Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Африка. Второй квартал 2025 года

18.09.2025

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 OT, 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: во втором квартале 2025 года — в 1,8 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 во втором квартале 2025 года превышает аналогичный среднемировой показатель в 4,8 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.

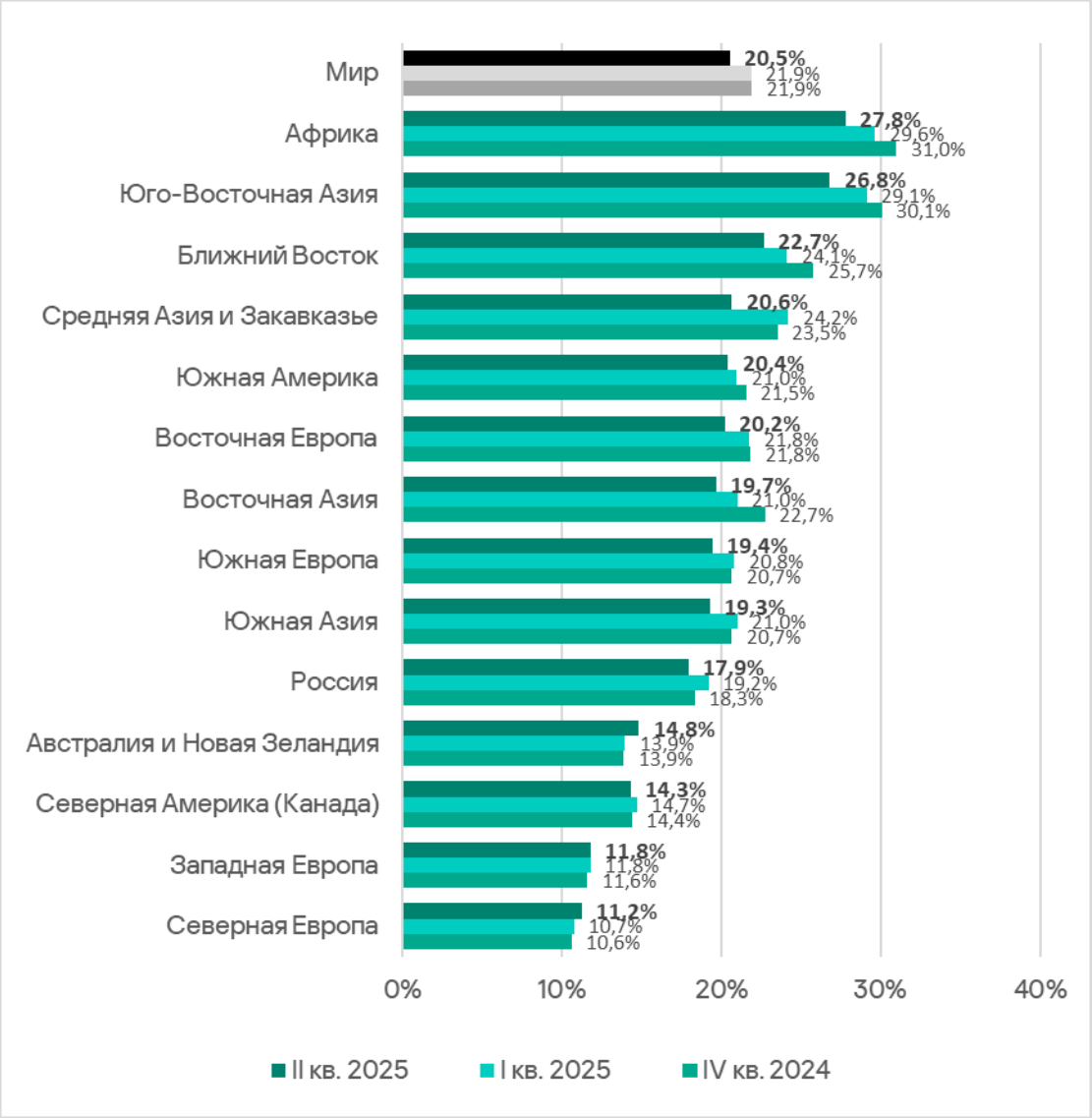
Скорость внедрения мер и средств кибербезопасности уступает темпам развития быстро развивающихся отраслей

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.

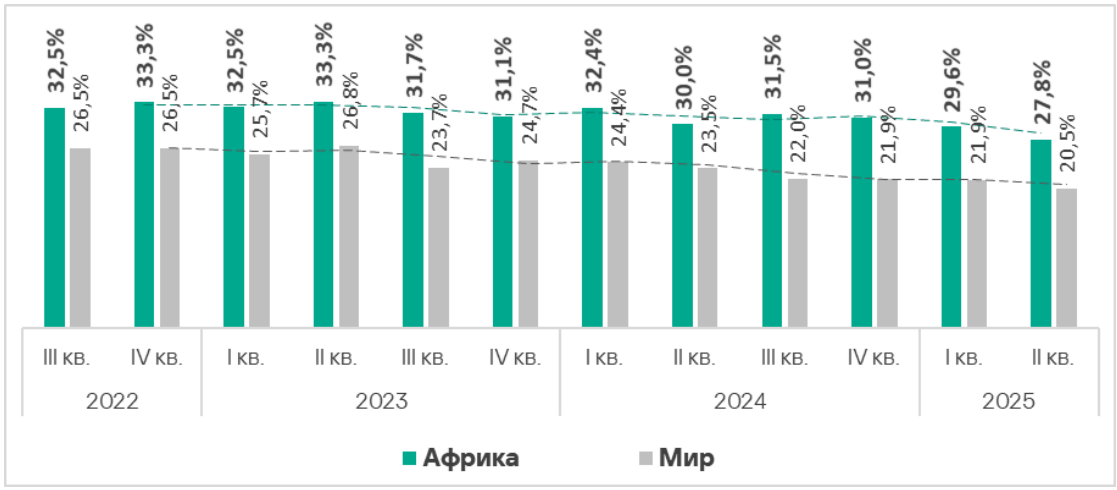
Эта тенденция хорошо просматривается на статистике по отраслям и типам инфраструктур в Африке (см. далее). Нефтегазовый сектор, энергетика, промышленное производство, строительство — быстро развивающиеся секторы. Инжиниринг — им сопутствующий.

Статистика по всем угрозам

Африка много лет лидирует в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. По сравнению со среднемировым значением показатель Африки во втором квартале 2025 года больше в 1,4 раза. По сравнению с Северной Европой, которая замыкает этот рейтинг, — в 2,5 раза.



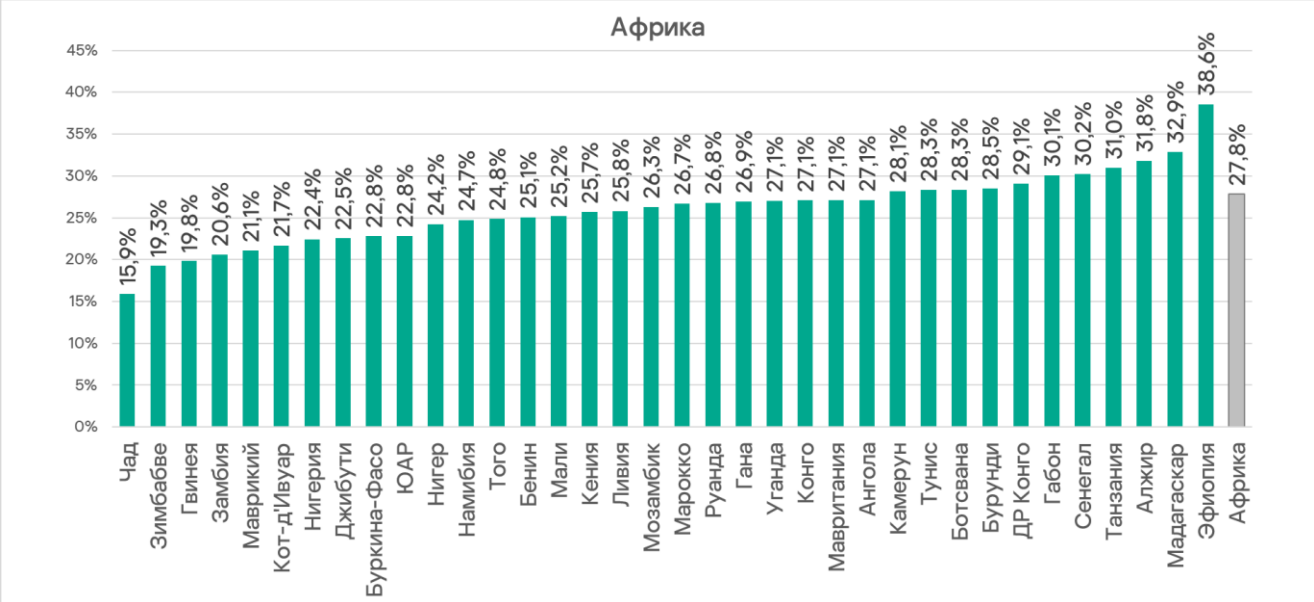
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Африке снизилась до 27,8%. Показатель в регионе снижается третий квартал подряд.



