Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Третий квартал 2025 года

11.12.2025

Версия 1.0

Цифры

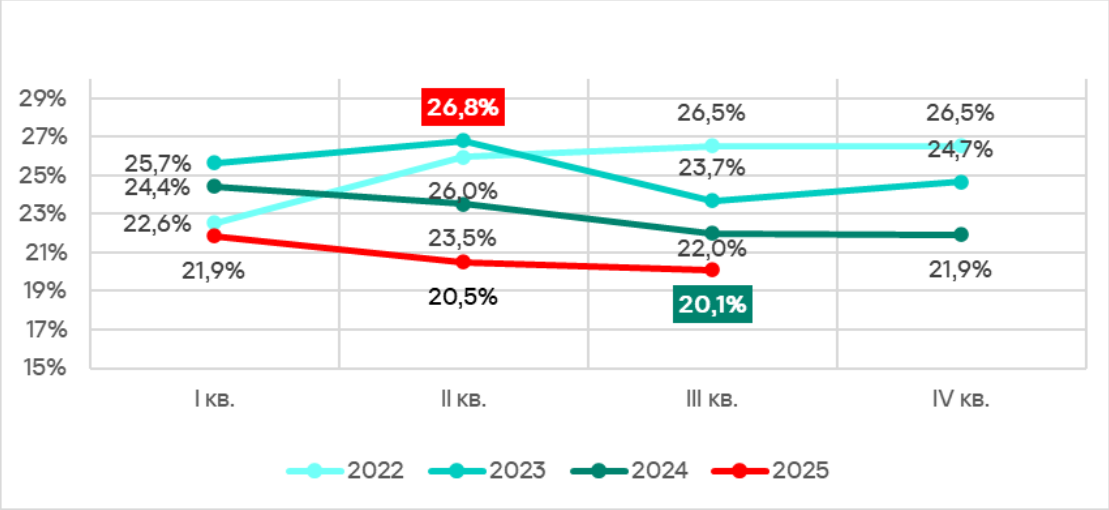
Показатель	II кв. 2025	III кв. 2025	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	20,5%	20,1%	▼0,4 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	6,49%	6,79%	▲0,30 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,84%	4,04%	▲0,20 п. п.
Ресурсы в интернете из списка запрещенных	5,91%	4,01%	▼1,90 п. п.
Вредоносные документы (MSOffice+PDF)	1,97%	1,98%	▲0,01 п. п.
Вирусы (Virus)	1,29%	1,40%	▲0,11 п. п.
Черви (Worm)	1,22%	1,26%	▲0,04 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,63%	0,57%	▼0,06 п. п.
Вредоносные программы для AutoCAD	0,29%	0,30%	▲0,01 п. п.
Веб-майнеры, выполняемые в браузерах	0,30%	0,25%	▼0,05 п. п.
Программы-вымогатели	0,14%	0,17%	▲0,03 п. п.
Основные источники угроз			
Интернет	9,76%	7,99%	▼1,77 п. п.
Почтовые клиенты	3,06%	3,01%	▼0,05 п. п.
Съемные носители	0,37%	0,33%	▼0,04 п. п.
Сетевые папки	0,05%	0,04%	▼0,01 п. п.

Итоги квартала

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты

В третьем квартале 2025 года в мире доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, продолжила уменьшаться и оказалась минимальной с 2022 года — 20,1%.

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

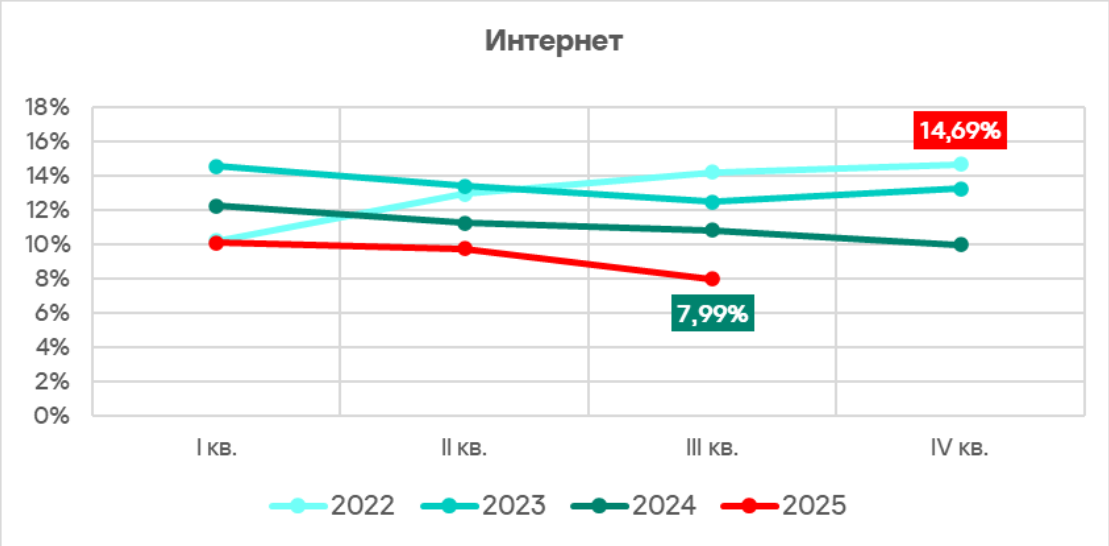


В регионах показатель варьировал от 9,2% в Северной Европе до 27,4% в Африке. Значения выросли в пяти регионах, лидирует по росту Восточная Азия.

Основные источники и категории угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций по-прежнему остаются интернет, почтовые клиенты и съемные носители. В третьем квартале 2025 года показатели всех источников угроз в среднем по миру уменьшились. Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, была минимальной с 2022 года.

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

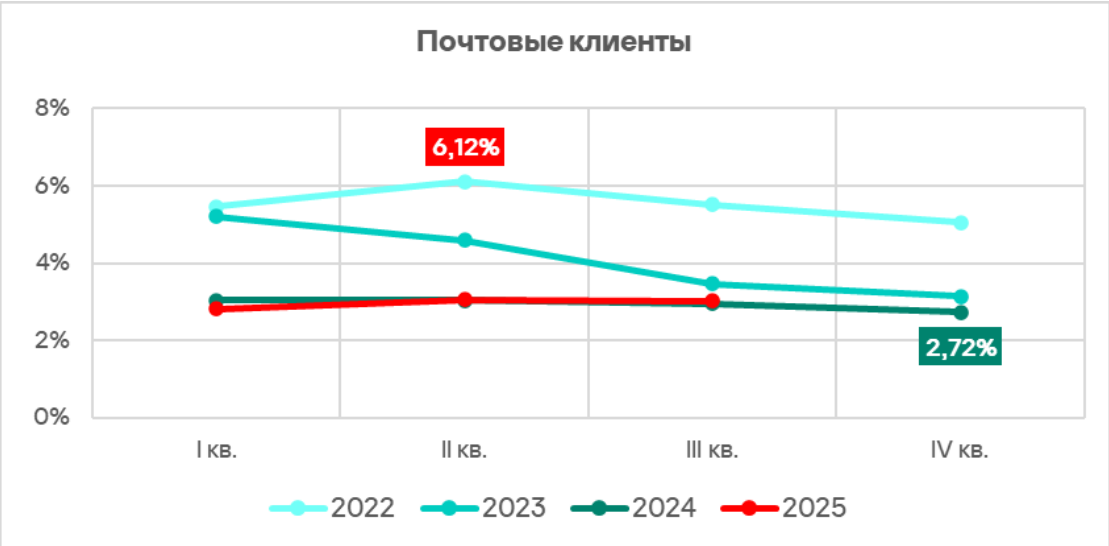


Основные категории угроз из интернета, которые были заблокированы на компьютерах АСУ в третьем квартале 2025 года: вредоносные скрипты и фишинговые страницы, а также ресурсы в интернете из списка запрещенных.

В третьем квартале 2025 года после роста в предыдущем квартале доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, заметно уменьшилась (на 1,9 п. п.) до минимального с 2022 года значения 4,01%.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, с начала 2024 года относительно стабильна.

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



Несмотря на уменьшение среднемирового показателя угроз из интернета, он более чем в 2,6 раза превышает показатель угроз из почтовых клиентов. Однако в некоторых регионах эта разница не столь значительна, например в Южной Европе значения сопоставимы — 6,97% и 6,85% соответственно.

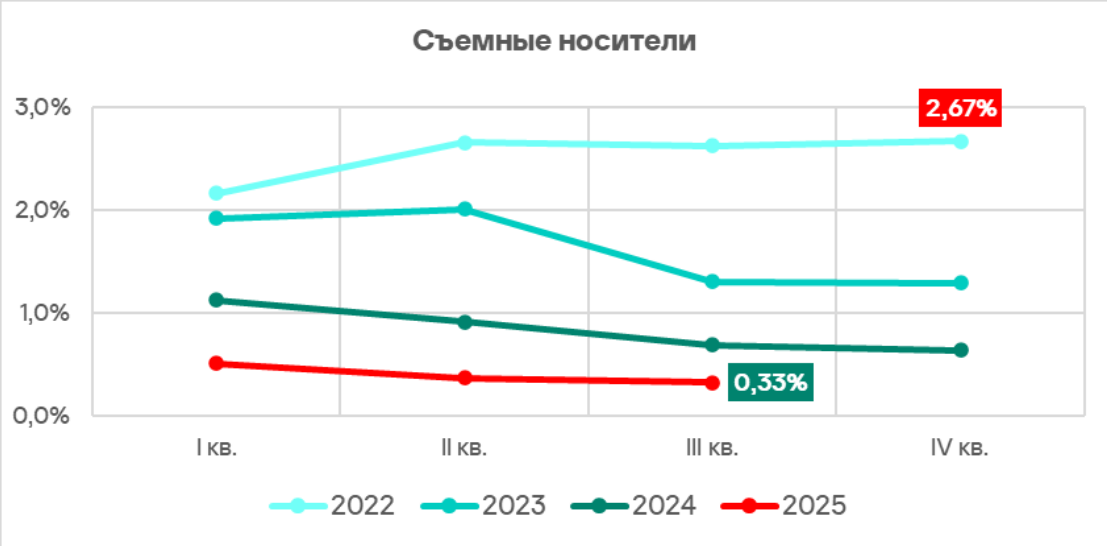
Этот регион лидирует по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов.

Основные категории угроз из почтовых клиентов: вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы.

Вредоносные скрипты и фишинговые страницы преимущественно распространяются через интернет и фишинговые письма, но также встречается и на следующих этапах атаки — для закрепления в системе, сбора данных и взаимодействия с серверами управления. Эта категория угроз в третьем квартале 2025 года лидирует по росту показателя (+0,3 п. п.). Шпионские программы на втором месте в этом рейтинге (+0,2 п. п.).

Доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, в третьем квартале 2025 года была минимальной с начала 2022 года — 0,33%.

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



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

Доли компьютеров АСУ, на которых в третьем квартале 2025 года были заблокированы вирусы и черви, за квартал немного увеличились.

Особенности детектирования некоторых категорий угроз

Две основные категории угроз в интернете — веб-ресурсы из списка запрещенных и вредоносные скрипты и фишинговые страницы — взаимосвязаны.

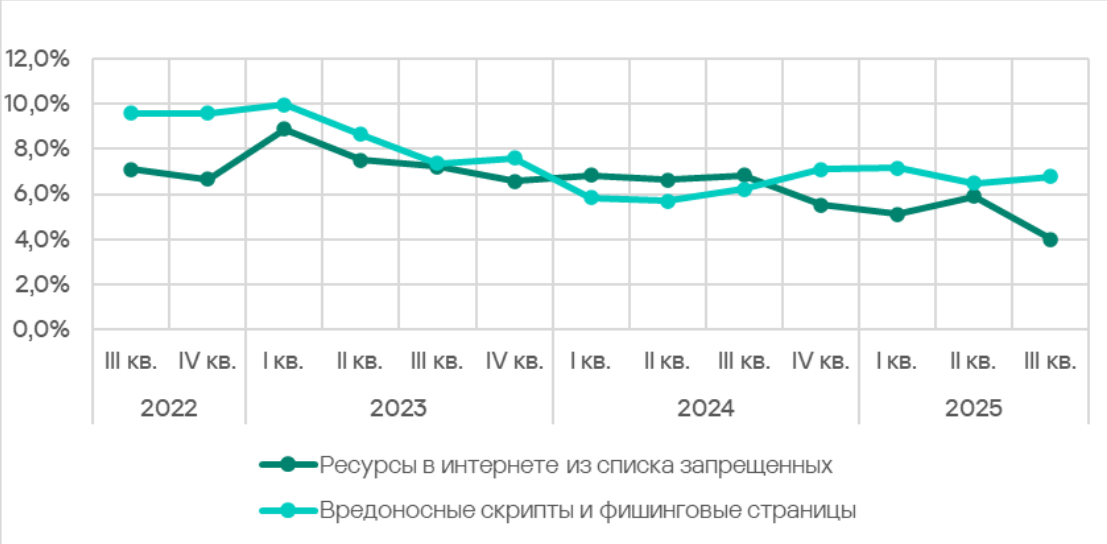
Значительная часть ресурсов в интернете, которые попадают в список запрещенных, используется злоумышленниками для распространения вредоносных скриптов и фишинговых страниц (HTML).

Адреса, добавляемые в списки запрещенных, оперативно распространяются через KSN — это препятствует загрузке вредоносного кода и, как следствие, он не блокируется как вредоносный скрипт или майнер. В результате соответствующие показатели снижаются.

Злоумышленники постоянно продолжают искать и использовать для распространения вредоносного кода новые интернет-ресурсы и альтернативные техники, что в дальнейшем однозначно приводит к росту детектирования скриптов и снижению детектирования по спискам запрещенных интернет-ресурсов.

Эти взаимозависимости отражаются в нашей статистике — видно, как эти показатели в масштабе кварталов колеблются в противофазе.

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

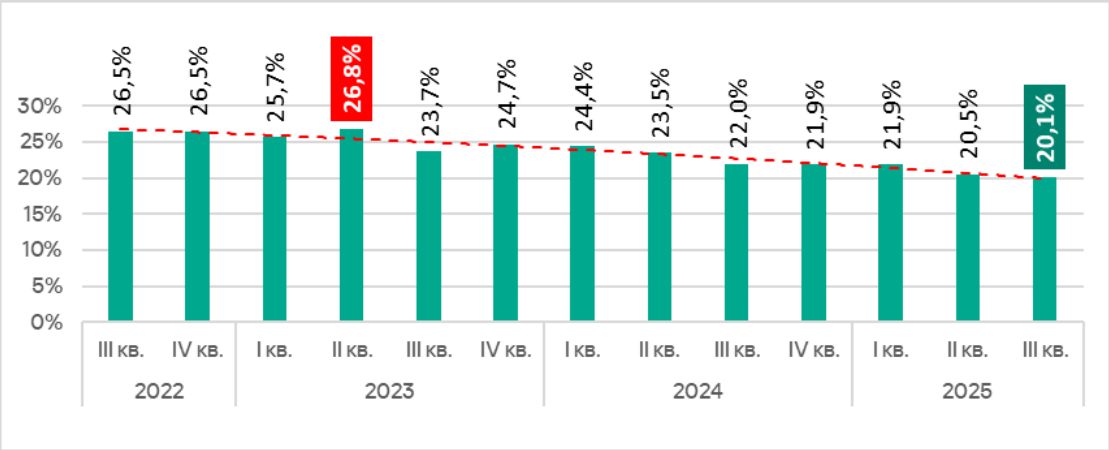


В третьем квартале 2025 года категория вредоносных скриптов и фишинговых страниц лидирует среди остальных категорий угроз и по доле компьютеров АСУ, на которых была заблокирована угроза, и по росту показателя.

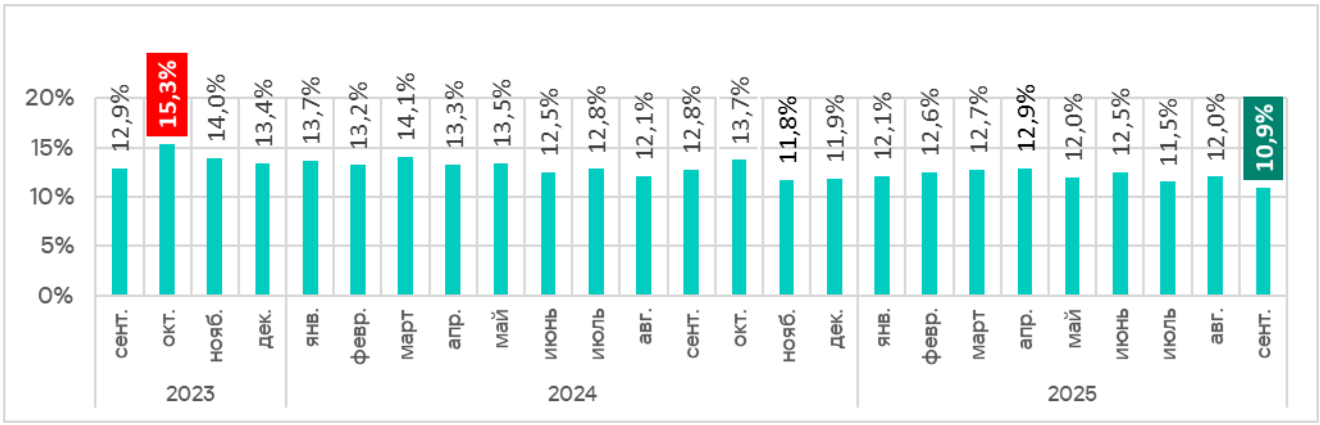
Статистика по всем угрозам

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, по сравнению с предыдущим кварталом уменьшилась на 0,4 п. п. и составила 20,1%. Это минимальный показатель за исследуемый период.

