

Ландшафт угроз для систем промышленной автоматизации

Африка. Третий квартал 2025 года

Африка.....	3
Основные проблемы кибербезопасности в регионе	3
Статистика по всем угрозам.....	4
Источники угроз.....	6
Съемные носители	7
Интернет.....	9
Почтовые клиенты	11
Категории угроз	12
Самораспространяющееся вредоносное ПО: черви и вирусы	14
Шпионские программы	17
Программы-вымогатели.....	18
Вредоносные скрипты и фишинговые страницы	19
Ресурсы в интернете из списка запрещенных	21
Отрасли.....	23
Источники и категории вредоносного ПО в отраслях: «горячие точки»	26
Методика подготовки статистики	31

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, 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 третьем 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 третьем квартале 2025 года превышает аналогичный среднемировой показатель в 4,3 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

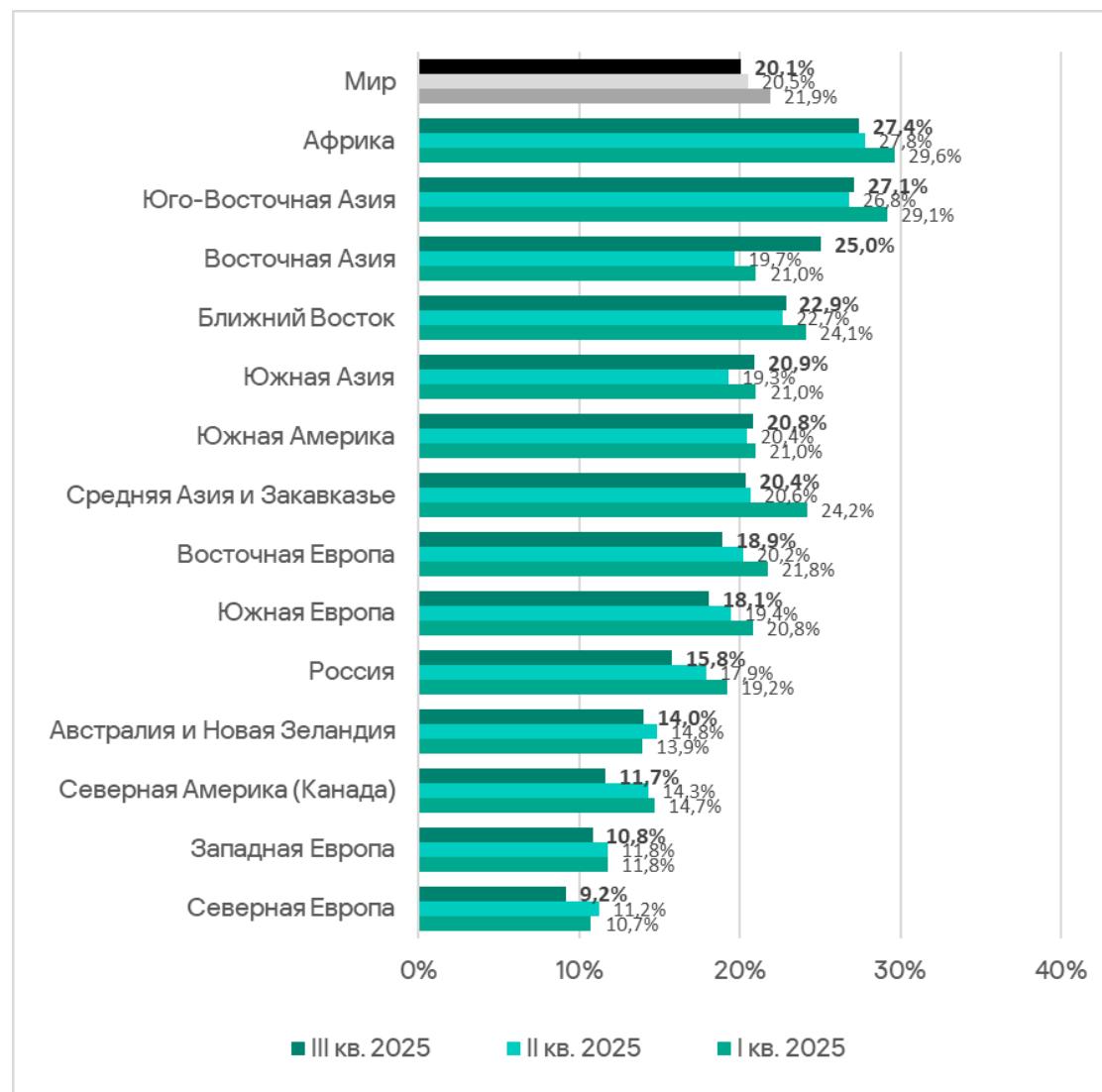
Один из общих выводов, которые можно сделать по итогам многолетних наблюдений за изменением показателей доступности ОТ-инфраструктур для угроз: скорость внедрения мер и средств кибербезопасности обычно уступает темпам развития отрасли. При введении объекта в эксплуатацию часто о его кибербезопасности 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.

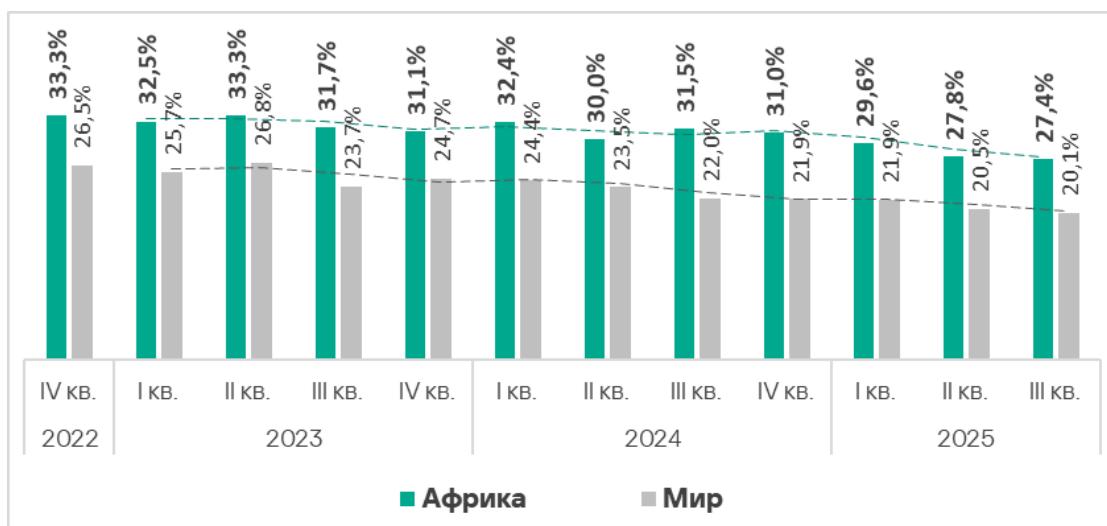
Статистика по всем угрозам

В третьем квартале 2025 года Африка по-прежнему лидирует в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Однако разрыв с Юго-Восточной Азией, которая занимает второе место в этом рейтинге, составляет всего лишь 0,3 п. п.

В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Африке еще немного уменьшилась – до 27,4%. Тем не менее, показатель Африки по-прежнему больше в 1,4 раза, чем среднемировое значение. А соотношение показателей Африки и Северной Европы, которая замыкает рейтинг, увеличилось с 2,5 до 3,0 раз.

