Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Ближний Восток. Четвертый квартал 2025 года

24.04.2026 Версия 1.0

Ближний Восток

Основные проблемы кибербезопасности в регионе

Высокий риск целевых атак

На Ближнем Востоке значительно выше среднемировых значений доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, — в 1,8 раза.

Высокие показатели угроз, распространяющихся через почтовые клиенты (фишинг), шпионского ПО и программ-вымогателей — явные признаки высокой доступности технологических систем в регионе для продвинутых категорий злоумышленников.

О высоком риске целевых атак на технологические инфраструктуры промышленных предприятий в регионе свидетельствует, в том числе, высокий показатель вредоносных скриптов и фишинговых страниц, многие из которых нацелены на кражу данных аутентификации.

Недостаточная сегментация сети

На Ближнем Востоке значительно выше среднемировых значений доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, — в 1,8 раза.

Относительно высокие показатели самораспространяющегося ПО свидетельствуют о наличии значительной части инфраструктуры, не защищенной от вредоносного ПО, и недостаточной сегментации сети.

Показатель вирусов в регионе превышает среднемировой в 1,4 раза, показатель червей — в 1,6 раза.

Высокий показатель шпионских программ

Доля компьютеров АСУ, на которых блокируются шпионские программы, на Ближнем Востоке в 1,3 раза, а показатель вредоносных документов — в 1,5 раза выше, чем в среднем в мире.

Шпионские программы используются злоумышленниками для кражи конфиденциальных данных. А в целевых атаках — еще и для распространения по сети атакованной организации и загрузки вредоносного ПО финального этапа. В ряде случаев попадание на компьютер шпионского ПО заканчивается установкой программ-вымогателей.

Высокий показатель программ-вымогателей

Показатель программ-вымогателей в регионе стабильно высокий и почти вдвое превышает среднемировой.

В четвертом квартале 2025 года Ближний Восток вновь лидирует по показателю программ-вымогателей.

Ближний Восток занимает не ниже пятого места в рейтингах регионов по показателю программ-вымогателей во всех отраслях, кроме производства. В нефтегазовой отрасли по этому показателю Ближний Восток лидирует.

Яркие различия в некоторых странах региона

На Ближнем Востоке оказались страны с очень разной ситуацией в сфере промышленной кибербезопасности. Йемен по доле атакованных компьютеров АСУ занимает второе место в мире, Израиль входит в десятку самых безопасных стран.

Йемен лидирует в большинстве региональных рейтингов, в случае майнеров обеих категорий, червей, вирусов и программ-вымогателей — с большим отрывом от остальных стран. Исключение — угрозы из почты и категории угроз, которые распространяются преимущественно через почту.

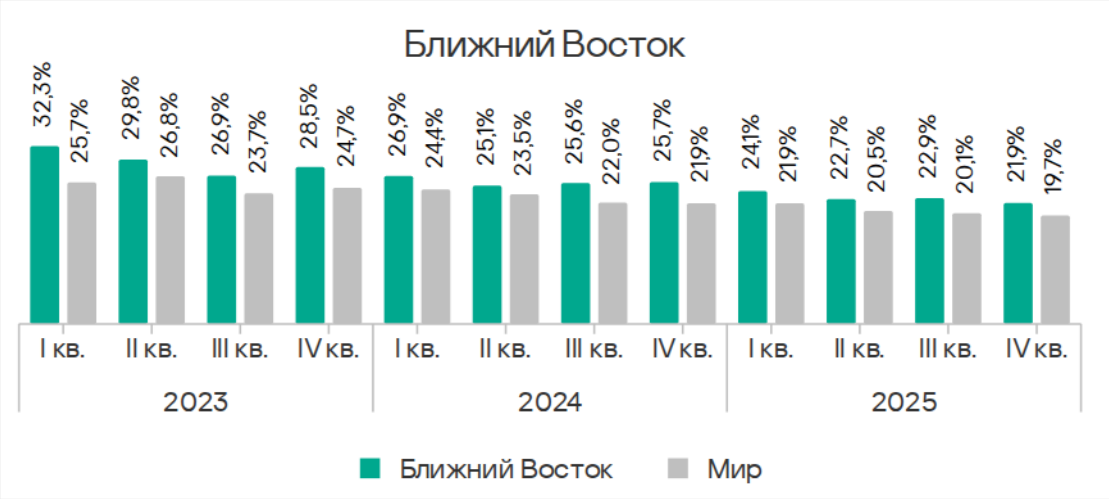
В рейтинге по угрозам из почтовых клиентов лидируют ОАЭ и Катар. Эти же страны занимают первые места в рейтингах по показателям категорий угроз вредоносные документы, вредоносные скрипты и фишинговые страницы и входят в топ-3 стран по показателям шпионских программ.

У Израиля в большинстве рейтингов — и часто с отрывом от остальных стран — показатель минимальный.

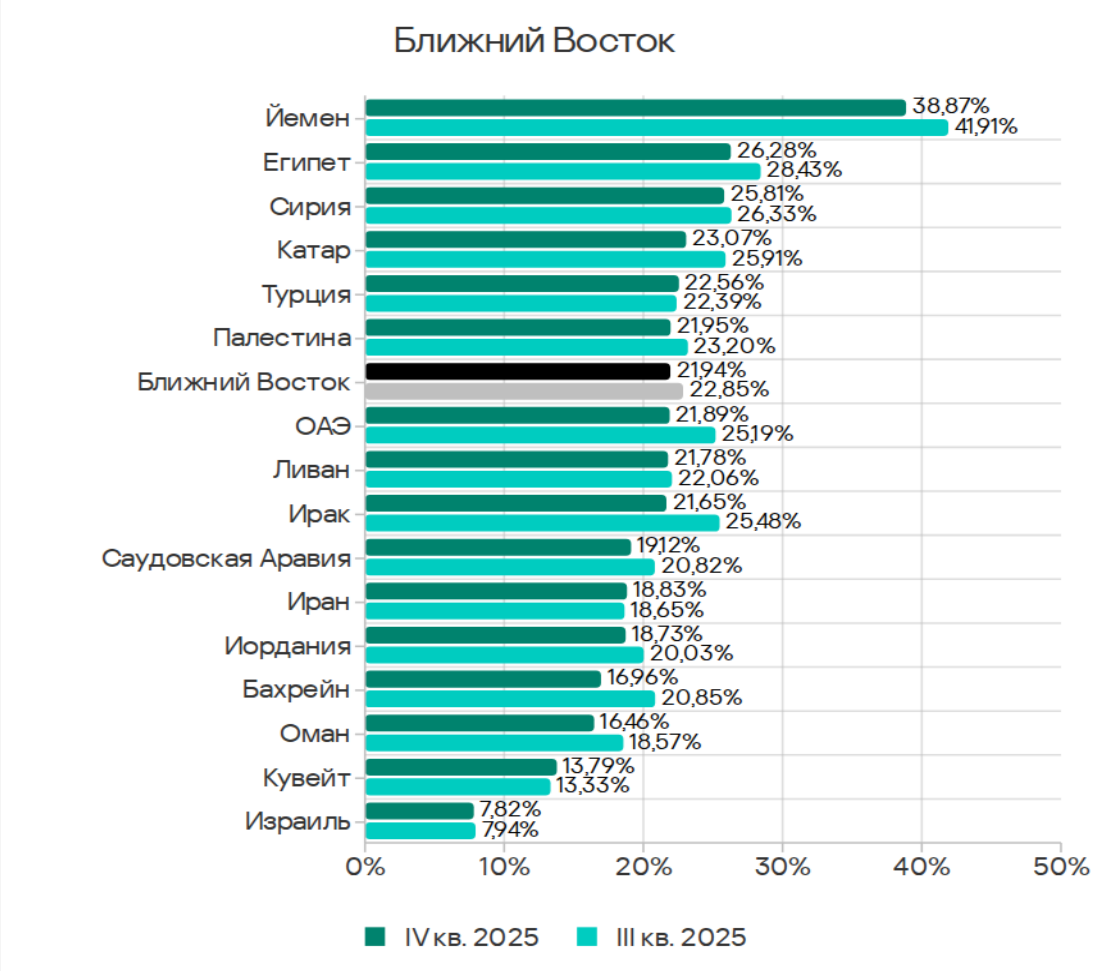
Статистика по всем угрозам

В четвертом квартале 2025 года Ближний Восток занял третье место в мире по доле компьютеров АСУ, на которых заблокированы вредоносные объекты. Показатель в регионе стабильно превышает среднемировое значение в 1,1 раза.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, на Ближнем Востоке за квартал уменьшилась до 21,9%. Это в 2,6 раза больше, чем в Северной Европе, где показатель минимальный.



Среди стран и территорий региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 7,82% в Израиле до 38,87% в Йемене. Показатели этих двух стран заметно отличаются от показателей остальных стран в регионе, которые попадают в диапазон от 13% до 27%.



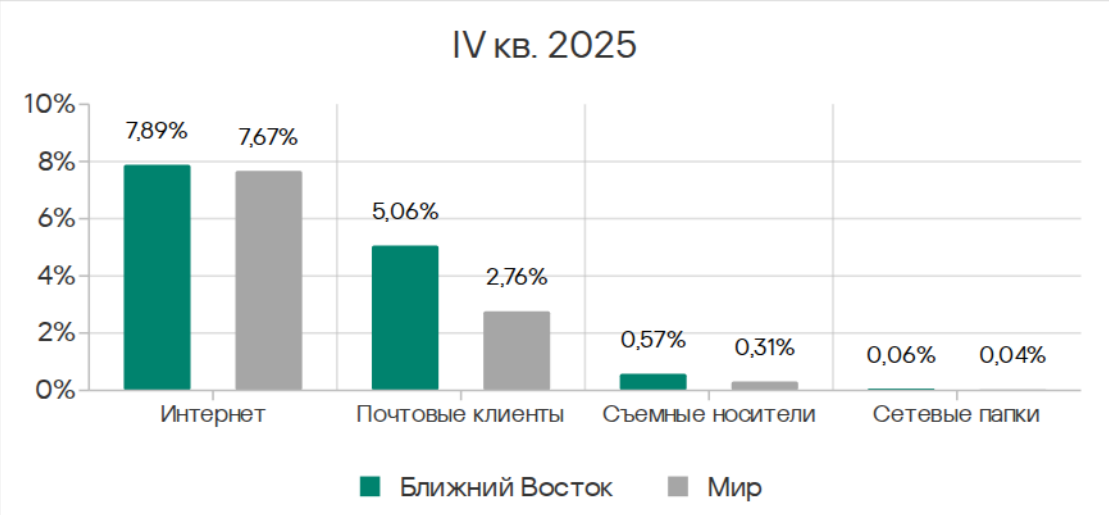
Йемен лидирует в большинстве региональных рейтингов как по источникам, так и по категориям вредоносного ПО. По показателям угроз из почты, категорий вредоносные документы, вредоносные скрипты и фишинговые страницы, вредоносные программы для AutoCAD — лидируют ОАЭ.

Израиль большинство региональных рейтингов замыкает.

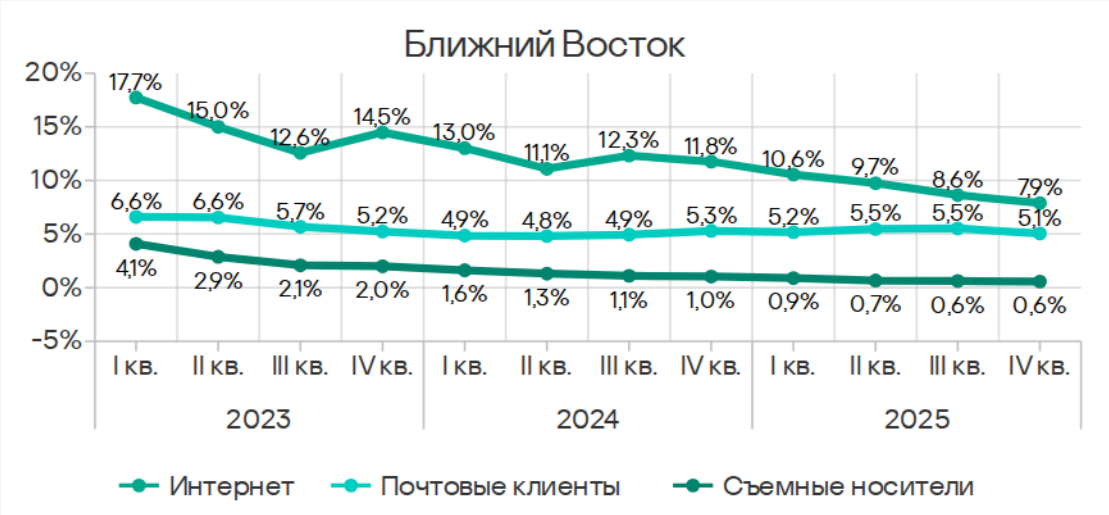
Источники угроз

Доля компьютеров АСУ, на которых угрозы были заблокированы из разных источников, на Ближнем Востоке выше среднемировых показателей у всех источников. Значительно превышает среднемировые значения доля компьютеров АСУ, на которых были заблокированы:

- угрозы из почтовых клиентов — в 1,8 раза;
- угрозы на съемных носителях — в 1,8 раза;
- угрозы в сетевых папках — в 1,5 раза.