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



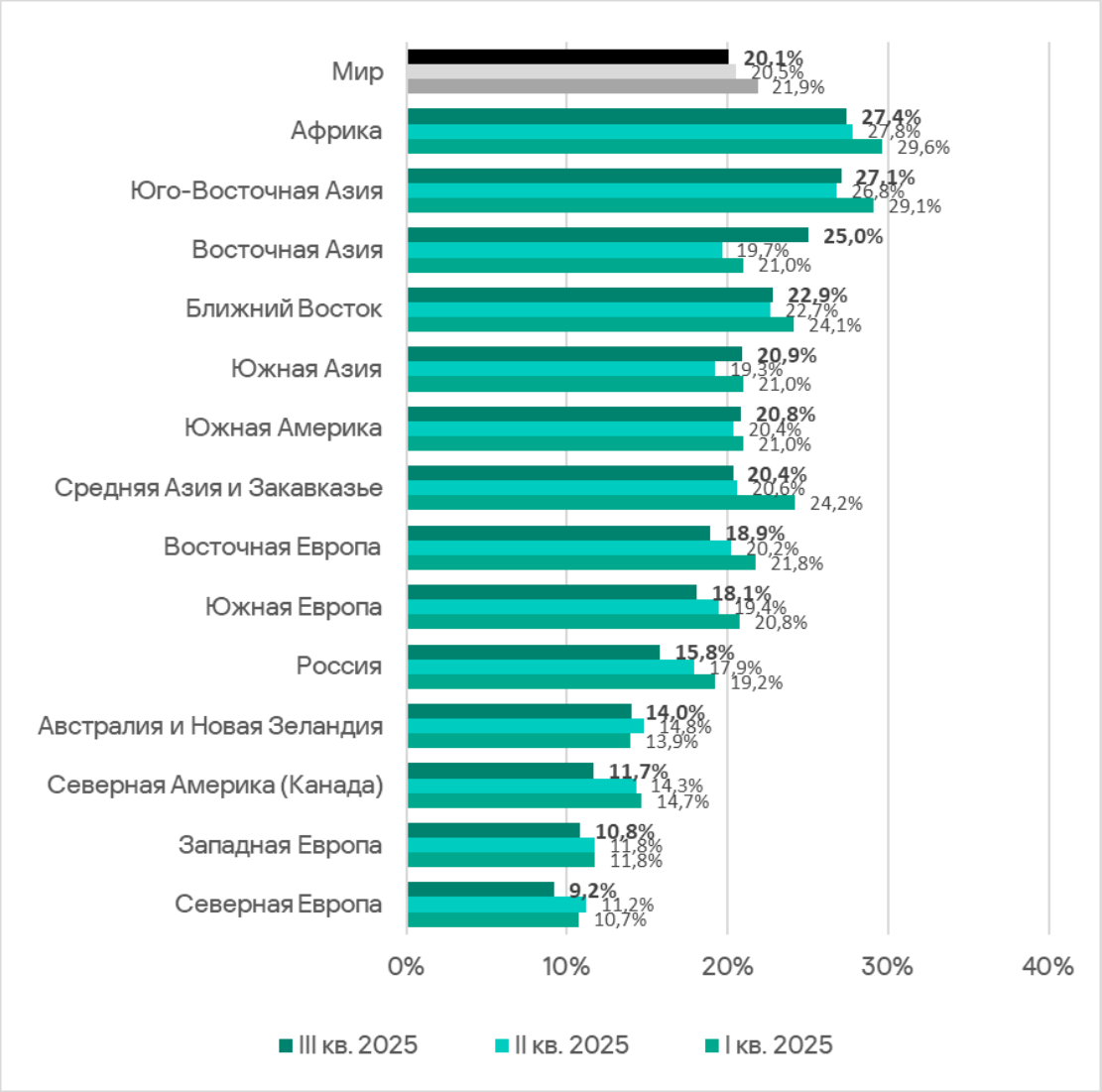
В течение третьего квартала 2025 года самой высокой доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, была в августе. В сентябре месячный показатель был наименьшим за два года.



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

В регионах доля компьютеров АСУ, на которых в третьем квартале 2025 года были заблокированы вредоносные объекты, варьирует от 9,2% в Северной Европе до 27,4% в Африке.

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



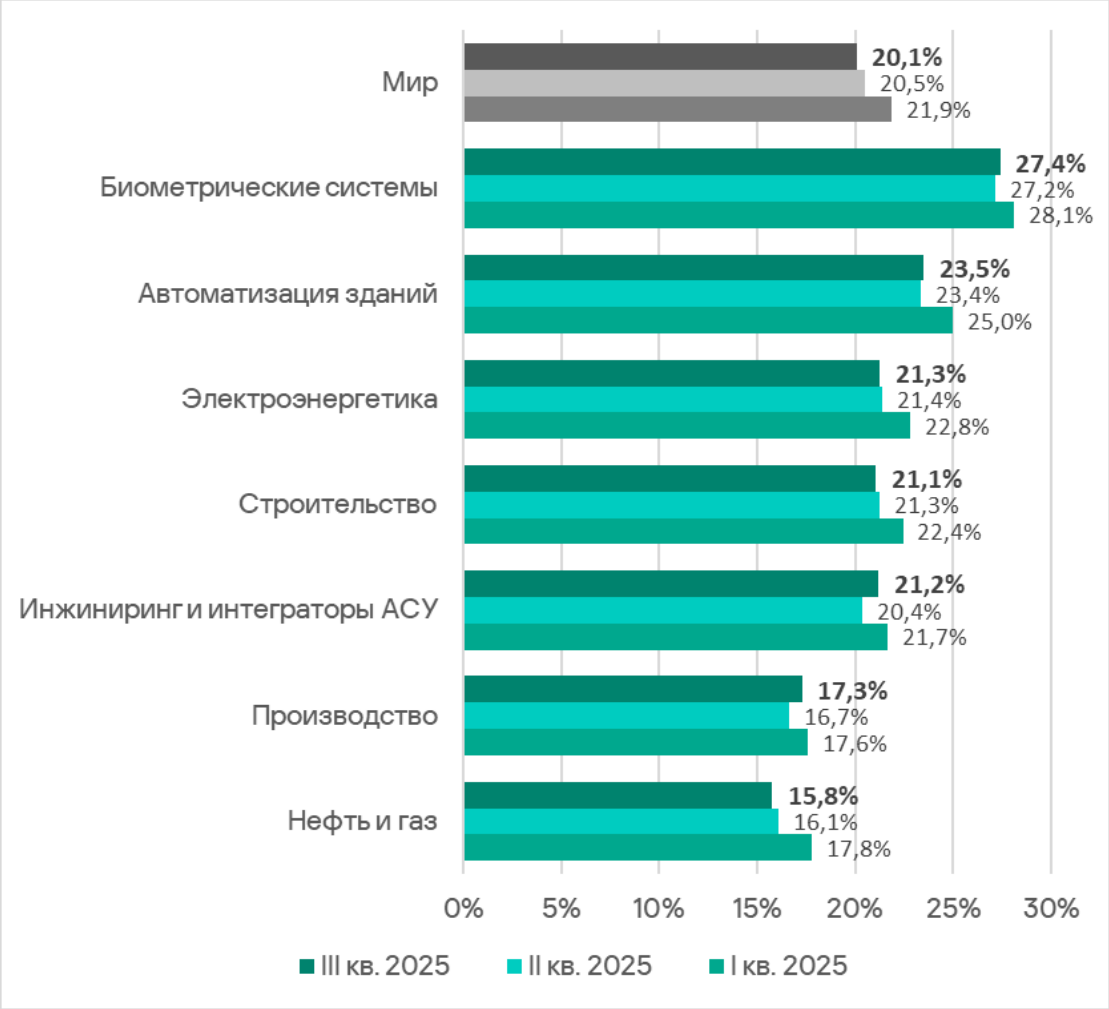
Показатель за квартал увеличился в пяти регионах, больше всего — в Восточной Азии, где был отмечен резкий рост доли компьютеров АСУ, связанный с локальным распространением вредоносных скриптов в OT-инфраструктуре организаций в сфере инжиниринга и интеграции АСУ.

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

Исследуемые отрасли

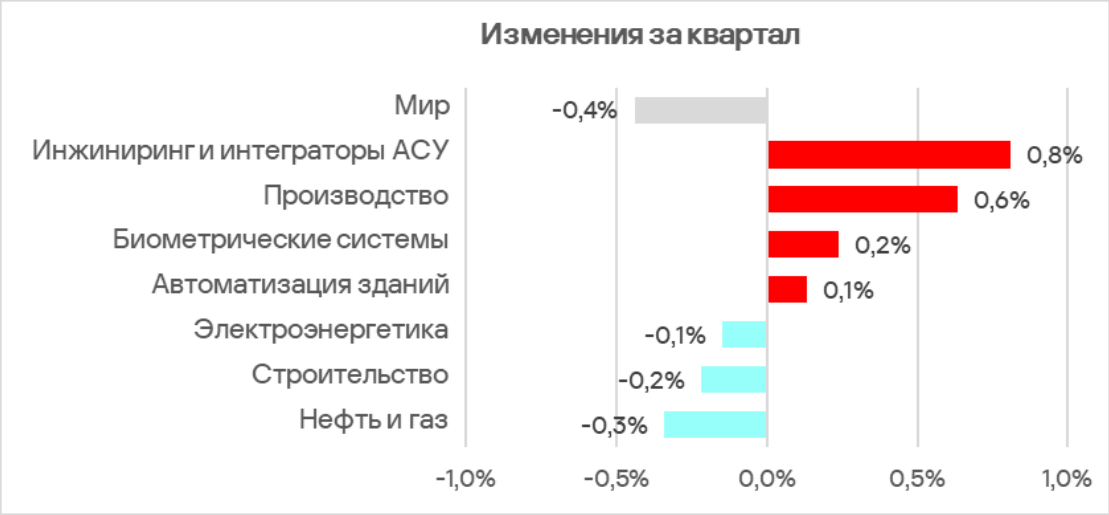
В третьем квартале 2025 года рейтинг исследуемых отраслей и типов OT-инфраструктур по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, традиционно возглавили биометрические системы.

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

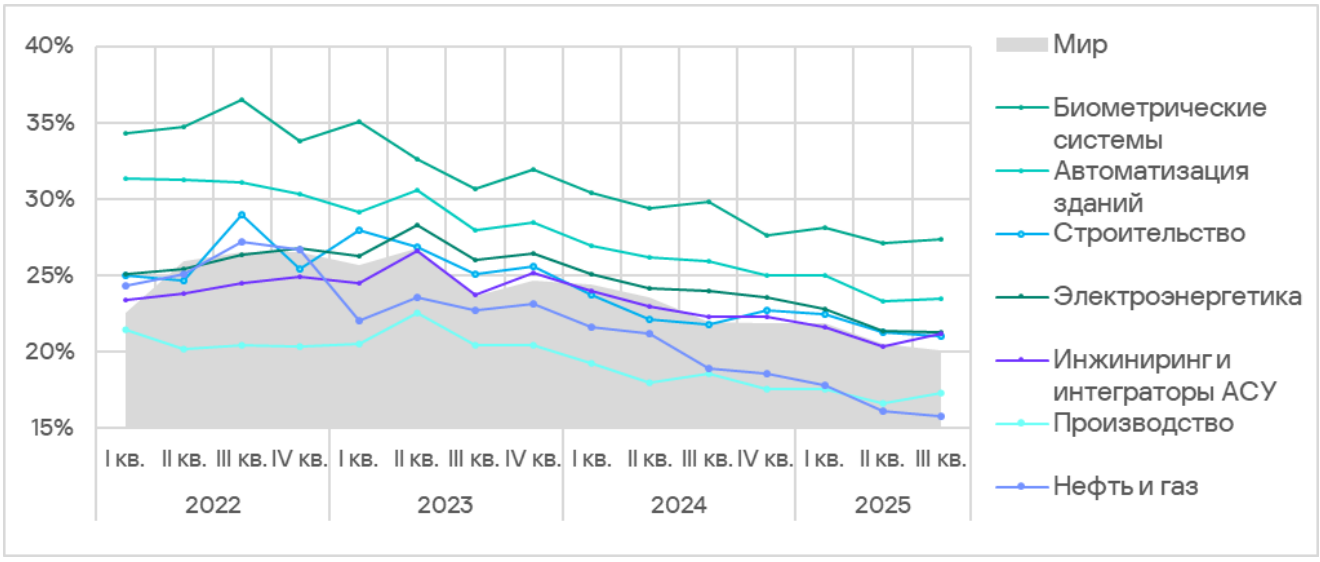


В четырех из семи исследуемых отраслей доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в третьем квартале 2025 года увеличилась. Больше всего показатель увеличился в отраслях инжиниринг и интеграторы АСУ, а также производство.

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



Во всех исследуемых отраслях наблюдается тенденция к уменьшению показателя, относительно пиковых значений в третьем квартале 2022 года.



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.

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.

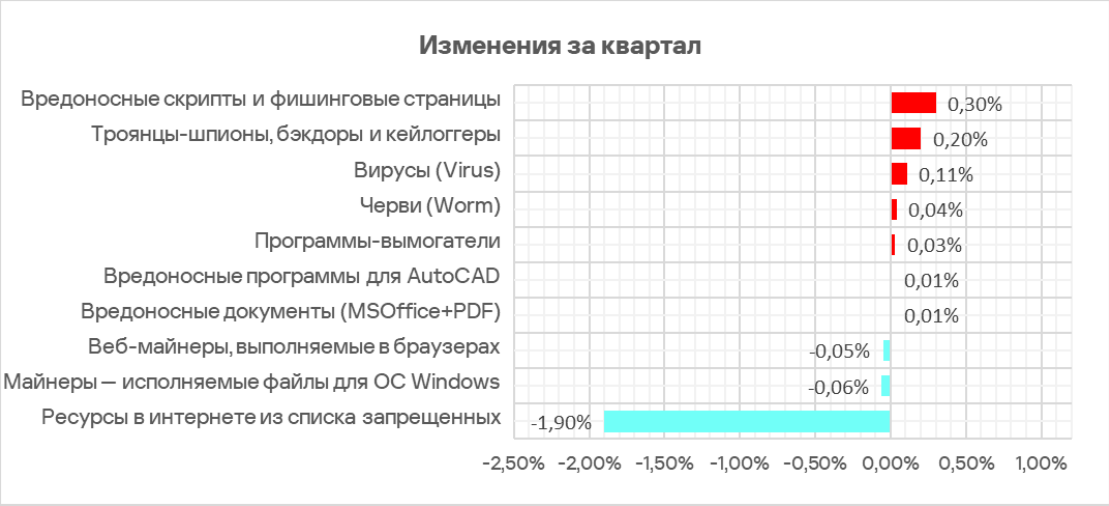
Следует заметить, что в небольшом проценте случаев категории угроз, которые мы относим к объектам первичного заражения, скажем, вредоносные ссылки, также используются на последующих этапах атаки. Так, например, иногда ссылка на вредоносный ресурс может быть обнаружена при сканировании реестра компьютера, где она появились, 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 третьем квартале 2025 года в рейтинге категорий вредоносного ПО по доле атакованных компьютеров лидирует категория вредоносных скриптов и фишинговых страниц. Программы-шпионы впервые оказались на втором месте в этом рейтинге.

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

Из всех исследуемых категорий в третьем квартале 2025 года уменьшилась доля компьютеров АСУ, на которых были заблокированы: ресурсы в интернете из списка запрещенных и майнеры обеих категорий.

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



Показатель ресурсов в интернете из списка запрещенных после роста в предыдущем квартале уменьшился на 1,9 п. п. Эта категория опустилась в рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, со второго на третье место.

Категории вредоносных объектов

В третьем квартале 2025 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 11 356 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).

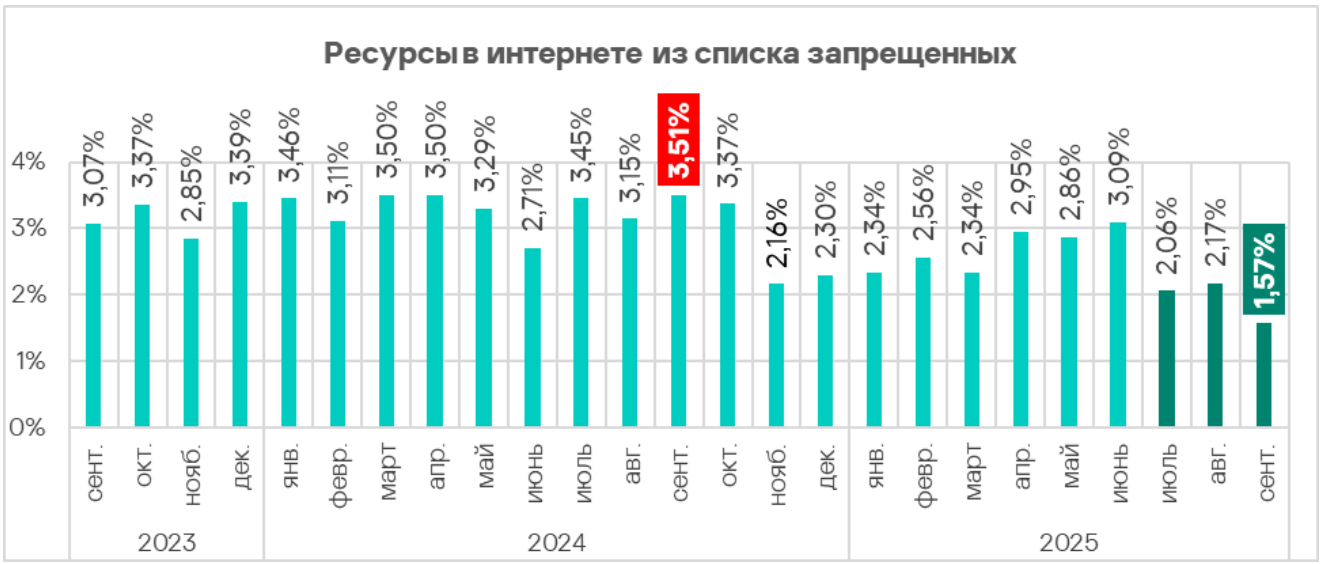
Обнаруженный опасный интернет-ресурс не всегда может быть легко добавлен в список запрещенных, поскольку злоумышленники все чаще используют легитимные интернет-ресурсы и сервисы, например платформы доставки контента (CDN), мессенджеры, репозитории и облачные хранилища. Подобные сервисы позволяют распространять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

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, уменьшилась до 4,01%. Это наименьший квартальный показатель с начала 2022 года. В рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, эта категория опустилась со второго на третье место.

