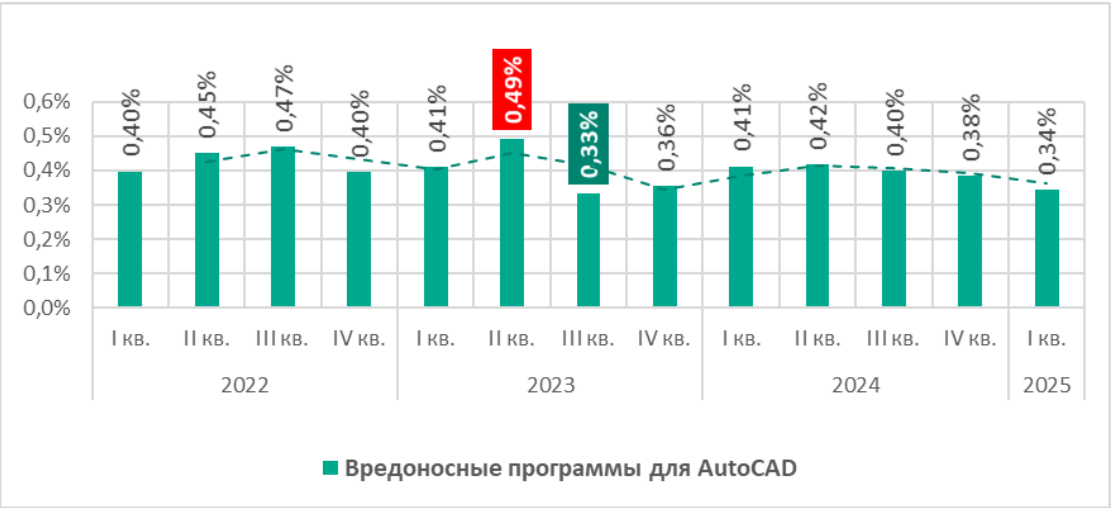
Вредоносные программы для AutoCAD

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

Как правило, вредоносные программы для AutoCAD — минорная угроза, которая в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых она была заблокирована, занимает последние места.

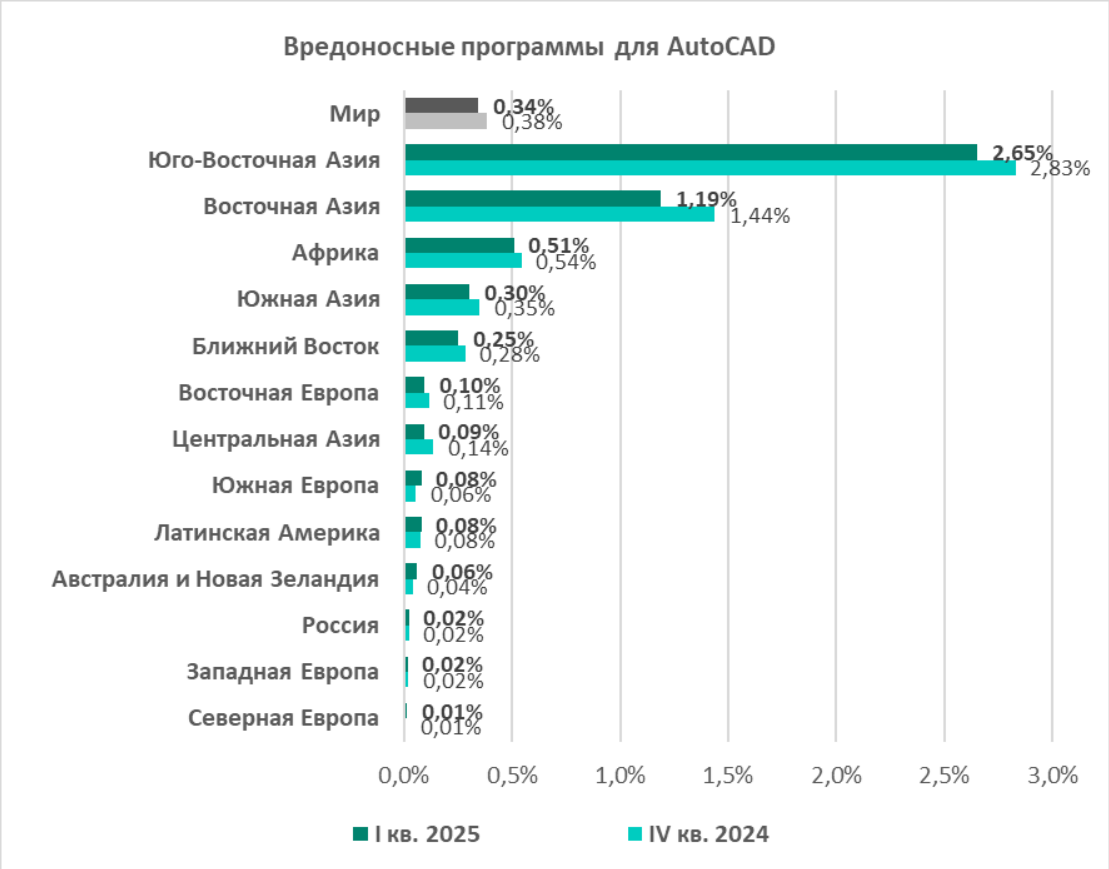
В первом квартале 2025 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, продолжила снижаться.

Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, I квартал 2022 года — I квартал 2025 года



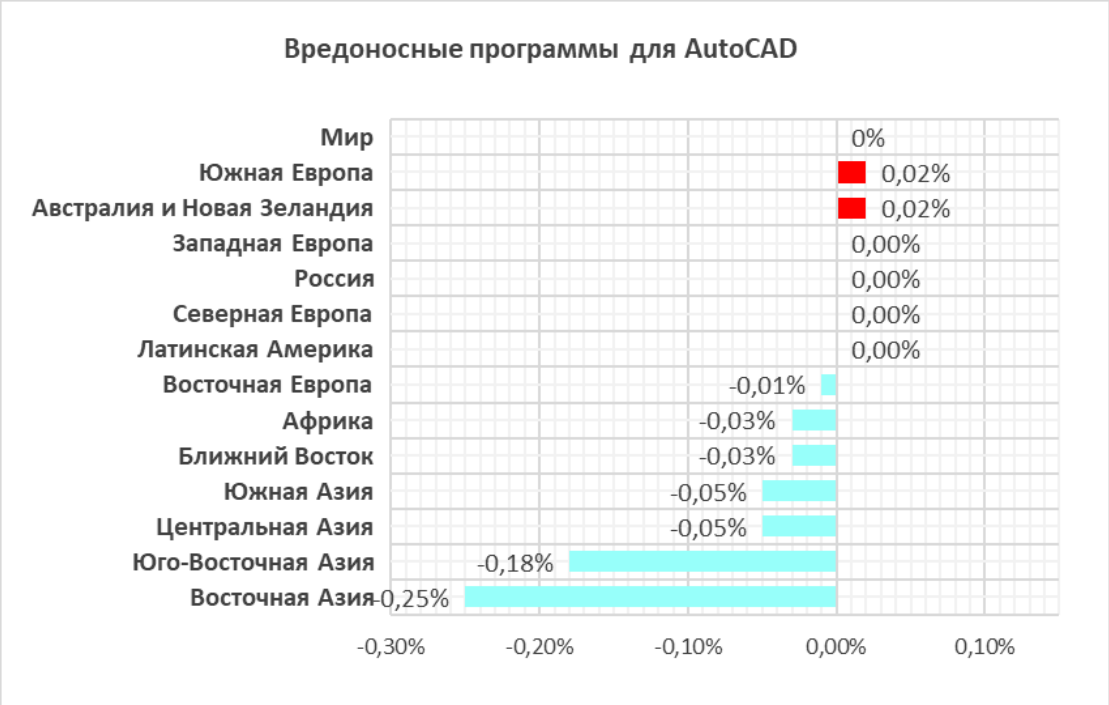
По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, лидируют те же регионы, что и в рейтинге по вирусам. Это Юго-Восточная Азия, Восточная Азия и Африка.

