Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Африка. Четвертый квартал 2025 года

16.04.2026

Версия 1.0

Африка

Основные проблемы кибербезопасности в регионе

Низкий уровень зрелости кибербезопасности промышленных предприятий

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

В Африке доля компьютеров АСУ, на которых были заблокированы все категории угроз, кроме майнеров в формате исполняемых файлов для ОС Windows, выше, чем в среднем по миру.

Наличие незащищенной технологической инфраструктуры, слабая сегментация сети предприятия

В Африке доля компьютеров АСУ, на которых блокируется самораспространяющееся вредоносное ПО — черви и вирусы, — значительно выше, чем в среднем по миру. По доле компьютеров АСУ, на которых были заблокированы черви, Африка с большим отрывом лидирует среди регионов, по показателю вирусов занимает второе место.

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

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

Отсутствие или неэффективность мер защиты периметра технологической сети

Показатель шпионских программ в регионе значительно превышает среднемировое значение: в четвертом квартале 2025 года — в 1,6 раза.

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 выполнение политики использования съемных носителей).

По доле компьютеров АСУ, на которых блокируется шпионское ПО, Африка неизменно лидирует в соответствующем рейтинге регионов.

Отсутствие контроля использования съемных носителей информации

Доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей**,** в регионе в четвертом квартале 2025 года превышает аналогичный среднемировой показатель в 4,5 раза. По этому показателю Африка с большим отрывом лидирует среди регионов.

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

- о низкой степени информатизации предприятия (отсутствии защищенных внутренних систем хранения и передачи файлов);
- о существовании значительной незащищенной части инфраструктуры предприятия, которая является источником заражения накопителей;
- об общей низкой культуре информационной безопасности.

Скорость внедрения мер и средств кибербезопасности уступает темпам развития быстро развивающихся отраслей

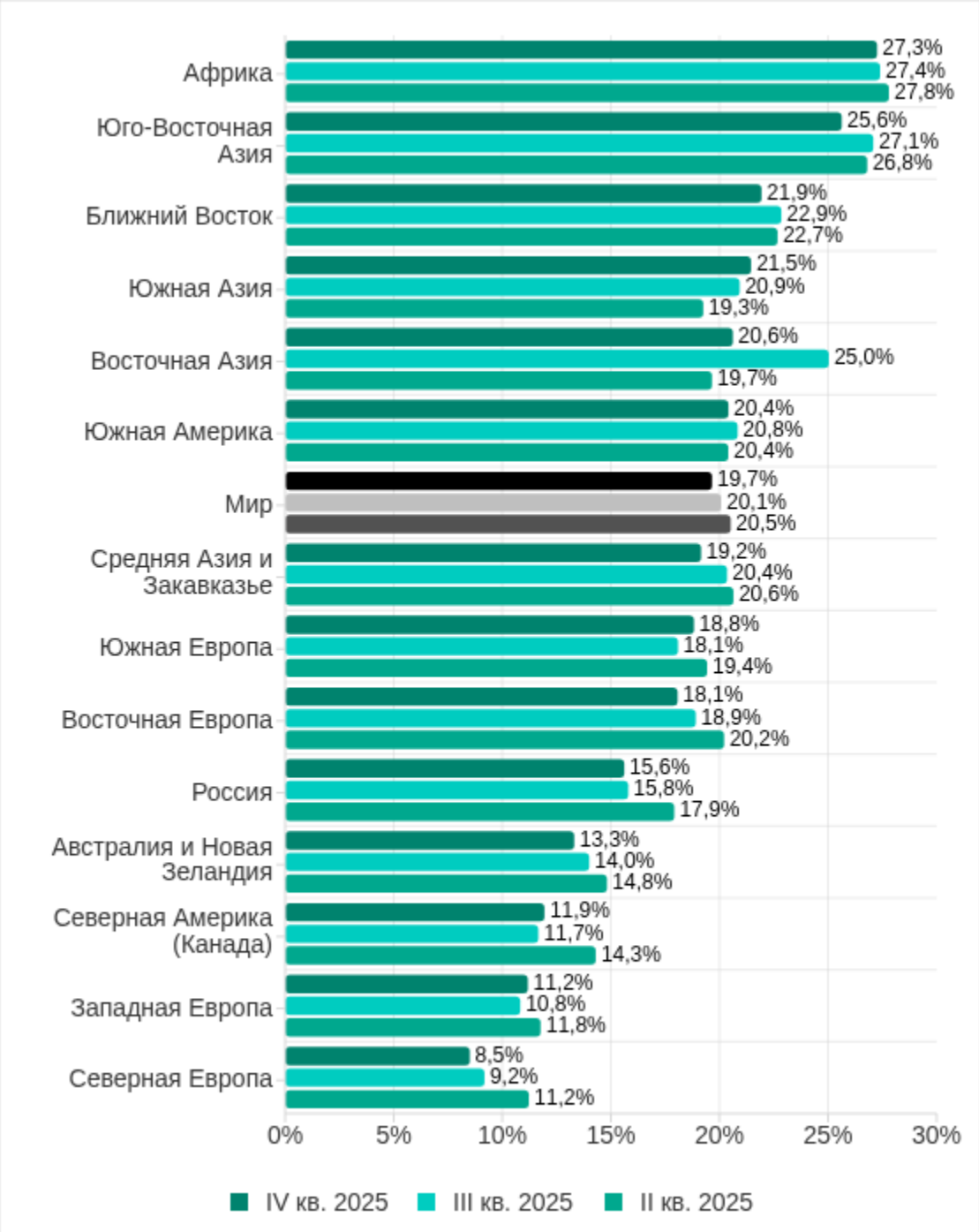
Один из общих выводов, которые можно сделать по итогам многолетних наблюдений за изменением показателей доступности OT-инфраструктур для угроз: скорость внедрения мер и средств кибербезопасности обычно уступает темпам развития отрасли. При введении объекта в эксплуатацию часто о его кибербезопасности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

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

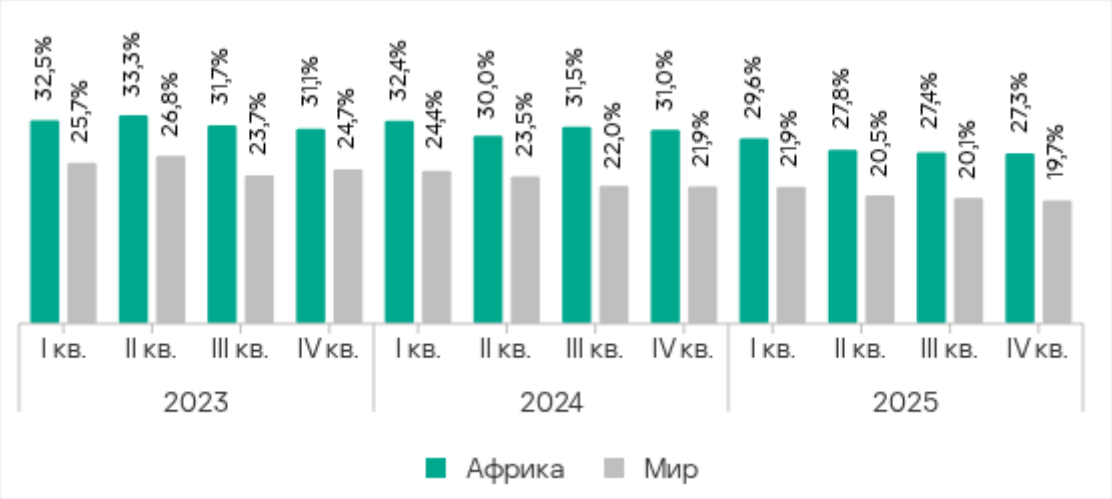
Статистика по всем угрозам

В четвертом квартале 2025 года Африка по-прежнему лидирует в рейтинге регионов по доле компьютеров АСУ, на которых были

заблокированы вредоносные объекты, с показателем, который больше в 1,4 раза, чем среднемировое значение.

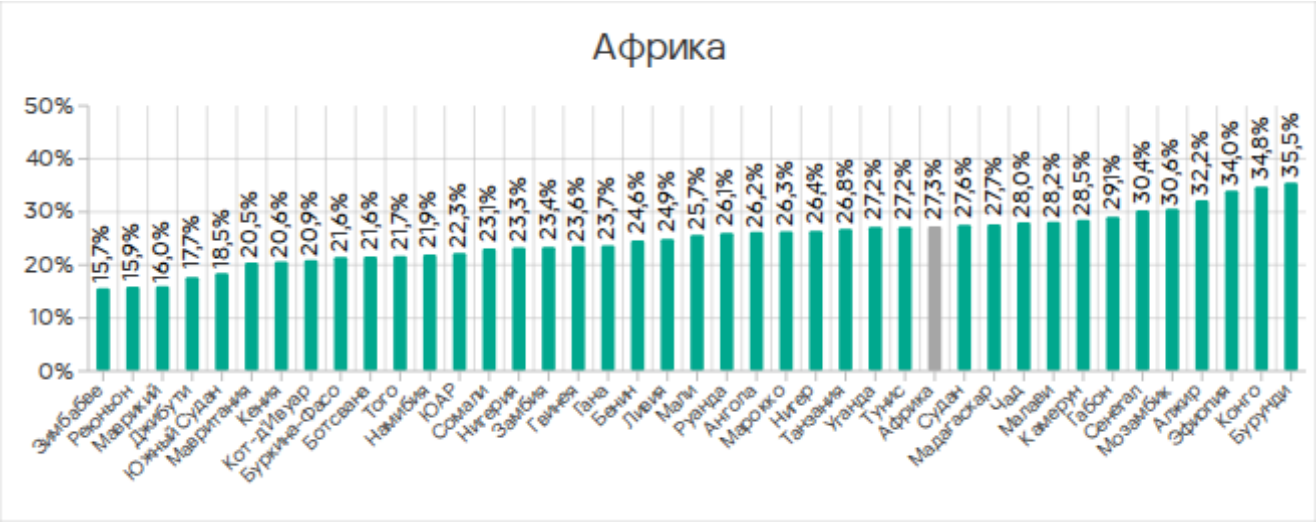


Показатель в регионе снижается пятый квартал подряд и достиг 27,3%. Это в 3,2 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.



