Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Ближний Восток. Второй квартал 2025 года

22.09.2025

Версия 1.0

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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, и высокий показатель вредоносных скриптов и фишинговых страниц, многие из которых нацелены напрямую 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.

Высокий показатель шпионских программ

Доля компьютеров АСУ, на которых блокируются шпионские программы, на Ближнем Востоке, как и у 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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В первом и втором кварталах 2025 года Ближний Восток занял второе место среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели (в 2024 году регион лидировал в этом рейтинге).

Яркие различия в некоторых странах региона

Йемен лидирует во многих региональных рейтингах, причем часто с большим отрывом от остальных стран. Исключение — угрозы из почты.

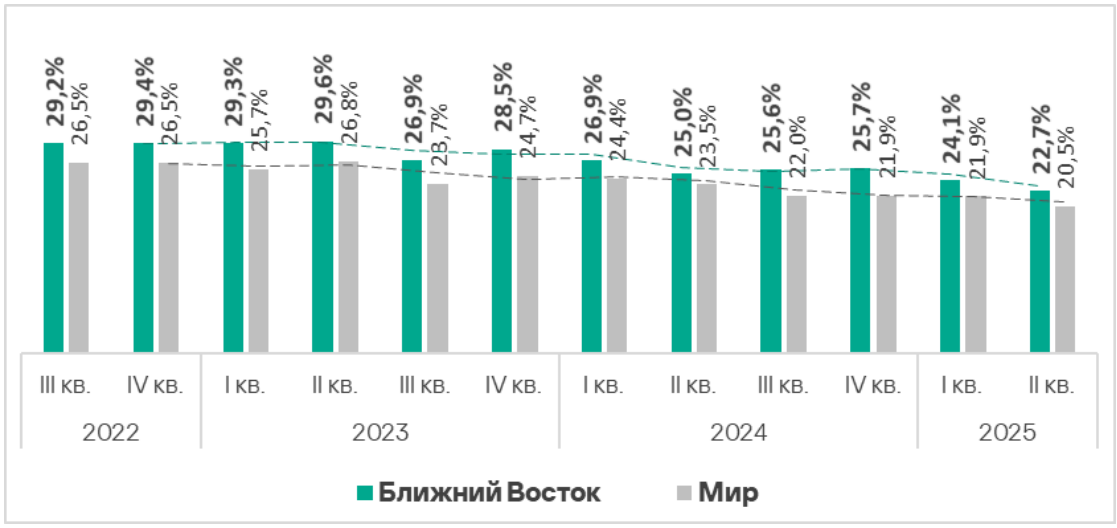
В рейтинге по угрозам из почтовых клиентов лидируют ОАЭ, Катар и Турция. Эти же страны находятся в числе лидеров в рейтингах по вредоносным скриптам и фишинговым страницам, вредоносным документам и программам-шпионам.

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

Статистика по всем угрозам

Во втором квартале 2025 года Ближний Восток занял третье место в мире по доле компьютеров АСУ, на которых заблокированы вредоносные объекты с показателем 22,7%. Показатель в регионе стабильно превышает среднемировое значение, во втором квартале 2025 года — в 1,1 раза. А по сравнению с регионом с минимальной долей атакованных компьютеров АСУ — Северной Европой, он больше в 2 раза.

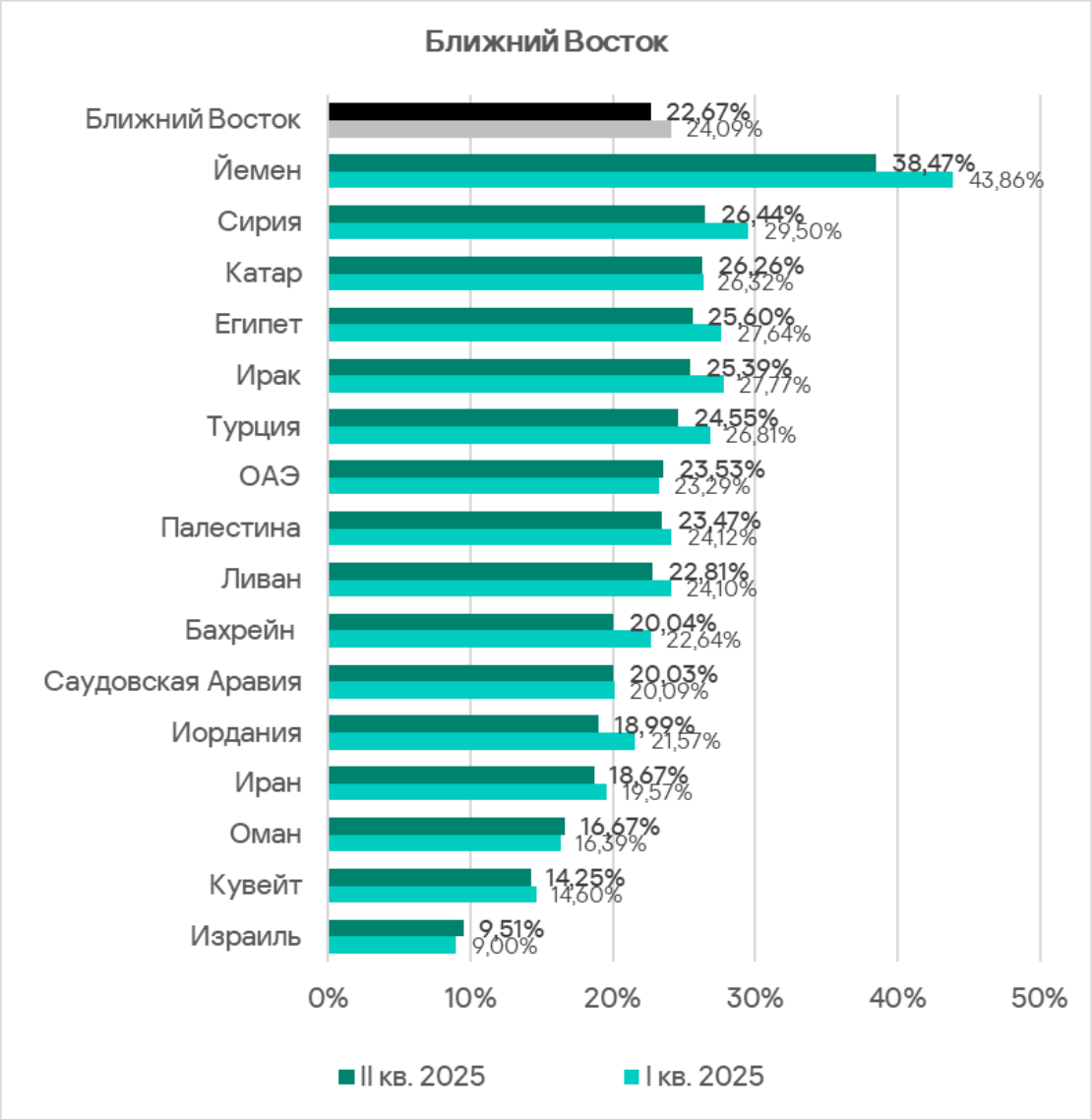
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, на Ближнем Востоке уменьшается второй квартал подряд, за отчетный период — на 1,4 п. п.



Среди стран и территорий региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 9,51% в Израиле до

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

38,47% в Йемене. Показатели этих двух стран заметно отличаются от показателей остальных стран в регионе, которые попадают в диапазон от 14% до 27%.