В странах региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 15,9% в Чаде до 38,6% в Эфиопии.

Показательно ниже 20% — лишь в трех странах: Чад, Зимбабве и Гвинея.

Две трети стран региона имеют показатель выше 25%. Из них в Габоне, Сенегале, Танзании, Алжире, Мадагаскаре и Эфиопии он превышает 30%.



Источники угроз

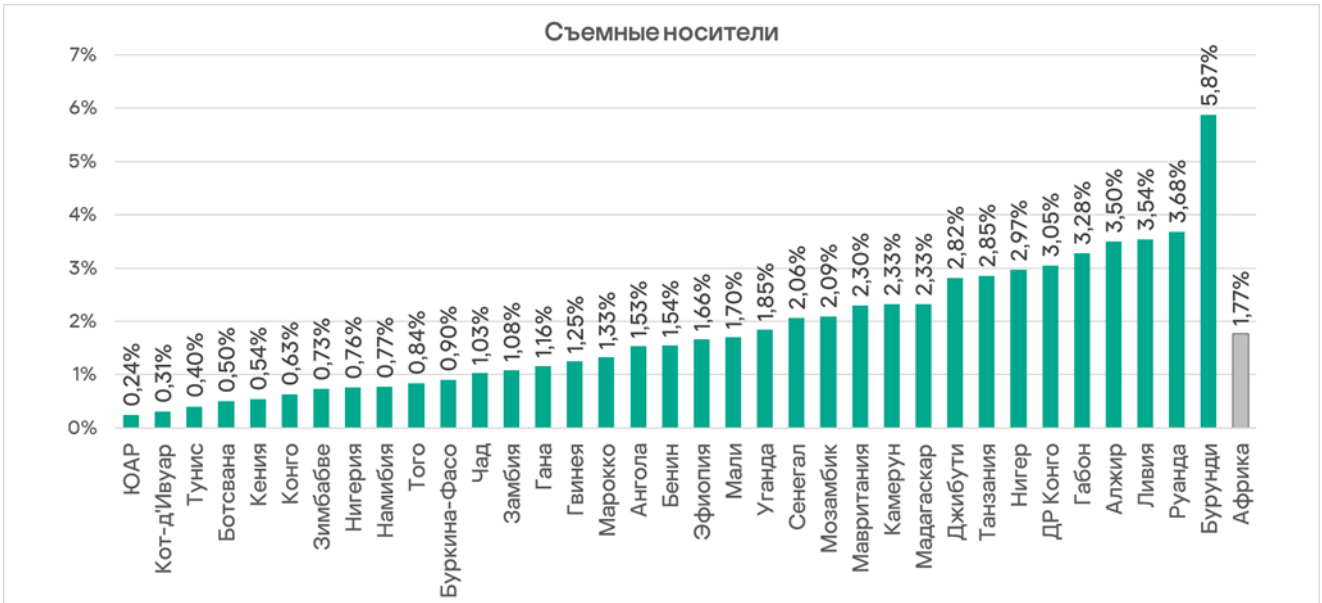
Значения по всем источникам угроз в регионе превышают среднемировые, в случае съемных носителей это превышение весьма значительно – в 4,8 раза.

Из всех источников угроз показатель растет только у почтовых клиентов.

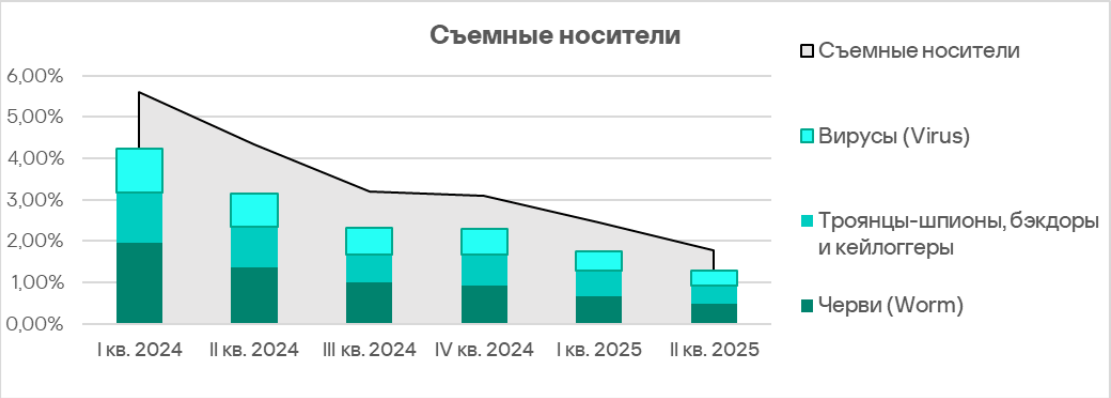
Съемные носители

Несмотря на явный тренд к снижению доли компьютеров АСУ, на которых были заблокированы угрозы со съемных носителей, по этому показателю Африка регулярно и с большим отрывом лидирует среди регионов. Показатель Африки превышает показатель Северной Америки (Канады), которая занимает последнее место в соответствующем рейтинге, в 66 раз.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с заметным отрывом лидирует Бурунди с 5,8%. Показатели остальных стран варьируют от 0,24% в ЮАР до 3,68% в Руанде.

