

Ландшафт угроз для систем промышленной автоматизации

Четвертый квартал 2025 года

Цифры	3
Итоги квартала.....	4
Особенность квартала: черви в почте.....	7
Статистика по всем угрозам.....	9
Исследуемые отрасли.....	12
Разнообразие обнаруженных вредоносных объектов	14
Категории вредоносных объектов	16
Вредоносные объекты, используемые для первичного заражения	17
Ресурсы в интернете из списка запрещенных	17
Вредоносные документы (MSOffice+PDF)	20
Вредоносные скрипты и фишинговые страницы (JS и HTML).....	23
Вредоносное ПО следующего этапа.....	26
Программы-шпионы.....	26
Программы-вымогатели.....	30
Майнеры – исполняемые файлы для ОС Windows	33
Веб-майнеры	37
Самораспространяющееся вредоносное ПО. Черви и вирусы.....	40
Черви	41
Вирусы.....	44
Вредоносные программы для AutoCAD	47
Основные источники угроз	51
Интернет.....	51
Почтовые клиенты	55
Съемные носители	59
Сетевые папки	62
Методика подготовки статистики.....	67

Цифры

Показатель	III кв. 2025	IV кв. 2025	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	20,1%	19,7%	▼ 0,4 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	6,79%	6,58%	▼ 0,21 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	4,04%	3,80%	▼ 0,24 п. п.
Ресурсы в интернете из списка запрещенных	4,01%	3,26%	▼ 0,75 п. п.
Вредоносные документы (MSOffice+PDF)	1,98%	1,76%	▼ 0,22 п. п.
Черви (Worm)	1,26%	1,60%	▲ 0,34 п. п.
Вирусы (Virus)	1,40%	1,33%	▼ 0,07 п. п.
Майнеры – исполняемые файлы для ОС Windows	0,57%	0,60%	▲ 0,03 п. п.
Вредоносные программы для AutoCAD	0,30%	0,29%	▼ 0,01 п. п.
Веб-майнеры, выполняемые в браузерах	0,25%	0,24%	▼ 0,01 п. п.
Программы-вымогатели	0,17%	0,16%	▼ 0,01 п. п.
Основные источники угроз			
Интернет	7,99%	7,67%	▼ 0,32 п. п.
Почтовые клиенты	3,01%	2,76%	▼ 0,25 п. п.
Съемные носители	0,33%	0,31%	▼ 0,02 п. п.
Сетевые папки	0,04%	0,04%	0,00 п. п.

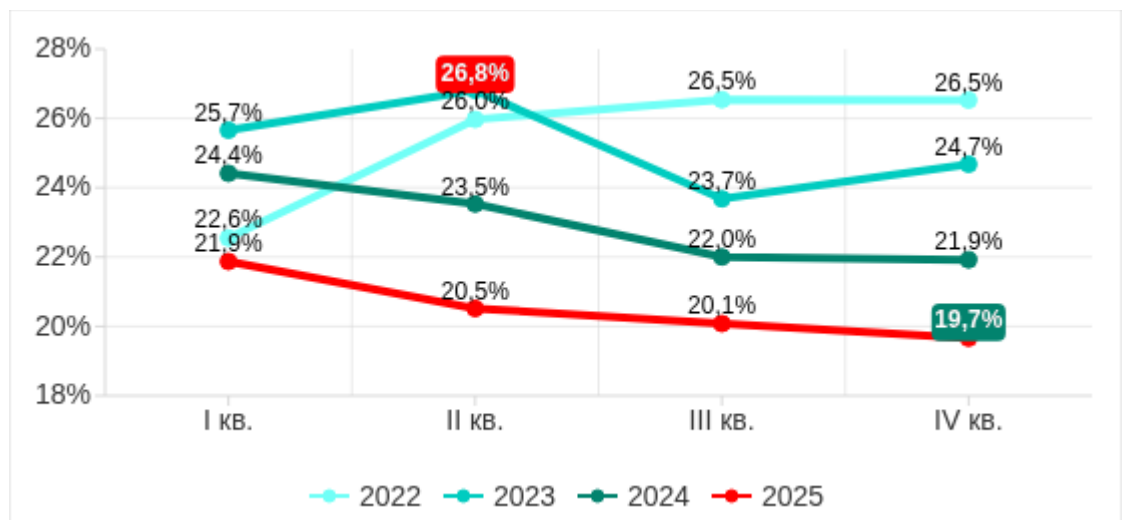
Итоги квартала

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты

В четвертом квартале 2025 года в мире доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, продолжила уменьшаться и оказалась минимальной с 2022 года — 19,7%.

В регионах показатель варьировал от 8,5% в Северной Европе до 27,3% в Африке. Значения выросли в четырех регионах, лидирует по росту Южная Европа.

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



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, неуклонно снижается с 2024 года. Квартальные показатели 2025 года были наименьшими с 2022 года.

Основные источники и категории угроз

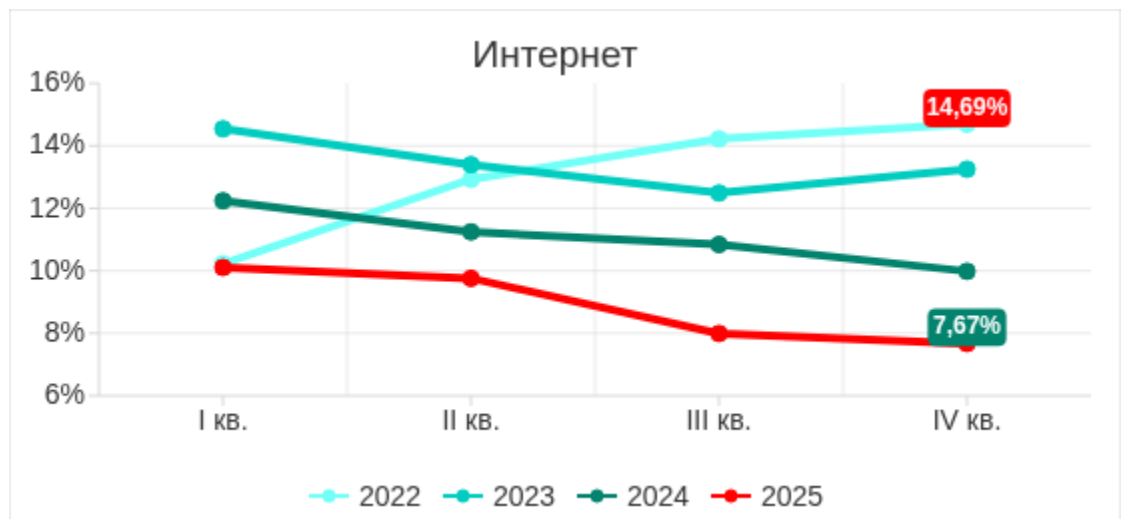
Основными источниками угроз для компьютеров в технологической инфраструктуре организаций по-прежнему остаются интернет, почтовые клиенты и съемные носители. В четвертом квартале 2025 года показатели всех источников угроз, кроме почтовых клиентов, оказались наименьшими с 2022 года.

Что касается категорий угроз, то доля компьютеров АСУ, на которых блокируются угрозы различных категорий, за квартал выросла только у червей и майнеров – исполняемых файлов для ОС Windows. У категории «Ресурсы в интернете из списка запрещенных» показатели также оказались наименьшими с 2022 года.

Интернет остается главным источником угроз в промышленных сетях. Нисходящий тренд, длящийся уже три года, указывает на то, что:

1. Все больше вредоносных веб-адресов и других веб-угроз блокируется на периметре сети, т. е. не добираясь до компьютеров АСУ, где последней надеждой являются компоненты веб-защиты.
2. Техники размещения вредоносного ПО в интернете становятся универсальнее и доступнее – стоимость создания ссылки на вредоносный контент стремится к нулю (практически любой публичный веб-сервис может быть использован для хранения вредоносного ПО), а разнообразие техник доставки увеличивается – это приводит к снижению эффективности детектирования вредоносных веб-адресов.

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



Очевидно, что плохо контролируемый доступ в интернет из промышленной сети – это не только источник случайных заражений вредоносным ПО начального этапа. При успешной компрометации доступ в интернет становится каналом доставки вредоносного ПО следующего этапа и эксфильтрации данных и удаленного управления.

Основные категории угроз из интернета, которые были заблокированы на компьютерах АСУ в четвертом квартале 2025 года: вредоносные скрипты и фишинговые страницы, а также ресурсы в интернете из списка запрещенных.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, с начала 2024 года относительно стабильна. Показатель четвертого квартала 2025 года – 2,76% – чуть выше, чем минимальное с 2022 года значение 2,72%, отмеченное в четвертом квартале 2024 года.

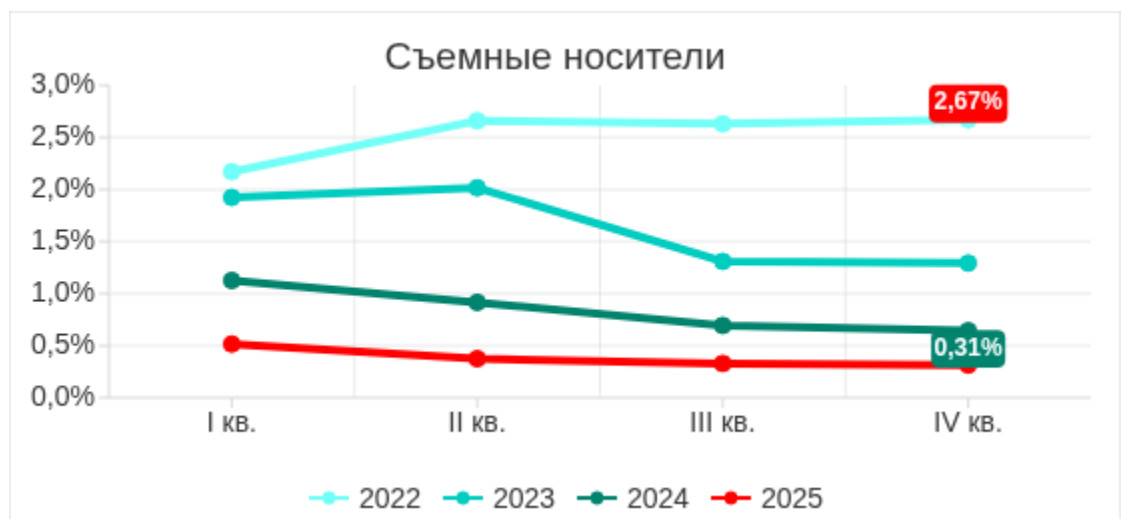
Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, I квартал 2022 года — IV квартал 2025 года



Основные категории угроз из почтовых клиентов: вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы. В четвертом квартале 2025 года в результате роста количества фишинговых атак, направленных на доставку вредоносного ПО Backdoor.MSIL.XWorm, вдвое выросла доля компьютеров АСУ, на которых были заблокированы черви, обнаруженные в почтовых вложениях.

Доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, неуклонно снижается последние три года. По сравнению с четвертым кварталом 2022 года показатель уменьшился в 8,6 раза.

Доля компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, I квартал 2022 года — IV квартал 2025 года



Случаи массового заражения компьютеров вирусами и червями через съемные носители и зараженные файлы в интернете сменились случаями небольших локальных эпидемий. Причиной такой эпидемии в пределах одной промышленной сети часто являются зараженные бэкапы или

зараженные компьютеры, которые считаются слишком старыми, чтобы применять к ним современные технологии защиты.

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

Особенность квартала: черви в почте

В четвертом квартале 2025 года во всех регионах мира выросла доля компьютеров АСУ, на которых были заблокированы черви (worms) в почтовых вложениях.

Значительная доля заблокированных угроз относится к червию-бэкдору Backdoor.MSIL.XWorm. Это вредоносное ПО предназначено для закрепления в системе и последующего удаленного управления.

Примечательно, что эта угроза не встречалась на компьютерах АСУ в предшествующем квартале, но в четвертом квартале 2025 года появилась во всех регионах.

Как показало исследование, активное распространение Backdoor.MSIL.XWorm в фишинговых письмах, вероятно, связано с применением злоумышленниками очередной техники обфускации вредоносного ПО, которая в четвертом квартале 2025 года активно использовалась в ходе массовых фишинговых кампаний, известных с 2024 года под названием Curriculum-vitae-catalina.

В ходе атаки злоумышленники распространяли фишинговые письма, адресованные HR-менеджерам, рекрутерам и сотрудникам компаний, отвечающих за наем персонала. Сообщения якобы от соискателя с темой Resume или Attached Resume были замаскированы под отклики на вакансии и под видом резюме (Curriculum Vitae) содержали вредоносный исполняемый файл. Как правило, он назывался Curriculum Vitae-Catalina.exe. При запуске файла Curriculum Vitae-Catalina.exe происходило заражение системы.

В четвертом квартале 2025 года угроза распространялась по регионам двумя волнами — в октябре и ноябре. В октябре были атакованы Россия, Западная Европа, Южная Америка, Северная Америка (Канада). В остальных регионах всплеск блокирования Backdoor.MSIL.XWorm был отмечен в ноябре. В декабре во всех регионах атака пошла на спад.

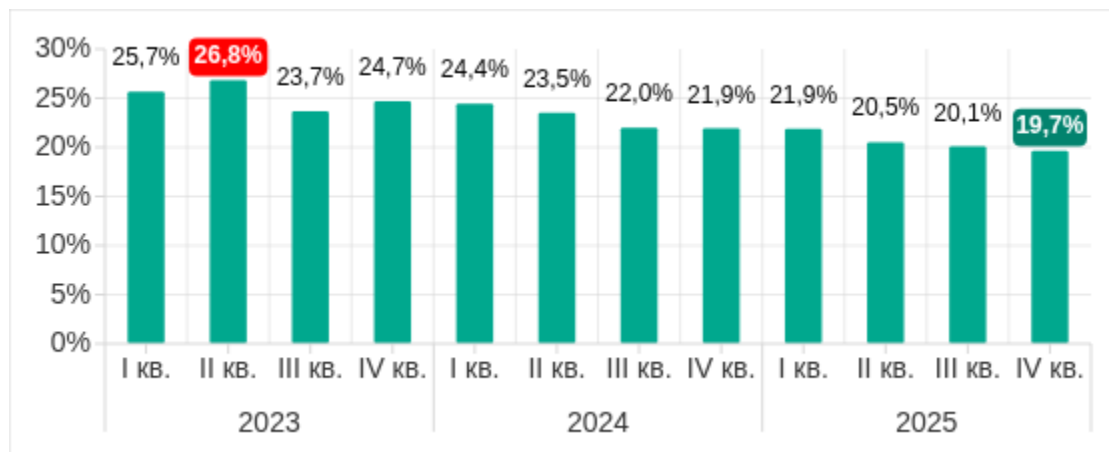
Самая высокая доля компьютеров АСУ, на которых блокировался Backdoor.MSIL.XWorm, отмечена в регионах, где традиционно высока доля компьютеров АСУ, на которых блокируются угрозы из почты: в Южной Европе, Южной Америке и на Ближнем Востоке.

В то же время в Африке, где по-прежнему активно используются USB-носители, угроза была обнаружена и при подключении к компьютерам АСУ съемных устройств.

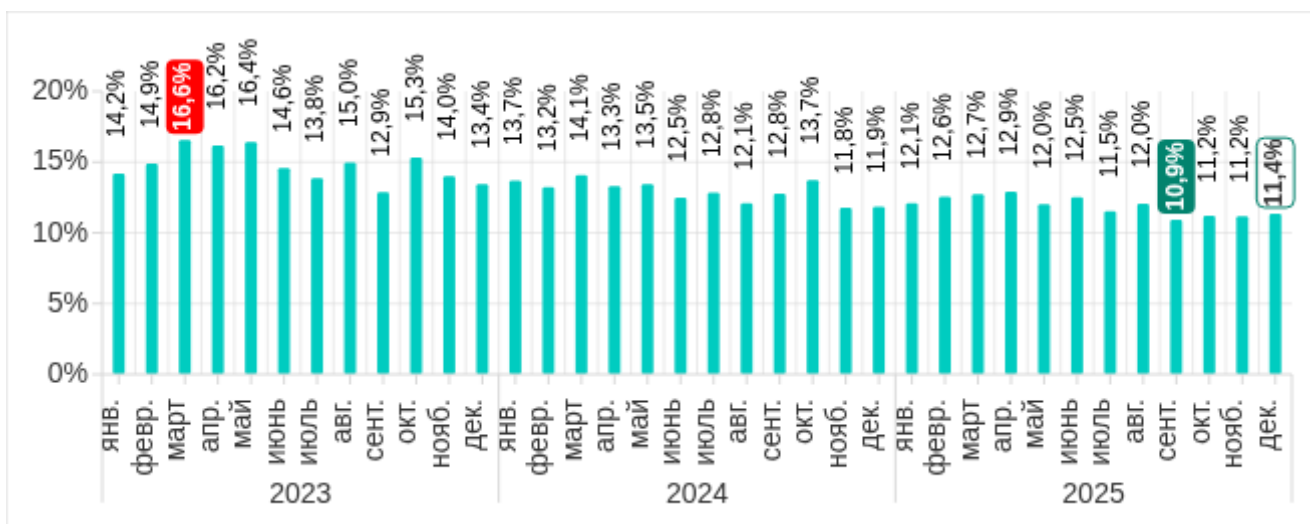
Статистика по всем угрозам

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, снижается с начала 2024 года. В четвертом квартале 2025 года она составила 19,7%. За три года показатель уменьшился в 1,35 раза, с четвертого квартала 2023 года – в 1,25 раза.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, I квартал 2023 года – IV квартал 2025 года



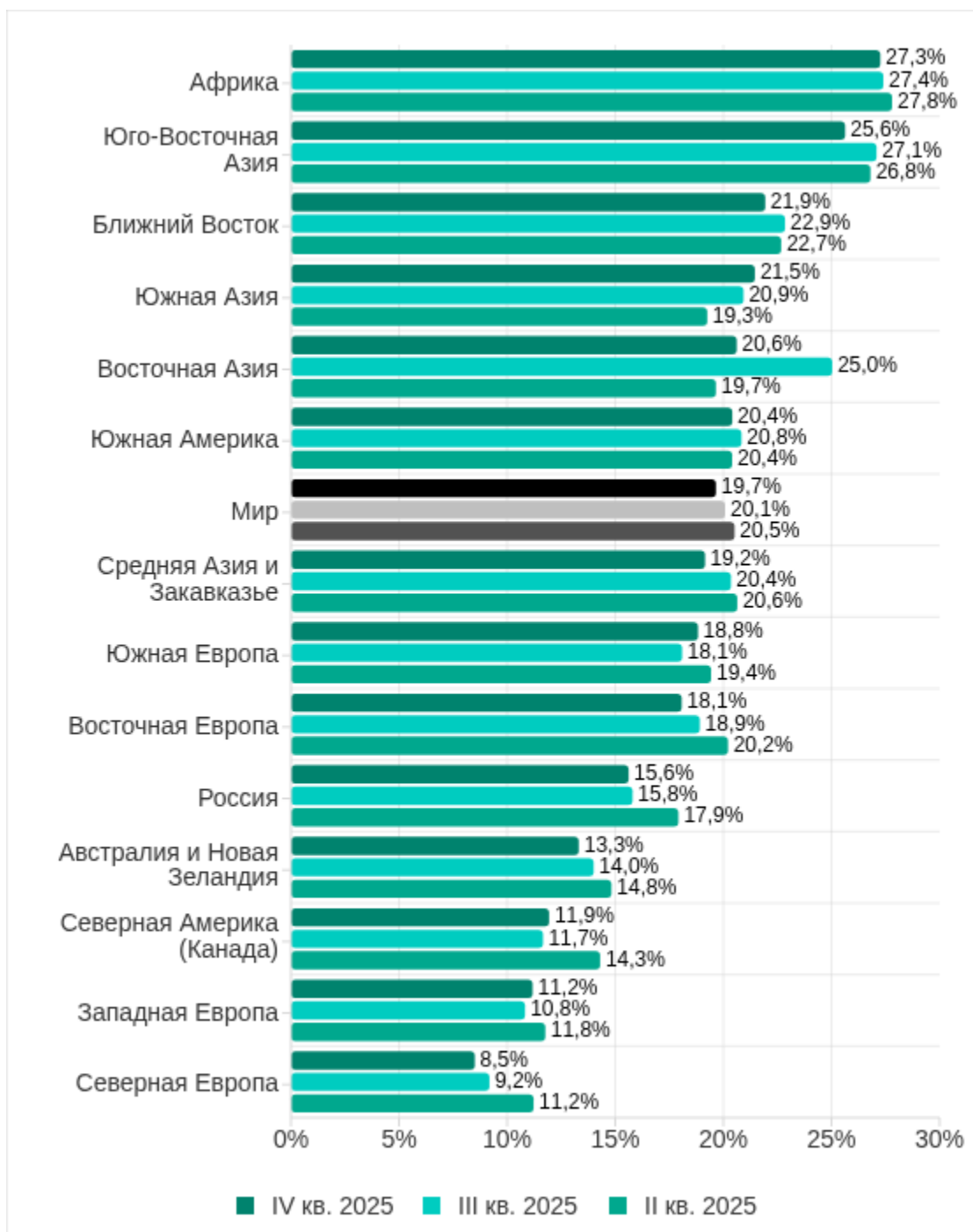
В течение 2025 года самой высокой долей компьютеров АСУ, на которых были заблокированы вредоносные объекты, была в апреле, а в четвертом квартале – в декабре.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года – декабрь 2025 года