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

Из трех месяцев третьего квартала 2025 года наибольшее значение доли компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, отмечено в августе. В сентябре месячный показатель был наименьшим за последние три года.



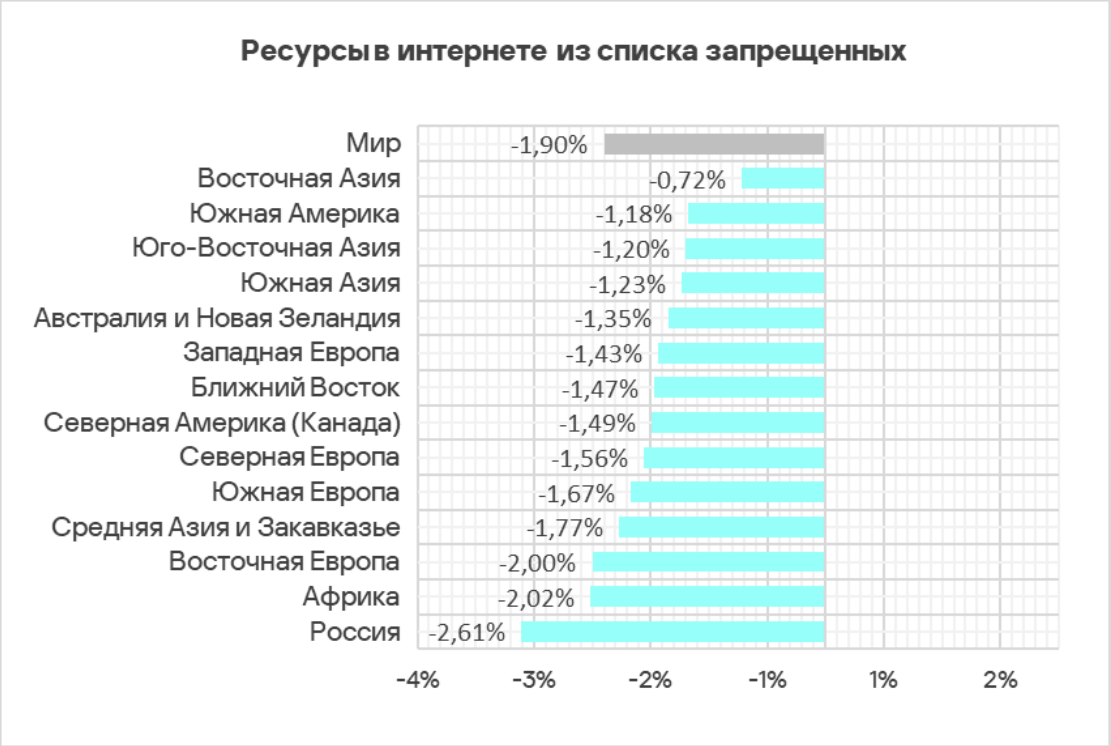
Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, сентябрь 2023 года — сентябрь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, варьирует от 2,35% в Австралии и Новой Зеландии до 4,96% в Африке. Кроме Африки в тройке лидеров по этому показателю Юго-Восточная и Южная Азия.

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

В третьем квартале 2025 года после роста в предыдущем квартале показатель уменьшился во всех регионах.

Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, III 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.

После снижения в конце 2024 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, растет третий квартал подряд.

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

Набольшее значение месячного показателя третьего квартала 2025 года отмечено в июле.

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

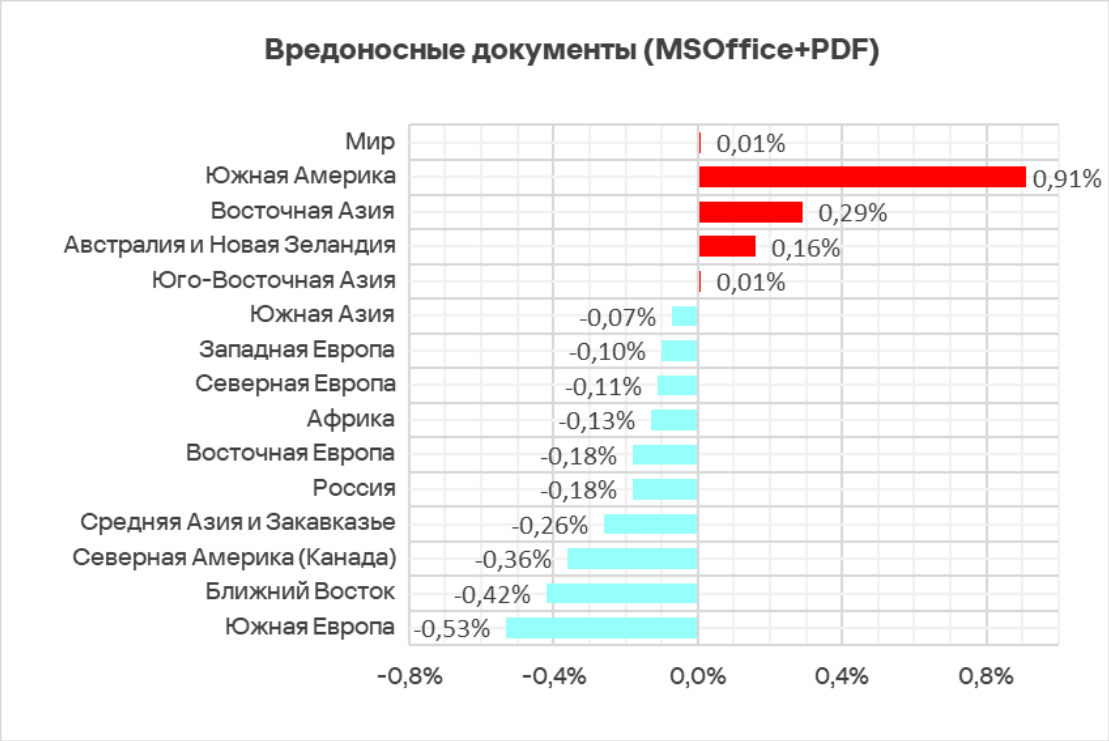
В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные документы, варьирует от 0,53% в Северной Европе до 4,17% в Южной Америке. Состав тройки лидеров не изменился: Южная Америка, Южная Европа и Ближний Восток.

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

В третьем квартале 2025 года показатель вырос в четырех регионах — в Южной Америке, Восточной Азии, Юго-Восточной Азии и в Австралии и Новой Зеландии. Наибольший рост отмечен в Южной Америке — в связи с масштабной фишинговой кампанией, в ходе которой злоумышленники использовали новые эксплойты для старой уязвимости CVE-2017-11882 в Microsoft Office Equation Editor для доставки на компьютеры жертв различного шпионского ПО.

Примечательно, что в этой волне фишинга злоумышленники использовали локализованные тексты писем на испанском языке, содержание которых похоже на деловую переписку.

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

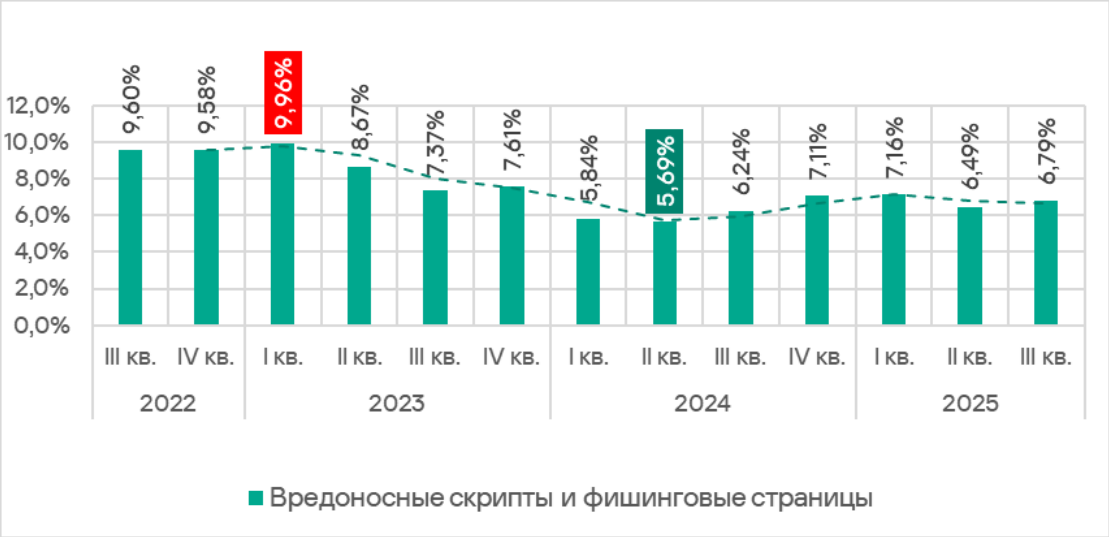


Вредоносные скрипты и фишинговые страницы (JS и HTML)

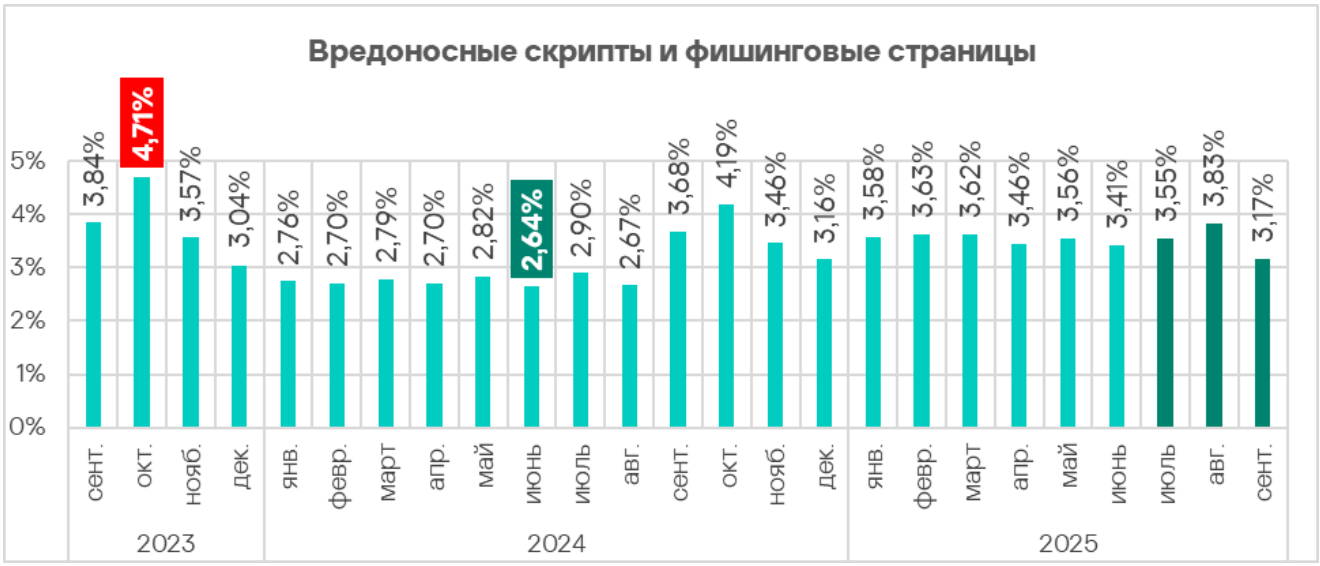
Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для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

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, выросла до 6,79%. 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, III квартал 2022 года — III квартал 2025 года



Из месячных показателей третьего квартала 2025 года наибольший был в августе.



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

В регионах показатель варьирует от 2,57% в Северной Европе до 9,41% в Африке. В топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вошли Африка, Восточная Азия и Южная Америка.

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

В регионах показатель больше всего увеличился в Восточной Азии (на драматичные 5,23 п. п.) в результате локального распространения вредоносных скриптов-шпионов, загружающихся в память популярных Torrent и MediaGet клиентов.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, III 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

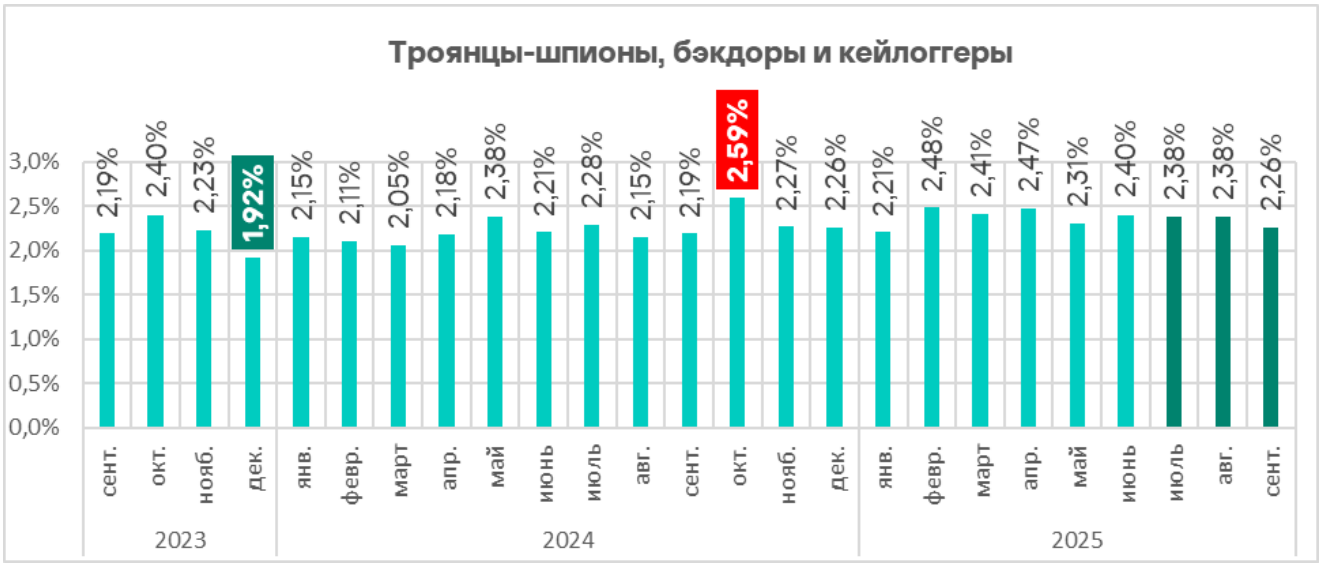
вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

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 третьем квартале 2025 года доля компьютеров АСУ, на которых было заблокировано шпионское ПО, увеличилась до 4,04%. Это не самый высокий показатель за исследуемый период, однако с ним шпионские программы впервые заняли второе место в рейтинге категорий по доле атакованных компьютеров.

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

В июле и августе значение месячного показателя не менялось, в сентябре оно уменьшилось.



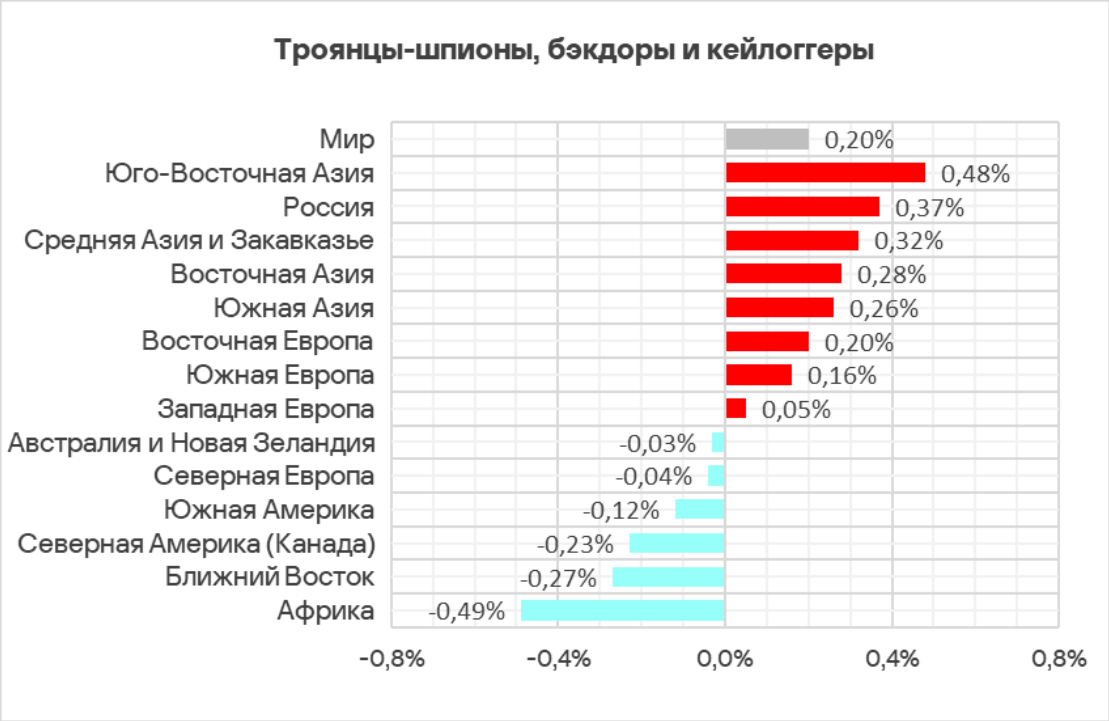
Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, сентябрь 2023 года — сентябрь 2025 года

В регионах доля компьютеров АСУ, на которых было заблокировано шпионское ПО, варьирует от 1,40% в Северной Европе до 6,33% в Африке. В топ 3 регионов по этому показателю, как и в прошлом квартале, вошли Африка, Юго-Восточная Азия и Южная Европа.