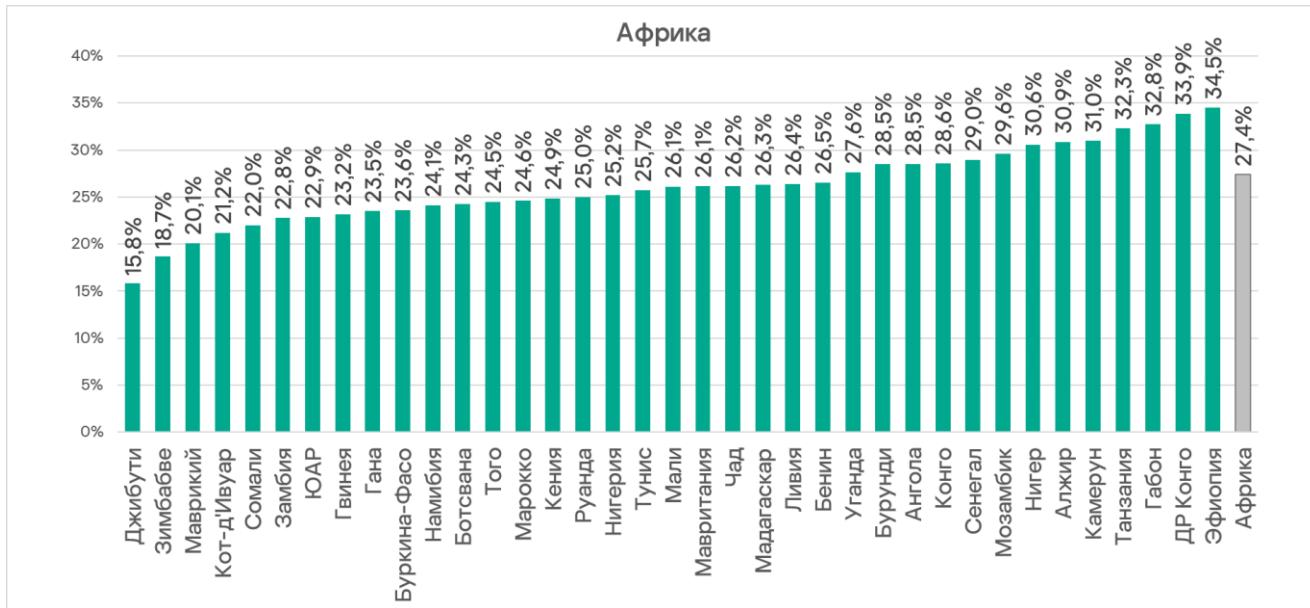


Показатель в регионе снижается четвертый квартал подряд.



В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 15,8% в Джибути до 34,5% в Эфиопии.

Ниже 20% показатель лишь в двух странах – Зимбабве и Джибути. В Нигере, Алжире, Камеруне, Танзании, Габоне, ДР Конго и Эфиопии он превышает 30%.



Источники угроз

В третьем квартале 2025 года значения по всем источникам угроз, кроме сетевых папок, в регионе превышают среднемировые. В случае съемных носителей это превышение весьма значительно – в 4,3 раз.

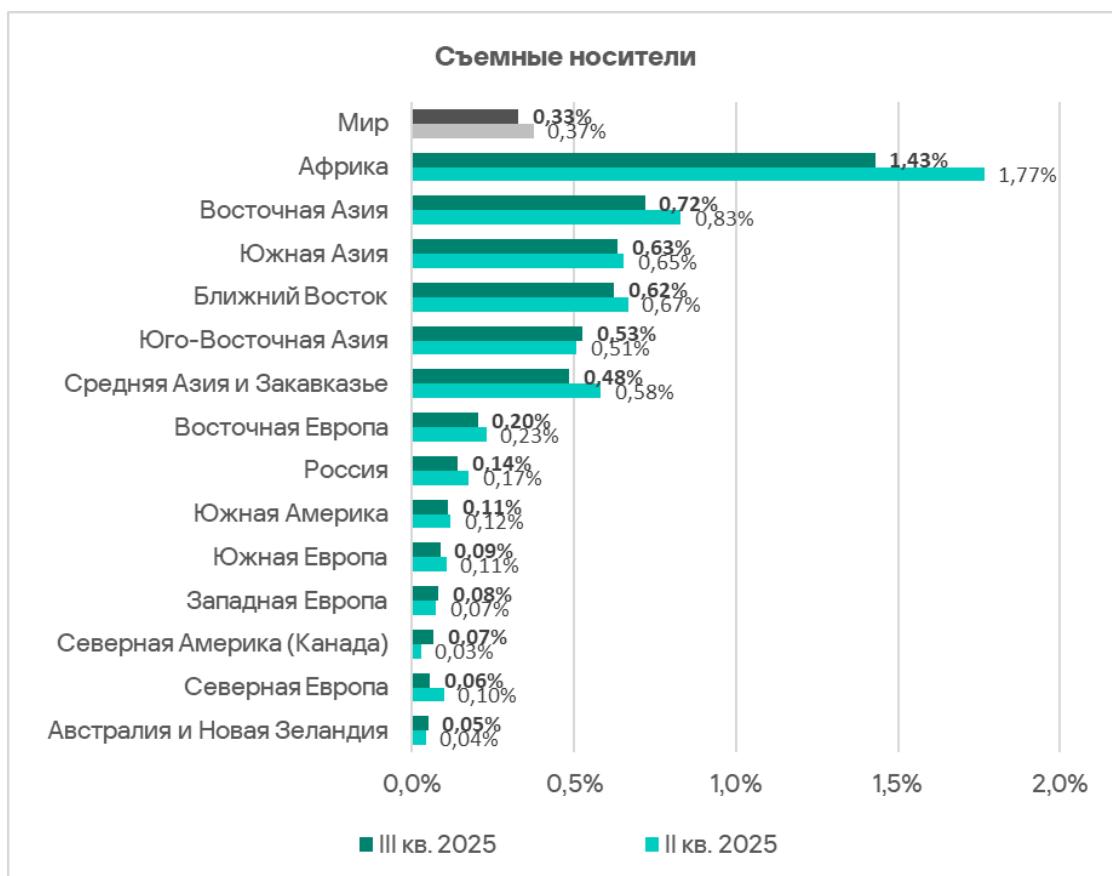


Показатели всех источников угроз за квартал уменьшились.



Съемные носители

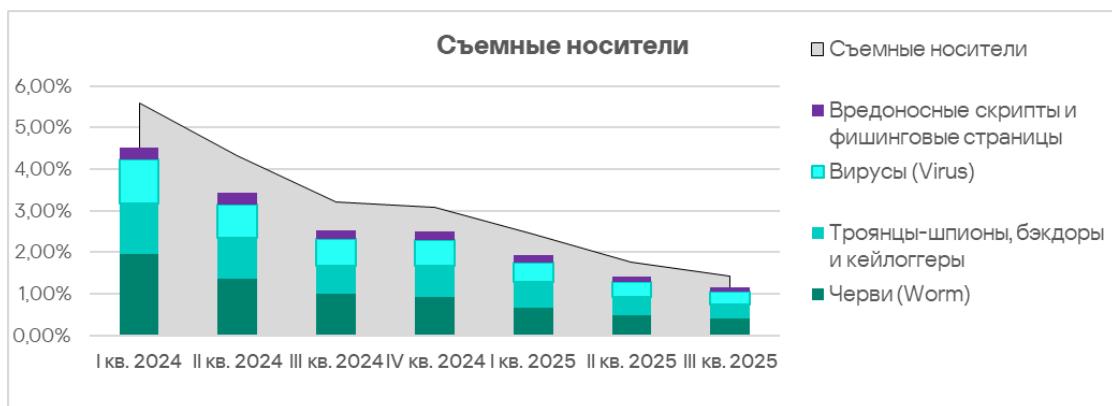
Несмотря на явный тренд к снижению доли компьютеров АСУ, на которых были заблокированы угрозы со съемных носителей, по этому показателю Африка по-прежнему с большим отрывом лидирует среди регионов. Показатель Африки (1,43%) превышает показатель региона Австралия и Новая Зеландия, который занимает последнее место в соответствующем рейтинге, в 28,6 раза.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с отрывом лидирует Бурунди с 4,68%. Показатели остальных стран варьируют от 0,22% в Того до 3,62% в Ливии.

