Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Ближний Восток. Второй квартал 2025 года

24.12.2025

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 1,9 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 1,7 раза.

Высокий показатель шпионских программ

Доля компьютеров АСУ, на которых блокируются шпионские программы, на Ближнем Востоке в 1,3 раза, а у вредоносных документов — в 1,4 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 2024 году Ближний Восток занимал первое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, в первом и втором кварталах 2025 года был на втором месте. В третьем квартале 2025 года Ближний Восток вновь лидирует по показателю программ-вымогателей.

Ближний Восток занимает не ниже четвертого места в рейтингах регионов по показателю программ-вымогателей во всех отраслях, кроме производства.

Яркие различия в некоторых странах региона

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

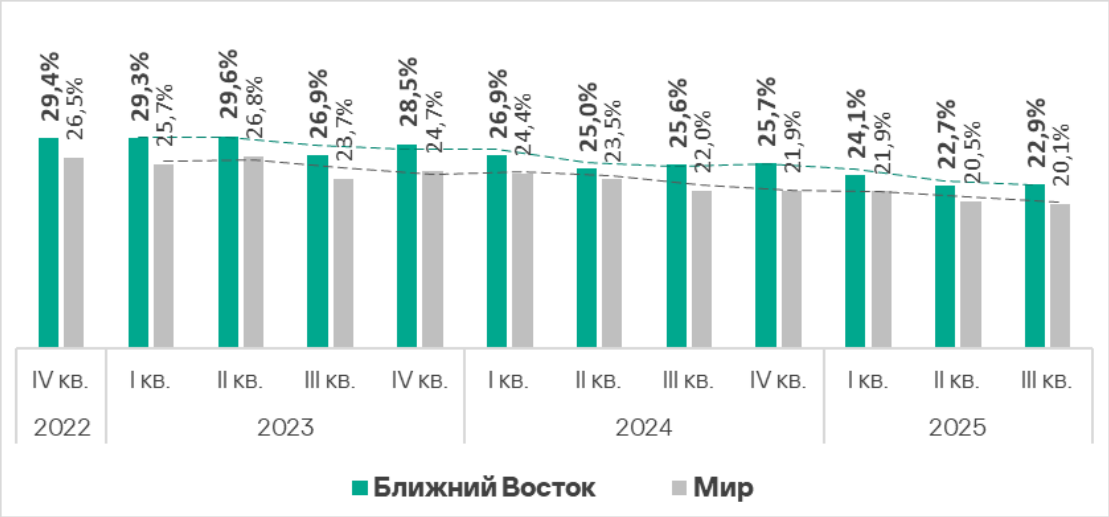
В рейтинге по угрозам из почтовых клиентов лидируют ОАЭ и Катар. Эти же страны находятся в числе лидеров в рейтингах по вредоносным скриптам и фишинговым страницам, вредоносным документам и программам-шпионам.

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

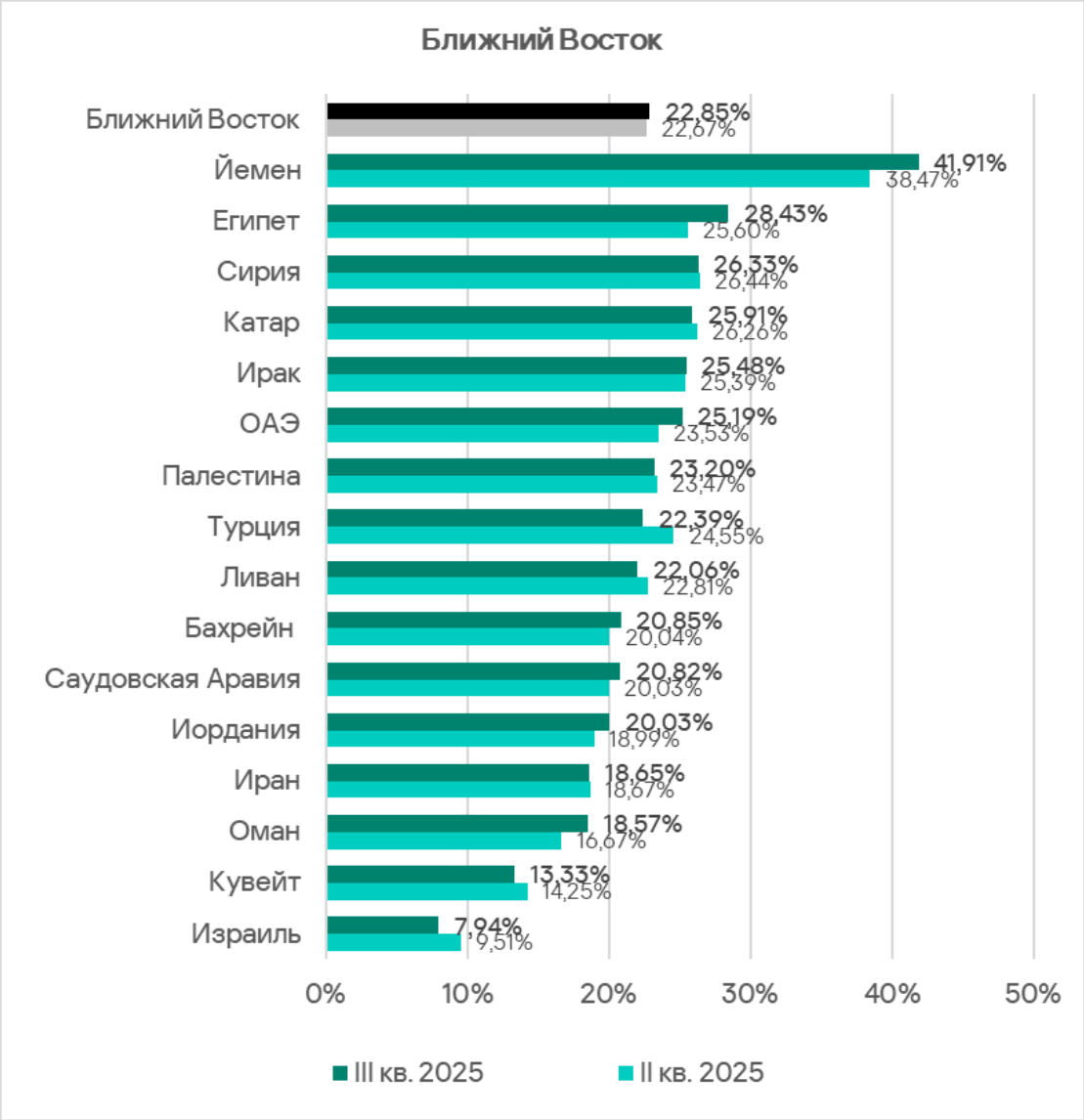
Статистика по всем угрозам

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

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, на Ближнем Востоке за квартал немного увеличилась — до 22,9%. Это в 2,5 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 7,54% в Израиле до 41,91% в Йемене. Показатели этих двух стран заметно отличаются от показателей остальных стран в регионе, которые попадают в диапазон от 13% до 29%.

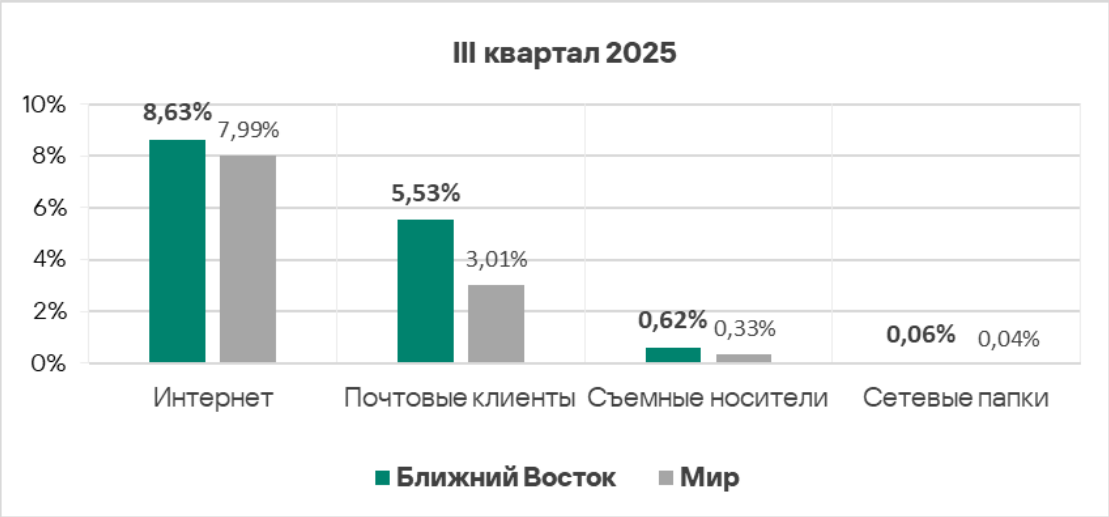


Йемен лидирует во многих региональных рейтингах как по источникам, так и по категориям вредоносного ПО. По показателям угроз из почты, категорий вредоносные документы, вредоносные скрипты и фишинговые страницы, вредоносные программы для AutoCAD — лидируют ОАЭ. По доле компьютеров АСУ, на которых блокируются программы-вымогатели — Сирия. 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. В регионе значительно превышает среднемировые значения доля компьютеров АСУ, на которых были заблокированы:

- угрозы из почтовых клиентов — в 1,8 раза;
- угрозы на съемных носителях — в 1,9 раза.