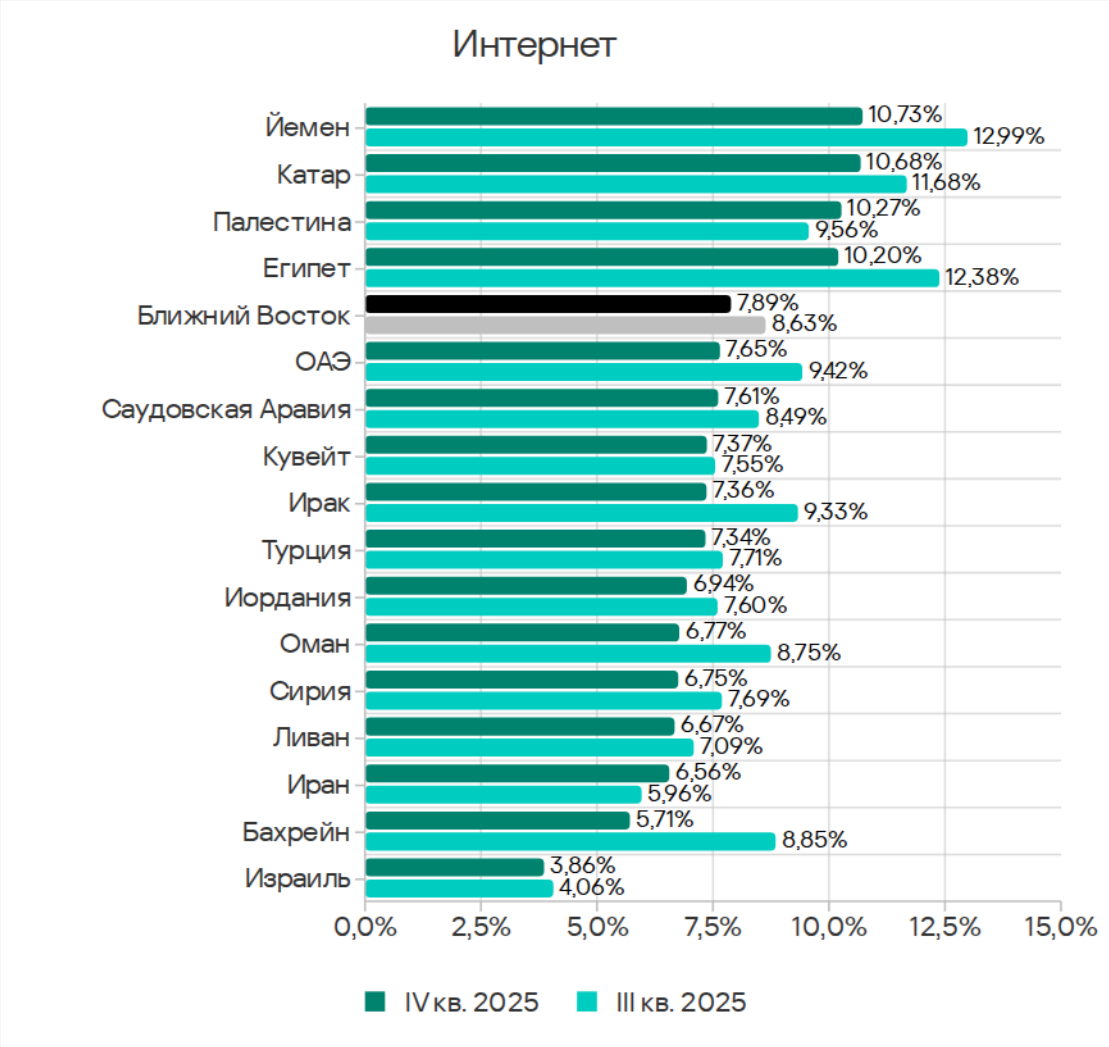
Доля атакованных компьютеров АСУ в четвертом квартале 2025 года уменьшилась у всех источников угроз.



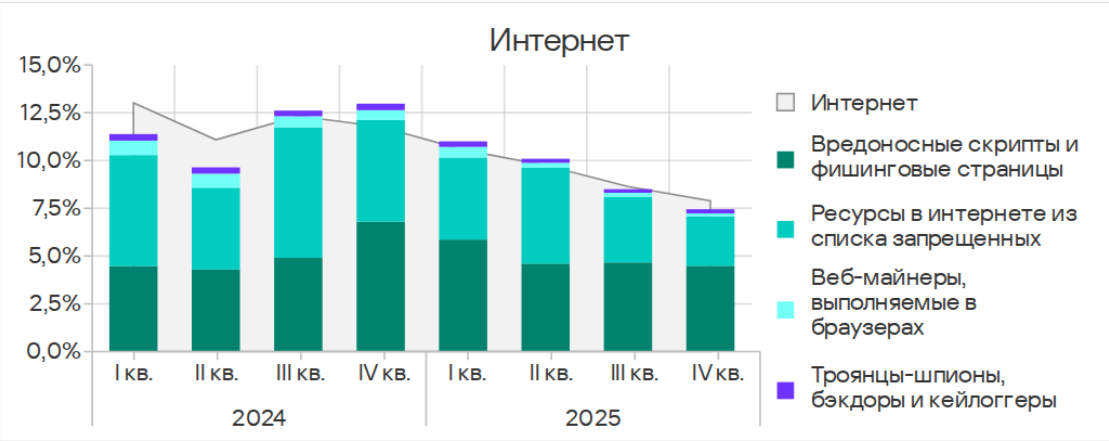
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Ближний Восток в четвертом квартале 2025 года занял шестое место в рейтинге регионов с показателем 7,89%, который превышает минимальный — у Северной Европы — в 2,0 раза.

Показатели стран и территорий региона варьируют от 3,86% в Израиле до 10,73% в Йемене.

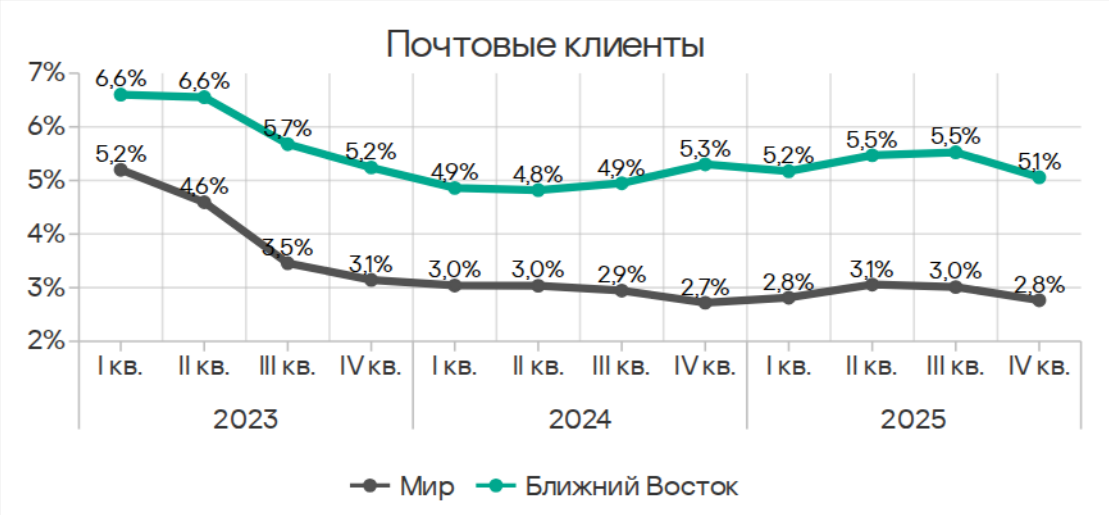


Основные категории угроз из интернета, которые блокируются на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.

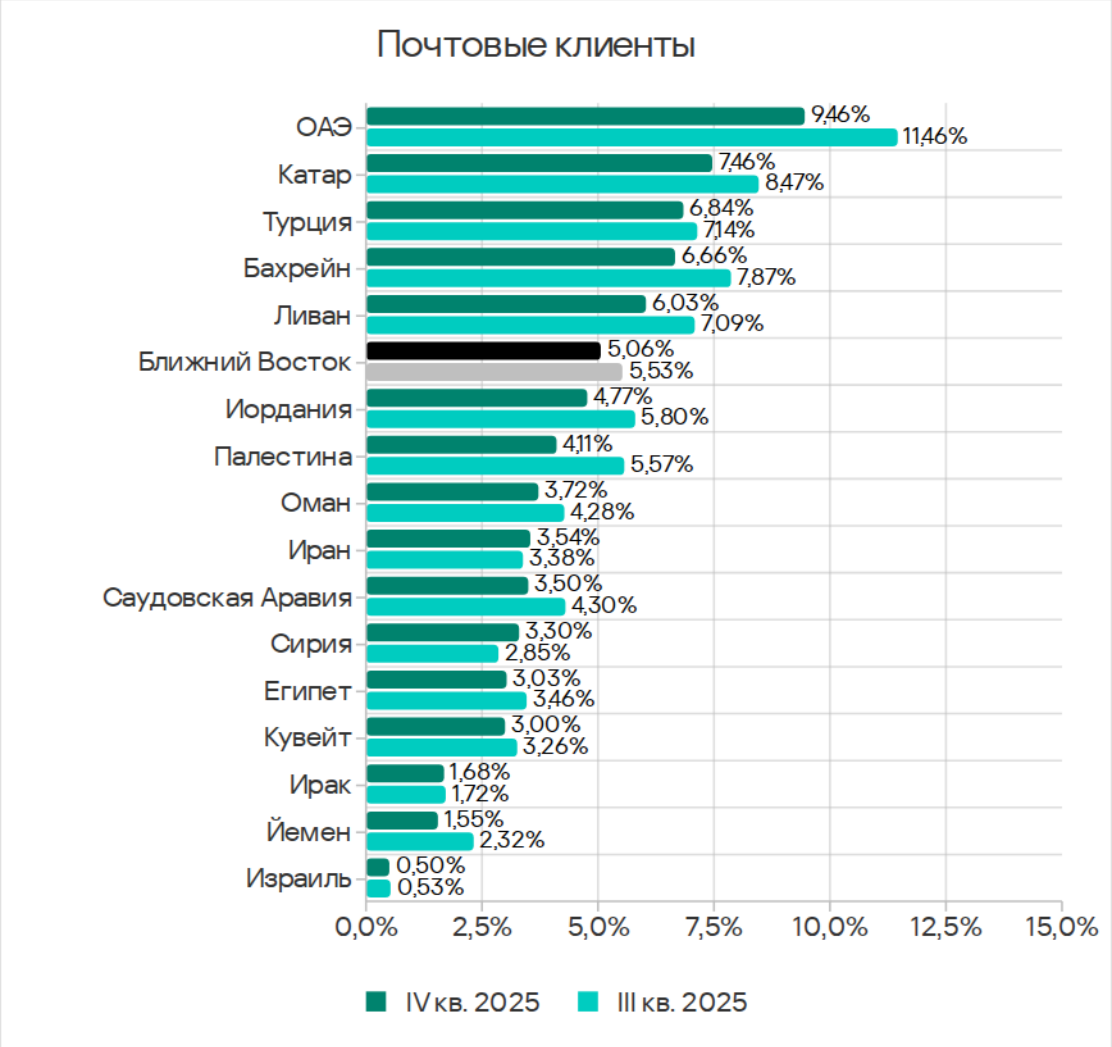


Почтовые клиенты

В рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в четвертом квартале 2025 года Ближний Восток опустился со второго на третье место. Показатель в регионе уменьшился до 5,06%. Это в 7,9 раза больше, чем в Северной Европе, где уровень угроз из почтовых клиентов минимальный.

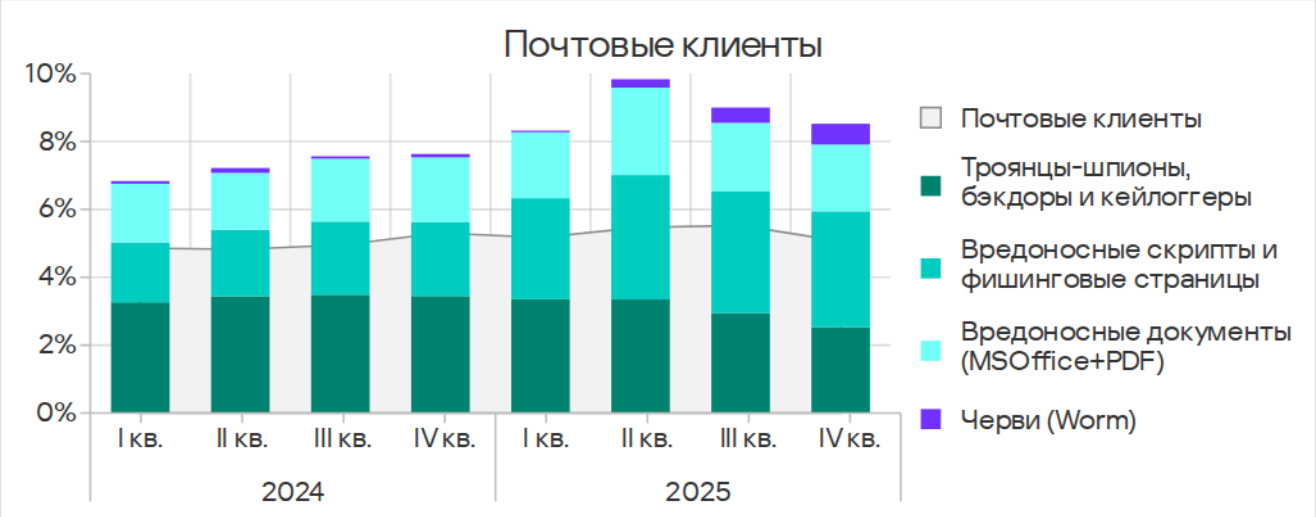


Среди стран и территорий региона по этому показателю стабильно лидируют ОАЭ, в четвертом квартале — с 9,46%. Меньше всего доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в Израиле — 0,50%. Отметим, что Йемен, который лидирует по показателям остальных источников угроз, в этом рейтинге занимает предпоследнее место.