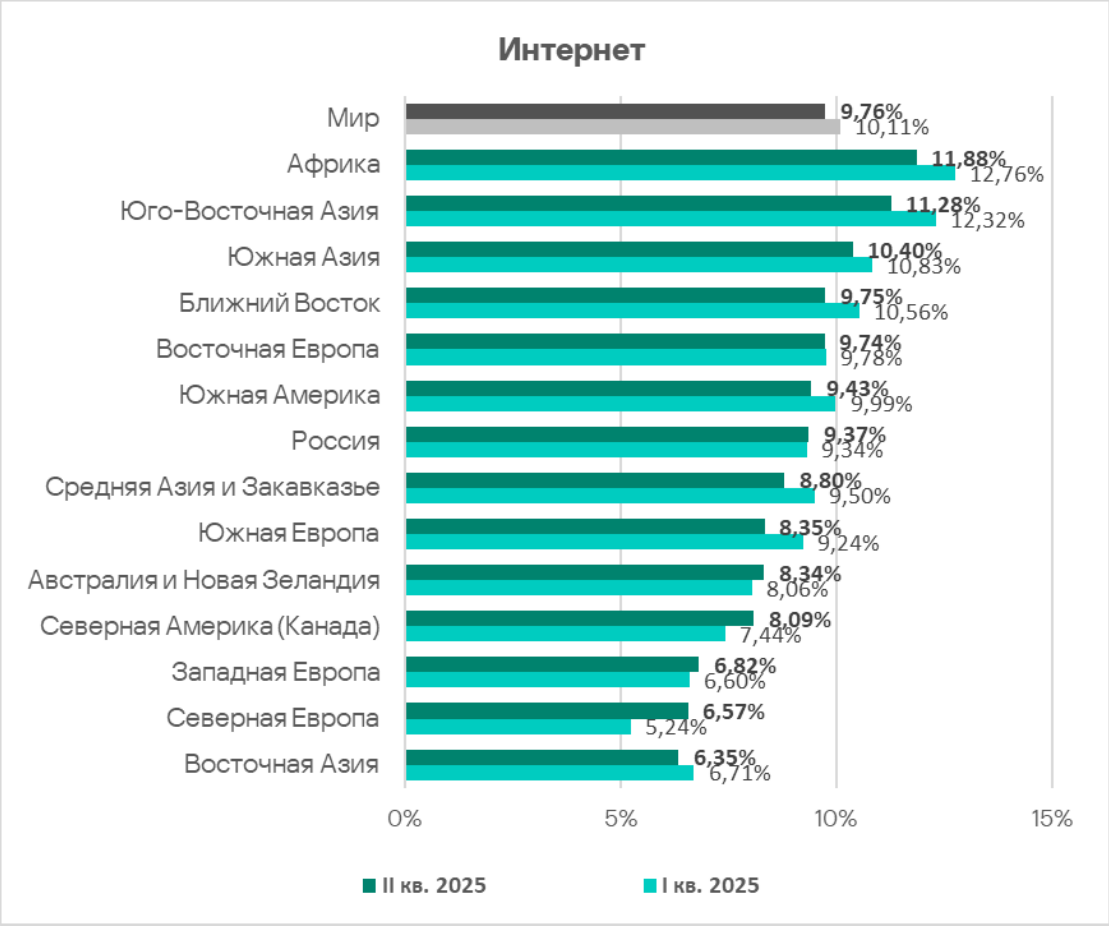


Основные категории угроз, которые блокируются при подключении съемных носителей к компьютерам АСУ, — черви, вирусы и шпионское ПО. По этим категориям Африка также лидирует среди регионов (по вирусам — на втором месте в рейтинге).

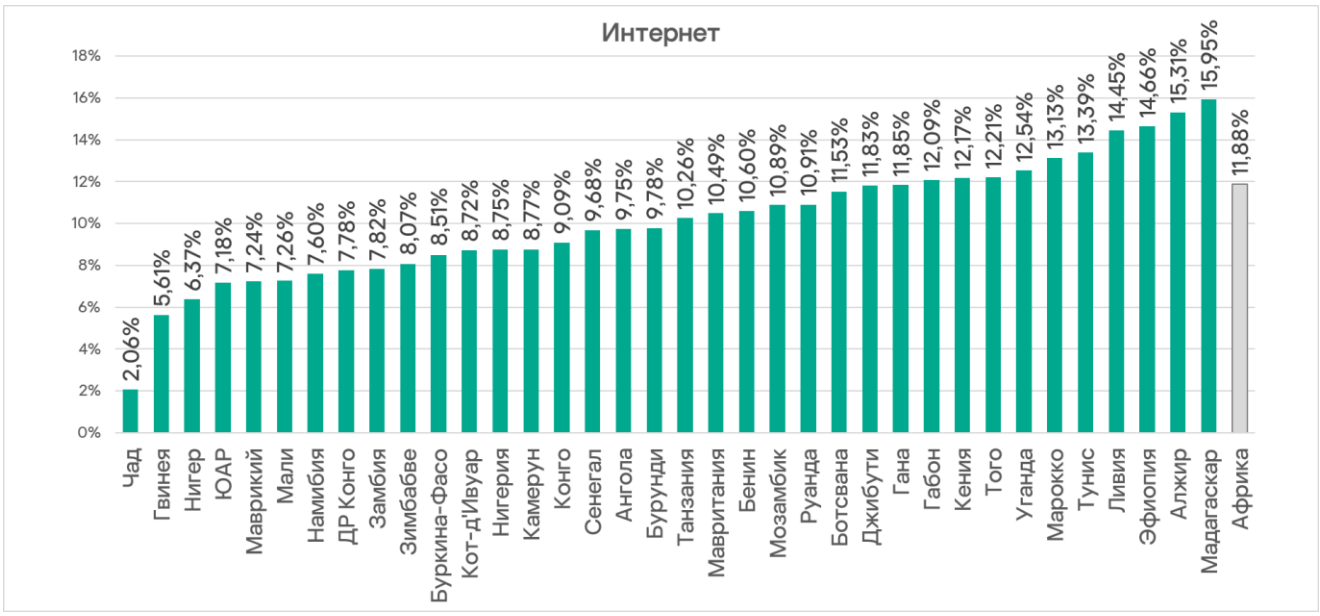


Интернет

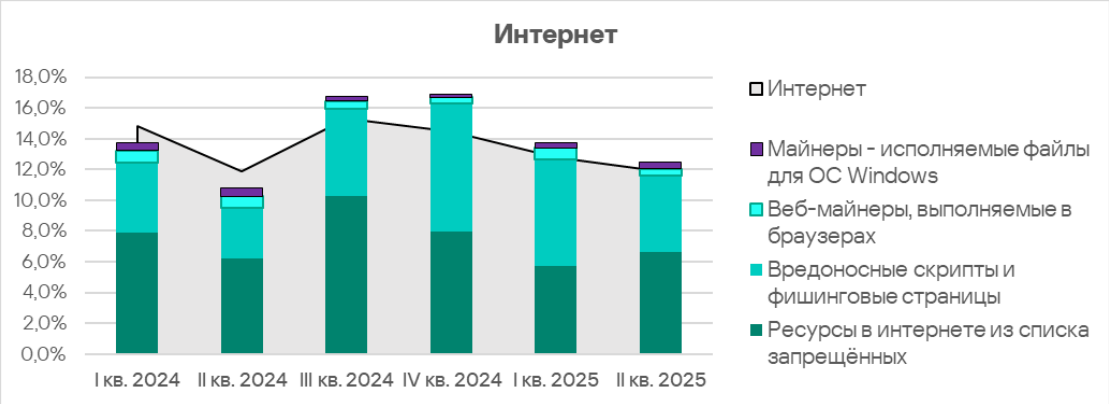
Еще один источник угроз, по которому Африка лидирует среди регионов — интернет. В случае этого источника угроз ситуация не столь драматична: показатель Африки превышает показатель Восточной Азии, которая занимает последнее место в соответствующем рейтинге, в 1,9 раз.



Среди стран региона нет ярко выраженного лидера по этому показателю, зато заметно меньше, чем в остальных странах, доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, в Чаде (2,06%). Максимальный показатель на Мадагаскаре — 15,95%.



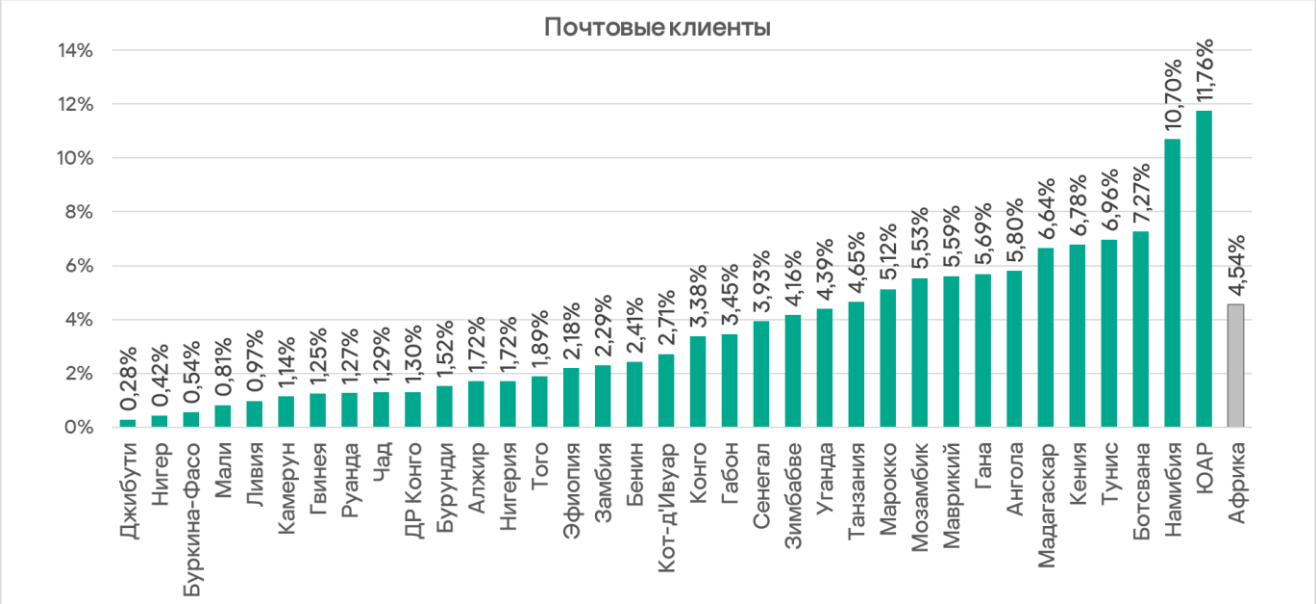
Основные категории угроз из интернета, блокируемые на компьютерах АСУ, — это интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы и майнеры.