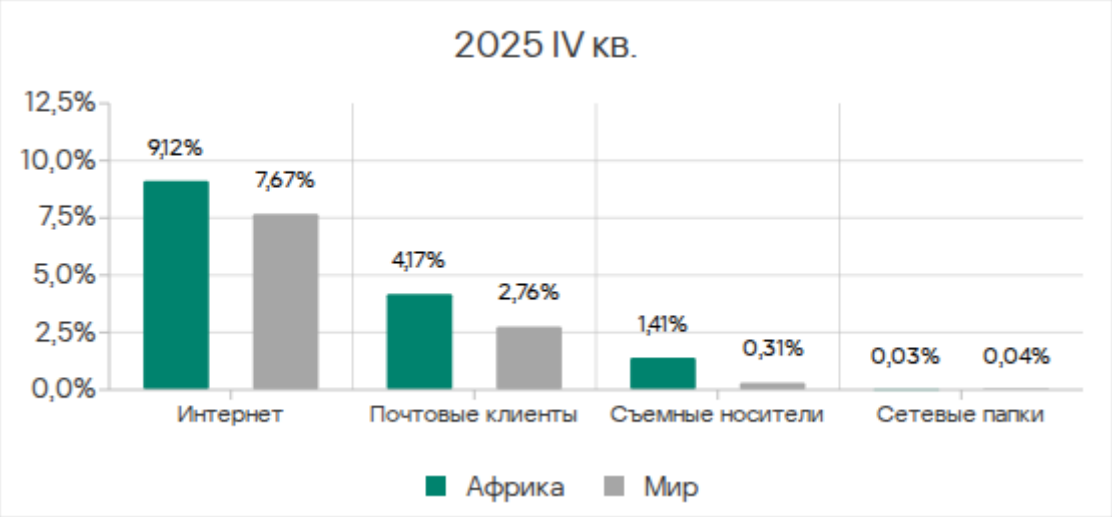
В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 15,7% в Зимбабве до 35,5% в Бурунди, где в четвертом квартале 2025 года показатель вырос сразу на 7 п. п.

Ниже 20% показатель лишь в трех странах — в Зимбабве, на Маврикии и в Джибути. В Сенегале, Мозамбике, Алжире, Эфиопии, ДР Конго и Бурунди он превышает 30%.



Источники угроз

В четвертом квартале 2025 года значения по всем источникам угроз, кроме сетевых папок, в регионе превышают среднемировые. В случае съемных носителей это превышение весьма значительно — в 4,5 раза. Показатель угроз из интернета в Африке выше среднемирового в 1,2 раза, почтовых клиентов — в 1,5 раза.



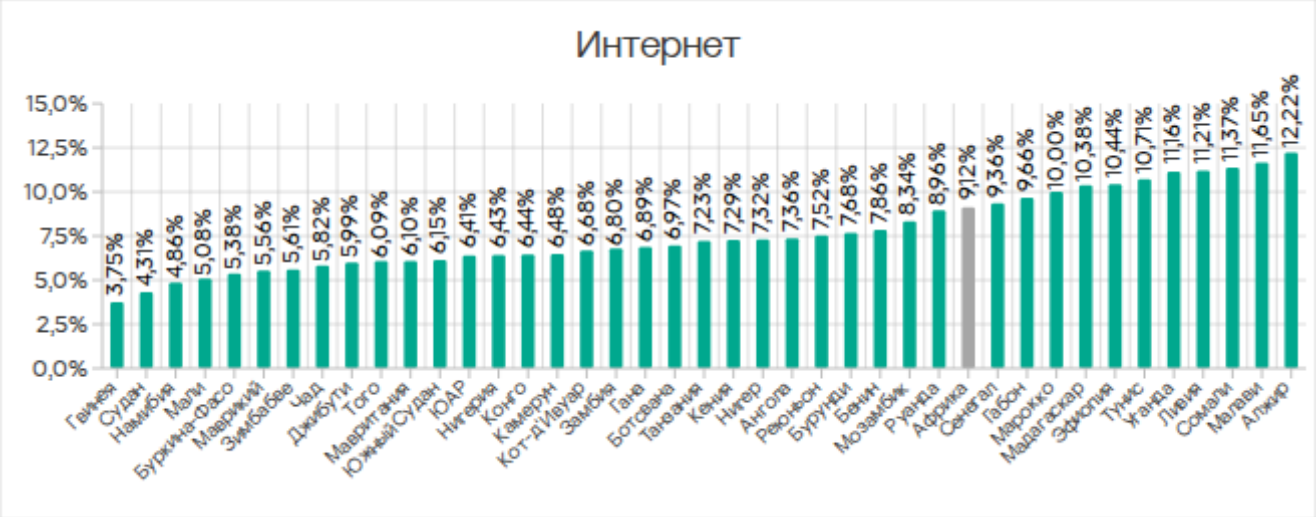
Показатели всех источников угроз, кроме сетевых папок, за квартал уменьшились. Доля компьютеров АСУ, на которых блокировались угрозы в сетевых папках, выросла на 0,007 п. п.

Интернет

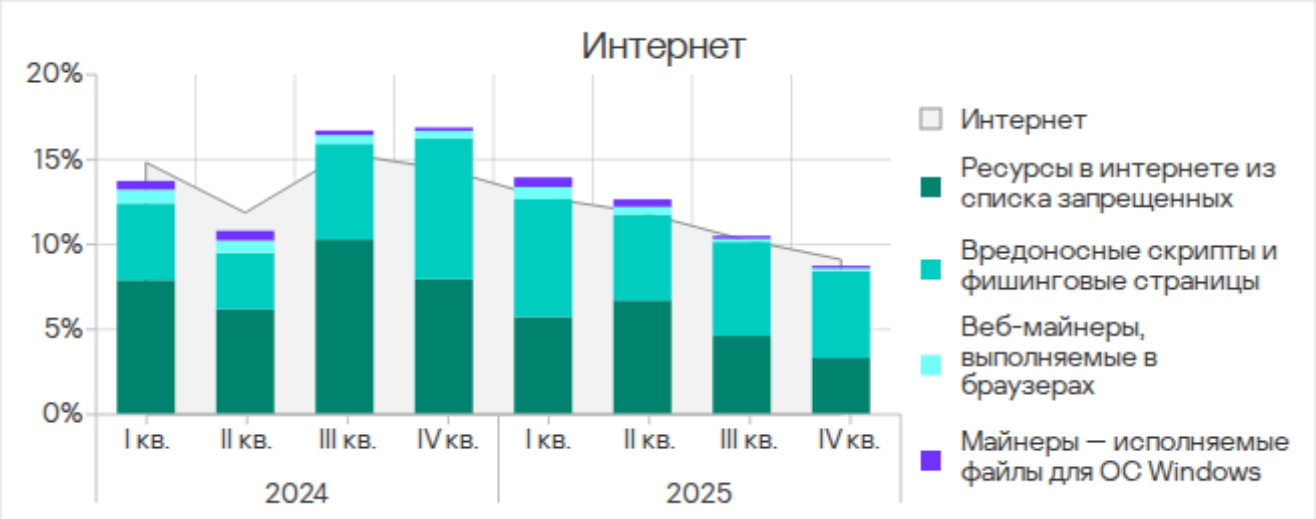
В четвертом квартале 2025 года в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Африка сместилась с первого на третье место. За три года это третий случай, когда регион уступает первенство в этом рейтинге.

Показатель Африки — 9,12% — превышает показатель Северной Европы, которая занимает последнее место в соответствующем рейтинге, в 2,3 раза.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, лидирует Алжир с 12,22%. Наименьший в регионе показатель — 3,75% — в Гвинее.



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



Почтовые клиенты

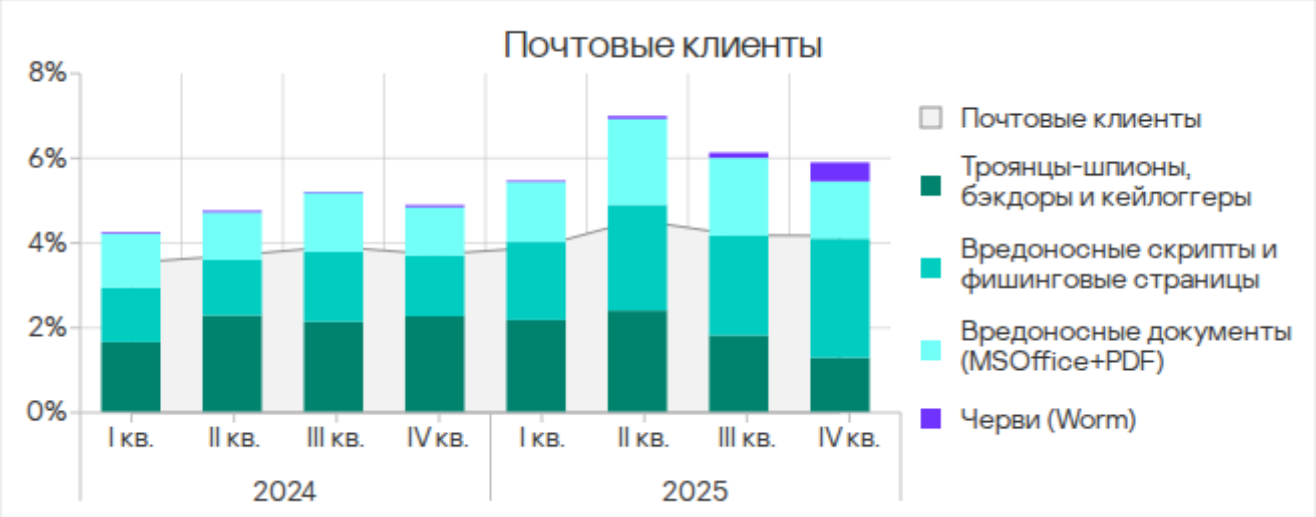
В рейтинге регионов по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, Африка по-прежнему находится на пятом месте.

После роста в первые два квартале 2025 года значения уменьшились. Несмотря на снижение во второй половине года, в 2025 году все квартальные показатели были выше, чем в предыдущие пять кварталов.

Доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, в Африке в четвертом квартале 2025 года составила 4,17%. Это в 6,5 раза выше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.

Среди стран региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, лидирует ЮАР с 11,60%. Минимальный показатель — в Буркина-Фасо (0,3%).

Основные категории угроз из электронной почты, которые были заблокированы на компьютерах АСУ в четвертом квартале 2025 года: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионское ПО и черви.