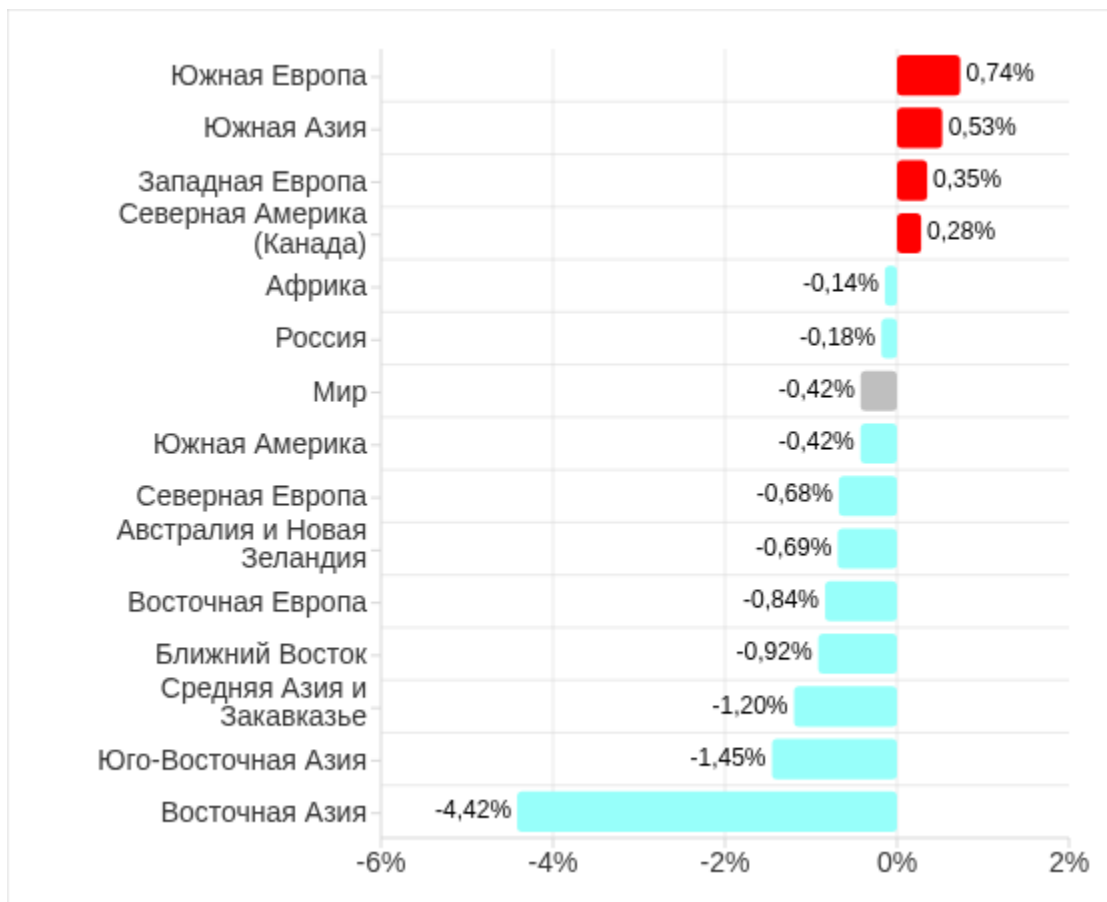
В регионах доля компьютеров АСУ, на которых в четвертом квартале 2025 года были заблокированы вредоносные объекты, варьирует от 8,5% в Северной Европе до 27,3% в Африке.

Рейтинг
регионов
по доле
атакованных
компьютеров
АСУ



Показатель за квартал увеличился в четырех регионах, больше всего — в Южной Европе и Южной Азии. В Восточной Азии, где в третьем квартале 2025 года был отмечен резкий рост доли компьютеров АСУ, связанный с локальным распространением вредоносных скриптов, показатель вернулся к норме.

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

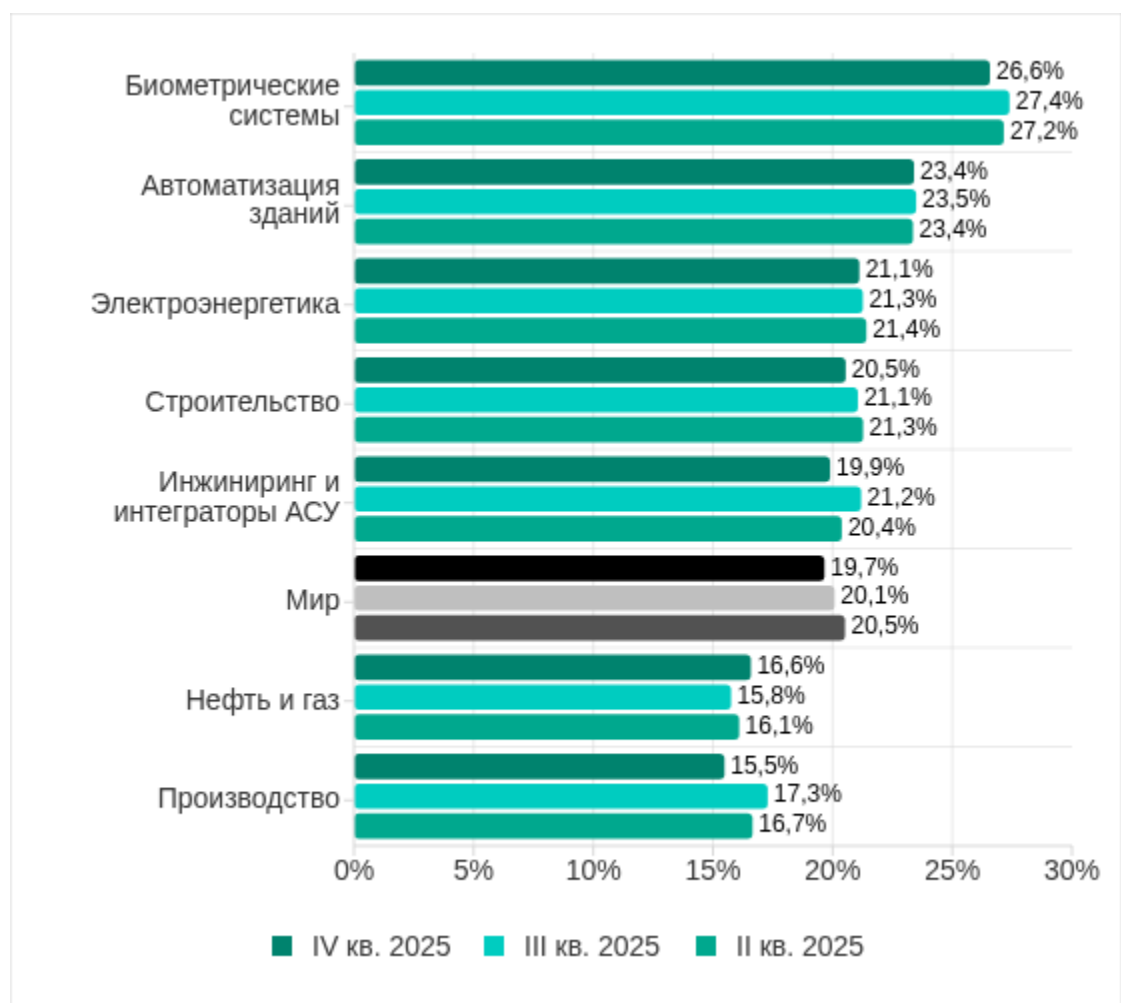


Исследуемые отрасли

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

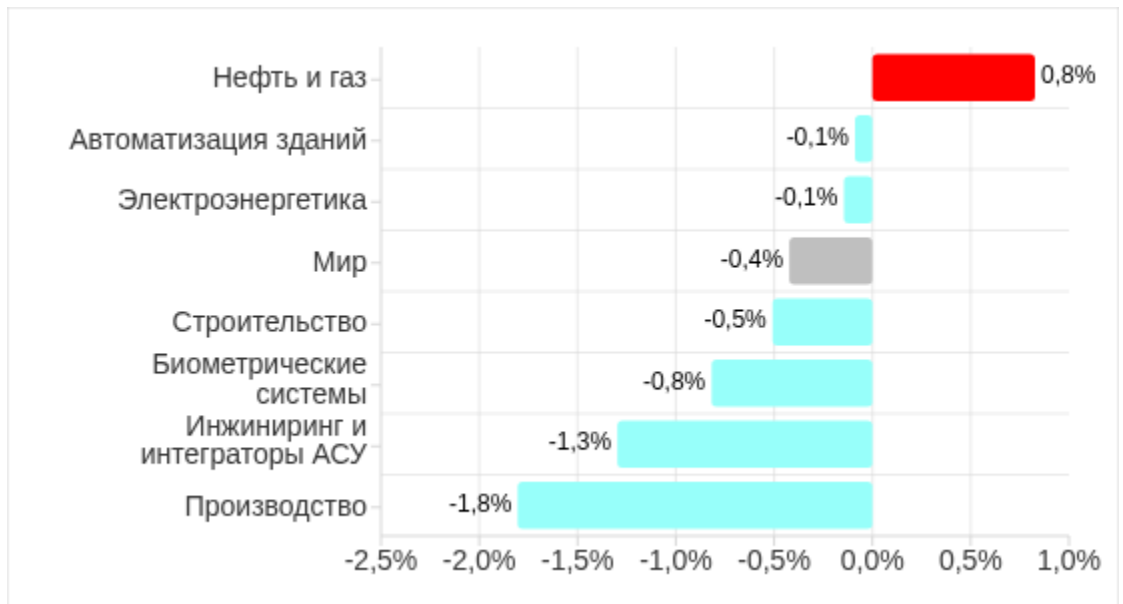
Для этих систем характерны доступность интернета и доступность их из интернета и часто минимальный контроль ИБ со стороны организации-потребителя.

Рейтинг исследуемых отраслей по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты

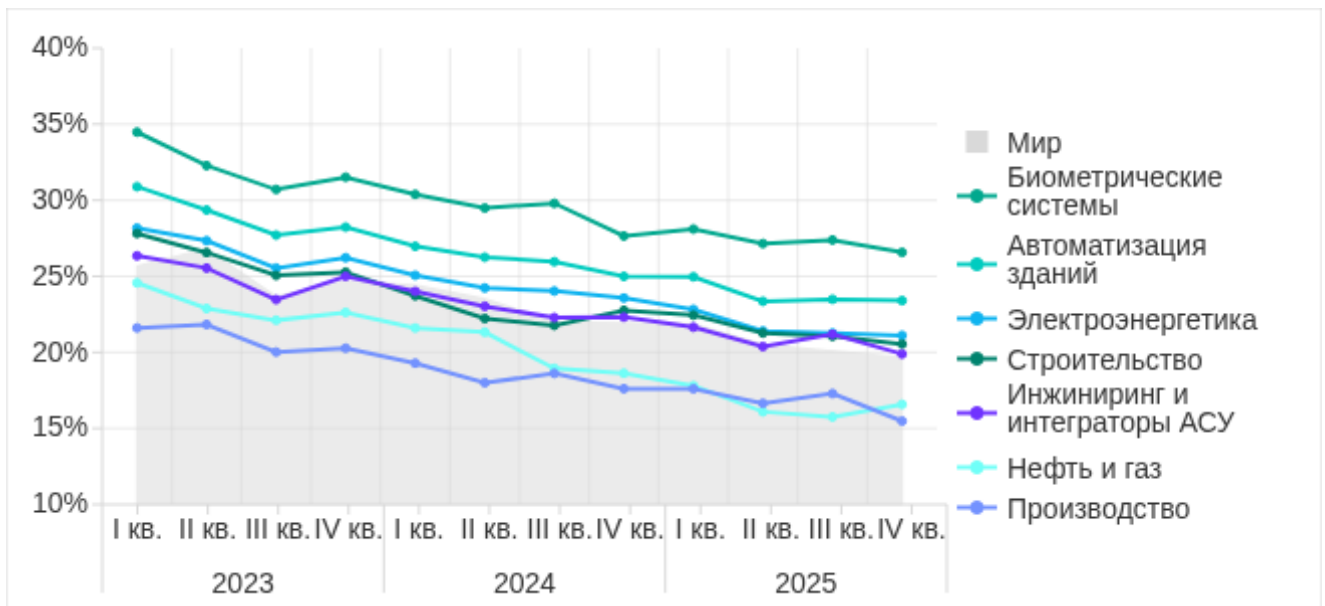


Из всех исследуемых отраслей в четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась только в нефтегазовой отрасли. Соответствующие показатели выросли в двух регионах: в России, а также Средней Азии и Закавказье.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, в исследуемых отраслях, IV квартал 2025 года



Во всех исследуемых отраслях наблюдается тенденция к уменьшению показателя.



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

Разнообразии 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.

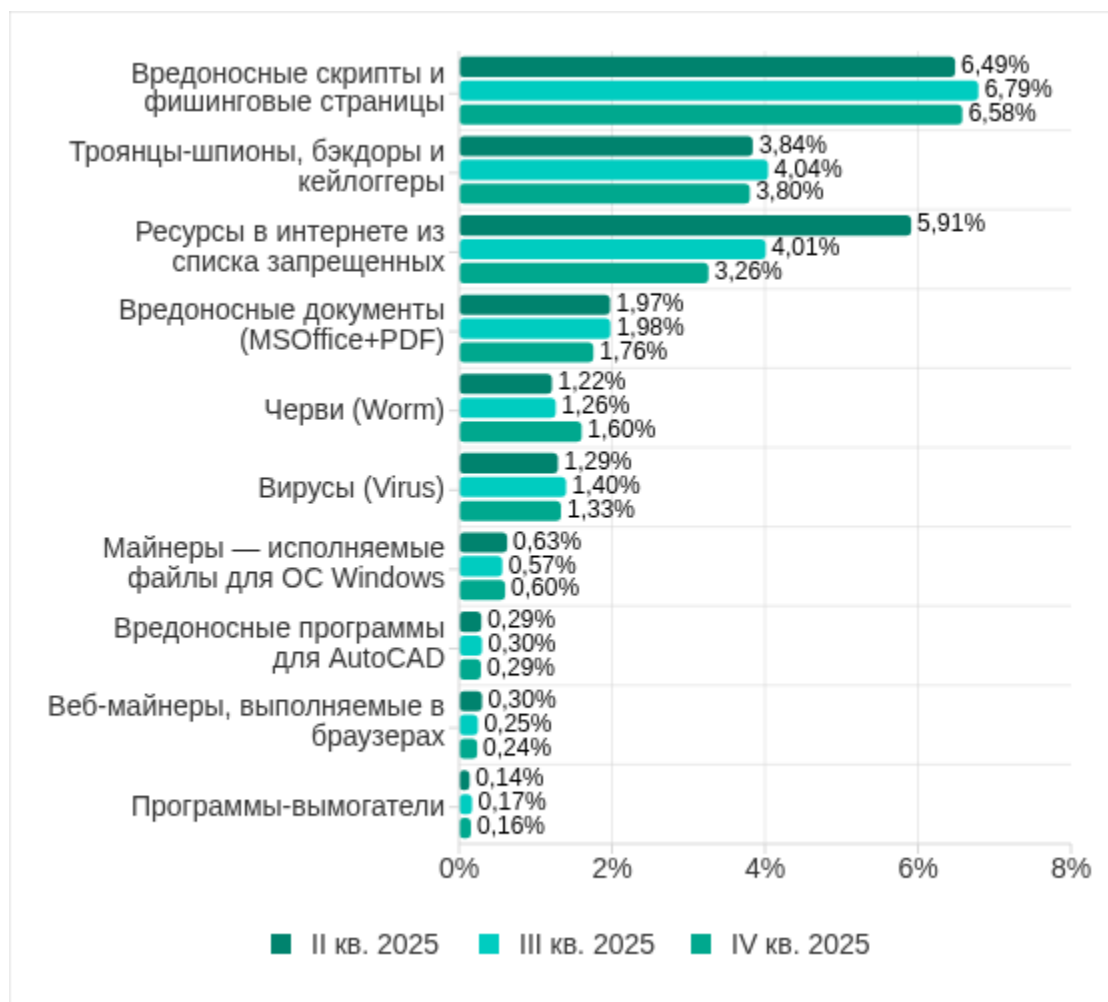
Вредоносные программы для AutoCAD распространяются разными способами, поэтому мы не относим их к конкретной группе по типу распространения.

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.

Следует заметить, что в небольшом проценте случаев категории угроз, которые мы относим к объектам первичного заражения, скажем, вредоносные ссылки, также используются на последующих этапах атаки. Так, например, иногда ссылка на вредоносный ресурс может быть обнаружена при сканировании реестра компьютера, где она появилась, очевидно, в результате работы другого вредоносного ПО – до того момента, как оно было идентифицировано и заблокировано. Более строгое деление атакованных компьютеров АСУ по категориям заблокированного на них вредоносного ПО и по источникам его попадания на компьютер описано в нашей статье [«Динамика внешних и внутренних угроз АСУ»](#), открывающей новый цикл публикаций результатов более глубокого исследования ландшафта угроз АСУ ТП по данным статистики срабатывания защитных компонентов наших продуктов.

