Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Европа. Второй квартал 2025 года

23.09.2025

Версия 1.0

Восточная Европа

Основные проблемы кибербезопасности в регионе

Высокий риск целевых атак

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

В Восточной Европе доля компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, в 1,3 раза выше среднемировых значений.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, превышает среднемировой показатель в 1,4 раза.

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

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 напрямую на кражу данных аутентификации.

Доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, в Восточной Европе в 1,1 раза выше среднемирового показателя.

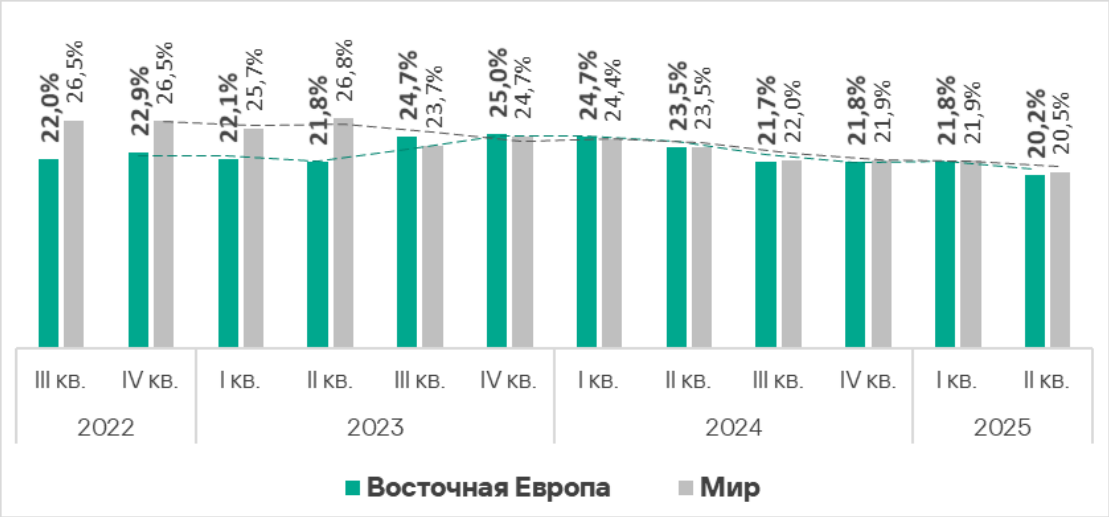
Высокий показатель шпионских программ

Доля компьютеров АСУ, на которых блокируются шпионские программы, в Восточной Европе в 1,1 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.

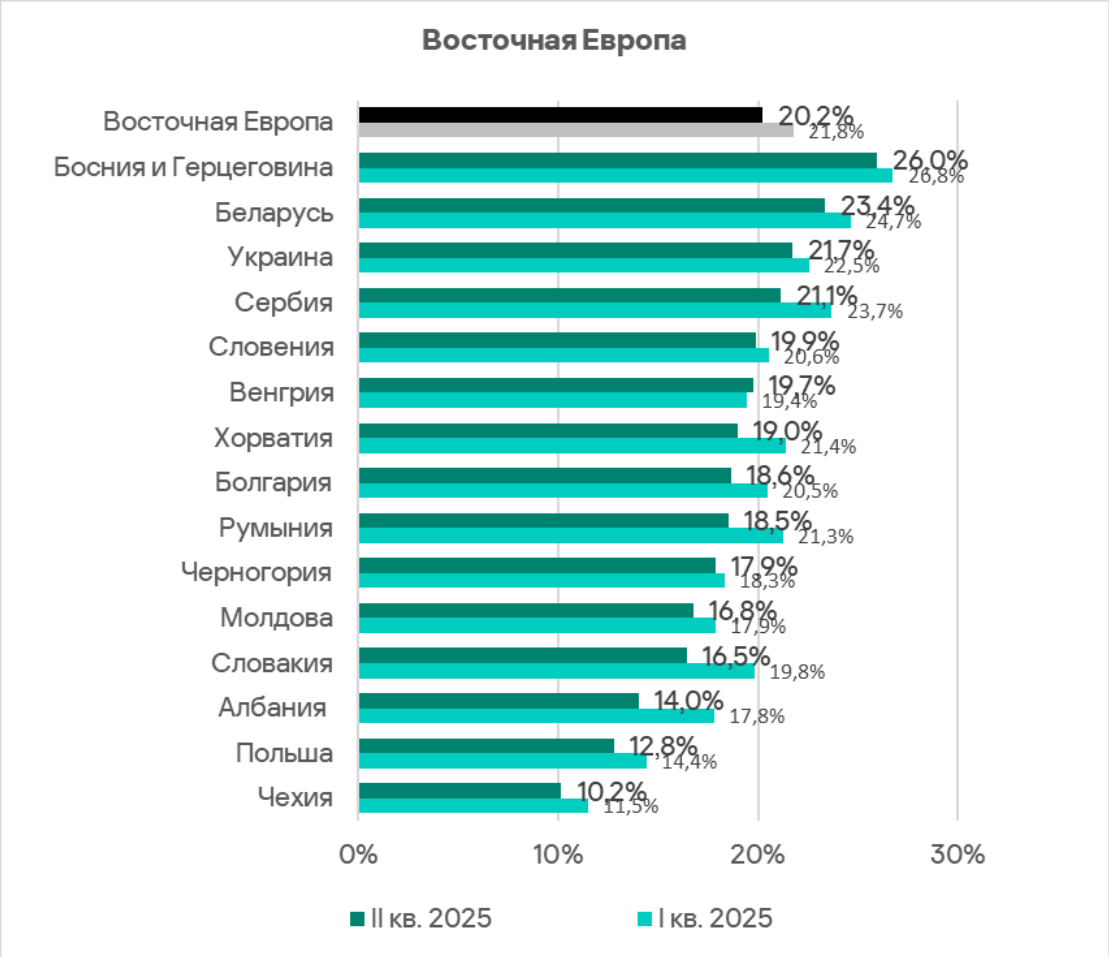
Статистика по всем угрозам

Во втором квартале 2025 года Восточная Европа заняла шестое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Это самая высокая позиция среди регионов Европы. До второго квартала 2023 года регион не поднимался в рейтинге выше девятого места.

Во втором квартале 2025 года показатель в регионе уменьшился до 20,2% — это немного ниже среднемирового значения и в 1,8 раза выше, чем в Северной Европе, где значение наименьшее из всех регионов.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, лидирует Босния и Герцеговина с 26,0%. Наименьший показатель в Чехии — 10,2%.

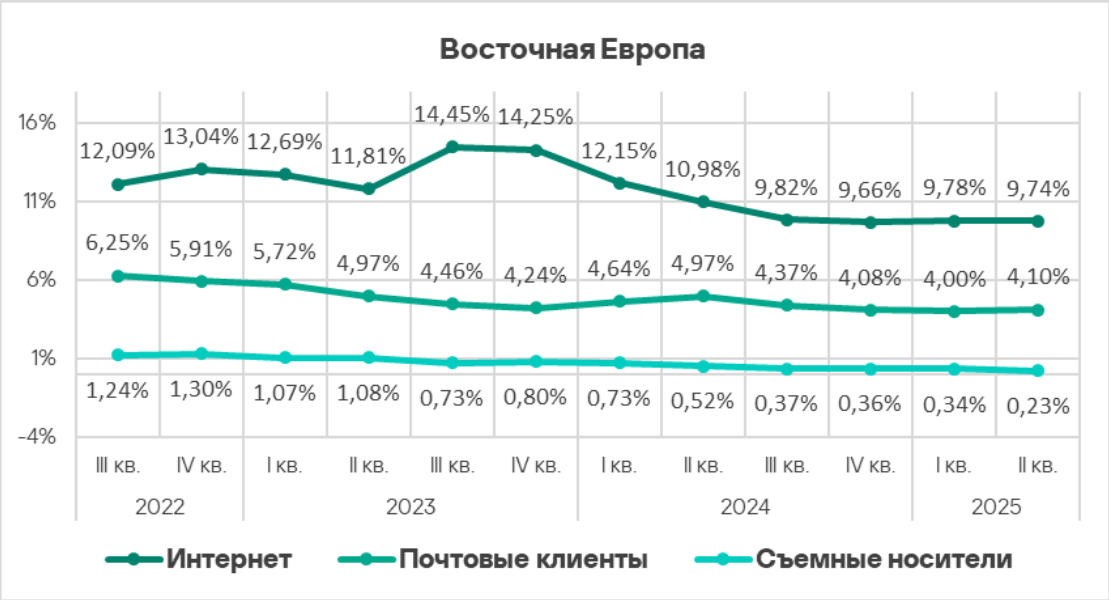


Источники угроз

Показатели всех источников угроз, кроме почтовых клиентов, в Восточной Европе ниже среднемировых. Доля компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, в регионе в 1,3 выше среднемирового показателя.

Вредоносные объекты в регионе распространяются преимущественно через интернет и почту. В рейтинге по доле компьютеров АСУ, на которых угрозы блокирвуются в сетевых папках, Восточная Европа занимает предпоследнее место.

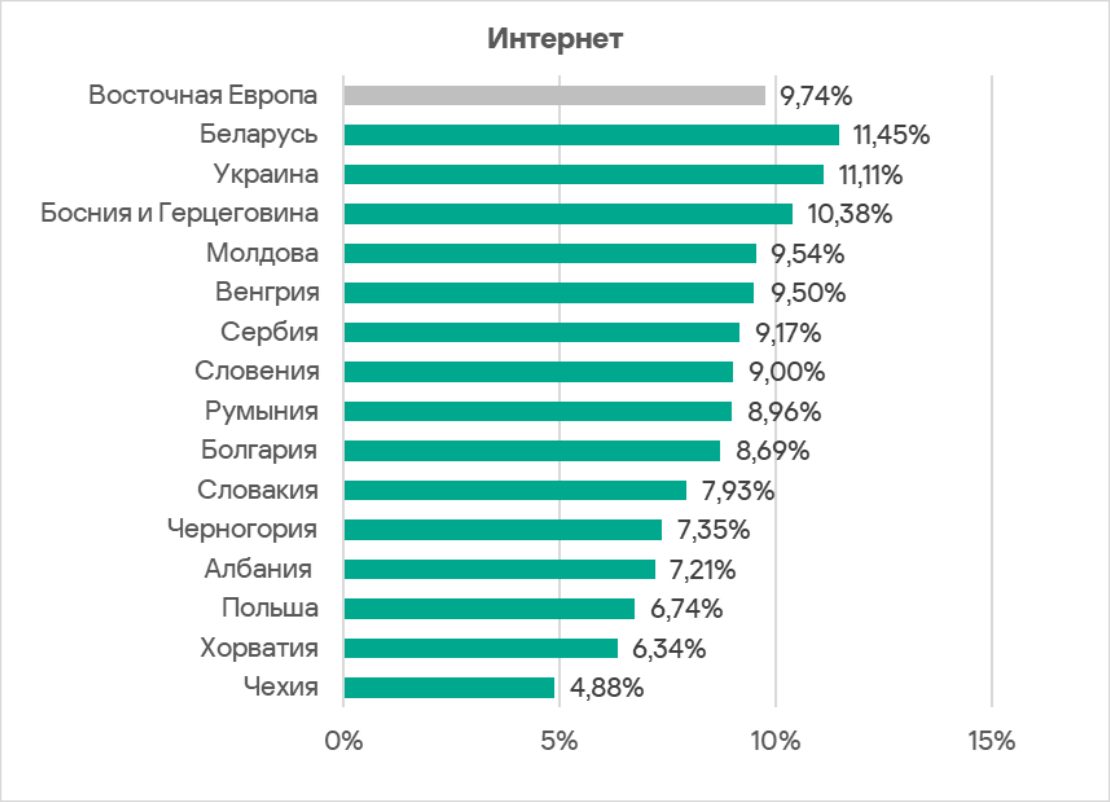
Во втором квартале 2025 года из всех источников угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного увеличилась только у почтовых клиентов.



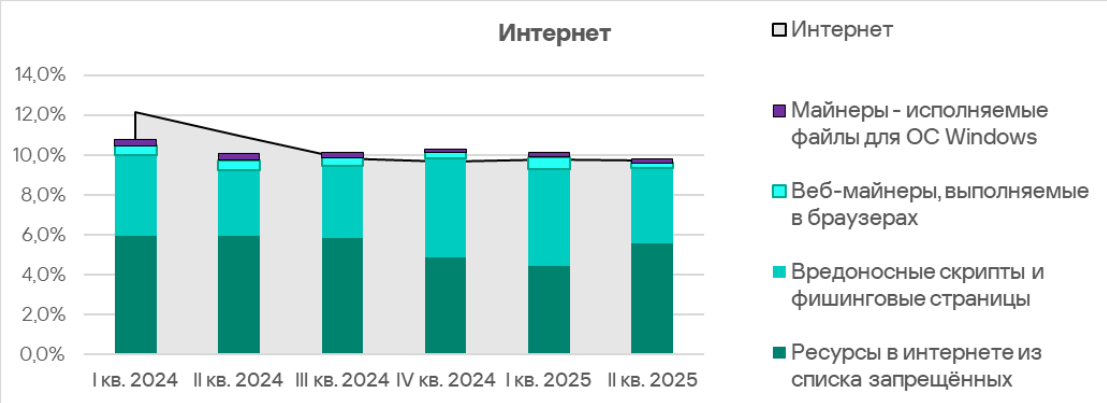
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Восточная Европа занимает пятое место в рейтинге регионов с показателем 9,74%, который превышает минимальный — у Восточной Азии — в 1,5 раза.

Показатели стран региона варьируют от 4,88% в Чехии до 11,45% в Беларуси.



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



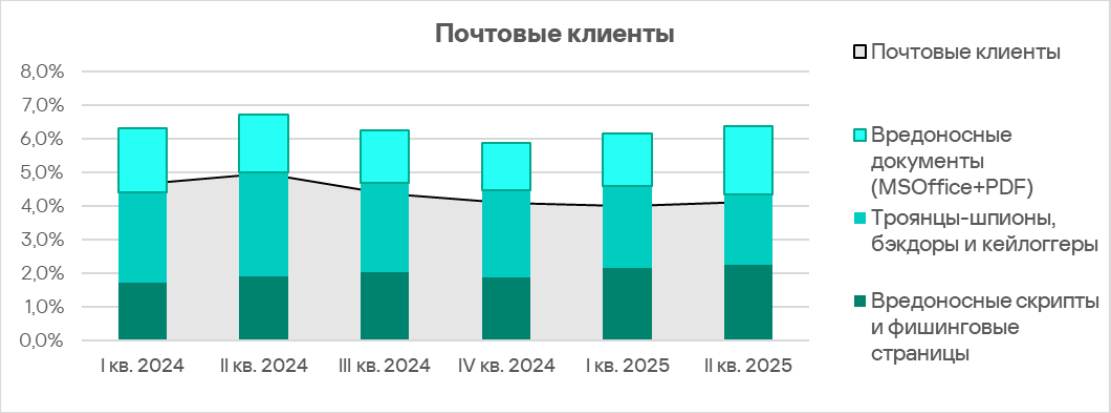
По показателю категории ресурсы в интернете из списка запрещенных Восточная Европа занимает третье место в соответствующем рейтинге регионов. По показателю майнеров в формате исполняемых файлов — четвертое место среди регионов.

Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Восточная Европа занимает шестое место среди регионов с показателем 4,10%. Это в 5,1 раза больше, чем в России, которая замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, лидирует Босния и Герцеговина с 11,55%. Наименьший показатель — в Украине (0,45%).