Две страны-лидера этого рейтинга — ОАЭ и Катар — также занимают первые места в рейтингах по вредоносным документам и вредоносным скриптам и фишинговым страницам. В рейтинге по показателям шпионских программ они находятся на второй и третьей позициях.

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



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это связано с очередной волной фишинговых атак, известных как Curriculum-vitae-catalina, затронувших все регионы мира. На Ближнем Востоке пик атак пришелся на ноябрь.

В ходе атак злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm), замаскированный под резюме (Curriculum Vitae). При запуске файла происходило заражение системы.

Как правило такие кампании направлены на доставку вредоносного ПО для кражи данных, программ-шпионов или инструментов для удаленного управления (RAT).

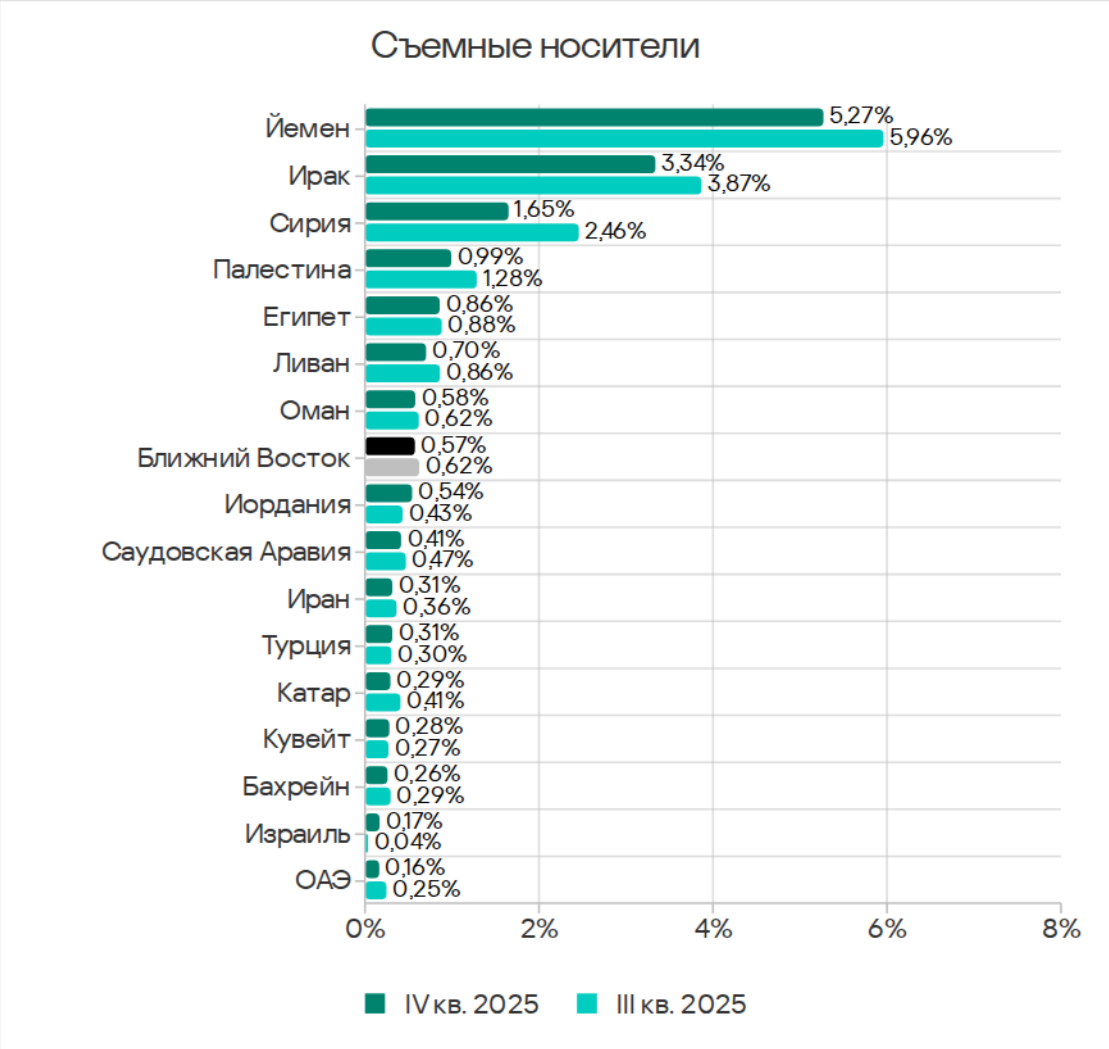
Самая высокая доля компьютеров АСУ, на которых был обнаружен Backdoor.MSIL.XWorm, отмечен в регионах, где традиционно высока доля компьютеров АСУ, на которых блокируются угрозы из почты, — в Южной Европе, Южной Америке и на Ближнем Востоке.

Съемные носители

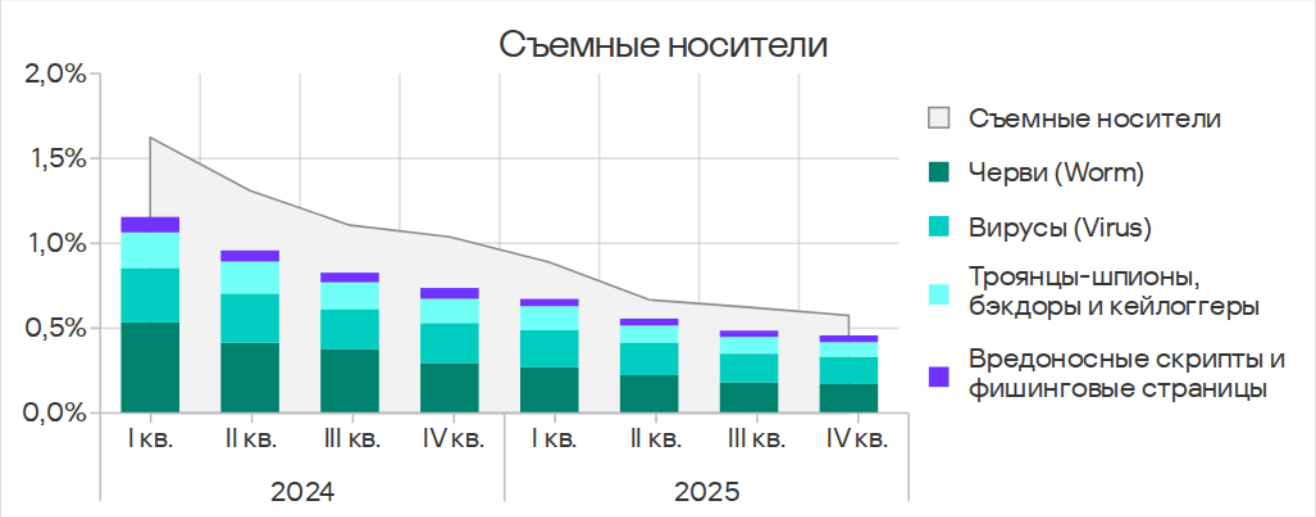
По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, в четвертом квартале 2025 года Ближний Восток занимает третье место среди регионов с 0,57%. Это в 11,4 раза больше, чем в регионе Австралия и Новая Зеландия, который занимает последнее место в соответствующем рейтинге.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей,

лидируют Йемен с 5,27% и Ирак с 3,34%. Показатели остальных стран варьируют от 0,16% в ОАЭ до 1,65% в Сирии.



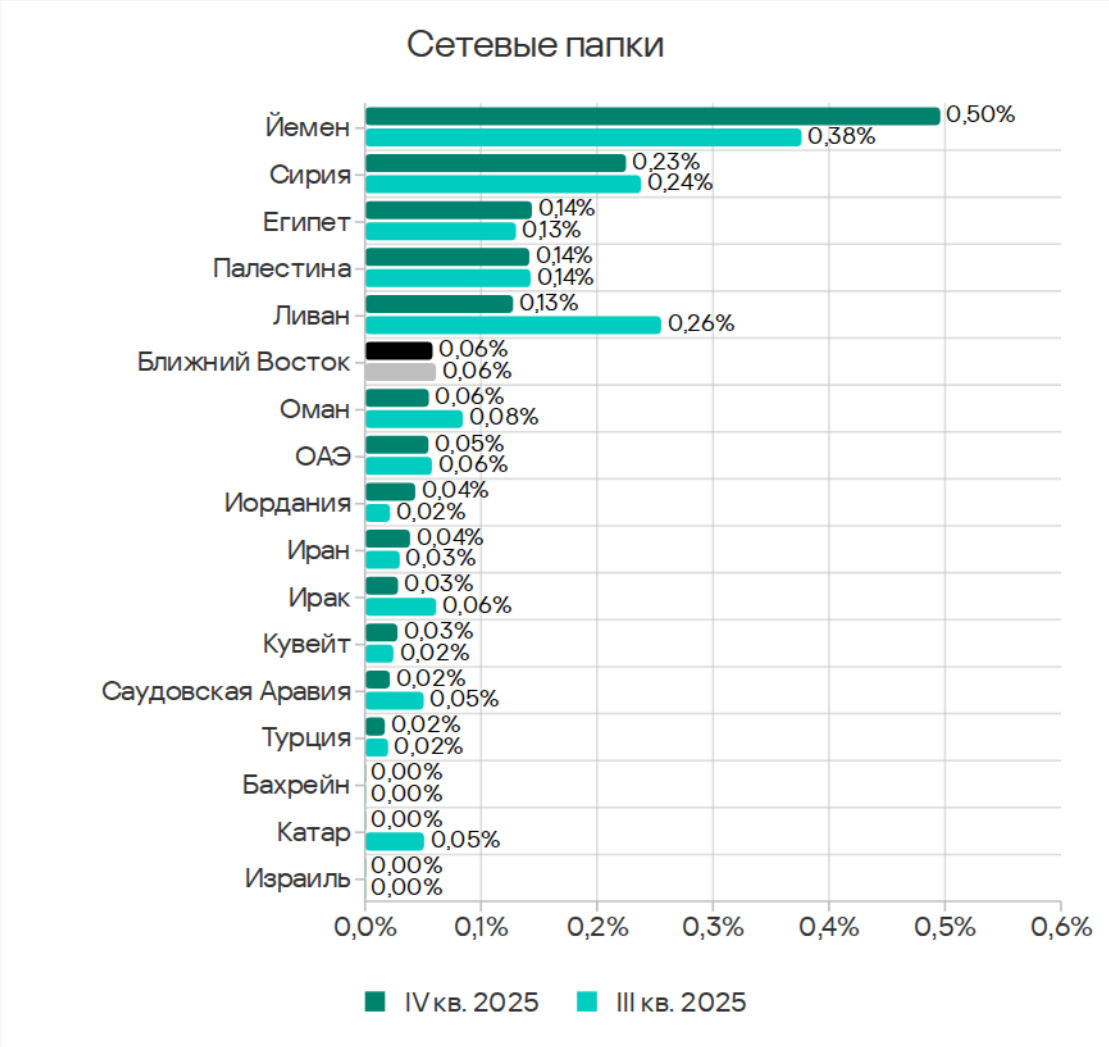
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионское ПО. По доле компьютеров АСУ, на которых были заблокированы черви, Ближний Восток занимает второе место среди регионов.