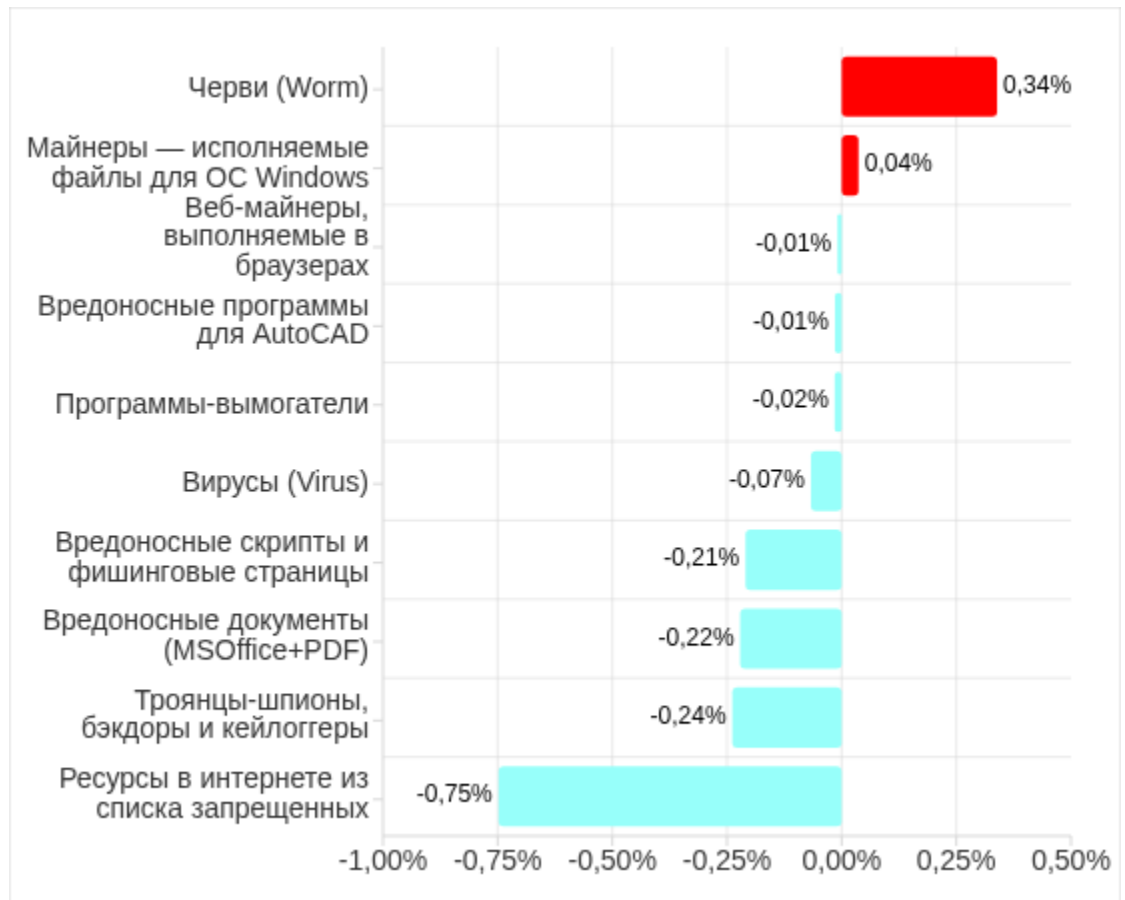
В четвертом квартале 2025 года в рейтинге категорий вредоносного ПО по доле атакованных компьютеров АСУ лидирует категория «Вредоносные скрипты и фишинговые страницы». Программы-шпионы, как и в предыдущем квартале, – на втором месте.

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



В четвертом квартале 2025 года показатель увеличился только у двух категорий: черви и майнеры – исполняемые файлы для ОС Windows.

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



Второй квартал подряд снижается доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных. Показатель этой категории со второго квартала 2025 года уменьшился почти вдвое (в 1,8 раза).

Стоит отметить, что техники размещения вредоносного ПО в интернете разнообразны, обширны и доступны любому злоумышленнику. Любой веб-сервис (даже самый защищенный) может быть использован как веб-хранилище, если он позволяет сохранять и запрашивать информацию. На практике это означает, что для защиты сети АСУ (как и любой другой) необходимо полагаться на весь стек технологий защиты, а не только на защиту периметра сети.

Категории вредоносных объектов

В четвертом квартале 2025 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 10 142 семейств, относящихся к различным категориям.

Типовые атаки, блокируемые в сети АСУ, представляют собой многошаговые последовательности вредоносных действий, где каждый

последующий шаг злоумышленников направлен на сбор дополнительной информации, повышение привилегий и/или получение доступа к другим системам путем эксплуатации проблем безопасности промышленных предприятий, в том числе технологических инфраструктур.

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 (небезопасные) 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 конфигураций и вредоносного ПО следующего этапа.

Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

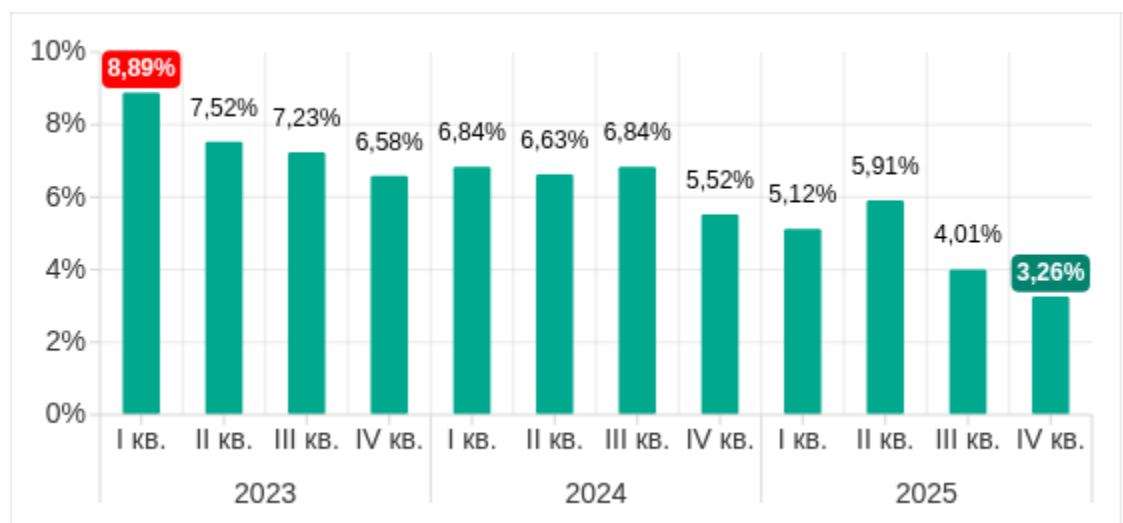
Обнаруженный опасный интернет-ресурс не всегда может быть легко добавлен в список запрещенных, поскольку злоумышленники все чаще используют легитимные интернет-ресурсы и сервисы, например платформы доставки контента (CDN), мессенджеры, репозитории и облачные хранилища. Подобные сервисы позволяют распространять 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.

Высокие значения параметра, как правило, свидетельствуют о слабом контроле выполнения политик ИБ (компьютеры АСУ имеют так или иначе

доступ к интернету, и этим доступом часто пользуются), недостатках защиты от фишинга (многие вредоносные ссылки доставляются в фишинговых сообщениях) и недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным веб-ресурсам и ссылкам из подозрительных писем и сообщений мессенджеров).

В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, снизилась до 3,26%. Это наименьший квартальный показатель с начала 2022 года, со второго квартала 2025 года он уменьшился в 1,8 раза.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, I квартал 2023 года — IV квартал 2025 года



С декабря 2024 года от месяца к месяцу показатель рос с незначительными колебаниями вплоть до июня 2025 года. Во второй половине года он вновь стал уменьшаться и в декабре оказался минимальным за рассматриваемый период.



Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, январь 2024 года — декабрь 2025 года

В рейтинге категорий вредоносных объектов по доле атакованных компьютеров ресурсы в интернете из списка запрещенных долгое время занимали первое или второе место. В третьем квартале 2025 эта категория впервые опустилась на третье место, на котором осталась и в четвертом квартале.

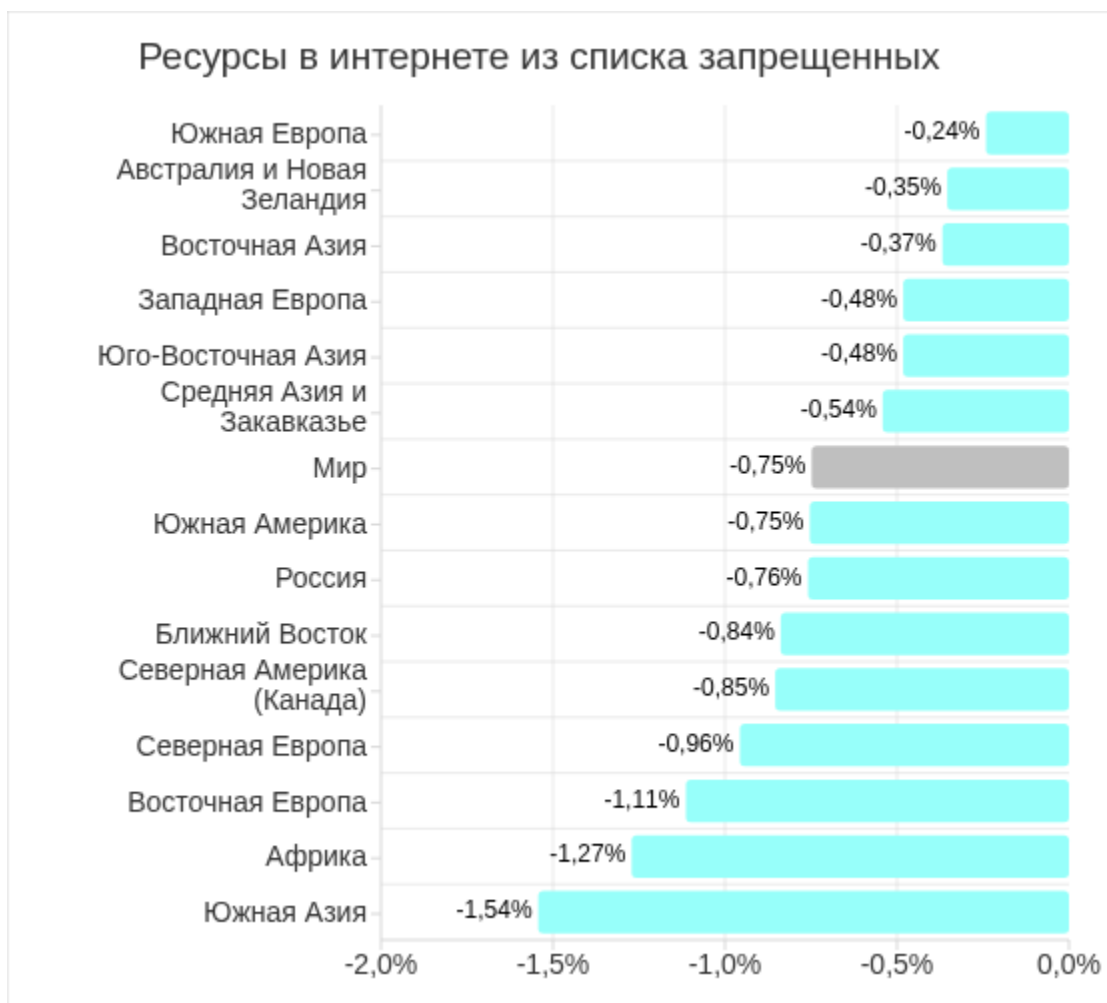
В регионах доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, варьирует от 1,74% в Северной Европе до 3,93% в Юго-Восточной Азии, которая потеснила Африку с первого места в соответствующем рейтинге. Замыкает тройку лидеров по этому показателю Россия.

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



В четвертом квартале 2025 года, как и в предыдущем квартале, показатель уменьшился во всех регионах.

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



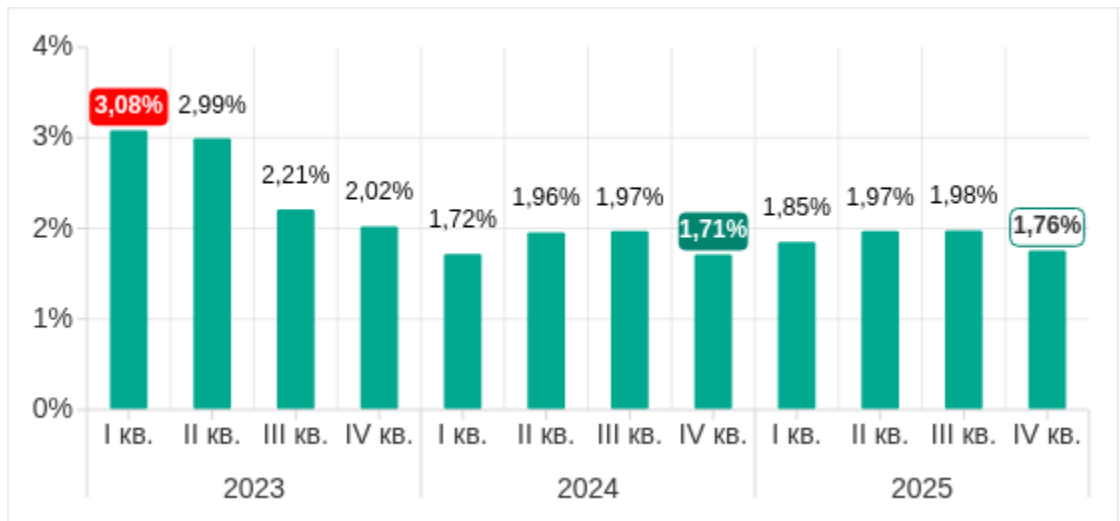
Вредоносные документы (MSOffice+PDF)

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.

Вредоносные документы остаются популярным вектором для целевых атак, особенно с использованием эксплойтов нулевого дня. В 2025 году CISA выпустила более 450 предупреждений безопасности, многие из которых касаются обработки файлов, включая популярные форматы документов.

После снижения в конце 2024 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, росла три квартала подряд, но в четвертом квартале уменьшилась на 0,22 п. п. до 1,76%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, I квартал 2023 года – IV квартал 2025 года



По месяцам 2025 года показатель рос до мая, когда значение оказалось самым высоким за два года, после чего он начал постепенно снижаться. В декабре доля компьютеров АСУ, на которых были обнаружены вредоносные документы, была наименьшей за год.



Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, январь 2024 года – декабрь 2025 года

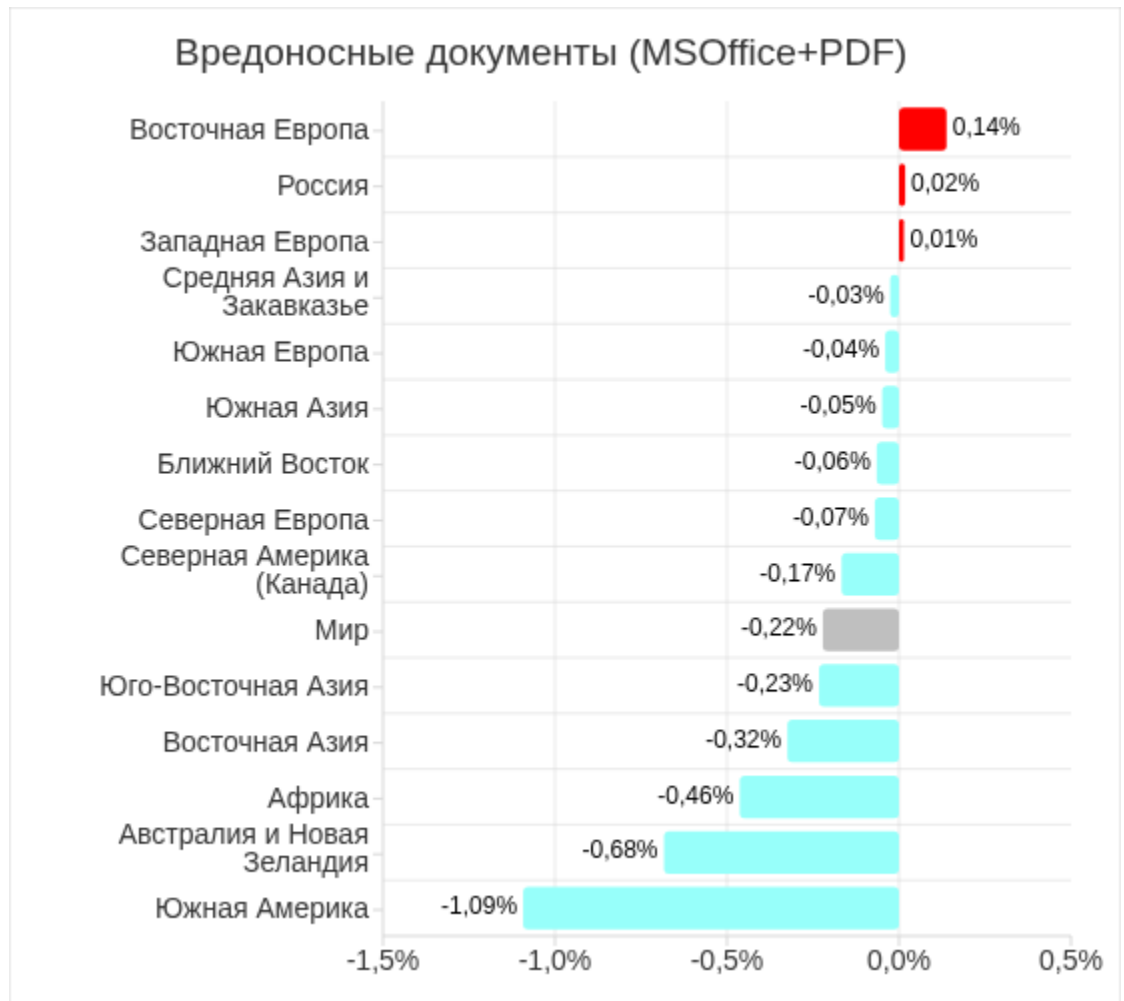
В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные документы, варьирует от 0,46% в Северной Европе до 3,82% в Южной Европе. В тройку лидеров по этому показателю по-прежнему входят Южная Европа и Южная Америка, а вот Ближний Восток с третьего места вытеснила Восточная Европа.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы



В четвертом квартале 2025 года показатель вырос в трех регионах: в Восточной Европе, России и Западной Европе.

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

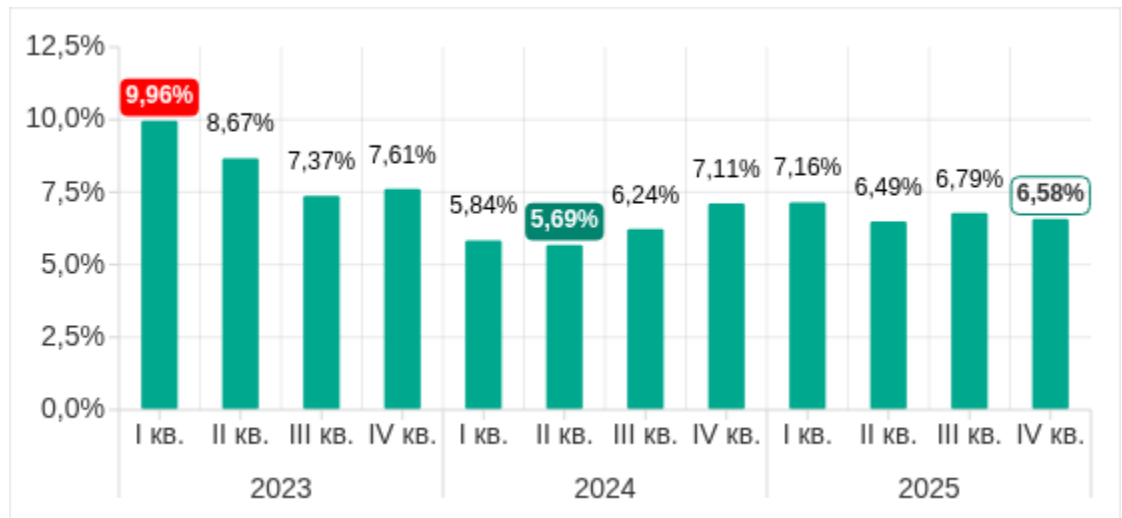


Вредоносные скрипты и фишинговые страницы (JS и HTML)

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 четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, уменьшилась до 6,58%. Несмотря на снижение показателя, эта категория заняла первое место в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, I квартал 2023 года – IV квартал 2025 года



В 2025 году наибольший месячный показатель был в августе. Из показателей трех месяцев четвертого квартала самый высокий отмечен в ноябре.



Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, январь 2024 года – декабрь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, варьирует от 2,52% в Северной Европе до 10,50% в Южной Азии, которая подскочила с восьмого на первое место в соответствующем рейтинге регионов.

В то же время Восточная Азия переместилась со второго на 12-е место. В третьем квартале 2025 года показатель в регионе увеличился на 5,23 п. п. в результате локального распространения вредоносных скриптов-шпионов, загружающихся в память популярных Torrent и MediaGet клиентов. В четвертом квартале он вернулся практически к обычному для региона значению.