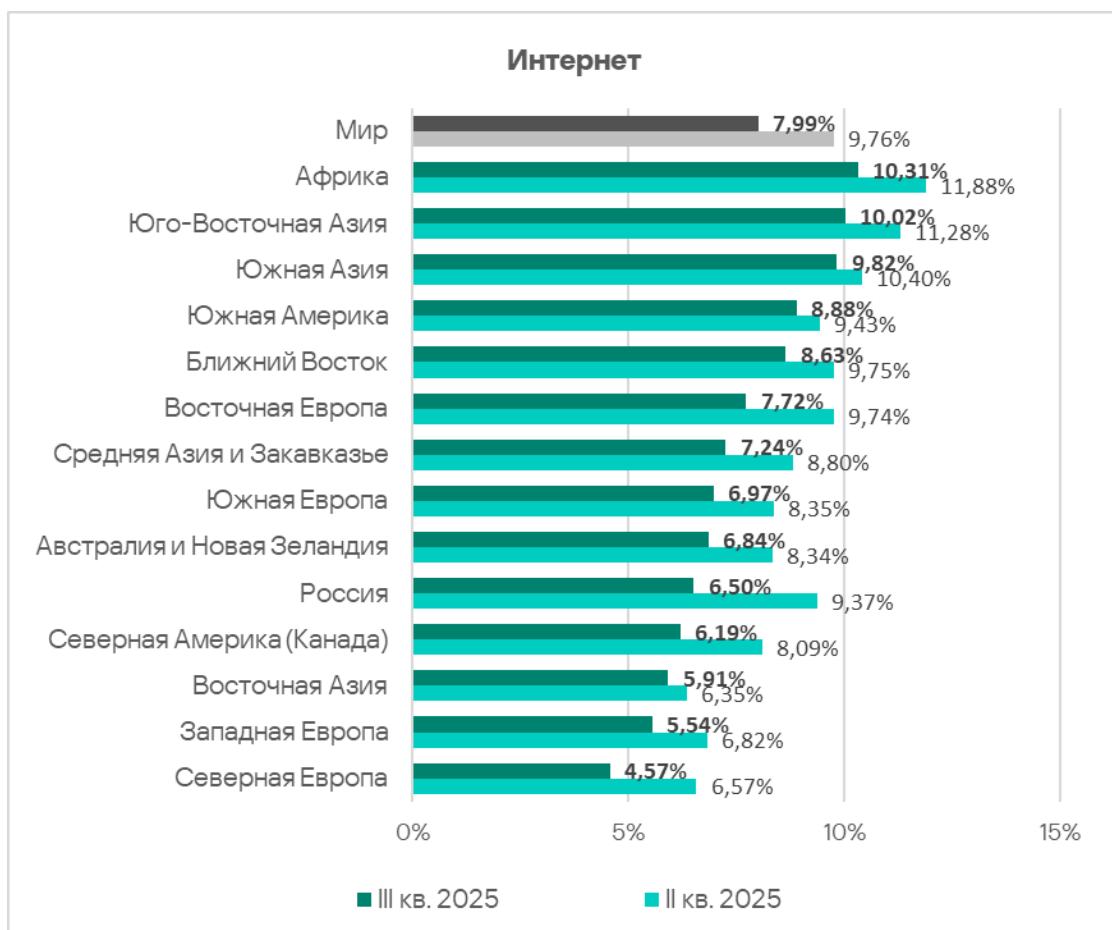


Основные категории угроз, которые в третьем квартале 2025 года были заблокированы при подключении съемных носителей к компьютерам АСУ, — черви, шпионское ПО, вирусы и вредоносные скрипты. По доле компьютеров АСУ, на которых блокировались эти категории угроз, Африка также лидирует среди регионов (по вирусам — на втором месте в рейтинге).

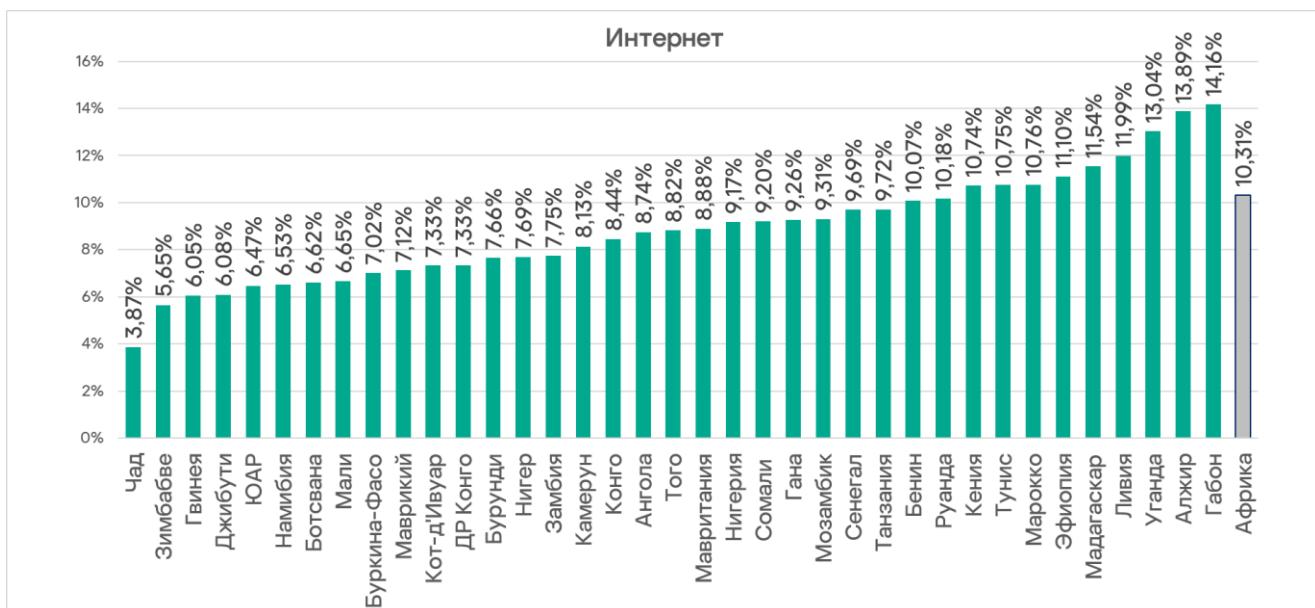


Интернет

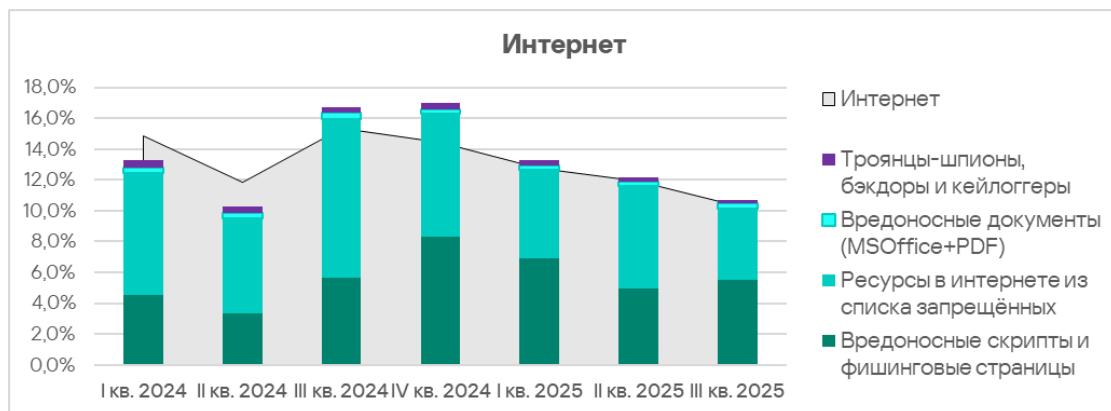
Еще один источник угроз, по которому Африка лидирует среди регионов, — интернет. В третьем квартале 2025 года по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, показатель Африки (10,31%) превышает показатель Северной Европы, которая занимает последнее место в соответствующем рейтинге, в 2,3 раза.



Среди стран региона по этому показателю лидирует Габон с 14,16%. Заметно меньше, чем в остальных странах, доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, в Чаде (3,87%).

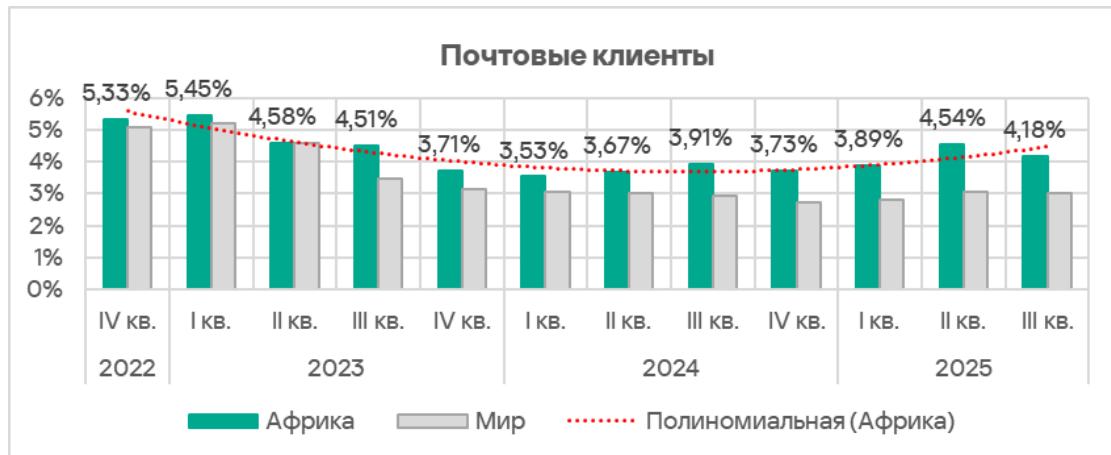


Основные категории угроз из интернета, которые в третьем квартале 2025 года были заблокированы на компьютерах АСУ, — это вредоносные скрипты и фишинговые страницы, интернет-ресурсы из списка запрещенных, вредоносные документы и шпионские программы.