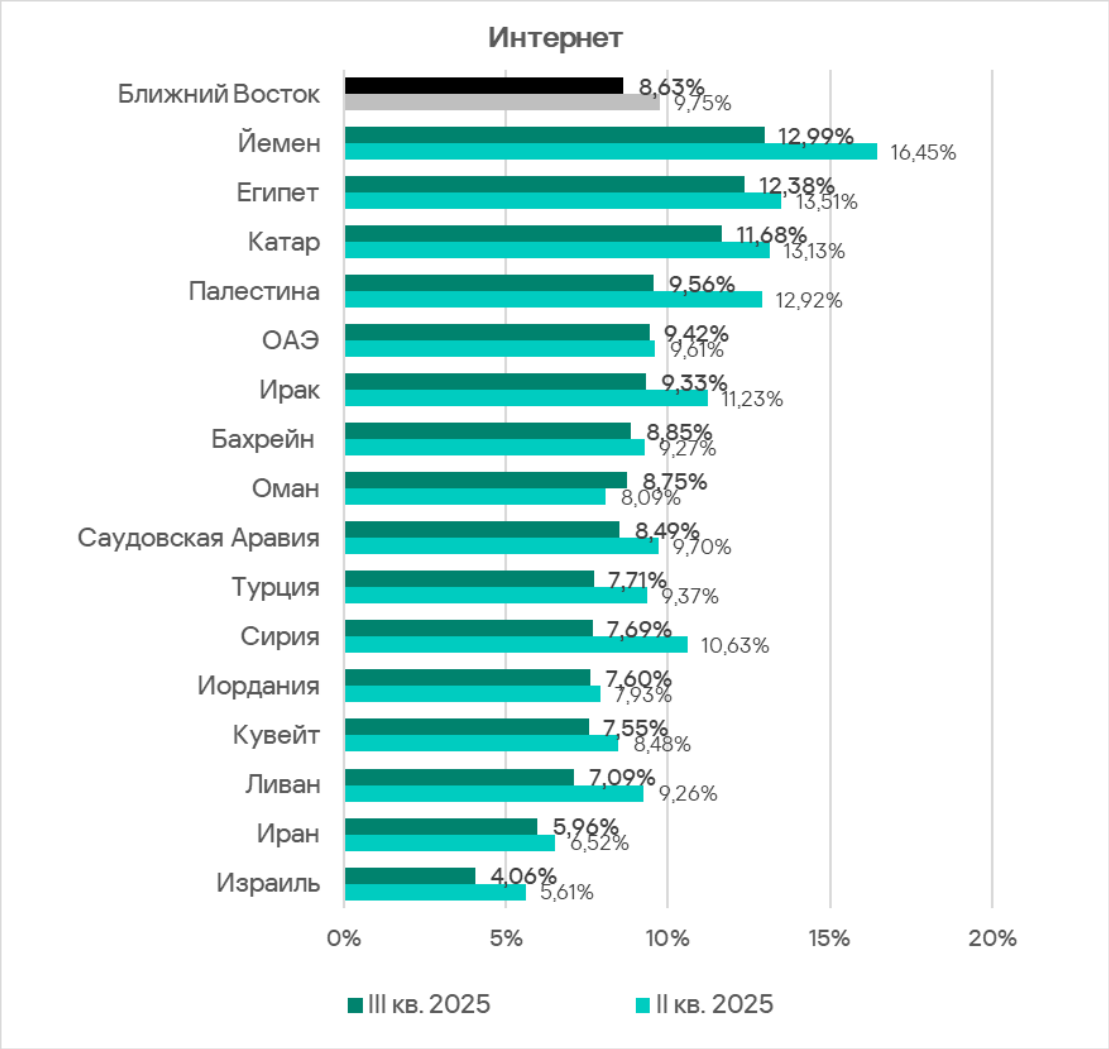


Доля атакованных компьютеров АСУ растет только у почтовых клиентов. У остальных источников угроз — явная тенденция к уменьшению значений.

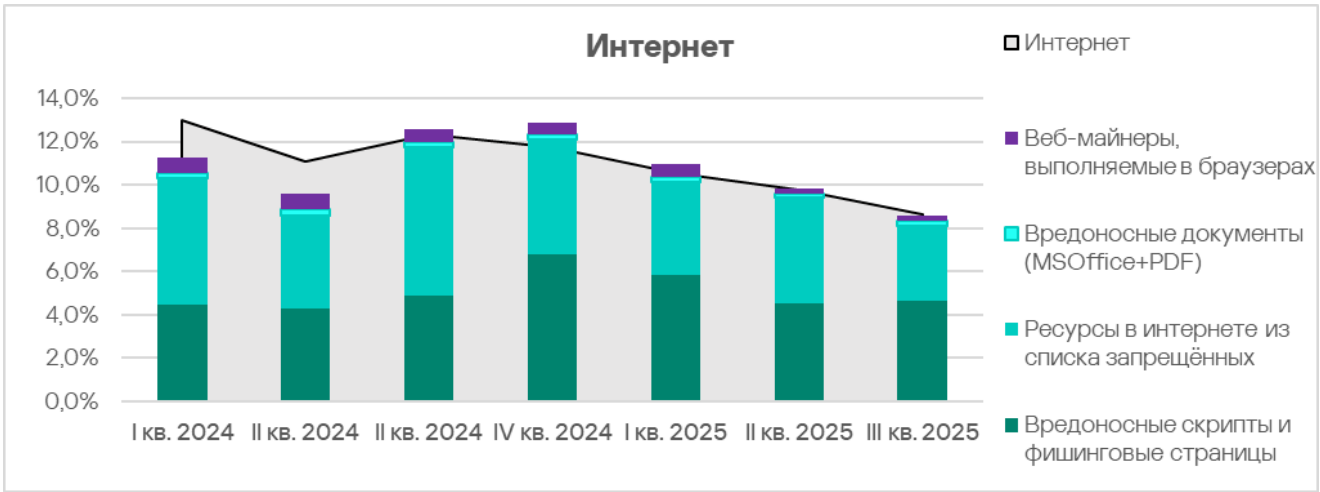
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Ближний Восток занимает пятое место в рейтинге регионов с показателем 8,63%, который превышает минимальный — у Северной Европы — в 1,9 раза.

Показатели стран и территорий региона варьируют от 4,06% в Израиле до 12,99% в Йемене.

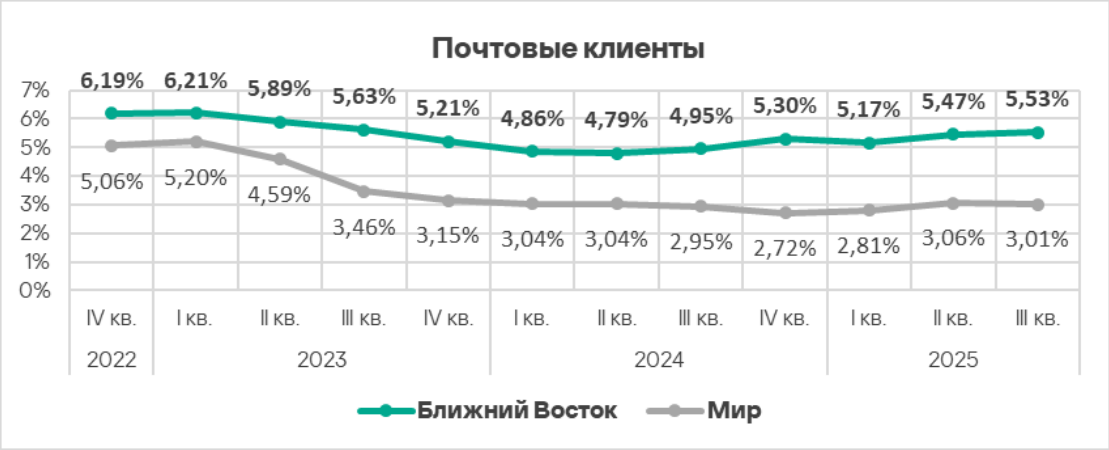


Основные категории угроз из интернета, которые блокируются на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.

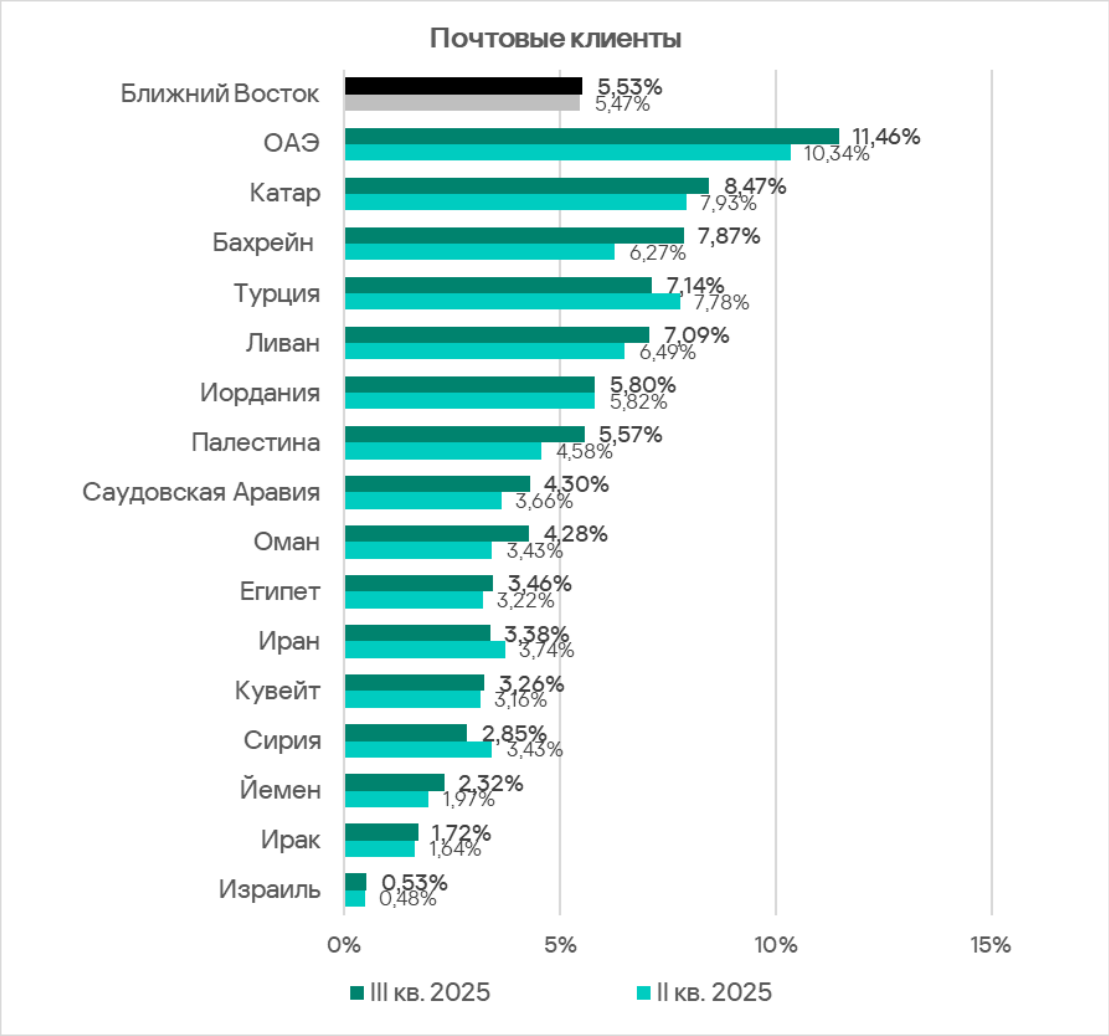


Почтовые клиенты

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, в третьем квартале 2025 года Ближний Восток среди регионов занимает второе место с 5,53%. Это в 7,1 раза больше, чем в России, которая замыкает этот рейтинг.