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

За квартал доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла в восьми регионах, больше всего — в Юго-Восточной Азии, в России и в Средней Азии и Закавказье.

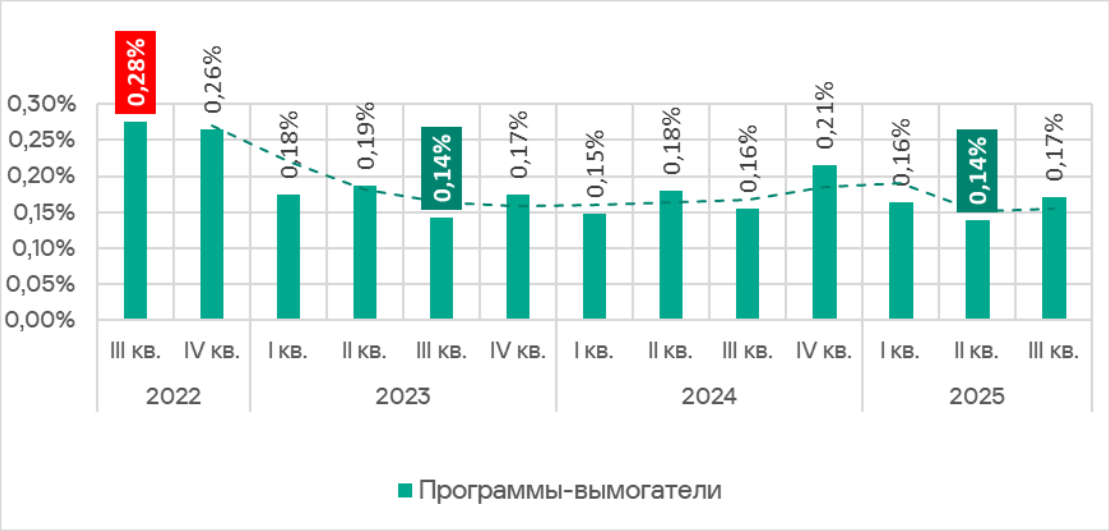
Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, III квартал 2025 года



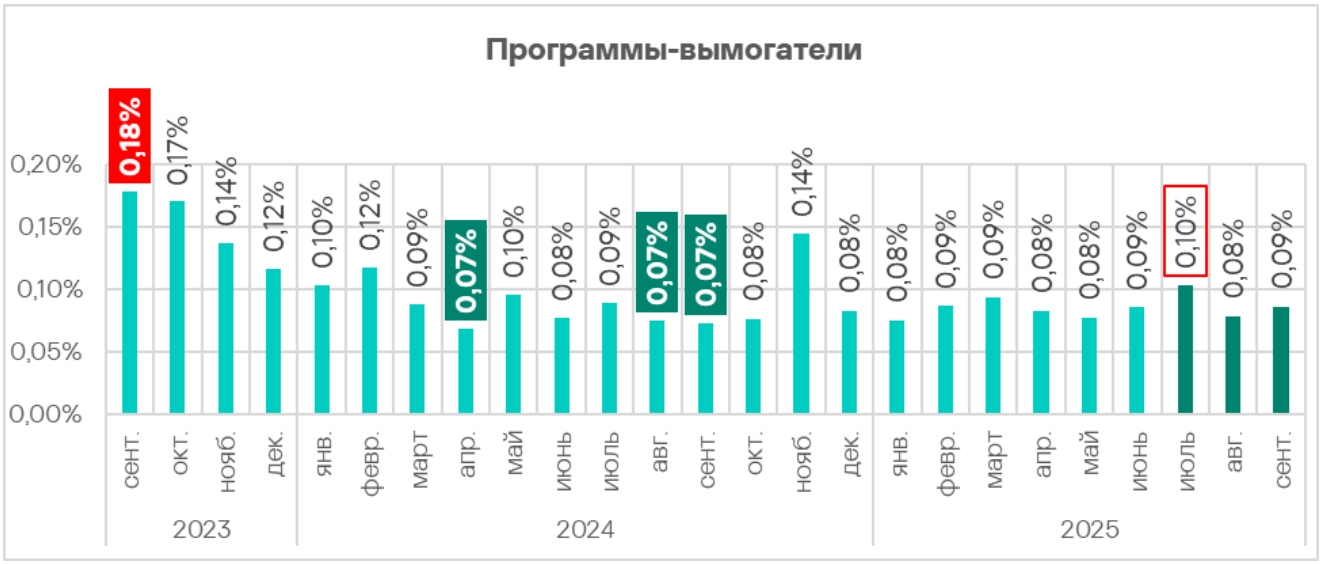
Программы-вымогатели

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, подросла до 0,17%, это чуть выше значения первого квартала года.

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



В июле значение месячного показателя было наибольшим с декабря 2024 года. Месячные показатели августа и сентября сопоставимы с предыдущими месяцами 2025 года.



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

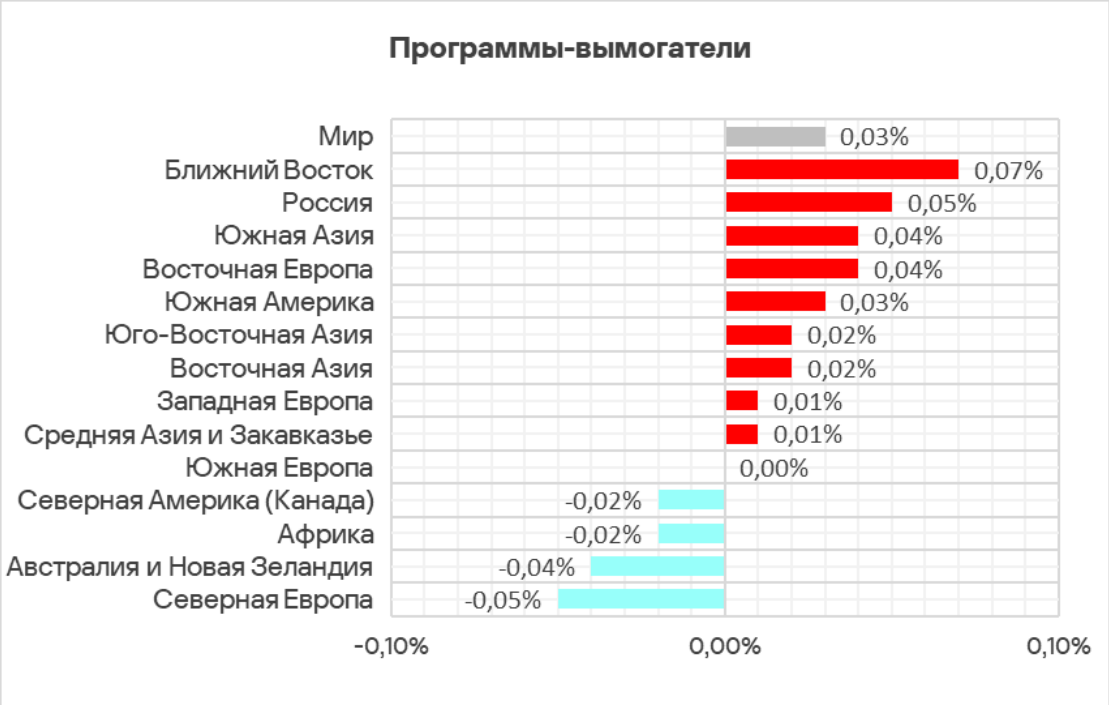
В регионах доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, варьирует от 0,05% в Северной Европе до 0,33% на Ближнем Востоке, который вернулся на позицию лидера в этом рейтинге. В топ 3 регионов также входят Африка и Южная Азия.

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

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, выросла в девяти регионах. Ближний Восток лидирует среди регионов и по росту этого показателя.

В этом регионе особенно заметен рост доли компьютеров АСУ, на которых блокируются программы-вымогатели, в нефтегазовой отрасли, а также в автоматизации зданий, инжиниринге и интеграции АСУ. Вредоносное ПО распространялось под видом клиентского ПО для удаленного доступа, пиратских игр и взломанных лицензионных приложений, в том числе — используемых в биометрических системах, автоматизации зданий и инженерии.

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



Майнеры — исполняемые файлы для ОС Windows

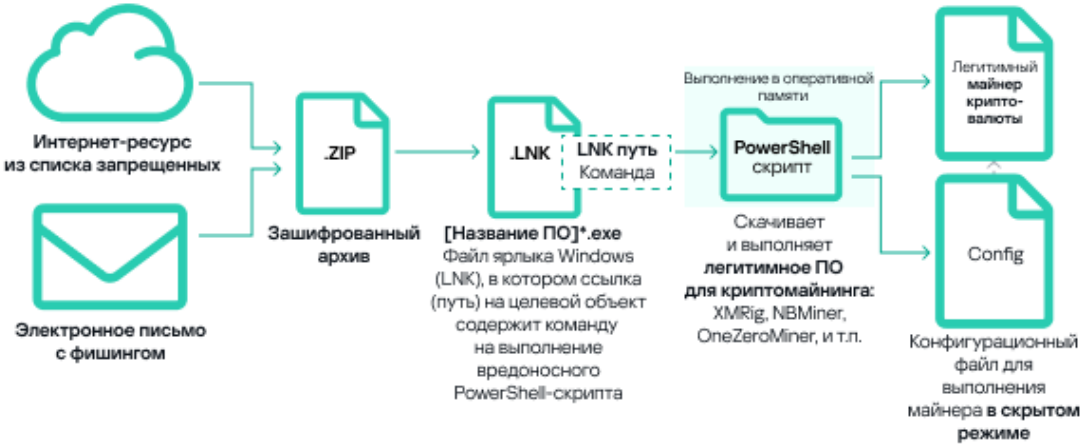
Наряду с «классическими» майнерами — приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют, — появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры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

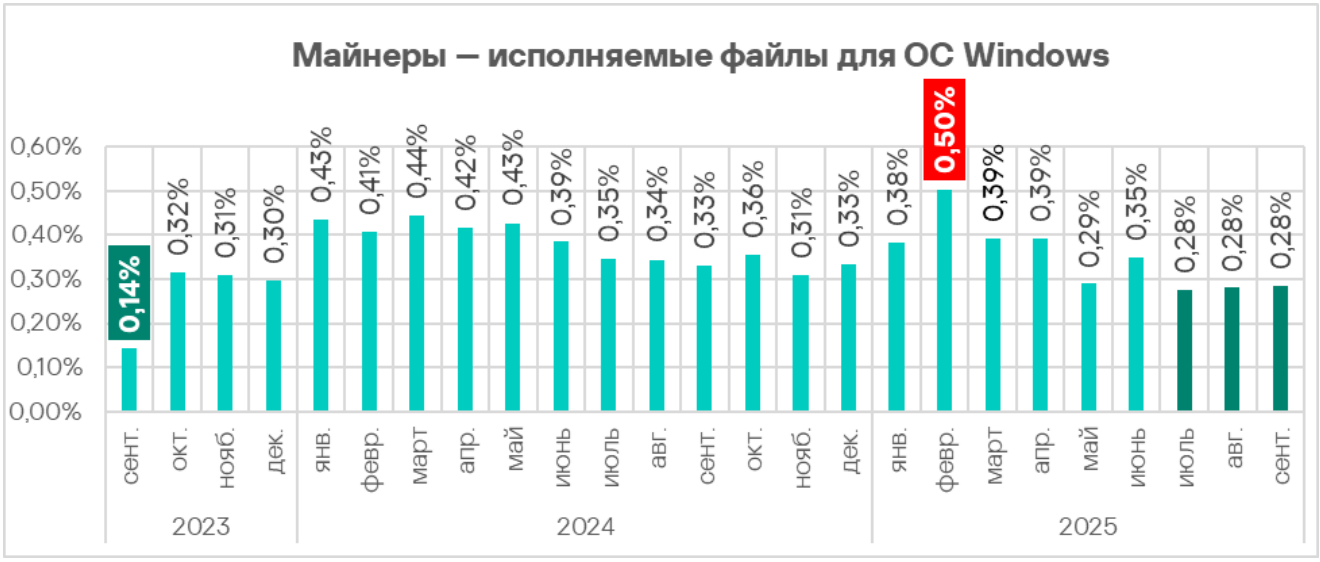
Цепочка атаки: пример с использованием легитимных криптомайнеров



В третьем квартале 2025 года доля компьютеров АСУ, на которых были выявлены майнеры в формате исполняемых файлов для Windows, уменьшилась до 0,57%. Это наименьший квартальный показатель за последние три года.

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

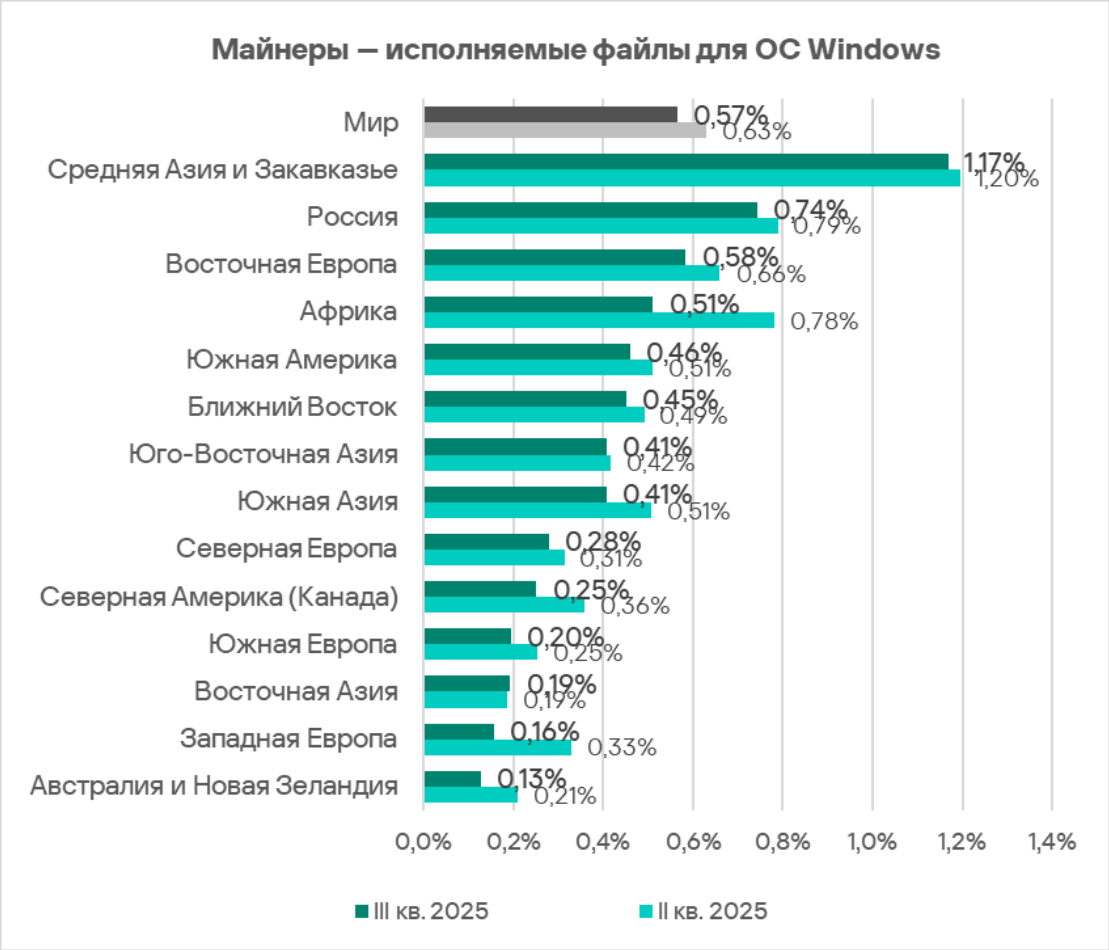
Месячные показатели квартала оставались неизменными — 0,28%.