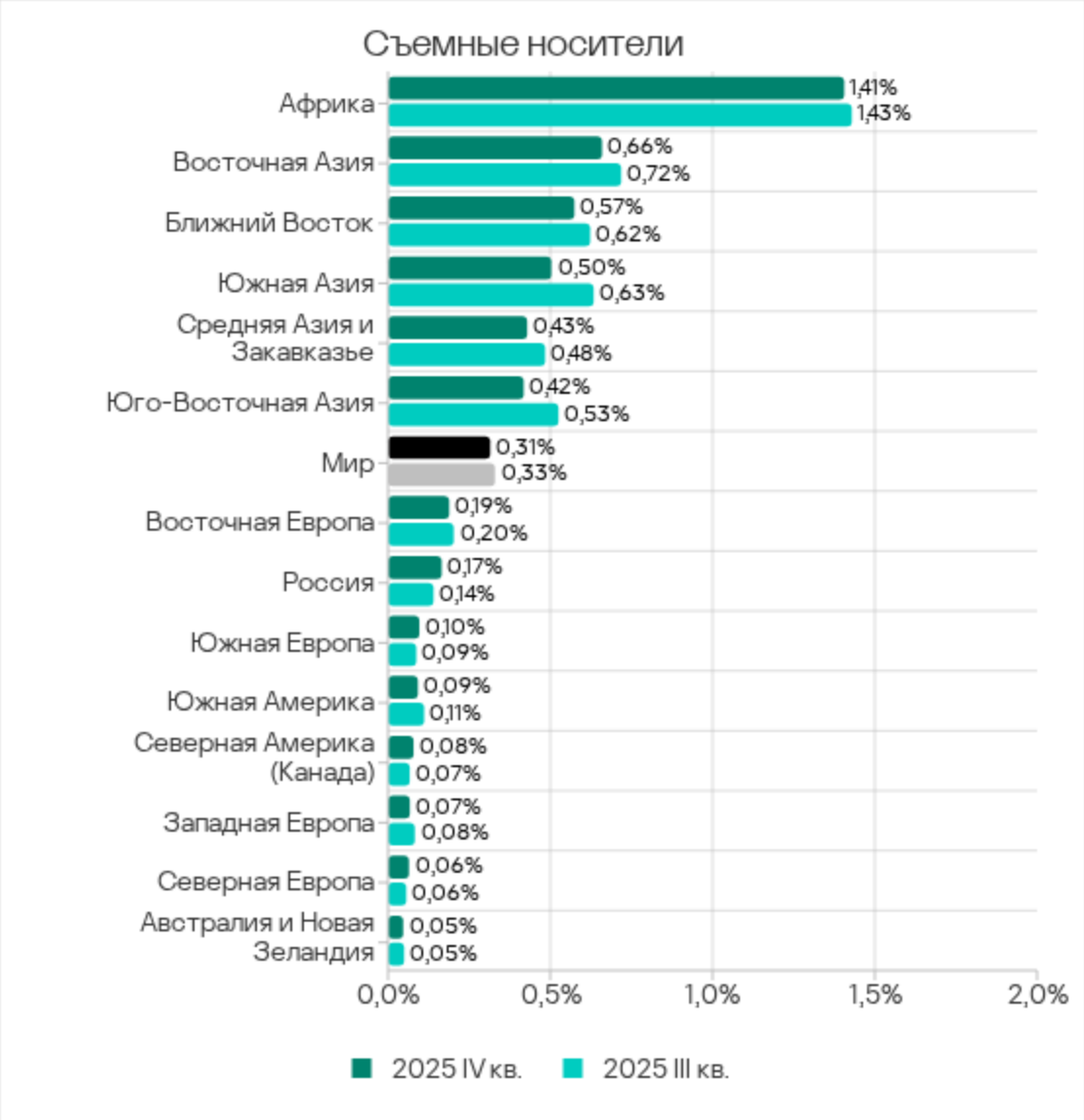


Доля червей, источником которых стали почтовые клиенты, в четвертом квартале 2025 года заметно выросла. Это обусловлено очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, в ходе которых жертвам рассылались фишинговые письма с вредоносным вложением (червь-бэкдор Backdoor.MSIL.XWorm), замаскированным под резюме. Пик атак в Африке пришелся на ноябрь.

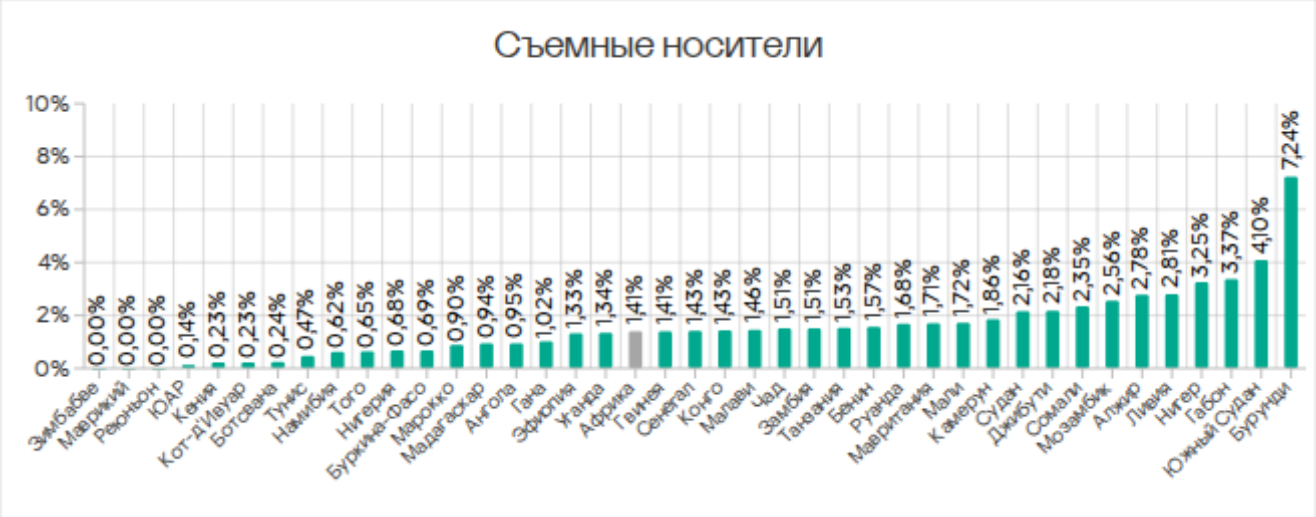
Хотя основным каналом распространения зловреда была электронная почта, в Африке, где по-прежнему активно используются USB-носители, угроза была обнаружена и при подключении к компьютерам АСУ съемных устройств.

Съемные носители

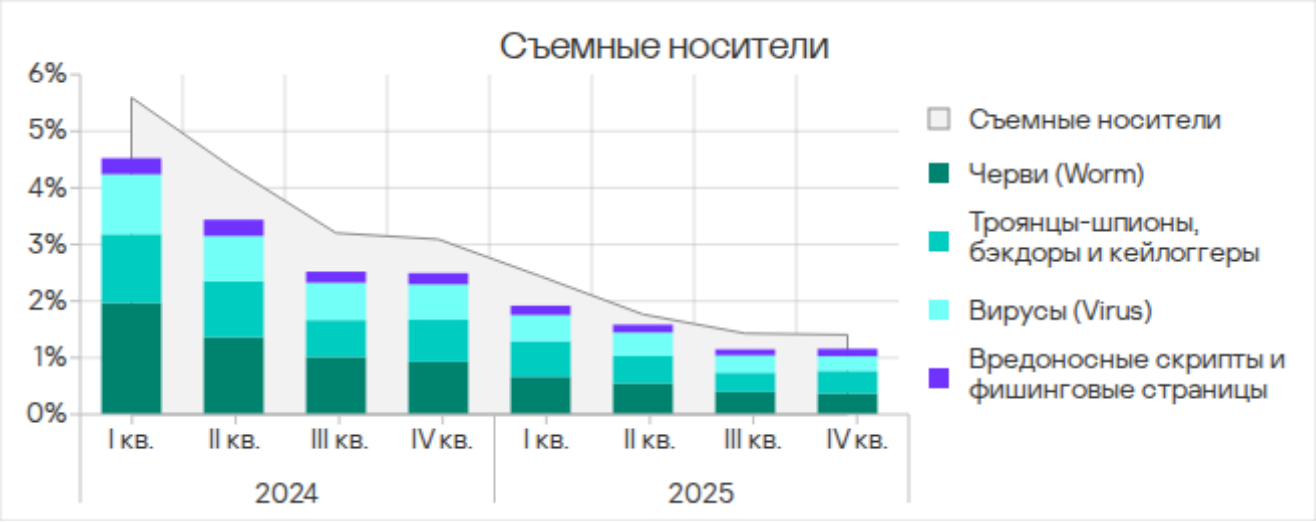
Несмотря на явный тренд к снижению доли компьютеров АСУ, на которых были заблокированы угрозы со съемных носителей, по этому показателю Африка по-прежнему с большим отрывом лидирует среди регионов с 1,41%. Показатель Африки превышает показатель региона Австралия и Новая Зеландия, который занимает последнее место в соответствующем рейтинге, в 28,2 раза.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с большим отрывом лидирует Бурунди с 7,24%. Показатели остальных стран варьируют от 0,14% в ЮАР до 3,37% в Габоне.