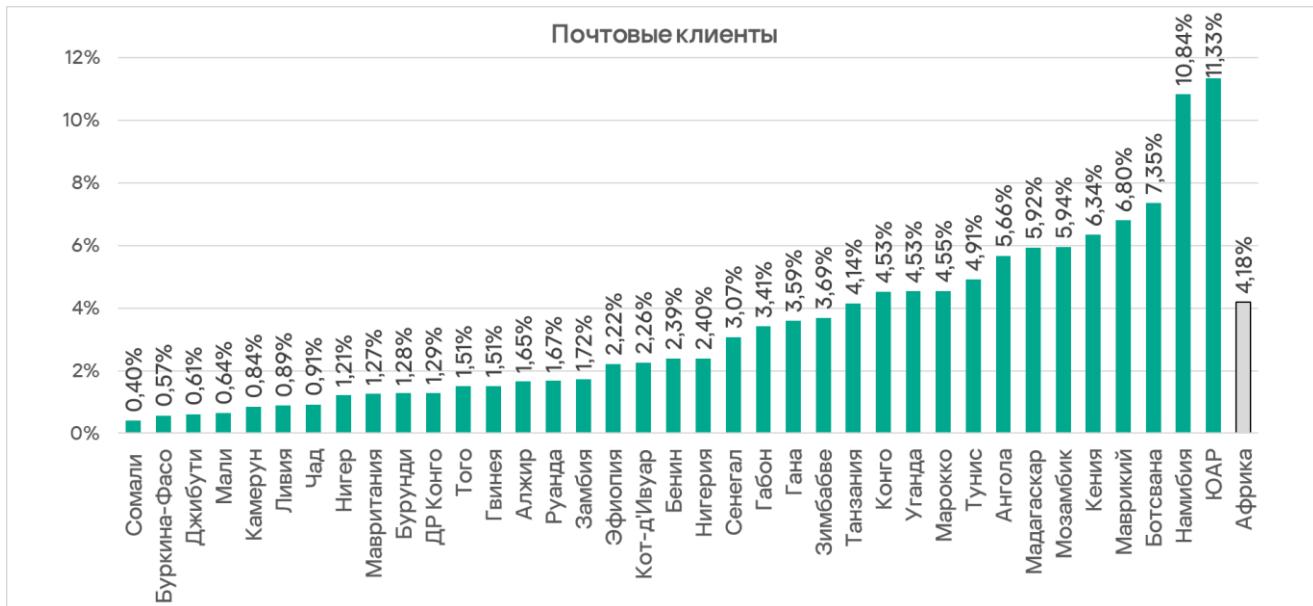


Почтовые клиенты

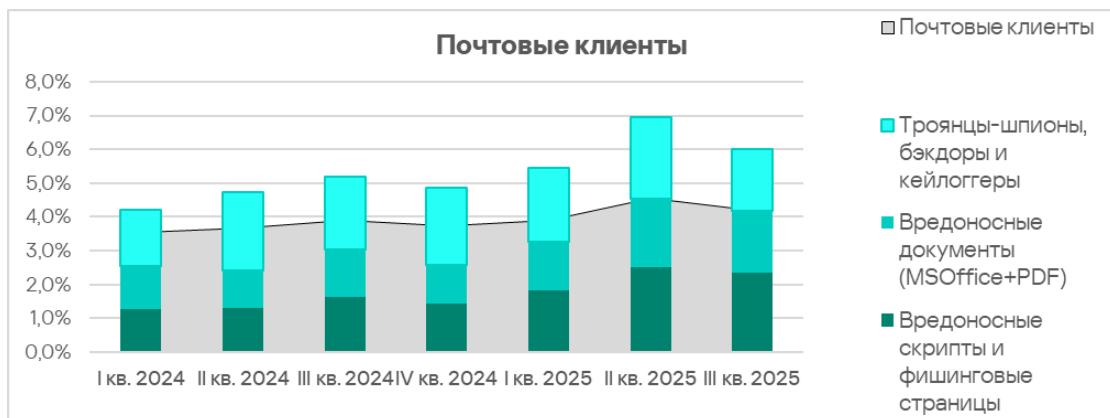
После роста в течение первых двух кварталов 2025 года, доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, в Африке снизилась. В соответствующем рейтинге регионов Африка находится на пятом месте с 4,18%. Это в 5,4 раза больше, чем в России, где показатель минимальный среди регионов.



Среди стран региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, явно лидируют ЮАР и Намибия с 11,33% и 10,84% соответственно. Минимальный показатель в Сомали — 0,4%.



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



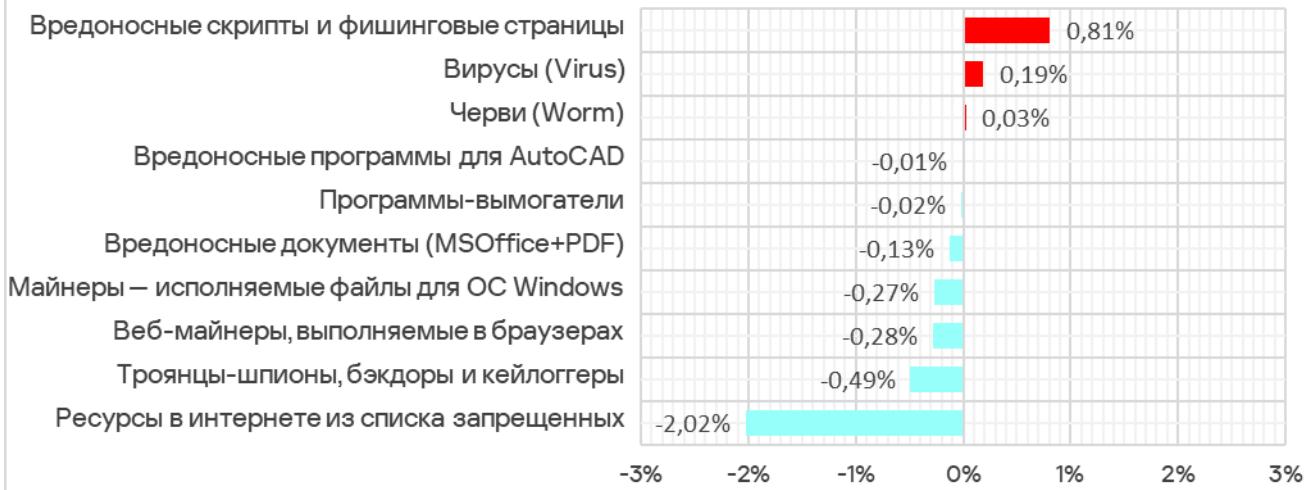
Категории угроз

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.

III квартал 2025



Африка, изменения за квартал



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

- вирусы – в Африке показатель в 2,5 раза выше;
- черви – в 2,5 раза;
- шпионские программы – в 1,6 раза.

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

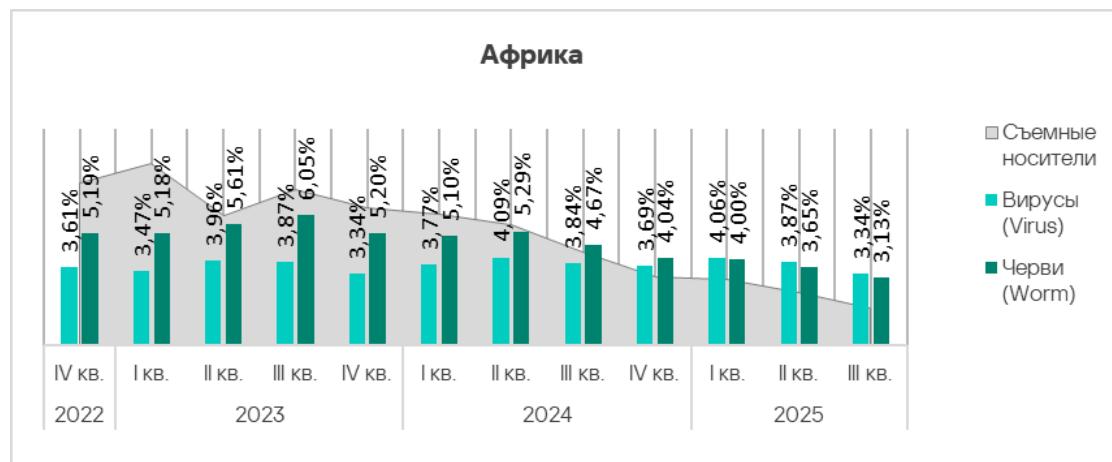
- вредоносные скрипты и фишинговые страницы (JS и HTML), причем Африка поднялась в рейтинге с четвертого на первое место;
- ресурсы в интернете из списка запрещенных;
- шпионские программы;
- черви.