Сетевые папки

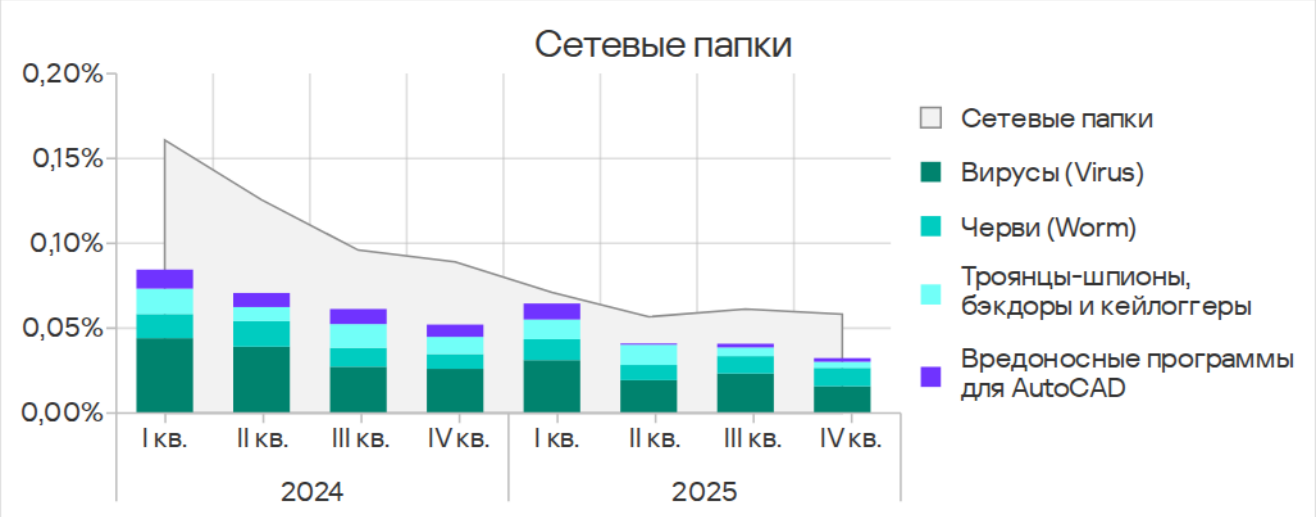
По доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, в четвертом квартале 2025 года Ближний Восток занимает третье место среди регионов с 0,06%. С регионом Северная Европа, который занимает последнее место в рейтинге, показатели отличаются в 8,3 раза.

Среди стран и территорий региона по показателю угроз в сетевых папках с большим отрывом лидирует Йемен с 0,50%.



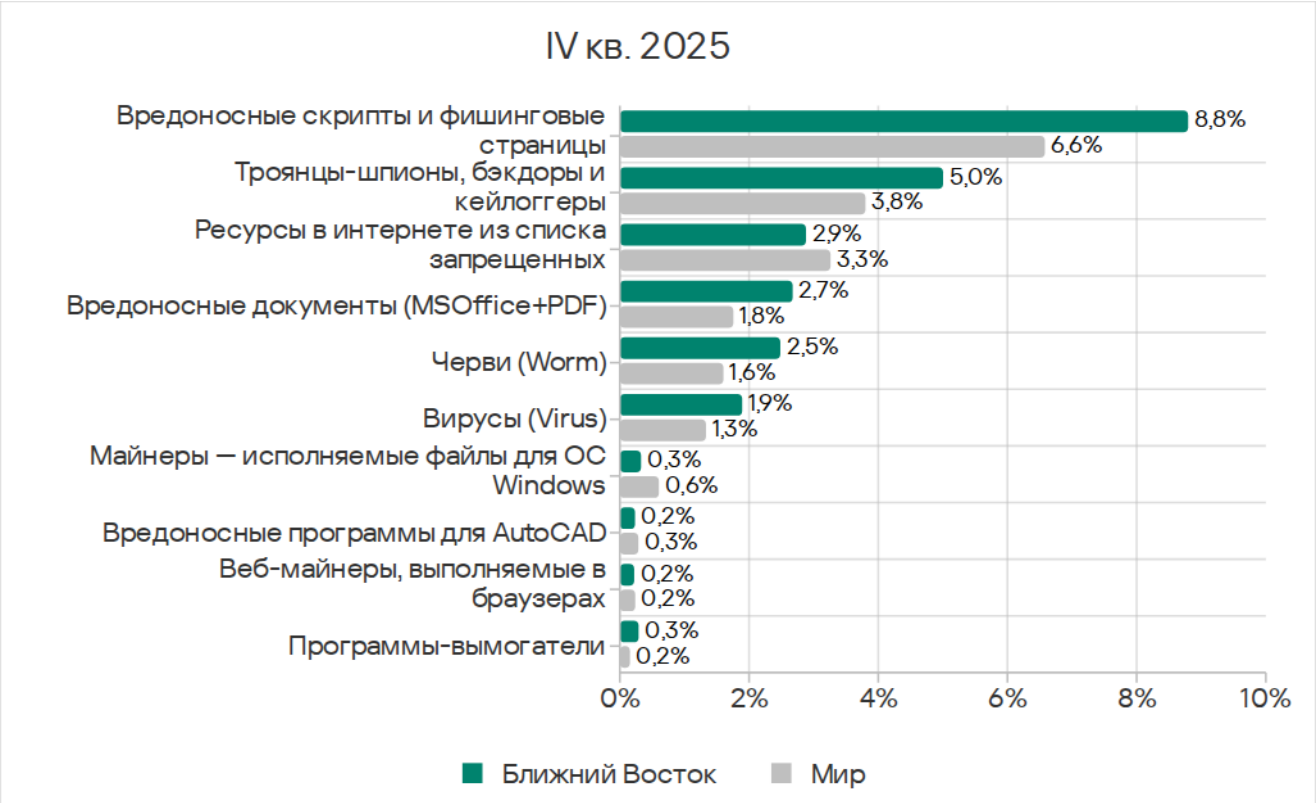
Отметим, что угрозы в сетевых папках обнаружены не во всех странах региона.

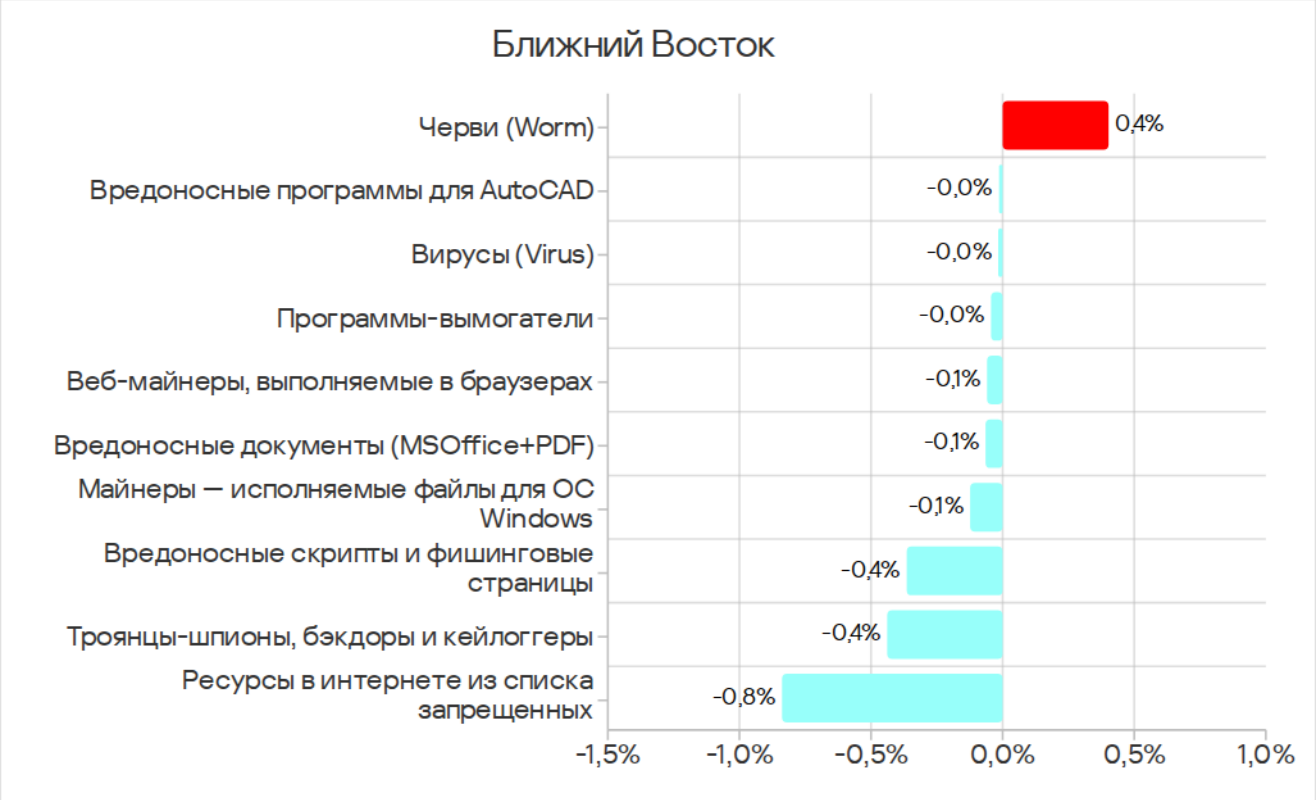
Основные категории угроз, которые распространяются через сетевые папки: вирусы, черви и шпионские программы.



Категории угроз

На Ближнем Востоке доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения у всех категорий, кроме ресурсов в интернете из списка запрещенных, майнеров обеих категорий, а также вредоносных программ для AutoCAD.





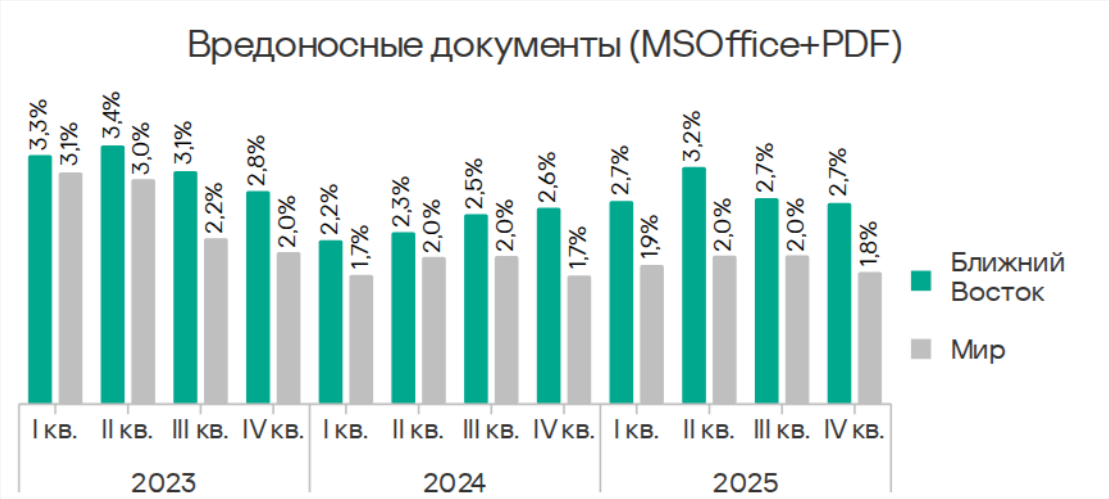
Наибольшая разница по сравнению со среднемировыми значениями у региональных показателей угроз следующих категорий:

- программы-вымогатели — в 1,8 раза, первое место среди регионов.
- черви — в 1,6 раза, второе место среди регионов;
- вредоносные документы — в 1,5 раза, четвертое место среди регионов;
- вирусы — в 1,4 раза, четвертое место среди регионов;
- шпионские программы — в 1,3 раза, четвертое место среди регионов;
- вредоносные скрипты и фишинговые страницы — в 1,3 раза, пятое место среди регионов.

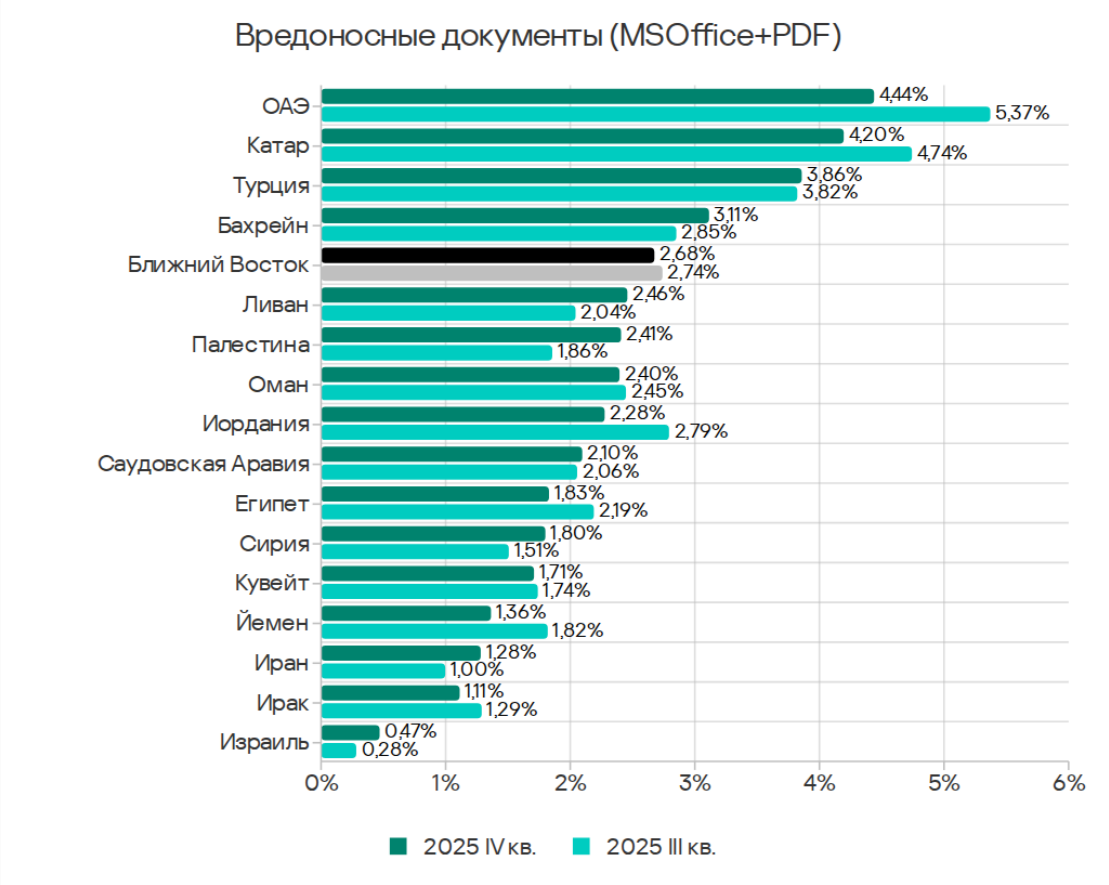
Вредоносные документы

В четвертом квартале 2025 года Ближний Восток по доле компьютеров АСУ, на которых блокируются вредоносные документы, занимает четвертое место среди регионов с 2,68%. Это в 5,8 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе росла со второго квартала 2024 года, но в последние два квартала 2025 года показатель за квартал уменьшался.