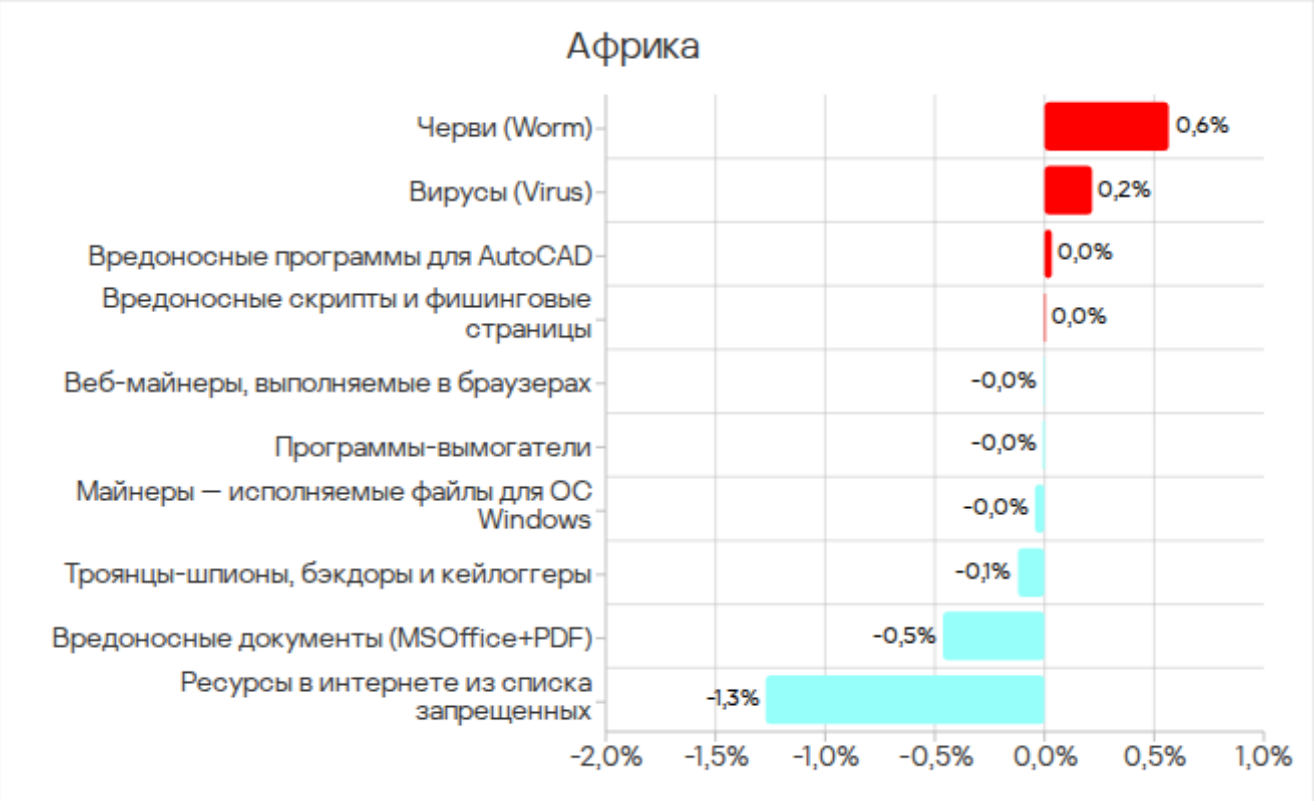


Основные категории угроз, которые в четвертом квартале 2025 года были заблокированы при подключении съемных носителей к компьютерам АСУ: шпионское ПО, черви и вирусы. По доле компьютеров АСУ, на которых блокировались шпионские программы и черви, Африка также лидирует среди регионов, в рейтинге по вирусам она находится на втором месте.



Категории угроз

В Африке у всех категорий угроз, кроме майнеров в формате исполняемых файлов для ОС Windows, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения.



Наиболее значимая разница региональных показателей со среднемировыми — у следующих категорий угроз:

- вирусы — в Африке показатель в 2,8 раза выше;
- черви — в 2,3 раза;
- программы-вымогатели — в 1,8 раза;
- шпионские программы — в 1,6 раза.

Среди регионов в четвертом квартале 2025 года Африка лидирует в рейтингах по доле компьютеров АСУ, на которых были заблокированы шпионские программы и черви.

По показателю вирусов и программ-вымогателей регион в соответствующих рейтингах находится на втором месте.

За квартал показатели выросли у самораспространяющегося вредоносного ПО (черви и вирусы), вредоносных программ для AutoCAD и немного у категории «Вредоносные скрипты и фишинговые страницы».

В рейтинге по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Африка сместилась с первого на второе место. Этот показатель в четвертом квартале 2025 года продолжил уменьшаться во всех регионах, и по его снижению Африка тоже заняла второе место.

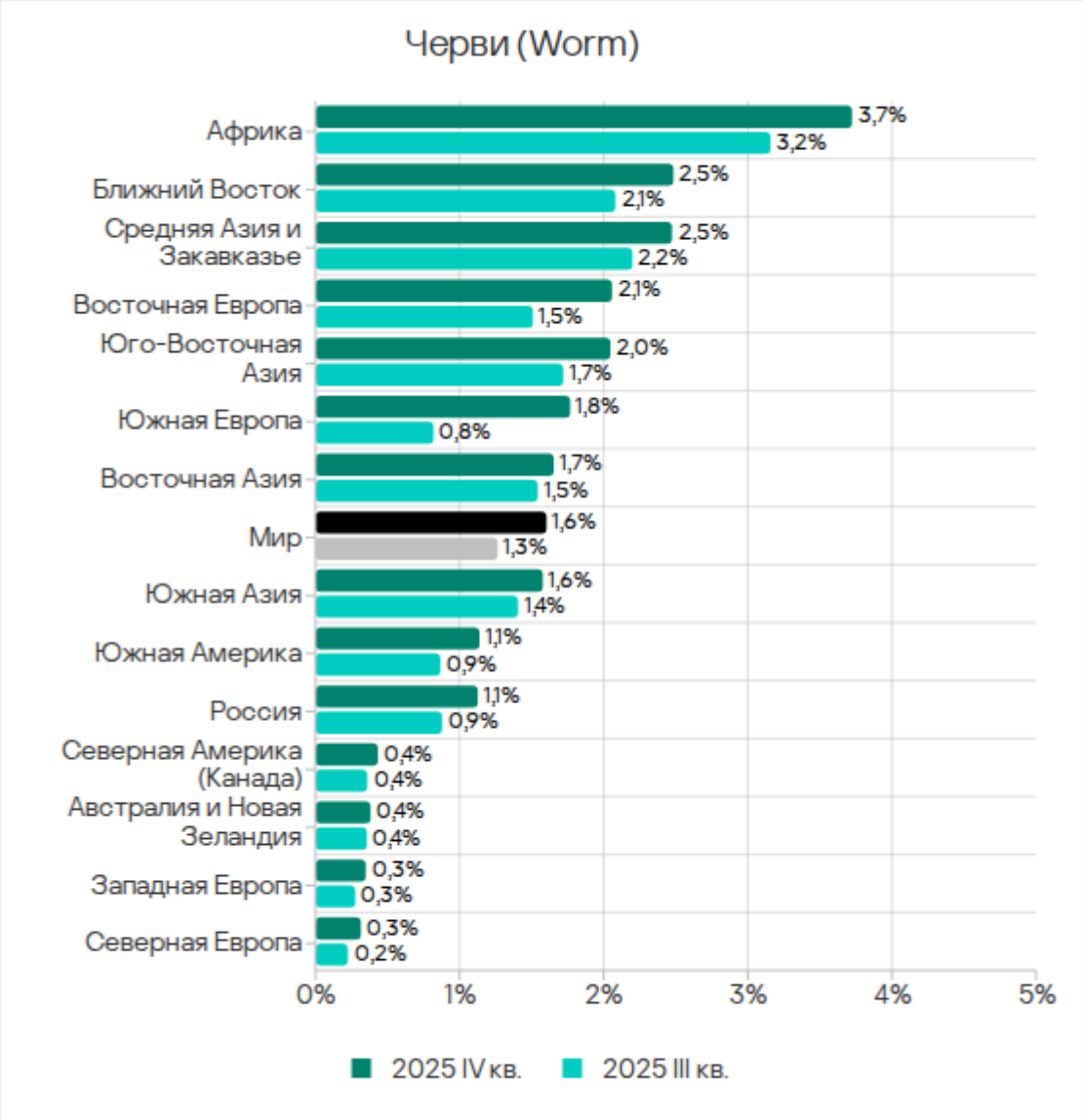
Самораспространяющееся вредоносное ПО: черви и вирусы

Черви и вирусы — основные категории угроз, которые блокируются при подключении к компьютерам АСУ съемных носителей. Учитывая постоянное лидерство Африки в рейтинге по этому источнику угроз, неудивительно, что и черви, и вирусы в Африке распространяются активнее, чем в других регионах.

Показатели червей в 2022–2023 годах были выше, чем у вирусов, но с четвертого квартала 2024 года доля компьютеров АСУ, на которых блокируются вирусы, чуть выше показателей червей.

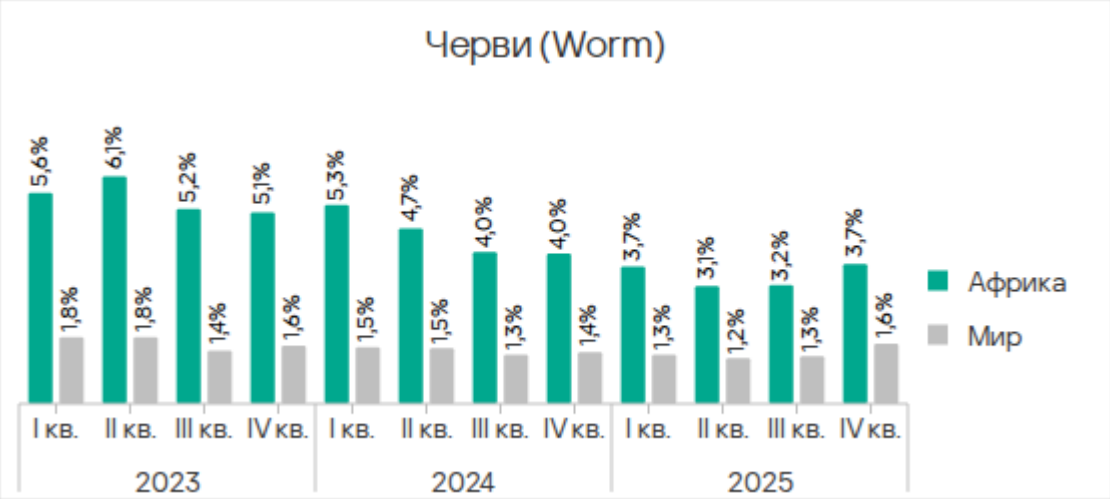
Черви

Африка — неизменный лидер среди регионов по доле компьютеров АСУ, на которых блокируются черви. Как и доля угроз со съемных носителей, показатель червей постепенно снижается. Несмотря на это, он по-прежнему значительно выше, чем в остальных регионах.