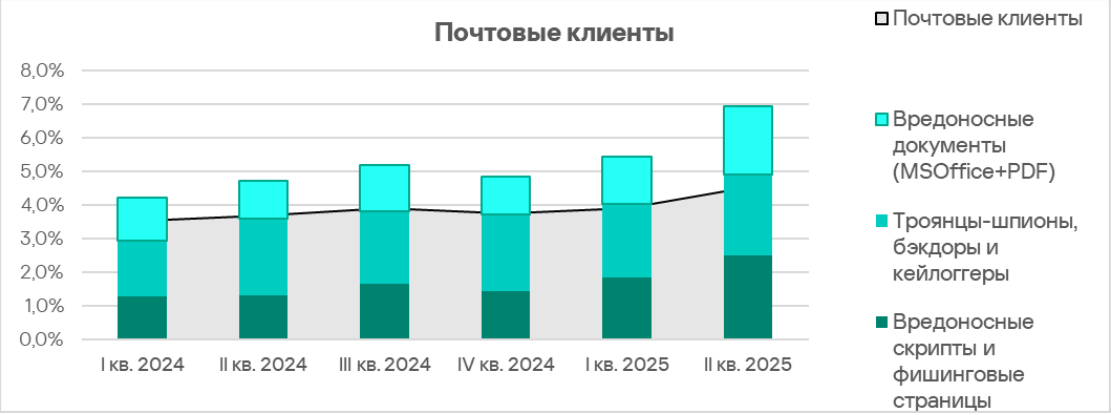
Почтовые клиенты

Почтовые клиенты — единственный источник угроз в регионе, показатель которого вот уже более года демонстрирует тенденцию к росту. В рейтинге регионов по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, Африка находится на четвертом месте с 4,54%. Это в 5,7 раз больше, чем в России с минимальным показателем среди регионов.

Среди стран региона по этому показателю явно лидируют ЮАР и Намибия.

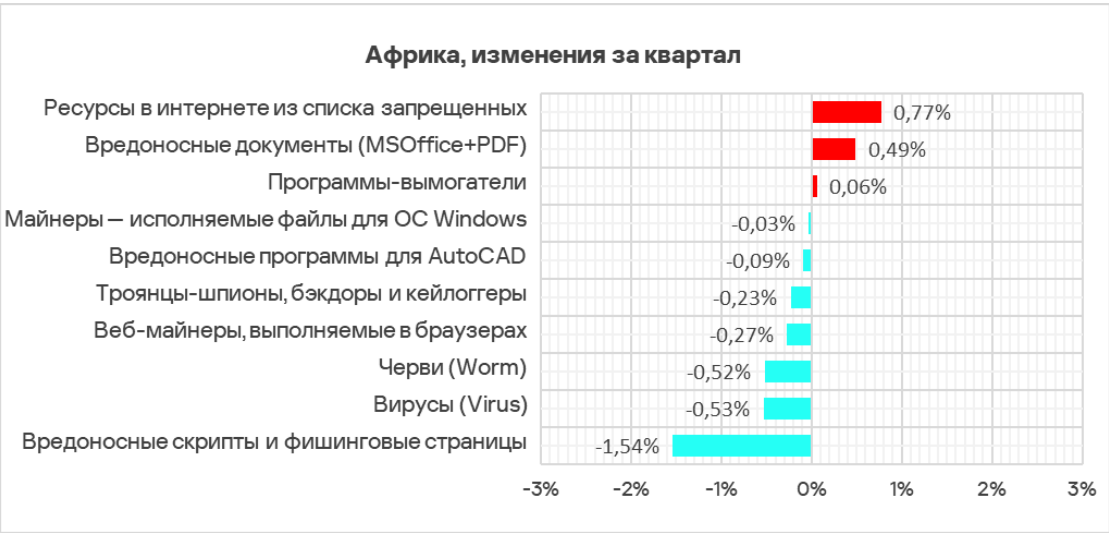


Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ, — это вредоносные документы, шпионское ПО, вредоносные скрипты и фишинговые страницы.



Категории угроз

В Африке у всех категорий угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения. Африка лидирует среди регионов по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, веб-майнеры, шпионские программы, программы-вымогатели, черви.



Самая драматичная ситуация в регионе сложилась с самораспространяющимся вредоносным ПО: показатели червей и вирусов превышают среднемировые в 2,6 раза каждый.

Показатель программ-вымогателей в Африке во втором квартале выше среднемирового значения в 2,2 раза.

В 1,8 раз в регионе больше, чем в мире, доля компьютеров АСУ, на которых блокируются шпионские программы и веб-майнеры.

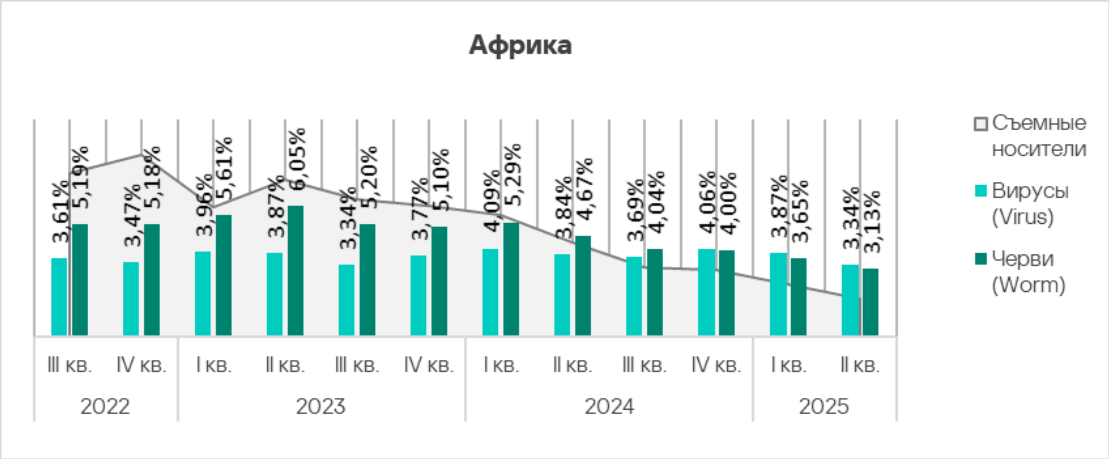
Среди регионов во втором квартале 2025 года Африка лидирует в рейтингах по доле компьютеров АСУ, на которых были заблокированы:

- ресурсы в интернете из списка запрещенных;
- шпионские программы;
- черви и вирусы (по вирусам второе место в рейтинге);
- веб-майнеры;
- программы-вымогатели.

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.