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



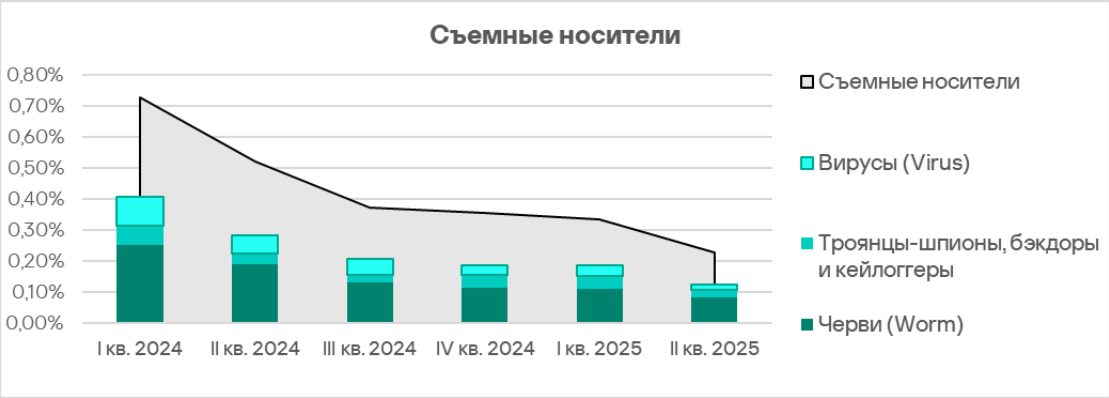
Тройка стран-лидеров по почтовым клиентам — Босния и Герцеговина, Хорватия и Сербия — также занимают верхние строчки в рейтинге по показателям вредоносных документов и шпионских программ. Босния и Герцеговина и Сербия лидируют еще и в рейтинге по показателям категории вредоносные скрипты и фишинговые страницы.

Съемные носители

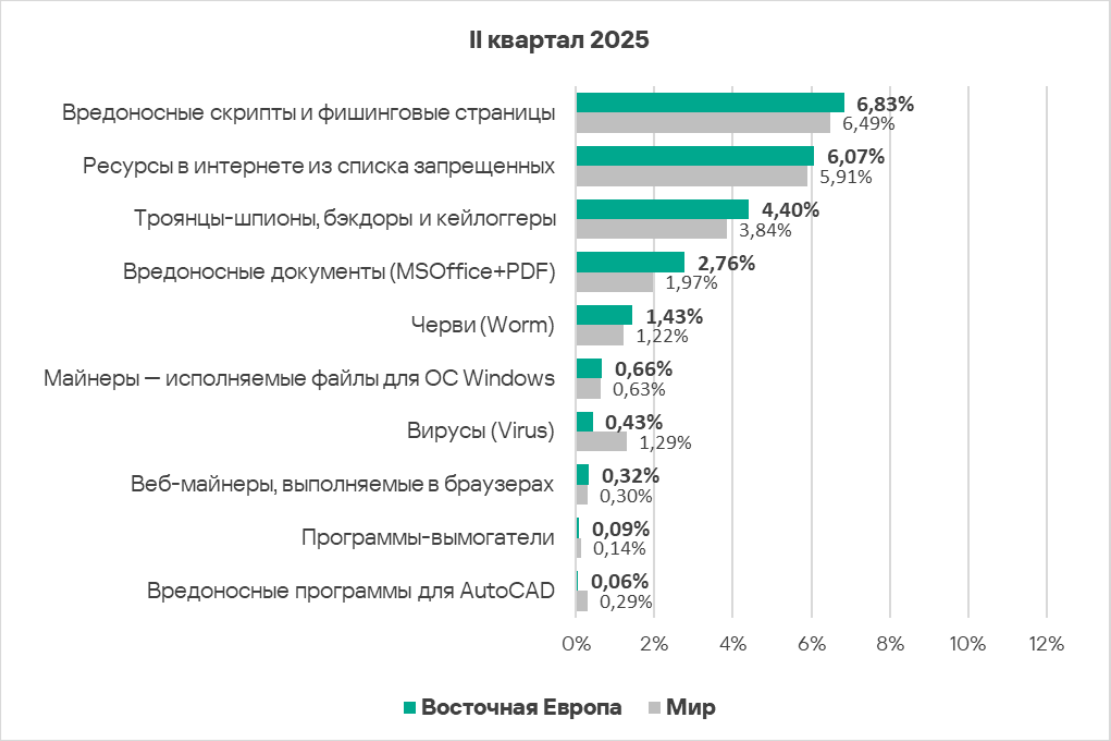
По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, во втором квартале 2025 года Восточная Европа занимает среди регионов седьмое место с 0,23%. В Северной Америке (Канада), которая занимает последнее место в рейтинге, показатель меньше в 8,6 раза.

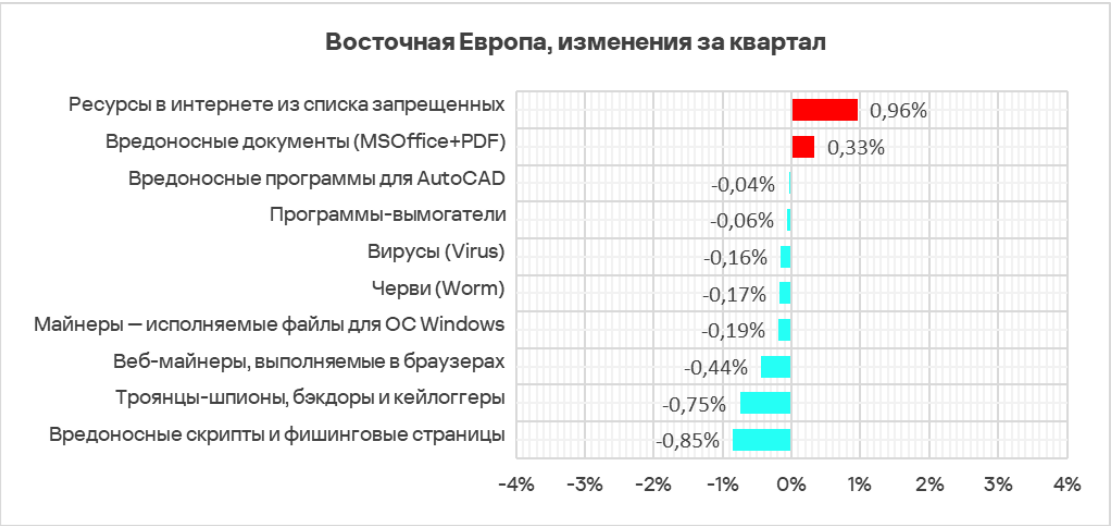
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с отрывом лидируют Украина с 0,44% и Болгария с 0,43%.

Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, шпионское ПО и вирусы.



Категории угроз





По сравнению с мировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

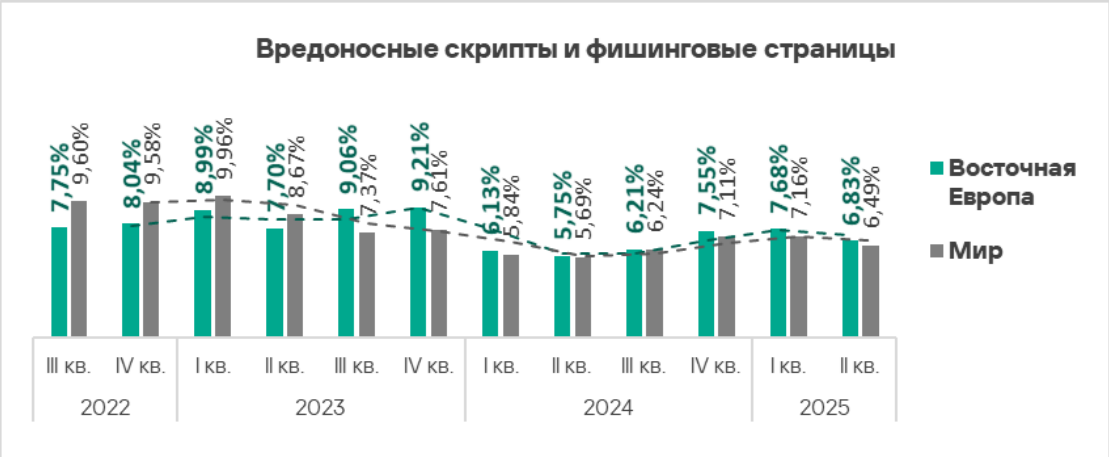
- вредоносные документы — в 1,4 раза;
- вредоносные скрипты и фишинговые страницы — в 1,1 раза;
- шпионские программы — в 1,1 раза;
- черви — в 1,2 раза;
- веб-майнеры — в 1,1 раза.

Вредоносные скрипты и фишинговые страницы, а также вредоносные документы используются злоумышленниками для распространения целевого вредоносного ПО — в том числе шпионских программ.

Босния и Герцеговина, Хорватия и Сербия входят в тройку стран региона по угрозам из почтовых клиентов и по доле компьютеров АСУ, на которых блокируются вредоносные документы и шпионские программы. Босния и Герцеговина и Сербия лидируют также в рейтинге по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы.

Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Восточная Европа занимает седьмое место в соответствующем рейтинге регионов с 6,83%. Это в 2,2 раза больше, чем в Северной Европе, где этот показатель наименьший.



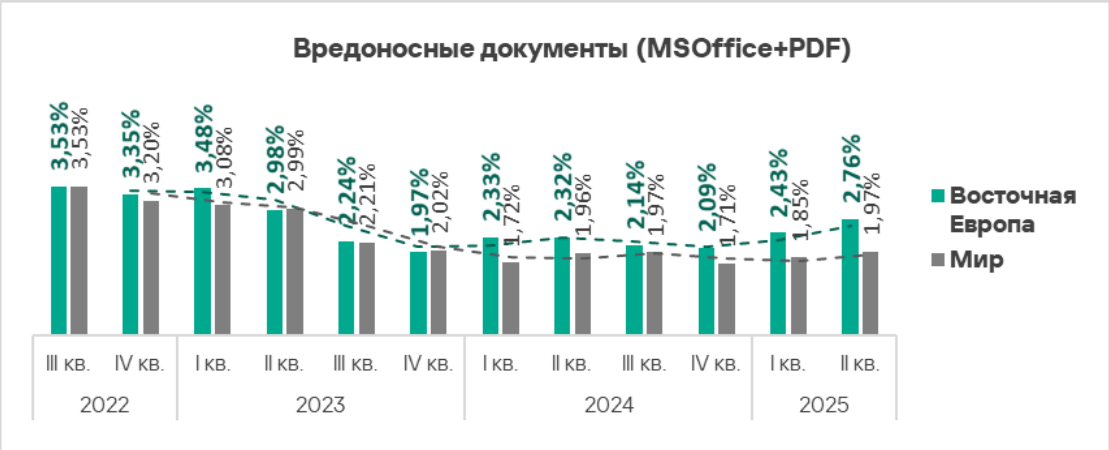
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Босния и Герцеговина с 12,49%.

Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

Вредоносные документы

Восточная Европа занимает пятое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы. Показатель в регионе — 2,76% — в 4,3 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, растет в регионе второй квартал подряд.



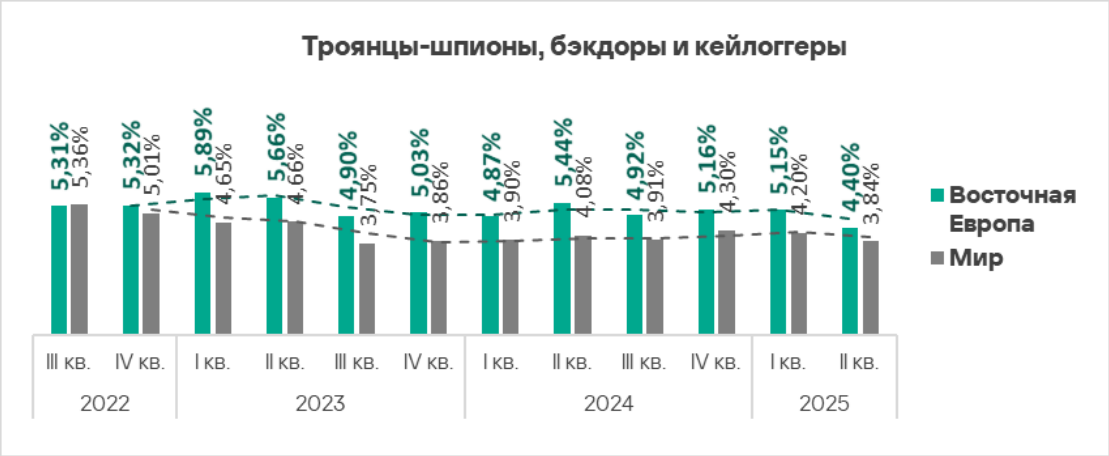
Среди стран региона по этому показателю лидирует Босния и Герцеговина с 7,70%.

Распространяются вредоносные документы преимущественно по электронной почте.

Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, в соответствующем рейтинге регионов Восточная Европа находится на шестом месте с 4,40%. Это в 3,2 раза больше, чем в Западной Европе, где этот показатель наименьший.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в Восточной Европе колеблется. Во втором квартале 2025 ода показатель был наименьшим за период с третьего квартала 2022 года.



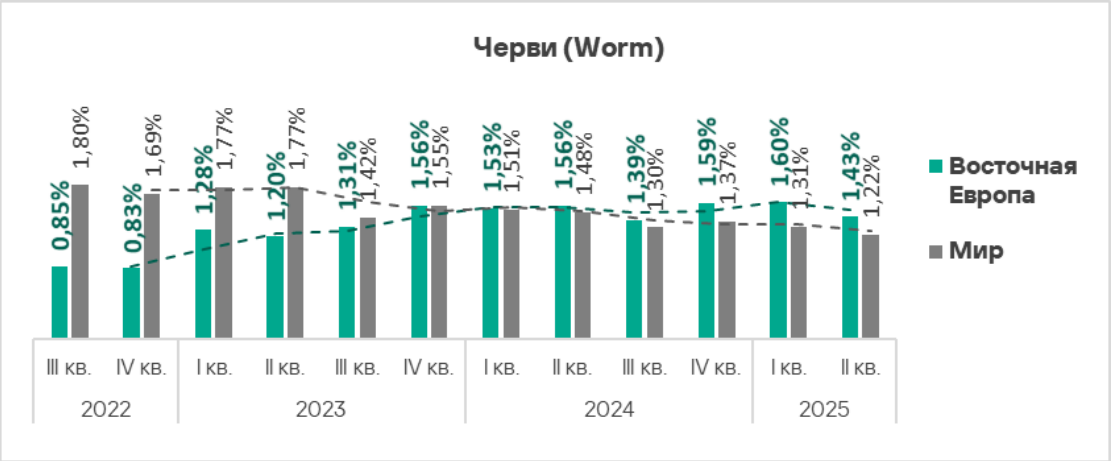
Среди стран региона по доле компьютеров АСУ, на которых блокируются шпионские программы, лидирует Босния и Герцеговина с 9,06%. Наименьший показатель — в Чехии (2,20%).

Шпионские программы в регионе блокируются во всех источниках угроз, преимущественно в почтовых клиентах.