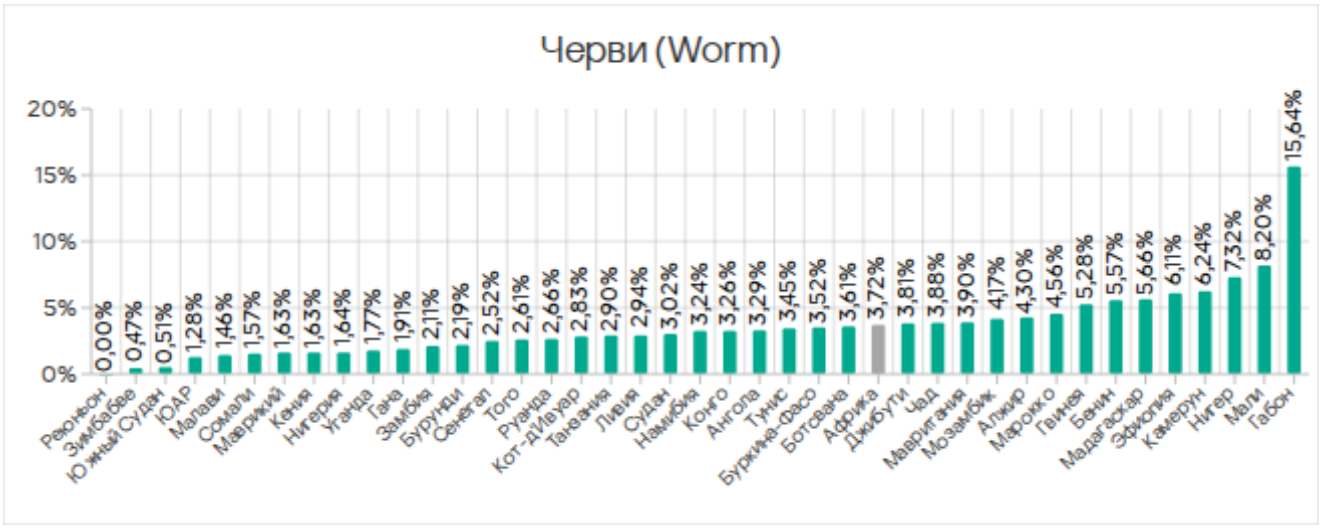


В четвертом квартале 2025 года в Африке доля компьютеров АСУ, на которых блокируются черви, выросла до 3,72%. По сравнению с Северной Европой, которая замыкает соответствующий рейтинг регионов, значение выше в 11,6 раза.

Отметим, что показатель червей вырос во всех регионах вследствие роста количества фишинговых атак, направленных на доставку вредоносного ПО Backdoor.MSIL.XWorm. По росту доли компьютеров АСУ, на которых блокировались черви, Африка занимает второе место среди регионов.



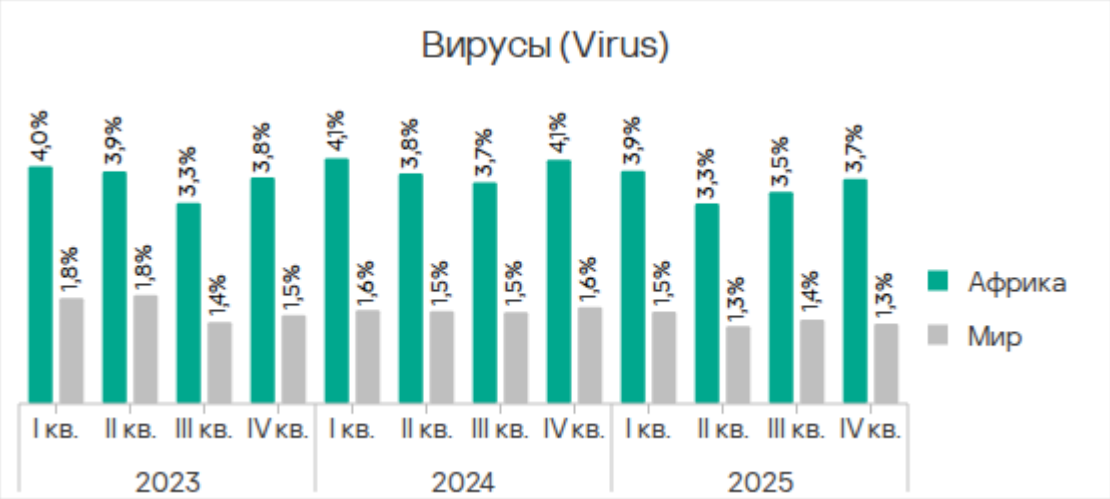
В странах региона по доле компьютеров АСУ, на которых блокируются черви, с большим отрывом лидирует Габон с аномально высоким показателем 15,64%. Это значение в 1,9 раза больше, чем у следующей страны в рейтинге — Мали (8,20%). Наименьший показатель — в Зимбабве (0,47%).



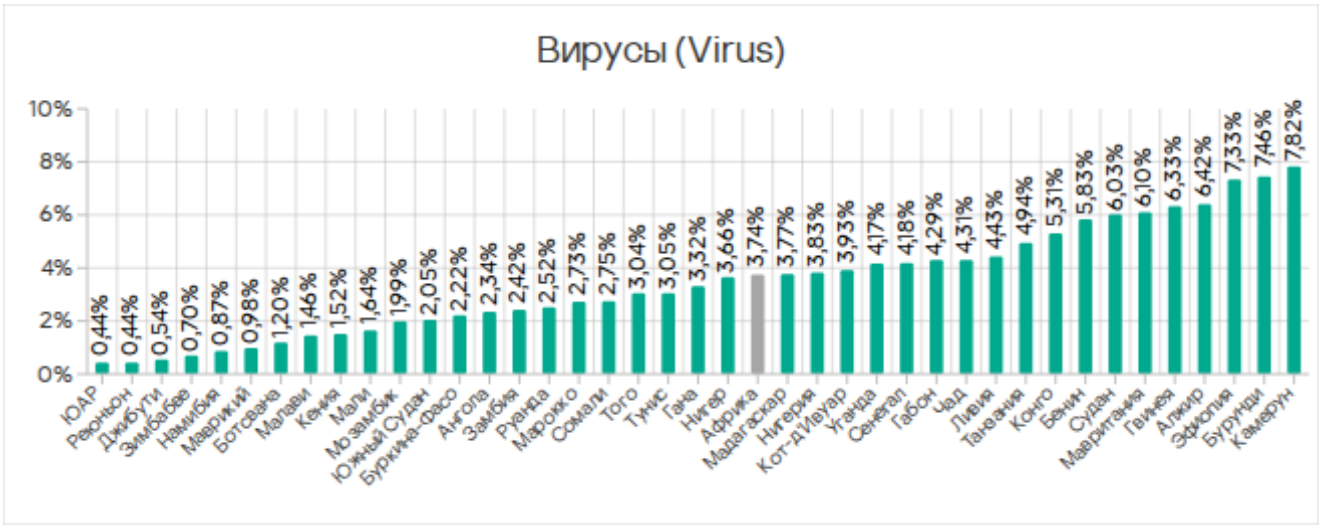
Вирусы

По доле компьютеров АСУ, на которых блокируются вирусы, Африка среди регионов занимает второе место с 3,74%. Это в 24,9 раза больше, чем в Западной Европе, которая замыкает соответствующий рейтинг.

В четвертом квартале 2025 года этот показатель в регионе вырос, и по его росту Африка лидирует среди регионов.



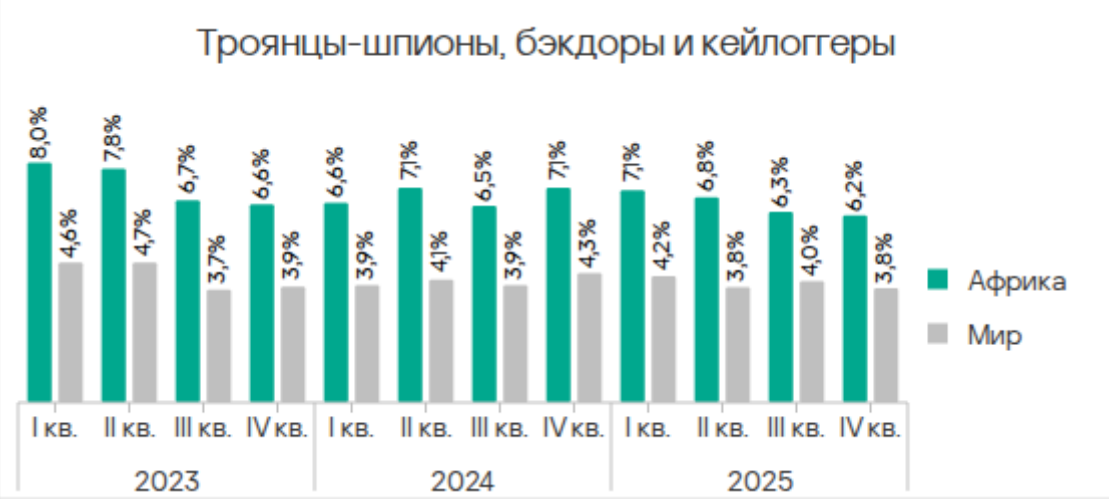
Среди стран Африки по доле компьютеров АСУ, на которых блокируются вирусы, лидирует Камерун с 7,82%. Наименьший показатель — в ЮАР (0,44%).



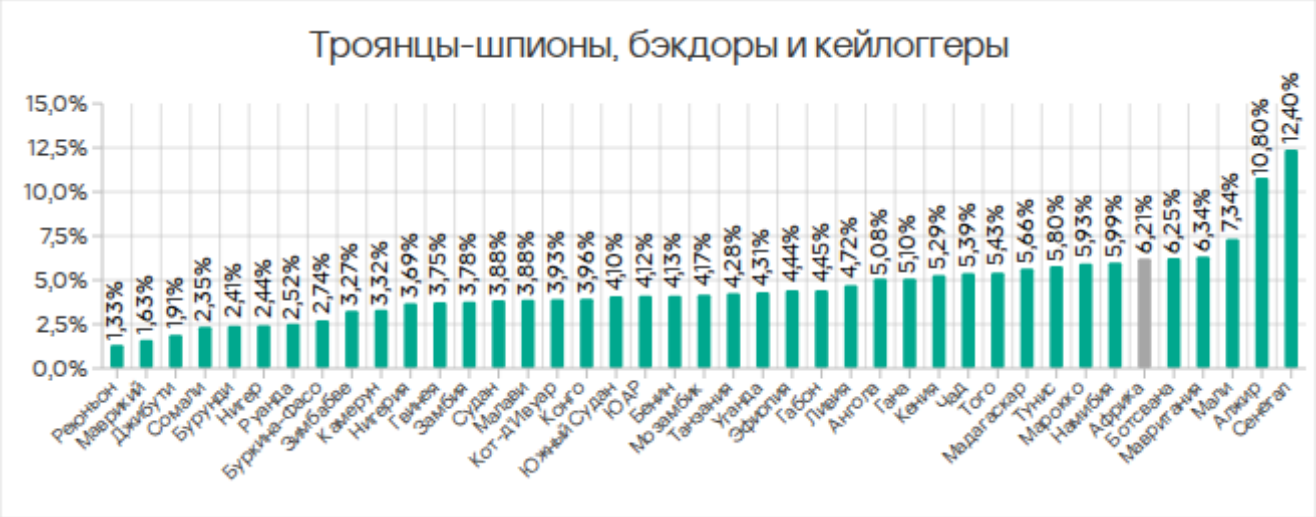
Шпионские программы

Африка устойчиво лидирует среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-шпионы.