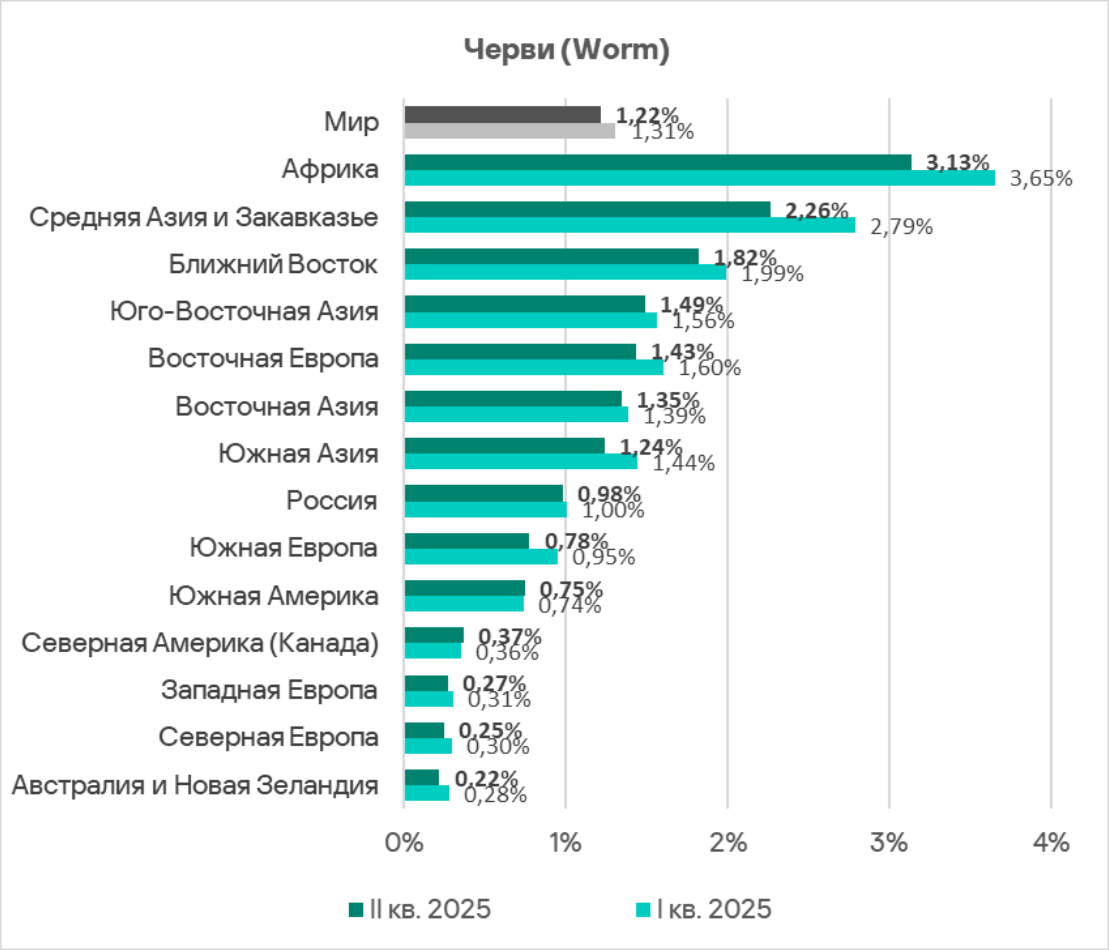
Показатель червей, как и доля угроз со съемных носителей в целом, постепенно снижается. У вирусов более сложная динамика, однако в последние два квартала мы также отмечаем снижение.



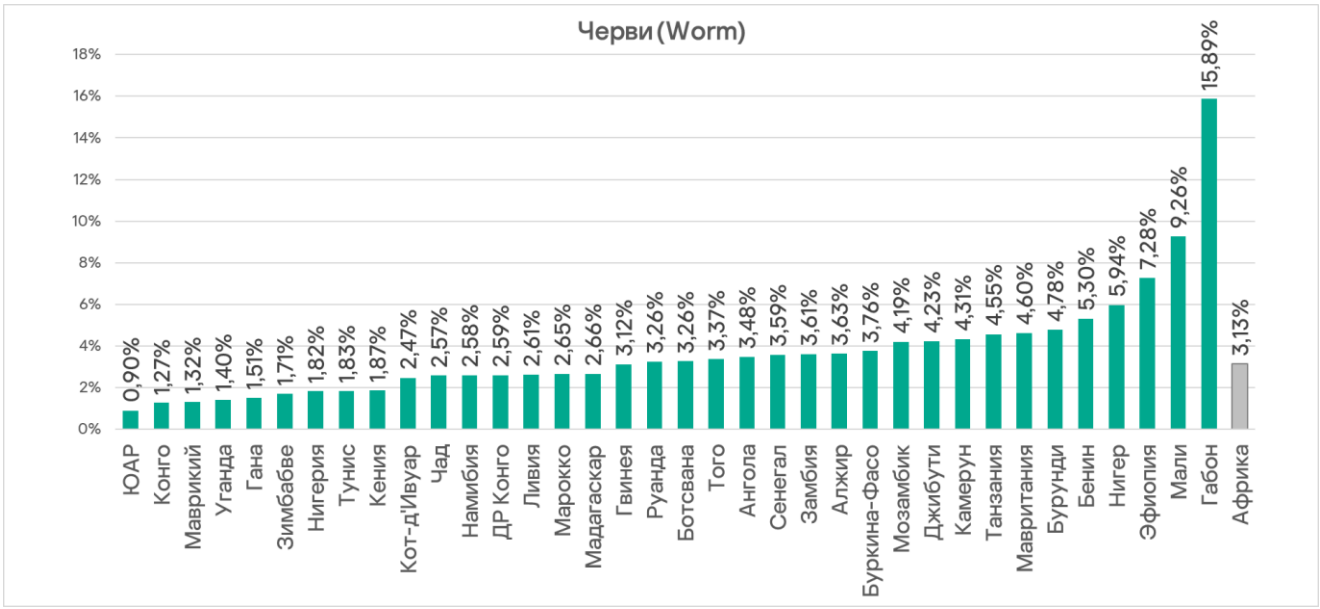
Несмотря на постепенное уменьшение показателей, эти угрозы в Африке все еще очень заметны по сравнению с другими регионами.

Черви

Африка — многолетний лидер среди регионов по доле компьютеров АСУ, на которых блокируются черви. Показатель в Африке во втором квартале 2025 года (3,13%) в 14,2 раза превышает долю в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.



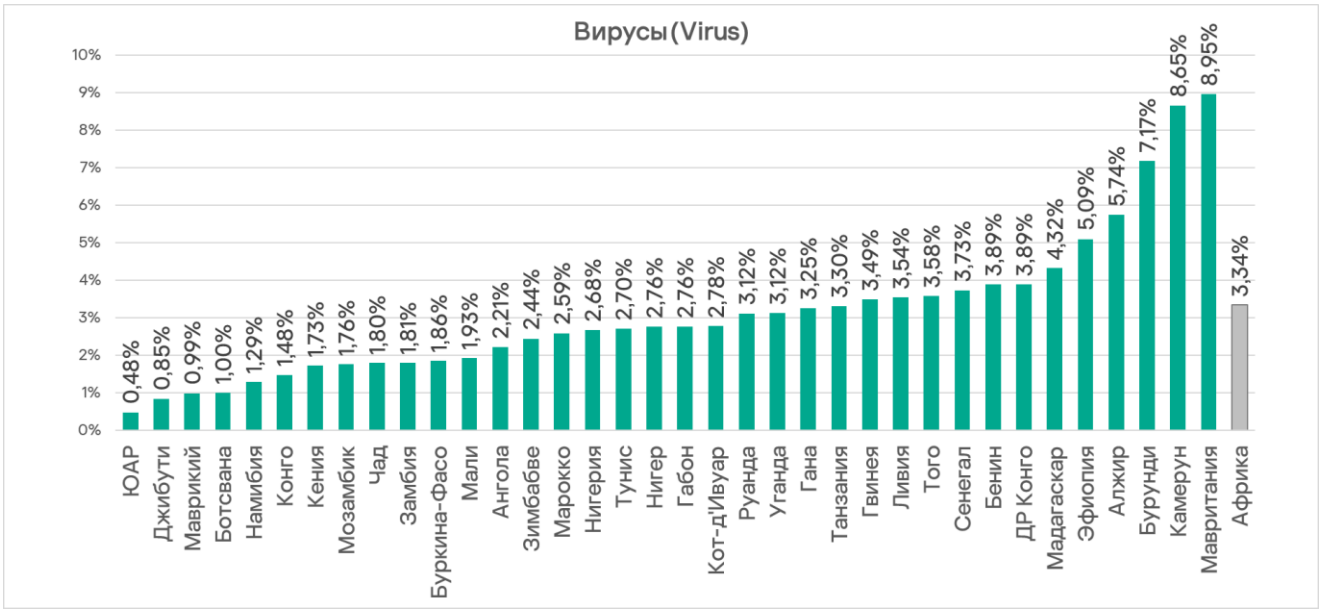
В странах региона по доле компьютеров АСУ, на которых блокируются черви, с большим отрывом лидирует Габон с аномально высокими 15,89%. Это в 1,7 раз больше значения следующей страны в рейтинге — Мали (9,26%) и в 17,7 раз — показателя ЮАР (0,90%), которая замыкает рейтинг.