Йемен лидирует во многих региональных рейтингах. Исключение — угрозы из почты. В рейтинге по угрозам из почтовых клиентов лидируют ОАЭ, Катар и Турция. Эти же страны среди находятся в числе лидеров в рейтингах по вредоносным скриптам и фишинговым страницам, вредоносным документам и программам-шпионам.

Израиль большинство региональных рейтингов замыкает.

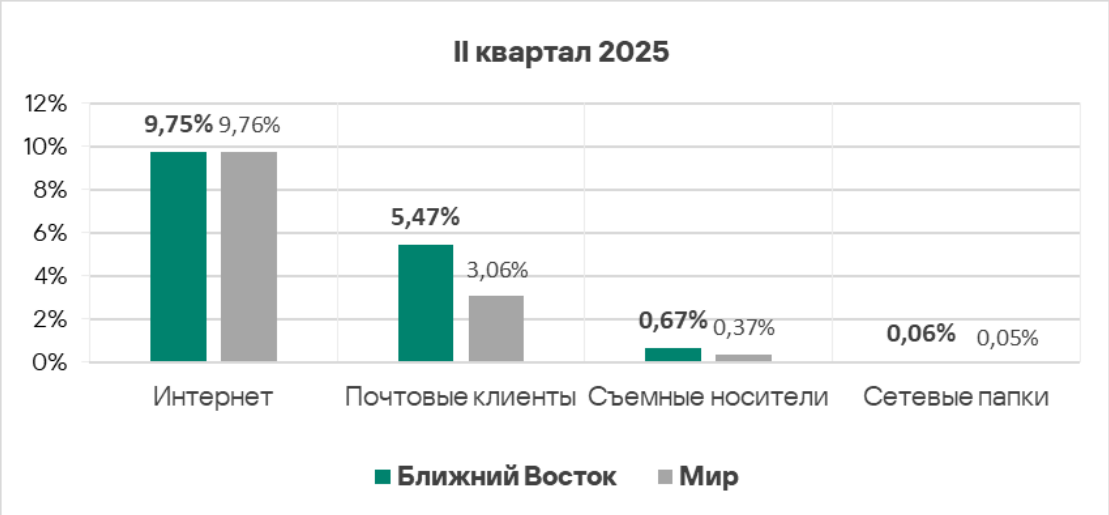
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Источники угроз

Доля компьютеров АСУ, на которых угрозы были заблокированы из разных источников, в регионе выше среднемировых показателей у всех источников, кроме интернета. Показатель интернета почти совпадает со среднемировым.

На Ближнем Востоке 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.



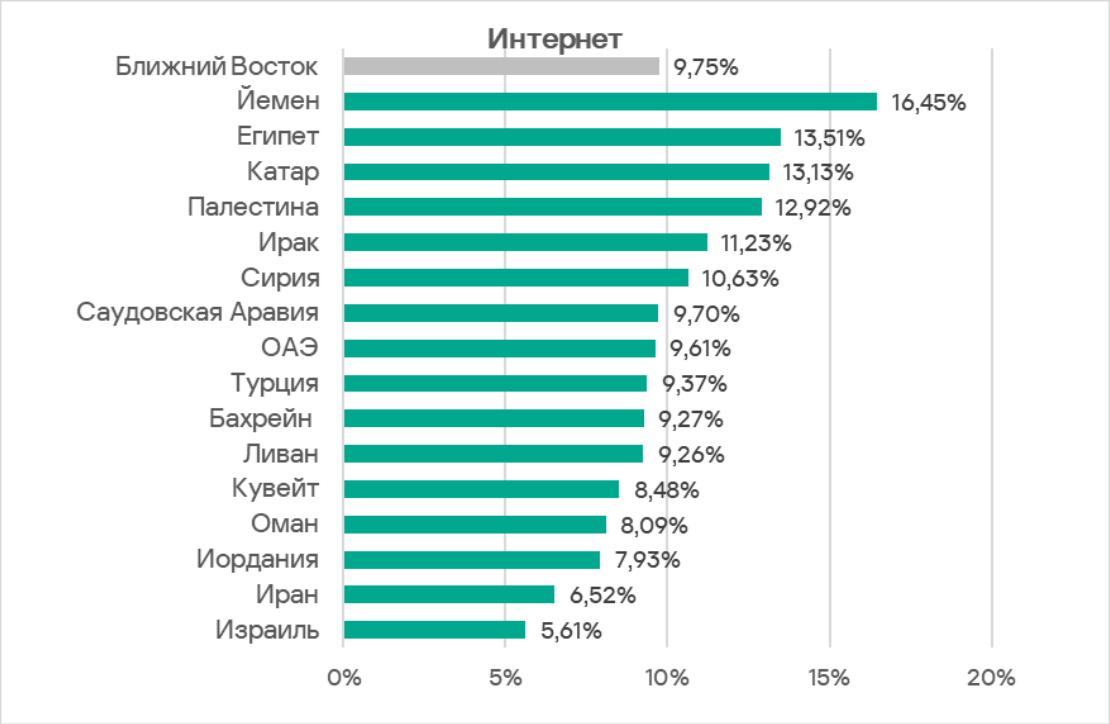
Доля атакованных компьютеров АСУ растет только у почтовых клиентов. У остальных источников угроз — явная тенденция к уменьшению значений.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

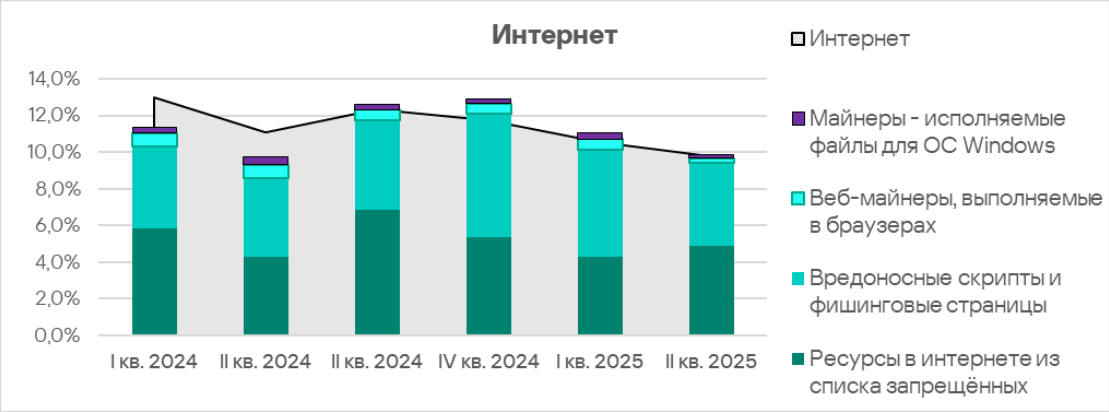
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Ближний Восток занимает четвертое место в рейтинге регионов с показателем, который превышает минимальный — у Восточной Азии — в 1,5 раза.

Показатели стран и территорий региона варьируют от 5,61% в Израиле до 16,45% в Йемене.