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



За квартал показатель вырос в четырех регионах: в Южной Азии, Южной Америке, Южной Европе и Африке. Самое значительное изменение — на 3,47 п. п. — отмечено в Южной Азии.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, IV 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 (тройные шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО (тройные шпионы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструментальный промежуточных этапов кибератаки (например, разведки и

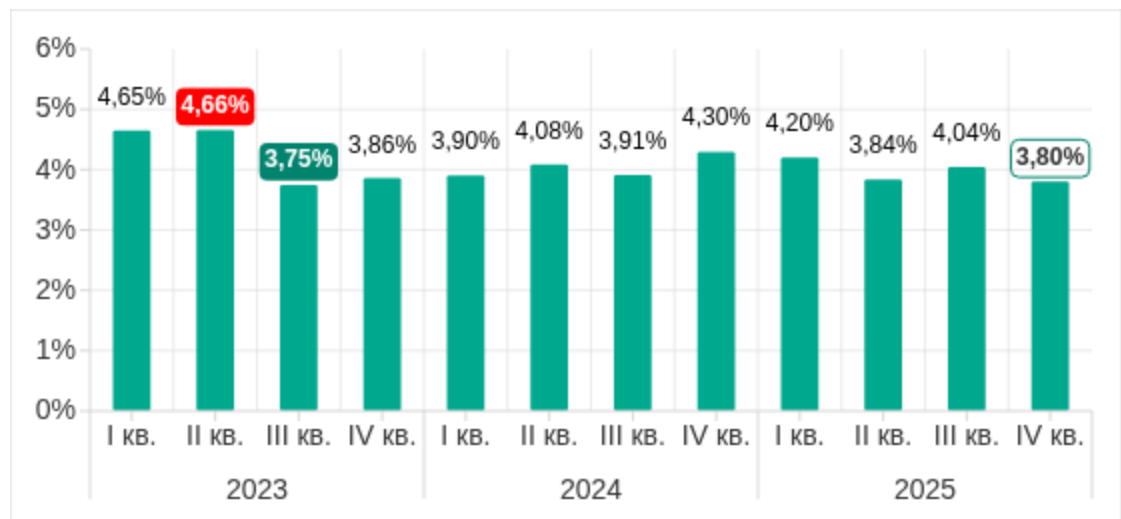
распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных. В большинстве случаев конечная цель атак с применением такого ПО — кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

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 четвертом квартале 2025 года доля компьютеров АСУ, на которых было заблокировано шпионское ПО, уменьшилась до 3,80%. При этом шпионские программы второй квартал подряд занимают второе место в рейтинге категорий угроз по доле атакованных компьютеров.

Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, I квартал 2023 года – IV квартал 2025 года



В 2025 году самым высоким месячный показатель шпионских программ был в феврале. В четвертом квартале 2025 года показатели в октябре и ноябре были меньше, чем в остальные месяцы года.



Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, январь 2024 года – декабрь 2025 года

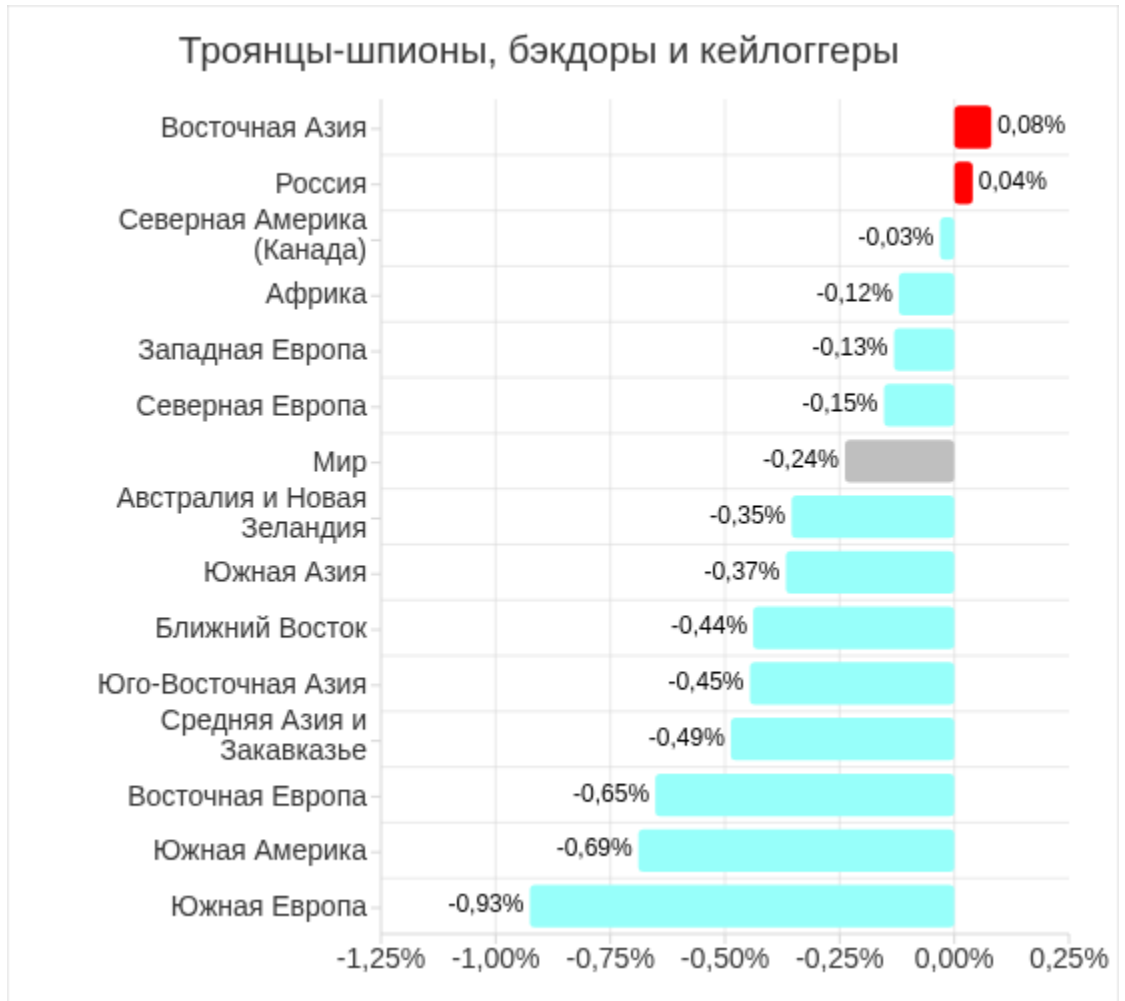
В регионах доля компьютеров АСУ, на которых было заблокировано шпионское ПО, варьирует от 1,25% в Северной Европе до 6,21% в Африке. В топ 3 регионов по этому показателю, как и прежде, входят Африка, Юго-Восточная Азия и Южная Европа.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы



За квартал доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла в Восточной Азии и России.

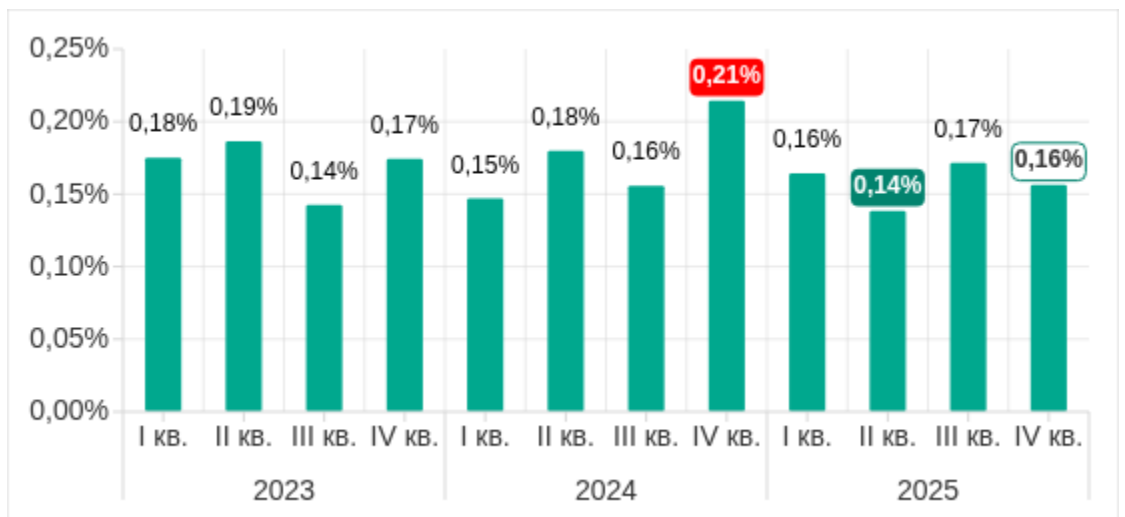
Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, IV квартал 2025 года



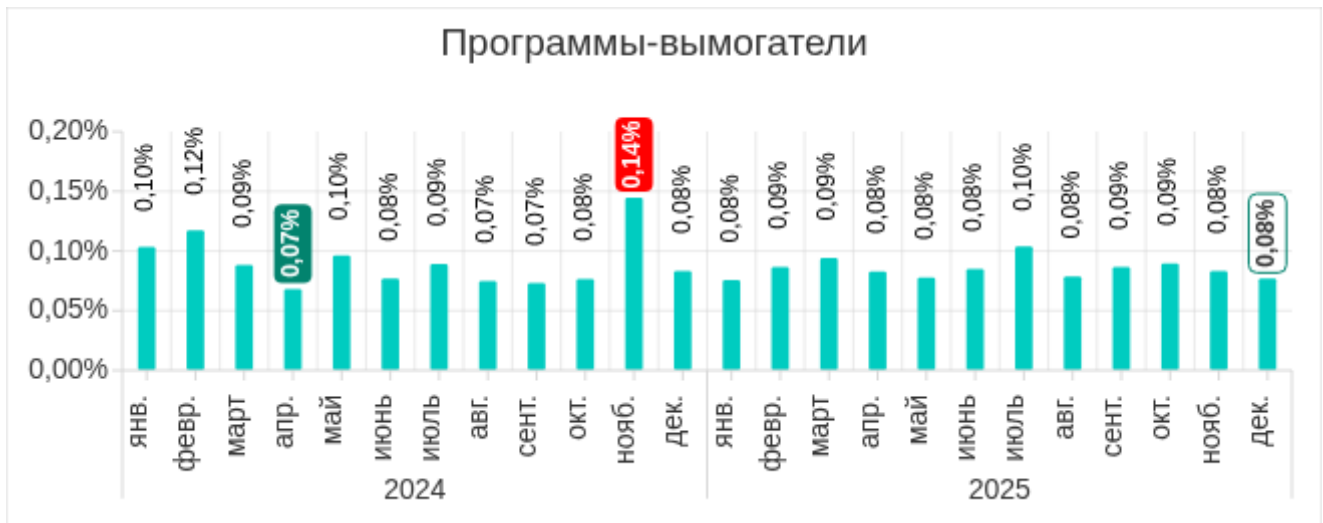
Программы-вымогатели

В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, уменьшилась до 0,16%.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, I квартал 2023 года – IV квартал 2025 года



Самым высоким за год значение месячного показателя было в июле.

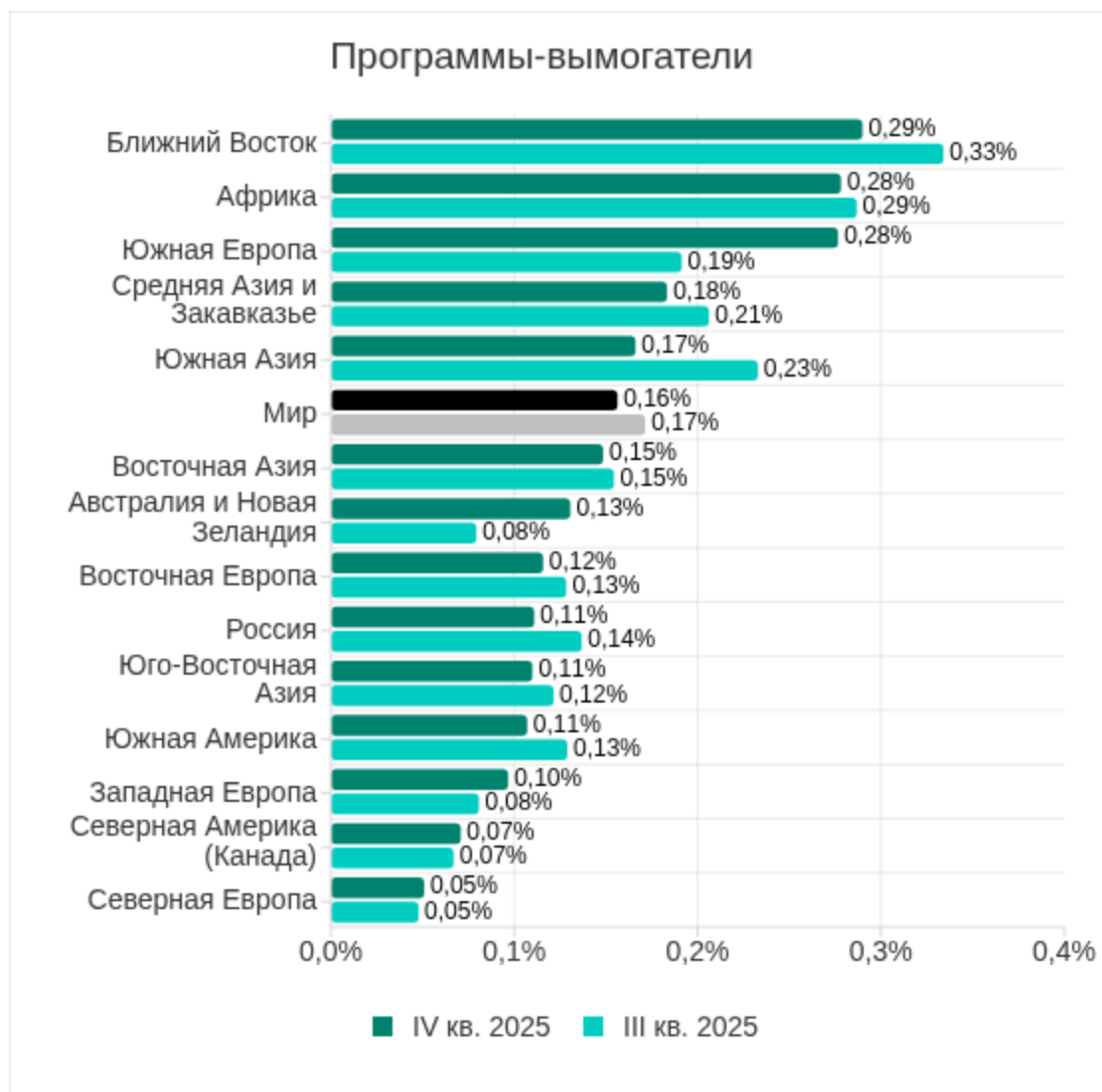


Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели,
январь 2024 года – декабрь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, варьирует от 0,05% в Северной Европе до 0,29% на Ближнем Востоке. Кроме Ближнего Востока в топ 3 регионов входят Африка и Южная Европа, которая в четвертом квартале 2025 года поднялась в этом рейтинге с пятого на третье место. Показатель в Южной Европе увеличился в 1,47 раза.

В четвертом квартале 2025 года Южная Европа лидирует среди регионов по показателю программ-вымогателей в отрасли автоматизация зданий с 0,61% – это в 1,5 раза больше, чем в предыдущем квартале (0,41%).

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, значительно выросла в трех регионах: в Южной Европе, Австралии и Новой Зеландии, а также в Западной Европе.

Изменение доли компьютеров АСУ, на которых были заблокированы программы-вымогатели, IV 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

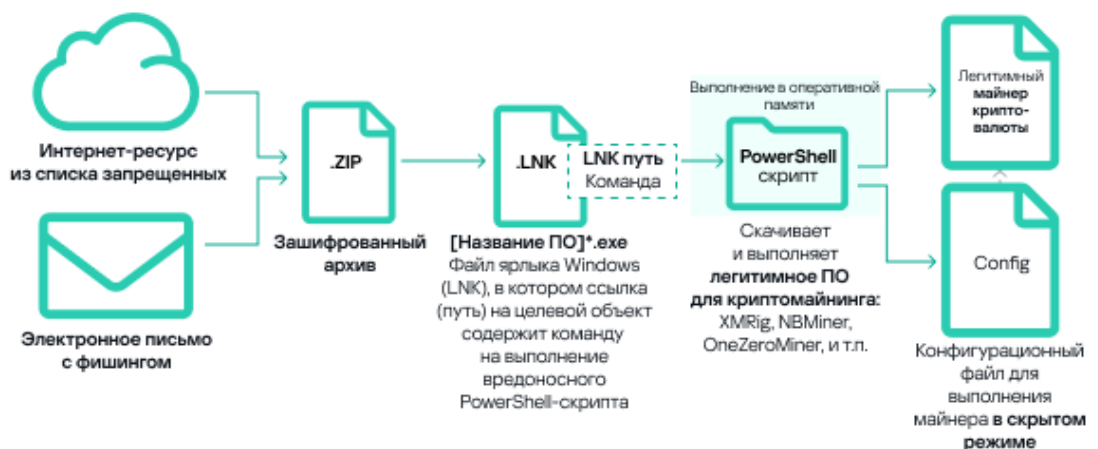
выбирают PowerShell, с помощью которого код вредоносного ПО (в том числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом. Бесфайловое выполнение майнера делает проблематичным его обнаружение средствами защиты.

Цепочка атаки:
пример
бесфайлового
исполнения в
майнинговых
атаках



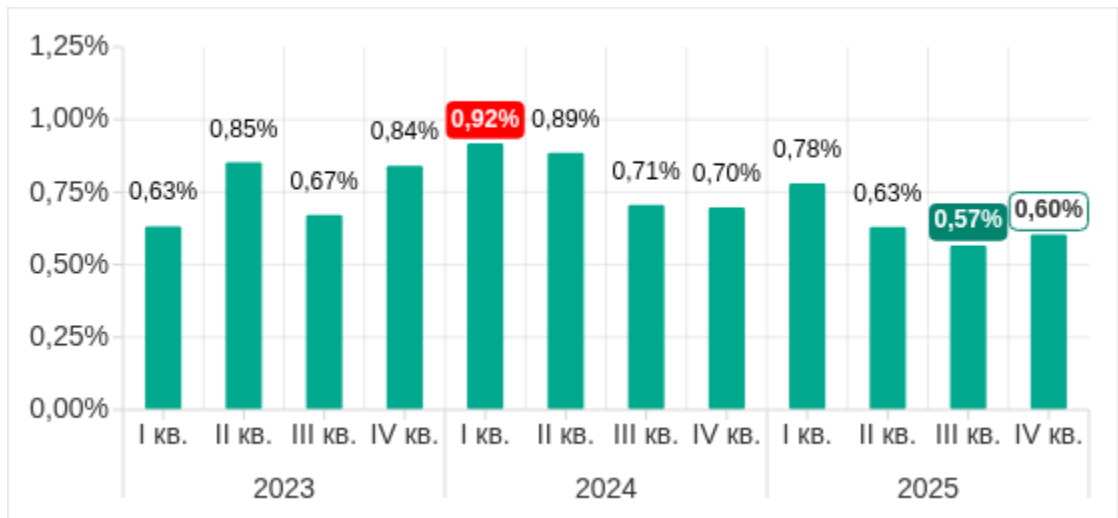
Еще одним популярным методом внедрения майнеров в технологическую инфраструктуру является использование легитимных криптомайнеров, таких как XMRig, NBMiner, OneZeroMiner и т. д. Сами по себе эти майнеры не являются вредоносными, однако защитные системы классифицируют их как [RiskTools](#). Злоумышленники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

Цепочка атаки:
пример
с использова-
нием
легитимных
крипто-
майнеров



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были выявлены майнеры в формате исполняемых файлов для Windows, увеличилась до 0,60%.

Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, I квартал 2023 года – IV квартал 2025 года



Самый высокий месячный показатель в 2025 году отмечен в феврале. Июль, август, сентябрь и декабрь стали месяцами с минимальными за год значениями.