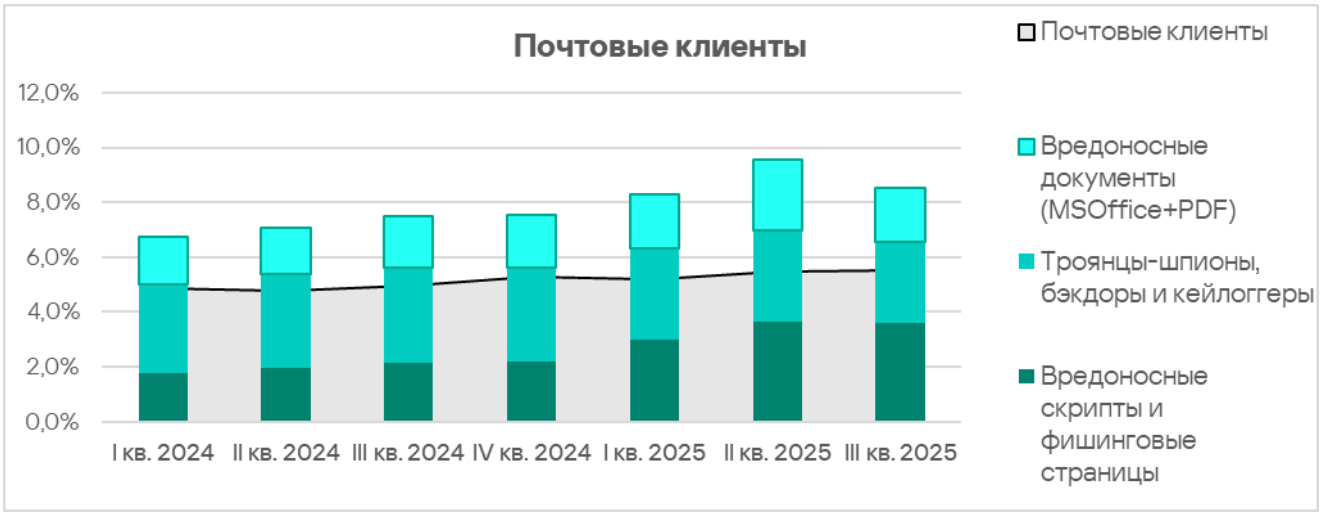


Среди стран и территорий региона по этому показателю с отрывом лидируют ОАЭ с 11,46%. Минимальная доля компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, в Израиле — 0,53%. Отметим, что Йемен, который лидирует по показателям остальных источников угроз, в этом рейтинге оказался на третьем месте с конца.



Три страны-лидера этого рейтинга — ОАЭ, Катар и Бахрейн — также находятся на верхних строчках рейтинга по вредоносным скриптам и фишинговым страницам.

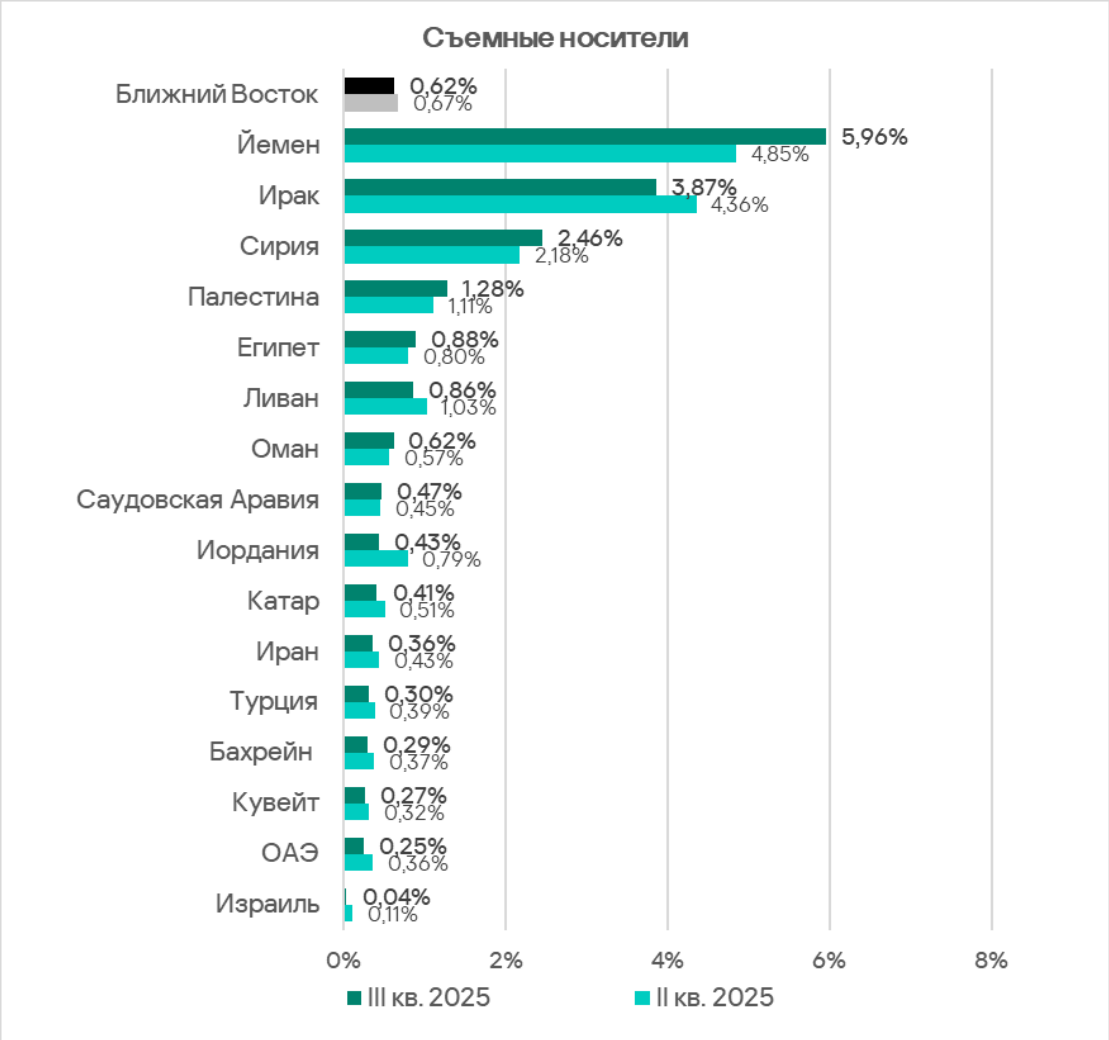
Основные категории угроз из электронной почты, заблокированные на компьютерах АСУ: вредоносные скрипты и фишинговые страницы, шпионское ПО и вредоносные документы.



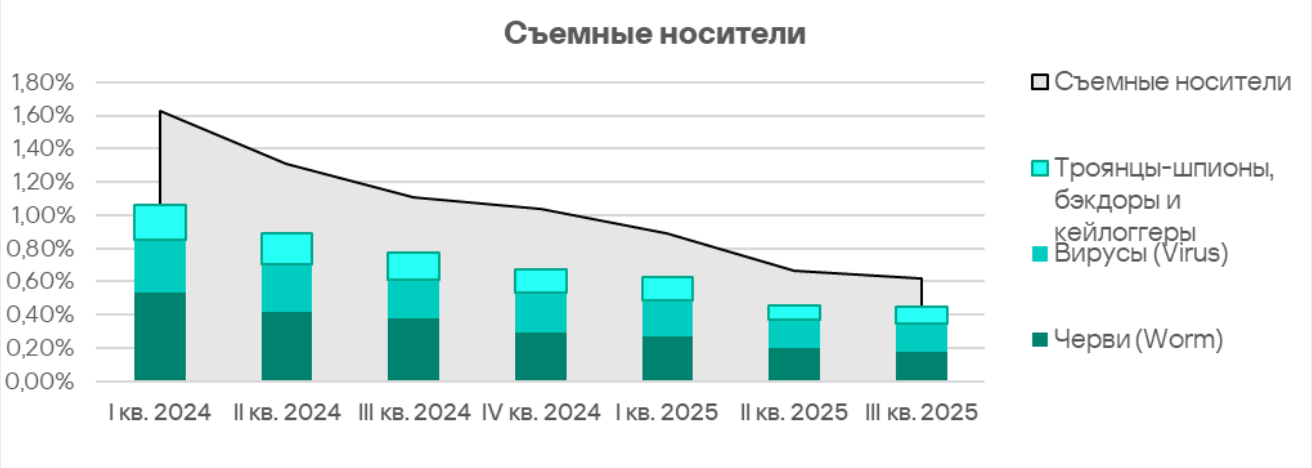
Съемные носители

По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, в третьем квартале 2025 года Ближний Восток занимает четвертое место среди регионов с 0,62%. Это в 12,4 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 5,96% и Ирак с 3,87%. Показатели остальных стран варьируют от 0,04% в Израиле до 2,46% в Сирии.