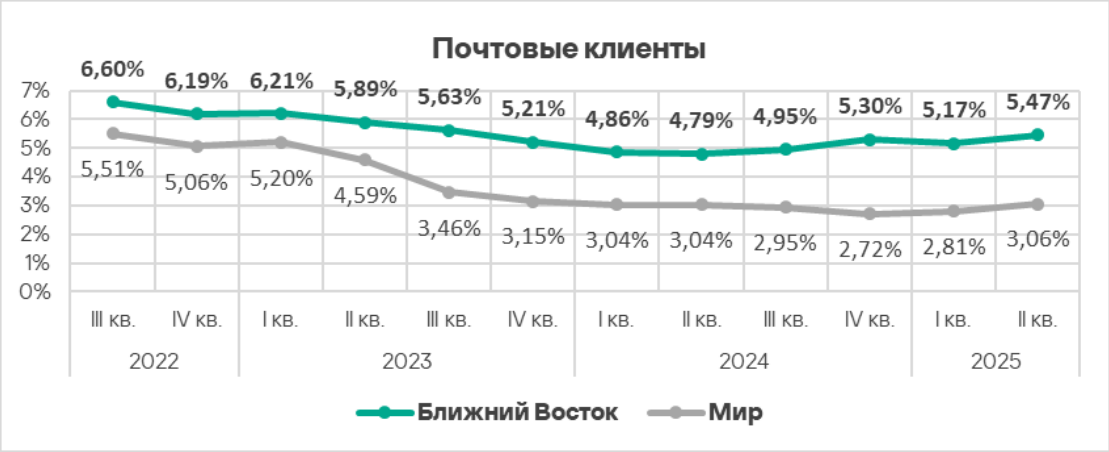
Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, майнеры.



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Почтовые клиенты

Почтовые клиенты — источник угроз в регионе, чей показатель демонстрирует тенденцию к росту с третьего квартала 2024 года. По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, во втором квартале 2025 года Ближний Восток среди регионов занимает третье место. Его показатель в 6,8 раз больше, чем в России, которая замыкает этот рейтинг.

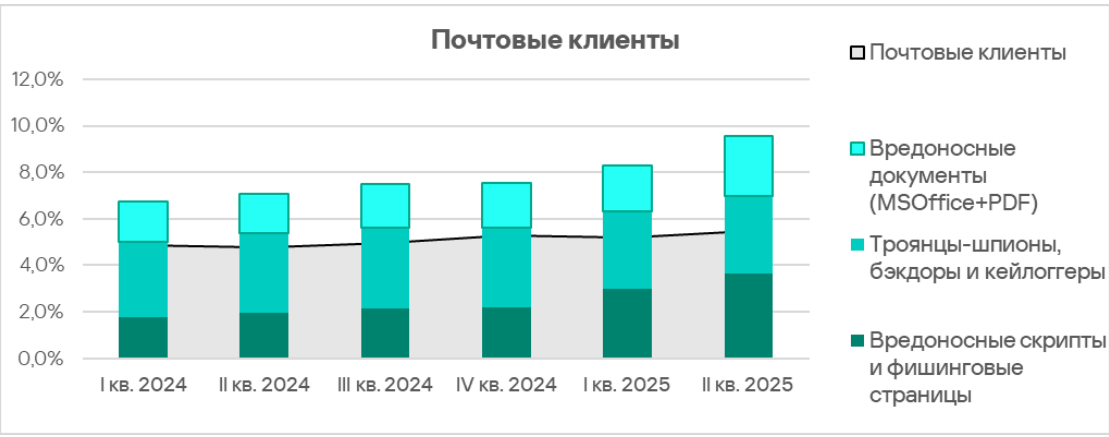


Среди стран и территорий региона по этому показателю с отрывом лидируют ОАЭ с 10,34%. Минимальная доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, — в Израиле (0,48%). Отметим, что Йемен, который лидирует по показателям остальных источников угроз, в этом рейтинге оказался на третьем месте с конца.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Тройка стран-лидеров этого рейтинга — ОАЭ, Катар и Турция — также находятся на верхних строчках рейтингов по вредоносным скриптам и фишинговым страницам, вредоносным документам и программам-шпионам.

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



Съемные носители

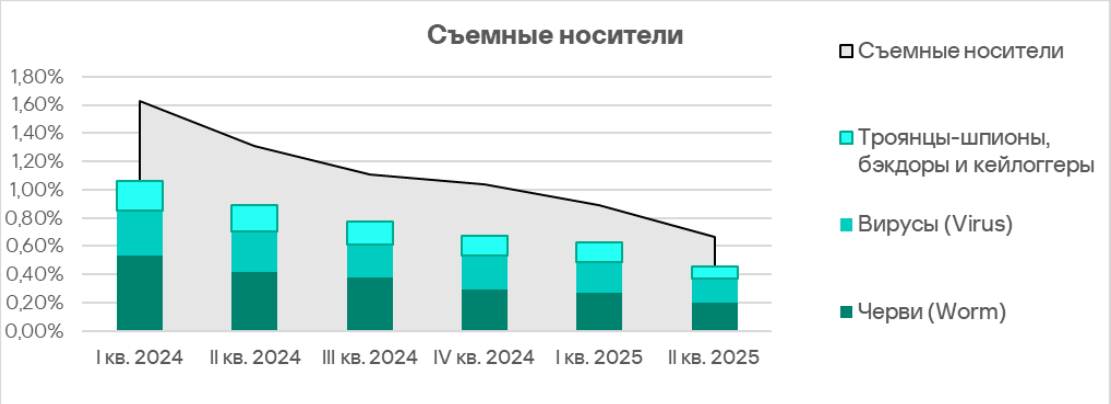
По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, во втором квартале 2025 года Ближний Восток занимает третье место среди регионов. В Северной Америке

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

(Канада), которая занимает последнее место в рейтинге, показатель меньше почти в 25 раз.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, два абсолютных лидера: Йемен с 4,85% и Ирак с 4,36%. Показатели остальных стран варьируют от 0,11% в Израиле до 2,18% 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 третье место среди регионов.



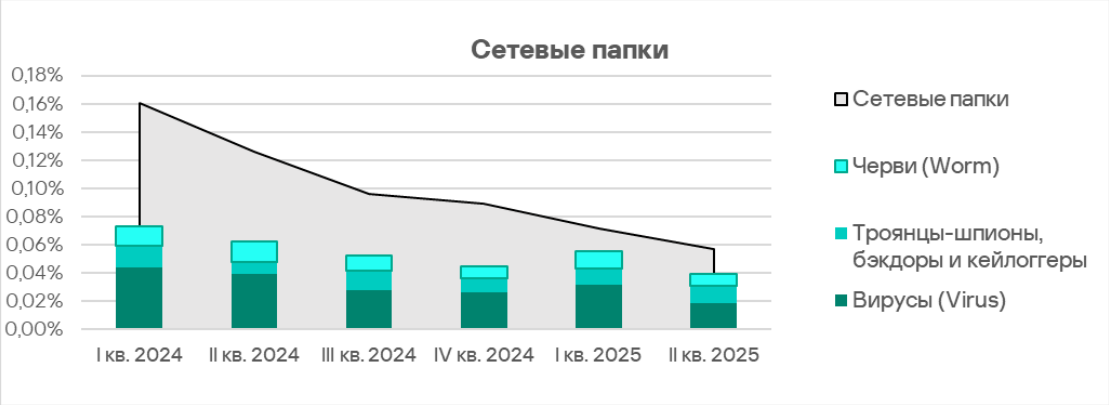
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Сетевые папки

По доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, Ближний Восток занимает четвертое место среди регионов с 0,06%. С Северной Европой, которая занимает последнее место в рейтинге, показатели отличаются в 5,9 раза.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, с впечатляющим отрывом лидирует Йемен с 0,59%.