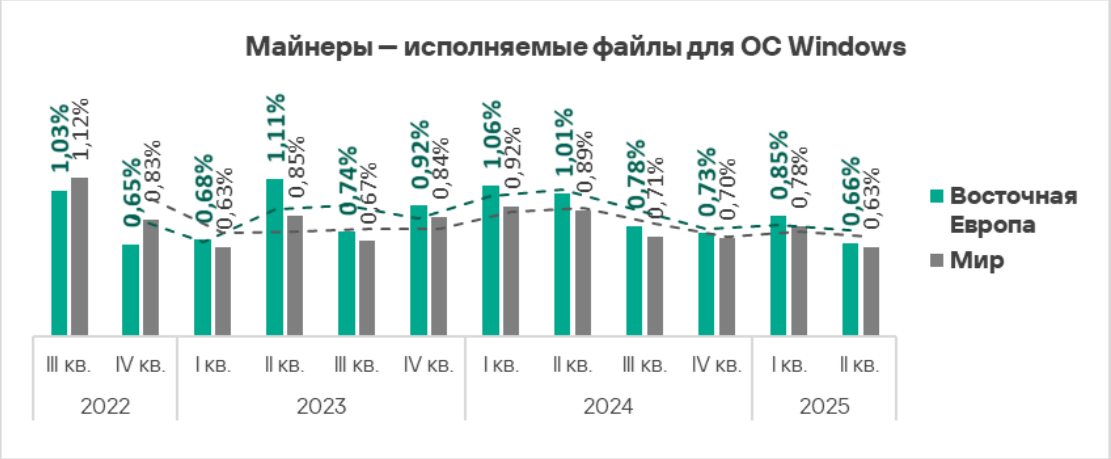
Черви и майнеры — исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых блокируются черви, Восточная Европа занимает пятое место в соответствующем рейтинге регионов с

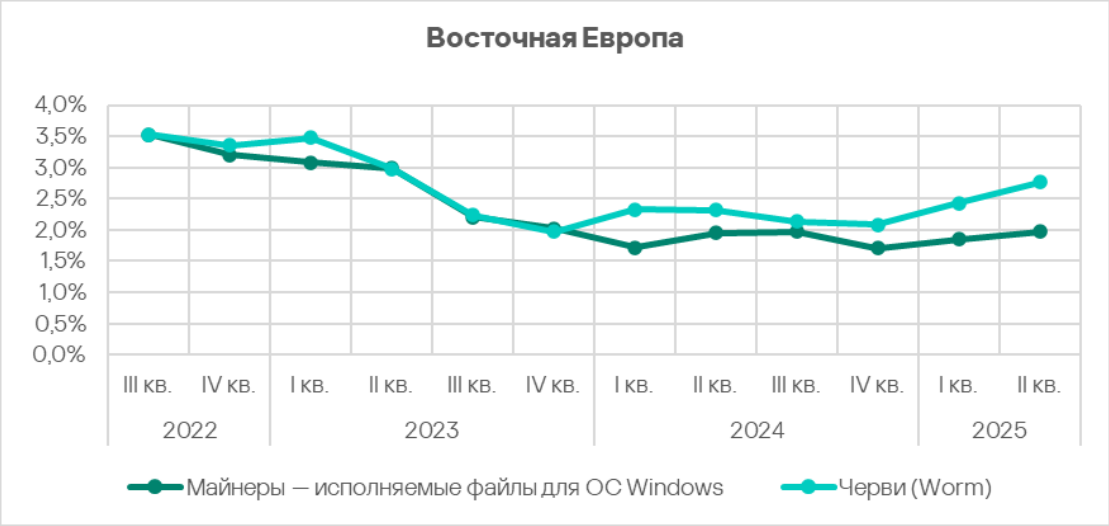
1,43%. Это в 6,5 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает этот рейтинг.



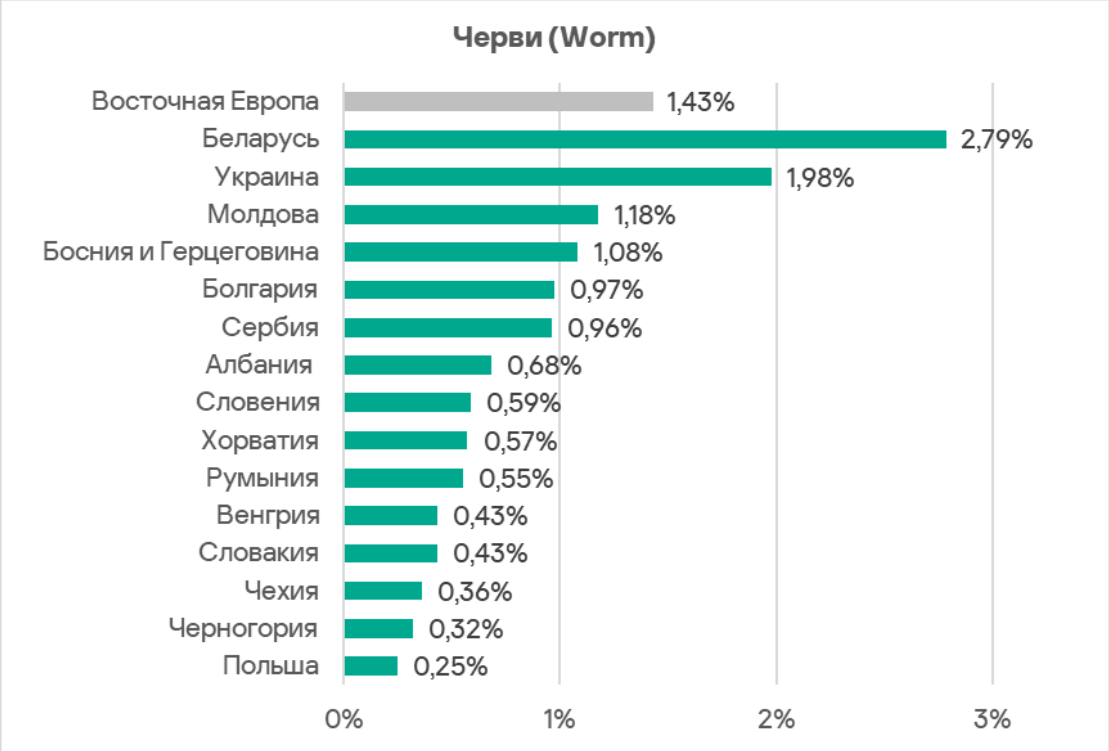
По показателю майнеров — исполняемых файлов для ОС Windows Восточная Европа находится на четвертом месте в соответствующем рейтинге с 0,65%. Этот показатель в 3,5 раза больше, чем в Восточной Азии, где значение минимальное среди регионов.

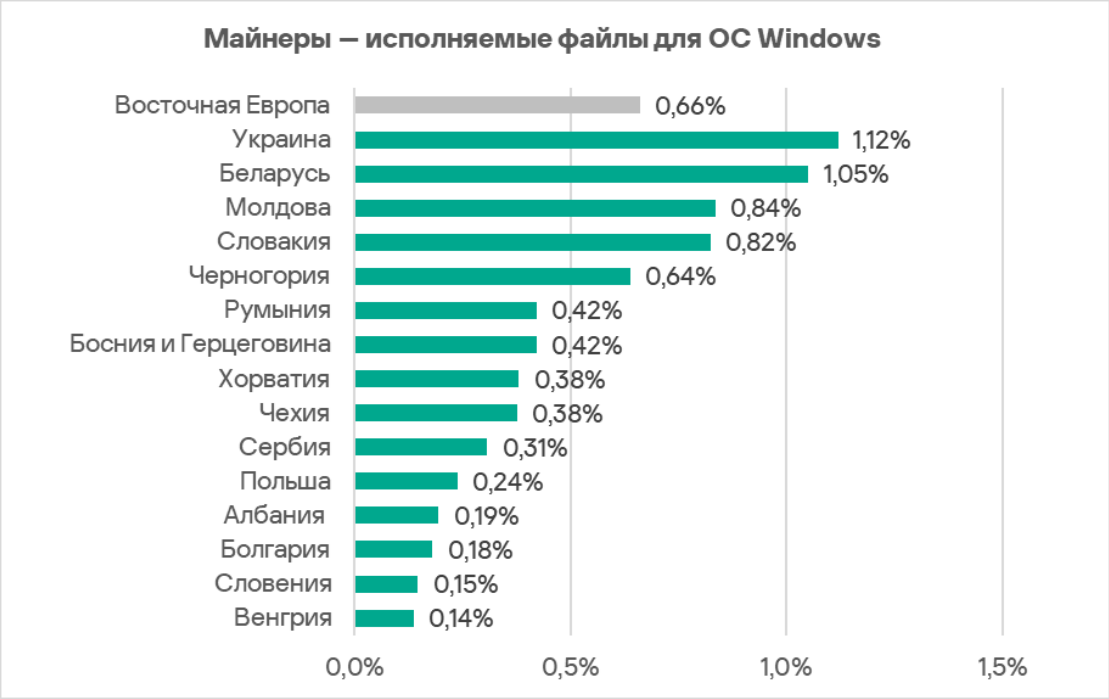


В Восточной Европе динамика показателей у этих двух категорий угроз очень схожая. Это объясняется тем, что в регионе майнеры для ОС Windows активно используют модули и компоненты, которые по сути являются червями и служат для доставки майнера на другие компьютеры в сети — автоматизированный lateral movement. Похожая ситуация и в России.



Среди стран региона в рейтинге по доле компьютеров АСУ, на которых блокируются черви, лидируют Беларусь, Украина и Молдова. Эти же страны входят в тройку лидеров по показателям майнеров — исполняемых файлов для ОС Windows.

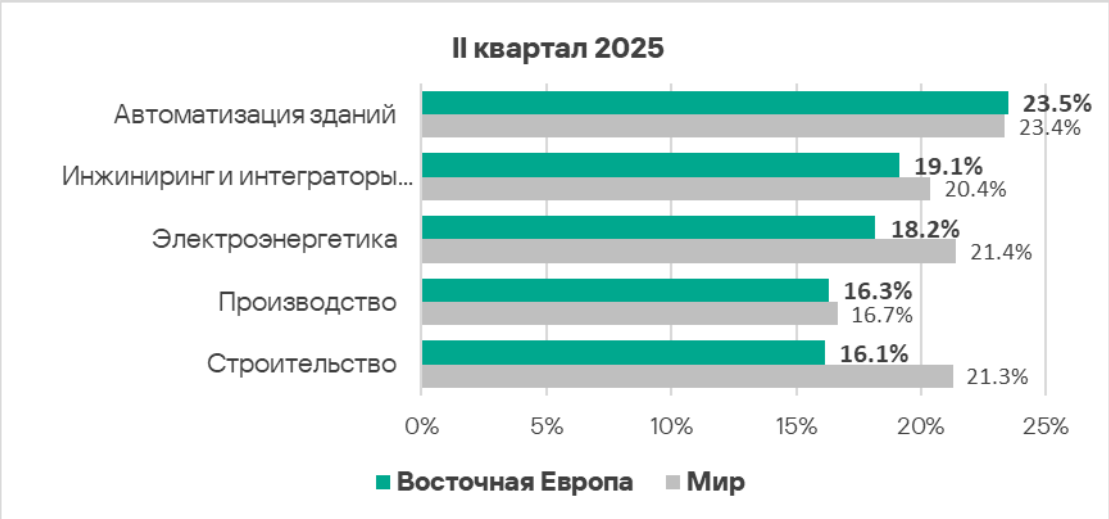




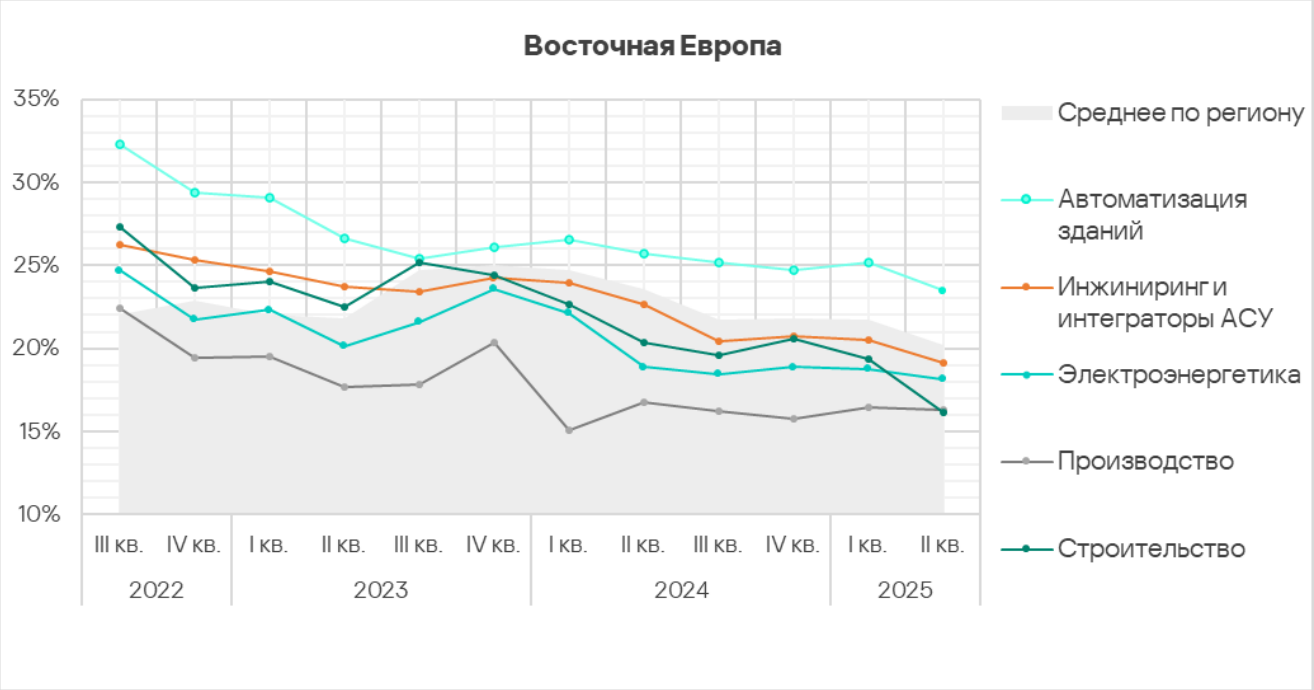
Украина и Беларусь также входят в топ 3 стран по доле компьютеров АСУ, на которых угрозы были заблокированы при присоединении съемных носителей.

Отрасли

Наиболее часто встречающейся с угрозами отраслью региона из рассмотренных в отчете является автоматизация зданий. Только у этой отрасли показатель немного превышает среднемировой. И это единственная отрасль, где показатель не уменьшился во втором квартале 2025 года.



Тренды в рассмотренных отраслях указывают на стабилизацию после значительного роста в 2022 году.



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 для индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В Восточной Европе значения, наиболее приближенные к максимальным, наблюдаются для совокупного показателя в сфере автоматизации зданий, а также в категории ресурсы в интернете из списка запрещенных в строительной отрасли.