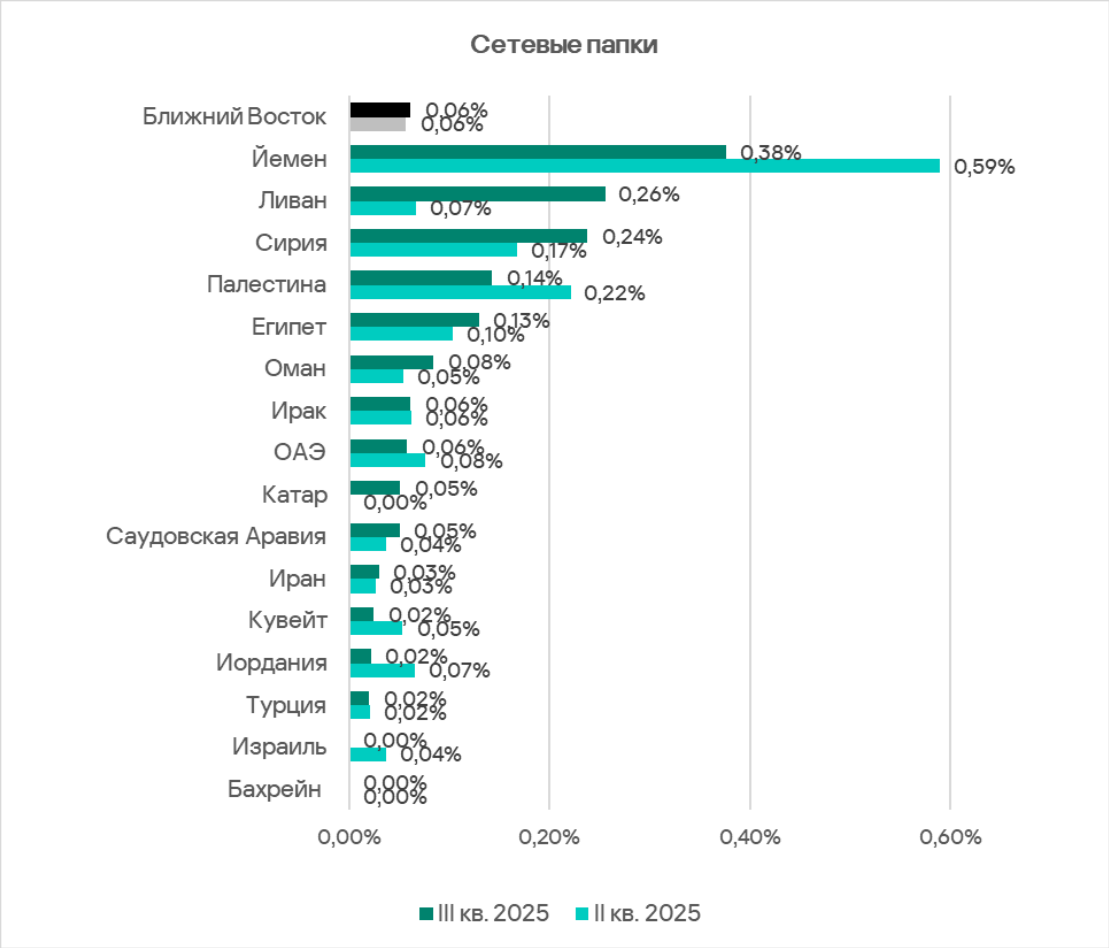
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионское ПО. По доле компьютеров АСУ, на которых были заблокированы черви, Ближний Восток занимает третье место среди регионов.



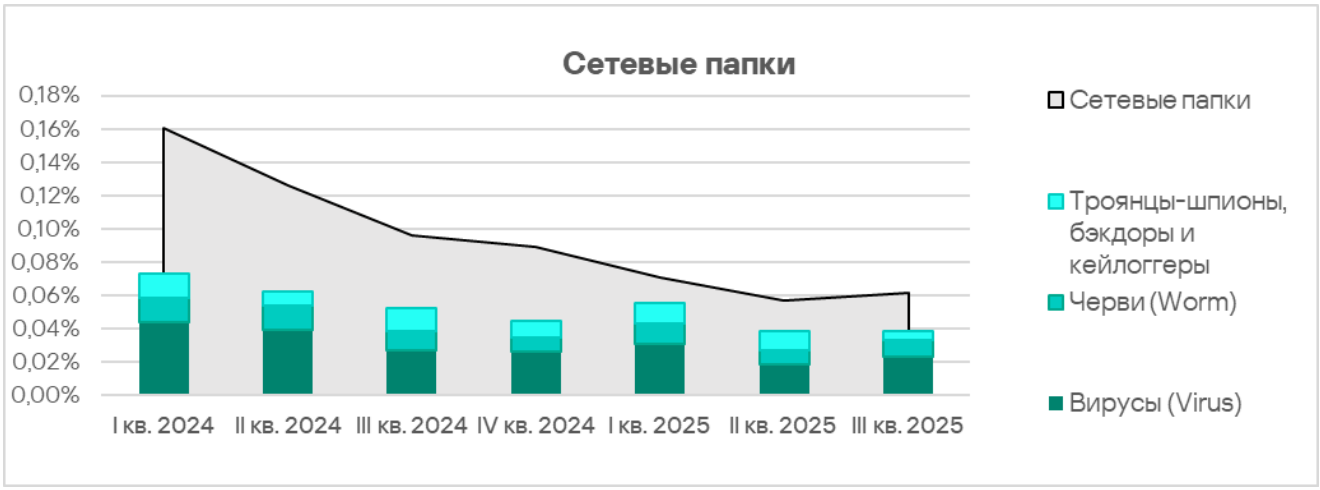
Сетевые папки

По доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, в третьем 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 10,2 раза.

Среди стран и территорий региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, с отрывом лидирует Йемен с 0,38%.

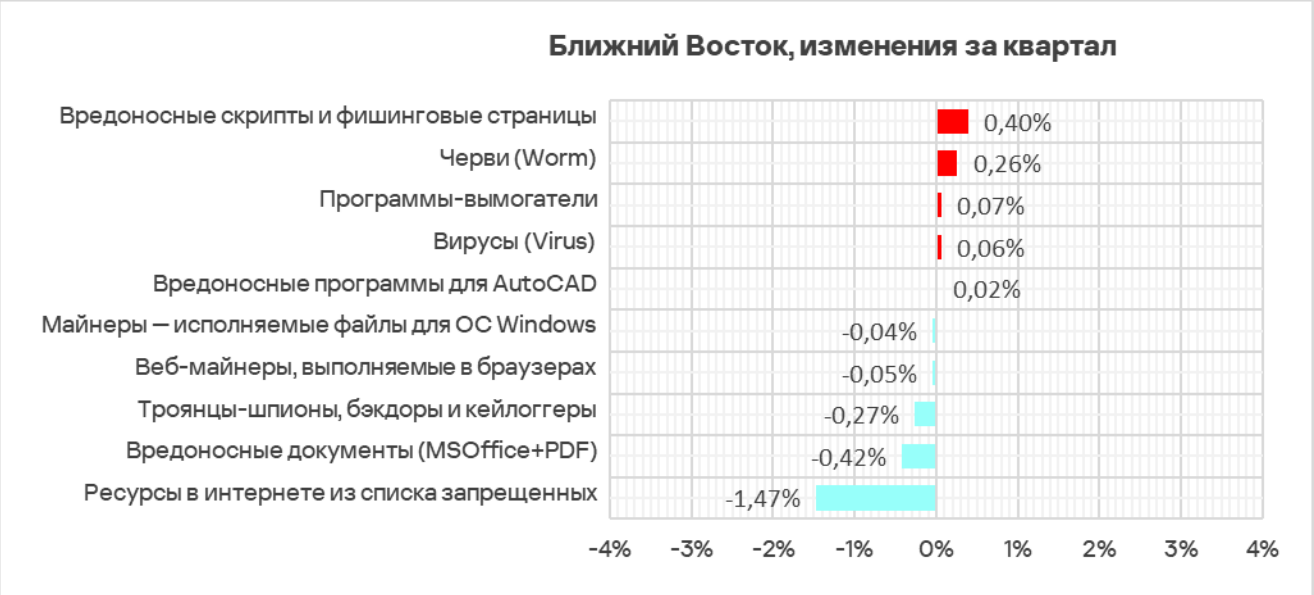


Основные категории угроз, которые распространяются через сетевые папки: вирусы, черви и шпионские программы.



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 значениями у региональных показателей следующих категорий угроз:

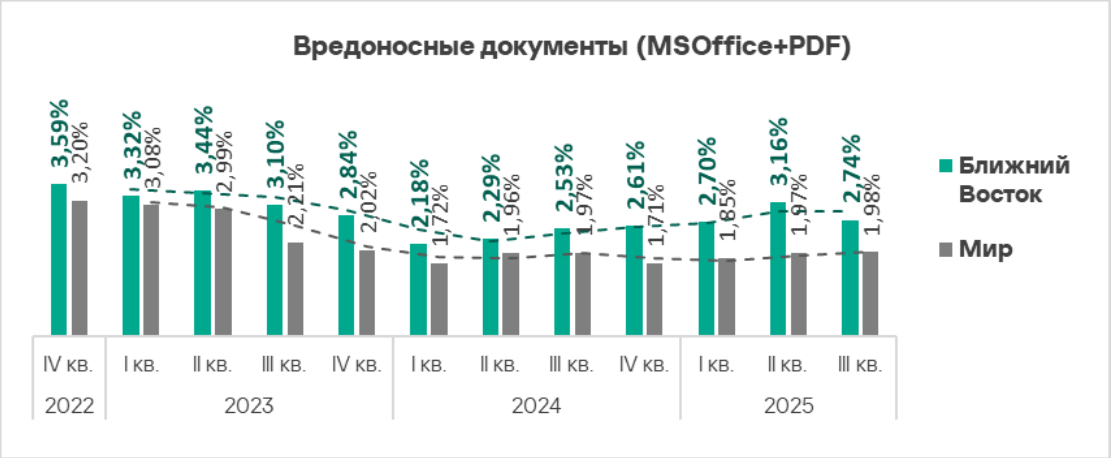
- вредоносные документы — в 1,4 раза, третье место среди регионов;
- вредоносные скрипты и фишинговые страницы — в 1,3 раза, четвертое место среди регионов;
- шпионские программы — в 1,3 раза, четвертое место среди регионов;
- вирусы — в 1,4 раза, четвертое место среди регионов;
- черви — в 1,7 раза, третье место среди регионов;
- программы-вымогатели — в 1,9 раза, первое место среди регионов.

По показателям веб-майнеров Ближний Восток занимает третье место среди регионов.