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



Два региона-лидера по росту этого показателя: Южная Европа и Австралия и Новая Зеландия.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, I квартал 2025 года



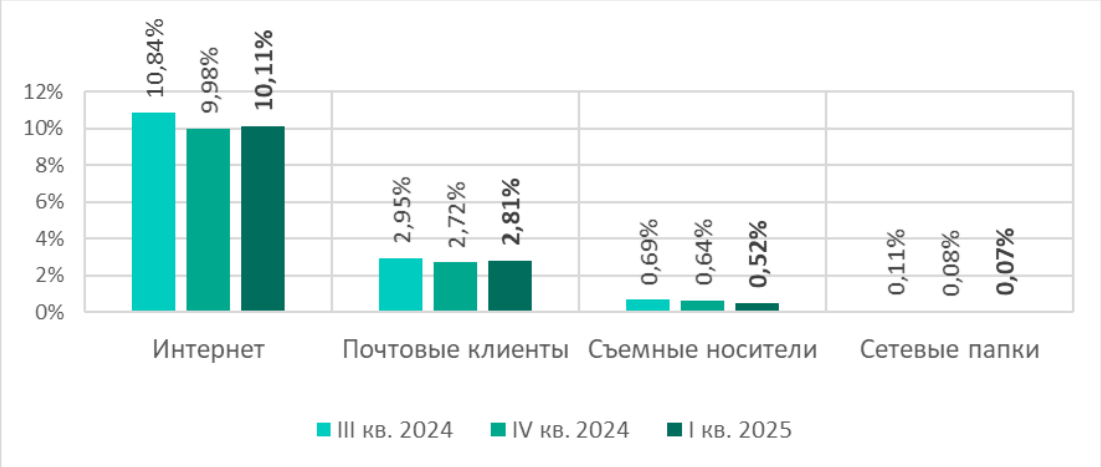
Основные источники угроз

В зависимости от сценария обнаружения и блокирования угрозы не всегда возможно надежно определить ее источник. Косвенным признаком того или иного источника может быть вид (категория) заблокированной угрозы.

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет (обращения к 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.

В первом квартале 2025 года впервые с начала 2023 года увеличилась доля компьютеров АСУ, на которых в течение квартала были заблокированы угрозы из интернета и угрозы, распространяемые через почту.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников



В регионах показатели по источникам угроз варьируют:

- Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, — от 5,2% в Северной Европе до 12,8% в Африке.
- Доля компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через электронную почту, — от 0,88% в России до 6,8% в Южной Европе.
- Доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, — от 0,06% в Австралии и Новой Зеландии до 2,4% в Африке.

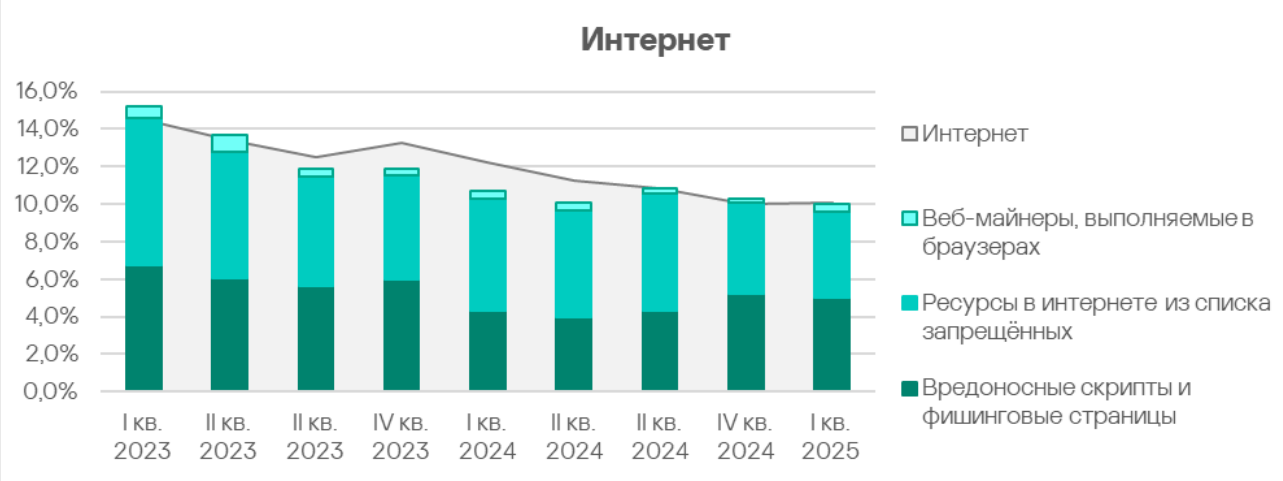
Интернет

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.