Показатели источников угроз в отраслях в Восточной Европе, II квартал 2025 года

Отрасль / Источник угрозы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	9,85%	9,50%	10,28%	10,78%	9,70%	9,74%
Почтовые клиенты	8,39%	3,25%	3,32%	2,08%	2,07%	4,10%
Съемные носители	0,32%	0,30%	0,20%	0,25%	0,13%	0,23%
Сетевые папки	0,01%	0,05%	0,01%	0,00%	0,00%	0,01%
Показатель отрасли в регионе	23,47%	18,17%	19,11%	16,13%	16,30%	

Показатели категорий угроз в отраслях в Восточной Европе, II квартал 2025 года

Отрасль / Категории вредоносного ПО	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	5.65%	6.45%	6.69%	7.75%	6.86%	6.07%
Вредоносные скрипты и фишинговые страницы	10.01%	6.30%	6.45%	6.49%	5.30%	6.83%
Троянцы-шпионы, бэкдоры и кейлоггеры	7.60%	3.69%	3.89%	2.52%	3.49%	4.40%
Черви (Worm)	1.44%	1.67%	1.10%	0.57%	1.68%	1.43%
Майнеры — исполняемые файлы для ОС Windows	0.66%	0.44%	0.72%	0.88%	0.65%	0.66%
Вредоносные документы (MSOffice+PDF)	5.59%	2.12%	2.06%	1.20%	1.55%	2.76%
Вирусы (Virus)	0.52%	0.59%	0.38%	0.63%	0.78%	0.78%
Программы-вымогатели	0.18%	0.10%	0.06%	0.06%	0.00%	0.00%
Веб-майнеры, выполняемые в браузерах	0.37%	0.34%	0.43%	0.44%	0.65%	0.32%
Вредоносные программы для AutoCAD	0.01%	0.00%	0.08%	0.25%	0.00%	0.06%
Показатель отрасли в регионе	23.47%	18.17%	19.11%	16.13%	16.30%	

Отрасль / Категории вредоносного ПО	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	5,65%	6,45%	6,69%	7,75%	6,86%	6,07%
Вредоносные скрипты и фишинговые страницы	10,01%	6,30%	6,45%	6,49%	5,30%	6,83%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,60%	3,69%	3,89%	2,52%	3,49%	4,40%
Черви (Worm)	1,44%	1,67%	1,10%	0,57%	1,68%	1,43%
Майнеры — исполняемые файлы для ОС Windows	0,66%	0,44%	0,72%	0,88%	0,65%	0,66%
Вредоносные документы (MSOffice+PDF)	5,59%	2,12%	2,06%	1,20%	1,55%	2,76%
Вирусы (Virus)	0,52%	0,59%	0,38%	0,63%	0,78%	0,78%
Программы-вымогатели	0,18%	0,10%	0,06%	0,06%	0,00%	0,00%
Веб-майнеры, выполняемые в браузерах	0,37%	0,34%	0,43%	0,44%	0,65%	0,32%
Вредоносные программы для AutoCAD	0,01%	0,00%	0,08%	0,25%	0,00%	0,06%
Показатель отрасли в регионе	23,47%	18,17%	19,11%	16,13%	16,30%	

«Горячие точки» отраслей

Автоматизация зданий

- Первое место среди отраслей в регионе по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах и на съемных носителях.
- Первое место в регионе среди отраслей по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, программы-вымогатели.

Инжиниринг и интеграторы АСУ

- Второе место в регионе среди отраслей по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и угрозы в почтовых клиентах.
- Второе место среди отраслей региона по показателю следующих категорий угроз: шпионские программы, майнеры — исполняемые файлы для ОС Windows, вредоносные программы для AutoCAD.

Электроэнергетика

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках. Второе место по показателю угроз на съемных носителях.
- Второе место в регионе среди отраслей по показателям следующих категорий: вредоносные документы, черви и программы-вымогатели.

Производство

- Лидер региона среди отраслей по показателям червей, вирусов и веб-майнеров.
- Второе место в регионе среди отраслей по доле компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных.

Строительство

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета.
- Первое место среди отраслей региона по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных и майнеры — исполняемые файлы для ОС Windows.
- Второе место среди отраслей в регионе по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, вирусы, веб-майнеры.

Южная Европа

Основные проблемы кибербезопасности в регионе

Высокий риск целевых атак

Во втором квартале 2025 года промышленные организации в странах Южной Европы столкнулись с очередной волной фишинговых рассылок, в наибольшей степени затронувших биометрические системы и системы автоматизации зданий. Атаки на компьютеры в этих областях промышленной автоматизации значительно повышают риск атаки на другие сектора, то есть реализации атаки через поставщика.

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

Южная Европа лидирует в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, с показателем, превышающим среднемировое значение в 2,4 раза.

Южная Европа также занимает первое место среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, с показателем, превышающим среднемировой в 2,2 раза.

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

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.

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Южная Европа занимает второе место в соответствующем рейтинге регионов с показателем, который в 1,4 раза выше среднемирового.

Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или браузер пользователя различных вредоносных

программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

Высокий показатель шпионских программ

По доле компьютеров АСУ, на которых блокируются шпионские программы, Южная Европа занимает второе место в соответствующем рейтинге регионов с показателем, который в 1,5 раза выше среднемирового.

Шпионские программы используются злоумышленниками для кражи конфиденциальных данных. А в целевых атаках — 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.

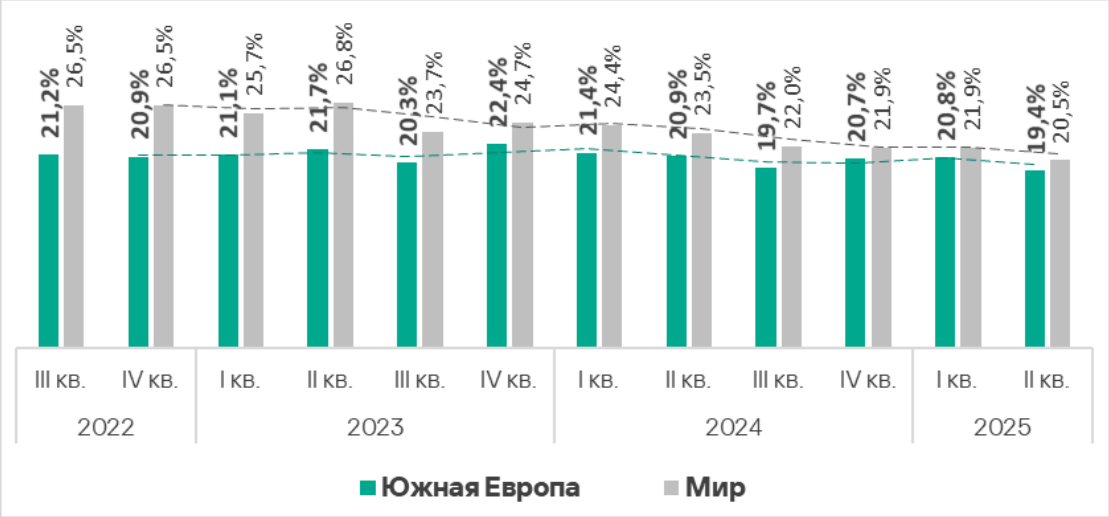
Высокий показатель программ-вымогателей

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в регионе в 1,4 раза больше среднемирового значения.

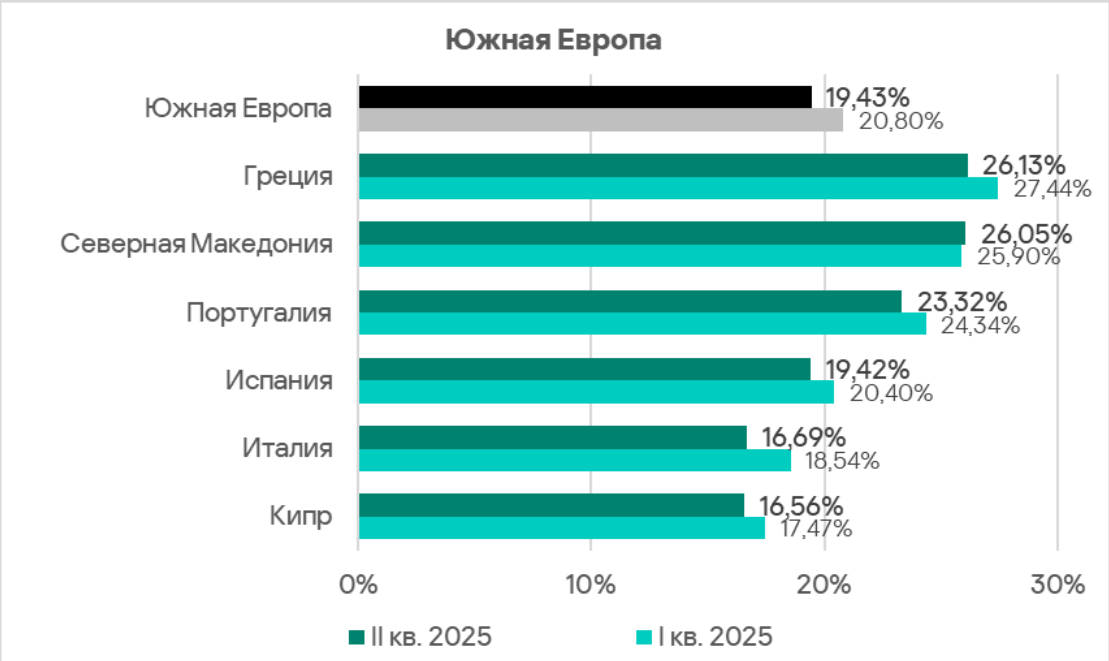
Статистика по всем угрозам

Во втором квартале 2025 года Южная Европа заняла восьмое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Во втором квартале 2025 года показатель в регионе уменьшился до наименьшего значения за период с третьего квартала 2022 года — 19,4%. Это ниже среднемирового значения, но в 1,7 раза больше, чем в Северной Европе, где показатель наименьший из всех регионов.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, лидируют Греция с 26,13% и Северная Македония с 26,05%. Эти же две страны лидируют в большинстве рейтингов стран региона и по источникам, и по категориям угроз.



Источники угроз

Южная Европа находится на первом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах. Значение показателя в регионе — 7,23% — превышает среднемировое в 2,4 раза.

Показатели всех источников угроз, кроме почтовых клиентов, в Южной Европе ниже среднемировых.

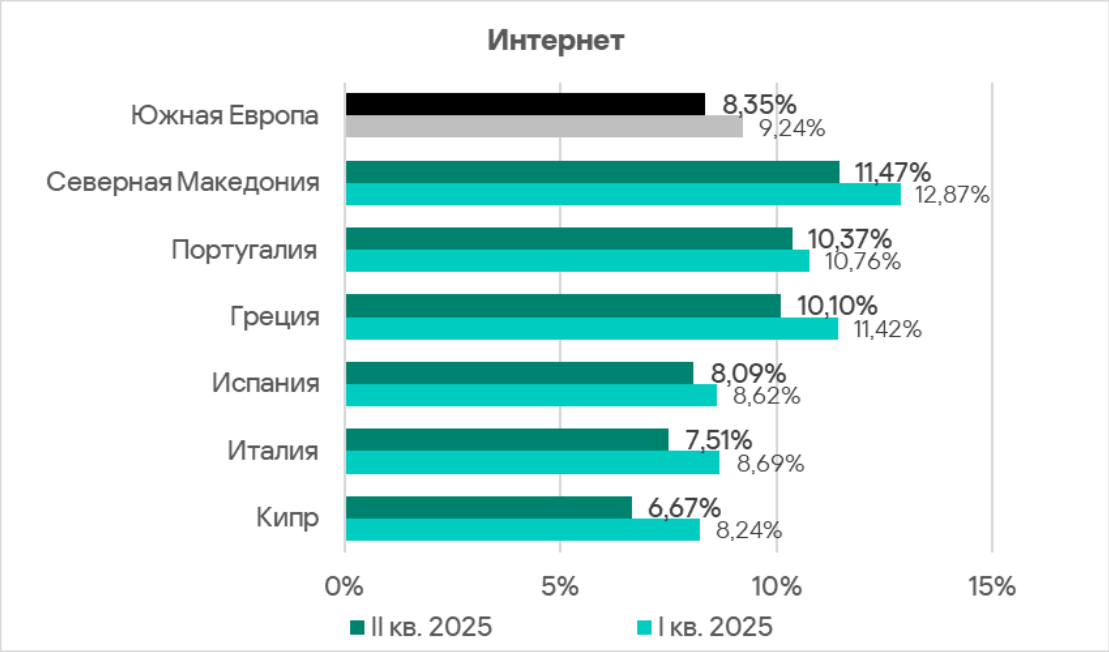
Основные каналы распространения вредоносного ПО в регионе — интернет и электронная почта.

Во втором квартале 2025 года из всех источников угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась только у почтовых клиентов.

Интернет

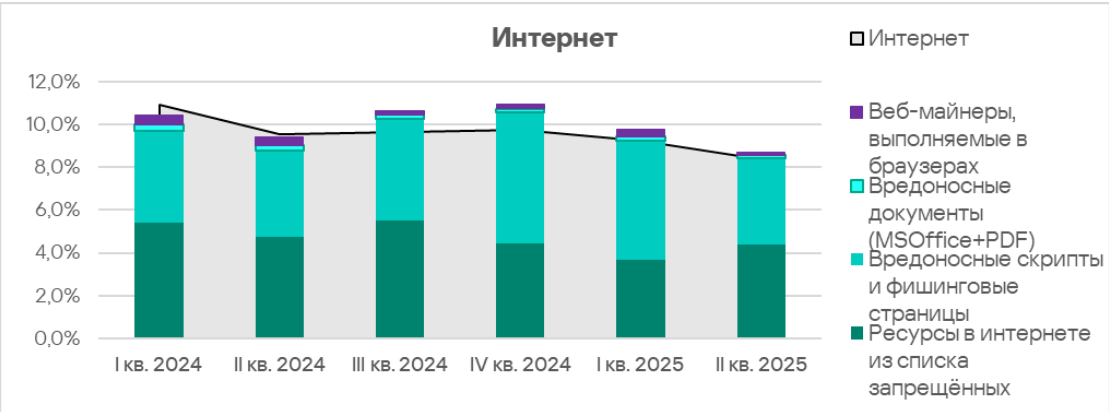
По доле компьютеров АСУ, на которых блокируются угрозы из интернета, Южная Европа занимает девятое место в рейтинге регионов с показателем 8,35%, который превышает минимальный — у Восточной Азии — в 1,3 раза.

Показатели стран региона варьируют от 6,67% на Кипре до 11,47% в Северной Македонии.



Португалия, которая занимает второе место в этом рейтинге, находится также на второй позиции в рейтингах по майнерам обеих категорий и лидирует по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных.

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



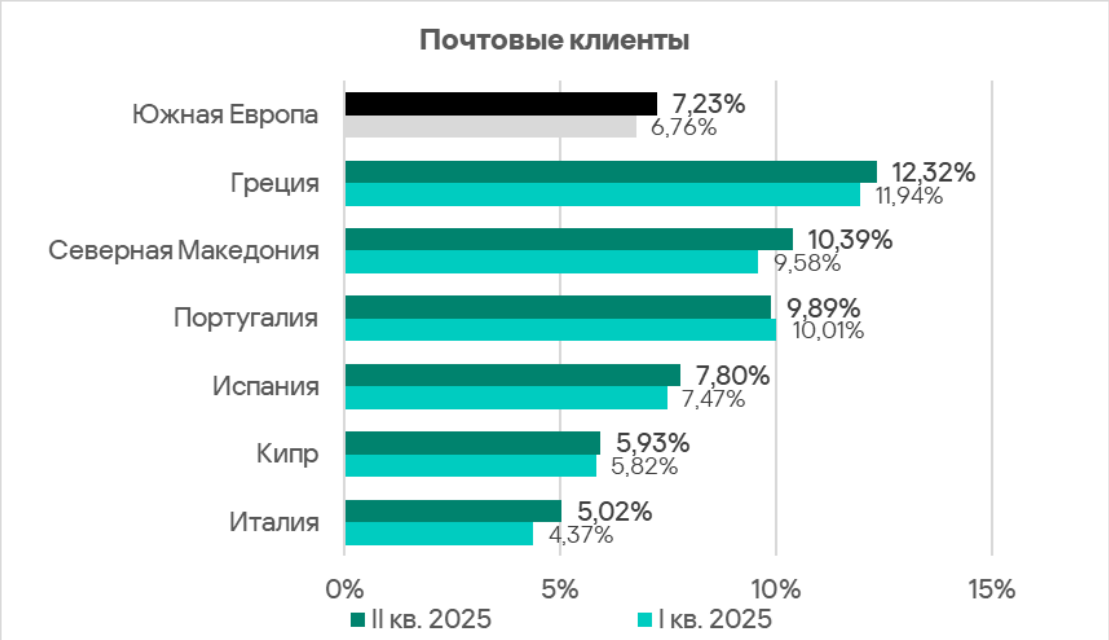
По показателю категории вредоносные скрипты и фишинговые страницы Южная Европа занимает второе место в соответствующем рейтинге регионов.