По показателю вирусов и программ-вымогателей регион на втором месте в рейтинге.

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.

Показатель червей, как и доля угроз со съемных носителей в целом, постепенно снижается. У вирусов более сложная динамика, однако в последние два квартала мы также отмечаем снижение.

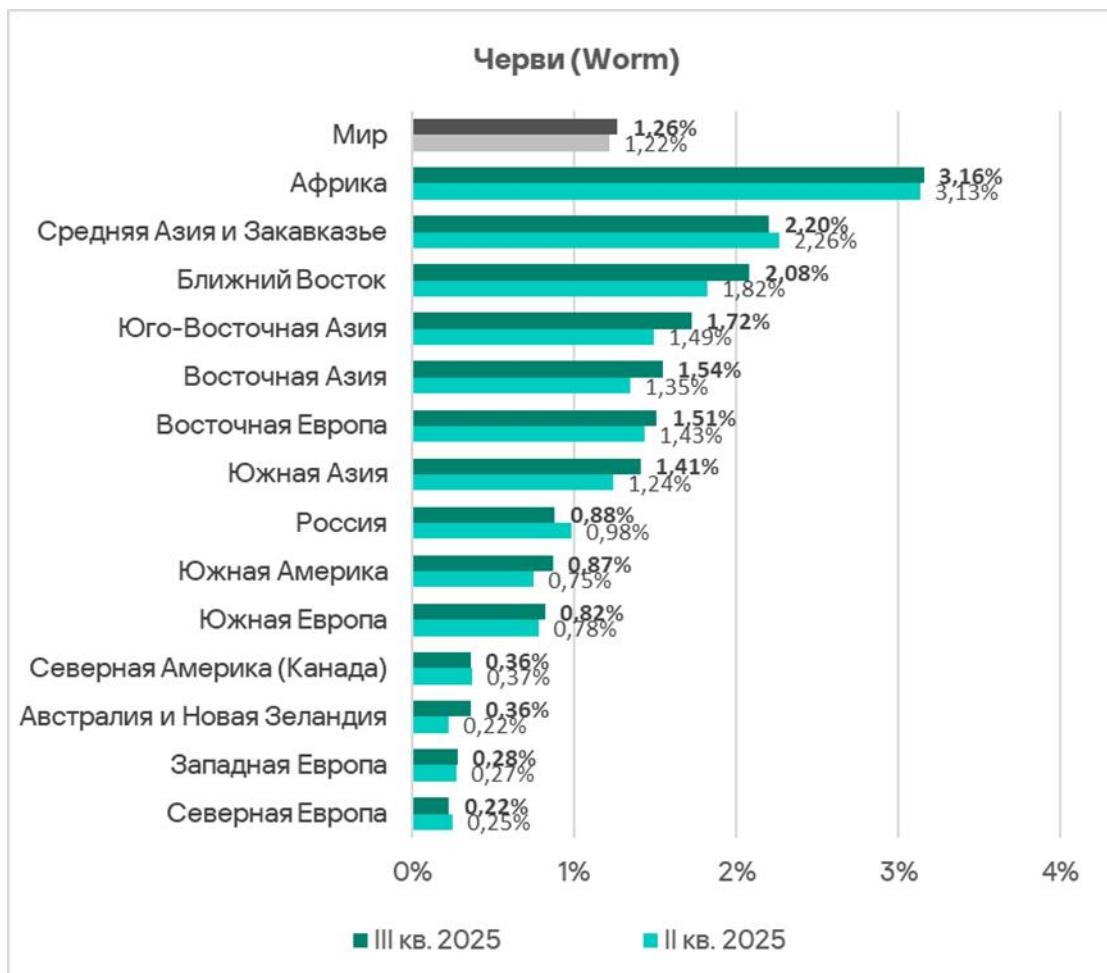


Черви

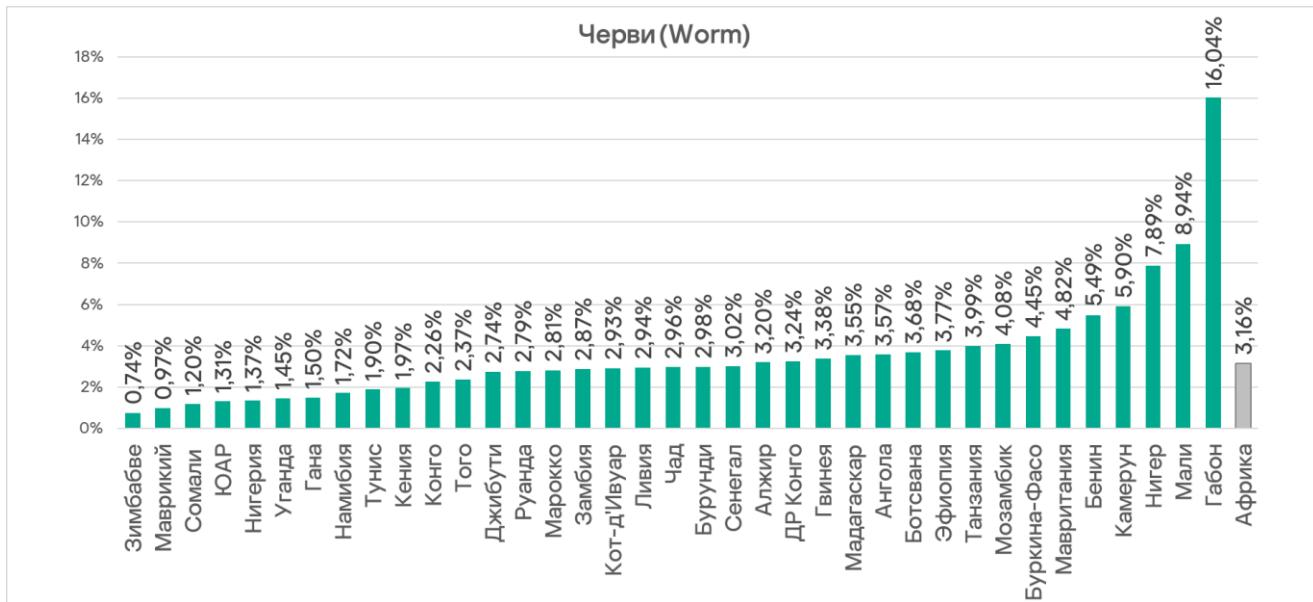
Африка — неизменный лидер среди регионов по доле компьютеров АСУ, на которых блокируются черви. Несмотря на постепенное уменьшение показателя, в Африке он все еще значительно выше, чем в остальных регионах.

Доля компьютеров АСУ, на которых блокируются черви, в Африке в третьем квартале 2025 года немного увеличилась — до 3,16%. Этот показатель в 14,4

раза выше, чем показатель Северной Европы, которая замыкает соответствующий рейтинг.



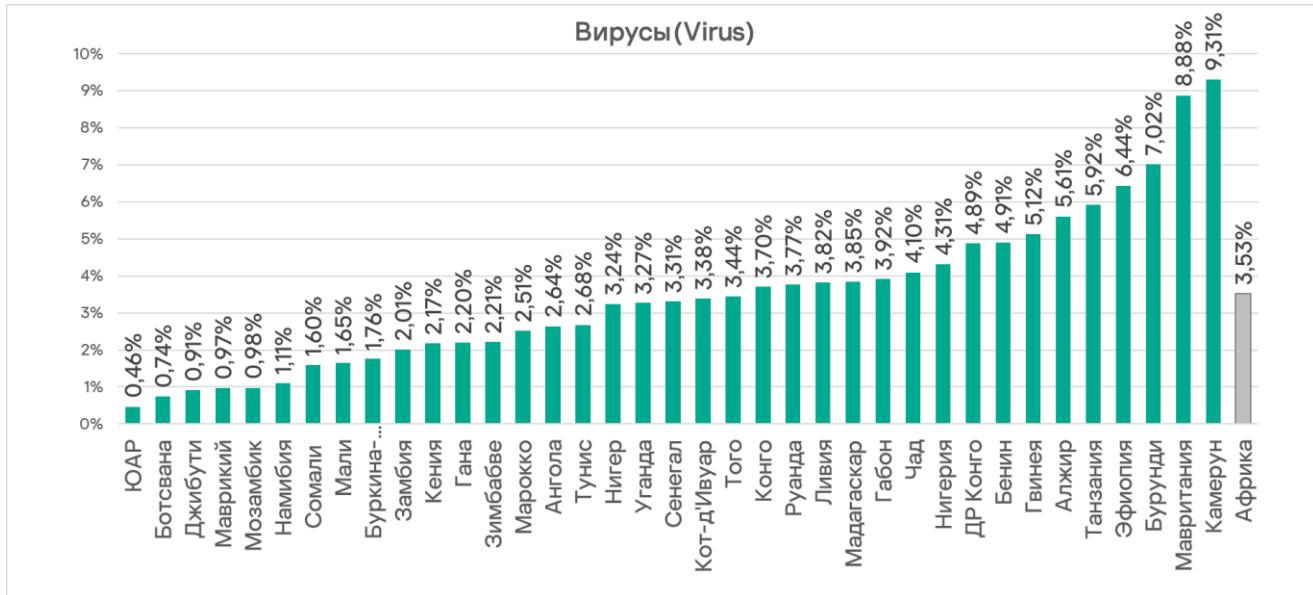
В странах региона по доле компьютеров АСУ, на которых блокируются черви, с большим отрывом лидирует Габон с аномально высокими 16,04%. Это в 1,8 раза больше значения у следующей страны в рейтинге – Мали (8,94%). Наименьший показатель в Зимбабве – 0,74%.