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, увеличилась — впервые с начала 2024 года.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, I квартал 2022 года — I квартал 2025 года

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

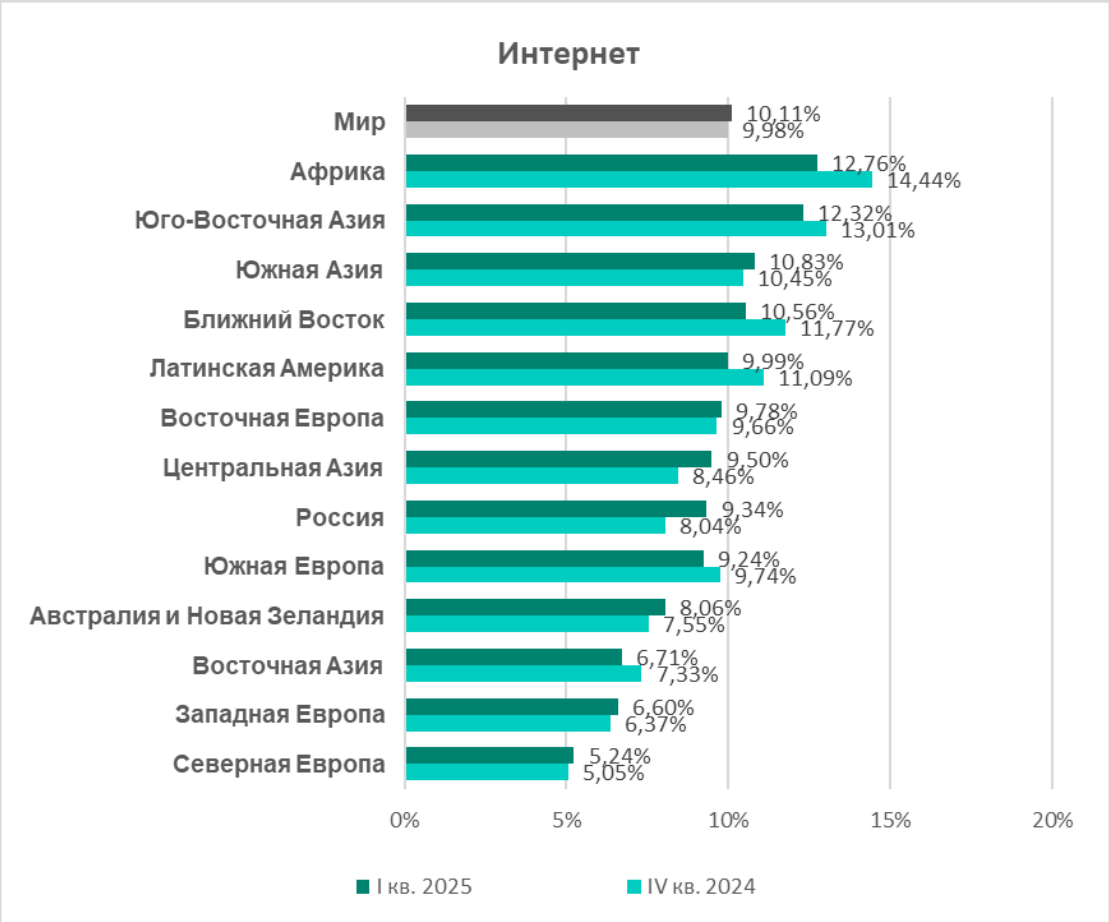


Угрозы из интернета и основные категории угроз из интернета, I квартал 2023 года — I квартал 2025 года

Напомним, что один и тот же ком компьютер в течение квартала может быть атакован несколькими категориями вредоносного ПО, которое распространяется из одного источника. Такой компьютер будет учтен при подсчете процента атакованных компьютеров для каждой категории угроз, но для источника угроз будет учитываться лишь один раз (мы считаем уникальные атакованные компьютеры). К тому же, однозначно определить первоначальной попытки заражения не всегда представляется возможным. Поэтому суммарная доля компьютеров АСУ, на которых были заблокированы различные категории угроз из определенного источника, превышает долю угроз из самого источника.

Топ 3 регионов по доле компьютеров АСУ, на которых в первом квартале 2025 года были заблокированы угрозы из интернета: Африка, Юго-Восточная Азия и Южная Азия.