Среди стран и территорий региона по этому показателю лидируют ОАЭ с 4,44%. Рейтинг замыкает Израиль с 0,47%.



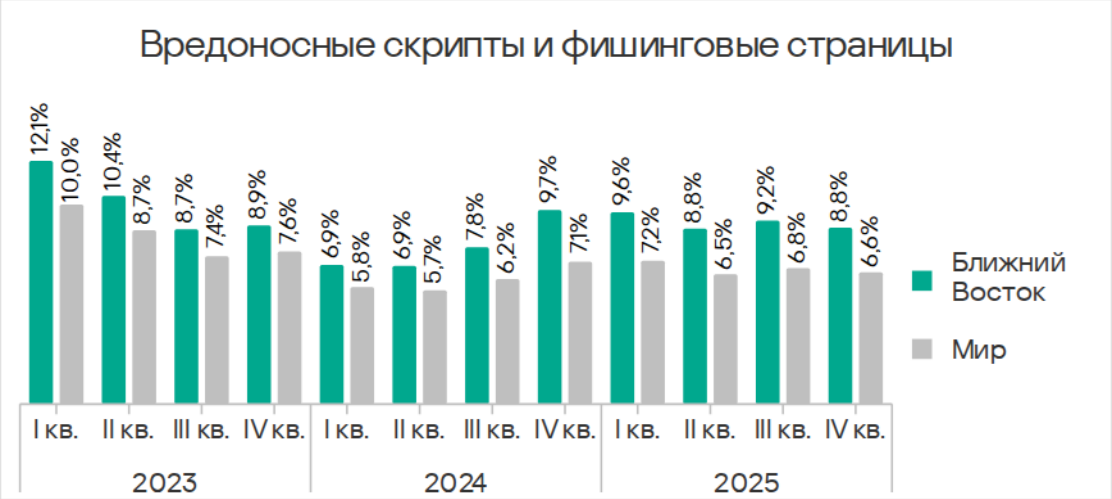
Распространяются вредоносные документы преимущественно по электронной почте.

Две страны, лидирующие в этом рейтинге — ОАЭ и Катар, — возглавляют также рейтинги по вредоносным скриптам и фишинговым страницам,

вредоносным документам и по угрозам из почтовых клиентов. Они же входят в тройку стран — лидеров по доле компьютеров АСУ, где были заблокированы шпионские программы.

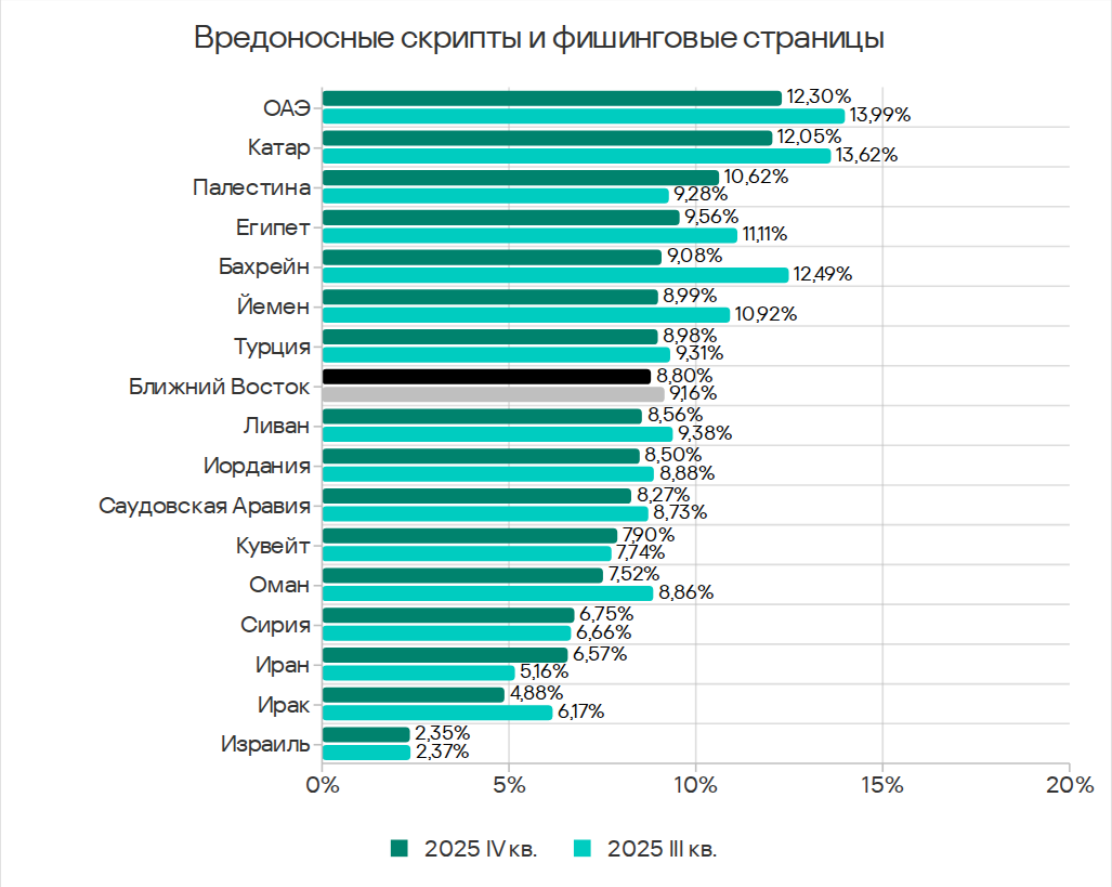
Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Ближний Восток занимает в соответствующем рейтинге регионов пятое место с 8,80%. Этот показатель в 3,5 раза больше, чем в Северной Европе, которая замыкает рейтинг.



Распространяется эта угроза в интернете и по электронной почте.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидируют ОАЭ с 12,30%. Наименьший показатель — в Израиле (2,35%).

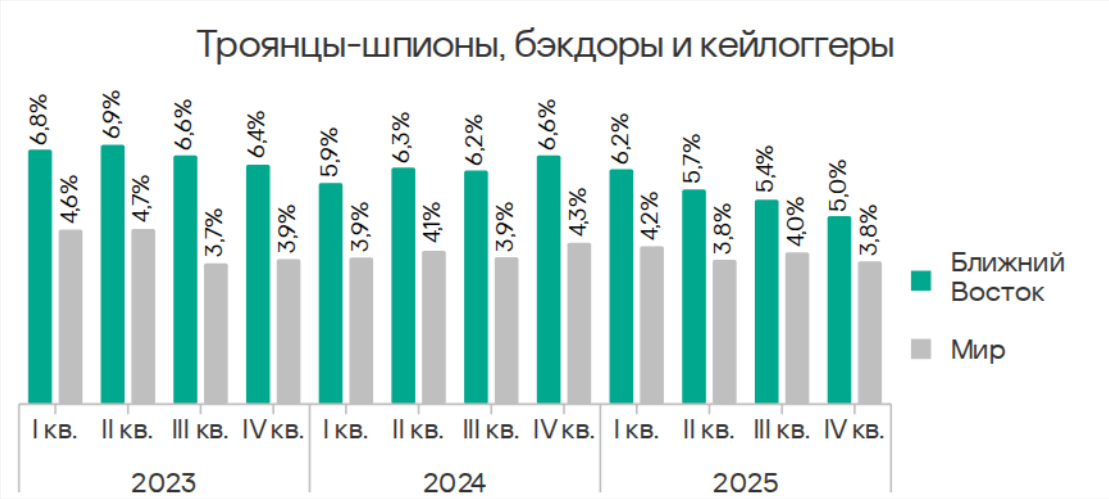


Две страны, лидирующие в этом рейтинге — ОАЭ и Катар, — возглавляют также рейтинг по показателям вредоносных документов и рейтинг стран региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах. Они же входят в тройку стран-лидеров по шпионским программам (возглавляет этот рейтинг Йемен).

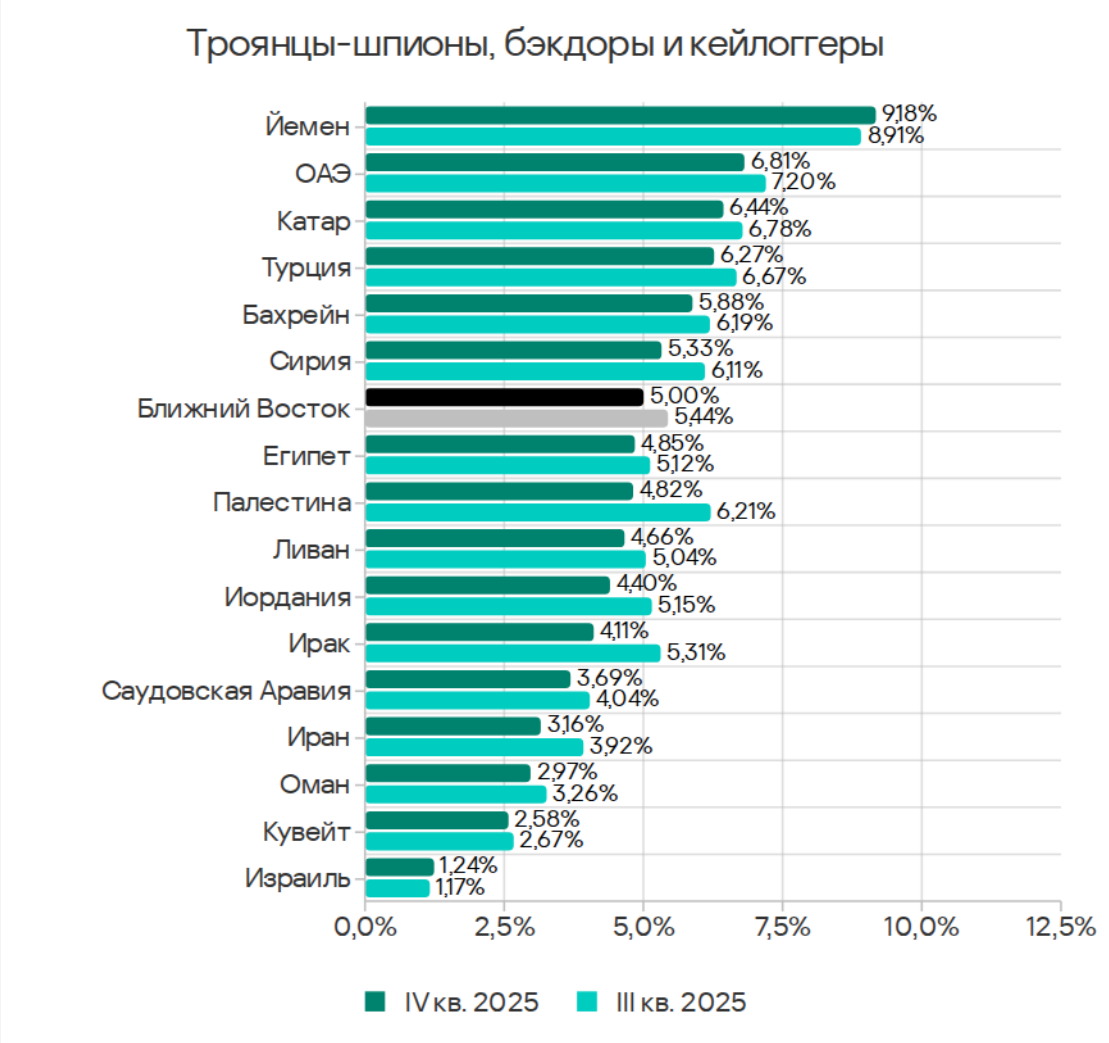
Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, Ближний Восток находится на четвертом месте с 5,00%. Это в 4,0 раза больше, чем в Северной Европе, где этот показатель наименьший.