Почтовые клиенты

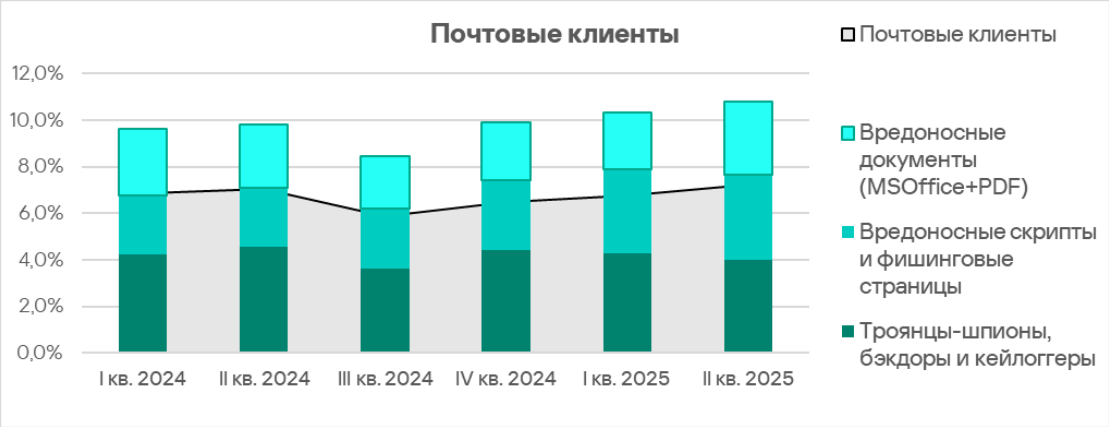
По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Южная Европа лидирует среди регионов с 7,23%. Этот показатель в 9 раз больше, чем в России, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, в Южной Европе растет третий квартал подряд.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, лидирует Греция с 12,32%. Наименьший показатель — в Италии (5,02%).



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

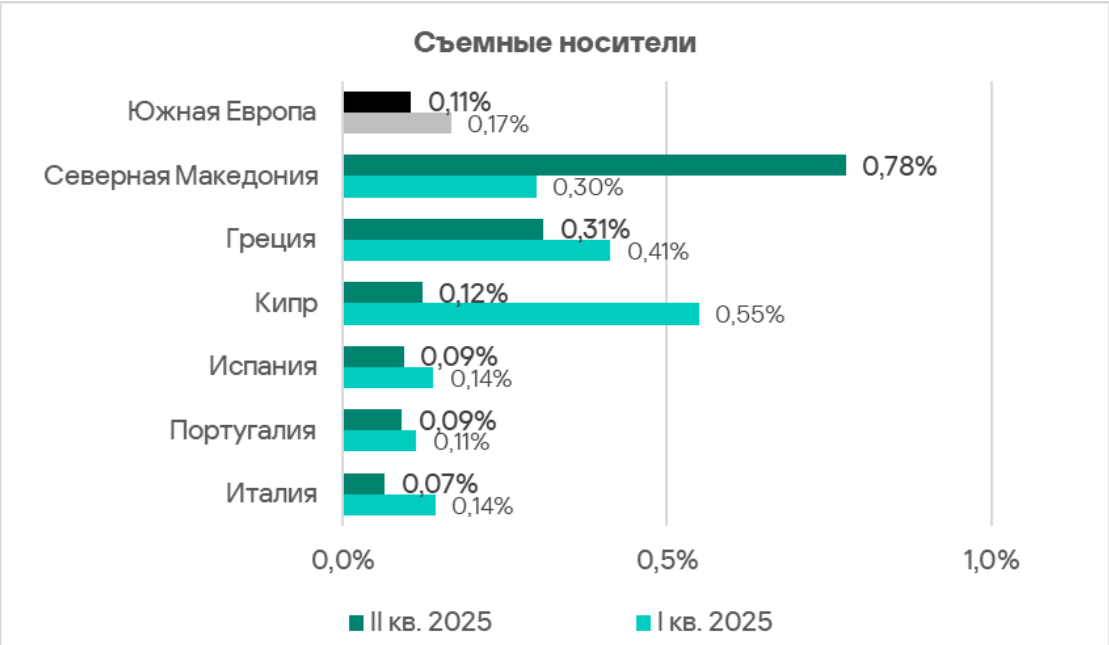


По доле компьютеров АСУ, на которых блокируются вредоносные документы, Южная Европа лидирует в соответствующем рейтинге регионов.

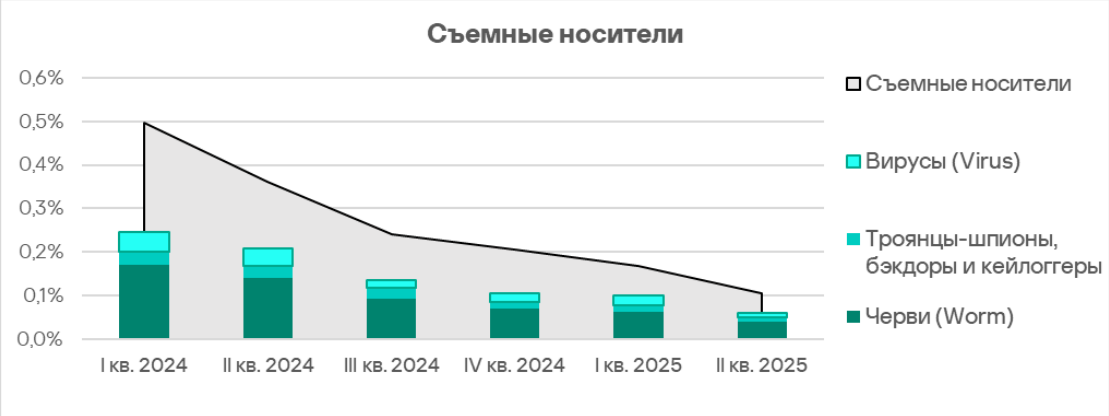
Съемные носители

По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, во втором квартале 2025 года Южная Европа занимает 10-е место в соответствующем рейтинге регионов. В Северной Америке (Канада), которая занимает последнее место, показатель меньше в 3,9 раза.

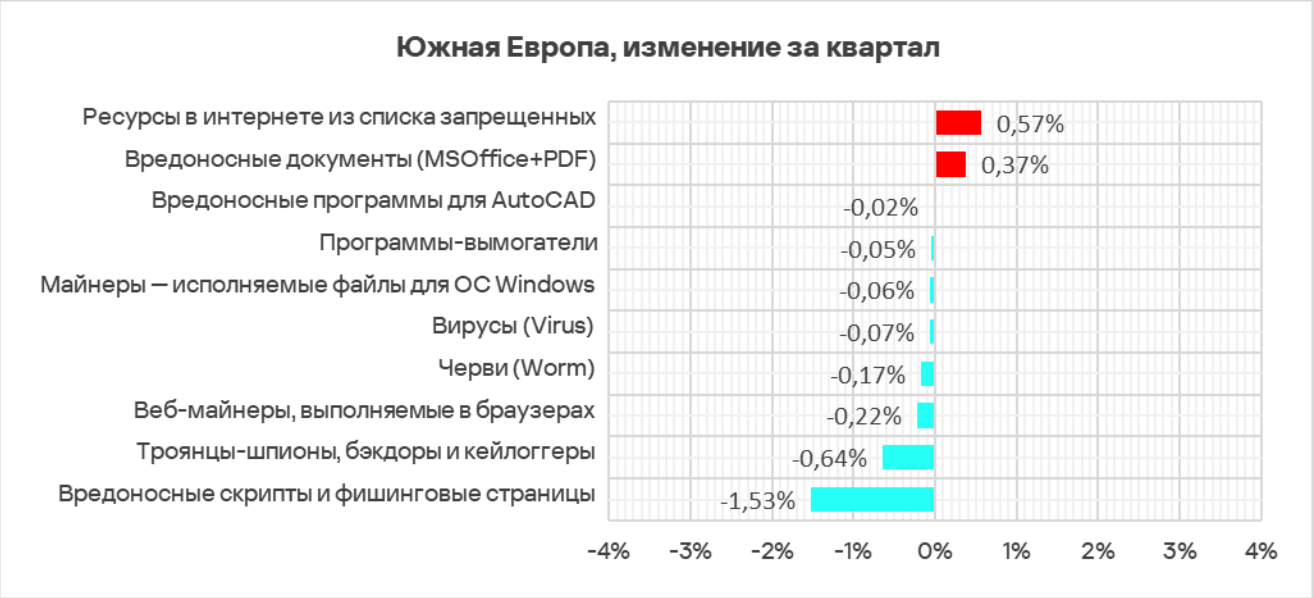
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с отрывом лидирует Северная Македония с 0,78%.



Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, шпионское ПО и вирусы.



Категории угроз



По сравнению со среднемировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- вредоносные документы — в 2,2 раза;
- шпионские программы — в 1,5 раза;
- вредоносные скрипты и фишинговые страницы — в 1,4 раза;
- программы-вымогатели — в 1,4 раза.

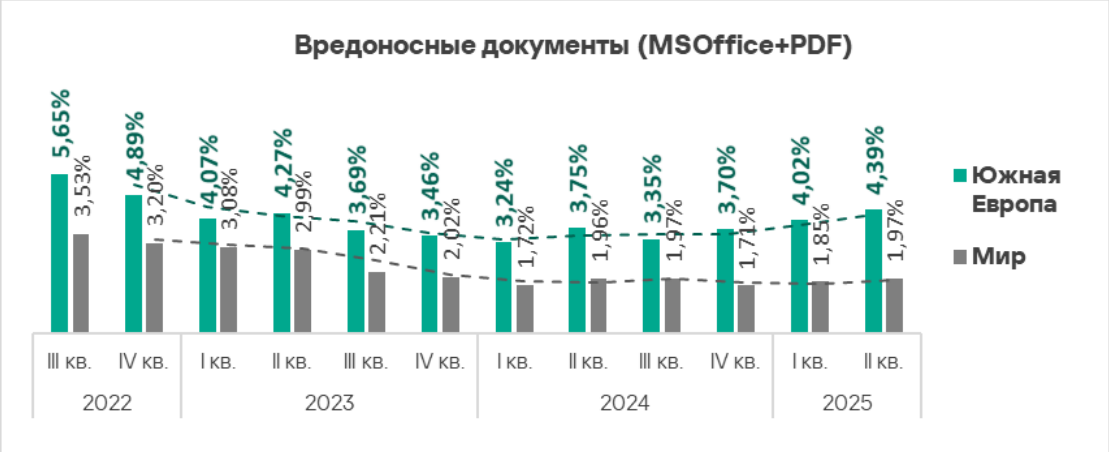
Вредоносные скрипты и фишинговые страницы, а также вредоносные документы используются злоумышленниками для распространения целевого вредоносного ПО, в том числе шпионских программ и программ-вымогателей.

В рейтингах по показателям этих четырех категорий лидируют Греция и Северная Македония. Они же возглавляют рейтинг по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах.

Вредоносные документы

Южная Европа лидирует в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы. Показатель в регионе — 4,39% — в 6,9 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе растет третий квартал подряд. Во втором квартале 2025 года по росту этого показателя Южная Европа находится на третьем месте среди регионов.

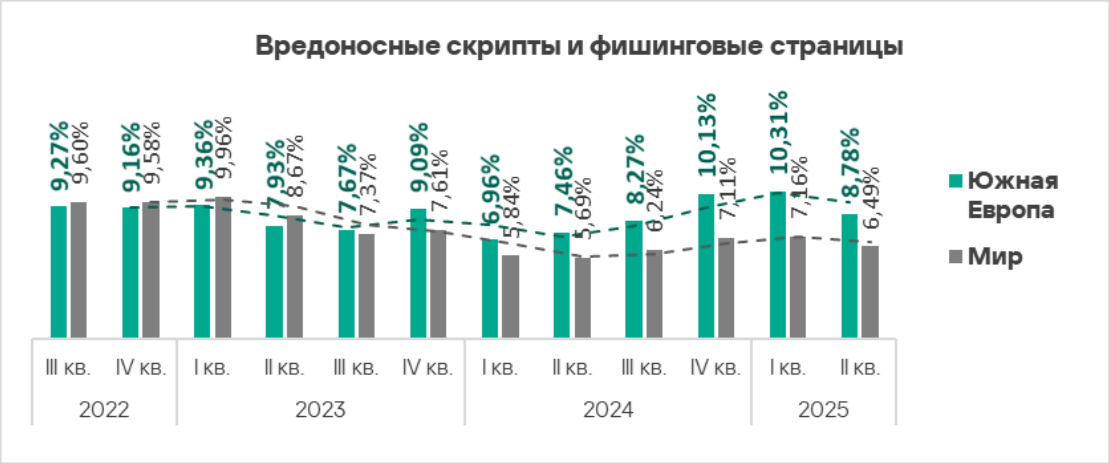


Среди стран региона по доле компьютеров АСУ, на которых блокируются вредоносные документы, лидирует Греция с 9,35%. За квартал показатель вырос во всех странах региона, кроме Португалии.

Распространяются вредоносные документы преимущественно по электронной почте.

Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Южная Европа занимает второе место в соответствующем рейтинге регионов с 8,78%. Это в 2,9 раза больше, чем в Северной Европе, где этот показатель наименьший.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Греция с 13,80%.