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

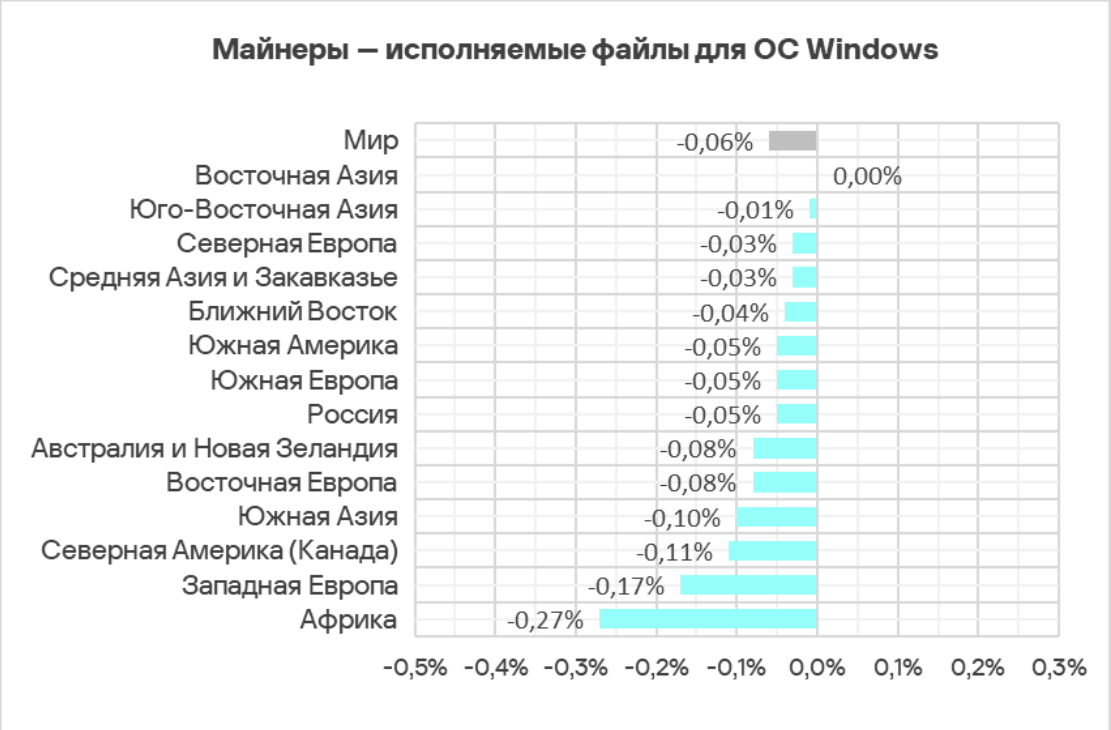
В регионах доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, варьирует от 0,13% в Австралии и Новой Зеландии до 1,17% в Средней Азии и Закавказье. В тройку лидеров по этому показателю, кроме Средней Азии и Закавказья, входят Россия и Восточная Европа.

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



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, в третьем квартале 2025 года уменьшилась во всех регионах, кроме Восточной Азии.

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



Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, в третьем квартале 2025 года уменьшилась до 0,25%. Это минимальное значение за период с третьего квартала 2022 года.

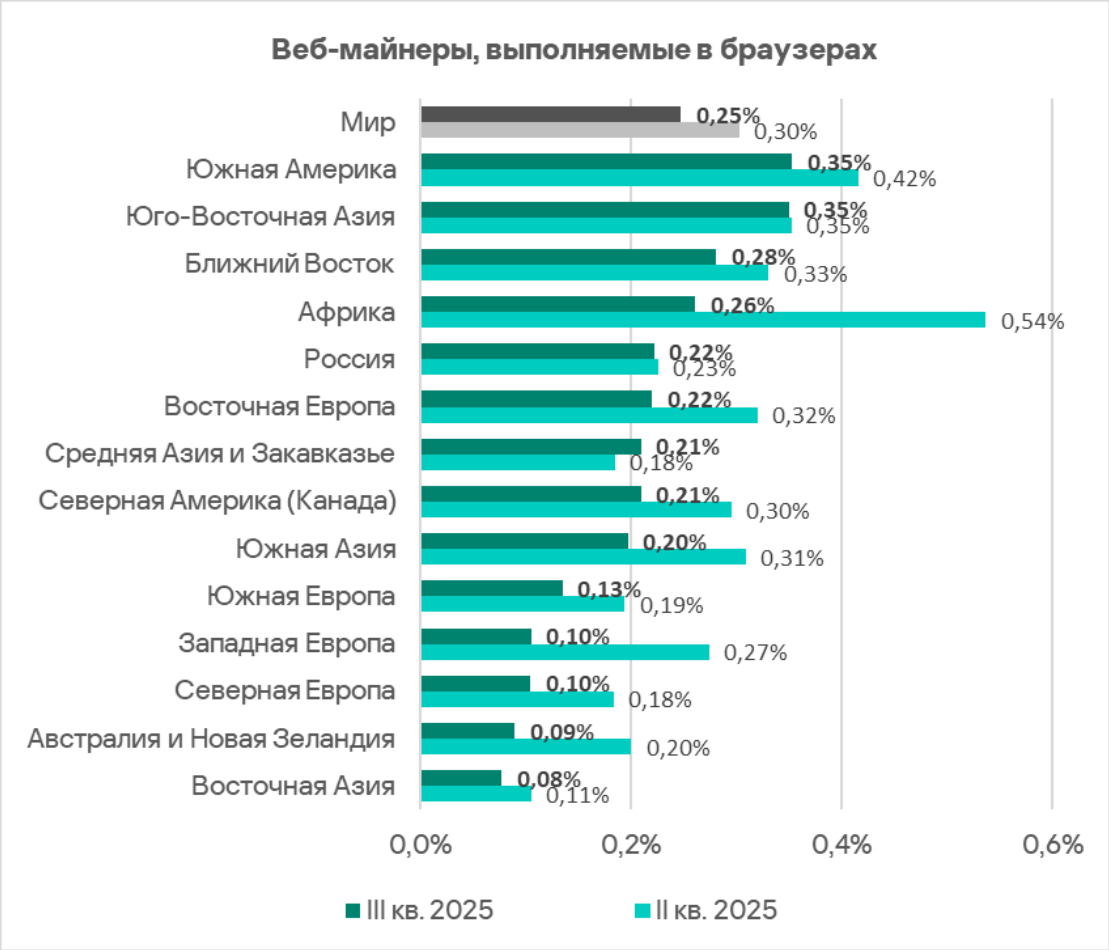
Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, III квартал 2022 года — III квартал 2025 года

В сентябре 2025 года был отмечен минимальный месячный показатель с января 2022 года.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, сентябрь 2023 года — сентябрь 2025 года

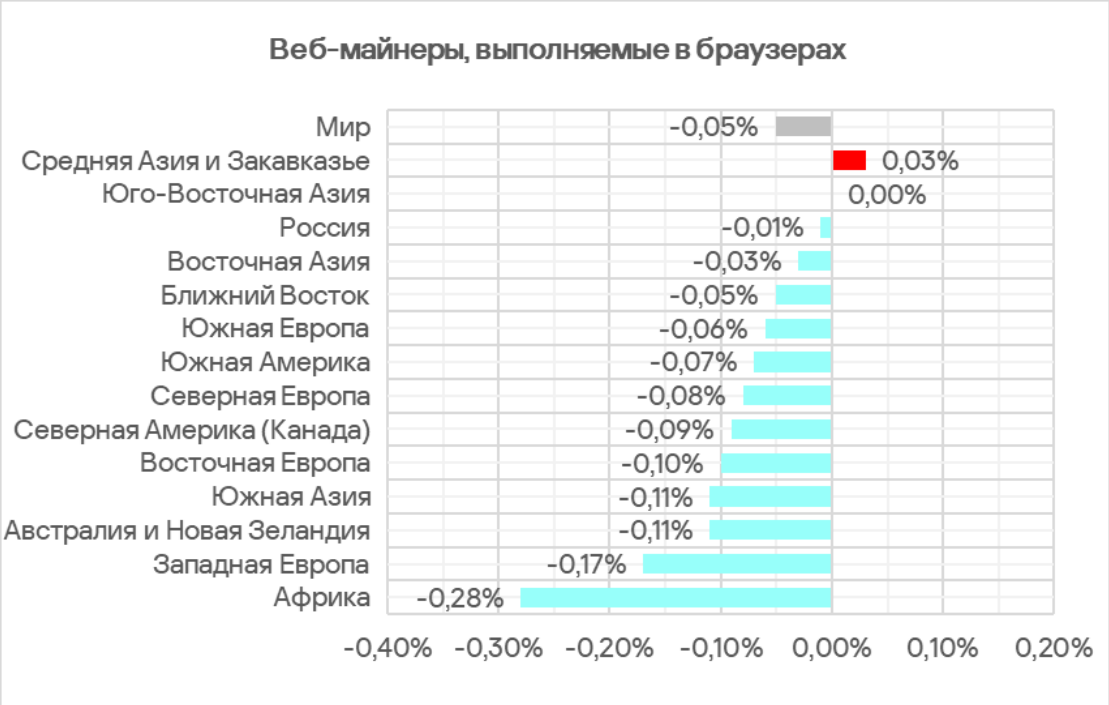
В регионах доля компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, варьирует от 0,08% в Восточной Азии до 0,35% в Южной Америке. Топ 3 регионов по этому показателю: Южная Америка, Юго-Восточная Азия и Ближний Восток.

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



В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы веб-майнеры, уменьшилась во всех регионах, кроме Средней Азии и Закавказья и Юго-Восточной Азии.

Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, III 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.

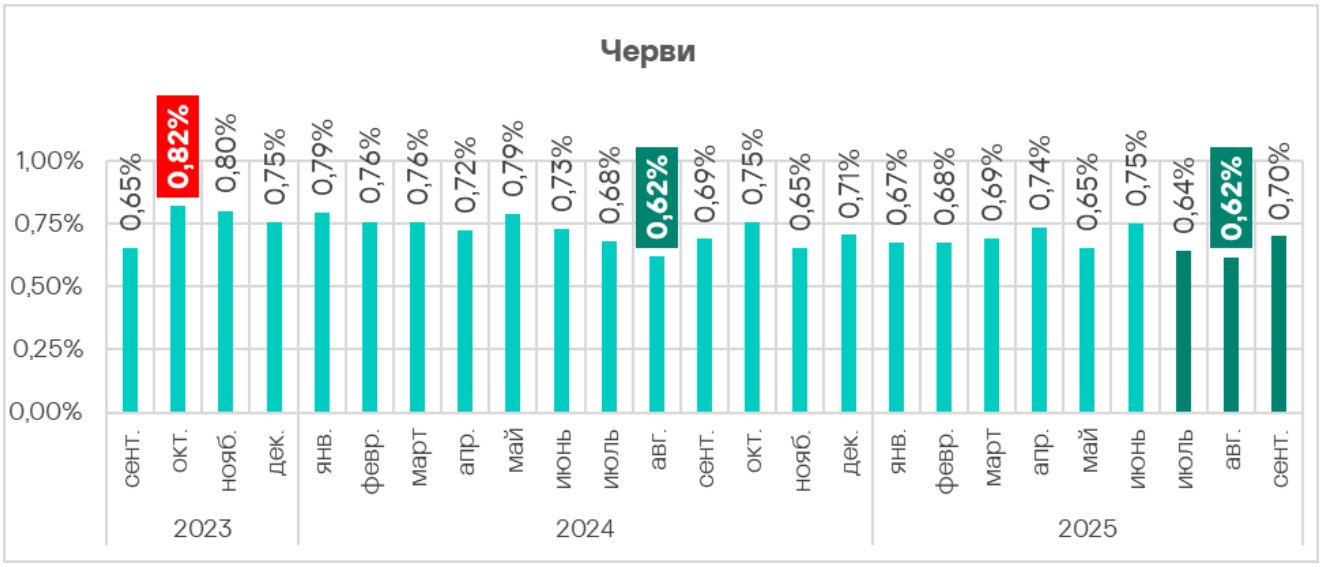
Высокие показатели обнаружения самораспространяющегося вредоносного ПО и ПО, которое распространяется через сетевые папки, на уровне отрасли, страны или региона, как правило, указывают на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных устройств. 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 третьем квартале 2025 года после минимума предыдущего квартала увеличилась до 1,26%.

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

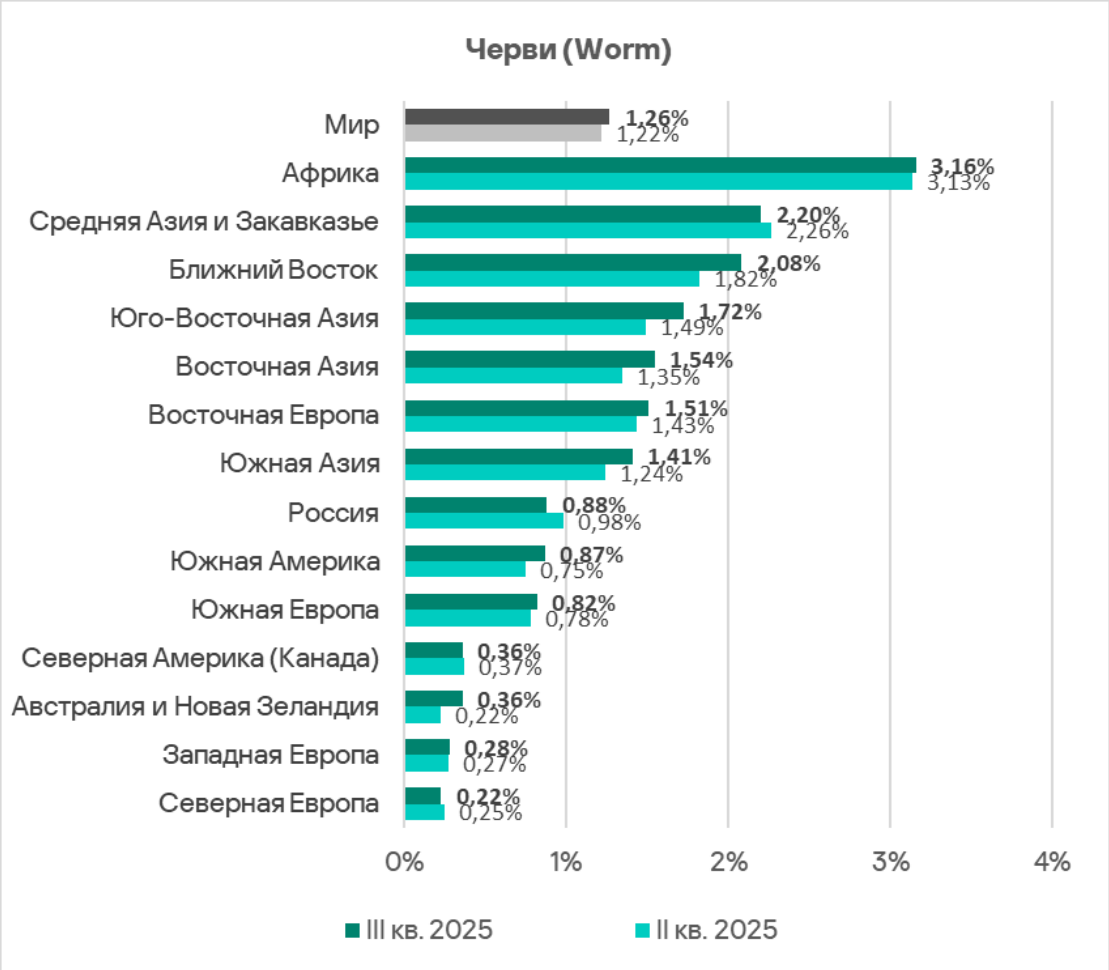
В течение квартала самым высоким показатель за месяц был в сентябре.



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

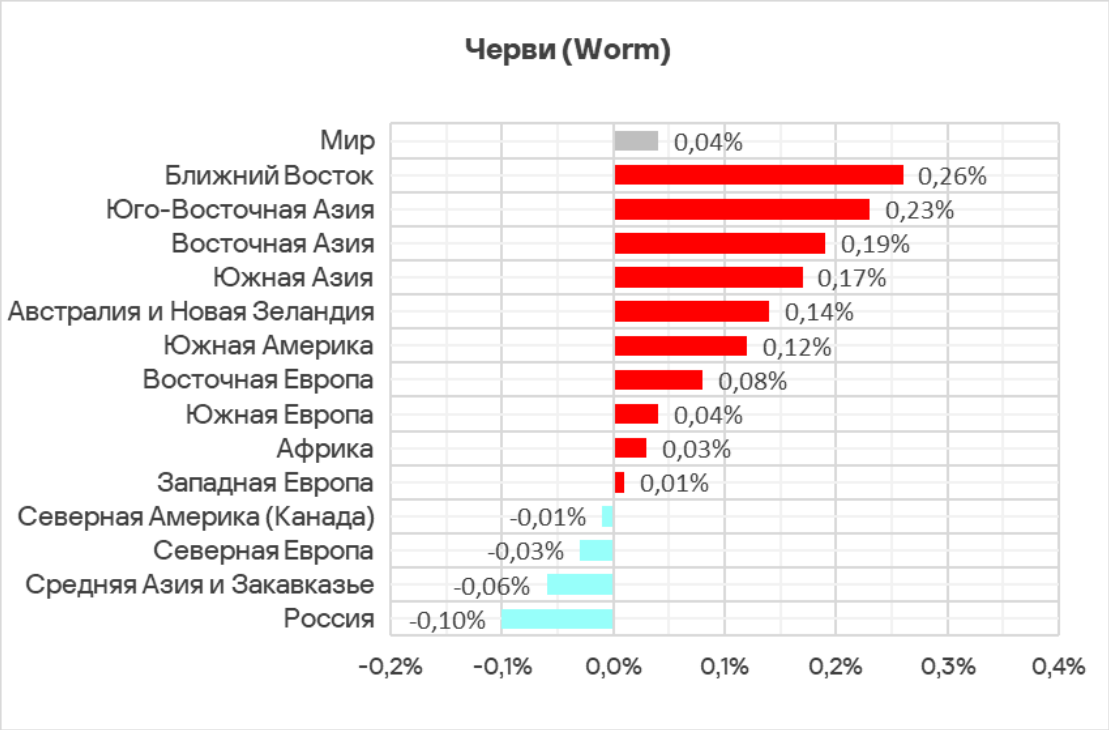
В регионах доля компьютеров АСУ, на которых были заблокированы черви, варьирует от 0,22% в Северной Европе до 3,16% в Африке. Топ 3 регионов по этому показателю неизменен: Африка, Средняя Азия и Закавказье, Ближний Восток.