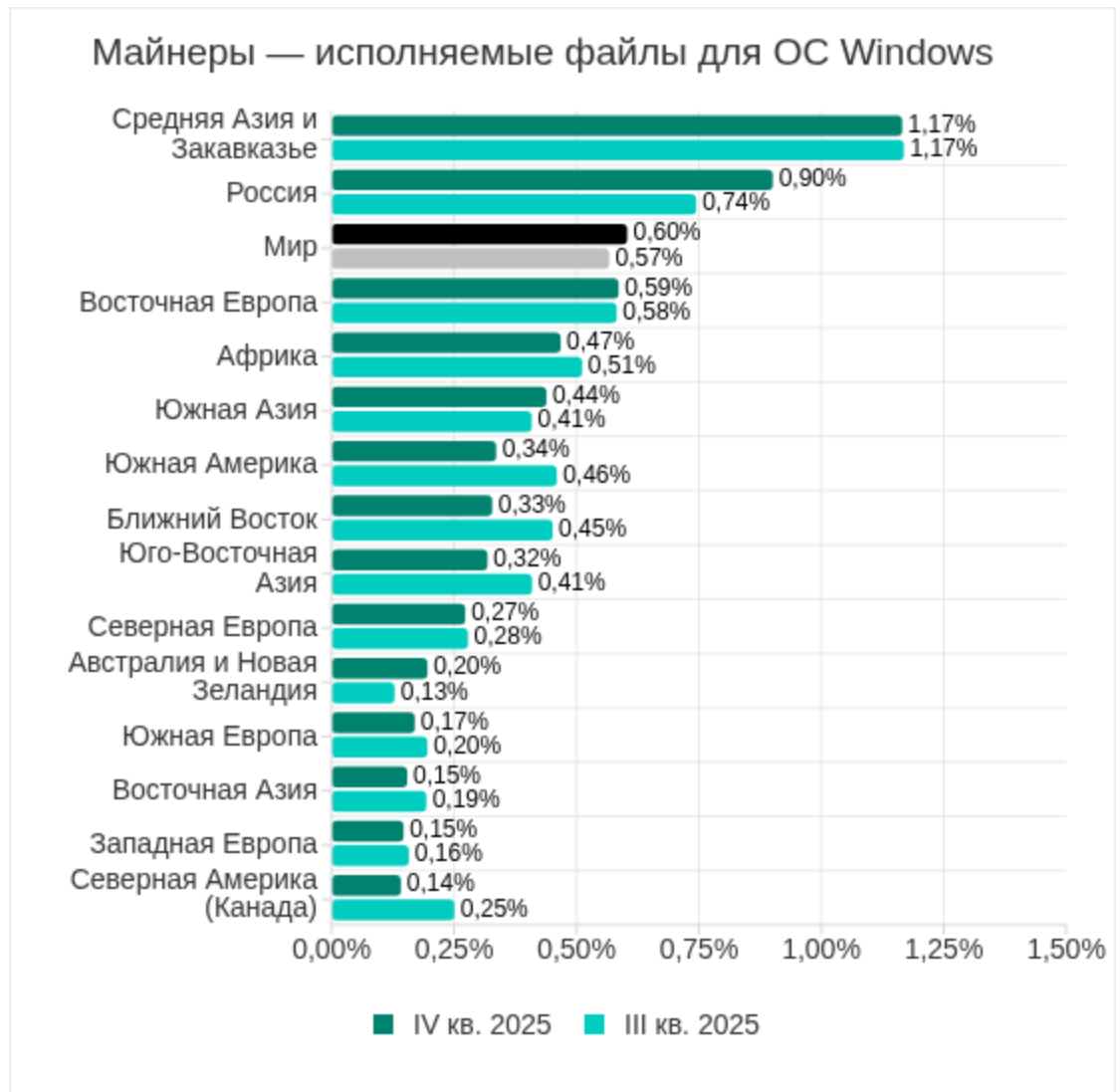
Майнеры — исполняемые файлы для ОС Windows



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, январь 2024 года – декабрь 2025 года

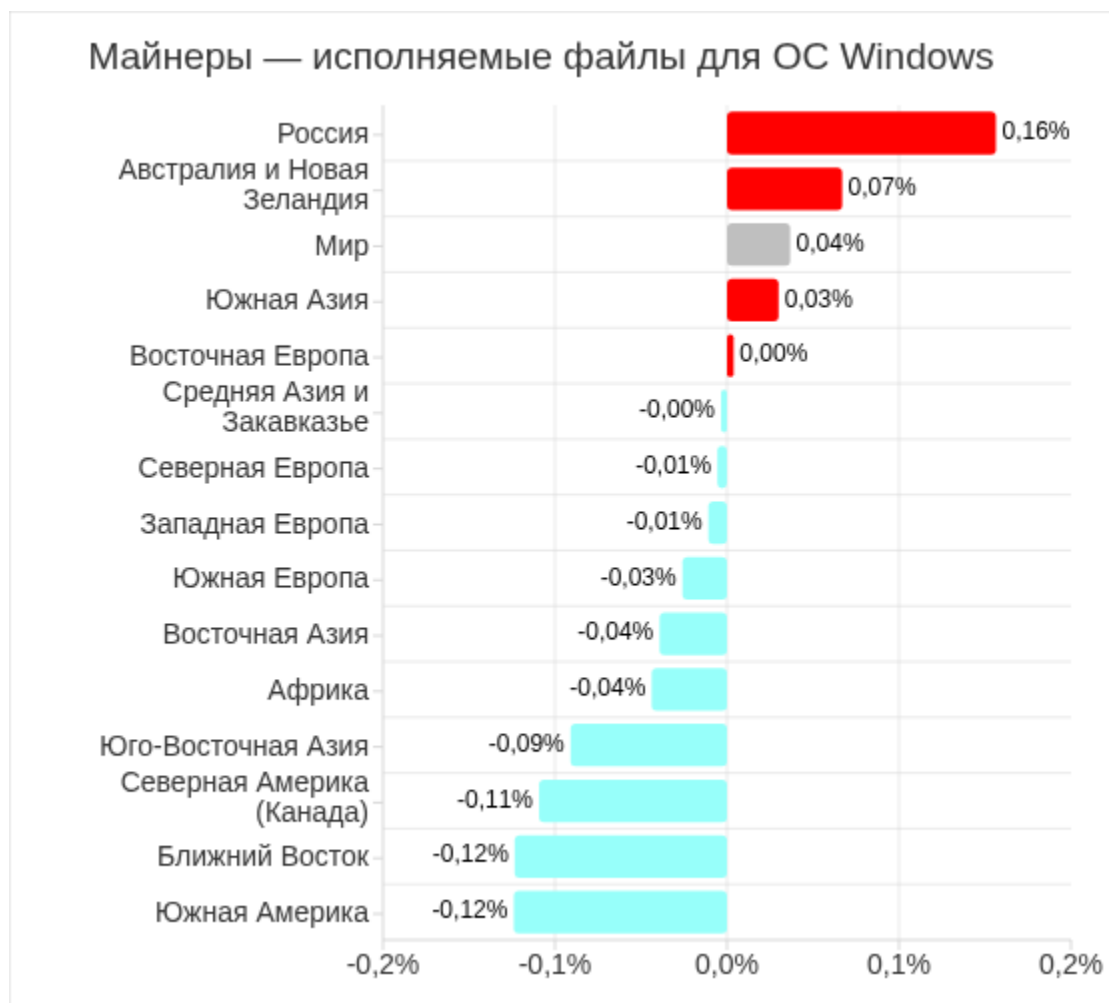
В регионах доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, варьирует от 0,14% в Северной Америке (Канада) до 1,17% в Средней Азии и Закавказье. В тройку лидеров по этому показателю по-прежнему входят Средняя Азия и Закавказье, Россия и Восточная Европа.

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



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, в четвертом квартале 2025 года увеличилась в четырех регионах: в России, Австралии и Новой Зеландии, Южной Азии и Восточной Европе. Больше всего показатель вырос в России.

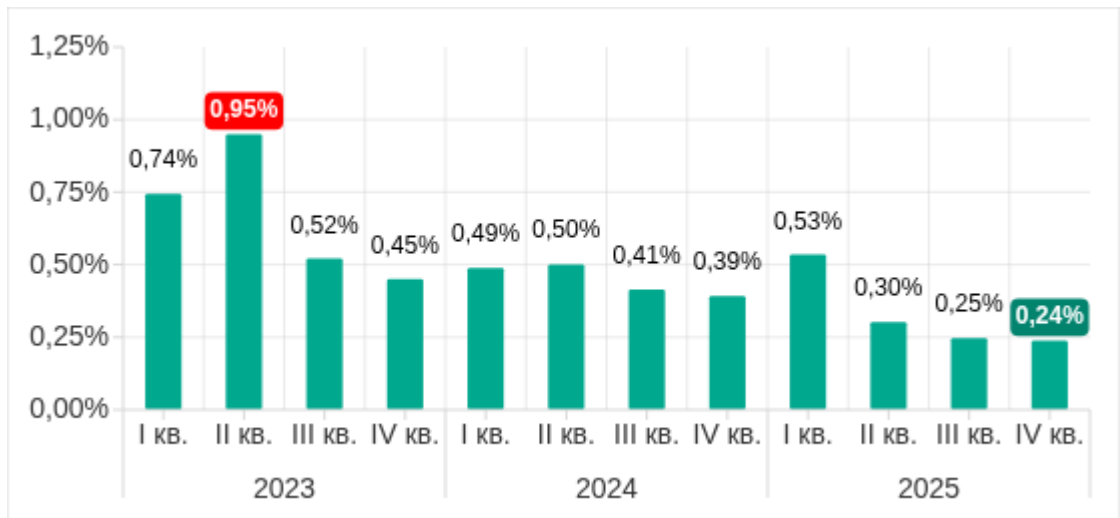
Изменение доли компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows, IV квартал 2025 года



Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, в четвертом квартале 2025 года уменьшилась до 0,24%. Это минимальное значение за рассматриваемый период.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, I квартал 2023 года – IV квартал 2025 года



Самым высоким месячным показателем за рассматриваемый период был отмечен в марте 2025 года. В сентябре и декабре 2025 года показатели были наименьшими.



Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, январь 2024 года – декабрь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, варьирует от 0,06% в Восточной Азии до 0,34% в Юго-Восточной Азии. Топ 3 регионов по этому показателю: Юго-Восточная Азия, Южная Америка и Африка.

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



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы веб-майнеры, увеличилась в трех регионах — Австралии и Новой Зеландии (в 1,67 раза), России и Северной Европе. В Австралии наиболее заметный рост показателя за квартал отмечен в отрасли автоматизация зданий — с 0,09% до 0,26%, почти в три раза.

Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, IV 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 в основном распространяются в сетях АСУ через съемные носители и сетевые папки в форме зараженных файлов — архивов с бэкапами, офисными документами, пиратскими играми и взломанными приложениями. В более редких и опасных случаях зараженными оказываются веб-страницы с настройками сетевого оборудования, а также файлы, хранящиеся во внутренних системах документооборота, управления жизненным циклом продукта (PLM), управления ресурсами (ERP) и других интранет-сервисах.

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

Следует иметь в виду, что распространение может происходить и в активной форме — с использованием техник перебора пароля, кражи и использования данных аутентификации пользователя (включая токены доступа), а также сетевых атак на уязвимое ПО — все это давно входит в модульный инструментарий любого современного майнера-червя.

Современные версии червей встречаются в сетях АСУ не часто, но наносимый в случае заражения ущерб всегда значительный — даже простое обслуживание сети, зараженной майнерами-червями, становится кратно дороже из-за большего времени простоя (downtime) и дополнительных человеко-часов, необходимых для восстановления работоспособности. А в случае загрузки через червя на компьютер в технологической сети программы-вымогателя после предварительного профилирования — дороже на порядок.

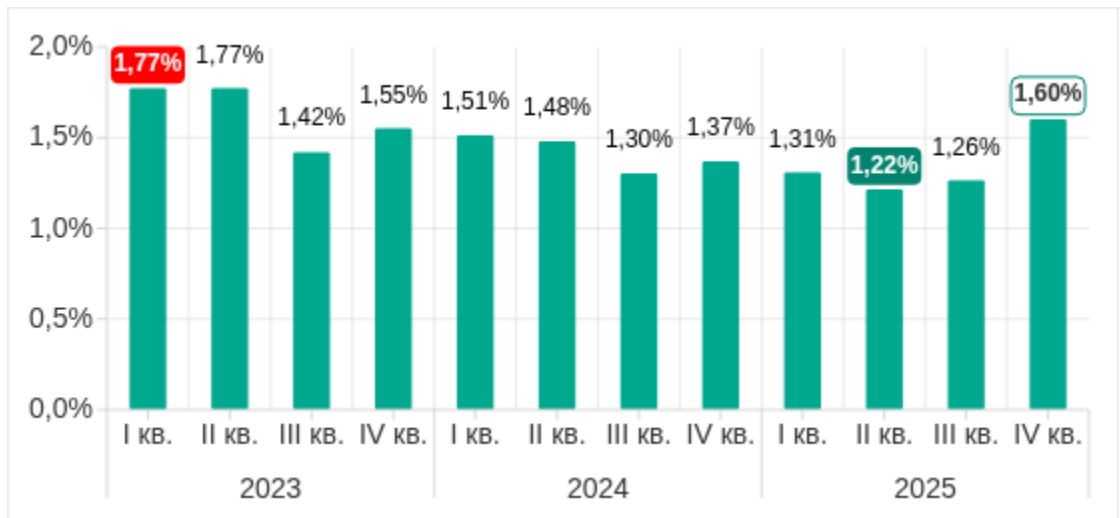
Вместе с тем, среди распространяющихся вирусов и червей довольно много старых модификаций, их командные серверы уже отключены. Тем не менее, они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, но также могут приводить к сбоям в работе ПО, 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.

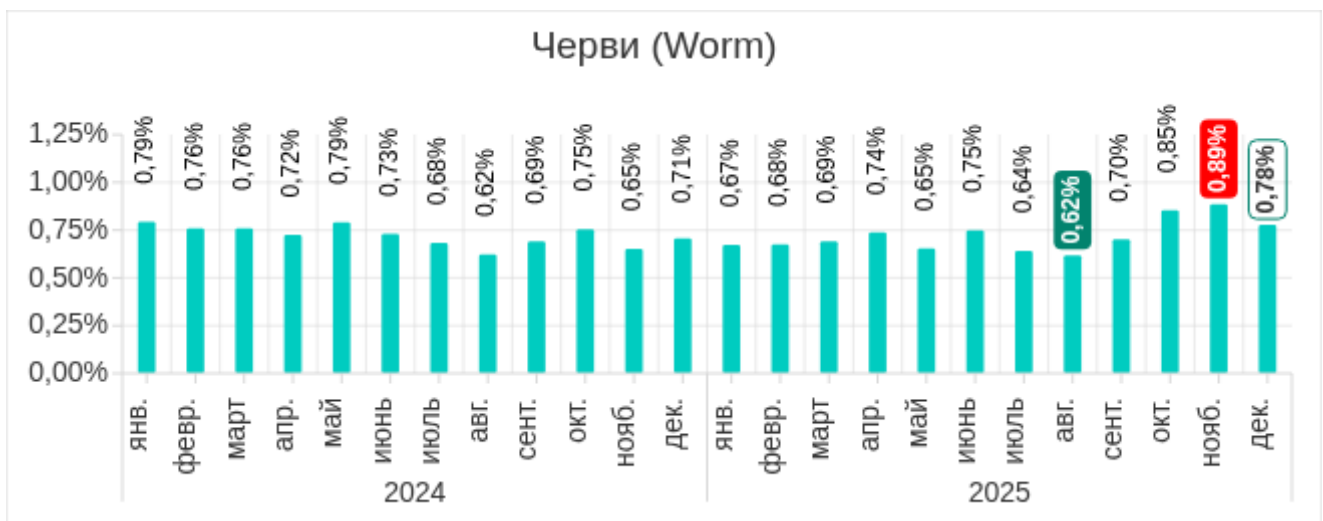
Черви

Доля компьютеров АСУ, на которых были заблокированы черви, в четвертом квартале 2025 года увеличилась в 1,6 раза — до 1,60%. Как мы писали выше, этот рост связан с глобальной фишинговой атакой, в ходе которой по всем регионам мира распространялся червь-бэкдор Backdoor.MSIL.XWorm.

Доля компьютеров АСУ, на которых были заблокированы черви, I квартал 2023 года – IV квартал 2025 года



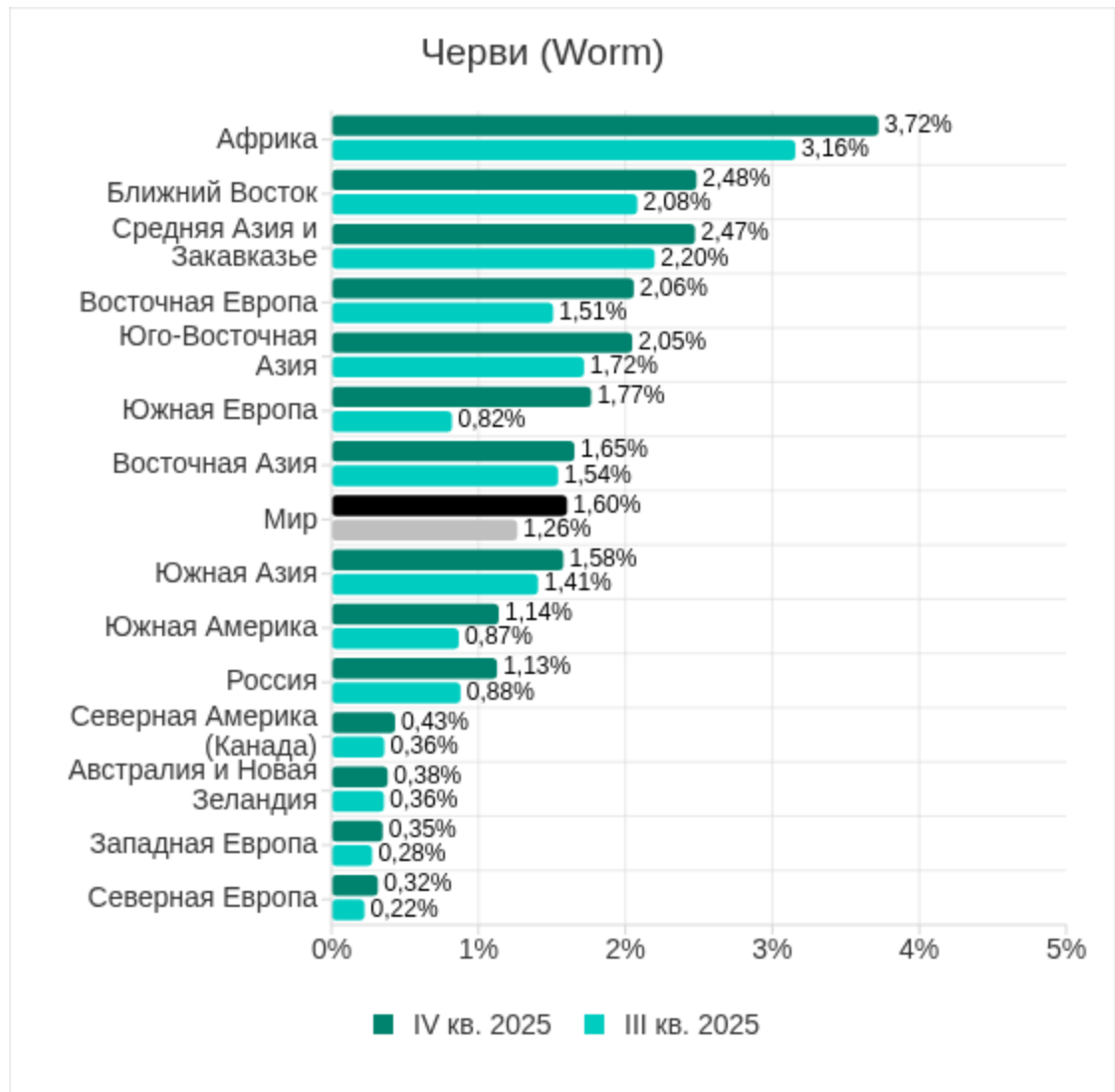
В 2025 году самыми высокими показателями за месяц были в четвертом квартале. В октябре и ноябре, в ходе двух волн фишинговой атаки, показатель рос. В декабре доля компьютеров АСУ, на которых блокировались черви, уменьшилась, однако значение все равно превысило показатели остальных месяцев 2025 года.