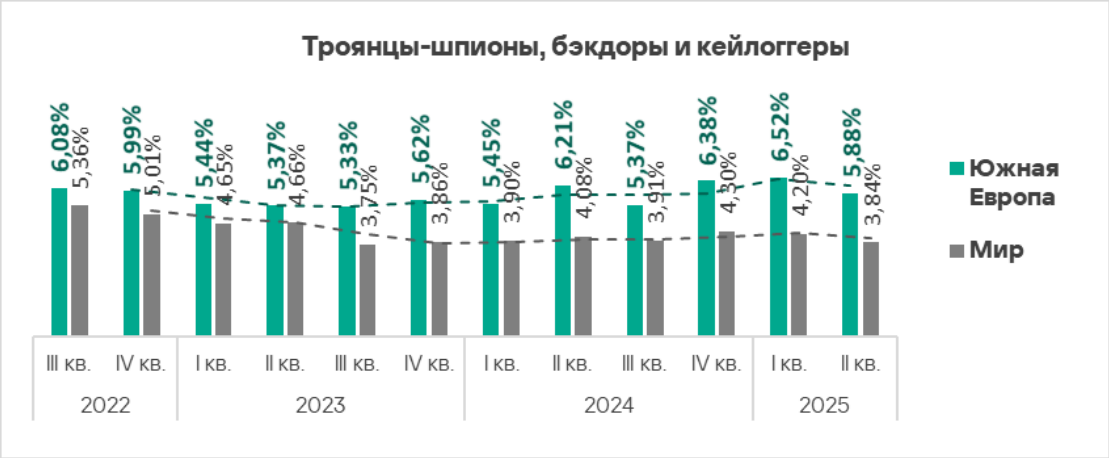
Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

Шпионские программы

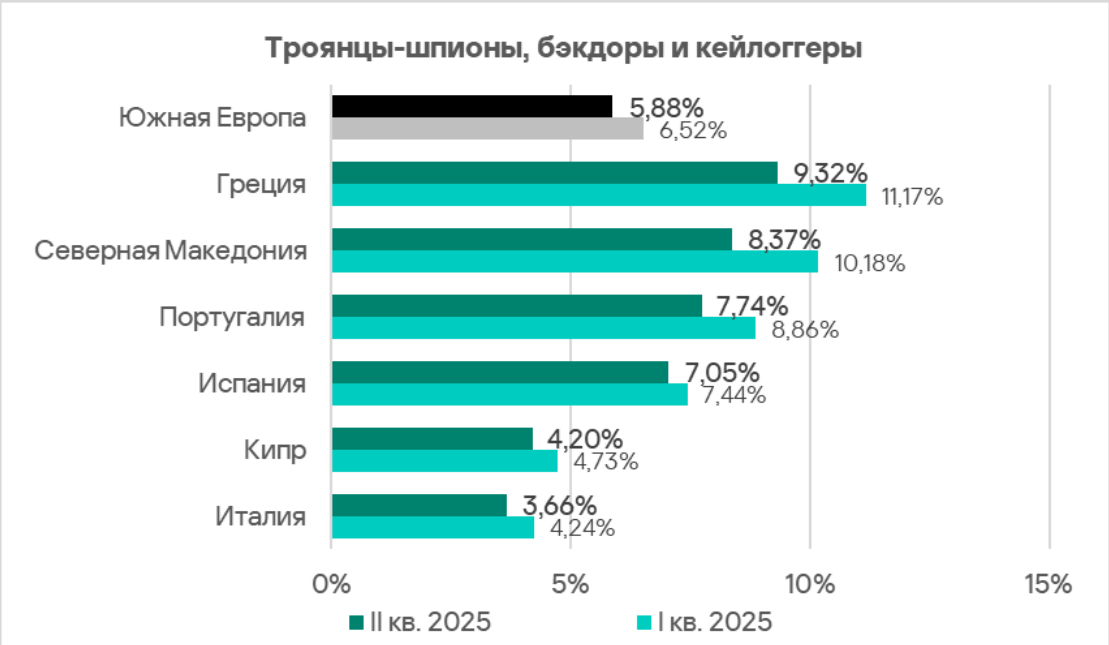
По доле компьютеров АСУ, на которых блокируются шпионские программы, Южная Европа находится на втором месте в соответствующем рейтинге регионов, уступая только Африке. Показатель в Южной Европе — 5,88% — в 4,3 раза больше, чем в Западной Европе, где он наименьший.

В региональном рейтинге категорий угроз шпионские программы также занимают второе место. Кроме Южной Европы, на второй позиции эта категория угроз находится еще в двух регионах — на Ближнем Востоке и в Южной Америке (в Восточной Азии она лидирует). Именно эти три региона — Южная Европа, Ближний Восток и Южная Америка — возглавляют рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почты.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в Южной Европе колеблется.



Среди стран региона по доле компьютеров АСУ, на которых заблокированы шпионские программы, лидирует Греция с 9,32%.

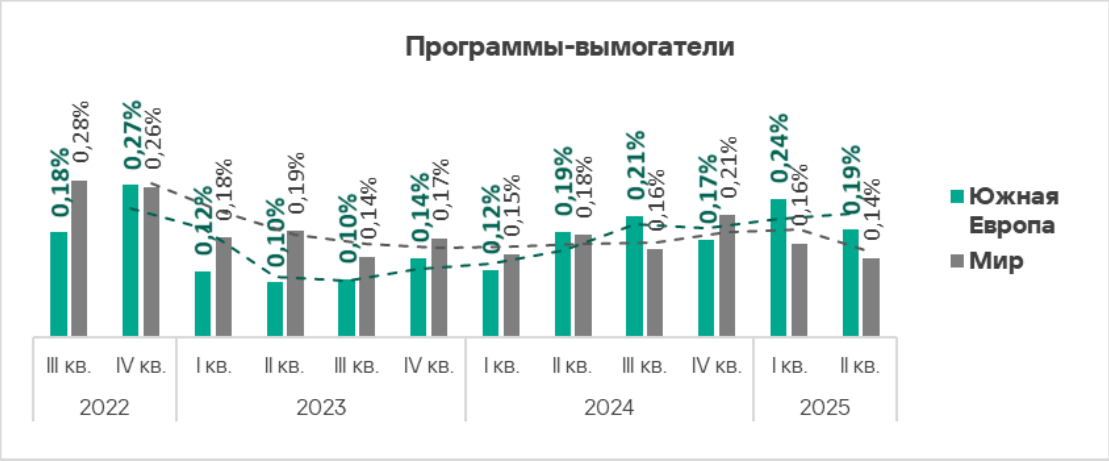


Шпионские программы в регионе блокируются преимущественно в почтовых клиентах.

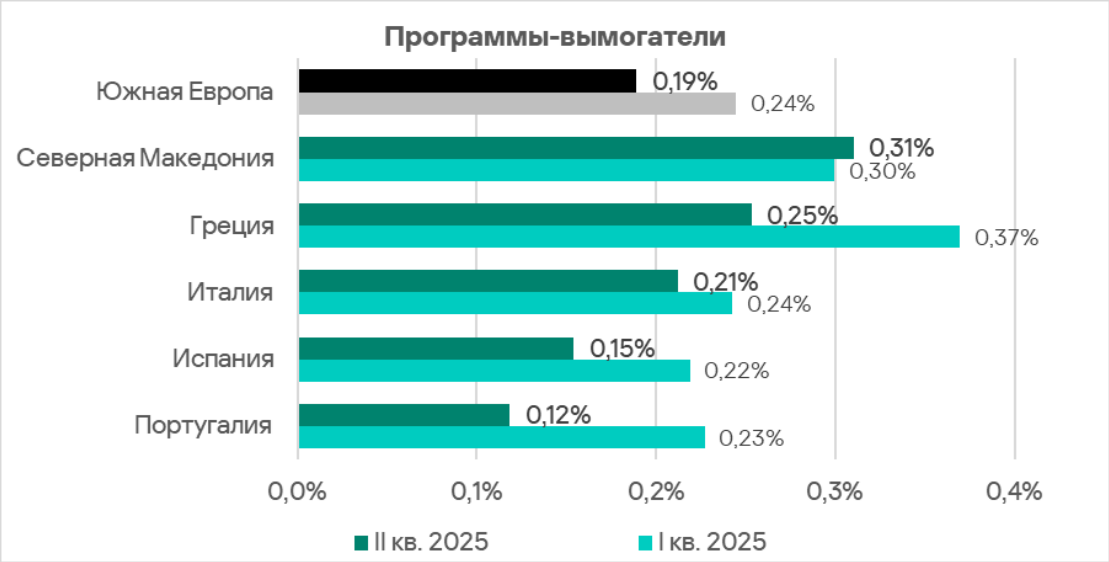
Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Южная Европа занимает пятое место в соответствующем рейтинге регионов с 0,19%. Это в 2,9 раза больше, чем в Западной Европе, которая замыкает этот рейтинг.

Показатель в регионе колеблется.



Среди стран региона в рейтинге по доле компьютеров АСУ, на которых блокируются программы-вымогатели, лидирует Северная Македония с 0,31%.



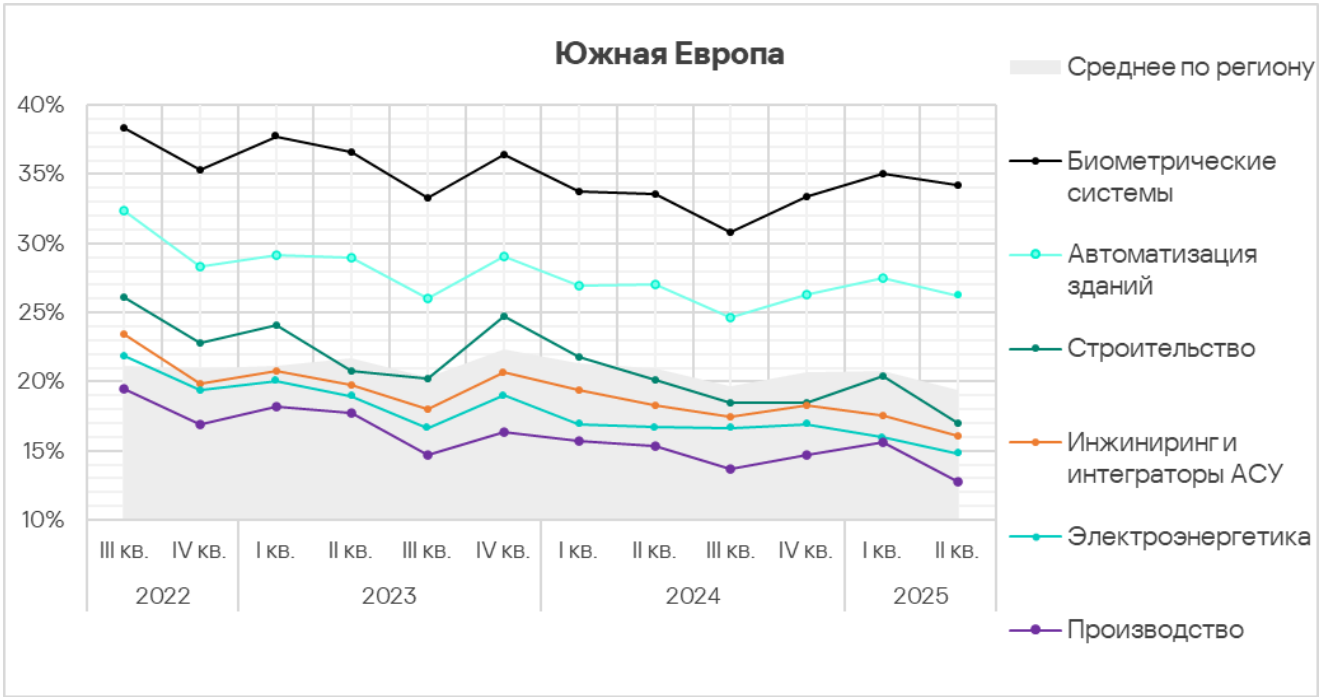
Отрасли

В Южной Европе из всех рассмотренных в отчете отраслей и OT-инфраструктур чаще всего вредоносные объекты блокируются в биометрических системах.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемировых показателей у OT-инфраструктуры биометрические системы и отрасли автоматизация зданий — в 1,2 и 1,1 раза соответственно. И только у этих отраслей показатель во втором квартале 2025 года вырос.

Во втором квартале 2025 года у всех исследуемых отраслей доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась.

Все рассмотренные отрасли демонстрируют колебательные тренды изменения доли компьютеров АСУ, на которых были заблокированы вредоносные объекты. Что касается биометрических систем и автоматизации зданий, то здесь значение показателя все еще значительно превышает среднее для региона.



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 для индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В Южной Европе значения, наиболее приближенные к максимальным, наблюдаются для компьютеров в составе биометрических систем. Так, максимальный показатель среди отраслей во всех регионах зафиксирован для почтовых клиентов и трех категорий угроз: троянцы-шпионы, вредоносные скрипты и фишинговые страницы, вредоносные документы. Более того, совокупный показатель для биометрических систем в регионе выше, чем в других регионах.

Показатели источников угроз в отраслях в Южной Европе, II квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	8,97%	8,81%	7,63%	8,11%	8,02%	5,08%	8,35%
Почтовые клиенты	20,38%	13,80%	3,19%	4,51%	5,20%	3,29%	7,23%
Съемные носители	0,06%	0,10%	0,16%	0,09%	0,06%	0,14%	0,11%
Сетевые папки	0,00%	0,03%	0,02%	0,02%	0,00%	0,00%	0,01%
Показатель отрасли в регионе	34,23%	26,25%	14,84%	16,04%	17,04%	12,76%	

Показатели категорий угроз в отраслях в Южной Европе, II квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	4,37%	4,25%	4,48%	4,41%	4,70%	2,89%	4,52%
Вредоносные скрипты и фишинговые страницы	16,91%	13,95%	5,31%	6,77%	6,53%	5,00%	8,78%
Троянцы-шпионы, бэкдоры и кейлоггеры	18,15%	10,61%	2,39%	3,60%	3,21%	2,93%	5,88%
Черви (Worm)	1,84%	1,14%	0,69%	0,54%	0,39%	0,68%	0,78%
Майнеры — исполняемые файлы для ОС Windows	0,41%	0,27%	0,27%	0,25%	0,22%	0,25%	0,25%
Вредоносные документы (MSOffice+PDF)	12,25%	9,00%	1,81%	2,45%	2,99%	1,82%	4,39%
Вирусы (Virus)	0,43%	0,43%	0,31%	0,21%	0,44%	0,14%	0,31%
Программы-вымогатели	0,60%	0,33%	0,05%	0,08%	0,00%	0,18%	0,19%
Веб-майнеры, выполняемые в браузерах	0,31%	0,20%	0,22%	0,20%	0,06%	0,07%	0,19%
Вредоносные программы для AutoCAD	0,04%	0,07%	0,02%	0,04%	0,39%	0,04%	0,06%
Показатель отрасли в регионе	34,23%	26,25%	14,84%	16,04%	17,04%	12,76%	

«Горячие точки» отраслей

Биометрические системы

- Первое место среди отраслей во всех регионах по показателю почтовых угроз и в следующих категориях угроз: шпионские программы, вредоносные документы, вредоносные скрипты и фишинговые страницы.
- Второе место среди отраслей всех регионов по показателю программ-вымогателей.
- Первое место среди отраслей в регионе по доле компьютеров АСУ, на которых угрозы были заблокированы в интернете и почтовых клиентах.
- Первое место среди отраслей в регионе по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви, майнеры обеих категорий и программы-вымогатели.

Автоматизация зданий

- Второе место среди отраслей во всех регионах по показателю угроз, доставляемых через почтовые клиенты, и угроз из категорий вредоносные документы и шпионские программы.
- Третье место среди отраслей во всех регионах по угрозам в категории вредоносные скрипты и фишинговые страницы.
- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках. Второе место среди отраслей по показателю угроз в интернете и в почтовых клиентах.
- Второе место среди отраслей региона по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви, вирусы, программы-вымогатели и вредоносные программы для AutoCAD.

Строительство

- Первое место в регионе среди отраслей по показателям категорий угроз ресурсы в интернете из списка запрещенных и майнеры — исполняемые файлы для ОС Windows.
- Лидер среди отраслей региона по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, вирусы и вредоносные программы для AutoCAD.

Инжиниринг и интеграторы АСУ

- Второе место в регионе среди отраслей по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.
- Третье место среди отраслей в регионе по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, ресурсы в интернете из списка запрещенных, веб-майнеры и вредоносные программы для AutoCAD.

Электроэнергетика

- Первое место в регионе среди отраслей по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.
- Второе место среди отраслей региона по показателям категорий ресурсы в интернете из списка запрещенных и майнеры обеих категорий. Третье место по показателю червей.

Производство

- Второе место в регионе среди отраслей по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.

- Третье место в регионе среди отраслей по доле компьютеров АСУ, на которых блокируются программы-вымогатели.

Западная Европа

Основные проблемы кибербезопасности в регионе

Один из наиболее благополучных с точки зрения кибербезопасности регионов.