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



Во всех регионах, кроме Северной Америки (Канада), Северной Европы, России и региона Средняя Азия и Закавказье, показатель вырос.

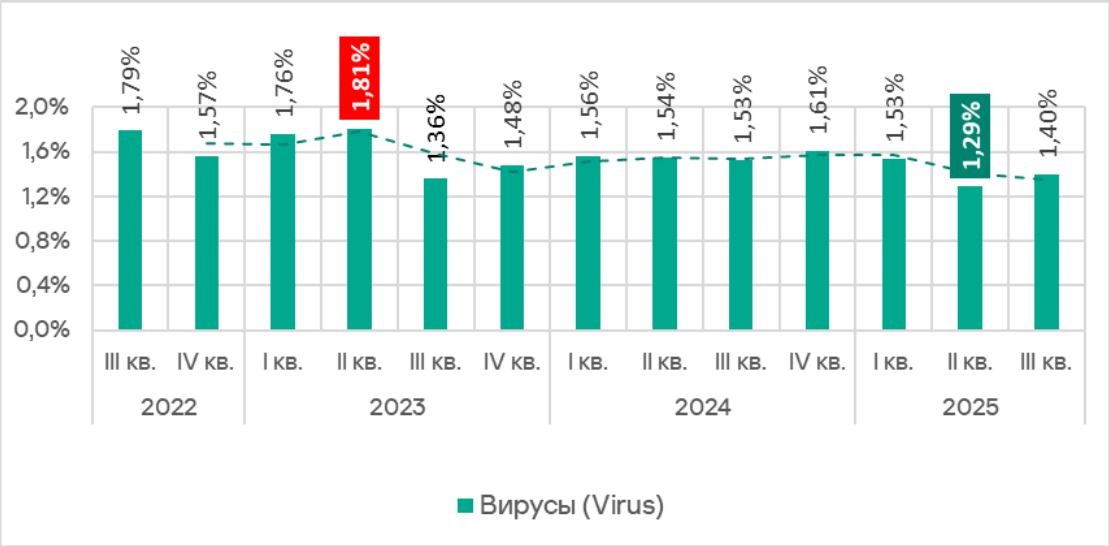
Изменение доли компьютеров АСУ, на которых были заблокированы черви, III квартал 2025 года



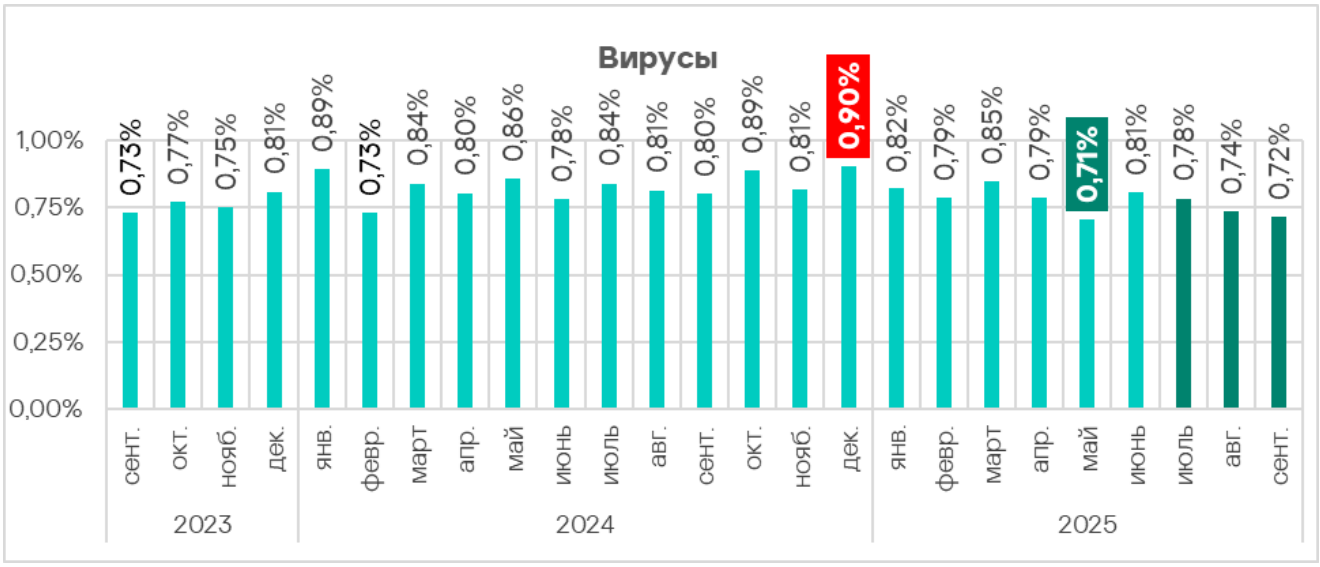
Вирусы

Доля компьютеров АСУ, на которых были заблокированы вирусы, в третьем квартале 2025 года после минимума предыдущего квартала увеличилась до 1,40%.

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



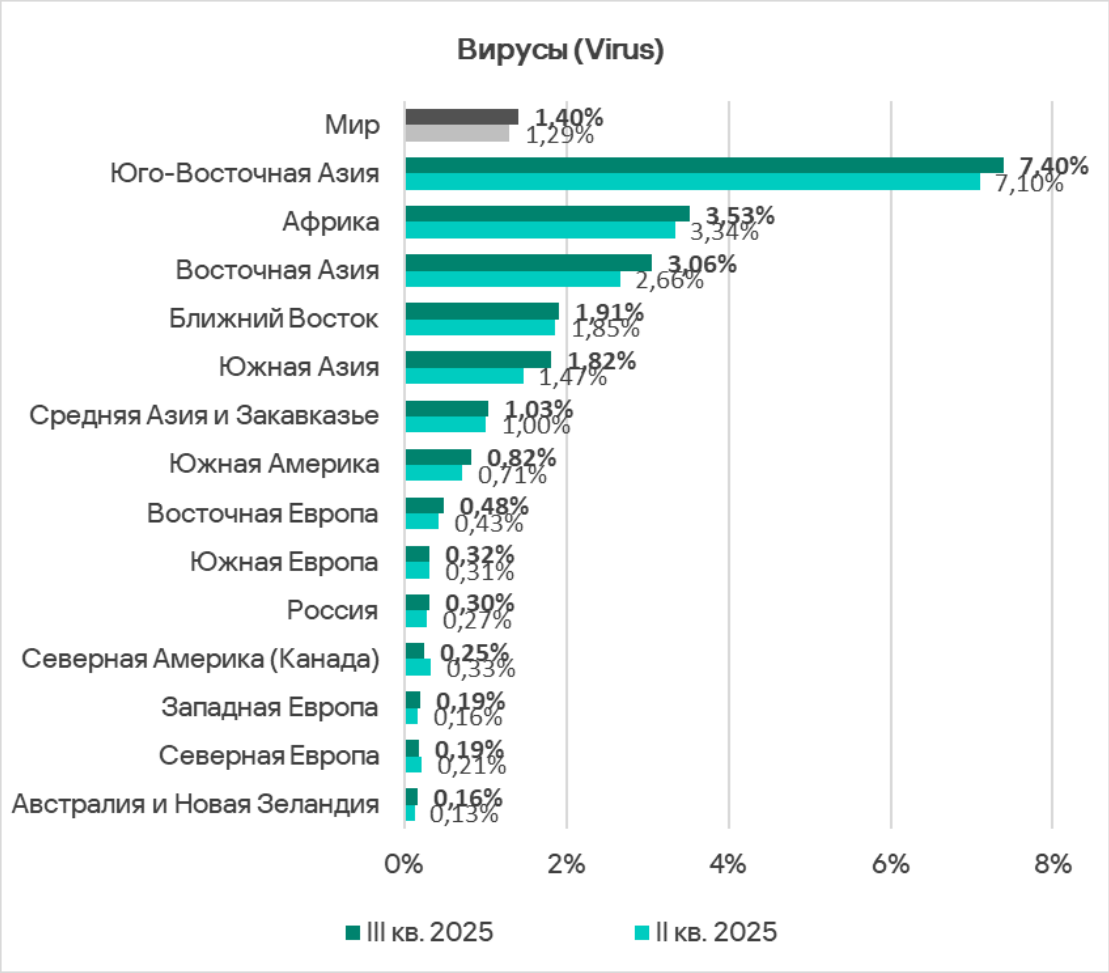
Наибольшее месячное значение показателя третьего квартала 2025 года было в июле.



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

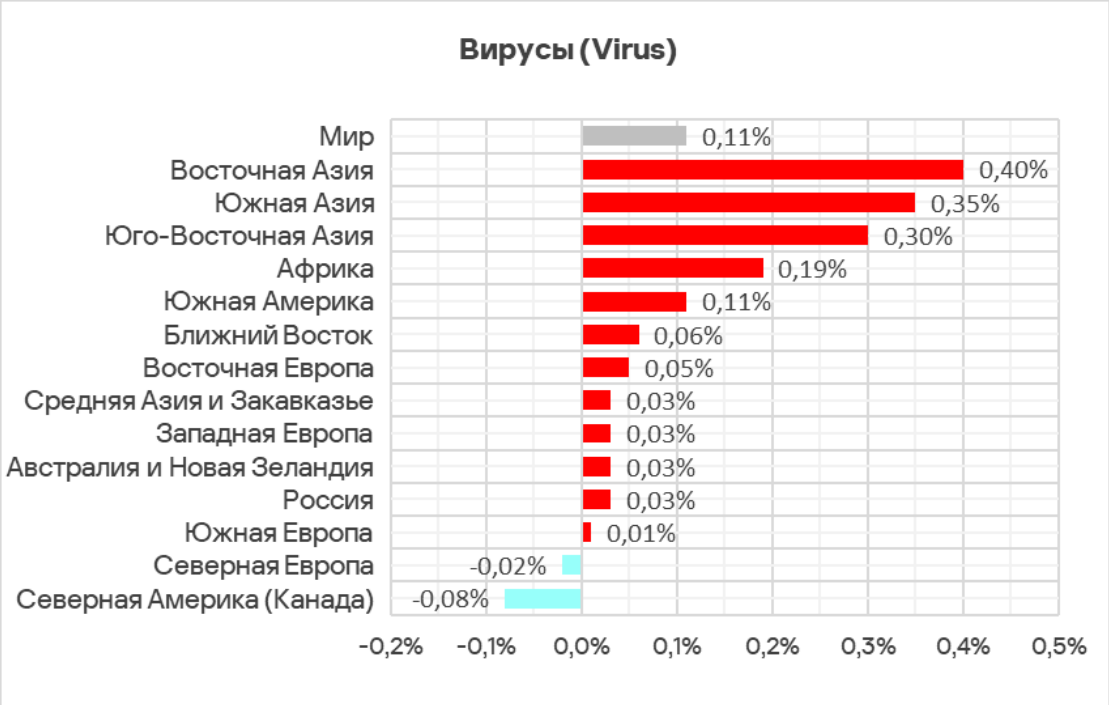
В регионах доля компьютеров АСУ, на которых были заблокированы вирусы, варьирует от 0,16% в Австралии и Новой Зеландии до 7,40% в Юго-Восточной Азии. Топ 3 регионов по этому показателю не изменился, и он такой же, как и в случае вредоносных программ для AutoCAD: Юго-Восточная Азия (с большим отрывом от остальных), Африка и Восточная Азия.

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



Доля компьютеров АСУ, на которых были заблокированы вирусы, в третьем квартале 2025 года увеличилась во всех регионах, кроме Северной Европы и Северной Америки (Канада). Больше всего показатель увеличился в Восточной, Южной и Юго-Восточной Азии.

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



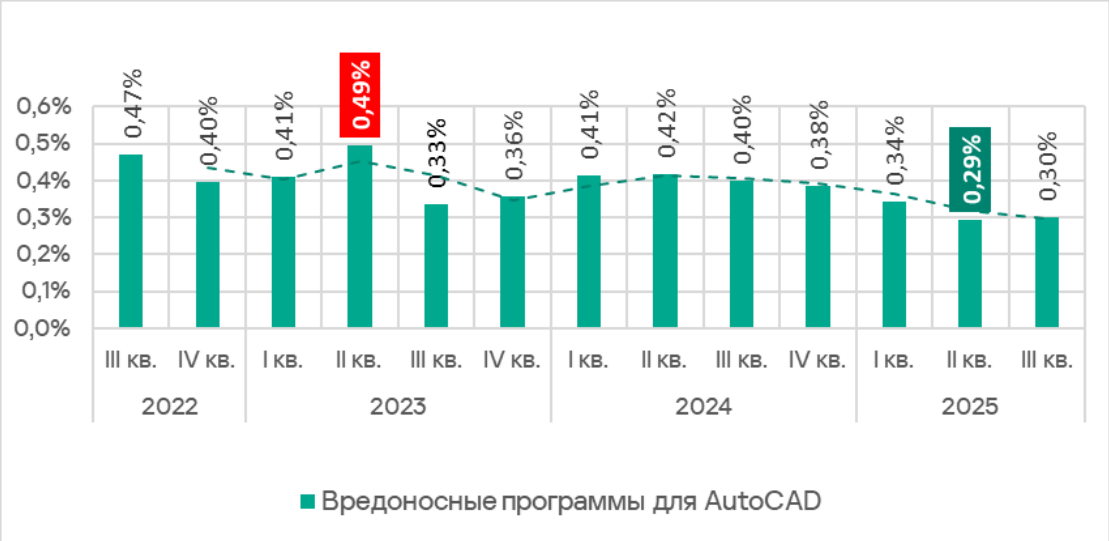
Вредоносные программы для AutoCAD

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.

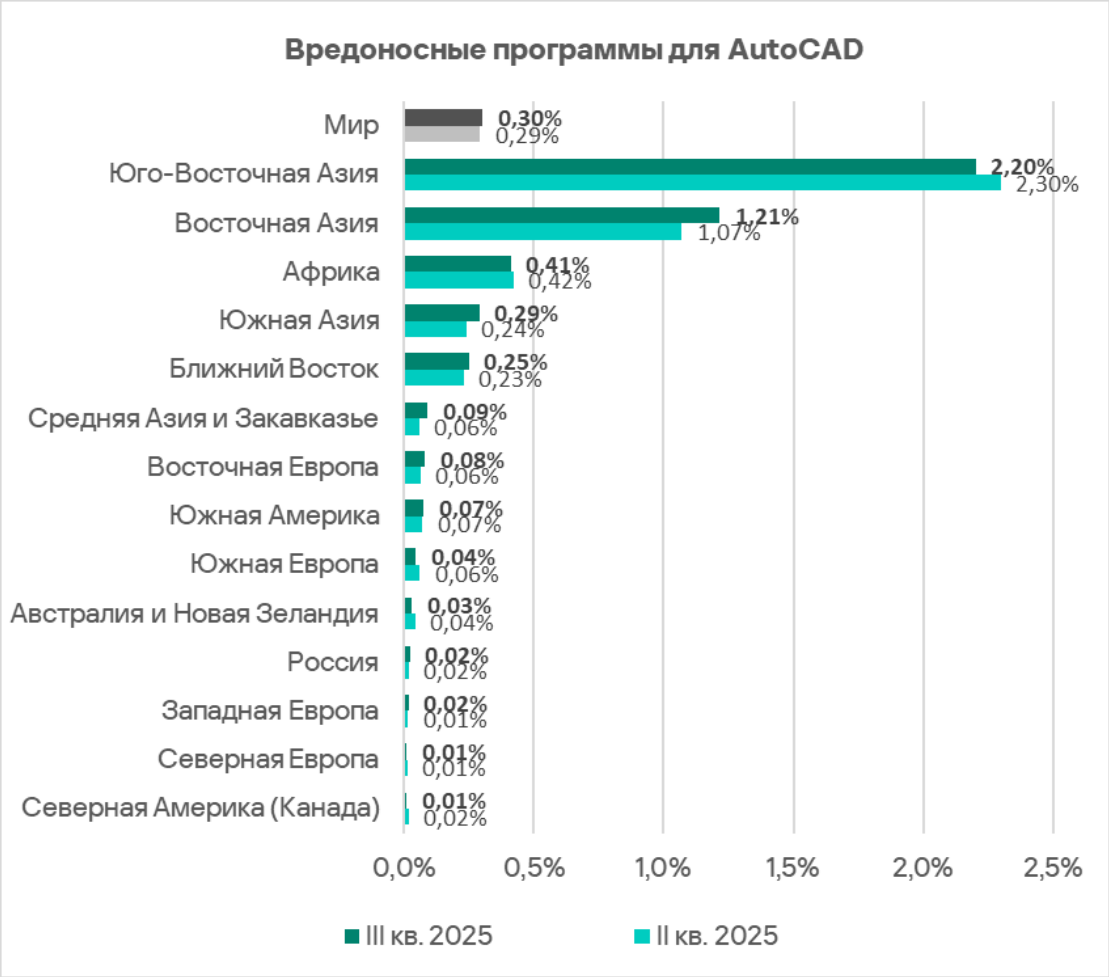
В третьем квартале 2025 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, после минимума предыдущего квартала подросла до 0,30%.