На Ближнем Востоке доля компьютеров АСУ, на которых блокируются шпионские программы, снижалась в течение всего 2025 года, в четвертом квартале она была минимальной за три года.



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются шпионские программы, в четвертом квартале 2025 года лидирует Йемен с 9,18%. Наименьший показатель — в Израиле (1,24%).



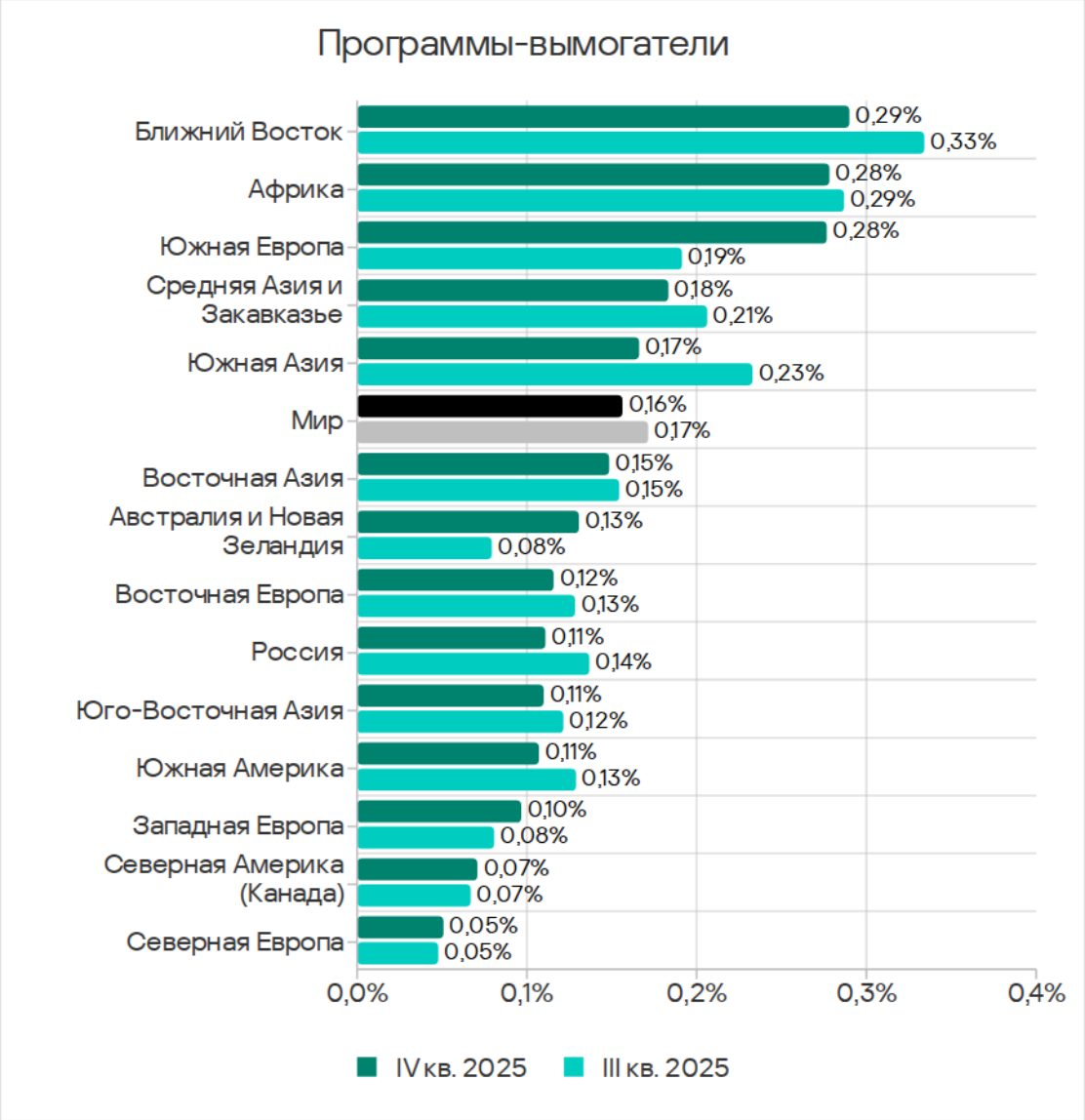
Шпионские программы в регионе блокируются во всех источниках угроз, но чаще всего они распространяются через почтовые клиенты.

Две страны из тройки лидеров в рейтинге по шпионским программам — ОАЭ и Катар — оказались также лидерами рейтинга по угрозам из почтовых клиентов. Они же лидируют среди стран региона по доле компьютеров АСУ, где были заблокированы вредоносные документы, а также вредоносные скрипты и фишинговые страницы.

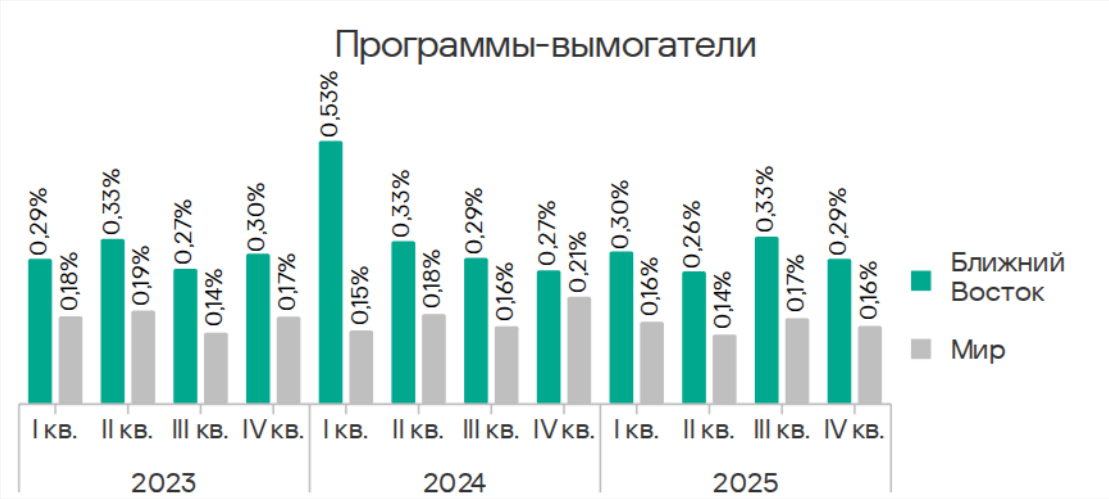
Шпионские программы используются злоумышленниками для кражи конфиденциальных данных, а в случае целевых атак еще и для распространения по сети атакованной организации и загрузки вредоносного ПО финального этапа. В ряде случаев попадание на компьютер шпионского ПО заканчивается установкой программ-вымогателей.

Программы-вымогатели

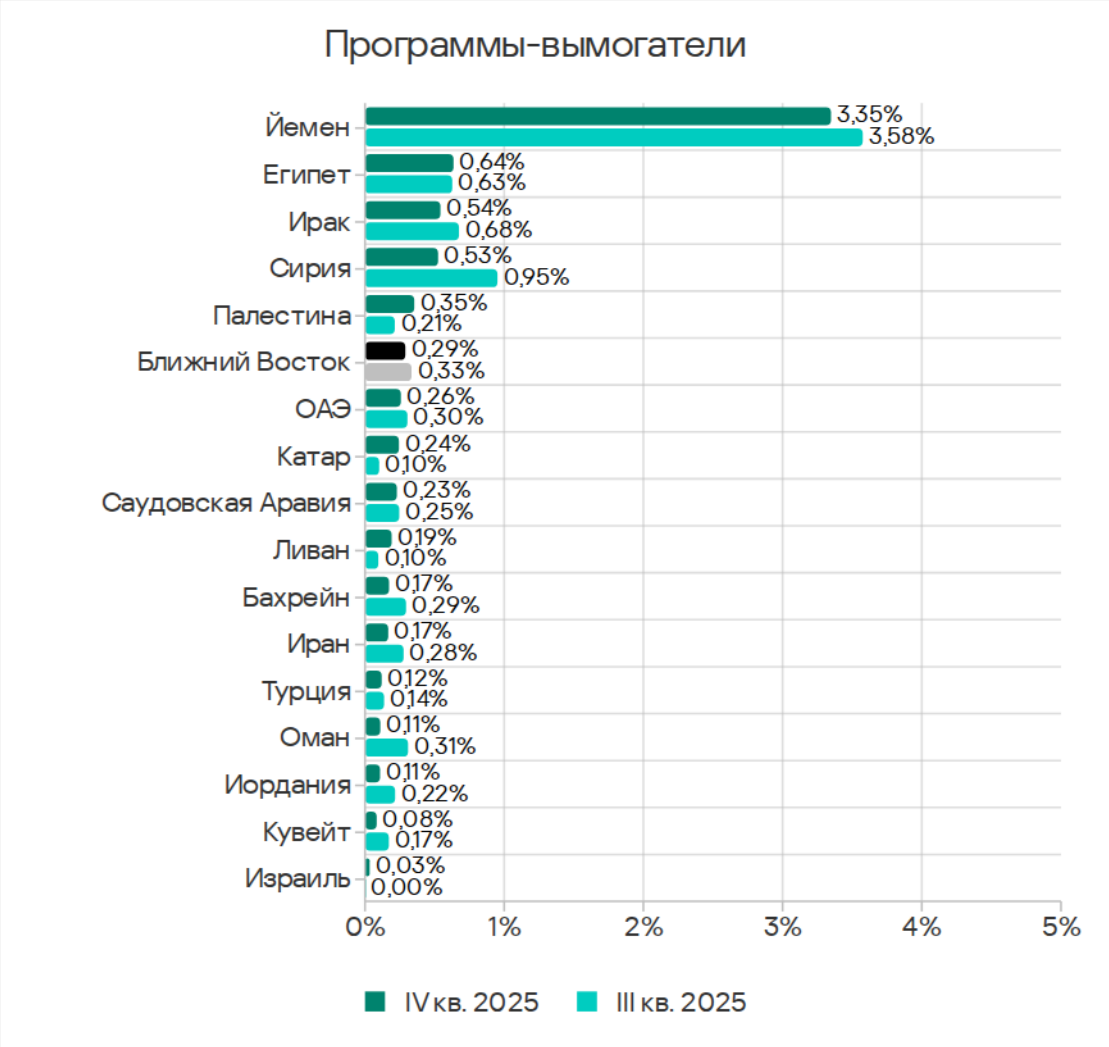
В четвертом квартале 2025 года Ближний Восток сохранил первенство среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели.



Показатель в регионе с 2023 года колеблется в диапазоне от 0,26% до 0,33%. В четвертом квартале 2025 года он уменьшился до 0,29%. Это в 5,8 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.



Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, с огромным отрывом лидирует Йемен с гигантским для этой категории угроз показателем 3,35%. В остальных странах значения попадают в диапазон от 0,64% в Египте до 0,03% в Израиле.



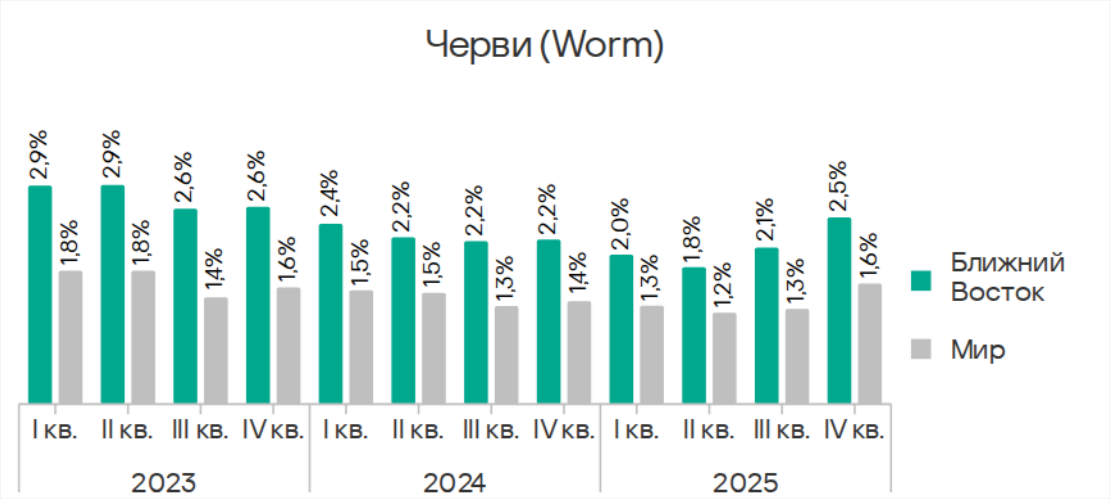
В регионе эта угроза чаще всего распространяется через почтовые клиенты и на съемных носителях.