Доля компьютеров АСУ, на которых были заблокированы черви, январь 2024 года – декабрь 2025 года

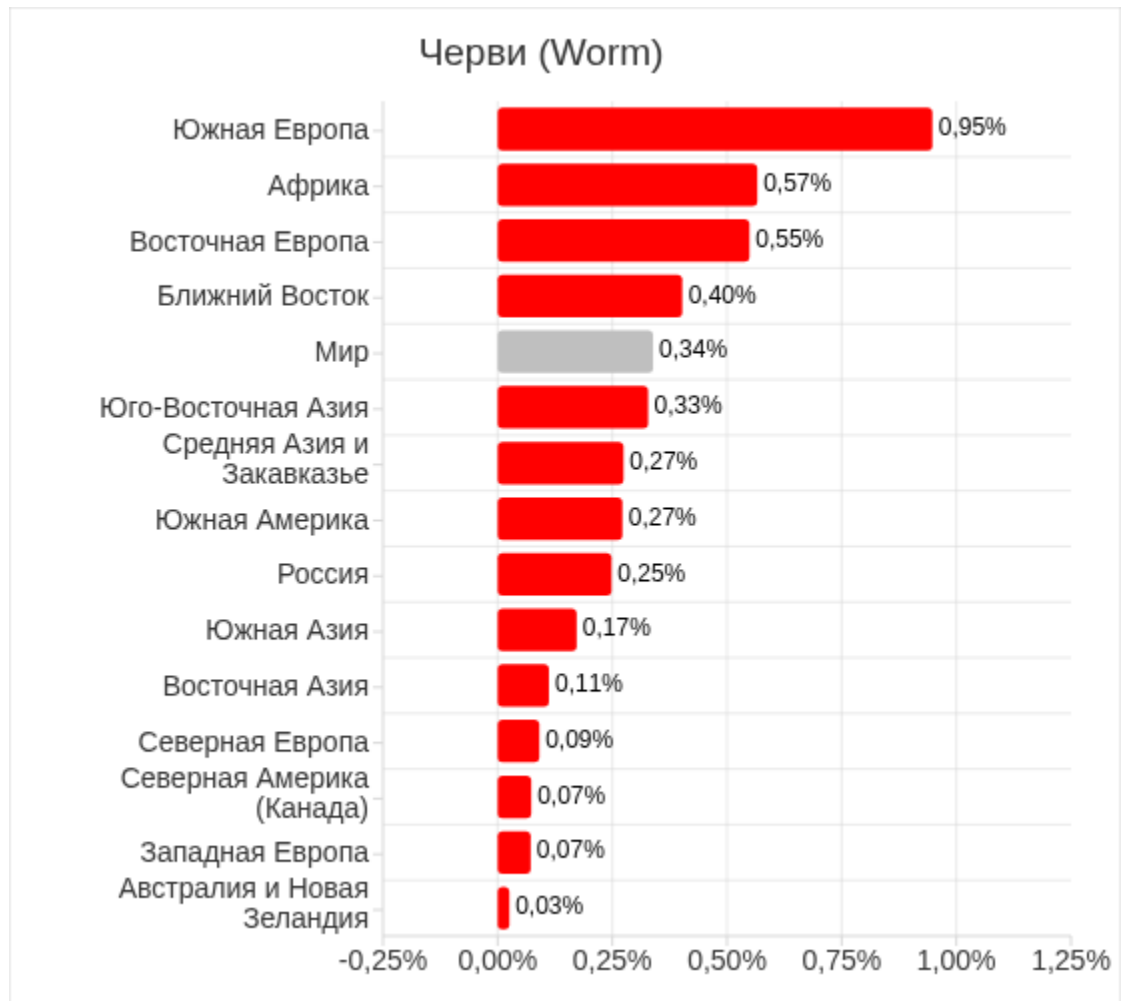
В регионах доля компьютеров АСУ, на которых были заблокированы черви, варьирует от 0,32% в Северной Европе до 3,72% в Африке. В тройку регионов, лидирующих по этому показателю, по-прежнему входят Африка, Ближний Восток, Средняя Азия и Закавказье.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы черви



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы черви, выросла во всех регионах, больше всего — в 2,16 раза — в Южной Европе. Основным каналом распространения вредоносного ПО была электронная почта, а Южная Европа лидирует по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов. В то же время в Африке, где все еще активно используются USB-носители, Backdoor.MSIL.XWorm блокировался и при подключении к компьютерам АСУ съемных устройств.

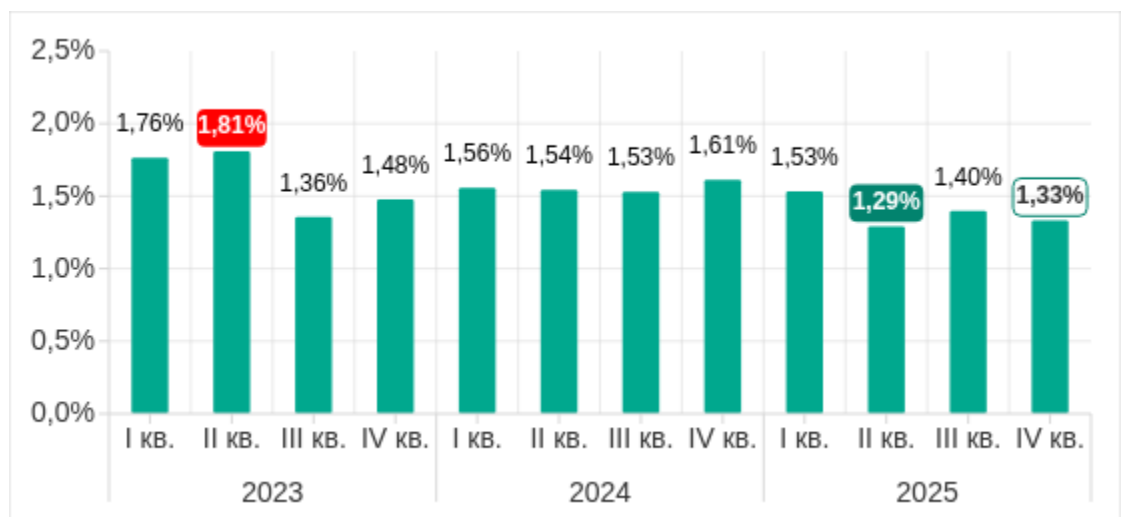
Изменение доли компьютеров АСУ, на которых были заблокированы черви, IV квартал 2025 года



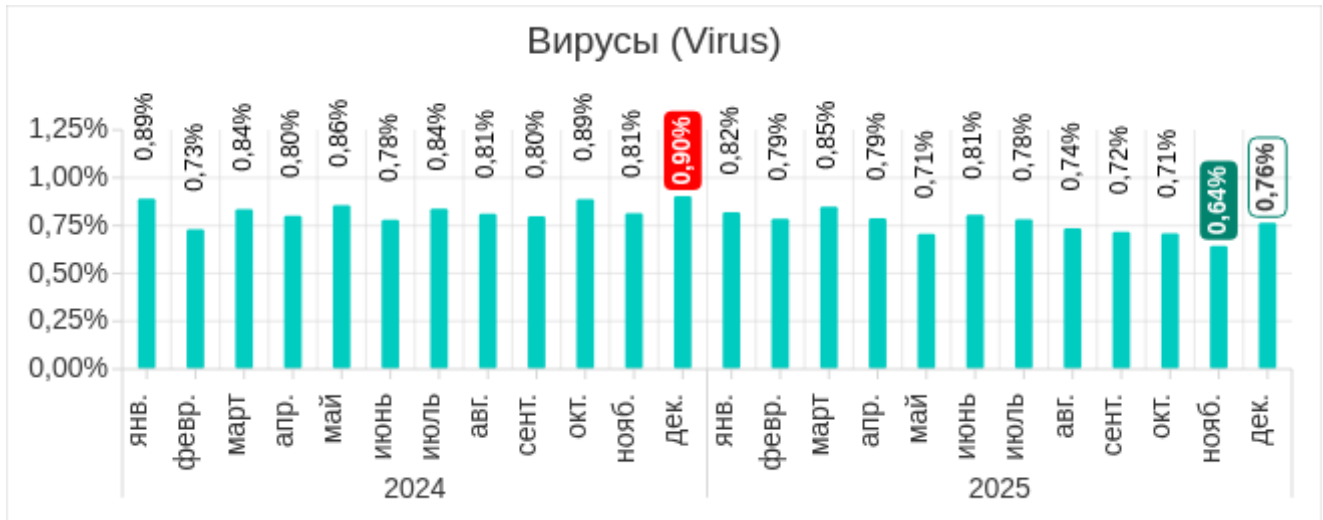
Вирусы

Доля компьютеров АСУ, на которых были заблокированы вирусы, в четвертом квартале 2025 года уменьшилась до 1,33%.

Доля компьютеров АСУ, на которых были заблокированы вирусы, I квартал 2023 года – IV квартал 2025 года



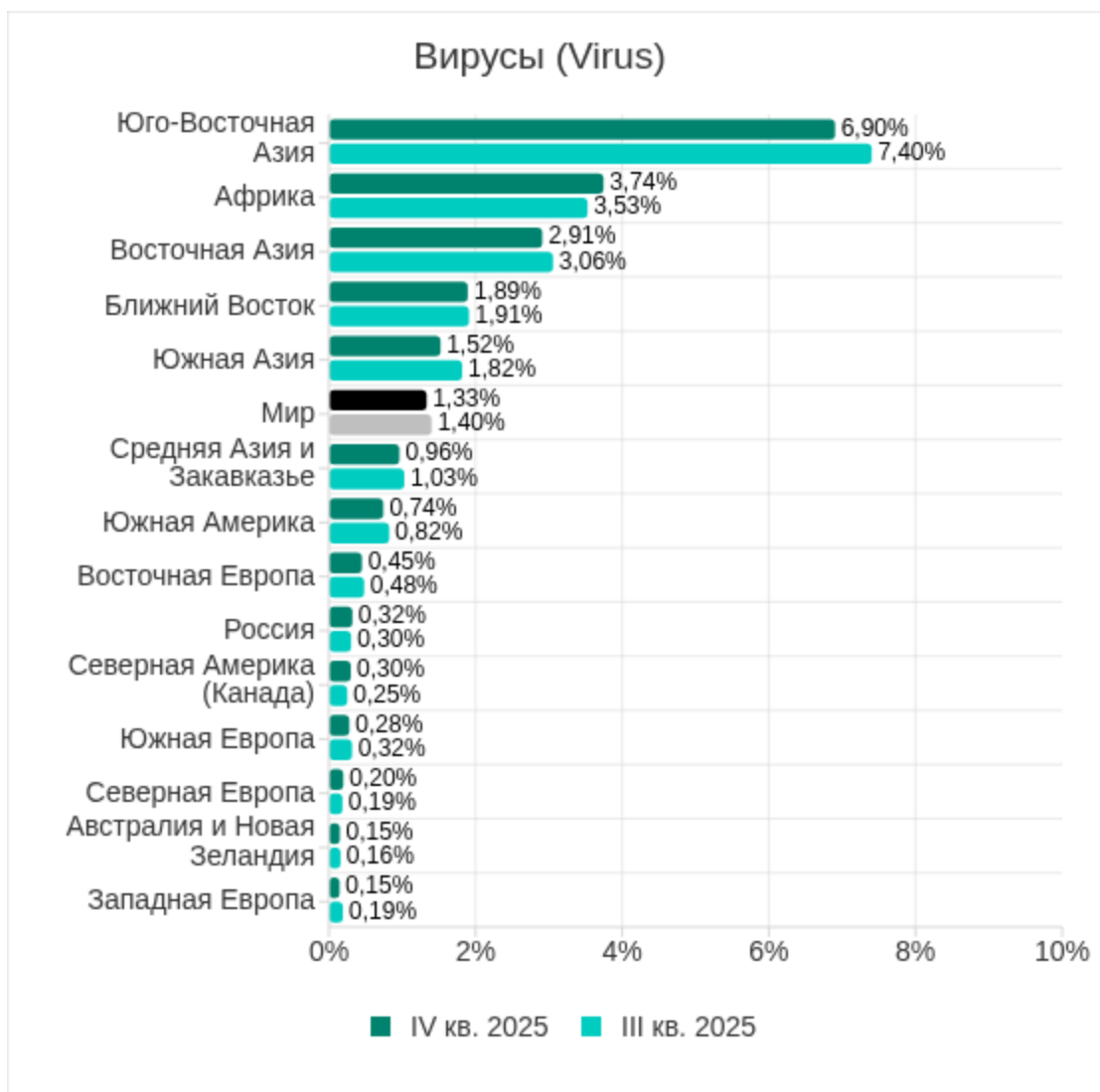
В 2025 году наибольшее месячное значение показателя было в марте. Минимум пришелся на ноябрь, в декабре показатель вырос.



Доля компьютеров АСУ, на которых были заблокированы вирусы,
январь 2024 года – декабрь 2025 года

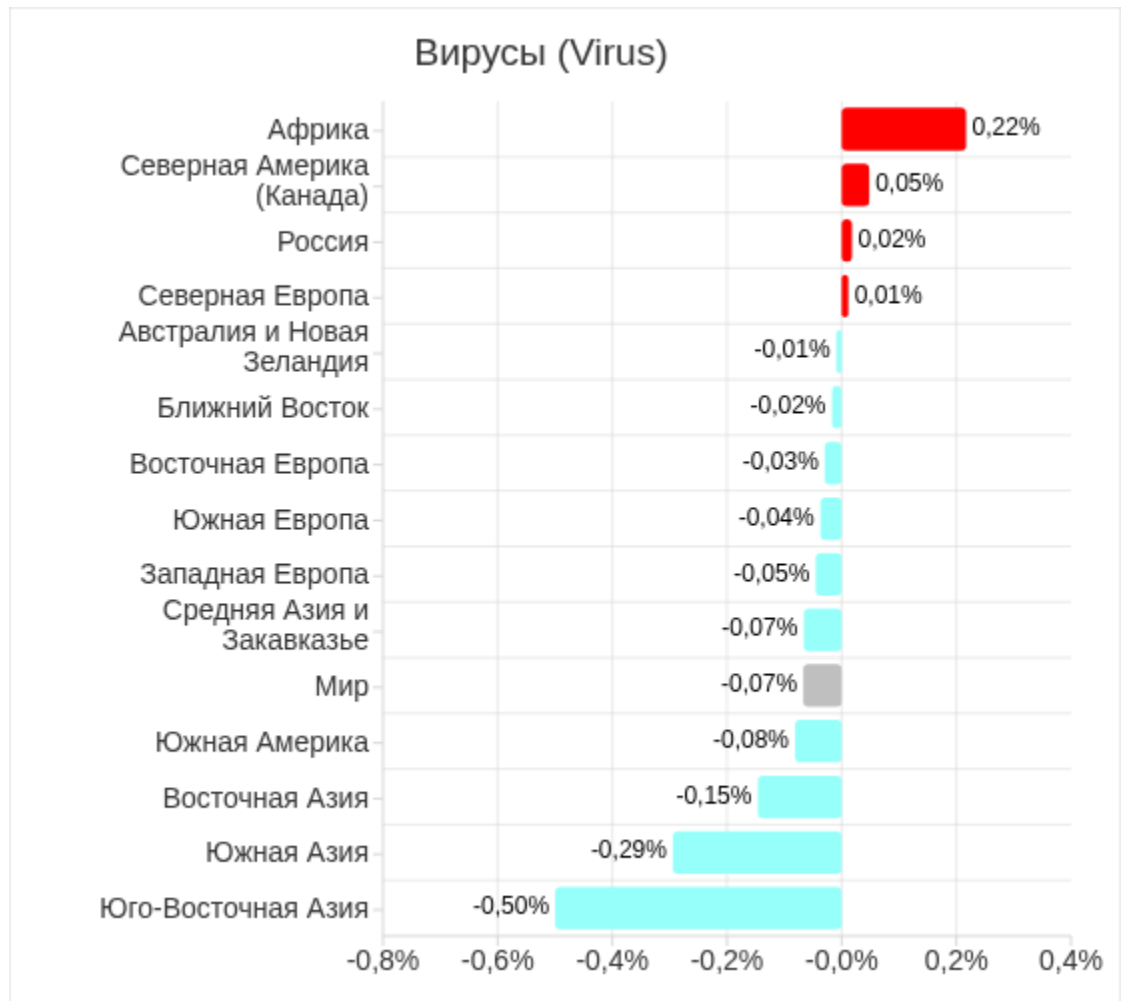
В регионах доля компьютеров АСУ, на которых были заблокированы вирусы, варьирует от 0,15% в Западной Европе до 6,90% в Юго-Восточной Азии. Топ 3 регионов по этому показателю не изменился: Юго-Восточная Азия (с большим отрывом от остальных), Африка и Восточная Азия, Эти же регионы входят в список лидеров и в случае вредоносных программ для AutoCAD.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вирусы



Доля компьютеров АСУ, на которых были заблокированы вирусы, в четвертом квартале 2025 года увеличилась в четырех регионах: в Африке, Северной Америке (Канада), России и Северной Европе. Больше всего показатель увеличился в Африке.

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



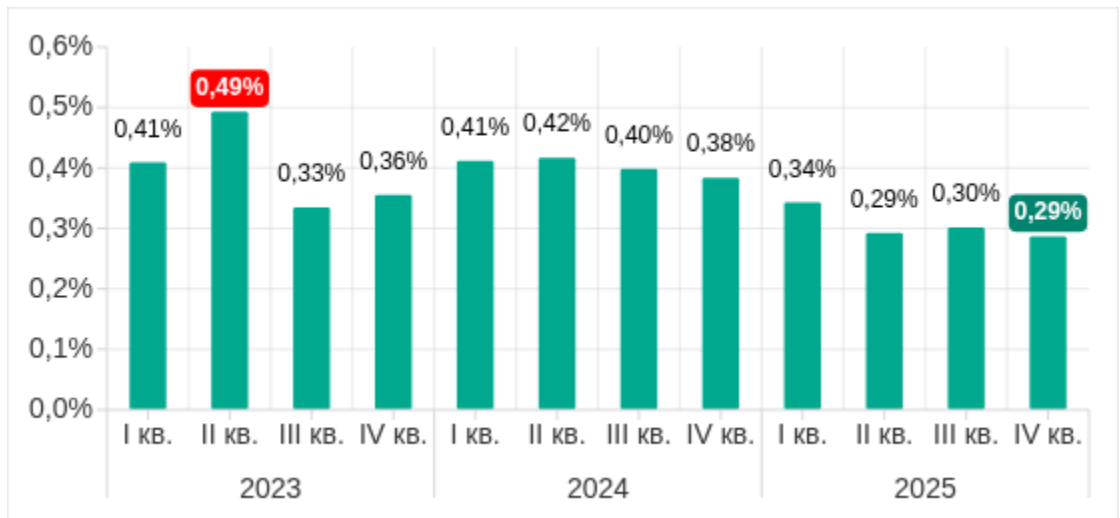
Вредоносные программы для AutoCAD

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

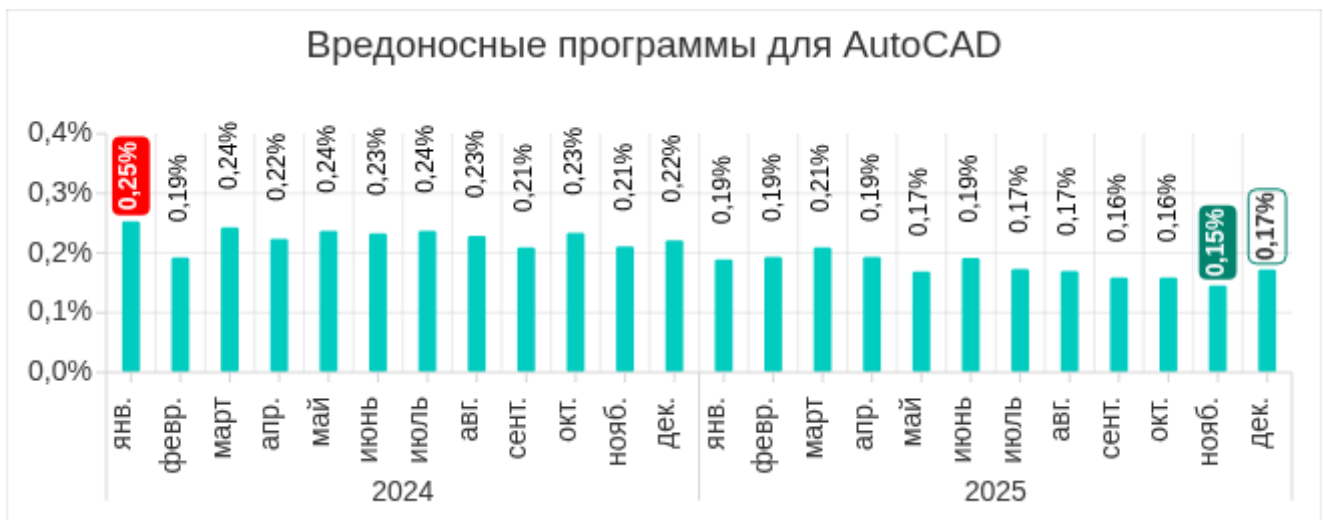
Как правило, вредоносные программы для AutoCAD — минорная угроза, которая в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых она была заблокирована, занимает последние места.