Вирусы

По доле компьютеров АСУ, на которых блокируются вирусы, Африка среди регионов занимает второе место с 3,53%. Этот показатель в Африке в 22,1 раза превышает показатель региона Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых блокируются вирусы, лидируют Камерун (9,31%) и Мавритания (8,88%). Наименьший из всех стран показатель в ЮАР — 0,46%.

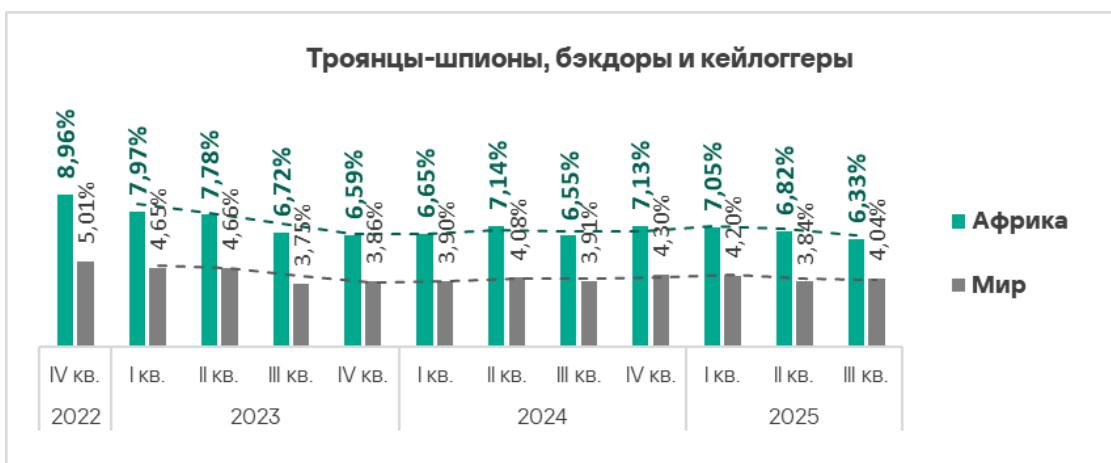


Шпионские программы

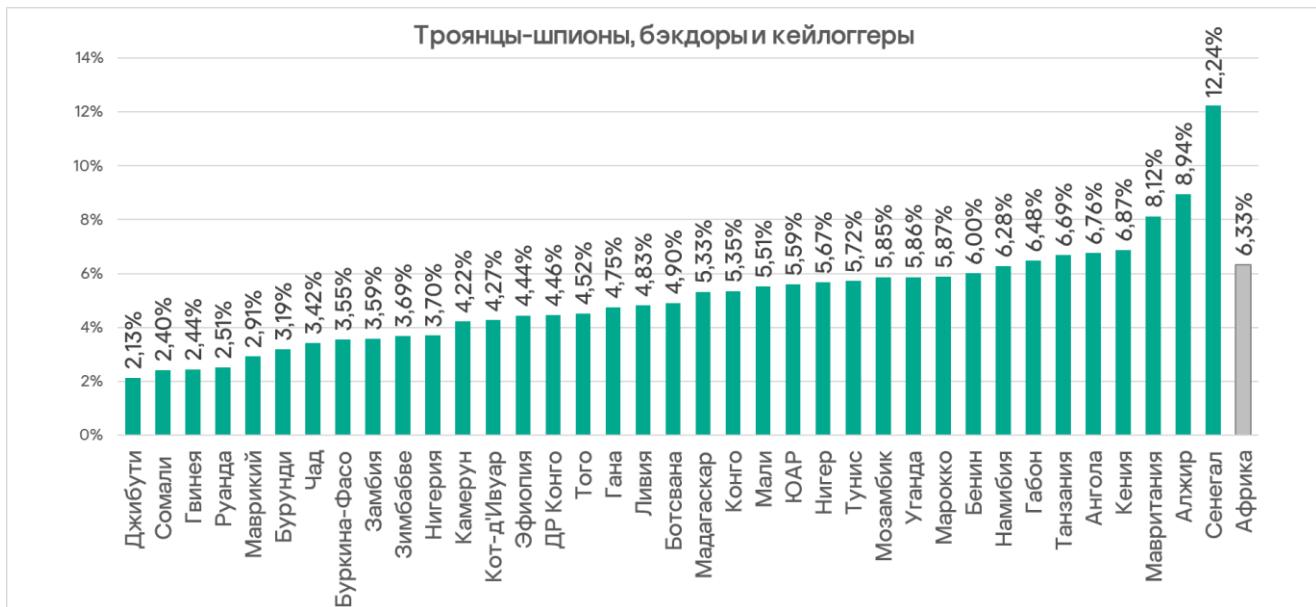
Африка устойчиво лидирует среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-шпионы. В третьем квартале 2025 года этот показатель в Африке уменьшился до 6,33% – это в 4,5 раза больше, чем в Северной Европе, где доля компьютеров АСУ, на которых блокируется шпионское ПО, наименьшая.



Показатель в Африке уменьшается третий квартал подряд.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы программы-шпионы, с отрывом лидирует Сенегал с 12,24%.



Программы-вымогатели

В третьем квартале 2025 года Африка занимает второе место среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели с 0,29%. Это в 5,8 раза больше доли региона с минимальным значением – Северной Европы.

Во втором квартале Африка лидировала по этому показателю. В третьем квартале доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, немного уменьшилась, и регион опустился на вторую строчку рейтинга.



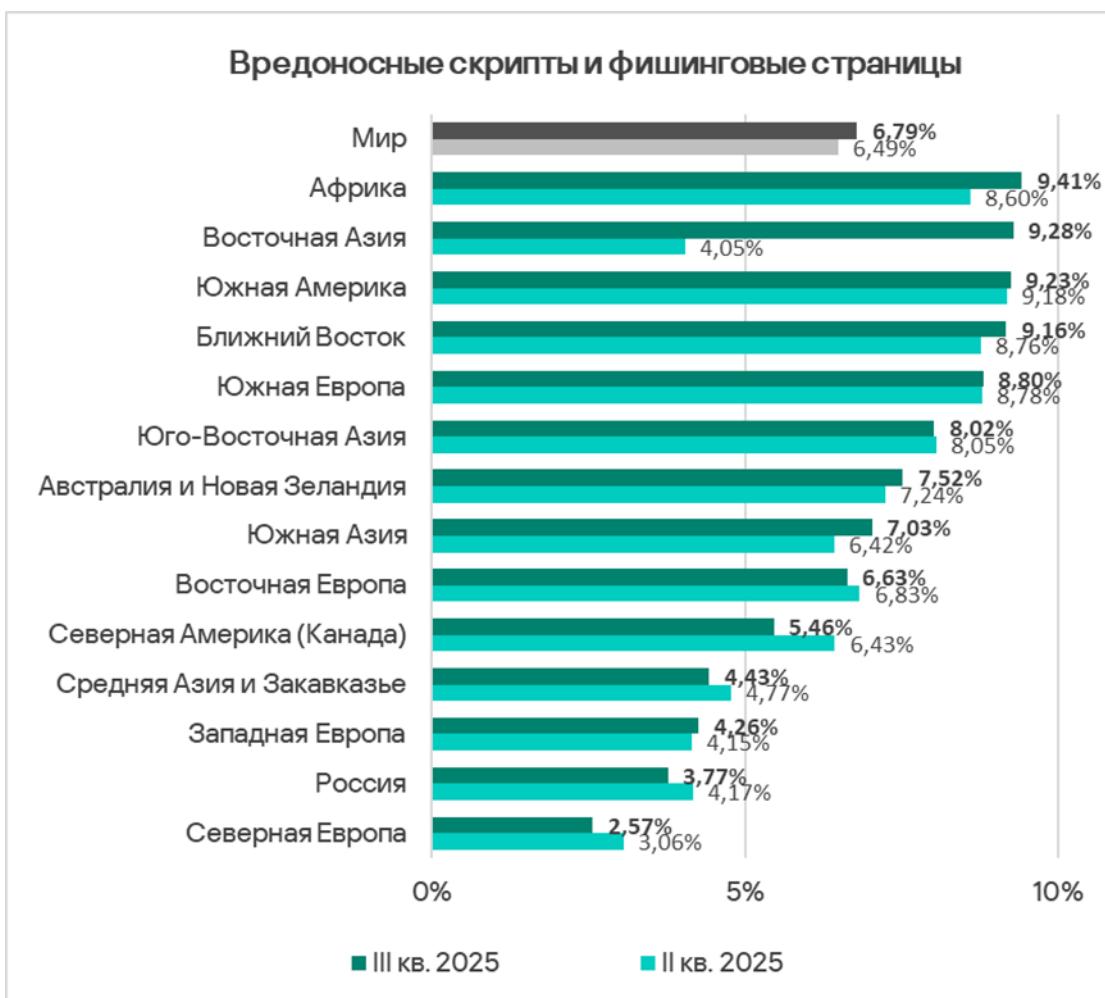
Среди стран региона лидируют по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Мадагаскар с 1,17% и Руанда с 0,84%.