Вирусы

Несмотря на то, что по доле компьютеров АСУ, на которых блокируются вирусы, Африка среди регионов занимает не первое, а второе место с 3,34%, показатель Африки в 26 раз превышает долю региона Австралия и Новая Зеландия, у которого значение среди регионов минимальное.

Среди стран региона по доле компьютеров АСУ, на которых блокируются вирусы, лидируют Мавритания, Камерун и Бурунди. Как и в случае с червями, разброс значений в странах довольно большой: показатель Мавритании (максимальные 8,95%) превышает показатель ЮАР (минимальные 0,48%) в 18,6 раза.

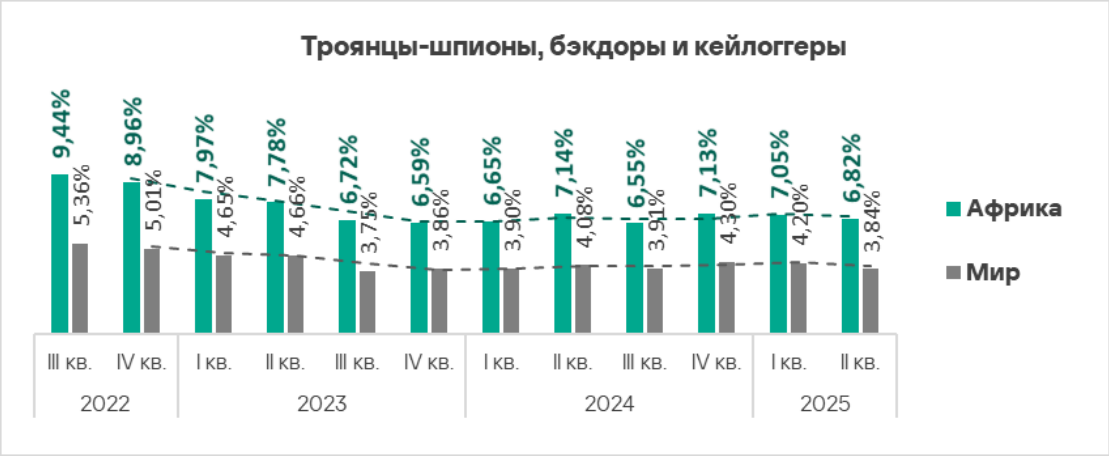


Отметим, что в ЮАР минимальные среди стран показатели по червям, по вирусам и по угрозам со съемных носителей. При этом страна лидирует по угрозам из почтовых клиентов.

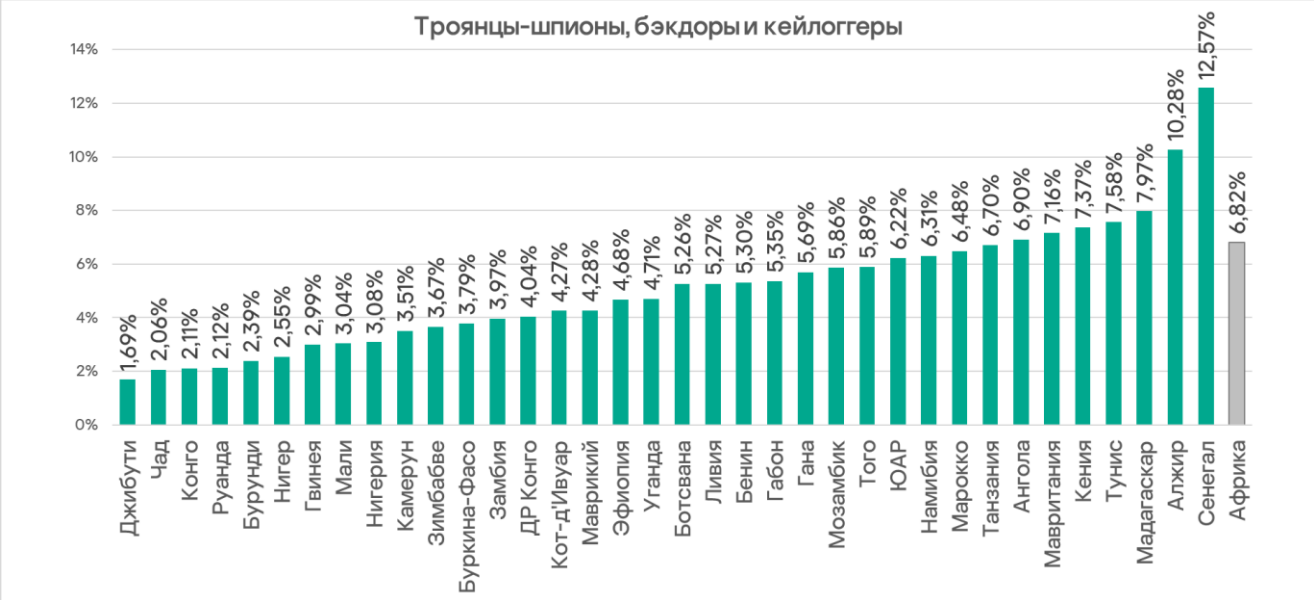
Шпионские программы

Еще одна постоянная беда региона — шпионские программы. Африка устойчиво лидирует среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-шпионы. Во втором квартале 2025 года показатель в Африке уменьшился до 6,82%, однако это в 4,9 раза больше, чем в Западной Европе, где это значение наименьшее.

Показатель региона с первого квартала 2024 года колеблется в диапазоне от 6,55% до 7,14%.

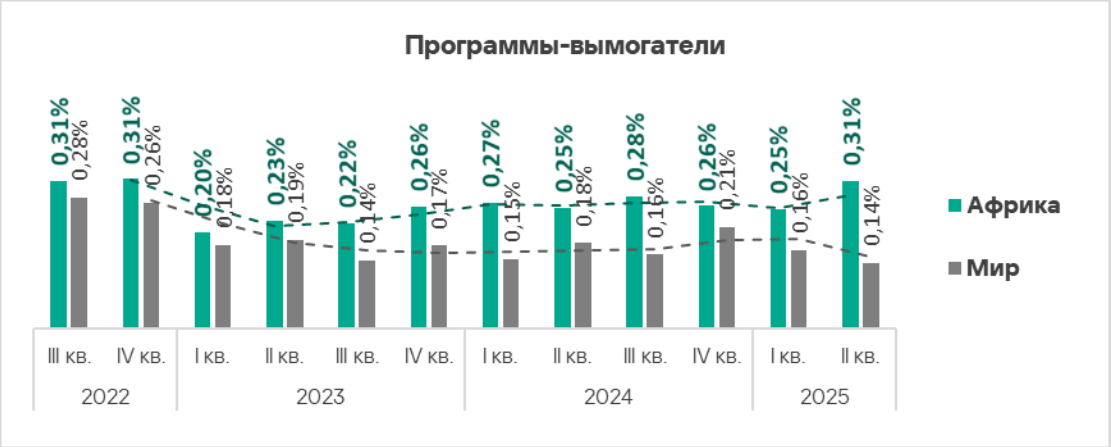


Среди стран региона по доле компьютеров АСУ, на которых заблокированы программы-шпионы, лидируют Сенегал и Алжир.