В четвертом квартале 2025 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, после роста в предыдущем квартале вновь уменьшилась до 0,29%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, I квартал 2023 года – IV квартал 2025 года



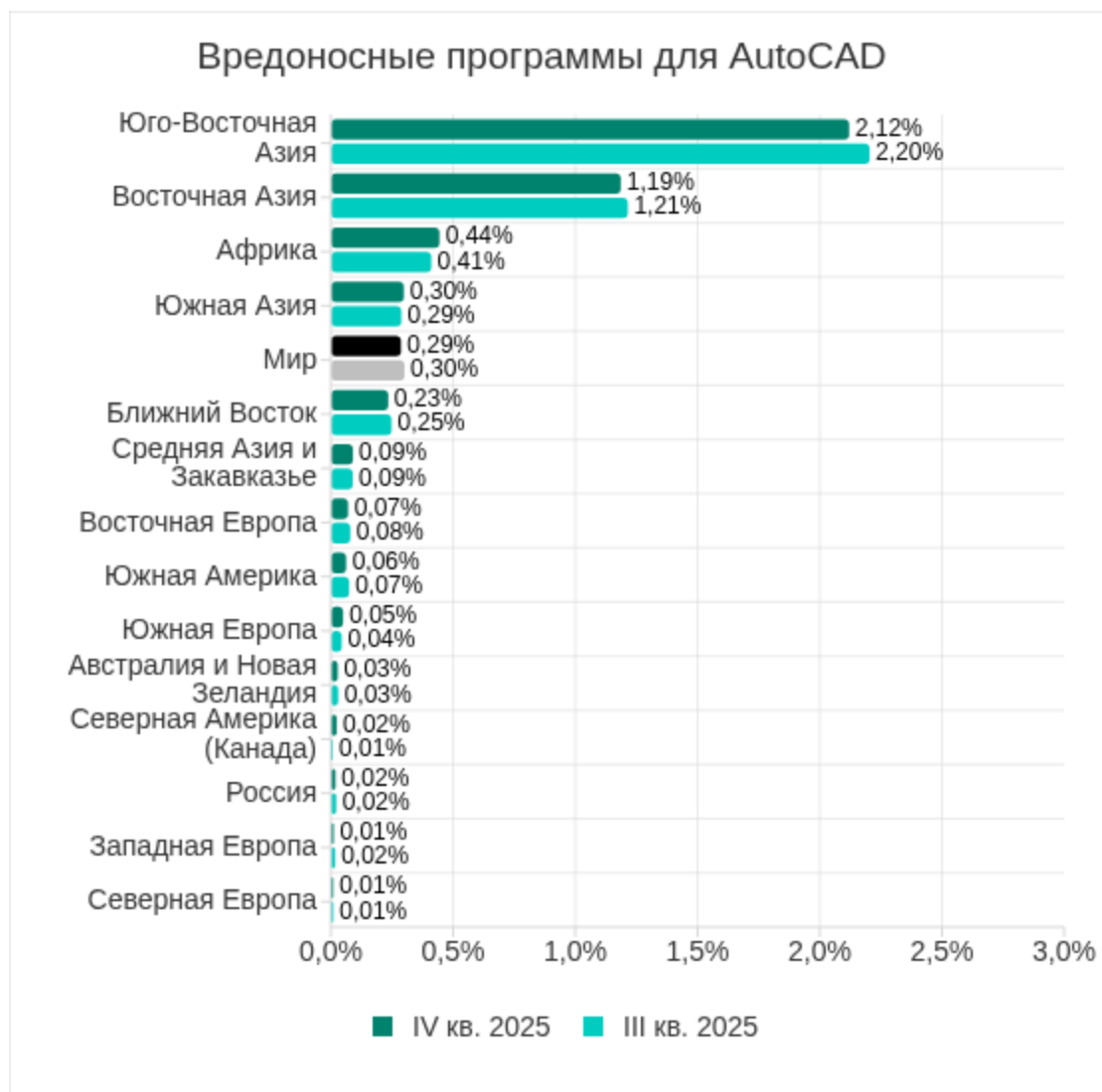
Как и в случае вирусов, максимальное месячное значение показателя было в марте, минимум 2025 года пришелся на ноябрь.



Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, январь 2024 года – декабрь 2025 года

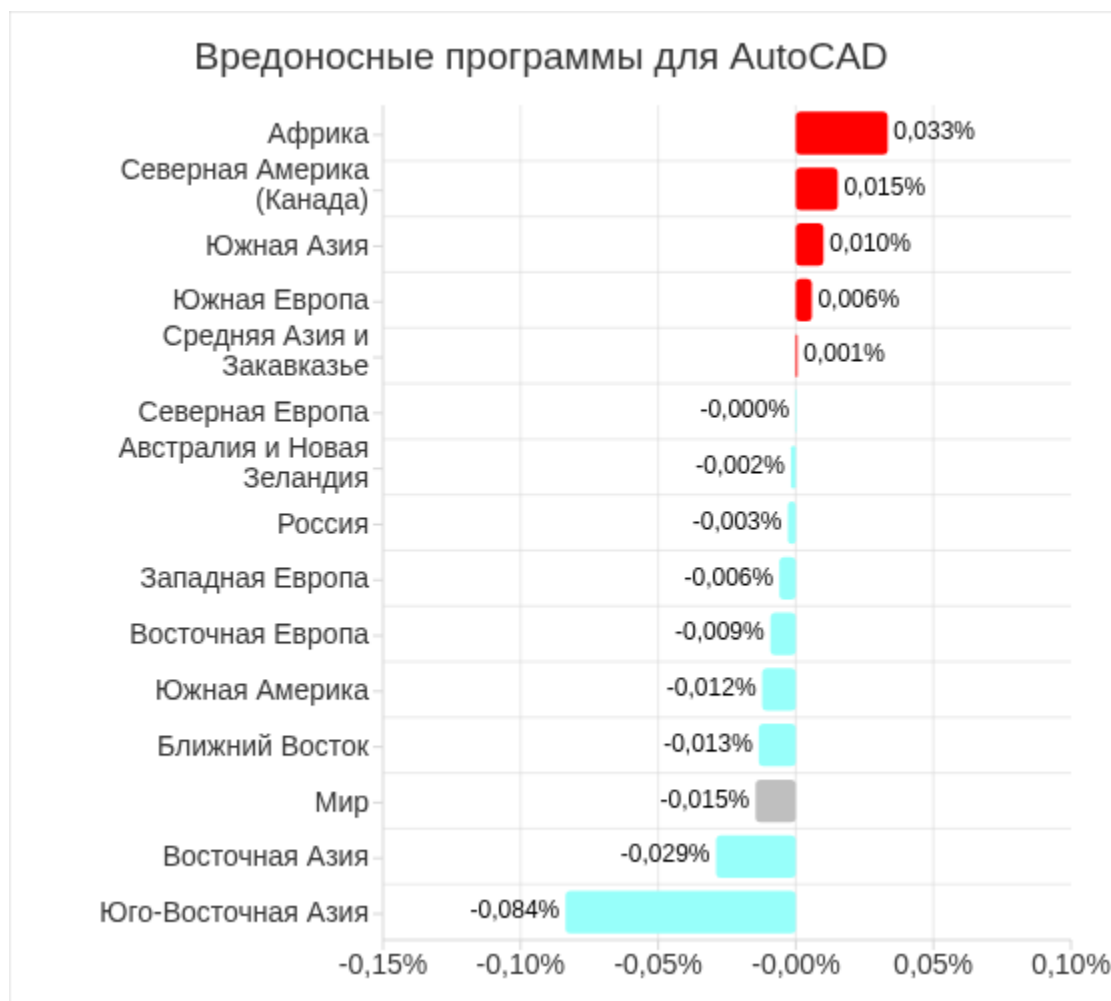
В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, варьирует от 0,01% в Северной Европе до 2,12% в Юго-Восточной Азии. Лидируют по этому показателю те же регионы, что и в рейтинге по вирусам: Юго-Восточная Азия, Восточная Азия (оба региона с отрывом от остальных) и Африка.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD



Показатель вредоносных программ для AutoCAD в четвертом квартале 2025 года увеличился в пяти регионах, больше всего — в Африке.

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



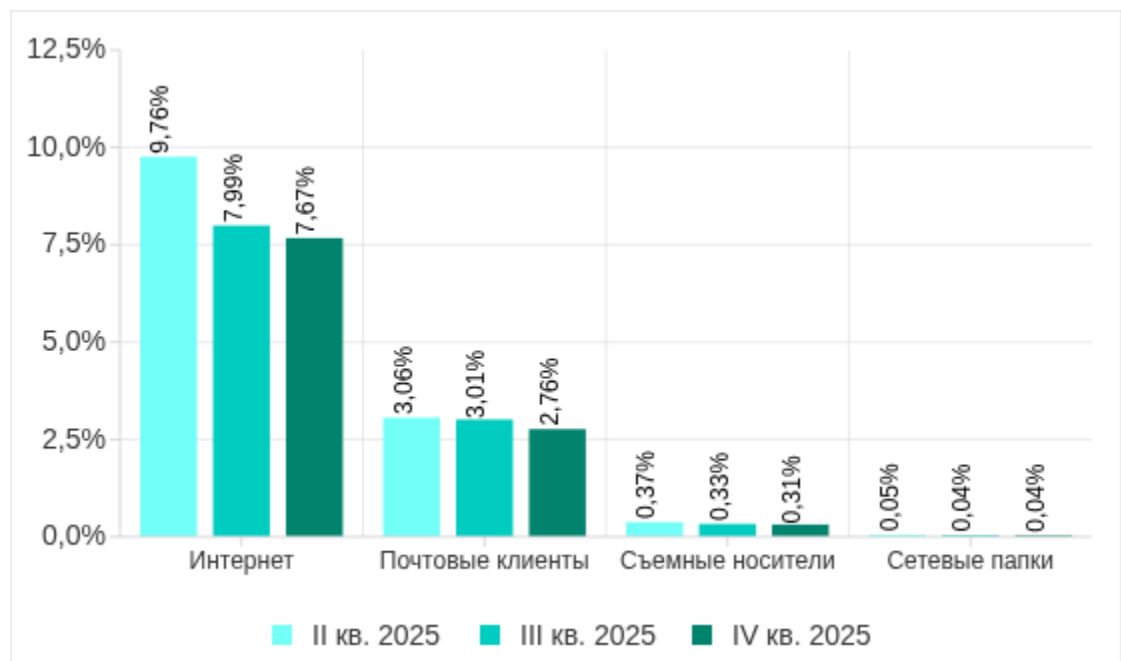
Основные источники угроз

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 четвертом квартале 2025 года показатели всех источников угроз в среднем по миру уменьшились. Показатели всех источников, кроме почтовых клиентов, были наименьшими за три года.

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

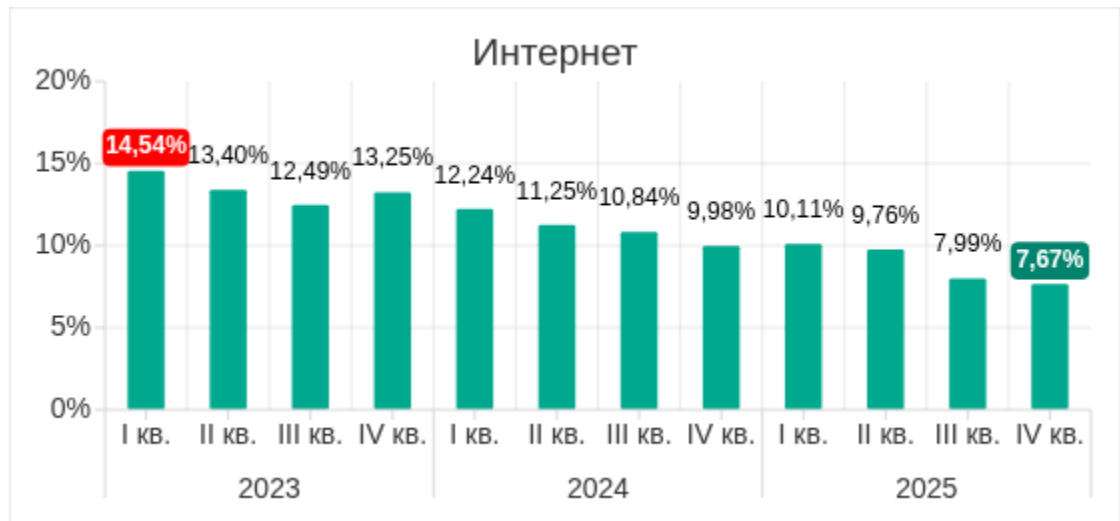


Интернет

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

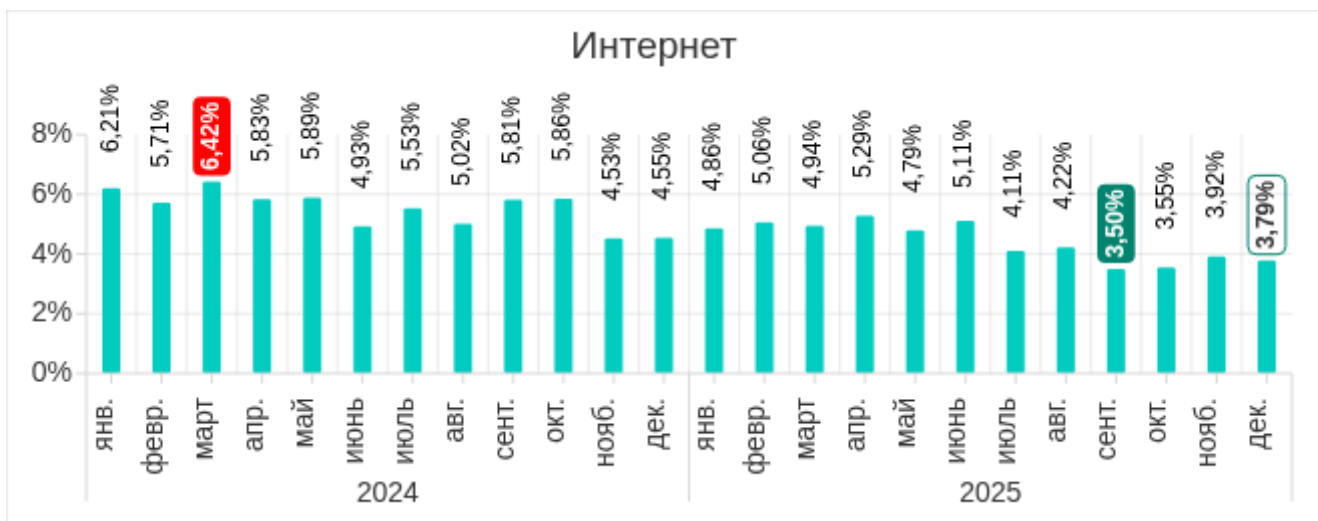
В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, уменьшилась до 7,67% — это наименьший показатель с начала 2023 года.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, I квартал 2023 года – IV квартал 2025 года



Наибольший месячный показатель в 2025 году был отмечен в апреле, минимум за год пришелся на сентябрь.

В четвертом квартале наибольшее значение доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, было в ноябре.



Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, январь 2024 года – декабрь 2025 года

Основные категории угроз из интернета*, которые были заблокированы на компьютерах АСУ в четвертом квартале 2025 года, – это вредоносные скрипты и фишинговые страницы, а также ресурсы в интернете из списка запрещенных.



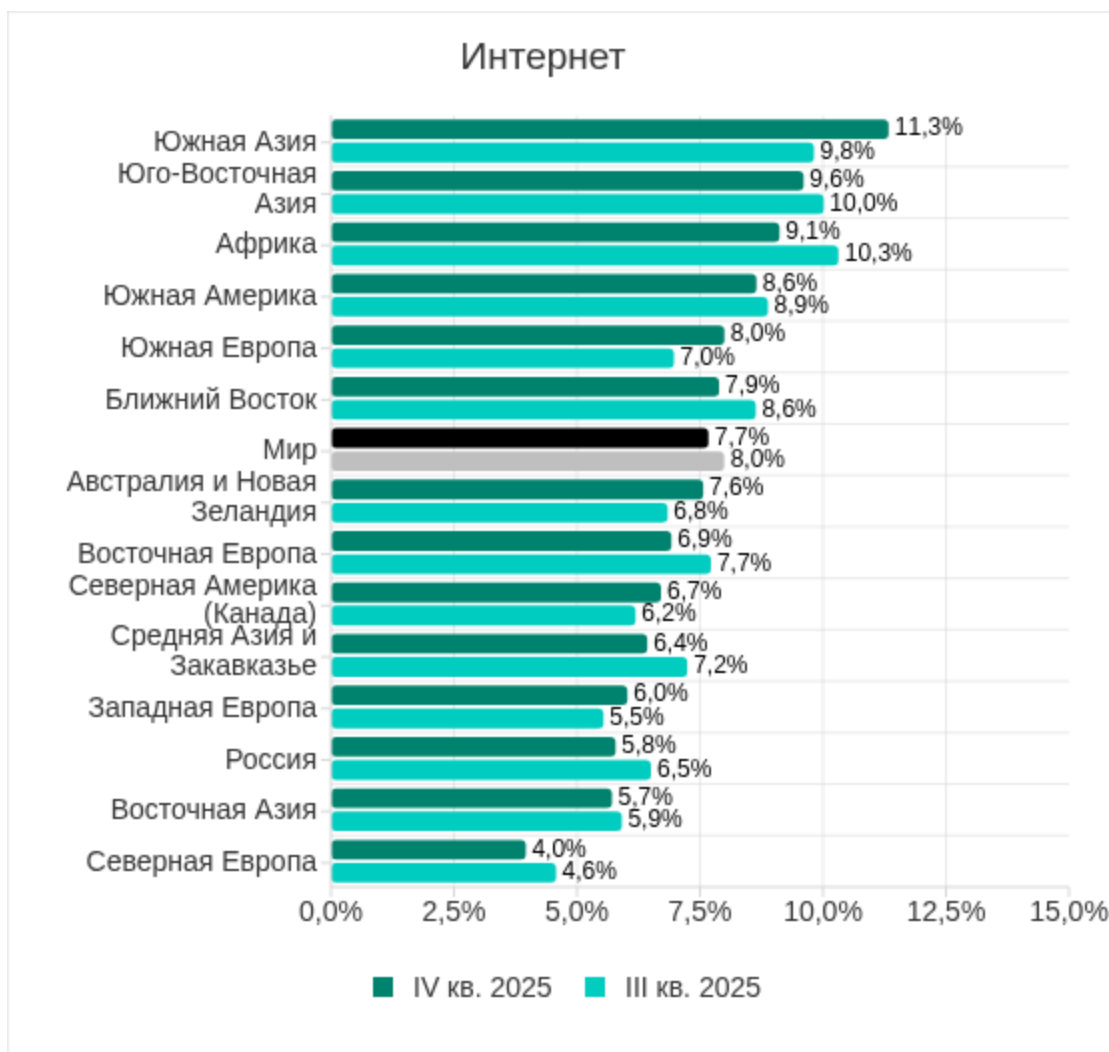
**Угрозы из интернета и основные категории угроз из интернета,
I квартал 2024 года – IV квартал 2025 года**

*Напомним, что один и тот же 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 угрозы будет учитываться лишь один раз (мы считаем уникальные атакованные компьютеры). К тому же, однозначно определить источник первоначальной попытки заражения не всегда представляется возможным. Поэтому суммарная доля компьютеров АСУ, на которых были заблокированы различные категории угроз из определенного источника, может превышать долю угроз из самого источника.