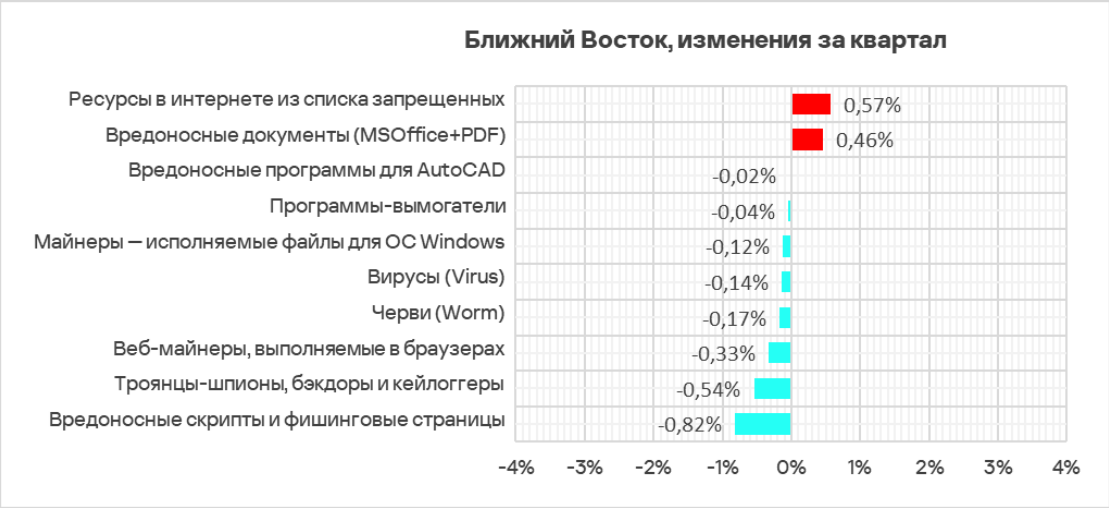
Основными категориями угроз, которые распространяются через сетевые папки, являются черви, вирусы, и шпионские программы.



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории угроз

В регионе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения у всех категорий, кроме ресурсов в интернете из списка запрещенных, майнеров — исполняемых файлов для ОС Windows, а также вредоносных программ для AutoCAD.



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

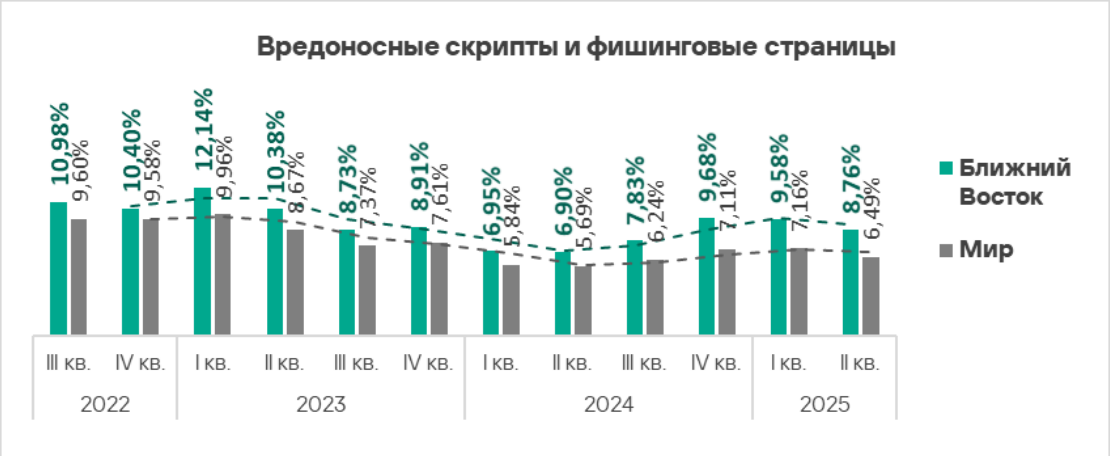
- программы-вымогатели — в 1,9 раза, второе место среди регионов;

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- вредоносные документы — в 1,5 раза, третье место среди регионов;
- шпионские программы — в 1,5 раза, четвертое место среди регионов;
- вредоносные скрипты и фишинговые страницы — в 1,3 раза, третье место среди регионов;
- черви — в 1,5 раза, третье место среди регионов;
- вирусы — в 1,4 раза, четвертое место среди регионов.

Вредоносные скрипты и фишинговые страницы

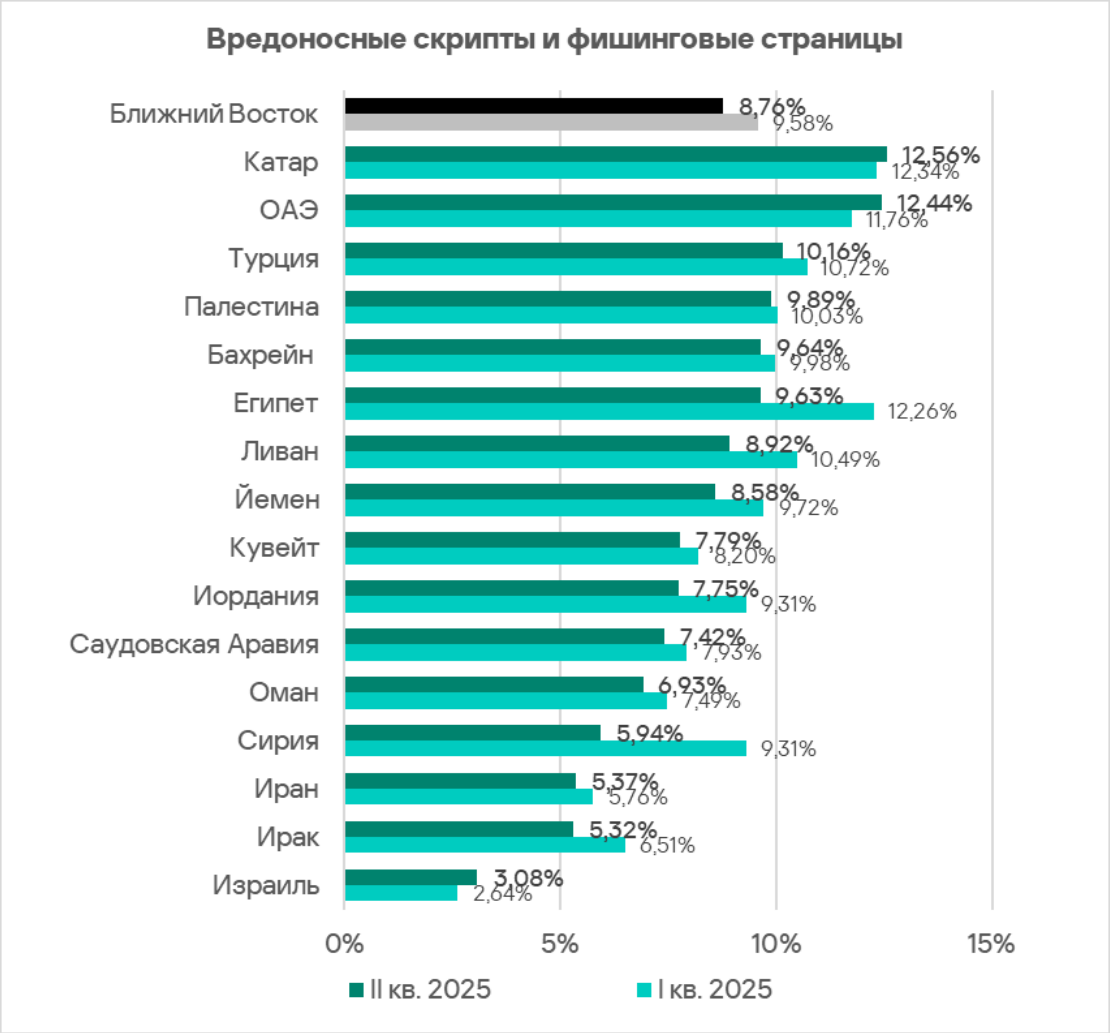
По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Ближний Восток занимает в соответствующем рейтинге регионов третье место с 8,76%. Этот показатель в 2,9 раза больше, чем в Северной Европе, где он минимальный.