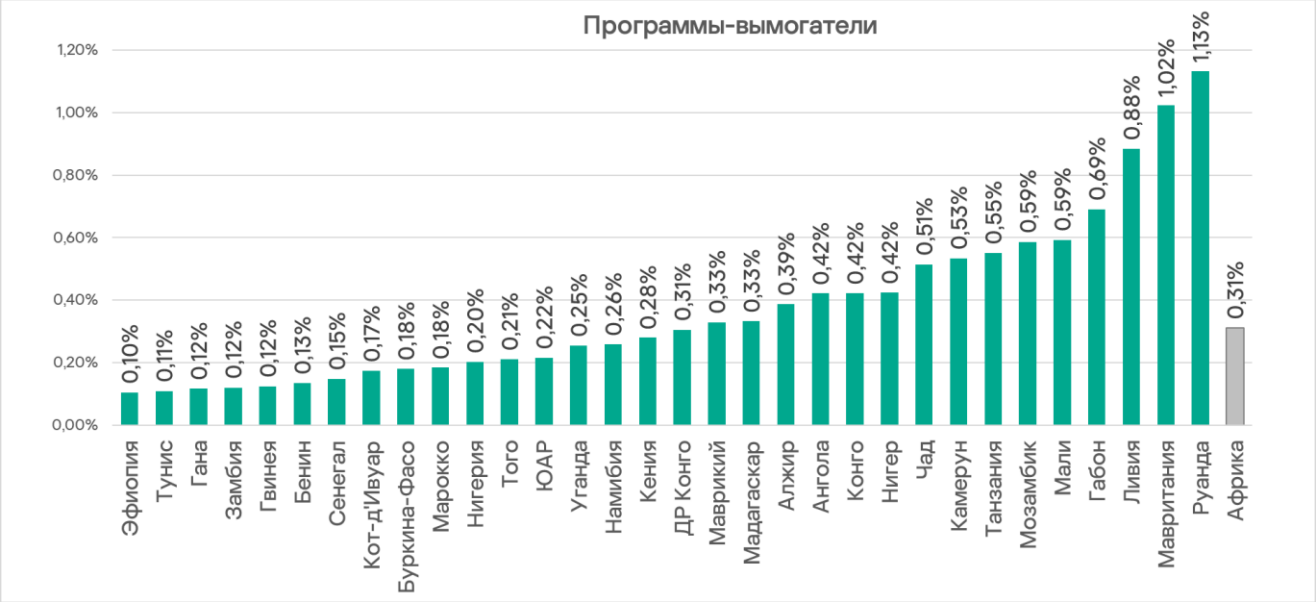
Угроза квартала: программы-вымогатели

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, выросла в Африке во втором квартале 2025 года на 0,6 п. п. Хотя эта величина не кажется значительной, для программ-вымогателей она весьма весома.

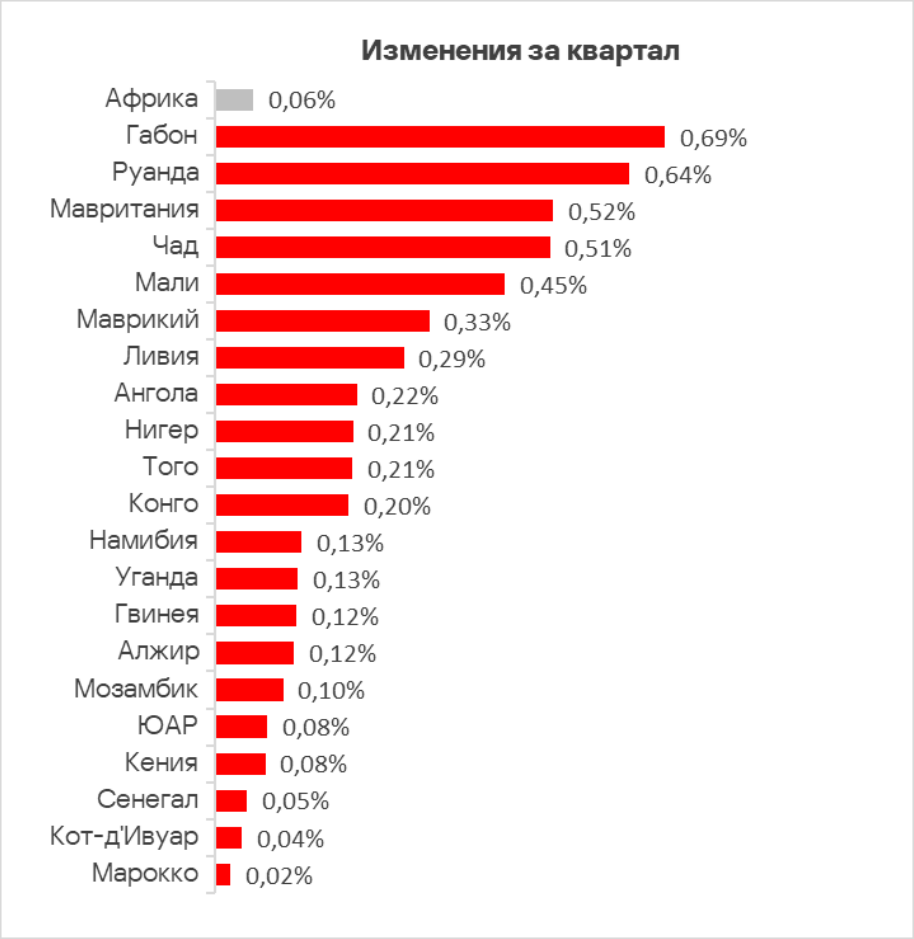


Африка занимает первое место среди регионов по росту доли компьютеров АСУ, на которых были заблокированы программы-вымогатели. В результате во втором квартале 2025 года регион возглавил рейтинг с показателем 0,31%. Это в 4,8 раза больше доли региона с минимальным значением — Западной Европы.

Среди стран региона в тройке лидеров по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели: Руанда, Мавритания, Ливия. На четвертом месте — Габон.



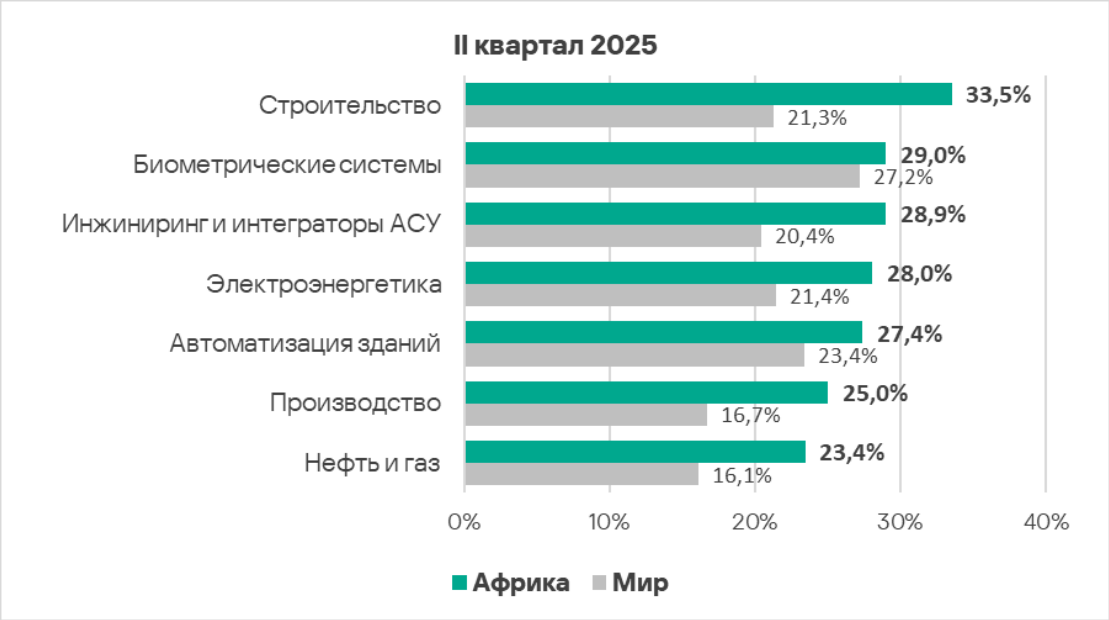
Доля атакованных вымогателями компьютеров АСУ выросла не во всех странах Африки, больше всего — в Габоне и Руанде. На диаграмме ниже показаны только те страны, где был отмечен рост показателя.