Показатель в Африке уменьшается четвертый квартал подряд. В четвертом квартале 2025 года он снизился до 6,21%. Это в 5,0 раза больше, чем в Северной Европе, где значение наименьшее среди регионов.



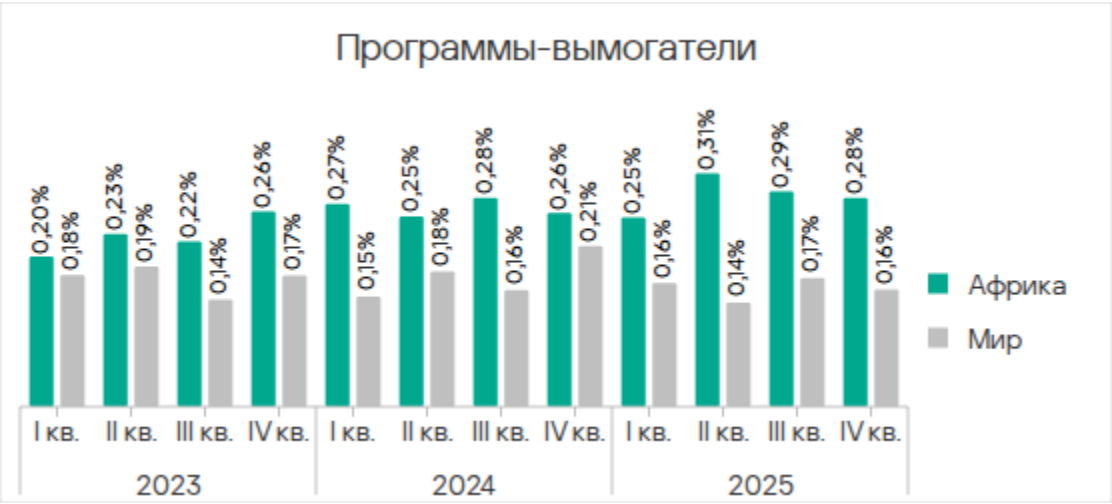
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы программы-шпионы, с отрывом лидируют Сенегал с 12,40% и Алжир с 10,8%. Наименьший показатель — на Маврикии (1,63%).



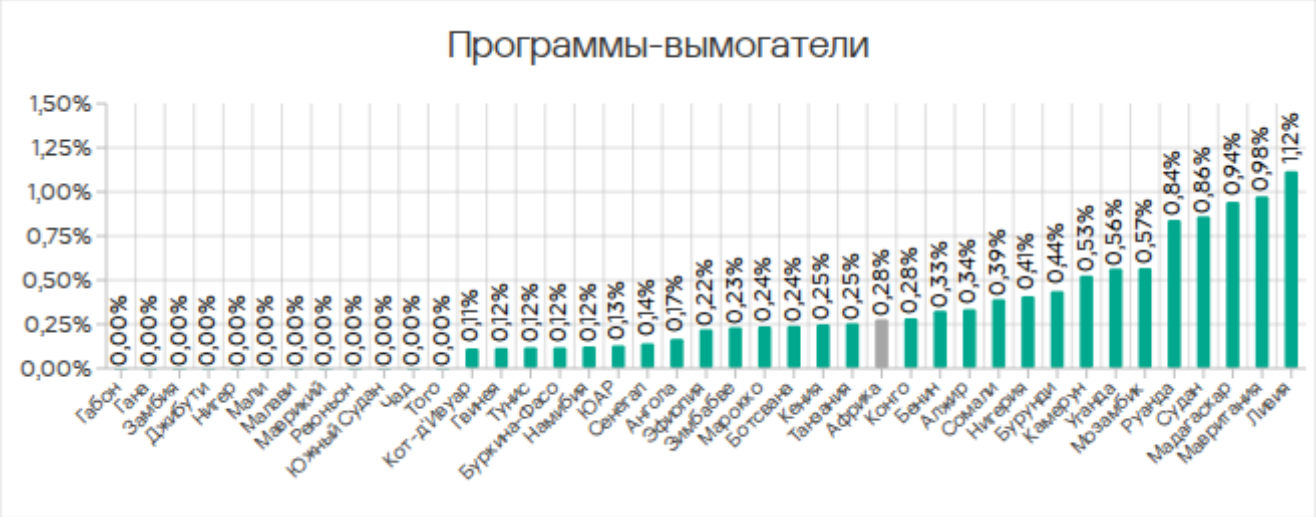
Программы-вымогатели

В четвертом квартале 2025 года Африка занимает второе место среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели с 0,28%. Это в 5,6 раза больше доли региона с минимальным значением — Северной Европы.

Показатель снижается второй квартал подряд.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, лидирует Ливия с 1,12%.

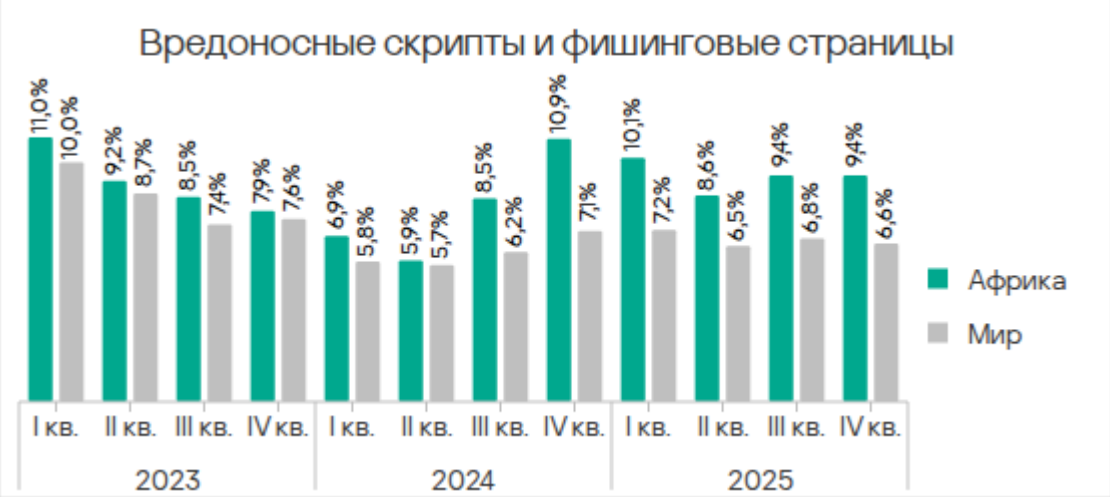


Отметим, что эта угроза в четвертом квартале 2025 года была обнаружена не во всех странах региона.

Вредоносные скрипты и фишинговые страницы

В третьем квартале 2025 года Африка поднялась с четвертого на первое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы. В четвертом квартале показатель чуть подрос — с 9,41% до 9,42%, но при этом Африка оказалась на третьем месте в этом рейтинге.

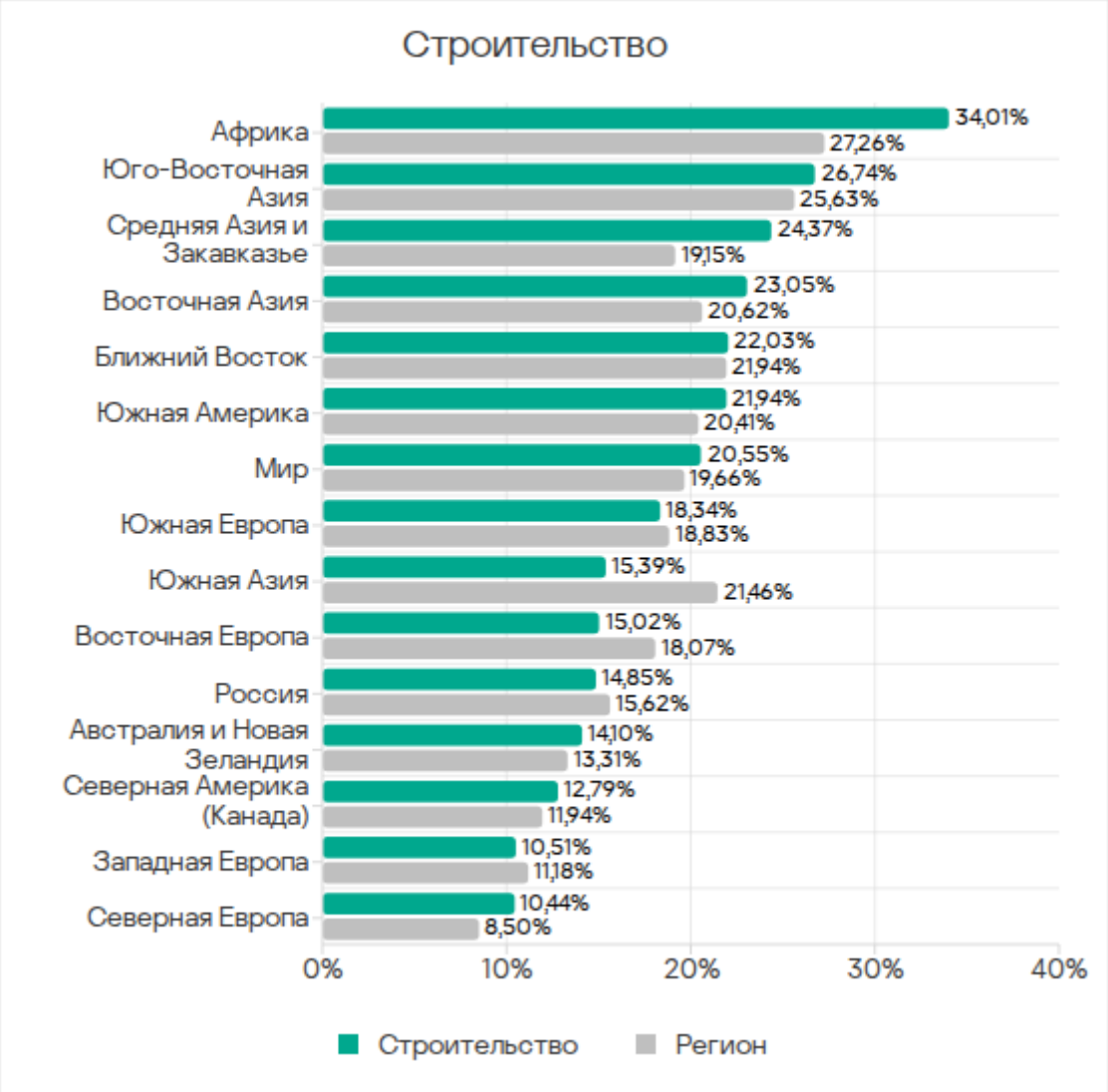
Значение в Африке в 1,4 раза выше среднемирового и в 3,7 раза больше, чем в Северной Европе, которая замыкает рейтинг.