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, лидирует Катар с 12,56%. Наименьший показатель — в Израиле, и он в 1,7 раза меньше предшествующего в рейтинге показателя Ирака.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



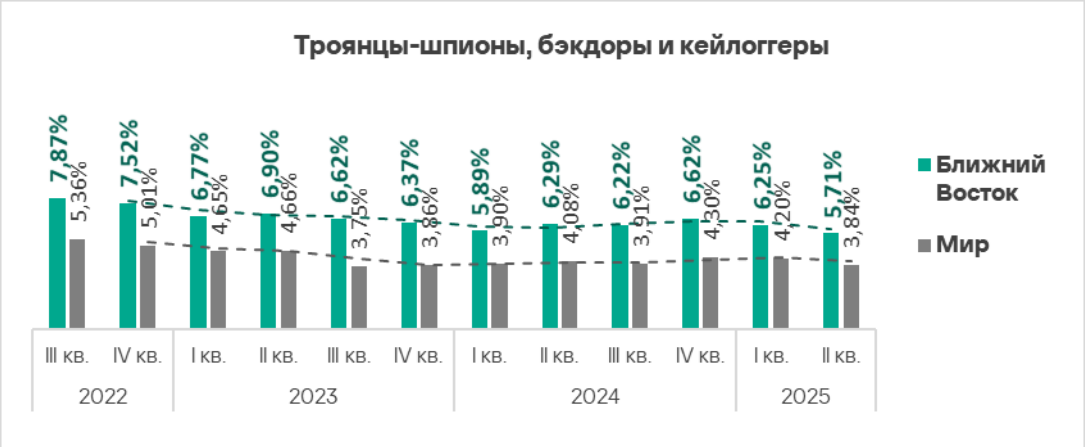
Топ 3 стран из этого рейтинга — Катар, ОАЭ и Турция — возглавляют также рейтинг по вредоносным документам. Они же входят в тройку стран по шпионским программам, а также в тройку по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах.

Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, Ближний Восток находится в соответствующем рейтинге регионов на четвертом месте с 5,71%. Это в 4,1 раза больше, чем в Западной Европе, где этот показатель наименьший.

На Ближнем Востоке доля компьютеров АСУ, на которых блокируются шпионские программы, с третьего квартала 2023 года колеблется в диапазоне от 5,71% до 6,62%. Во втором квартале 2025 года показатель был минимальным с третьего квартала 2022 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Среди стран и территорий региона по доле компьютеров АСУ, на которых заблокированы шпионские программы, лидируют ОАЭ с 7,87%. Наименьший показатель — в Израиле, он в 3,2 раза меньше предшествующего в рейтинге показателя Кувейта.

Шпионские программы в регионе блокируются во всех источниках угроз, но распространяется эта угроза преимущественно через почтовые клиенты.

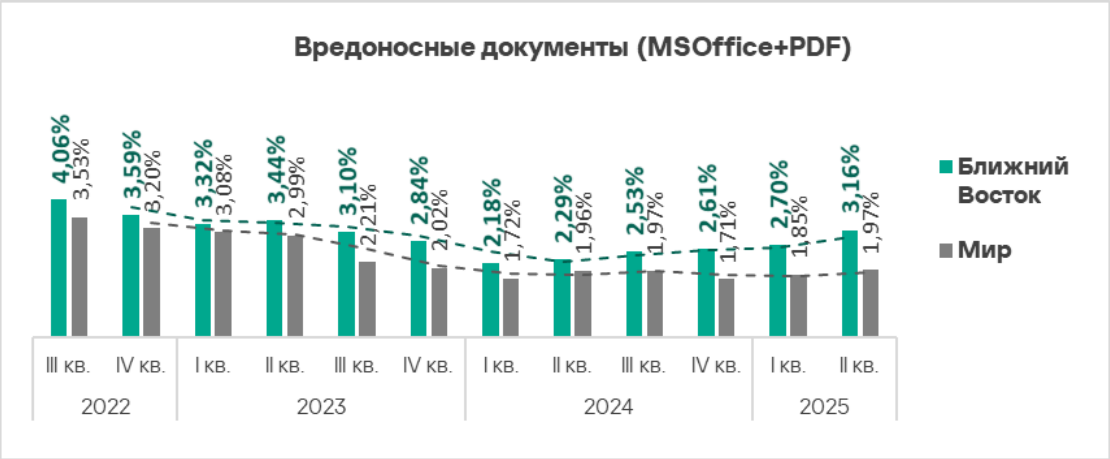
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Первые три страны в рейтинге по шпионским программам оказались также лидерами по угрозам из почтовых клиентов. Они же входят в тройку стран по доле компьютеров АСУ, где были заблокированы вредоносные документы и вредоносные скрипты и фишинговые страницы.

Вредоносные документы

Вредоносные документы распространяются преимущественно по электронной почте. Ближний Восток в рейтингах регионов и по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, и по показателю вредоносных документов, занимает третье место. Показатель вредоносных документов в регионе — 3,16%, это в 4,9 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе растет со второго квартала 2024 года.



Среди стран и территорий региона по этому показателю лидирует Катар с 5,97%. Рейтинг замыкает Израиль с 0,30% — это в 4,2 раза меньше предшествующего в рейтинге показателя Ирака.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Топ 3 стран из этого рейтинга — Катар, ОАЭ и Турция — возглавляют также рейтинг по вредоносным скриптам и фишинговым страницам и шпионским программам. Они же входят в тройку стран по доле компьютеров АСУ, где угрозы были заблокированы в почтовых клиентах.

Самораспространяющееся вредоносное ПО: черви и вирусы

Черви и вирусы — основные категории угроз, которые блокируются при подключении к компьютерам АСУ съемных устройств. Ближний Восток находится на третьем месте среди регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных устройств. Третье место у региона и по показателю червей, четвертое — по показателю вирусов.

Доля компьютеров АСУ, на которых блокируются черви, на Ближнем Востоке — 1,82%. Это в 8,2 раза больше, чем в регионе с минимальным показателем — Австралии и Новой Зеландии.