Отрасли

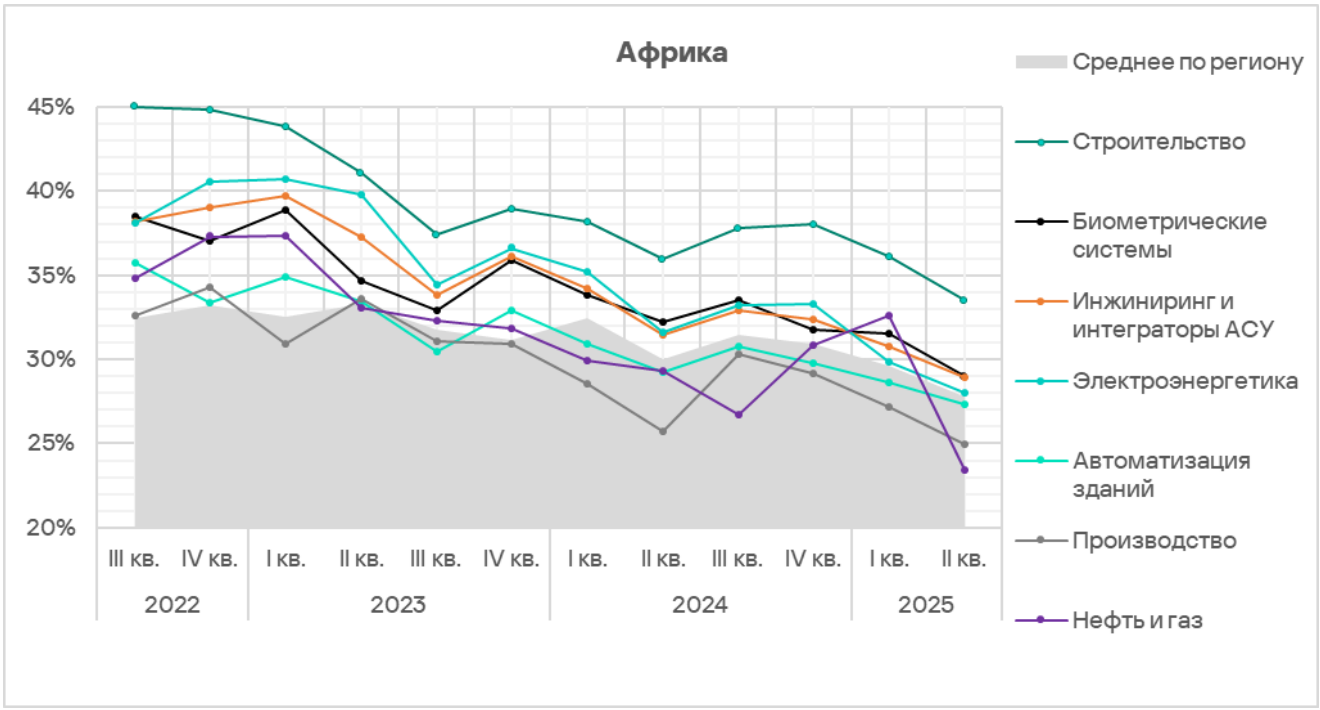
В Африке наиболее часто встречающейся с угрозами отраслью среди рассмотренных в отчете по-прежнему остается строительство.

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



Африка лидирует среди регионов по доле атакованных компьютеров АСУ, в следующих отраслях: строительство, инжиниринг и интеграторы АСУ, производство.

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 мы используем тепловые карты. На них ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В Африке максимальные значения наблюдаются для суммарных показателей по ряду отраслей: производство, строительство, инжиниринг и интеграторы АСУ.

На тепловых картах хорошо видны «горячие точки» отраслей — позиции источников и категорий вредоносного ПО, показатель по которым выше ожидаемого в соответствии с местом отрасли и местом угрозы или источника угрозы в соответствующих региональных рейтингах.

Показатели источников угроз в отраслях в Африке, II 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	10,78%	10,97%	13,60%	14,00%	11,18%	14,44%	11,68%	11,88%
Почтовые клиенты	6,87%	7,84%	2,97%	2,85%	0,97%	3,55%	3,81%	4,54%
Съемные носители	1,86%	1,26%	1,69%	1,94%	1,65%	1,85%	1,50%	1,77%
Сетевые папки	0,12%	0,03%	0,03%	0,04%	0,00%	0,09%	0,00%	0,04%
Показатель отрасли в регионе	29,00%	27,36%	28,00%	28,94%	23,42%	33,50%	24,96%	

Показатели категорий угроз в отраслях в Африке, II 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	5,71%	5,90%	8,94%	8,52%	7,09%	9,31%	7,88%	6,98%
Вредоносные скрипты и фишинговые страницы	10,20%	10,43%	8,30%	8,46%	6,12%	8,74%	7,43%	8,60%
Троянцы-шпионы, бэкдоры и кейлоггеры	8,42%	7,79%	6,72%	6,24%	4,28%	8,53%	4,96%	6,82%
Черви (Worm)	3,31%	2,88%	3,56%	3,16%	2,43%	4,19%	3,36%	3,13%
Майнеры — исполняемые файлы для ОС Windows	0,69%	0,82%	0,86%	1,02%	0,97%	1,09%	0,88%	0,78%
Вредоносные документы (MSOffice+PDF)	4,35%	4,72%	2,09%	1,95%	1,07%	1,97%	1,95%	2,85%
Вирусы (Virus)	3,28%	2,60%	3,53%	3,28%	3,40%	5,25%	2,92%	3,34%
Программы-вымогатели	0,45%	0,37%	0,19%	0,32%	0,19%	0,33%	0,27%	0,31%
Веб-майнеры, выполняемые в браузерах	0,62%	0,63%	0,59%	0,60%	0,87%	0,42%	0,53%	0,54%
Вредоносные программы для AutoCAD	0,17%	0,07%	0,24%	0,35%	0,49%	2,00%	0,44%	0,42%
Показатель отрасли в регионе	29,00%	27,36%	28,00%	28,94%	23,42%	33,50%	24,96%	

Для всех отраслей основной источник угроз — интернет. Как следствие, актуальны такие категории угроз как вредоносные скрипты и фишинговые страницы и опасные ссылки из списка запрещенных.

«Горячие точки» отраслей

Строительство

- Лидер среди отраслей по всем регионам по показателю угроз из интернета. Второе место в регионе по показателю угроз в сетевых папках. Третье место в регионе по доле компьютеров АСУ, на которых угрозы блокировались при подключении съемных носителей.
- Второе место среди отраслей во всех регионах по показателю ресурсов в интернете из списка запрещенных.
- Лидер среди отраслей региона по показателям сразу нескольких категорий: ресурсы в интернете из списка запрещенных, вирусы, черви, троянцы-шпионы, вредоносные программы для AutoCAD и майнеры-исполняемые файлы для ОС Windows.

Биометрические системы

- Лидер среди отраслей в регионе по показателю угроз в сетевых папках. Второе место в регионе по показателям угроз в почтовых клиентов и на съемных носителях.

- Лидер в регионе по показателям угроз из категории программ-вымогателей.
- Второе место среди отраслей в регионе по показателям в категориях вредоносные скрипты и фишинговые страницы, вредоносные документы.

Инжиниринг и интеграторы АСУ

- Лидер среди отраслей в регионе по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей. Второе место в регионе по показателю угроз из интернета, третье — по показателю угроз в сетевых папках.
- Второе место по показателям категорий майнеры — исполняемые файлы.
- Третье место по показателю ресурсов в интернете из списка запрещенных.

Электроэнергетика

- Третье место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета. Четвертое место в регионе по показателю угроз на съемных носителях.
- Второе место в регионе среди отраслей по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, черви и вирусы.
- Третье место среди отраслей в регионе по показателю вредоносных документов.
- Четвертое место в регионе по показателю шпионских программ.

Автоматизация зданий

- Лидер среди отраслей по показателю угроз из почтовых клиентов; на четвертом месте по показателю угроз в сетевых папках.
- Лидер среди отраслей в регионе по доле компьютеров АСУ, на которых блокировались вредоносные скрипты и фишинговые страницы, вредоносные документы.
- Второе место в регионе по доле компьютеров АСУ, на которых блокировались программы-вымогатели.
- Третье место по показателю веб-майнеров.

Производство

- Третье место среди отраслей региона по показателю угроз из почтовых клиентов. Четвертое — по показателю угроз из интернета в регионе.

- Третье место среди отраслей в регионе по показателям червей и вредоносных программ для AutoCAD.
- Четвертое место в регионе по показателю следующих категорий: ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows.

Нефтегазовая отрасль

- Лидер среди отраслей региона по показателю веб-майнеров.
- Второе место в регионе среди отраслей по показателю вредоносных программ для AutoCAD.
- Третье место в регионе среди отраслей по показателям следующих категорий: вирусы и майнеры-исполняемые файлы для ОС Windows.

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