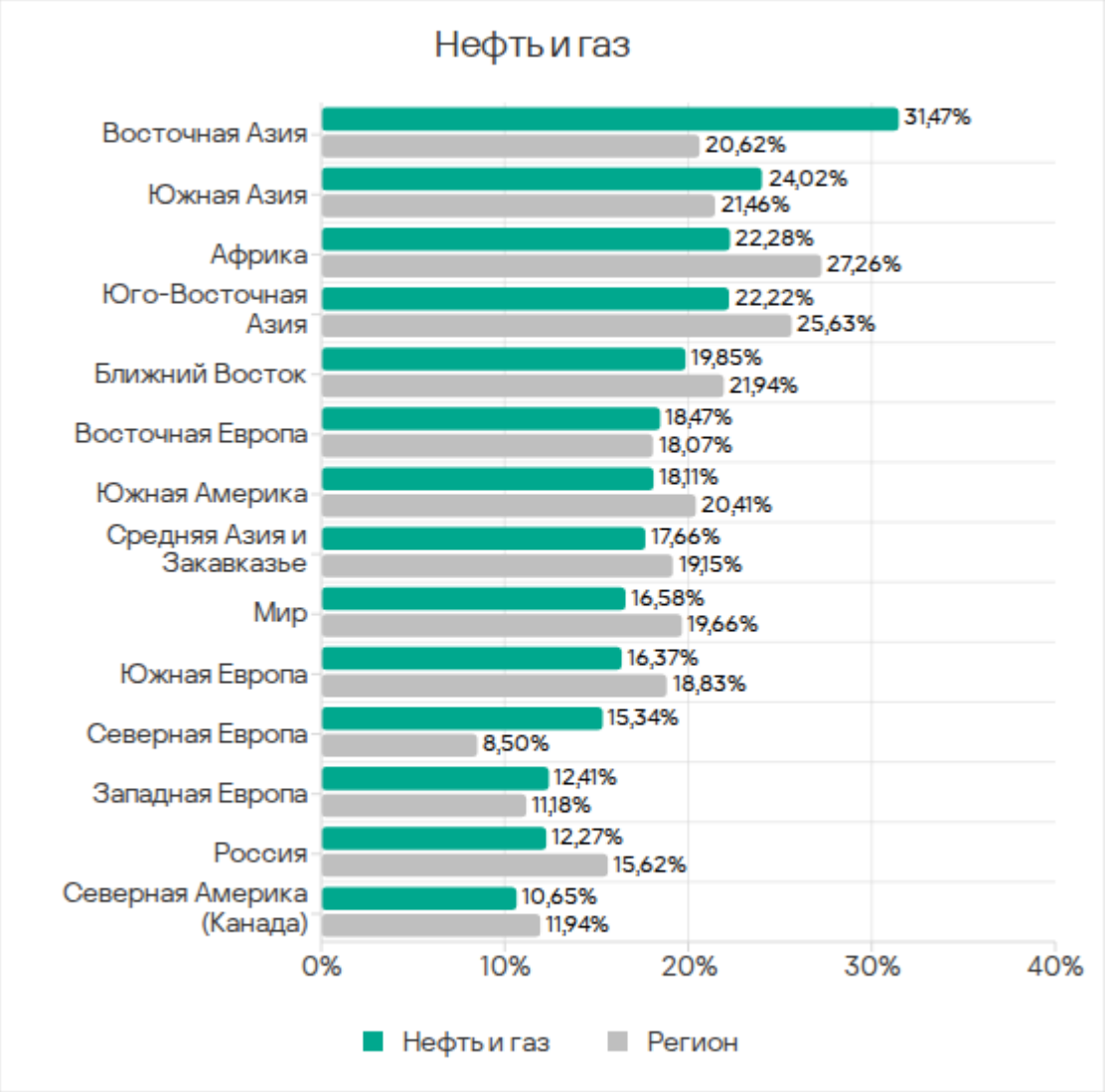
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Мозамбик с 12,61%. Наименьший показатель — в Буркина-Фасо (3,10%).

Отрасли

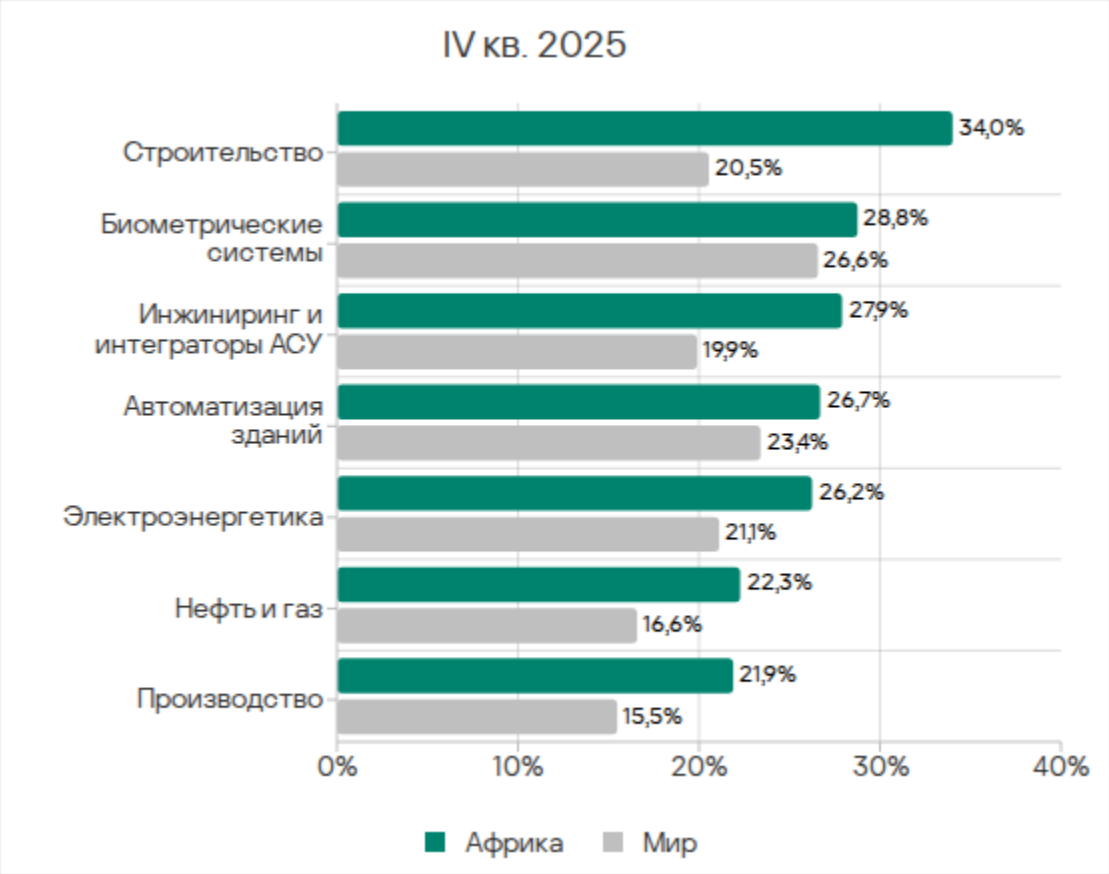
В Африке наиболее часто встречающейся с угрозами отраслью среди рассмотренных в отчете по-прежнему является строительство. По доле компьютеров АСУ, на которых в этой отрасли были заблокированы вредоносные объекты, Африка лидирует среди регионов.



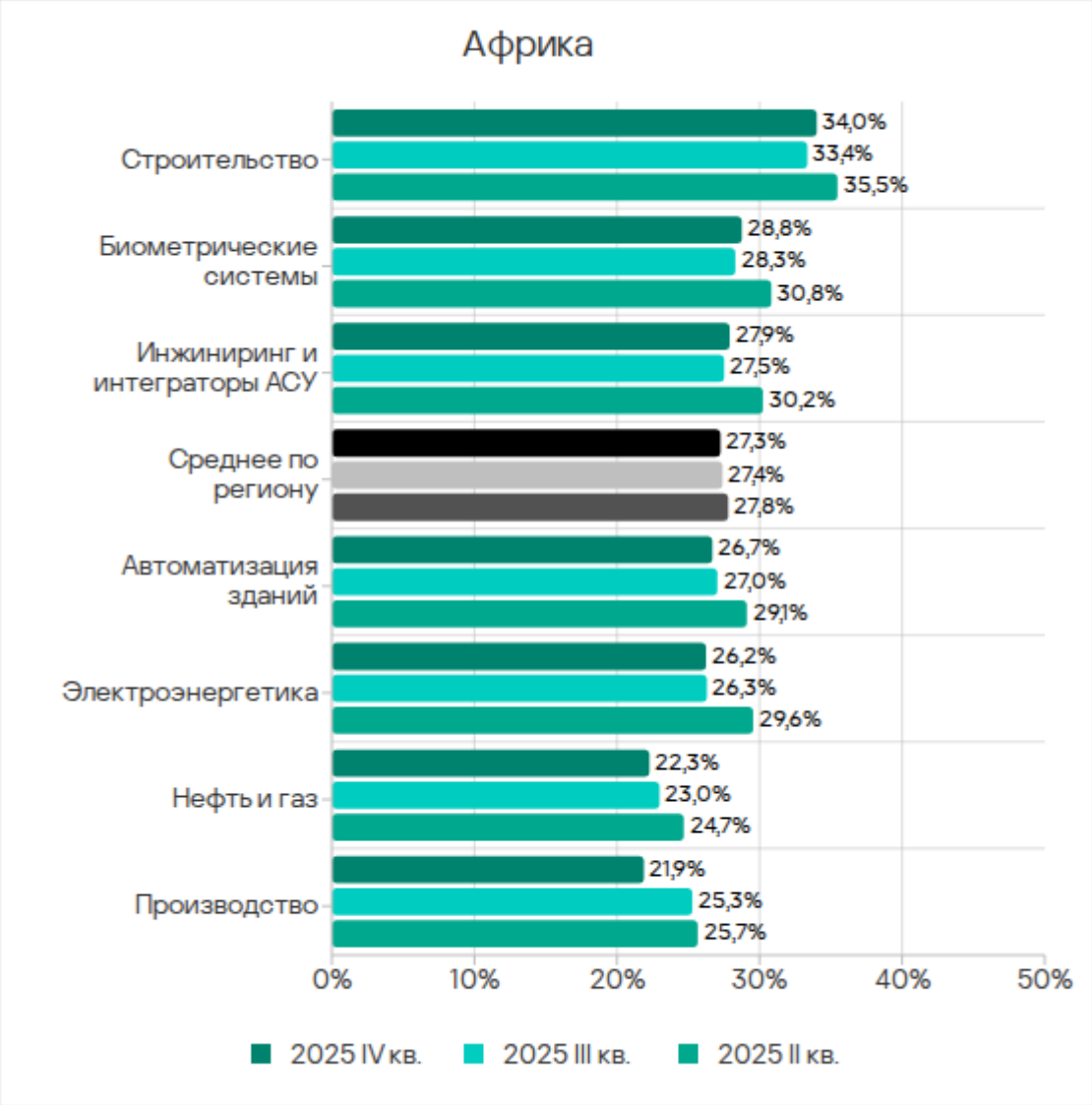
Африка также лидирует среди регионов по показателям отрасли инжиниринг и интеграторы АСУ, а также нефтегазовой отрасли.