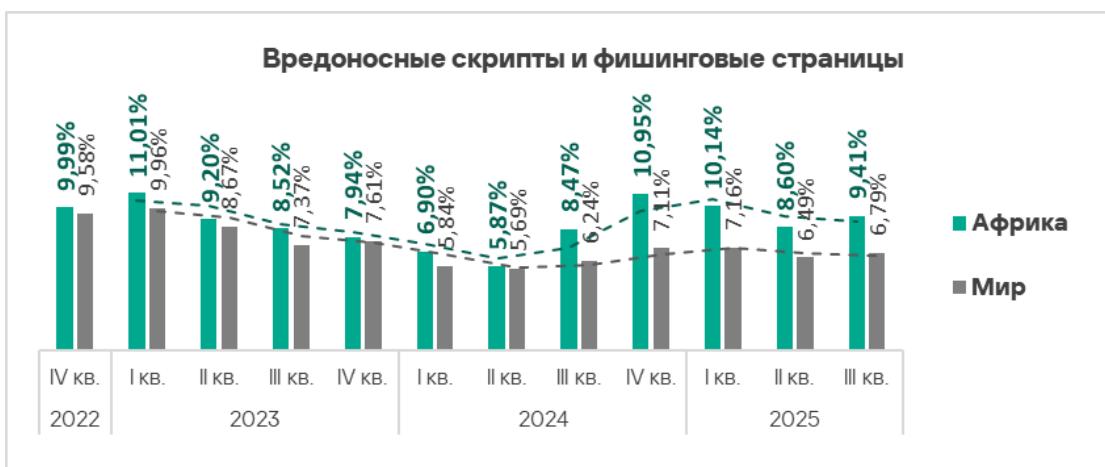
Отметим, что эта угроза в третьем квартале 2025 года была обнаружена не во всех странах региона.

Вредоносные скрипты и фишинговые страницы

В третьем квартале Африка поднялась с четвертого на первое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы. Показатель за квартал увеличился до 9,41%. Это в 3,7 раза больше, чем в Северной Европе, где значение минимальное.



Несмотря на столь заметный подъем позиции региона в рейтинге, квартальный показатель оказался не самым высоким за последние три года. Отметим, что в этот период Африка лидировала по доле компьютеров АСУ, на которых блокировались вредоносные скрипты и фишинговые страницы, еще дважды — в третьем и четвертом кварталах 2024 года.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует ЮАР с 12,0%. Эта же страна возглавляет рейтинг по угрозам из почтовых клиентов. Наименьший показатель в Чаде – 2,51%.



Ресурсы в интернете из списка запрещенных

В третьем квартале 2025 года доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, уменьшилась во всех регионах. По этому показателю Африка сохранила лидирующую позицию с 4,96%. Это в 2,1 раза выше, чем в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.



Среди стран региона по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, лидирует Уганда с 8,94%. Эта страна также входит в топ-3 стран по доле компьютеров АСУ, на которых блокируются угрозы из интернета. Наименьший показатель в Чаде – 1,82%.

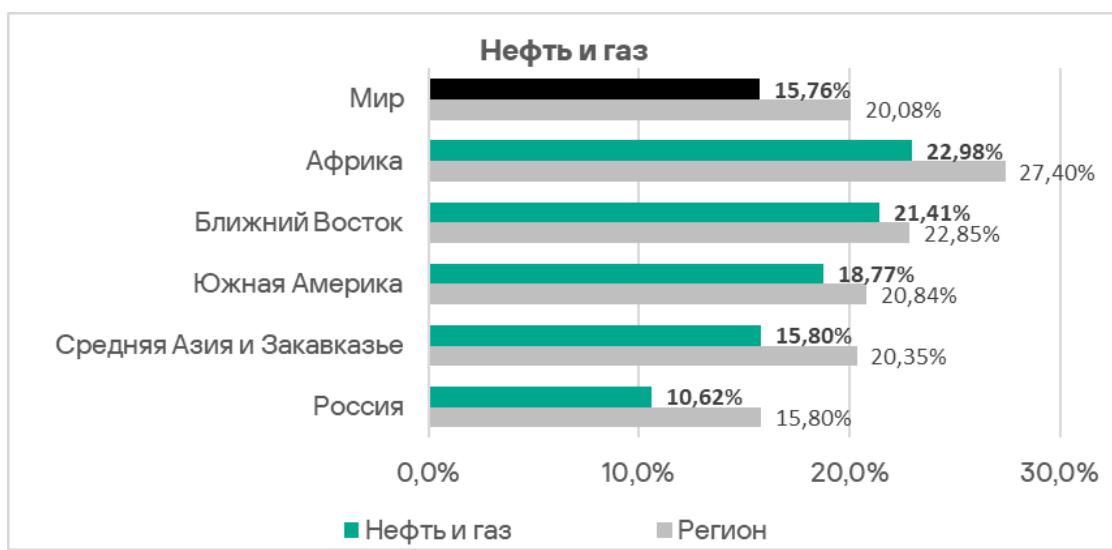


Отрасли

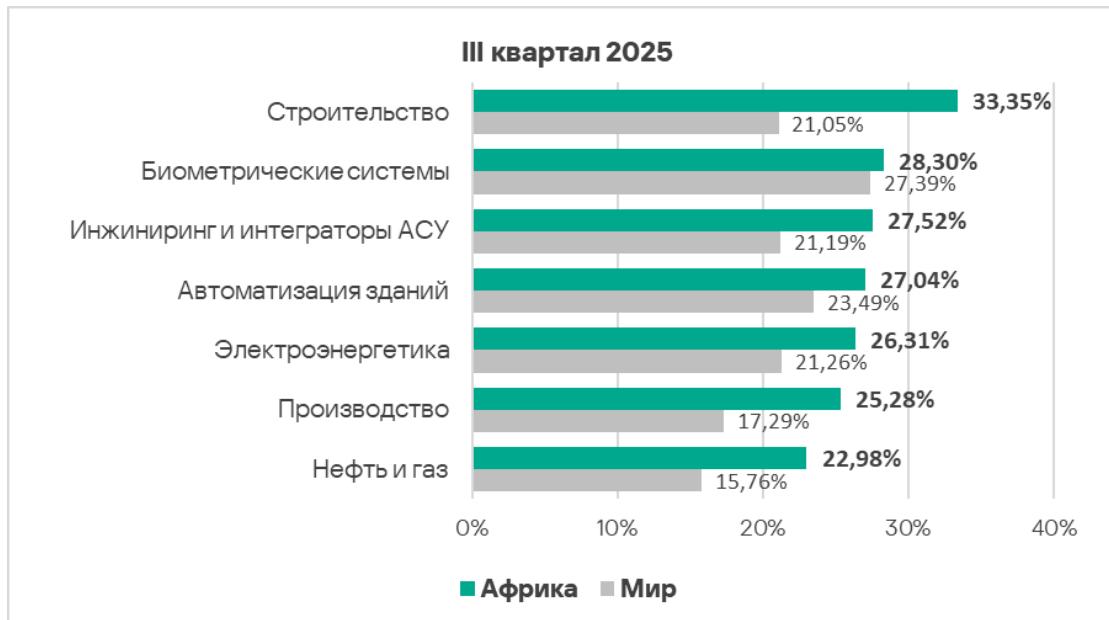
В Африке наиболее часто встречающейся с угрозами отраслью среди рассмотренных в отчете по-прежнему является строительство. По доле компьютеров АСУ, на которых в этой отрасли были заблокированы вредоносные объекты, Африка лидирует среди регионов.