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



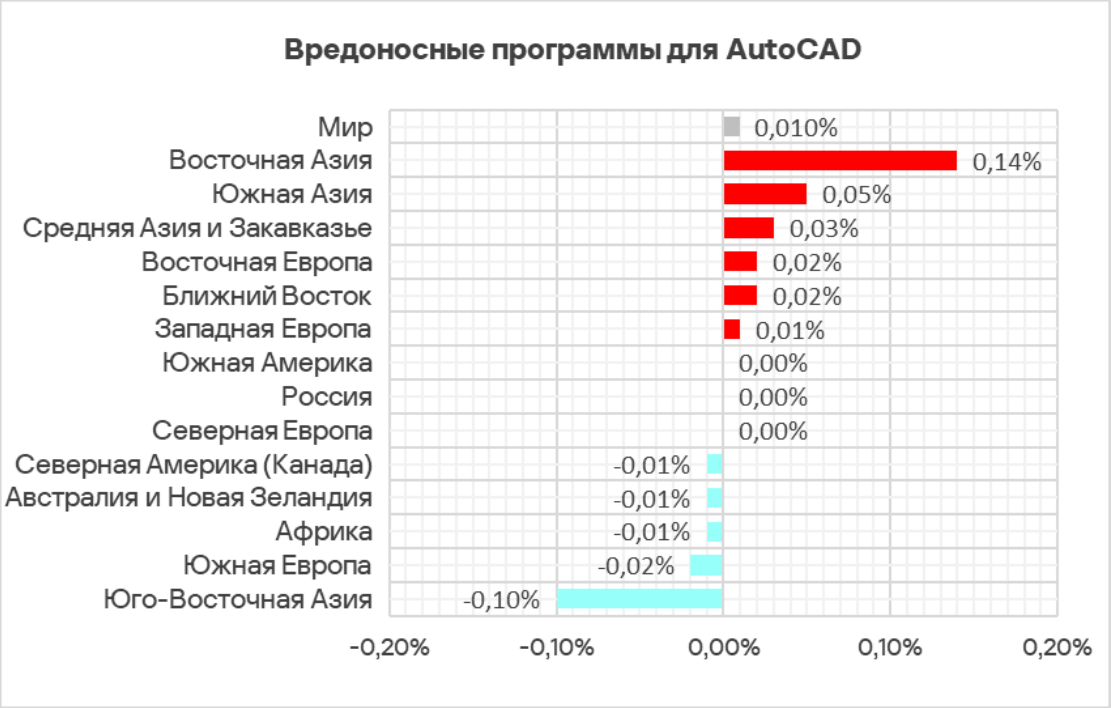
В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, варьирует от 0,01% в Северной Америке (Канада) до 2,20% в Юго-Восточной Азии. Лидируют по этому показателю те же регионы, что и в рейтинге по вирусам: Юго-Восточная Азия, Восточная Азия (оба региона с отрывом от остальных) и Африка.

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



Показатель вредоносных программ для AutoCAD в третьем квартале 2025 года увеличился в шести регионах, больше всего — в Восточной Азии.

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



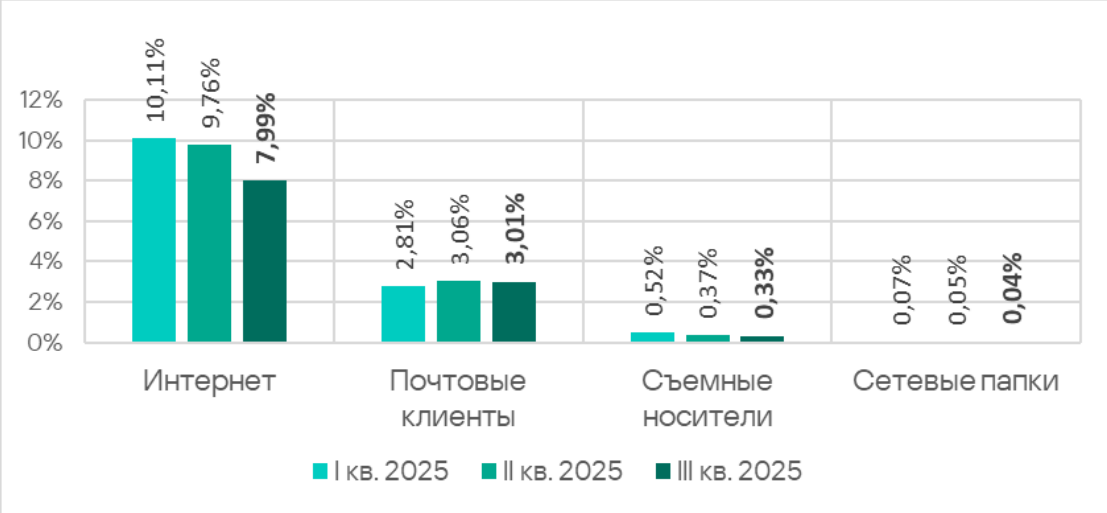
Основные источники угроз

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 третьем квартале 2025 года показатели всех источников угроз в среднем по миру уменьшились.

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 с них был разрешен доступ к внешним сервисам.

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, уменьшилась до 7,99% — это минимальный показатель с начала 2022 года.

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

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

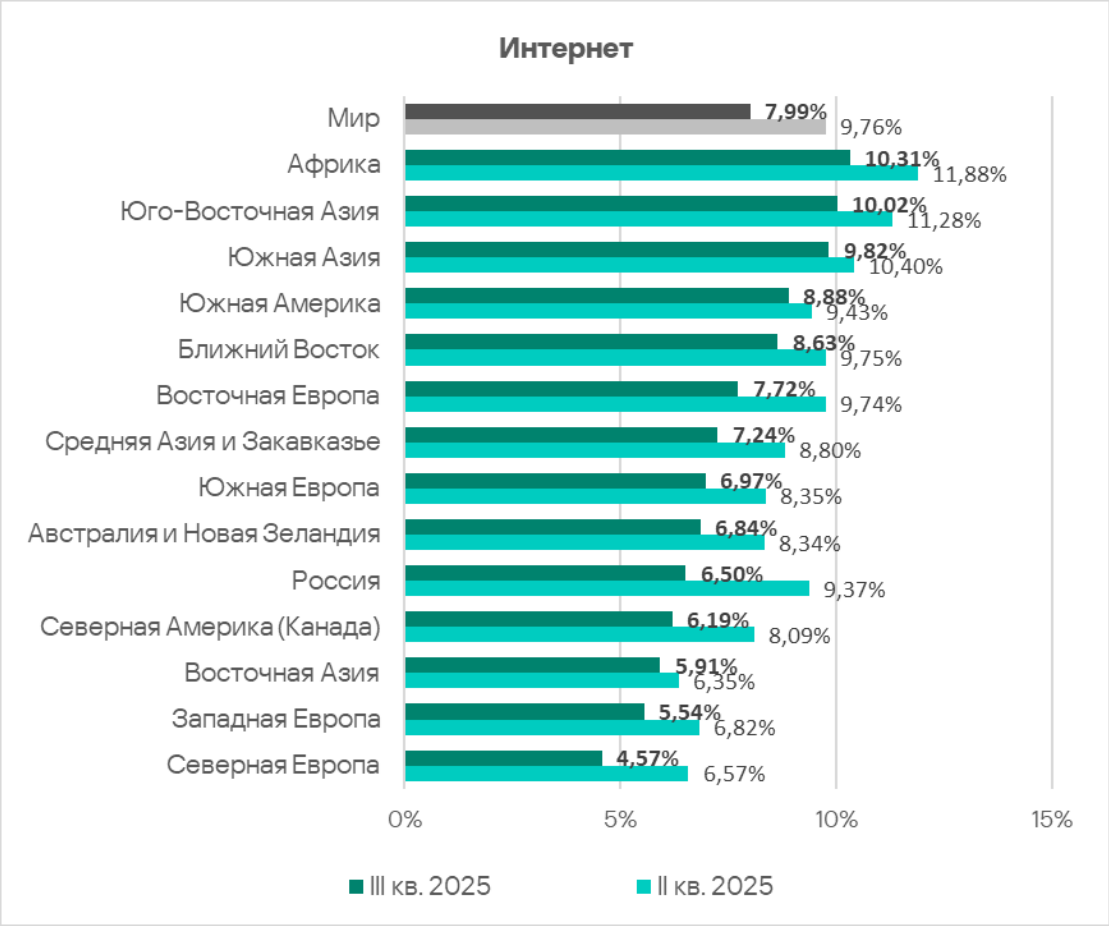
Угрозы из интернета и основные категории угроз из интернета, III квартал 2025 года — III квартал 2025 года

*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 4,57% в Северной Европе до 10,31% в Африке.

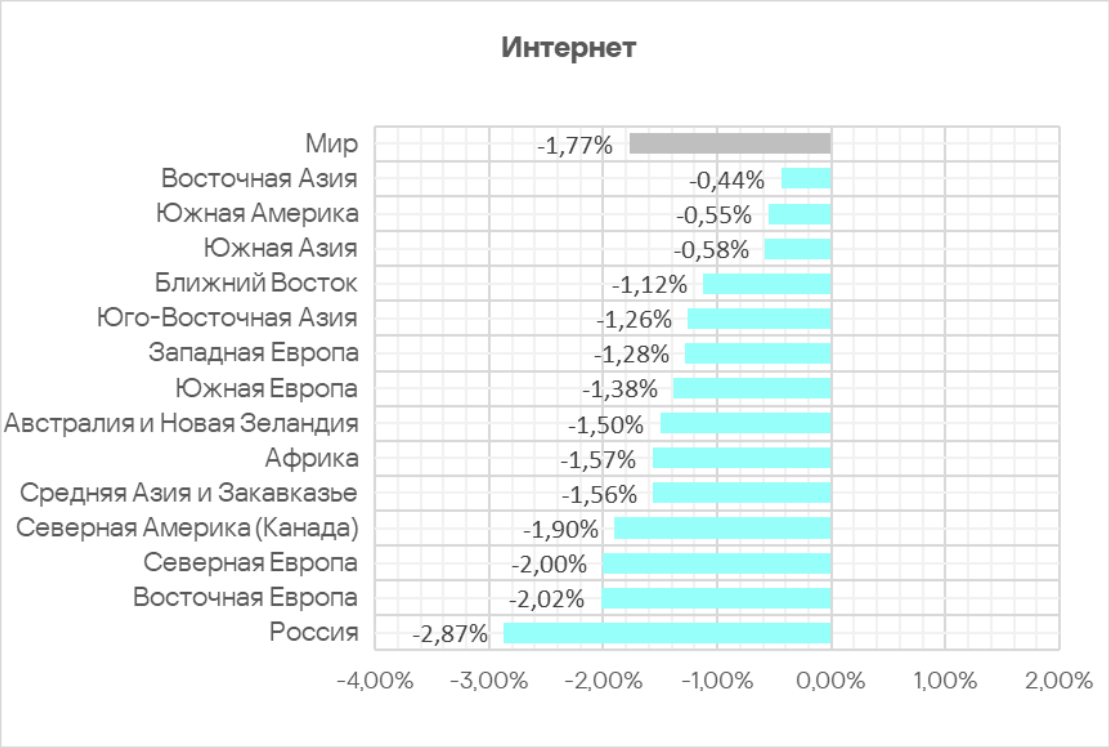
Топ 3 регионов по доле компьютеров АСУ, на которых в третьем квартале 2025 года были заблокированы угрозы из интернета: Африка, Юго-Восточная Азия и Южная Азия.

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



В третьем квартале 2025 года показатель угроз из интернета уменьшился во всех регионах.

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



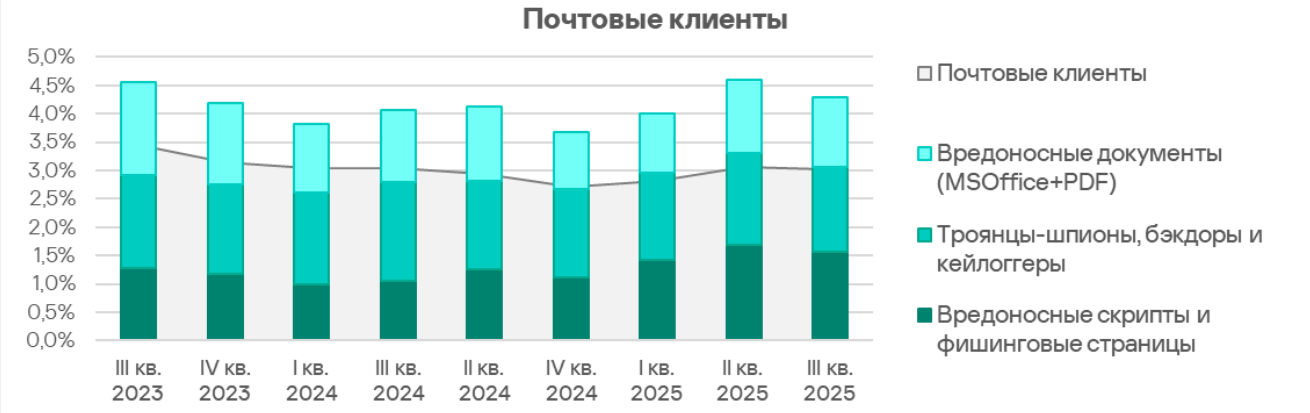
Почтовые клиенты

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 третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы такие угрозы, немного уменьшилась — до 3,01%.

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

Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ в третьем квартале 2025 года, — это вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы.



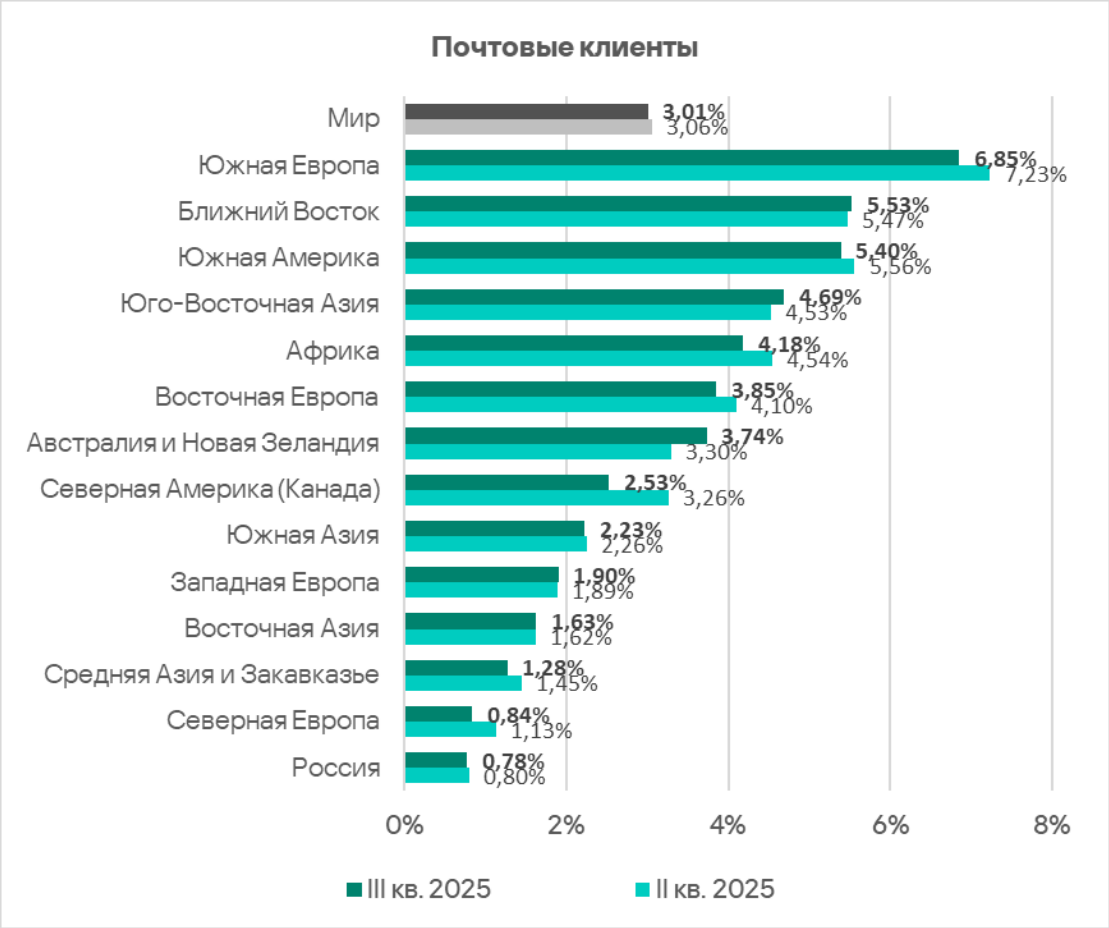
Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов, III квартал 2023 года — III квартал 2025 года

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 0,78% в России до 6,85% в Южной Европе.

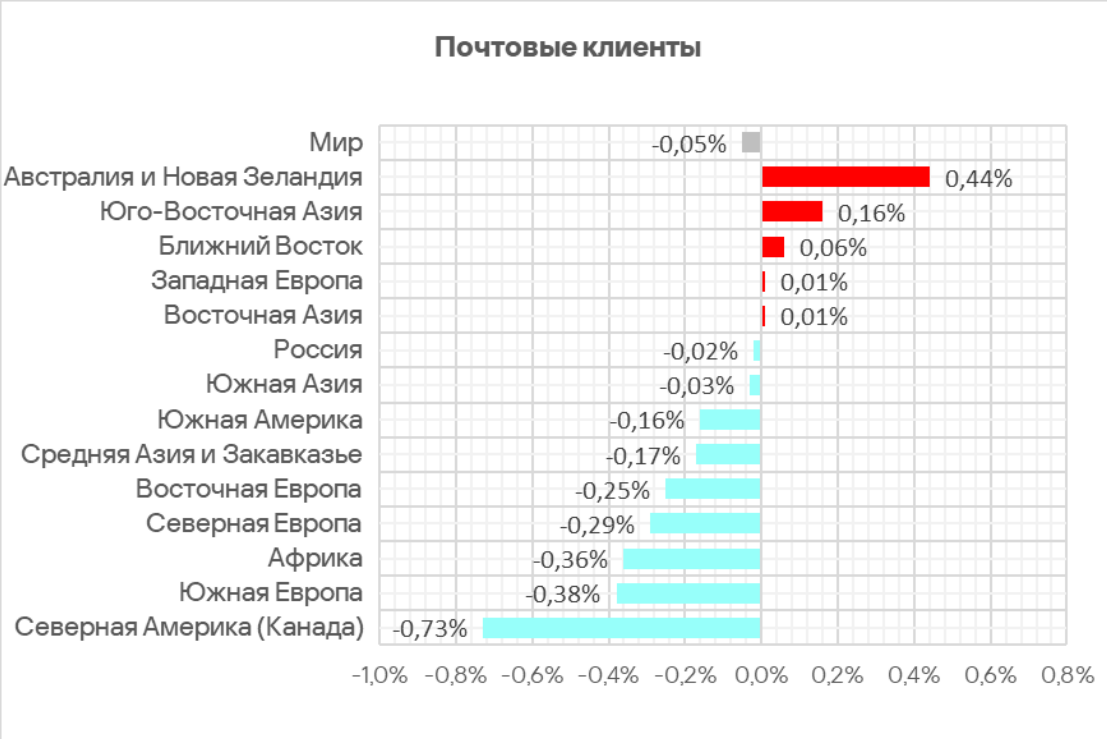
Состав топ 3 регионов по уровню угроз из почтовых клиентов не изменился. В него вошли: Южная Европа, Ближний Восток и Южная Америка.