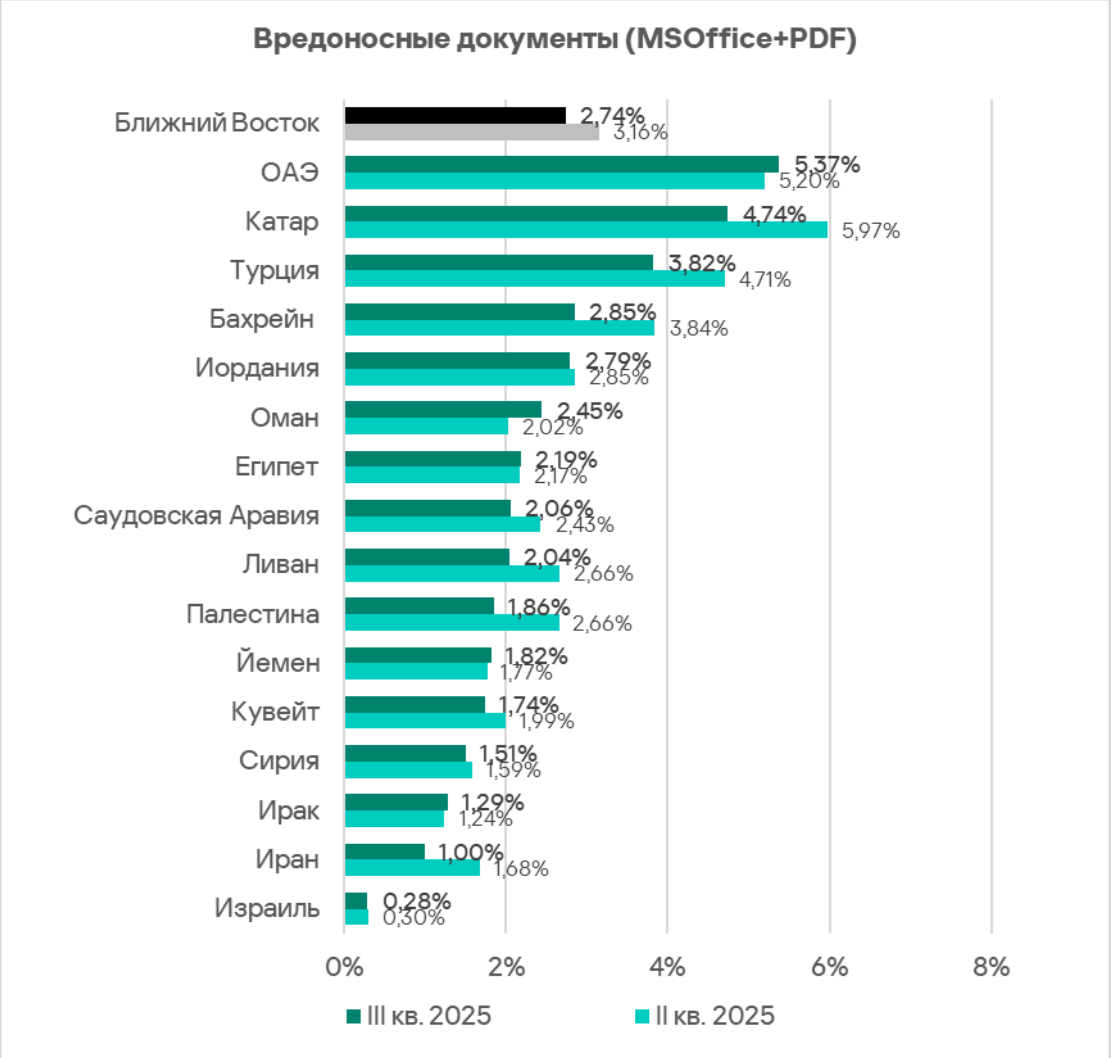
Вредоносные документы

В третьем квартале 2025 года Ближний Восток по показателю вредоносных документов занимает третье место с 2,74%. Это в 5,2 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 третьем квартале 2025 года показатель за квартал уменьшился.



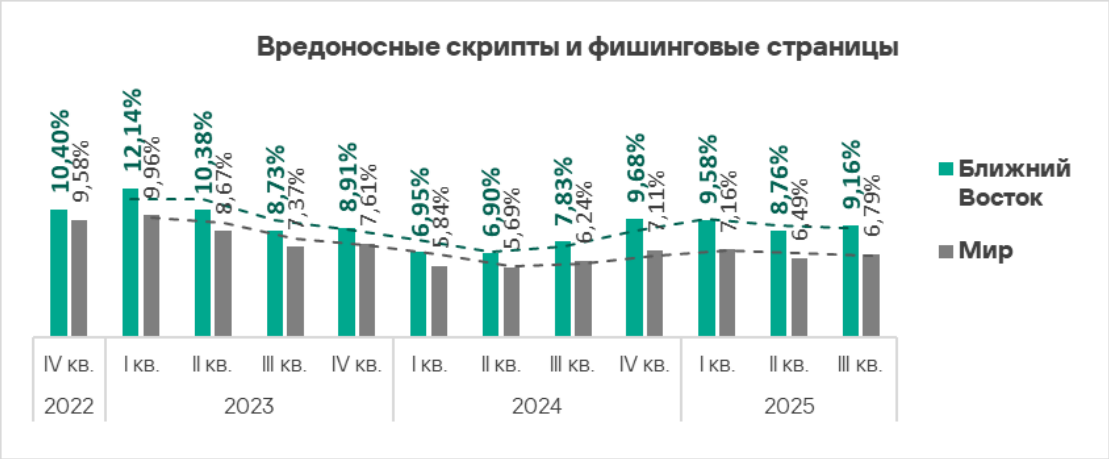
Среди стран и территорий региона по этому показателю лидируют ОАЭ с 5,37%. Рейтинг замыкает Израиль с 0,28% — это в 3,6 раза меньше показателя предшествующего в рейтинге Ирана.



Две страны из тройки лидеров этого рейтинга — ОАЭ и Катар — возглавляют также рейтинги по вредоносным документам и вредоносным скриптам и фишинговым страницам, а также по угрозам из почтовых клиентов. Они же входят в тройку стран — лидеров по доле компьютеров АСУ, где были заблокированы шпионские программы.

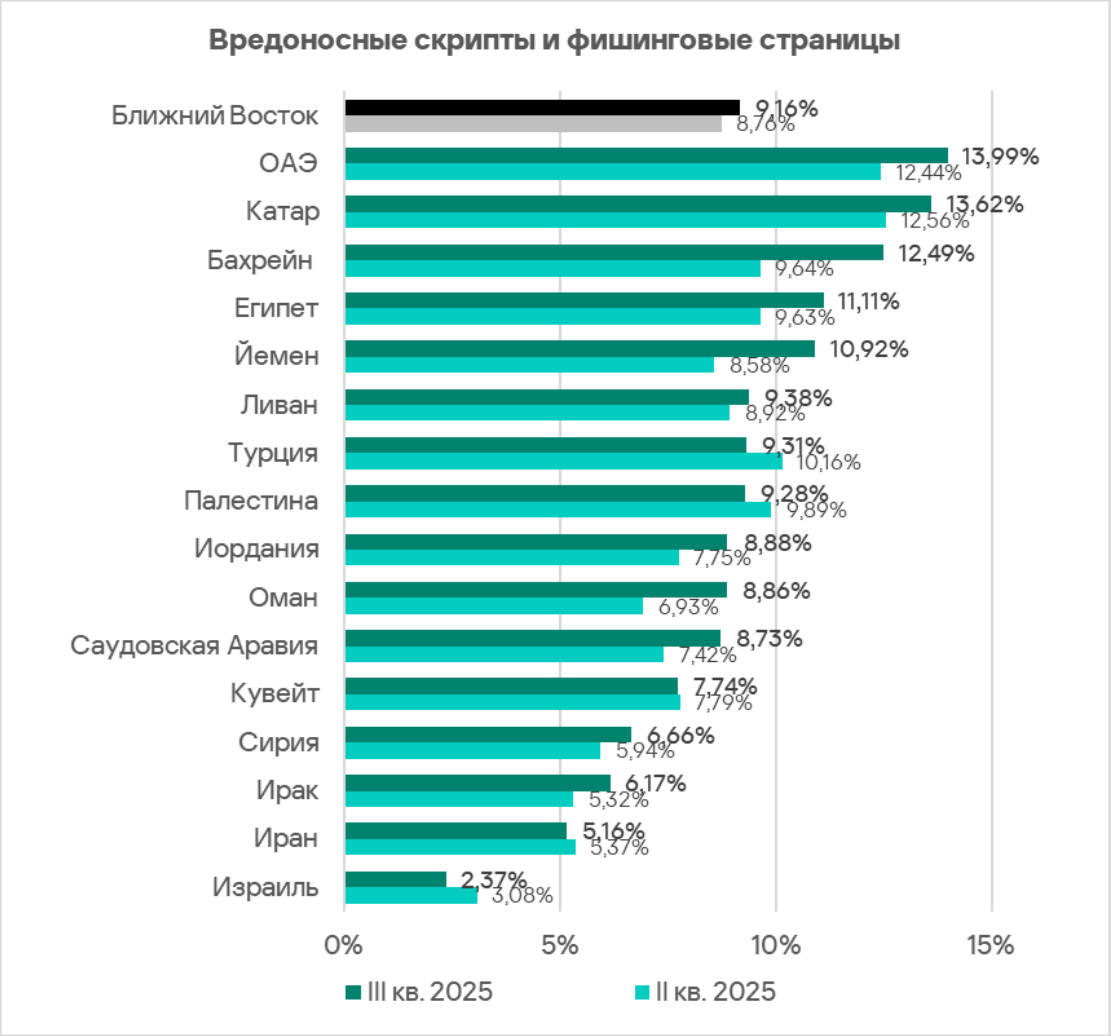
Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Ближний Восток занимает в соответствующем рейтинге регионов четвертое место с 9,16%. Этот показатель в 3,6 раза больше, чем в Северной Европе, где он наименьший.



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 13,99%. Наименьший показатель — в Израиле (2,37%), и он в 2,1 раза меньше, чем показатель предшествующего в рейтинге Ирана.