Во втором квартале 2025 года Западная Европа заняла предпоследнее, 13-е, место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

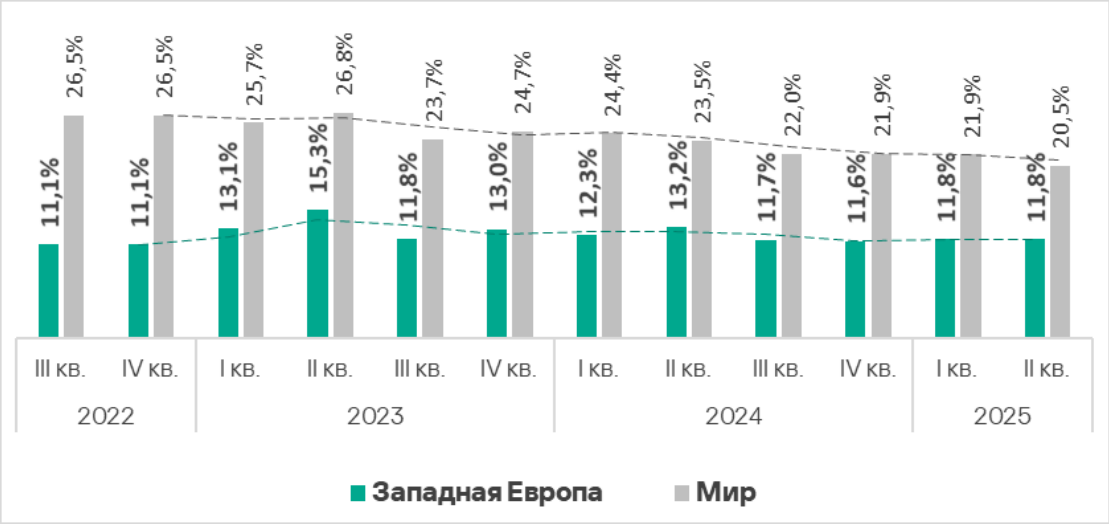
В рейтинге по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, Западная Европа занимает восьмое место. Атаки с использованием веб-майнеров часто совпадают с массовыми кампаниями по заражению уязвимых веб-сайтов, которые в случае компрометации используются в качестве C2-инфраструктуры.

На фоне возврата среднего по региону показателя в категории веб-майнеры к значениям 2024 года, после очередной волны распространения через зараженные сайты, доля компьютеров в нефтегазовой отрасли Западной Европы, на которых продолжают блокироваться попытки запуска веб-майнеров остается очень высокой.

В рейтингах по остальным показателям — и по источникам, и по категориям угроз — Западная Европа не поднимается выше девятого места.

Статистика по всем угрозам

Во втором квартале 2025 года Западная Европа заняла предпоследнее, 13-е, место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Показатель остался прежним — 11,8%. Это значительно ниже среднемирового значения.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, лидирует Франция с 12,09%. Наименьший показатель у Швейцарии — 9,20%.

Источники угроз

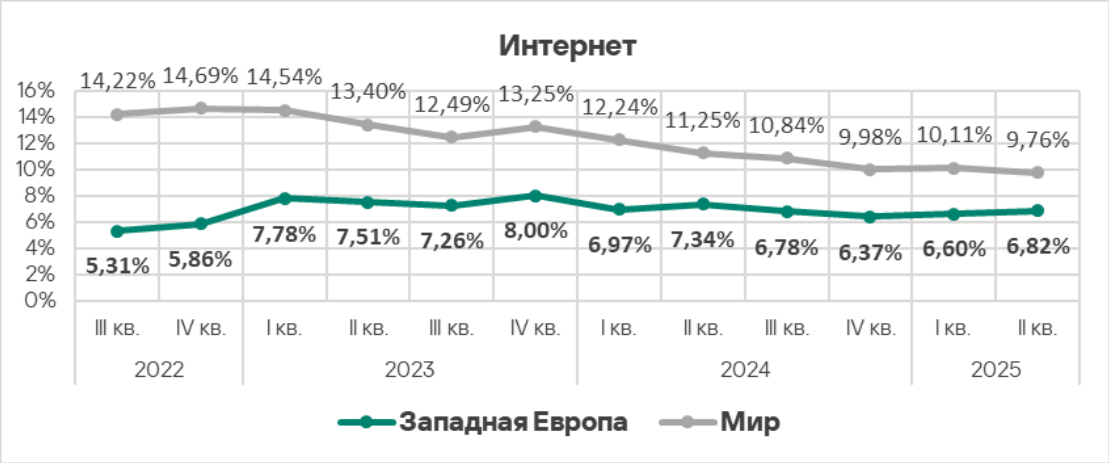
Показатели всех источников угроз в Западной Европе ниже среднемировых.

Вредоносные объекты в регионе распространяются преимущественно через интернет и почту. В рейтинге по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, Западная Европа занимает третье место с конца.

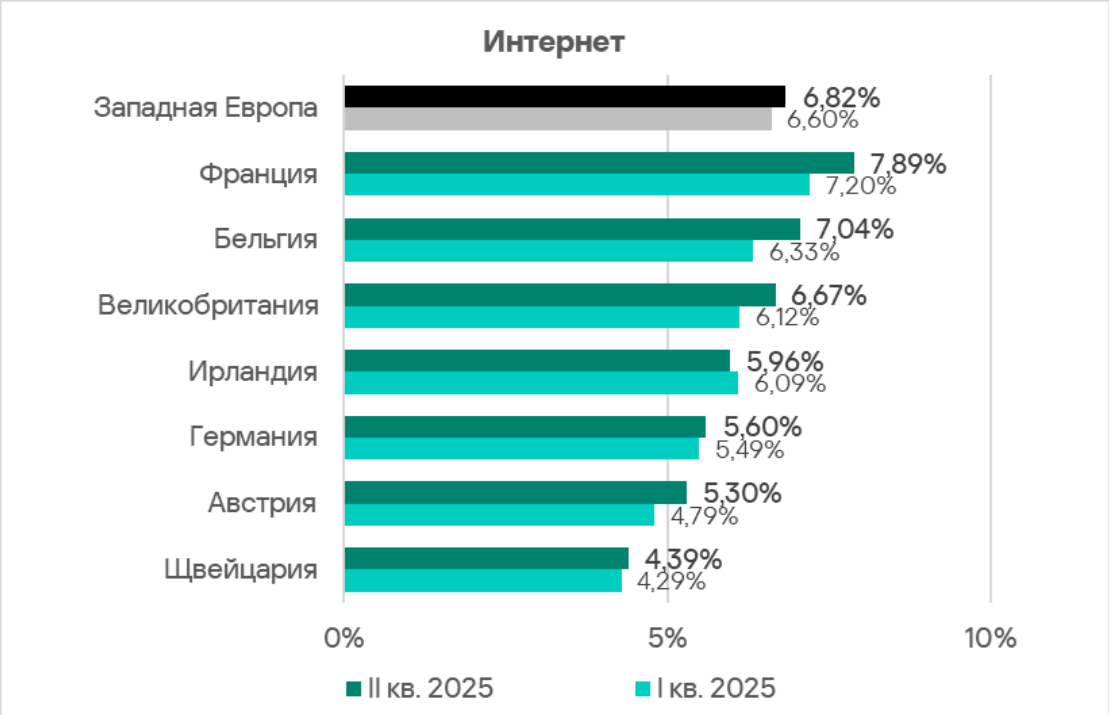
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного увеличилась у показателей угроз из интернета и из почтовых клиентов.

Интернет

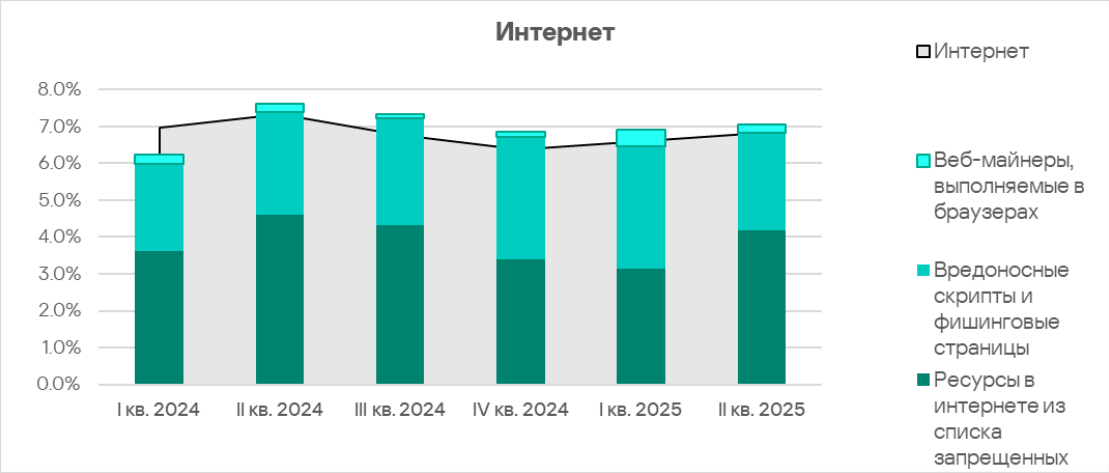
По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Западная Европа занимает 12-е место в рейтинге регионов с показателем 6,82%. Он превышает минимальный — у Восточной Азии — в 1,1 раза.



Показатели стран региона варьируют от 4,39% в Швейцарии до 7,89% во Франции. Доля компьютеров АСУ, на которых блокируются угрозы из интернета, выросла во всех странах региона, кроме Ирландии.



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

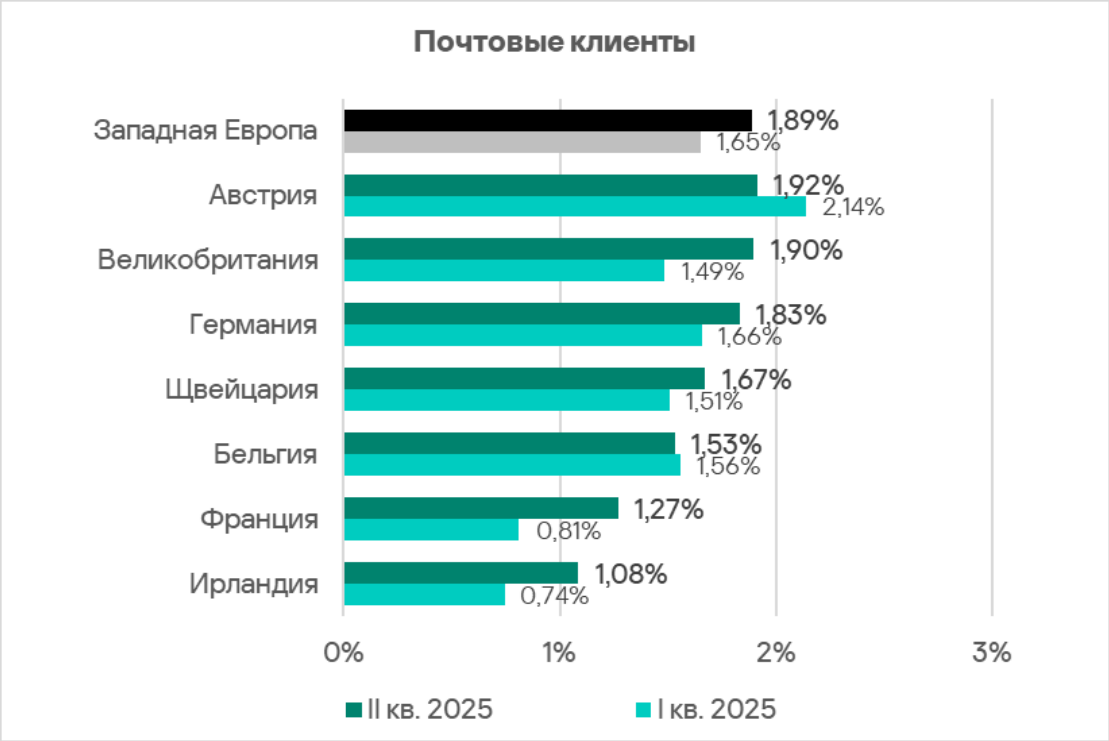


По показателю веб-майнеров Западная Европа занимает восьмое место в соответствующем рейтинге регионов.

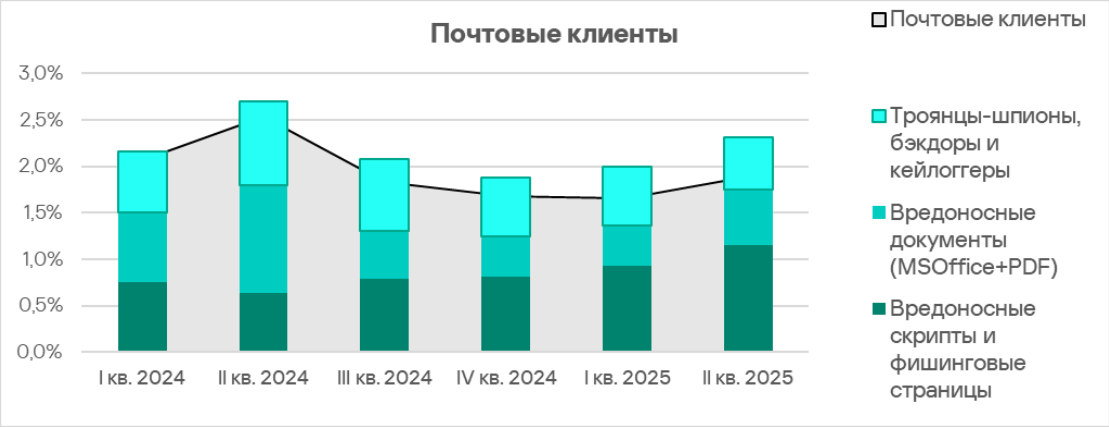
Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Западная Европа занимает 10-е место среди регионов с показателем 1,89%. Это в 2,4 раза больше, чем в России, которая замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, лидирует Австрия с 1,92%. Наименьший показатель — в Ирландии (1,08%). Показатель за квартал вырос во всех странах региона, кроме Австрии и Бельгии.



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



Шпионское ПО в регионе распространяется преимущественно через почту.

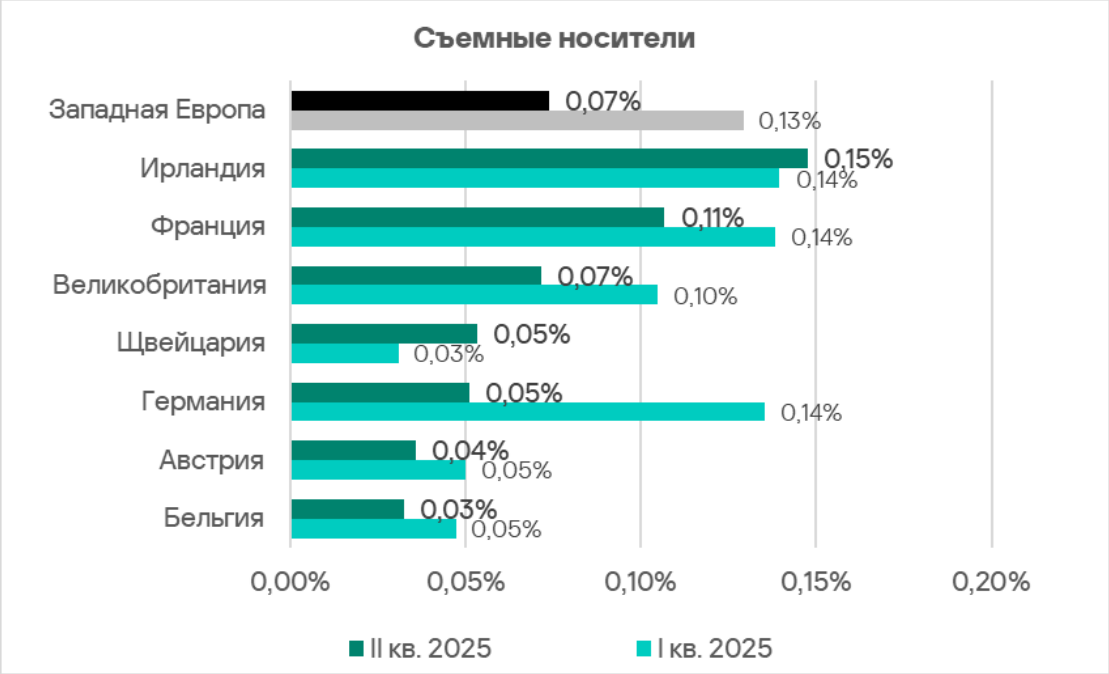
Страны-лидеры рейтинга по почтовым клиентам — Австрия, Великобритания и Германия — также входят занимают верхние строчки в рейтинге по показателям шпионских программ.