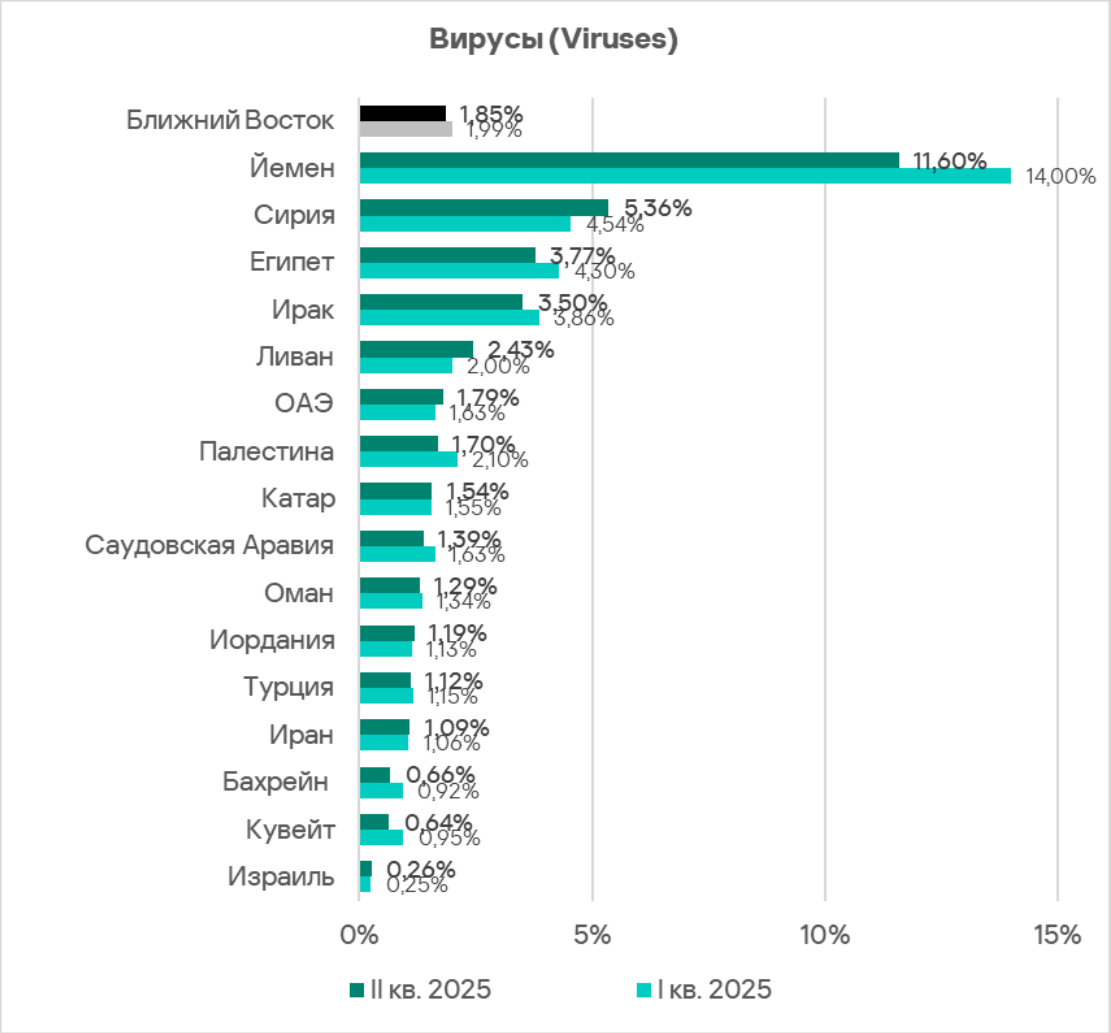
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых блокируются вирусы, на Ближнем Востоке — 1,85%. Это в 14,7 раза больше, чем в регионе с минимальным показателем — Австралии и Новой Зеландии.

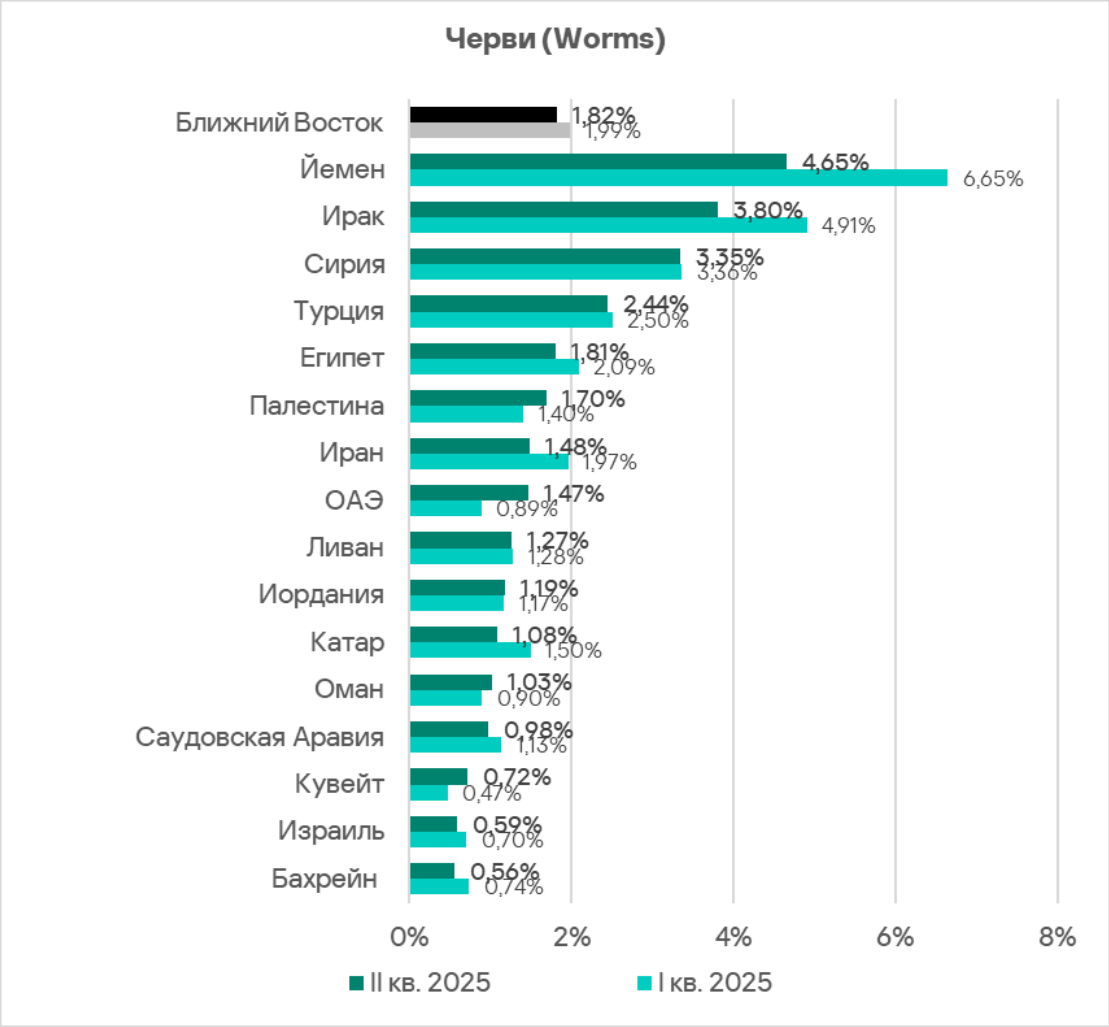
Показатель червей, как и доля угроз со съемных носителей в целом, постепенно снижается. У вирусов более сложная динамика.