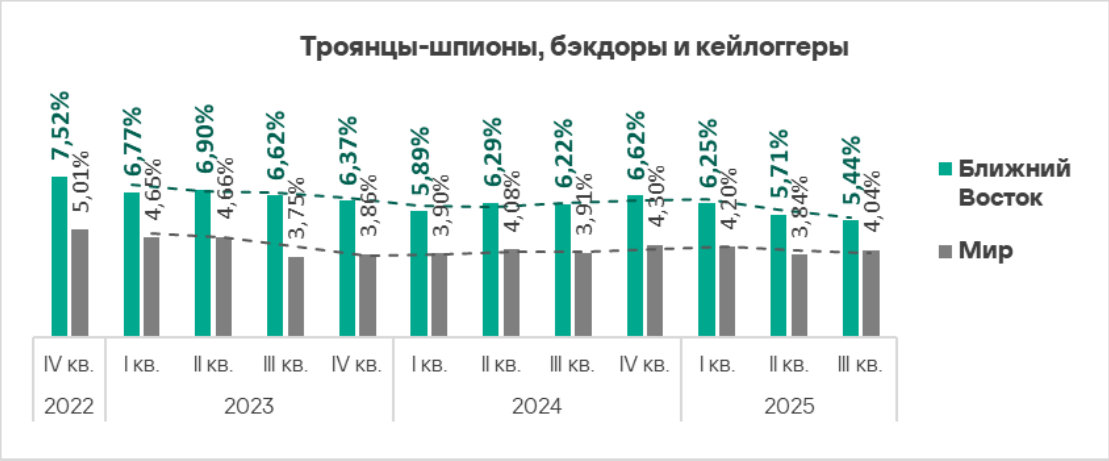


Две страны, лидирующие в этом рейтинге, — ОАЭ и Катар — возглавляют также рейтинг по показателям вредоносных документов и рейтинг стран региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах. Они же входят в тройку стран-лидеров по шпионским программам (возглавляет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

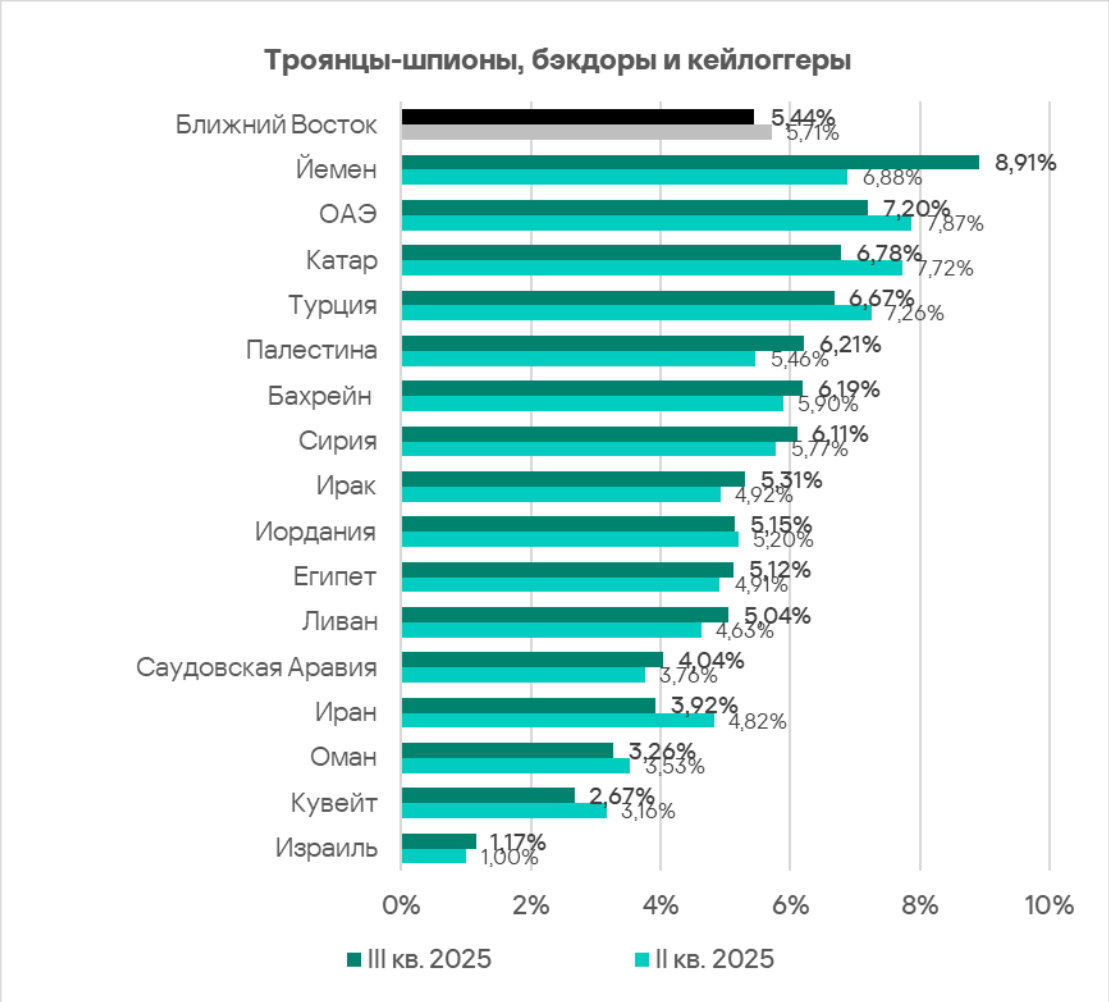
Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, Ближний Восток находится на четвертом месте с 5,44%. Это в 3,9 раза больше, чем в Северной Европе, где этот показатель наименьший.

На Ближнем Востоке доля компьютеров АСУ, на которых блокируются шпионские программы, снижается третий квартал подряд, в третьем квартале 2025 года она была минимальной за три года.



Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются шпионские программы, в третьем квартале 2025 года лидирует Йемен с 8,91%. В этой стране значение за квартал увеличилось в 1,3 раза. Наименьший показатель – в Израиле, он в 2,3 раза меньше, чем показатель предшествующего в рейтинге Кувейта.



Шпионские программы в регионе блокируются во всех источниках угроз, но чаще всего эта угроза распространяется 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.

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 четвертом месте среди регионов по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных устройств. Третье место у региона по показателю червей, четвертое — по показателю вирусов.

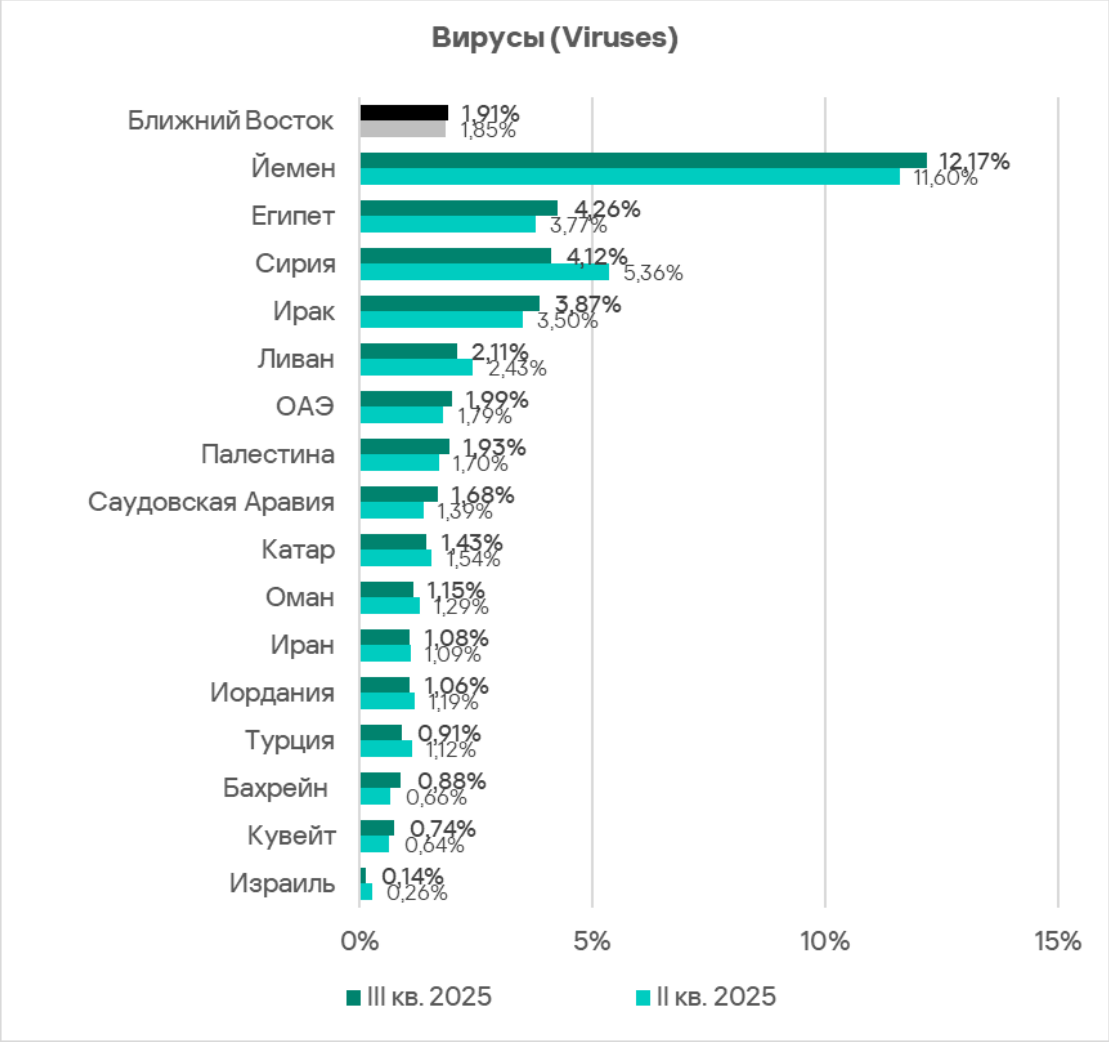
Доля компьютеров АСУ, на которых блокируются черви, на Ближнем Востоке — 2,08%. Это в 9,5 раза больше, чем в Северной Европе, регионе с минимальным показателем.

Доля компьютеров АСУ, на которых блокируются вирусы, на Ближнем Востоке — 1,91%. Это в 11,9 раза больше, чем в регионе с минимальным показателем — Австралии и Новой Зеландии.