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



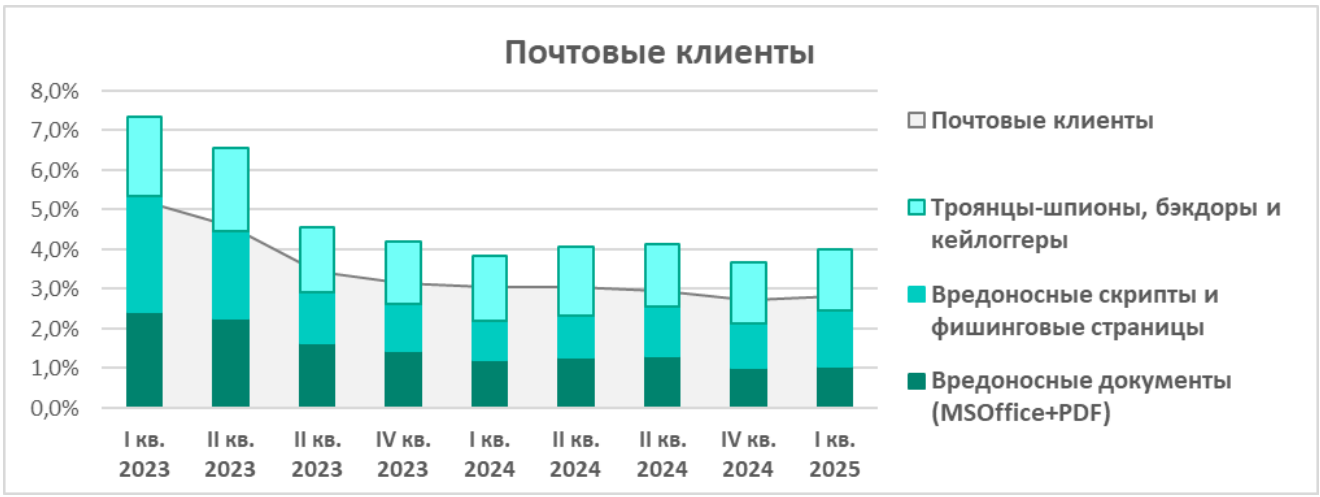
Почтовые клиенты

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

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы такие угрозы, также увеличилась — впервые с начала 2023 года.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, I квартал 2022 года — I квартал 2025 года

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



Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов, I квартал 2023 года — I квартал 2025 года

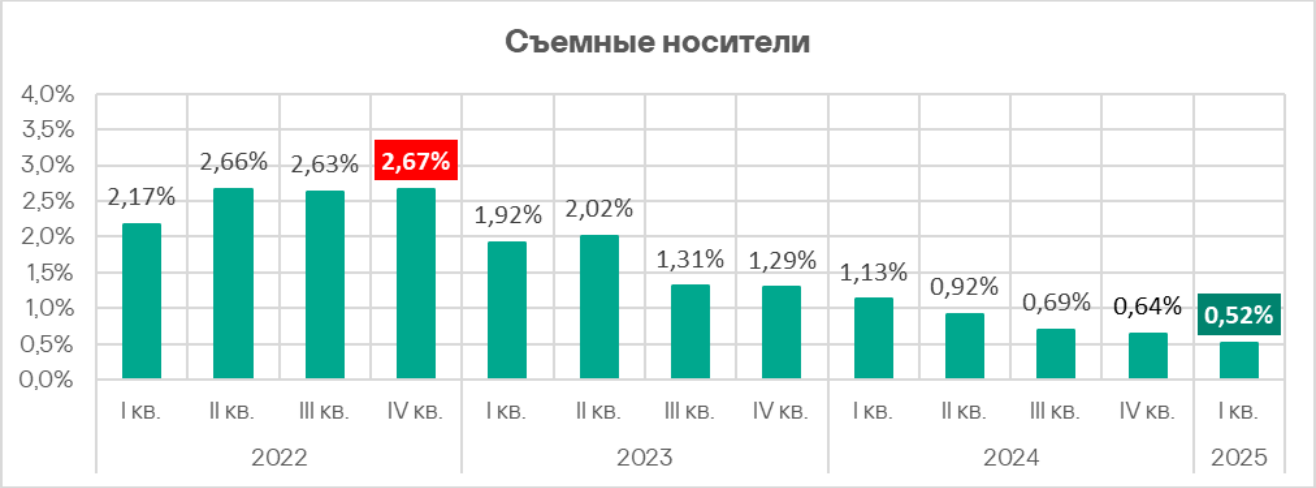
Чтобы избежать обнаружения, большинство шпионских программ, обнаруженных в фишинговых письмах, доставлялись в форме архива или многослойного скрипта, либо в виде отдельного файла, либо встроенного в форматы офисных документов.