Черви

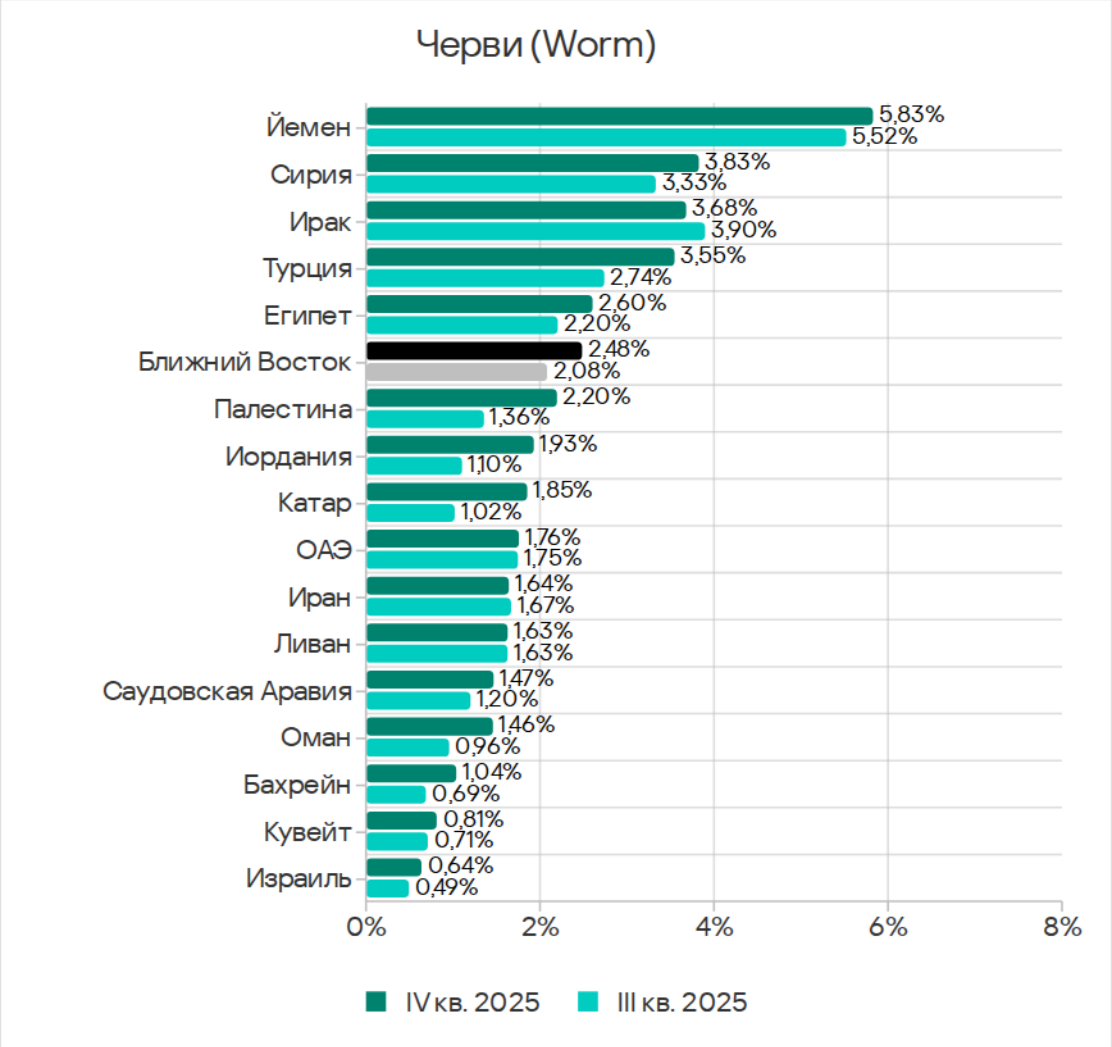
По доле компьютеров АСУ, на которых блокируются черви, Ближний Восток занимает второе место среди регионов с 2,48%. Это в 7,8 раза больше, чем в Северной Европе, регионе с минимальным показателем.

В четвертом квартале 2025 года в результате волны фишинговых атак, в ходе которых распространялся червь-бэкдор Backdoor.MSIL.XWorm, доля компьютеров АСУ, на которых были заблокированы черви, выросла во всех регионах.

Черви — единственная категория угроз на Ближнем Востоке, показатель которой в четвертом квартале 2025 года увеличился. По его росту Ближний Восток находится на четвертом месте среди регионов.



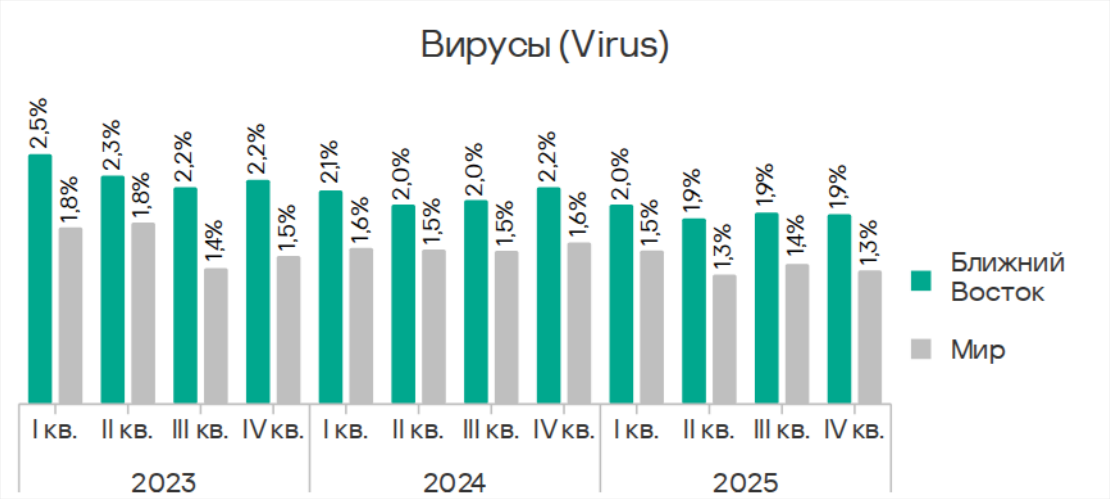
Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются черви, с большим отрывом лидирует Йемен с 5,83%. Отметим, что показатель за квартал вырос во всех странах, за несколькими исключениями: в Ливане он не изменился, а в Иране и Ираке уменьшился.



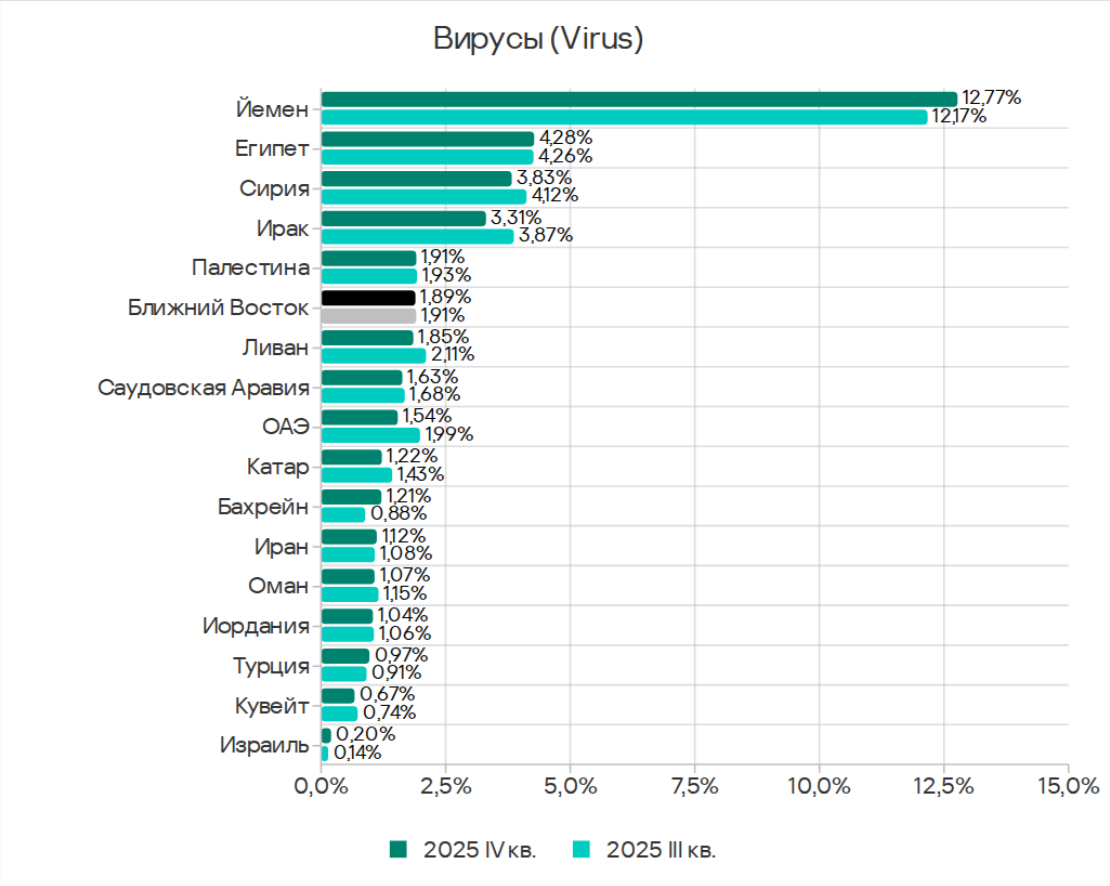
Вирусы

Ближний Восток находится на четвертом месте среди регионов по показателю вирусов.

Доля компьютеров АСУ, на которых блокируются вирусы, в регионе уменьшилась до 1,89%. Это в 12,6 раза больше, чем в Западной Европе, где этот показатель — наименьший из всех регионов.



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются вирусы, с большим отрывом лидирует Йемен с 12,77%. Показатель Йемена втрое превышает показатель следующей в рейтинге страны — Египет. По сравнению же с показателем Израиля, который замыкает рейтинг, значение в Йемене больше в 63,9 раза.