Среди стран и территорий региона и по доле компьютеров АСУ, на которых блокируются черви, и по показателю вирусов, лидирует Йемен, в случае вирусов — с большим отрывом.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



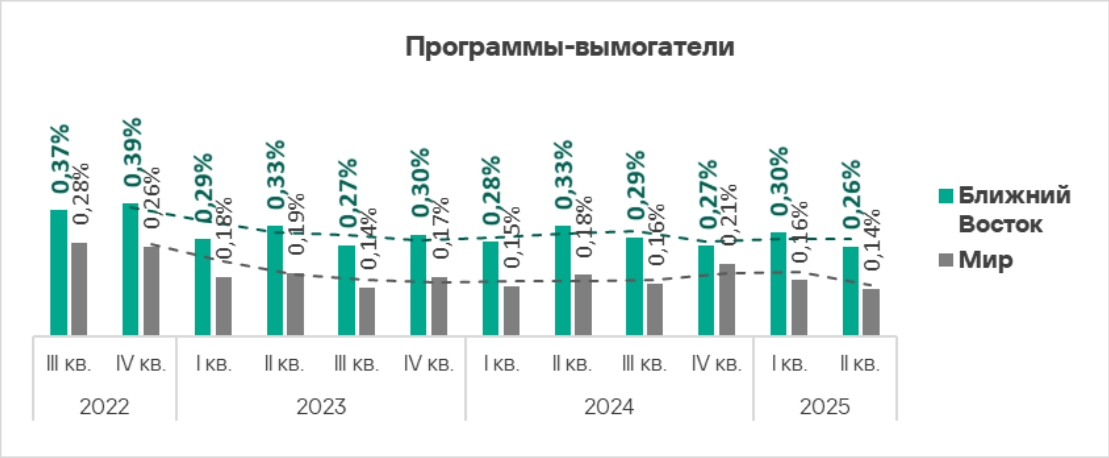
Программы-вымогатели

На Ближнем Востоке доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, стабильно высокая и почти вдвое превышает среднемировой показатель. В 2024 году регион лидировал в соответствующем рейтинге. Во втором квартале 2025 года (как и в первом) Ближний Восток занял второе место — с 0,26%.

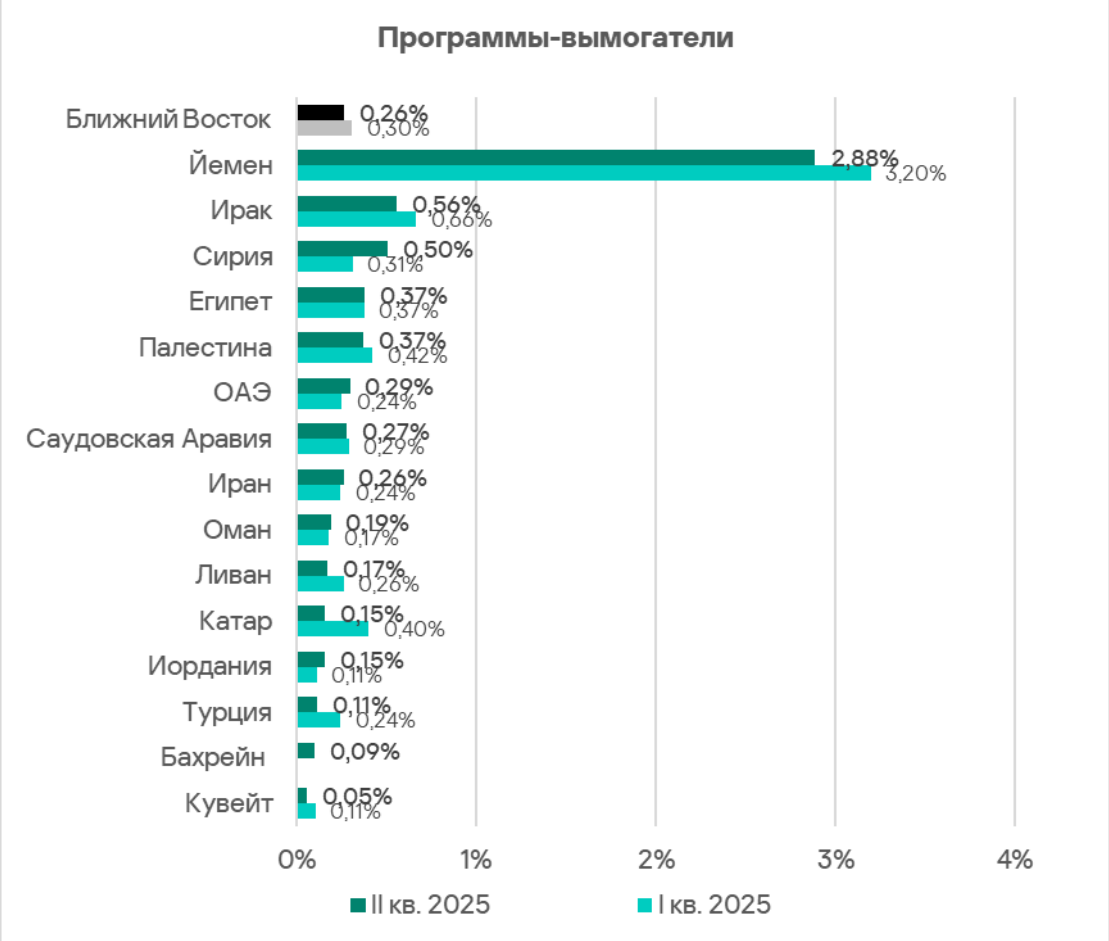
По сравнению с Западной Европой, где показатель наименьший, доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, на Ближнем Востоке больше в 4,1 раза.

Показатель в регионе с 2023 года попадает в диапазон от 0,26% до 0,33%. Во втором квартале 2025 года он был наименьшим за период с третьего квартала 2022 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, с огромным отрывом лидирует Йемен. По сравнению с Ираком, который занимает второе место в этом рейтинге, показатель Йемена больше в 5,2 раза.