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

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

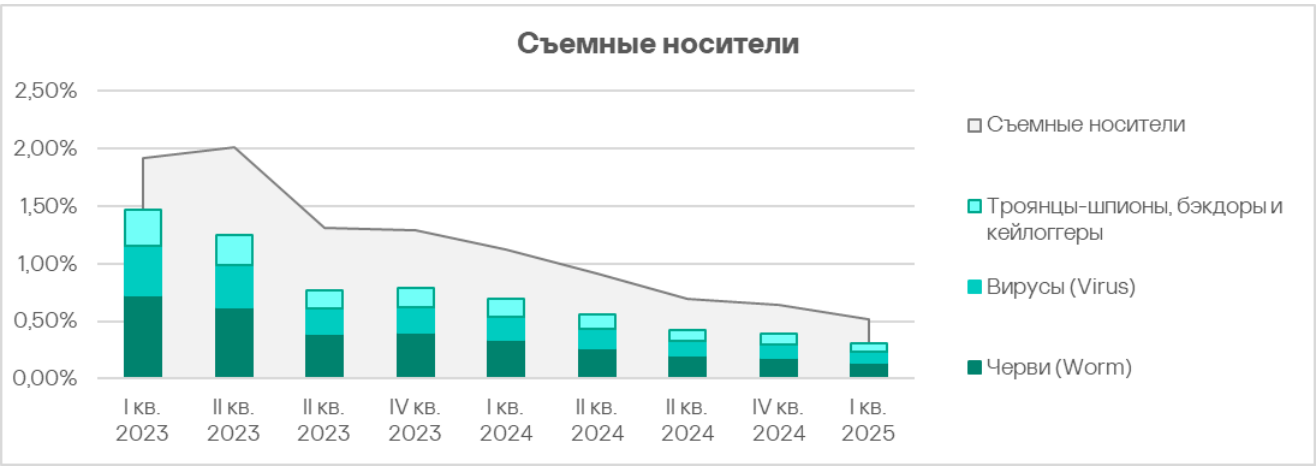
Съемные носители

Доля компьютеров АСУ, на которых угрозы были обнаружены при подключении съемных носителей, продолжила снижаться и достигла минимальных значений с начала 2022 года.



Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, I квартал 2022 года — I квартал 2025 года

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



Угрозы на съемных носителях и основные категории угроз на съемных носителях, I квартал 2023 года — I квартал 2025 года

Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры. Эти современные 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).

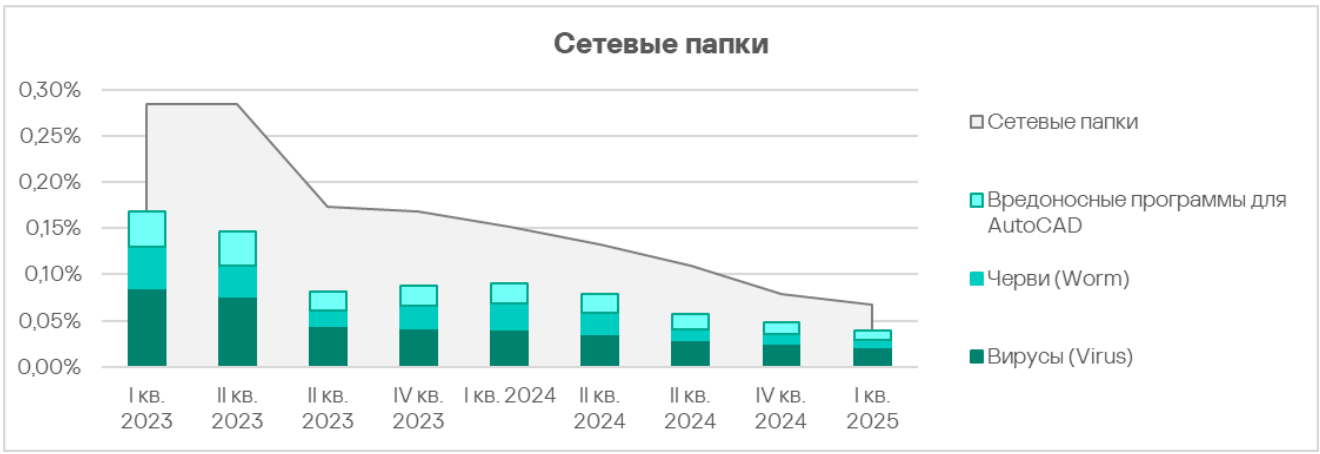
Большинство шпионских программ, обнаруженных на съемных носителях, состояли из универсальных компонентов как современных, так и устаревших червей, таких как стилеры, загрузчики, AV-киллеры.