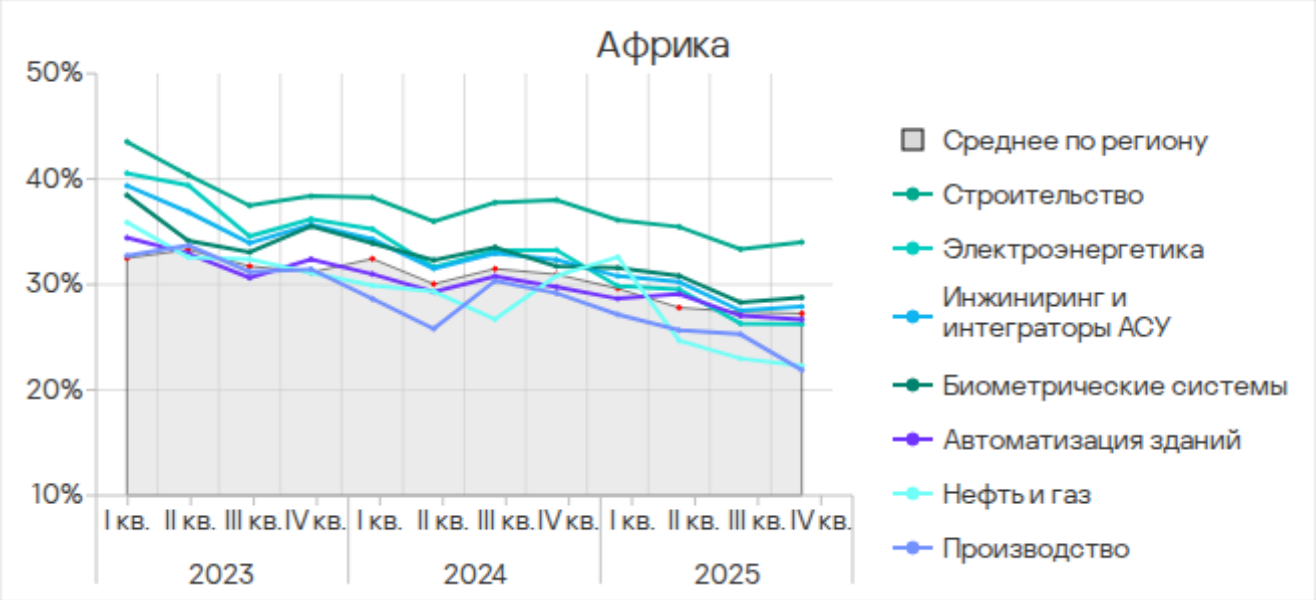
Показатели всех отраслей в регионе превышают аналогичные среднемировые. Больше всего разница у строительной (в 1,6 раза), производственной и нефтегазовой отраслей (в 1,5 раза каждая).



За квартал увеличились показатели трех отраслей: строительство, биометрические системы, инжиниринг и интеграторы АСУ.



Все рассмотренные отрасли демонстрируют положительную динамику долгосрочных трендов (показатели снижаются) с периодическими значительными колебаниями.



Источники и категории вредоносного ПО в отраслях: «горячие точки»

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

Показатели источников угроз в отраслях в Африке, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	9,18%	8,47%	11,00%	9,65%	8,56%	12,02%	8,83%	9,12%
Почтовые клиенты	6,00%	7,12%	2,65%	2,37%	0,29%	3,35%	3,06%	4,17%
Съемные носители	1,49%	1,00%	1,53%	1,79%	1,36%	1,34%	0,36%	1,41%
Сетевые папки	0,10%	0,03%	0,02%	0,03%	—	0,03%	—	0,03%
Показатель отрасли в регионе	28,76%	26,69%	27,91%	26,25%	22,28%	34,01%	21,89%	

Показатели категорий угроз в отраслях в Африке, IV квартал 2025 года

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	3,25%	3,11%	4,52%	4,41%	4,18%	4,93%	3,96%	3,69%
Вредоносные скрипты и фишинговые страницы	11,00%	11,46%	9,54%	8,06%	6,61%	10,34%	7,75%	9,42%
Вредоносные документы (MSOffice+PDF)	3,36%	3,60%	1,63%	1,81%	0,68%	2,16%	1,35%	2,25%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,10%	6,25%	5,97%	6,28%	5,64%	9,31%	3,60%	6,21%
Программы-вымогатели	0,35%	0,31%	0,29%	0,42%	0,49%	0,43%	0,27%	0,28%
Майнеры — исполняемые файлы для ОС Windows	0,66%	0,44%	0,61%	0,47%	0,29%	0,88%	0,36%	0,47%
Веб-майнеры, выполняемые в браузерах	0,45%	0,29%	0,25%	0,22%	0,10%	0,33%	0,18%	0,26%
Вредоносные программы для AutoCAD	0,18%	0,13%	0,34%	0,39%	0,88%	2,43%	0,18%	0,44%
Черви (Worm)	4,74%	3,65%	3,50%	3,82%	3,31%	3,50%	2,79%	3,72%
Вирусы (Virus)	3,91%	2,93%	3,77%	4,30%	3,79%	6,60%	2,88%	3,74%
Показатель отрасли в регионе	28,76%	26,69%	27,91%	26,25%	22,28%	34,01%	21,89%	

Строительство

Африка находится на первом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

В глобальном рейтинге среди всех индустрий во всех регионах строительный сектор в Африке занимает:

- второе место по доле компьютеров, на которых были заблокированы черви.

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, и второе – по показателю угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются угрозы следующих категорий: вредоносные скрипты и фишинговые страницы, шпионские программы, черви;
- второе место по показателям категорий ресурсы в интернете из списка запрещенных, программы-вымогатели, вирусы;
- третье место по показателю вредоносных программ для AutoCAD.

Среди отраслей в регионе строительство занимает:

- первое место по показателю угроз из интернета, третье место — по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов и в сетевых папках;
- первое место по показателям многих категорий угроз: ресурсы в интернете из списка запрещенных, шпионские программы, вирусы, вредоносные программы для AutoCAD, майнеры – исполняемые файлы для ОС Windows;
- второе место по показателю веб-майнеров и программ-вымогателей;
- третье место по показателю категорий вредоносные скрипты и фишинговые страницы и вредоносные документы.

Биометрические системы

Африка находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

В глобальном рейтинге среди всех индустрий во всех регионах биометрические системы в Африке занимают:

- третье место по доле компьютеров, на которых были заблокированы черви.

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, и второе — по показателям угроз из интернета и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются вирусы и черви;
- второе место по показателю шпионских программ;

- третье место по показателю ресурсов в интернете из списка запрещенных.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

- первое место по показателю угроз в сетевых папках, второе – по доле компьютеров АСУ, на которых угрозы блокируются в почтовых клиентах и третье — при подключении съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются веб-майнеры и черви;
- второе место по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, майнеры в формате исполняемых файлов;
- третье место по показателю вирусов.

Инжиниринг и интеграторы АСУ

Африка находится на первом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, и второе — по показателю угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, шпионские программы, программы-вымогатели, вирусы и черви;
- второе место по показателю категории вредоносные скрипты и фишинговые страницы,
- третье место по показателю майнеров в формате – исполняемых файлов для ОС Windows.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и при подключении съемных носителей;
- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных;
- третье место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows.

Автоматизация зданий

Африка находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей;
- второе место по доле компьютеров АСУ в отрасли, на которых блокируются вирусы;
- третье место по показателю червей и веб-майнеров.

Среди отраслей в регионе автоматизация зданий занимает:

- первое место по показателю угроз из почтовых клиентов и второе – по показателю угроз в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются вредоносные документы, а также вредоносные скрипты и фишинговые страницы;
- третье место по доле компьютеров АСУ, на которых блокируются черви и веб-майнеры.

Электроэнергетика

Африка находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли электроэнергетика.

Среди регионов по показателям в отрасли Африка занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в интернете и при подключении съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются черви;
- второе место по показателям шпионских программ и программ-вымогателей;
- третье место по показателям категорий вредоносные скрипты и фишинговые страницы, вирусы и вредоносные программы для AutoCAD.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, третье место по показателю угроз из интернета;

- второе место по показателям червей и вирусов;
- третье место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, шпионские программы, программы-вымогатели, вредоносные программы для AutoCAD.

Производство

Африка находится на втором месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли производство.

Среди регионов по показателям в отрасли Африка занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и из почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и черви;
- второе место по показателю программ-вымогателей;
- третье место по показателю вредоносных скриптов и фишинговых страниц, шпионских программ и вирусов.

Нефтегазовая отрасль

Африка находится на первом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в нефтегазовой отрасли.

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей, и второе — по показателю угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются шпионские программы, программы-вымогатели, вирусы, черви, вредоносные программы для AutoCAD;
- на втором месте по показателям следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- первое место по доле компьютеров АСУ, на которых блокируются программы-вымогатели;
- второе место по показателю вредоносных программ для AutoCAD.

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