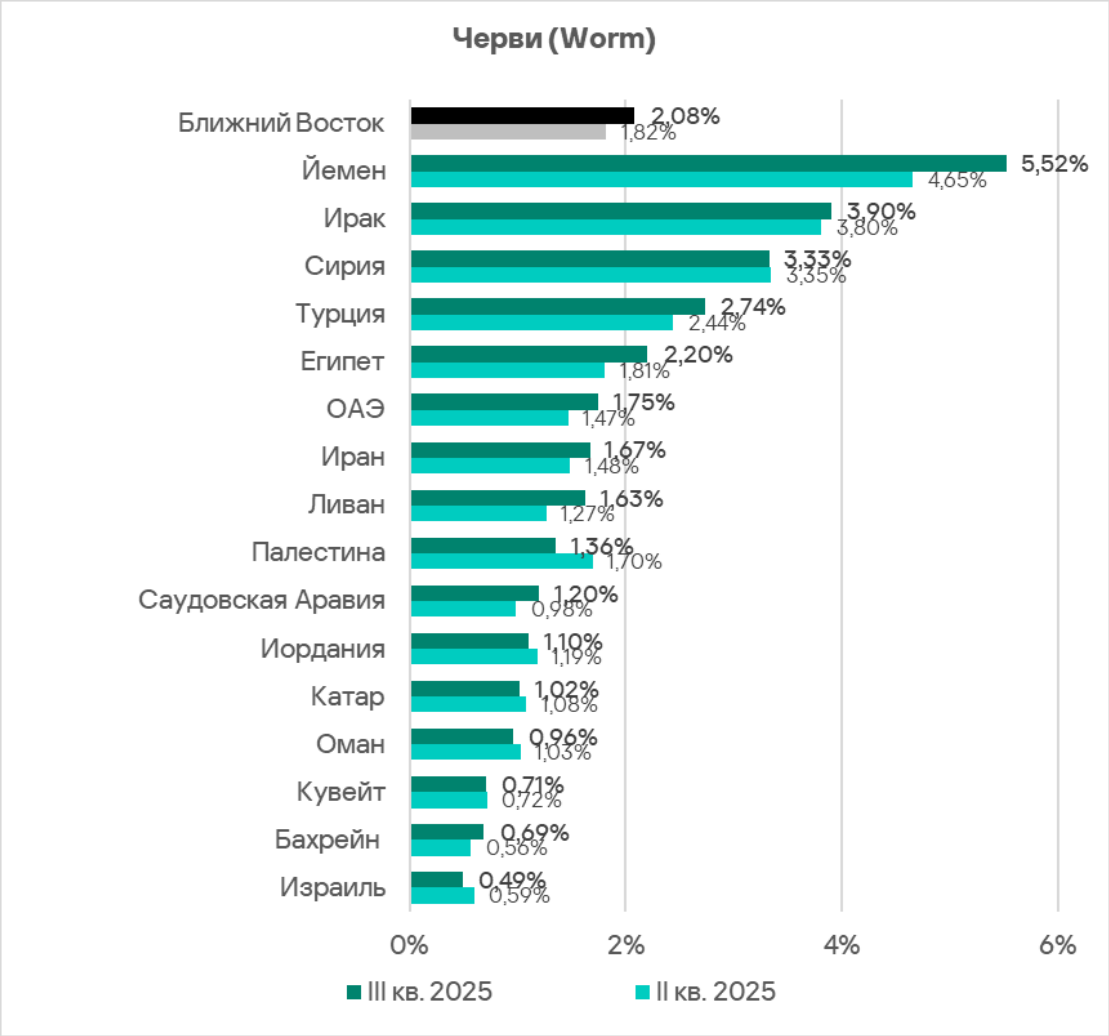
Показатель червей и вирусов, как и доля угроз со съемных носителей в целом, с некоторыми колебаниями постепенно снижается, хотя и отстает в этом показателей съемных носителей. В третьем квартале 2025 года значения обеих категорий угроз увеличились.

Среди стран и территорий региона по доле компьютеров АСУ, на которых блокируются и черви, и вирусы, с большим отрывом лидирует Йемен.

В случае вирусов показатель Йемена (12,17%) превышает показатель Египта, который занимает второе место в этом рейтинге, в 2,9 раза. По сравнению же с показателем Израиля, который замыкает рейтинг, значение в Йемене больше в 86,9 раза.



Разница показателя червей в Йемене (5,52%) и в остальных странах заметная, но не столь значительная.

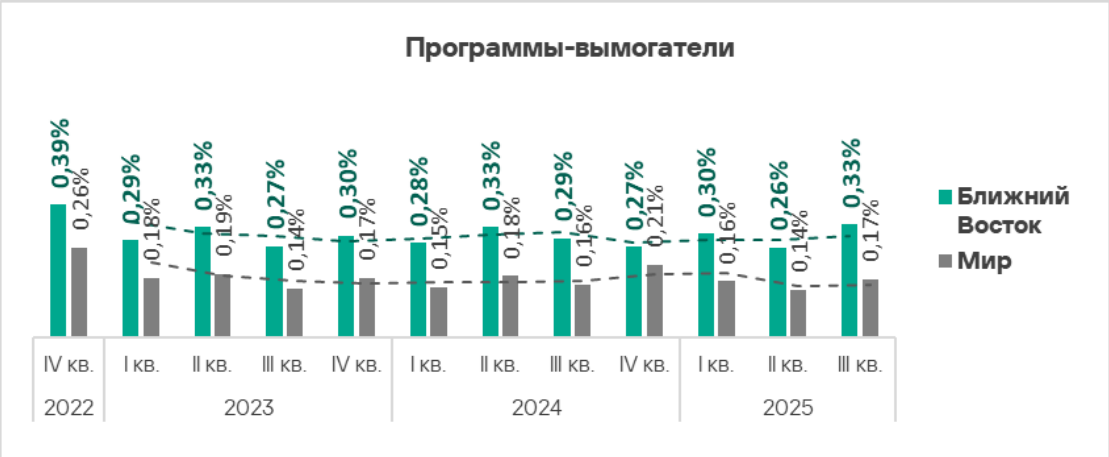


Программы-вымогатели

На Ближнем Востоке доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, стабильно высокая и почти вдвое превышает среднемировой показатель. Регион лидировал по этому показателю в 2024 году, но в двух первых кварталах 2025 года был на втором месте.

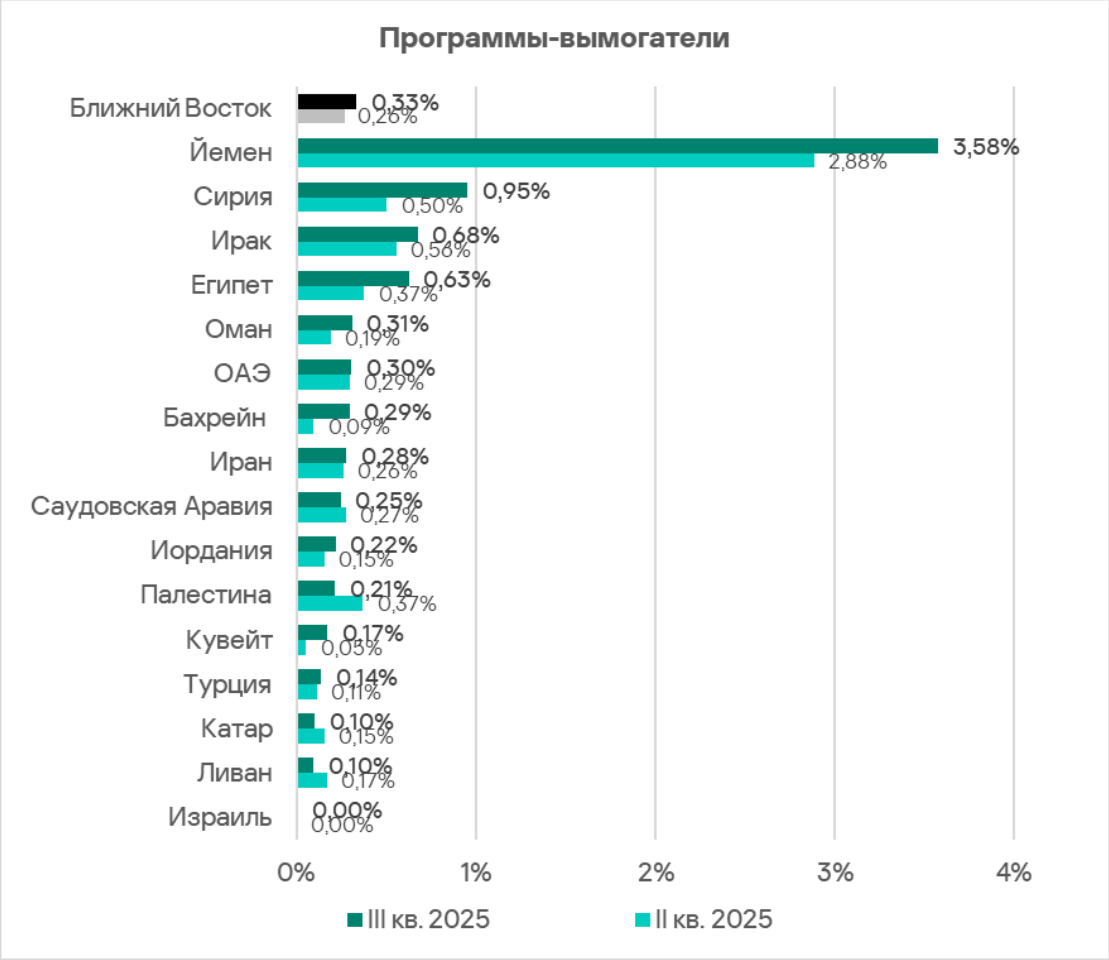
В третьем квартале 2025 года Ближний Восток вернул первенство среди регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели.

Показатель в регионе с 2023 года колеблется в диапазоне от 0,26% до 0,33%. В третьем квартале 2025 года он подрос до 0,33%. Это в 6,6 раза больше, чем в Северной Европе, где показатель наименьший.



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 3,58%. По

сравнению с Сирией, которая занимает второе место в этом рейтинге, показатель Йемена больше в 3,8 раза.