Африка также лидирует среди регионов по показателям нефтегазовой отрасли.

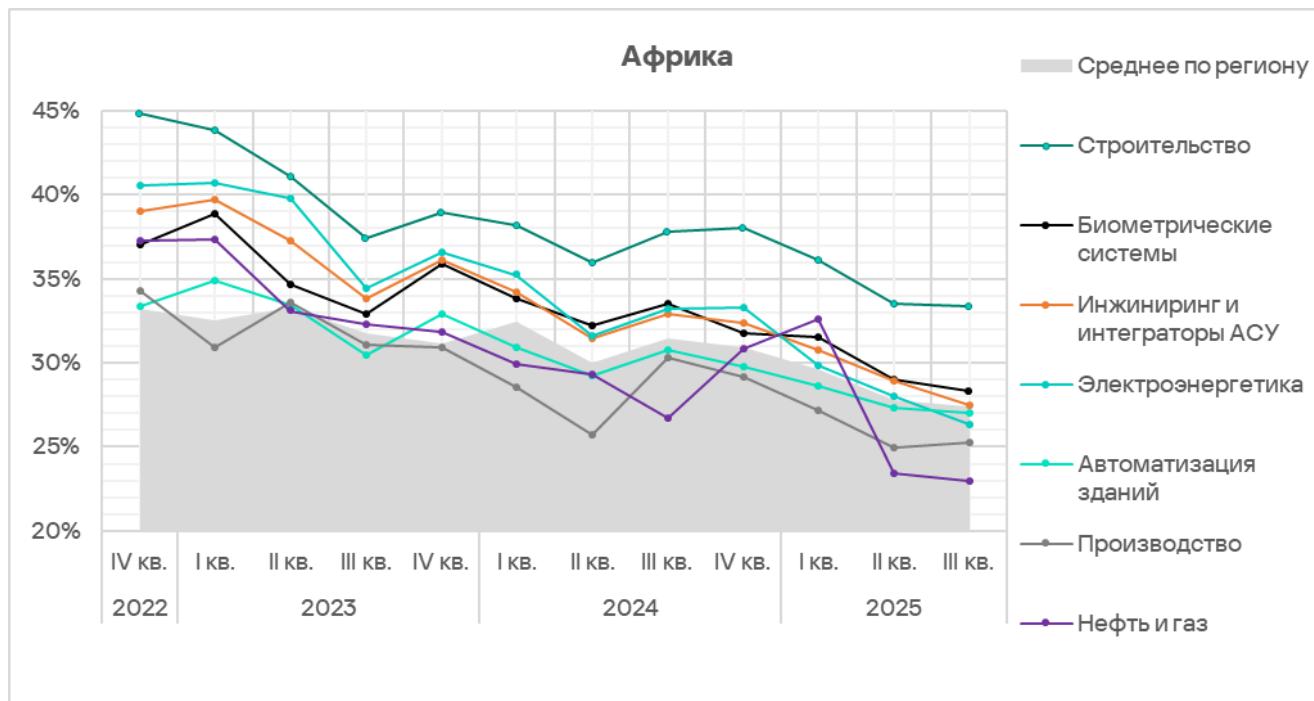


Показатели всех отраслей в регионе превышают аналогичные среднемировые. Больше всего разница у отраслей строительство (в 1,6 раза), производство и нефтегазовой отрасли (в 1,5 раза каждая).



Показатели всех отраслей, кроме отрасли производство, за квартал уменьшились.

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, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	10,07%	9,60%	11,69%	11,96%	9,59%	12,06%	11,32%	10,31%
Почтовые клиенты	6,08%	7,18%	2,74%	2,49%	0,85%	3,46%	2,83%	4,18%
Съемные носители	1,60%	1,11%	1,15%	1,46%	1,33%	1,94%	0,09%	1,43%
Сетевые папки	0,02%	0,02%	0,00%	0,01%	0,00%	0,00%	0,00%	0,02%
Показатель отрасли в регионе	28,30%	27,04%	26,31%	27,52%	22,98%	33,35%	25,28%	

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

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	4,58%	4,25%	6,23%	6,15%	6,48%	6,32%	5,60%	4,96%
Вредоносные скрипты и фишинговые страницы	10,69%	11,06%	8,83%	9,44%	9,90%	8,77%	7,22%	9,41%
Троянцы-шипионы, бэкдоры и кейлоггеры	8,42%	7,16%	5,62%	5,65%	7,50%	3,58%	4,18%	6,33%
Черви (Worm)	3,87%	2,84%	3,05%	2,71%	3,46%	2,55%	2,28%	3,16%
Майнеры — исполняемые файлы для ОС Windows	0,67%	0,47%	0,50%	0,68%	0,83%	0,28%	0,47%	0,51%
Вредоносные документы (MSOffice+PDF)	3,69%	4,55%	1,79%	1,69%	2,19%	2,08%	1,04%	2,72%
Вирусы (Virus)	3,65%	2,95%	3,89%	3,33%	6,02%	1,98%	3,61%	3,53%
Программы-вымогатели	0,44%	0,33%	0,36%	0,27%	0,31%	0,38%	0,09%	0,29%
Веб-майнеры, выполняемые в браузерах	0,30%	0,28%	0,11%	0,37%	0,28%	0,19%	0,19%	0,26%
Вредоносные программы для AutoCAD	0,12%	0,10%	0,36%	0,38%	1,88%	0,28%	0,47%	0,41%
Показатель отрасли в регионе	28,30%	27,04%	26,31%	27,52%	22,98%	33,35%	25,28%	

Строительство

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

- первое место по доле компьютеров, на которых угрозы блокировались на съемных носителях;
- 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: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, шпионские программы, программы-вымогатели, черви.

Среди отраслей в регионе строительство занимает:

- первое место по показателю угроз из интернета и по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей;
- первое место по показателям сразу нескольких категорий: ресурсы в интернете из списка запрещенных, вирусы, майнеры – исполняемые файлы для ОС Windows, вредоносные программы для AutoCAD. Также строительство находится на втором месте среди отраслей по показателям шпионских программ и червей.

Биометрические системы

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

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

Среди регионов по показателям в отрасли Африка занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы при подключении съемных носителей;
- первое место по доле компьютеров АСУ, на которых блокируются черви, и второе – по показателю вирусов.

Среди отраслей в регионе ОТ-инфраструктура биометрические системы занимают:

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

Инжиниринг и интеграторы АСУ

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета и на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, шпионские программы и черви, а также второе место – по показателю следующих категорий: вредоносные скрипты и фишинговые страницы, программы-вымогатели.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, и третье – по показателю угроз на съемных носителях и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются веб-майнеры;
- второе место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows, и третье – по показателю вредоносных программ для AutoCAD.

Автоматизация зданий

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ в отрасли, на которых угрозы блокируются при подключении съемных носителей, и третье место – по показателю угроз из интернета;
- второе место по доле компьютеров АСУ в отрасли, на которых блокируются черви и вирусы;
- третье место по показателю категории вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе автоматизация зданий занимает:

- первое место по показателю угроз из почтовых клиентов и третье – 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 шпионские программы и веб-майнеры.

Электроэнергетика

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, и второе – по показателю угроз на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, второе – по показателю червей и третье – по показателю вредоносных скриптов.

Среди отраслей в регионе электроэнергетика занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- второе место по показателям вирусов;
- третье место по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, черви, программы-вымогатели.

Производство

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, и третье – по показателю почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и программы-вымогатели. Регион также находится на втором месте по показателю вредоносных скриптов и фишинговых страниц, и на третьем – по показателю червей.

Среди отраслей в регионе производство занимает:

- четвертое место по показателю угроз из интернета и почтовых клиентов;
- второе место по показателям следующих категорий: ресурсы в интернете из списка запрещенных и программы-вымогатели.

Нефтегазовая отрасль

Среди регионов по показателям в отрасли Африка занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из интернета, и третье – по показателю почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых блокируются следующие категории: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, шпионские программы, вирусы, черви, вредоносные программы для AutoCAD.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- 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 АРТ¹.

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