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



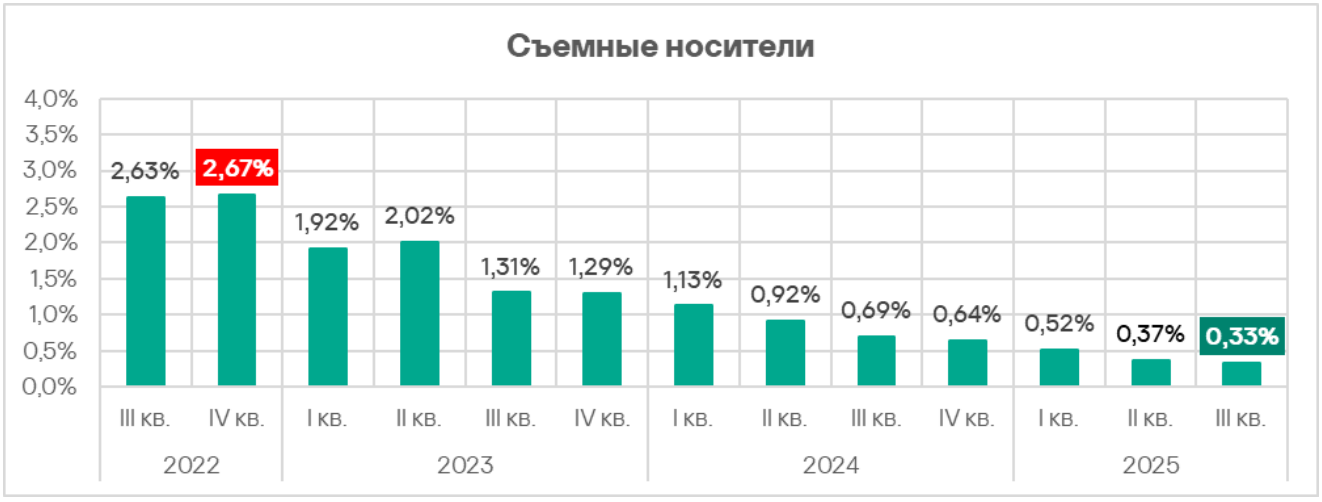
В третьем квартале 2025 показатель угроз из почтовых клиентов увеличился в пяти регионах, больше всего — в Австралии и Новой Зеландии.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, III 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 2022 года — 0,33%.



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

Основными категориями угроз, которые в третьем квартале 2025 года были заблокированы при подключении съемных устройств к компьютерам АСУ, являются черви, вирусы и шпионское ПО.

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

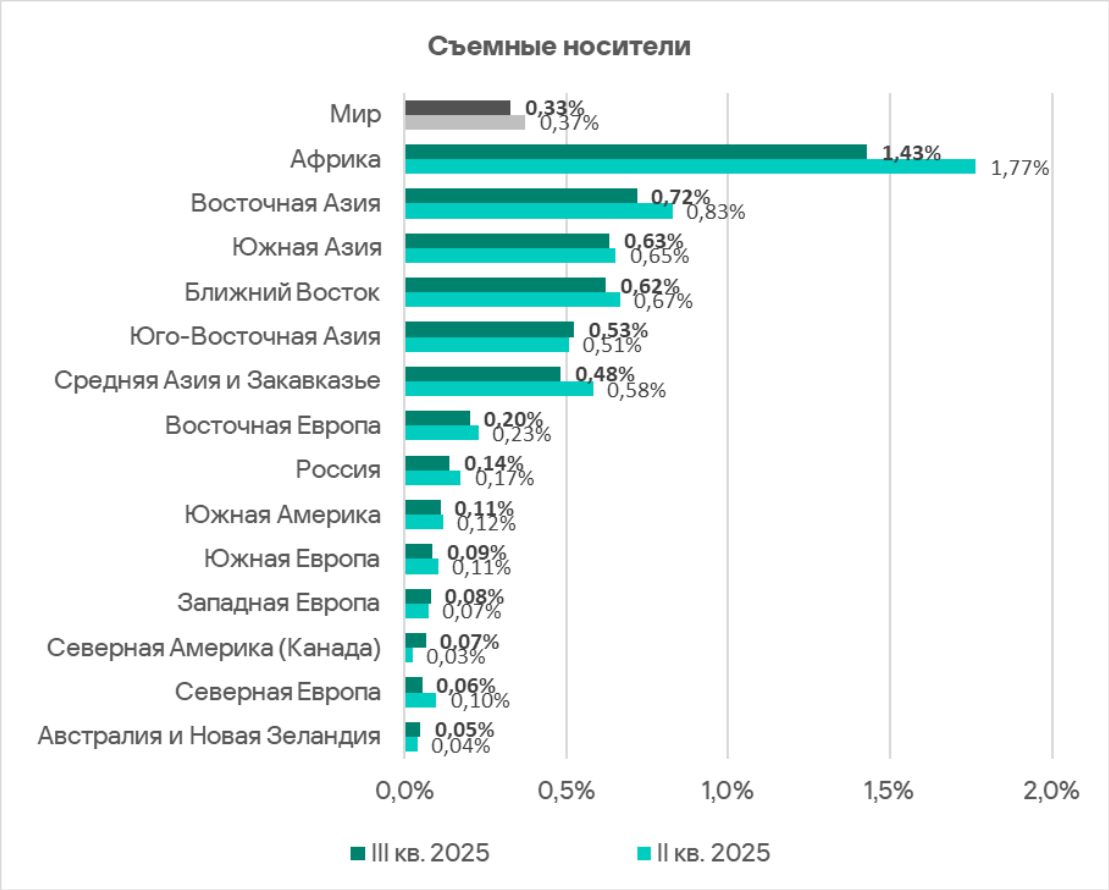
Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры. Эти современные криптомайнеры способны распространяться по локальным сетям, используя кражу учетных данных 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 1,43% 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 и Южная Азия.

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

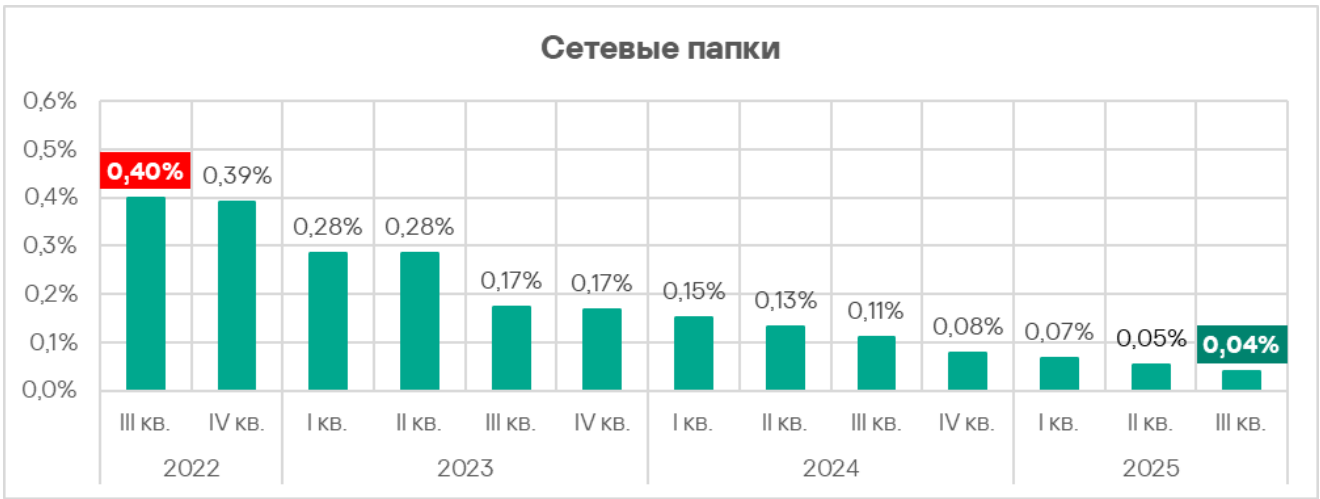


В третьем квартале 2025 показатель угроз со съемных носителей уменьшился во всех регионах, кроме Северной Америки (Канада), Юго-Восточной Азии, Западной Европы и Австралии и Новой Зеландии.

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

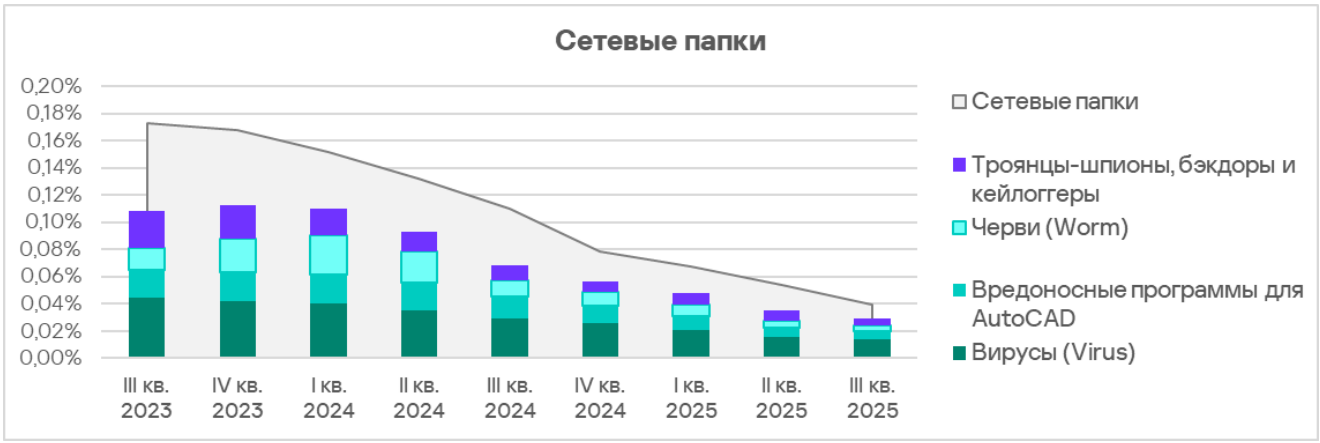
Сетевые папки

В третьем квартале 2025 года показатель по сетевым папкам достиг минимального значения с начала 2022 года.



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

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

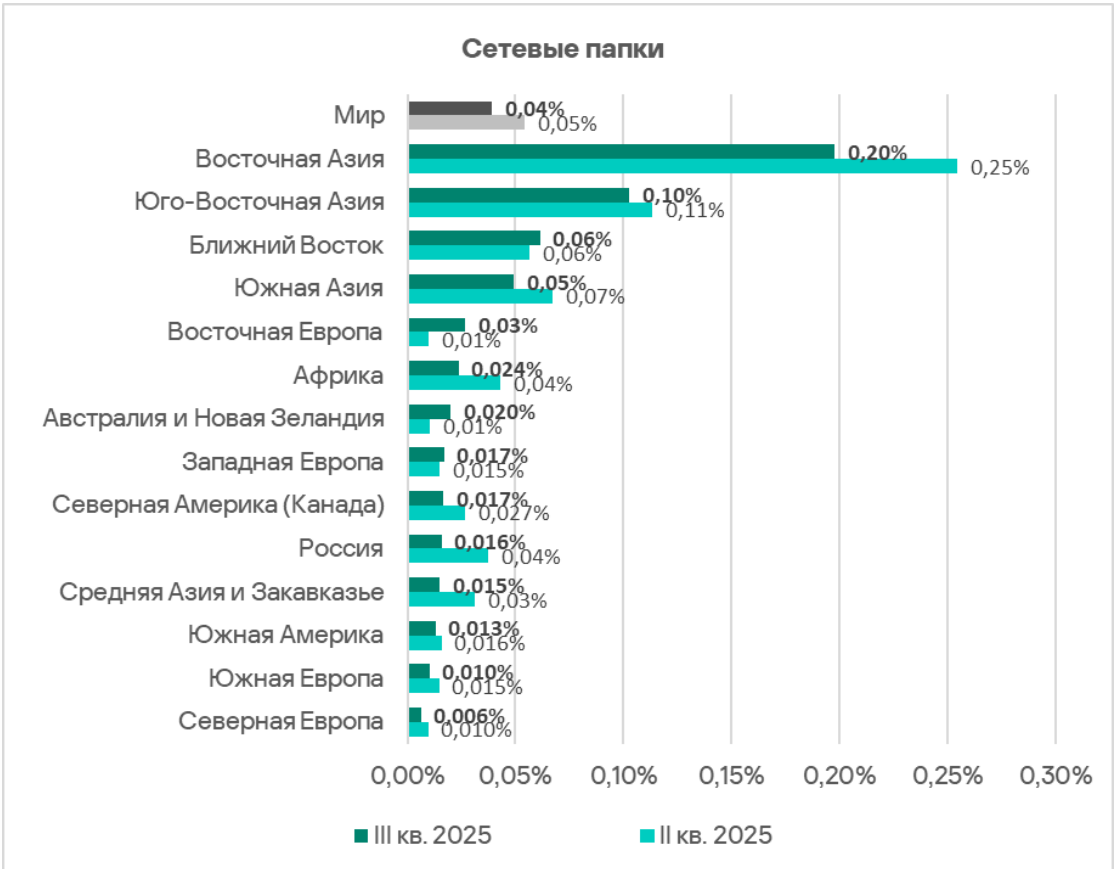


Угрозы в сетевых папках и основные категории угроз в сетевых папках, III квартал 2023 года — III квартал 2025 года

В регионах доля компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, варьирует от 0,006% в Северной Европе до 0,20% в Восточной Азии.

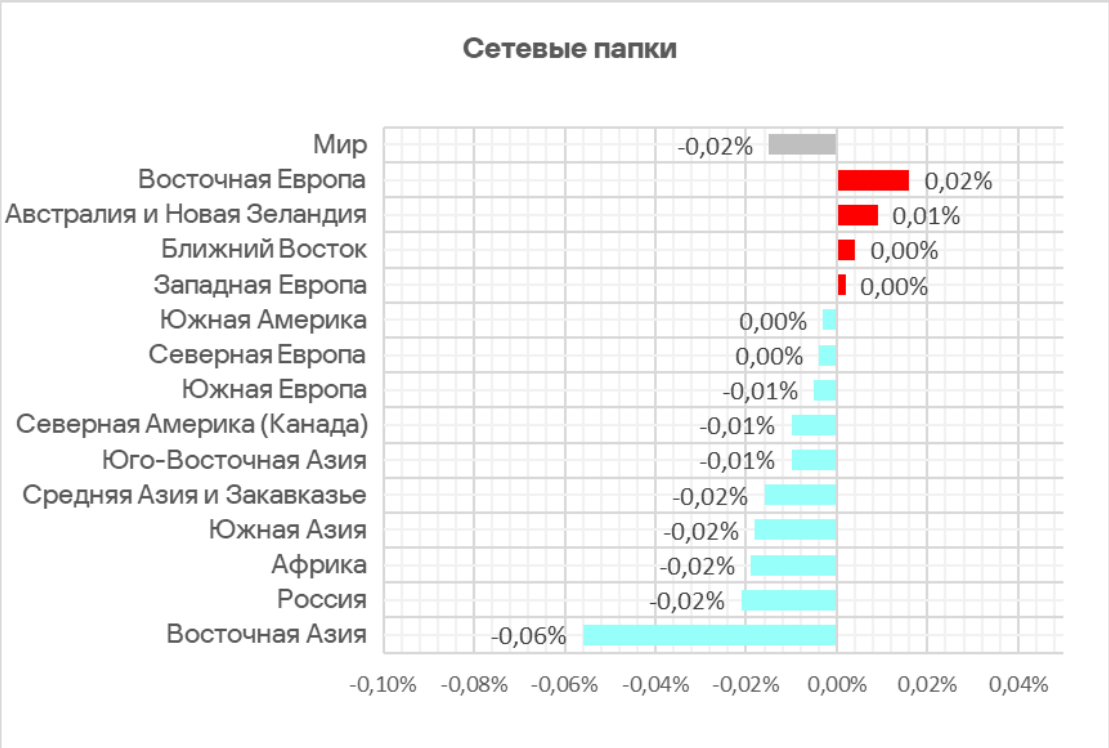
Топ 3 регионов по уровню угроз в сетевых папках: Восточная и Юго-Восточная Азия, Ближний Восток.

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



В третьем квартале 2025 показатель угроз в сетевых папках вырос в четырех регионах, больше всего — в Восточной Европе.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, III 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», 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