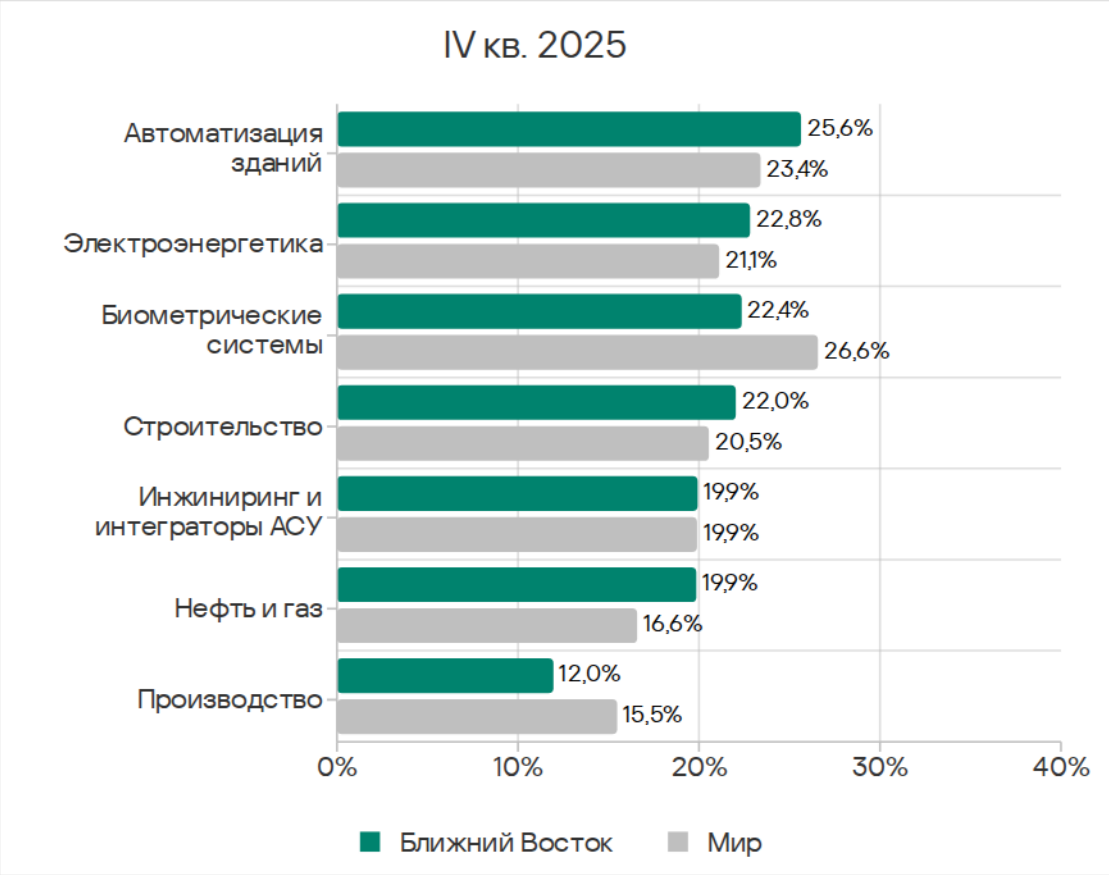


Отрасли

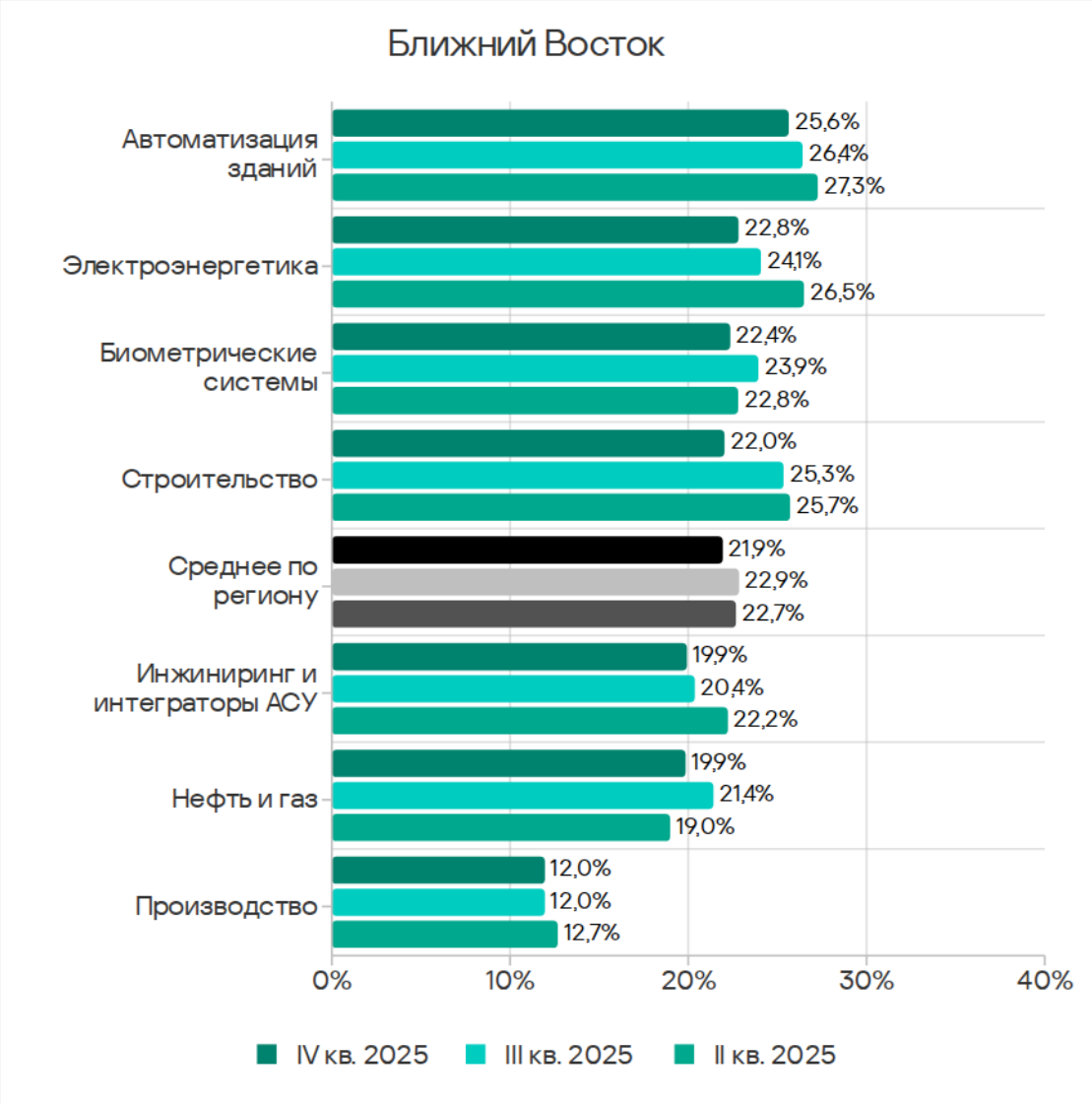
Среди рассмотренных в отчете отраслей чаще всего с угрозам встречается автоматизация зданий.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает среднемировые значения в следующих отраслях:

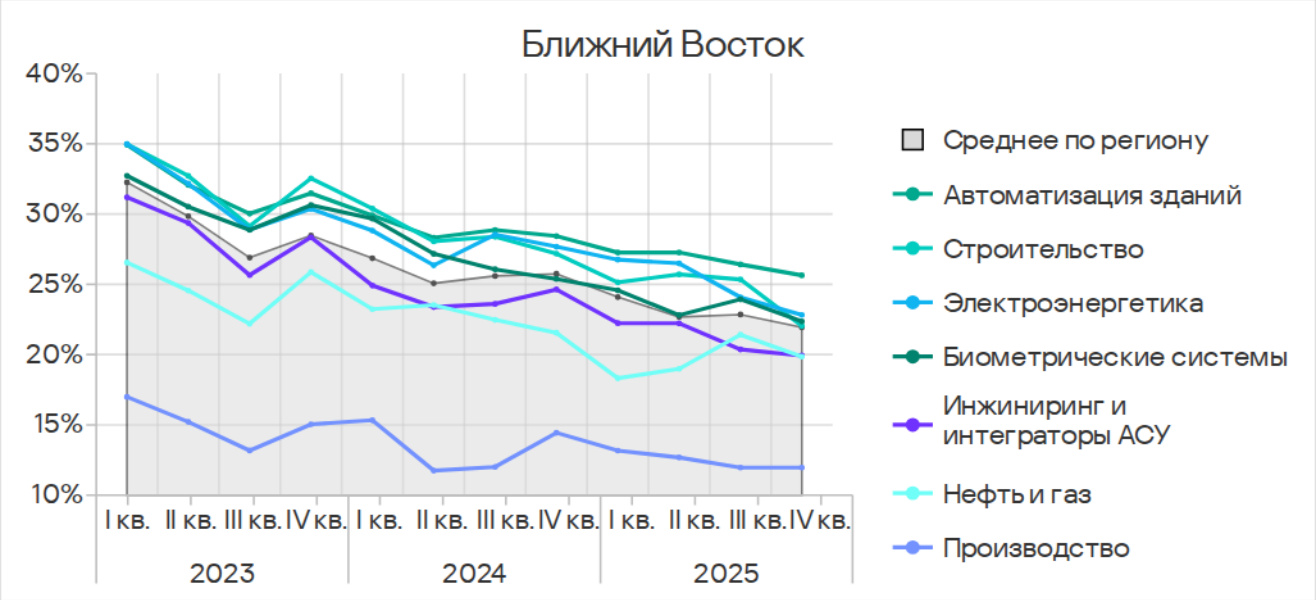
- автоматизация задний — в 1,1 раза;
- электроэнергетика — в 1,1 раза;
- строительство — в 1,1 раза;
- нефть и газ — в 1,2 раза.



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех отраслях, кроме производства, где показатель не изменился.



Несмотря на периодические колебания, тренды демонстрируют в целом положительную динамику (показатели снижаются).



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 на Ближнем Востоке, 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	7,49%	8,55%	7,86%	8,71%	6,94%	8,88%	4,67%	7,89%
Почтовые клиенты	4,60%	7,57%	3,57%	3,71%	2,03%	4,48%	1,92%	5,06%
Съемные носители	1,21%	0,66%	0,42%	0,55%	0,39%	0,41%	0,35%	0,57%
Сетевые папки	0,13%	0,08%	0,04%	0,04%	—	0,06%	—	0,06%
Показатель отрасли в регионе	22,36%	25,64%	19,93%	22,82%	19,85%	22,03%	11,96%	

Показатели категорий угроз в отраслях на Ближнем Востоке, 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	3,05%	3,10%	2,94%	3,05%	2,93%	2,69%	1,92%	2,88%
Вредоносные скрипты и фишинговые страницы	8,41%	11,43%	7,28%	7,80%	5,53%	8,88%	4,29%	8,80%
Вредоносные документы (MSOffice+PDF)	3,23%	4,18%	1,70%	2,25%	1,02%	1,83%	0,92%	2,68%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,75%	7,26%	3,60%	4,36%	1,97%	3,60%	2,05%	5,00%
Программы-вымогатели	0,53%	0,45%	0,15%	0,34%	0,17%	0,21%	0,06%	0,29%
Майнеры — исполняемые файлы для ОС Windows	0,32%	0,36%	0,40%	0,34%	0,28%	0,43%	0,19%	0,33%
Веб-майнеры, выполняемые в браузерах	0,29%	0,20%	0,28%	0,25%	0,34%	0,40%	0,13%	0,22%
Вредоносные программы для AutoCAD	0,18%	0,20%	0,23%	0,13%	0,17%	1,02%	0,16%	0,23%
Черви (Worm)	2,44%	3,46%	1,98%	2,46%	1,35%	1,39%	1,48%	2,48%
Вирусы (Virus)	2,84%	2,55%	1,23%	1,97%	1,97%	1,81%	1,04%	1,89%
Показатель отрасли в регионе	22,36%	25,64%	19,93%	22,82%	19,85%	22,03%	11,96%	

Основные проблемы в отраслях региона

Высокий показатель программ-вымогателей. Ближний Восток занимает первое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются программы-вымогатели. Во всех отраслях, кроме производства, по этому показателю Ближний Восток занимает не ниже пятого места в соответствующих рейтингах регионов.

Высокий уровень угроз из почтовых клиентов. Эта проблема актуальна для нескольких отраслей. По доле компьютеров АСУ, на которых были

заблокированы угрозы из почтовых клиентов в различных отраслях, Ближний Восток среди регионов занимает:

- первое место в электроэнергетике, кроме того, в этой отрасли регион находится на втором месте по показателям вредоносных документов;
- второе место в нефтегазовой и строительной отраслях;
- третье место в отраслях автоматизация зданий и инжиниринг и интеграторы АСУ.

Актуальность съемных носителей как источника угрозы для инфраструктуры биометрических систем, отраслей инжиниринг и интеграторы АСУ и нефтегазовой отрасли. По показателям угроз на съемных носителях в этих отраслях Ближний восток занял третье место среди регионов. По показателю червей в отрасли инжиниринг и интеграторы АСУ Ближний Восток на втором месте среди регионов.

Автоматизация зданий

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

Среди регионов по показателям в отрасли Ближний Восток занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- третье место по показателям угроз из почтовых клиентов;
- второе место по доле компьютеров АСУ, на которых блокируются программы-вымогатели;
- третье место по показателю следующих категорий: вредоносные документы, шпионские программы и вредоносные программы для AutoCAD.

Среди отраслей в регионе у отрасли автоматизация зданий:

- самый высокий показатель среди отраслей в регионе по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах;
- второе место по показателям угроз на съемных носителях и в сетевых папках;
- третье место по показателю угроз из интернета;
- первое место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и

фишинговые страницы, вредоносные документы, шпионские программы, черви;
- второе место по показателю вирусов и программ-вымогателей;
- третье место по показателю майнеров в формате исполняемых файлов и вредоносных программ для AutoCAD.

Электроэнергетика

Ближний Восток находится на четвертом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

Среди регионов по показателям в отрасли Ближний Восток занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов;
- третье место по показателю угроз в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокируются вредоносные документы.

Среди отраслей в регионе электроэнергетика занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из интернета;
- третье место по показателю угроз на съемных носителях;
- второе место по показателю ресурсов в интернете из списка запрещенных и червей;
- третье место по показателям угроз следующих категорий: вредоносные документы, шпионские программы и программы-вымогатели.

Биометрические системы

Ближний Восток находится на шестом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

В рейтингах регионов по доле компьютеров, на которых блокировались угрозы в биометрических системах, Ближний Восток занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- третье место по показателю угроз на съемных носителях;
- третье место по доле компьютеров АСУ, на которых блокируются вирусы и вредоносные программы для AutoCAD.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

- первое место по показателю угроз на съемных носителях и в сетевых папках;
- второе место по показателю угроз из почтовых клиентов;
- первое место по показателю вирусов и программ-вымогателей;
- второе место по показателям вредоносных документов и шпионских программ;
- третье место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, черви, веб-майнеры.

Строительство

Ближний Восток находится на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

Среди регионов по показателям в отрасли Ближний Восток занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов;
- третье место по доле компьютеров АСУ, на которых блокируются следующие категории: вредоносные скрипты и фишинговые страницы, веб-майнеры.

Среди отраслей в регионе строительство занимает:

- первое место по показателю угроз из интернета;
- третье место по показателям угроз из почтовых клиентов и в сетевых папках;
- первое место по показателям майнеров обеих категорий и вредоносных программ для AutoCAD;
- второе место по показателю категории вредоносные скрипты и фишинговые страницы.

Инжиниринг и интеграторы АСУ

Ближний Восток находится на пятом 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 Ближний Восток занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;

- третье место по показателям угроз из почтовых клиентов и на съемных носителях;
- второе место по доле компьютеров АСУ, на которых блокируются черви.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает второе место по показателям майнеров в формате исполняемых файлов и вредоносных программ для AutoCAD.

Нефть и газ

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

Среди регионов по показателям в отрасли Ближний Восток занимает:

- второе место по показателям угроз из почтовых клиентов;
- третье место по показателю угроз из интернета и на съемных носителях;
- второе место по доле компьютеров АСУ, на которых блокируются вирусы и вредоносные программы для AutoCAD;
- третье место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, вредоносные документы, вредоносные скрипты и фишинговые страницы, веб-майнеры и черви.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- второе место по показателю веб-майнеров;
- третье место по показателю вирусов.

Производство

Ближний Восток находится на 10-м месте по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

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