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

Отрасли

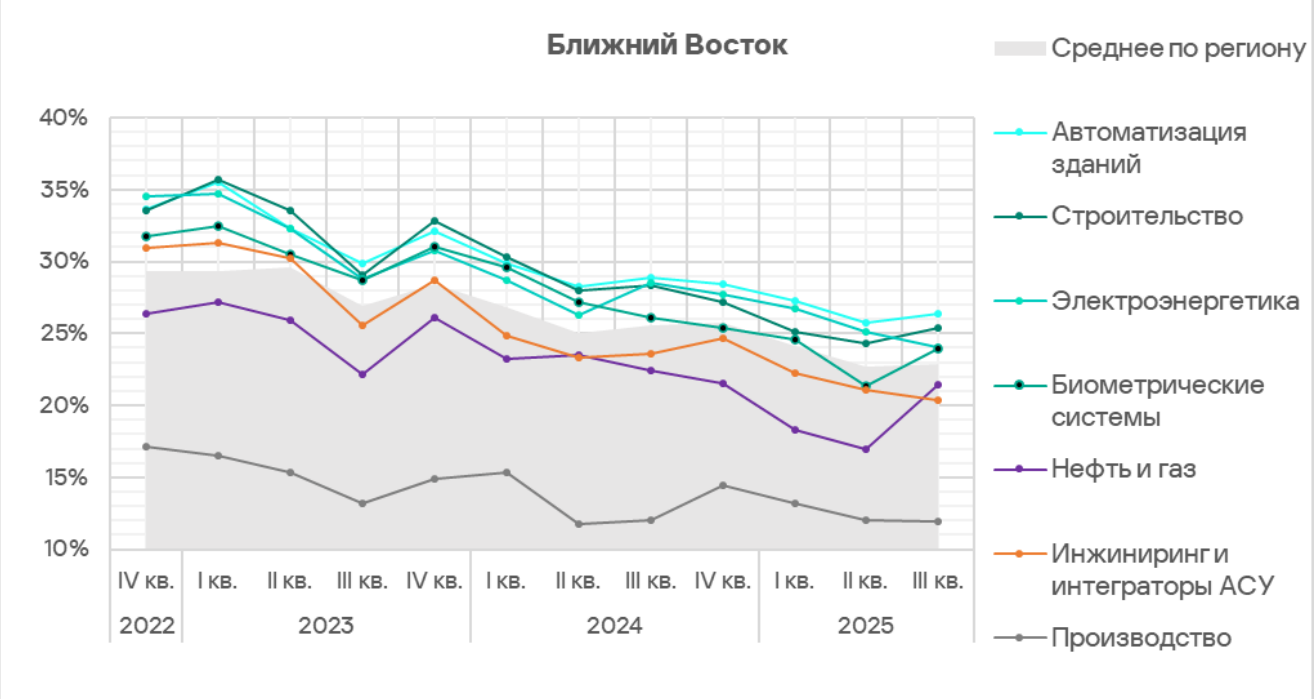
Наиболее часто встречающейся с угрозами отраслью региона среди рассмотренных в отчете является автоматизация зданий.

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 1,2 раза;
- нефть и газ — в 1,4 раза.

В первом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась во всех отраслях, показатели которых выше среднемировых.

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, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	8,48%	9,25%	10,30%	8,31%	7,57%	10,07%	4,86%	8,63%
Почтовые клиенты	5,23%	8,28%	4,36%	3,65%	1,86%	5,49%	1,80%	5,53%
Съемные носители	1,16%	0,68%	0,66%	0,46%	0,79%	0,55%	0,38%	0,62%
Сетевые папки	0,05%	0,10%	0,06%	0,03%	0,11%	0,12%	0,06%	0,06%
Показатель отрасли в регионе	23,93%	26,41%	24,08%	20,37%	21,41%	25,35%	11,96%	

Показатели категорий угроз в отраслях на Ближнем Востоке, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	3,62%	3,93%	4,50%	3,67%	3,79%	4,02%	2,29%	3,72%
Вредоносные скрипты и фишинговые страницы	9,75%	11,96%	9,07%	7,15%	6,44%	9,44%	4,20%	9,16%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,52%	7,87%	4,90%	3,89%	3,50%	4,07%	2,23%	5,44%
Черви (Worm)	2,43%	2,68%	2,28%	1,69%	1,69%	1,44%	1,24%	2,08%
Майнеры — исполняемые файлы для ОС Windows	0,48%	0,46%	0,50%	0,51%	0,73%	0,97%	0,26%	0,45%
Вредоносные документы (MSOffice+PDF)	2,72%	4,23%	2,14%	1,73%	1,07%	2,07%	0,90%	2,74%
Вирусы (Virus)	3,25%	2,62%	2,10%	1,12%	1,53%	2,36%	1,19%	1,91%
Программы-вымогатели	0,48%	0,48%	0,33%	0,21%	0,28%	0,23%	0,09%	0,33%
Веб-майнеры, выполняемые в браузерах	0,26%	0,27%	0,29%	0,32%	0,40%	0,68%	0,17%	0,28%
Вредоносные программы для AutoCAD	0,26%	0,19%	0,15%	0,19%	0,28%	1,24%	0,29%	0,25%
Показатель отрасли в регионе	23,93%	26,41%	24,08%	20,37%	21,41%	25,35%	11,96%	

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).

В большинстве отраслей региона высока доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы. Ближний Восток занимает второе место в рейтингах регионов по этому показателю в отраслях:

- автоматизация зданий;
- строительство;
- электроэнергетика;
- нефть и газ.

Ближний Восток занимает не ниже четвертого места в рейтингах регионов по показателю программ-вымогателей во всех отраслях, кроме производства:

- нефть и газ – первое место;
- автоматизация зданий — второе место;
- строительство — третье место;
- инжиниринг и интеграторы АСУ — третье место;

- электроэнергетика — четвертое место;
- биометрические системы — четвертое место.

Ближний Восток занимает не ниже четвертого места в рейтингах регионов по показателям самораспространяющегося ПО (черви и вирусы) и вредоносных программ для AutoCAD. Эти категории вредоносных объектов попали в топ-4 вместе или по отдельности во всех отраслях, кроме электроэнергетики.

По показателю вредоносных программ для AutoCAD в OT-инфраструктуре биометрические системы Ближний Восток лидирует среди регионов.

Автоматизация зданий

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

В глобальном рейтинге по индустриям во всех регионах автоматизация зданий на Ближнем Востоке занимает:

- пятое место по показателю угроз, доставляемых через почтовые клиенты;
- пятое место по доле компьютеров АСУ, на которых блокировались вредоносные скрипты и фишинговые страницы.

Среди регионов по показателям в отрасли Ближний Восток занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов и в сетевых папках;
- четвертое место по показателям угроз из интернета и на съемных носителях;
- второе место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, а также программы-вымогатели;
- третье место по показателю червей, вирусов и вредоносных программ для AutoCAD;
- четвертое место по показателю шпионских программ.

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;
- третье место по показателям угроз из интернета, на съемных носителях и в сетевых папках;

- первое место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви, программы-вымогатели;
- второе место по показателю вирусов;
- третье место по показателю ресурсов в интернете из списка запрещенных.

Строительство

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

В глобальном рейтинге по индустриям во всех регионах отрасль на Ближнем Востоке занимает:

- пятое место по доле компьютеров АСУ, на которых блокировались веб-майнеры.

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;
- четвертое место по показателю съемных носителей;
- второе место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы;
- третье место по показателям майнеров обеих категорий, червей и программ-вымогателей;
- четвертое место по показателю вирусов и вредоносных программ для AutoCAD.

Среди отраслей в регионе строительство занимает:

- первое место по показателю угроз в сетевых папках;
- второе место по показателям угроз из интернета и почтовых клиентов;
- первое место по показателям майнеров обеих категорий и вредоносных программ для AutoCAD;
- второе место среди отраслей региона по показателю интернет-ресурсов из списка запрещенных;
- третье место в регионе по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, вирусы.

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;
- второе место по показателю угроз в сетевых папках;
- третье место по показателю угроз на съемных носителях, четвертое — по показателю угроз в интернете;
- второе место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы;
- четвертое место по показателям следующих категорий угроз: вредоносные документы, шпионские программы, программы-вымогатели.

Среди отраслей в регионе электроэнергетика занимает:

- первое место по показателю угроз из интернета;
- первое место по показателю ресурсов в интернете из списка запрещенных;
- третье место по показателям следующих категорий угроз: вредоносные документы, шпионские программы, черви 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 OT-инфраструктуре биометрические системы.

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

- третье место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях и в сетевых папках;
- четвертое место по показателям угроз из интернета;
- первое место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD;
- третье место по показателям вирусов;
- четвертое место по показателям червей и программ-вымогателей.

Среди отраслей в регионе OT-инфраструктура биометрические системы занимает:

- первое место по показателю угроз на съемных носителях;
- третье место по показателю угроз из почтовых клиентов;
- первое место по показателю вирусов;
- второе место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви и программы-вымогатели.

Нефть и газ

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

Среди регионов по показателям в отрасли Ближний Восток занимает:

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

Среди отраслей в регионе нефтегазовая отрасль занимает:

- второе место по показателям угроз на съемных носителях и в сетевых папках;
- второе место по показателям майнеров обеих категорий;
- третье место по показателю вредоносных программ для AutoCAD.

Инжиниринг и интеграторы АСУ

Ближний Восток находится на четвертом 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:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, на съемных носителях и в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокируются черви;
- третье место по показателю программ-вымогателей, четвертое — по показателю шпионских программ.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает третье место по показателям майнеров обеих категорий.

Производство

Ближний Восток находится на 12-м месте по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди регионов по показателям в отрасли Ближний Восток занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- четвертое место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD.

Среди отраслей в регионе производство занимает второе место по показателю вредоносных программ для AutoCAD.

Методика подготовки статистики

В отчете представлены результаты анализа статистических данных, полученных с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые добровольно подтвердили свое согласие на их анонимную передачу и обработку с целью, описанной в Соглашении KSN для установленного на их компьютере продукта «Лаборатории Касперского».

Подключение к сети KSN дает нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счет обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за ее объема и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и 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