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

Сетевые папки

Показатели по сетевым папкам достигли минимальных значений с начала 2022 года. Это минорный источник угроз, однако не стоит его недооценивать — через сетевые папки распространяются черви, вирусы и вредоносное ПО для AutoCAD.

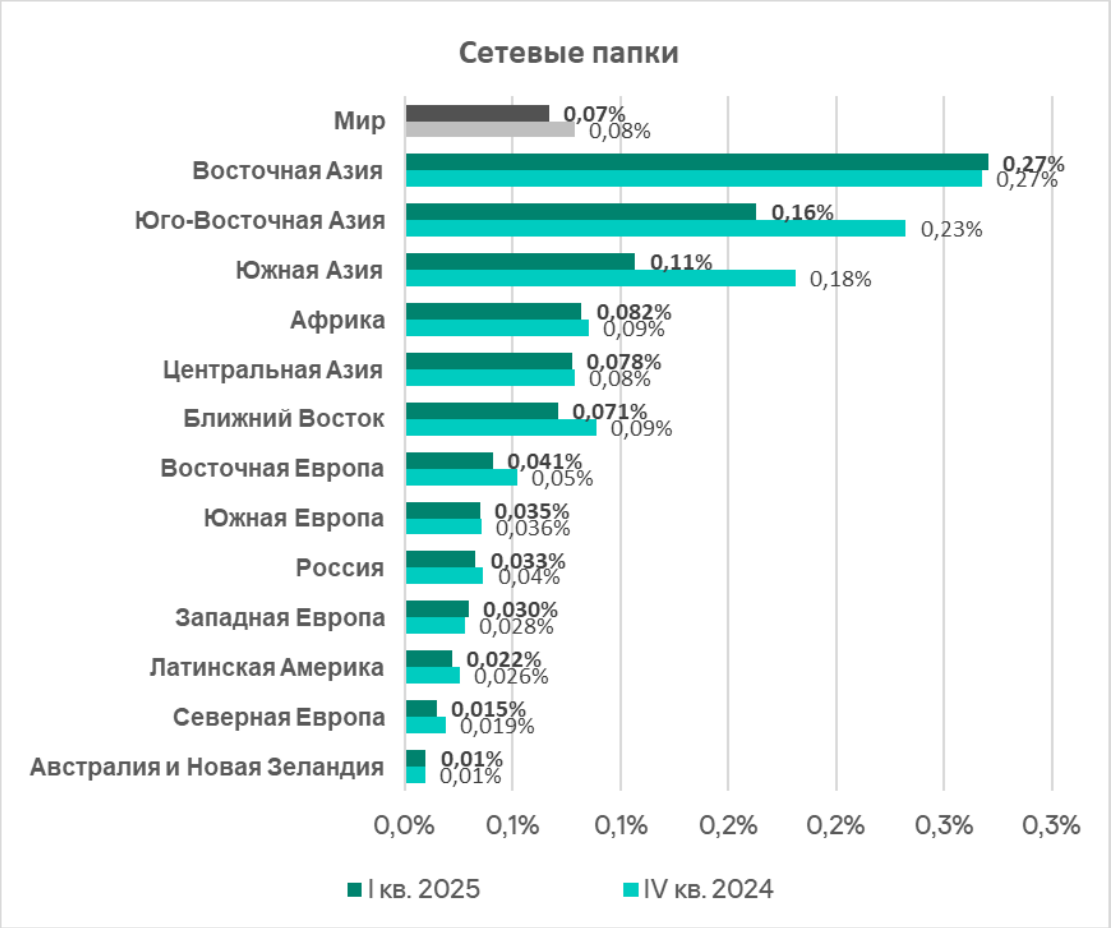
Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, I квартал 2022 года — I квартал 2025 года



Угрозы в сетевых папках и основные категории угроз в съемных папках, I квартал 2023 года — I квартал 2025 года

Топ 3 регионов по уровню угроз в сетевых папках: Восточная, Юго-Восточная и Южная Азия.

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



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);
- 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,

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

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.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com