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, варьирует от 3,96% в Северной Европе до 11,33% в Южной Азии.

Топ 3 регионов по доле компьютеров АСУ, на которых в четвертом квартале 2025 года были заблокированы угрозы из интернета, остался прежним: Южная Азия, Юго-Восточная Азия и Африка. При этом два региона поменялись местами – Африка опустилась на третье место, Южная Азия поднялась с третьего на первое.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета



В четвертом квартале 2025 года показатель угроз из интернета увеличился в пяти регионах, больше всего – в Южной Азии.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, IV квартал 2025 года



Почтовые клиенты

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

В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы такие угрозы, уменьшилась до 2,76%. Это значение второе по величине за три года.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, I квартал 2023 года – IV квартал 2025 года

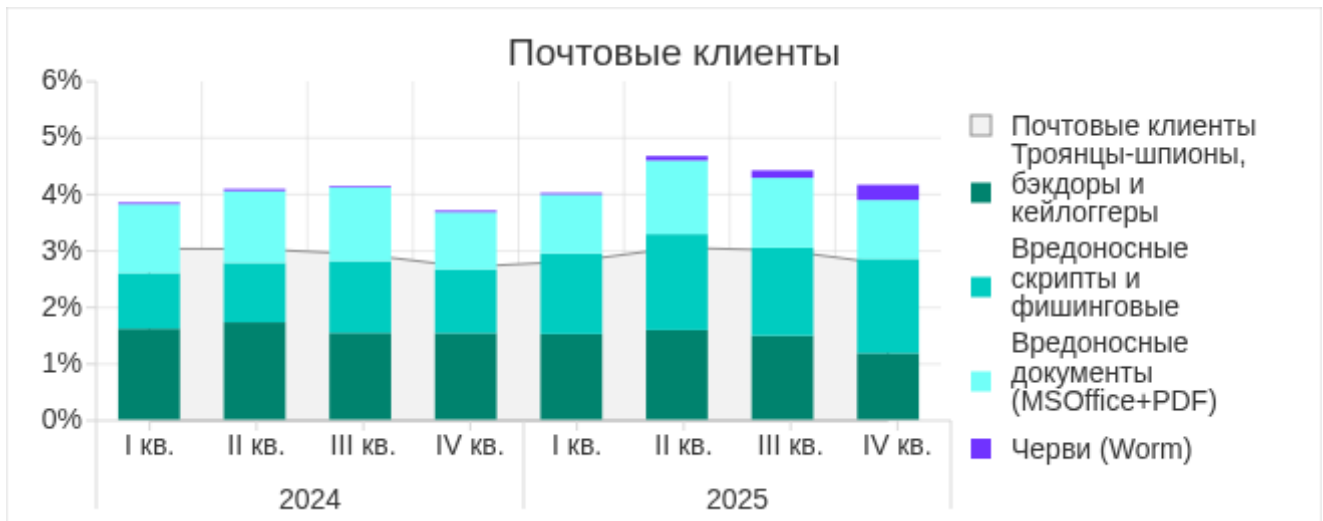


В 2025 году наибольший месячный показатель был отмечен в июне, с июля доля компьютеров АСУ, на которых в течение месяца были заблокированы угрозы в почтовых клиентах, снижалась.



Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, январь 2024 года – декабрь 2025 года

Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ в четвертом квартале 2025 года, – это вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы. На диаграмме также виден рост в четвертом квартале 2025 года доли компьютеров, на которых были заблокированы черви из почтовых клиентов.



Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов,
I квартал 2024 года – IV квартал 2025 года

Большинство шпионских программ, обнаруженных в фишинговых письмах, доставлялись в форме архива с паролем или многослойного скрипта, встроенного в файлы офисных документов.

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через электронную почту, варьирует от 0,64% в Северной Европе до 6,34% в Южной Европе.

Состав топ 3 регионов по уровню угроз из почтовых клиентов не изменился. В него вошли: Южная Европа, Южная Америка и Ближний Восток.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов



В четвертом квартале 2025 показатель угрозы из почтовых клиентов уменьшился почти во всех регионах.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, IV квартал 2025 года



Съемные носители

Доля компьютеров АСУ, на которых угрозы были обнаружены при подключении съемных носителей, продолжила снижаться и достигла минимального значения с начала 2023 года – 0,31%.

Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, I квартал 2023 года – IV квартал 2025 года

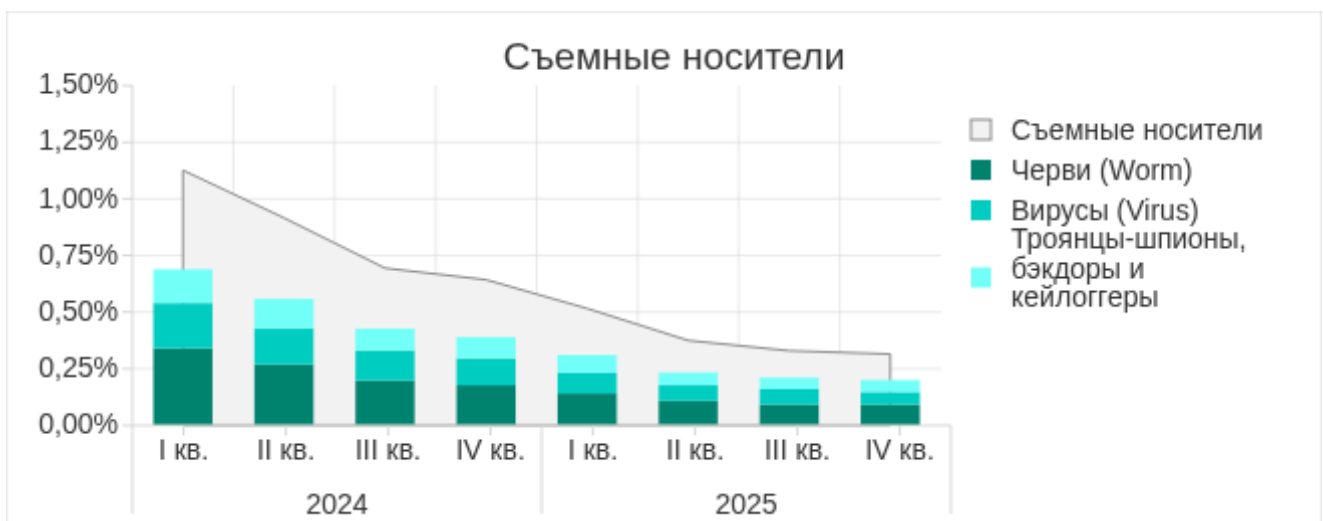


Месячный показатель с незначительными колебаниями также уменьшается от месяца к месяцу, минимальное значение отмечено в ноябре.



Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, январь 2024 года – декабрь 2025 года

Основные категории угроз, которые в четвертом квартале 2025 года были заблокированы при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионское ПО.



Угрозы на съемных носителях и основные категории угроз на съемных носителях, I квартал 2024 года – IV 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.

В регионах доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, варьирует от 0,05% в Австралии и Новой Зеландии до 1,41% в Африке.

Топ 3 регионов по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей: Африка, которая лидирует с большим отрывом от остальных регионов, Восточная Азия и Ближний Восток.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях



В четвертом квартале 2025 показатель угроз со съемных носителей увеличился в России, Северной Америке (Канада), Южной Европе и Северной Европе.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, IV квартал 2025 года



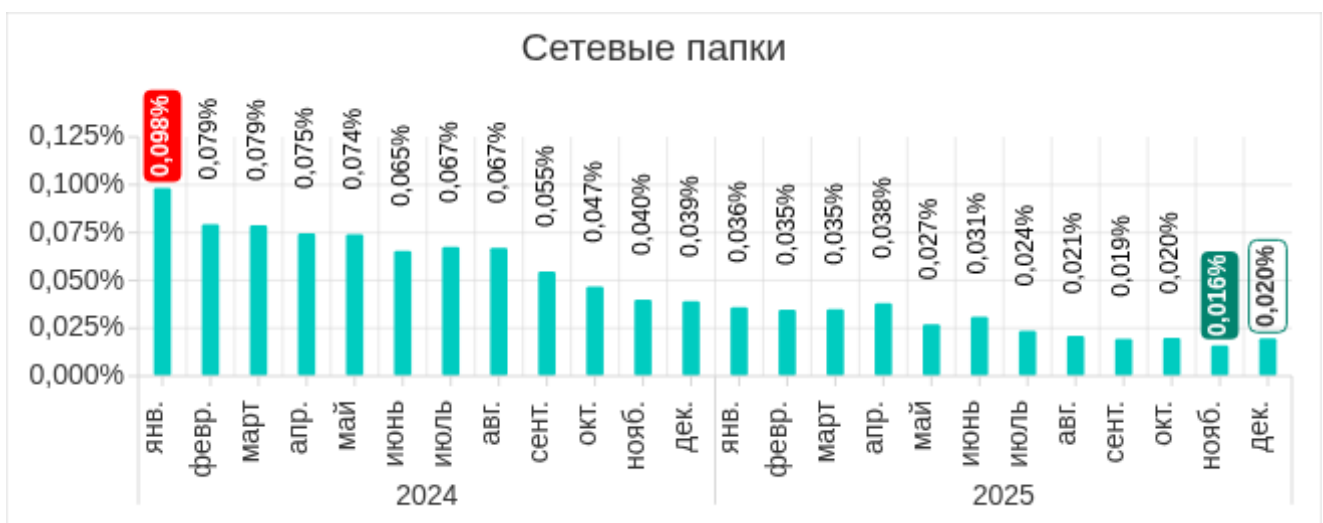
Сетевые папки

В четвертом квартале 2025 года показатель по сетевым папкам достиг минимального значения с начала 2023 года.

Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, I квартал 2023 года – IV квартал 2025 года

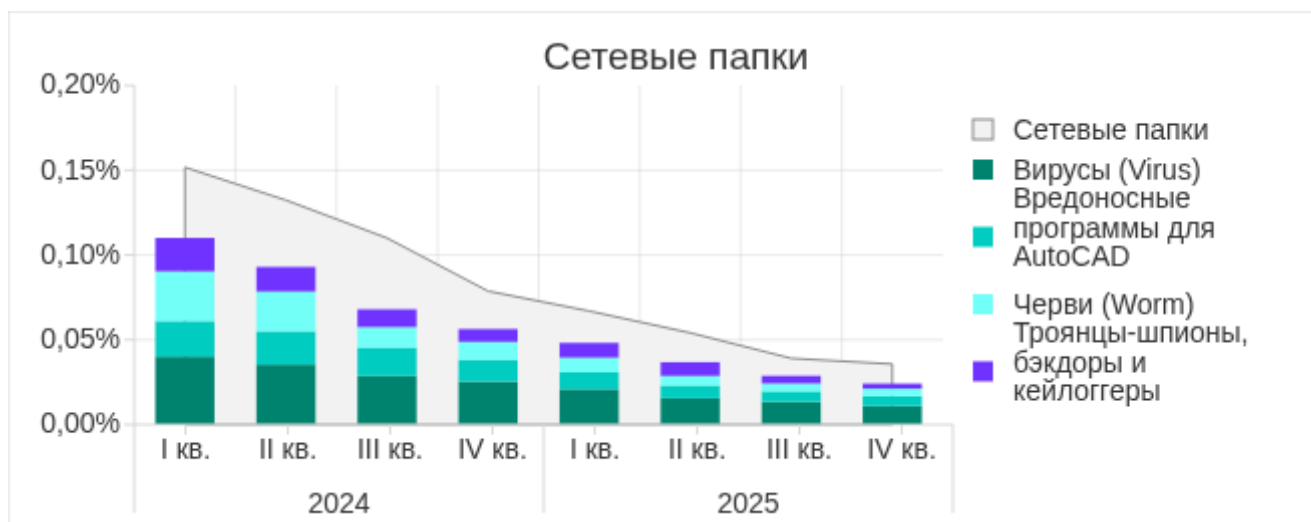


Месячные показатели демонстрируют явную тенденцию к снижению. В 2025 году наибольшее значение было отмечено в апреле, минимум пришелся на ноябрь.



Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, январь 2024 года – декабрь 2025 года

Основными категориями угроз, которые распространялись через сетевые папки в четвертом квартале 2025 года, были вирусы, вредоносное ПО для AutoCAD, черви и шпионское ПО.

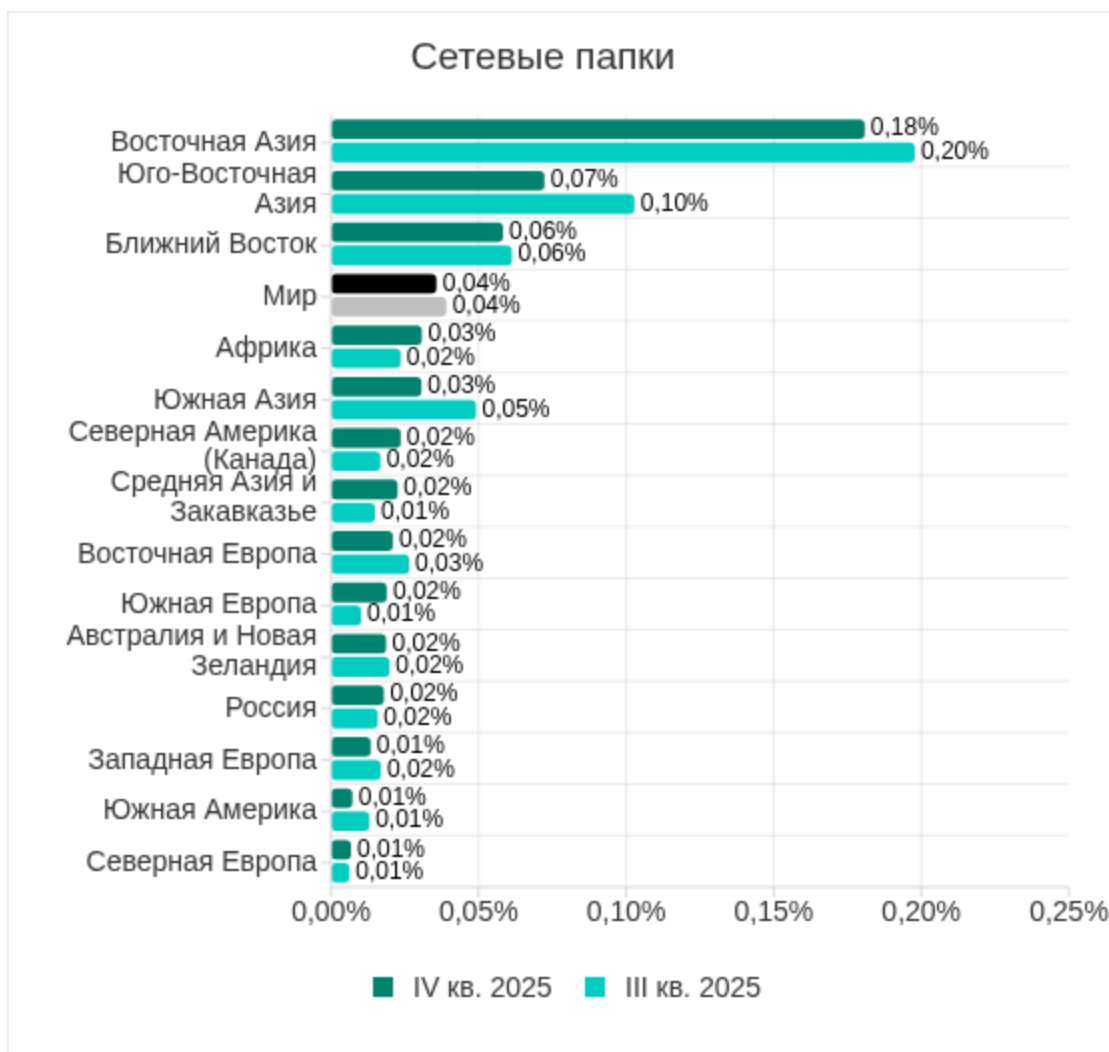


Угрозы в сетевых папках и основные категории угроз в сетевых папках,
I квартал 2024 года – IV квартал 2025 года

В регионах доля компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, варьирует от 0,01% в Северной Европе до 0,18% в Восточной Азии.

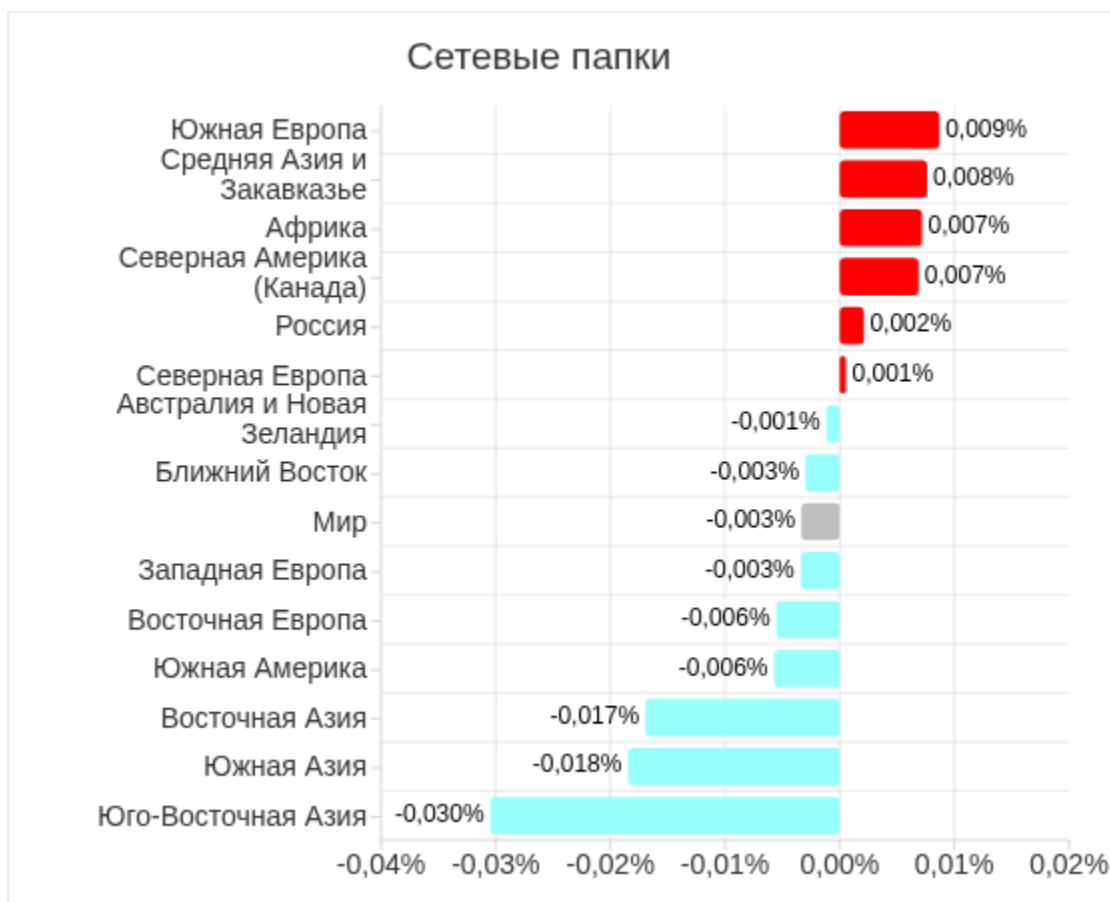
Топ 3 регионов по уровню угроз в сетевых папках: Восточная и Юго-Восточная Азия, Ближний Восток. Восточная Азия традиционно лидирует по этому показателю с большим отрывом от остальных регионов.

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках



В четвертом квартале 2025 показатель угроз в сетевых папках вырос в шести регионах, больше всего — в Южной Европе и в Средней Азии и Закавказье.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, IV 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 APT¹.

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 вонне 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», 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