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отрасли

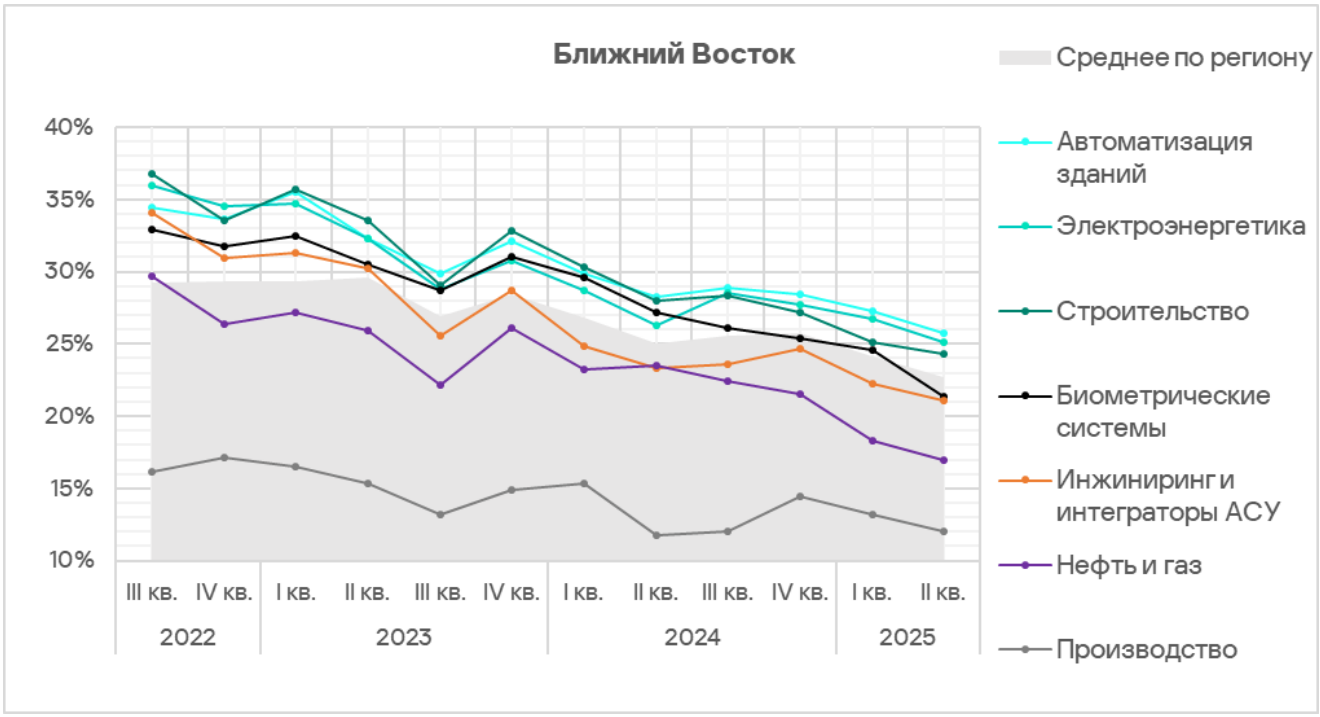
Наиболее часто встречающейся с угрозами отраслью региона среди рассмотренных в отчете является автоматизация зданий.

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

- электроэнергетика — в 1,2 раза;
- строительство — в 1,1 раза;
- автоматизация зданий — в 1,1 раза.

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех исследуемых отраслях. Несмотря на периодические колебания, тренды демонстрируют в целом положительную динамику (показатели снижаются).

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



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

При оценке проблем отраслей мы используем тепловые карты. На таких картах 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. На Ближнем Востоке значения, наиболее приближенные к максимальным, наблюдаются для совокупного показателя в сфере автоматизации зданий, а также в категории веб-майнеры в строительной отрасли.

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Показатели источников угроз в отраслях на Ближнем Востоке, 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	8,50%	10,26%	11,17%	9,65%	7,23%	11,37%	5,27%	9,75%
Почтовые клиенты	4,77%	8,27%	4,34%	3,93%	2,26%	4,68%	2,04%	5,47%
Съемные носители	1,39%	0,75%	0,61%	0,46%	0,39%	0,39%	0,65%	0,67%
Сетевые папки	0,08%	0,09%	0,06%	0,02%	0,05%	0,03%	0,03%	0,06%
Показатель отрасли в регионе	21,36%	25,79%	25,10%	21,08%	16,97%	24,35%	16,78%	

Показатели категорий угроз в отраслях на Ближнем Востоке, 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	5,09%	5,34%	6,46%	5,20%	4,03%	5,47%	2,64%	5,19%
Вредоносные скрипты и фишинговые страницы	7,67%	11,47%	8,10%	7,23%	6,64%	8,51%	4,50%	8,76%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,46%	8,08%	5,16%	4,56%	3,44%	4,30%	2,31%	5,71%
Черви (Worm)	1,76%	2,35%	2,10%	1,49%	1,52%	1,18%	1,27%	1,82%
Майнеры — исполняемые файлы для ОС Windows	0,45%	0,48%	0,61%	0,54%	0,44%	1,14%	0,15%	0,49%
Вредоносные документы (MSOffice+PDF)	2,64%	5,01%	2,69%	2,08%	1,43%	2,12%	1,04%	3,16%
Вирусы (Virus)	2,90%	2,53%	2,16%	1,17%	1,62%	2,21%	1,42%	1,85%
Программы-вымогатели	0,53%	0,42%	0,31%	0,15%	0,15%	0,18%	0,03%	0,26%
Веб-майнеры, выполняемые в браузерах	0,43%	0,31%	0,47%	0,33%	0,44%	0,92%	0,09%	0,33%
Вредоносные программы для AutoCAD	0,29%	0,17%	0,29%	0,15%	0,34%	1,32%	0,36%	0,23%
Показатель отрасли в регионе	21,36%	25,79%	25,10%	21,08%	16,97%	24,35%	12,00%	

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

«Горячие точки» отраслей

Автоматизация зданий

- Самый высокий показатель среди отраслей в регионе по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах и сетевых папках.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Лидер среди отраслей региона по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви.
- Второе место среди отраслей региона по показателям вирусов и программ-вымогателей.
- Третье место в регионе по показателю ресурсов в интернете из списка запрещенных.
- Пятое место среди отраслей во всех регионах по показателю в категории вредоносные скрипты и фишинговые страницы.

Электроэнергетика

- Второе место в регионе по показателю угроз из интернета, третье — по показателю угроз в сетевых папках.
- Лидер среди отраслей региона по показателю ресурсов в интернете из списка запрещенных.
- Второе место среди отраслей региона по показателям следующих категорий: вредоносные документы, майнеры обеих категорий, черви.
- Третье место в регионе по показателю следующих категорий: вредоносные скрипты и фишинговые страницы, шпионские программы, программы-вымогатели.

Строительство

- Первое место среди отраслей в регионе по показателю угроз из интернета, третье — по показателю угроз из почтовых клиентов.
- Первое место среди отраслей в регионе по показателям майнеров обеих категорий и вредоносных программ для AutoCAD.
- Второе место среди отраслей региона по показателям следующих категорий: интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы.
- Третье место в регионе по показателю вирусов.
- Четвертое место среди отраслей во всех регионах по показателю веб-майнеров.

Биометрические системы

- Самый высокий из всех отраслей региона показатель угроз на съемных носителях, второе место по показателям угроз из почтовых клиентов и в сетевых папках.
- Лидер среди отраслей в регионе по показателям вирусов и программ-вымогателей.
- Второе место в регионе среди отраслей по показателю шпионских программ.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Третье место в регионе по показателям вредоносных документов и червей.

Инжиниринг и интеграторы АСУ

- Четвертое место среди отраслей региона по показателю угроз из интернета.
- Третье место среди отраслей региона по показателю категории майнеры — исполняемые файлы для ОС Windows.
- Четвертое место в регионе по показателям следующих категорий: шпионские программы и ресурсы в интернете из списка запрещенных.

Нефтегазовая отрасль

- Четвертое место среди отраслей региона по показателю угроз в сетевых папках.
- Третье место среди отраслей в регионе по показателям следующих категорий: веб-майнеры и вредоносные программы для AutoCAD.
- Четвертое место в регионе по доле компьютеров АСУ, на которых блокируются черви.

Производство

- Третье место среди отраслей в регионе по показателю угроз на съемных носителях.
- Второе место среди отраслей региона по показателю вредоносных программ для AutoCAD.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»