Съемные носители

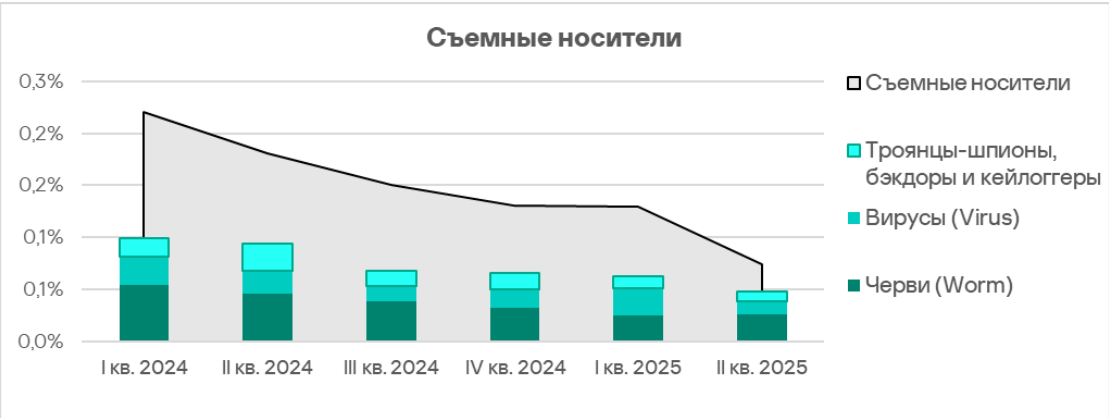
По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, во втором квартале 2025 года Западная

Европа занимает 12-е место среди регионов с 0,07%. В Северной Америке (Канада), которая замыкает рейтинг, показатель меньше в 2,8 раза.

Доля компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, в регионе варьирует от 0,03% в Бельгии до 0,15% в Ирландии. Ирландия и Швейцария — две страны региона, где этот показатель во втором квартале 2025 года вырос.



Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионские программы.

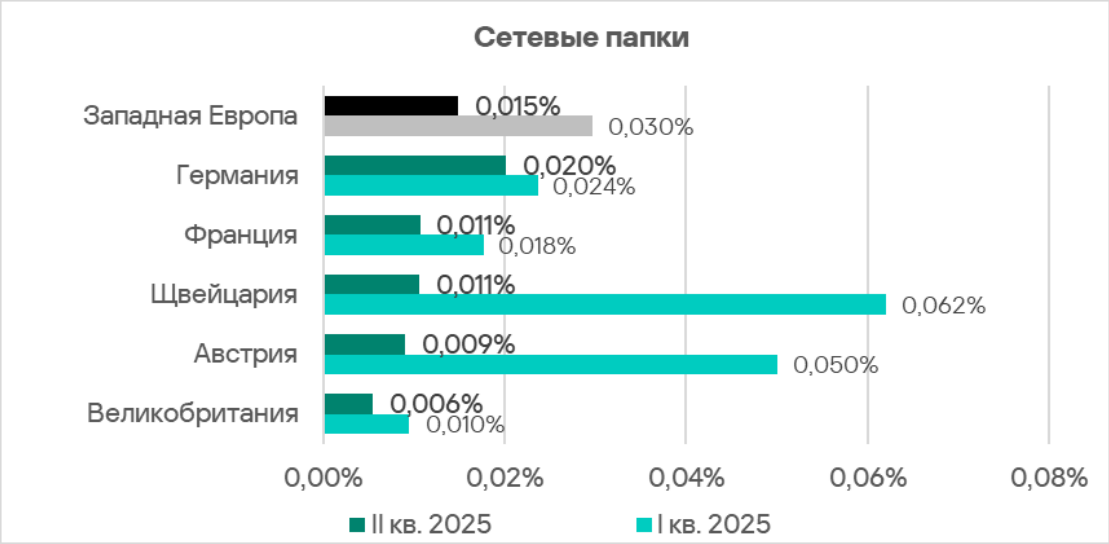


Сетевые папки

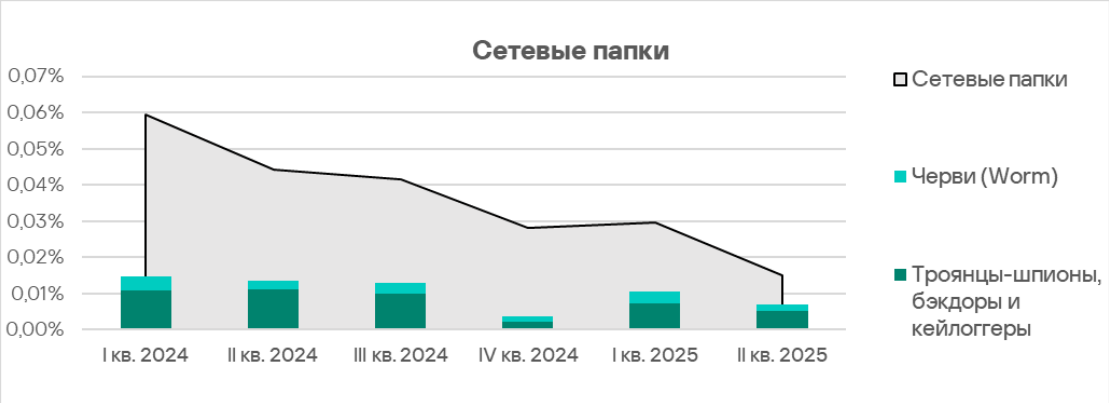
По доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, во втором квартале 2025 года Западная Европа занимает 10-е место

среди регионов с 0,015%. В Северной Европе, которая замыкает соответствующий рейтинг, показатель меньше в 1,5 раза.

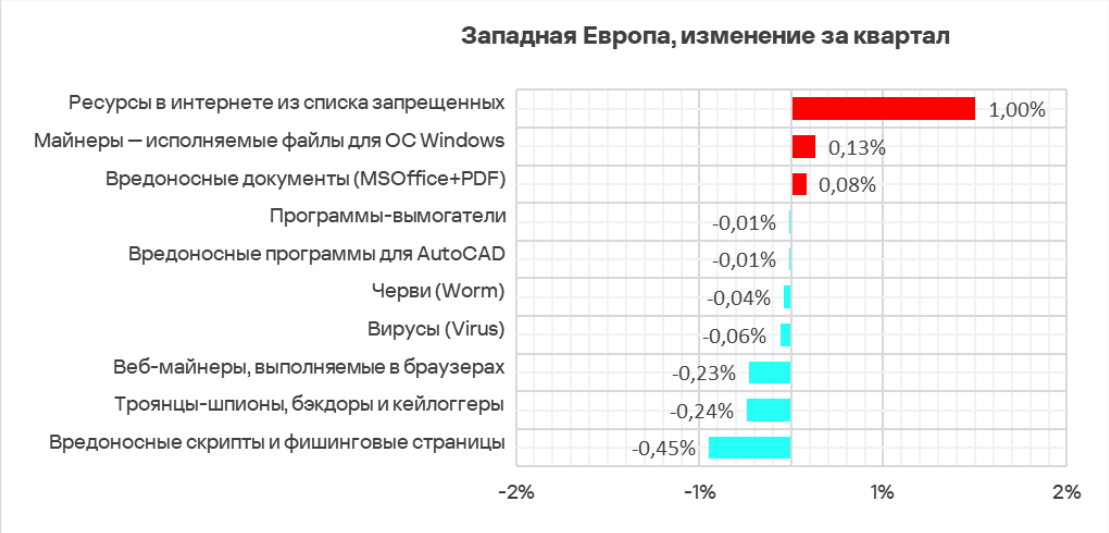
Среди стран региона по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках, лидирует Германия с 0,02%.



Основные категории угроз, которые блокируются в регионе в сетевых папках: шпионские программы и черви.



Категории угроз



Для всех категорий угроз показатели в регионе меньше, чем среднемировые.

Самая высокая позиция в рейтингах регионов по доле компьютеров АСУ, на которых блокировались угрозы определенной категории, касается веб-майнеров — Западная Европа занимает по этому показателю восьмое место.

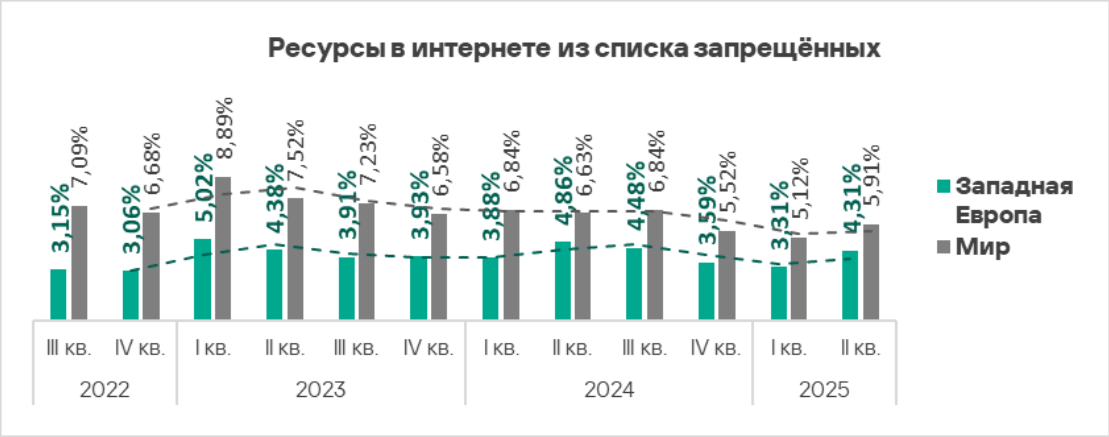
Рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

- ресурсы в интернете из списка запрещенных — в 1,3 раза, третье место среди регионов по росту этого показателя;
- майнеры — исполняемые файлы для ОС Windows — в 1,7 раза, первое место среди регионов по росту этого показателя;
- вредоносные документы — в 1,1 раза.

Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Западная Европа занимает девятое место в соответствующем рейтинге регионов с 4,31%. Это в 1,3 раза больше, чем в Восточной Азии, где этот показатель наименьший.

В втором квартале 2025 года Западня Европа находится на третьем месте среди регионов по росту доли компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных.

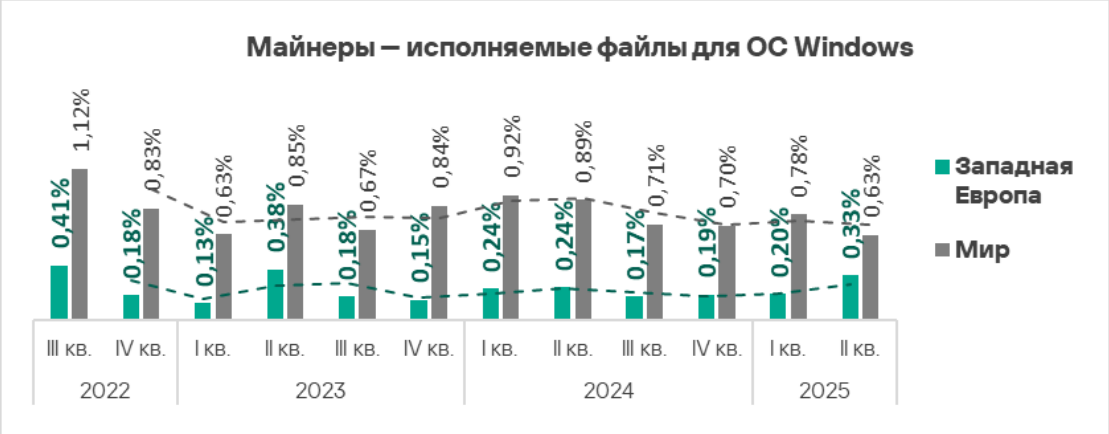


Среди стран региона по этому показателю лидирует Франция с 4,85%. Доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, выросла во всех странах региона, кроме Ирландии.

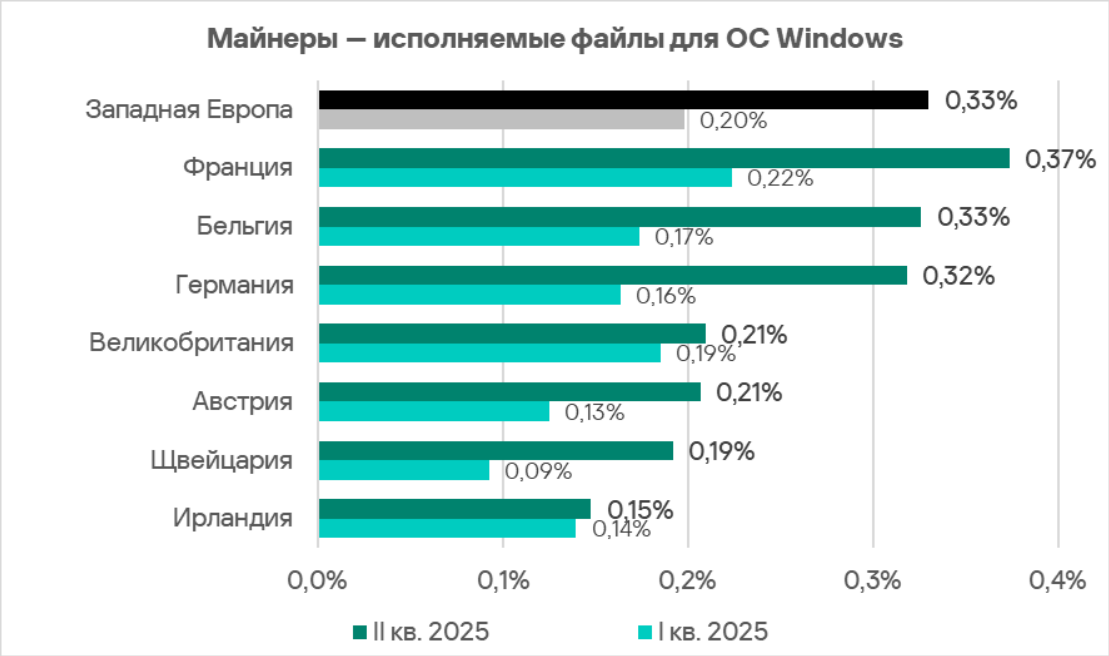
Майнеры — исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, Западная Европа занимает 10-е место в соответствующем рейтинге с 0,33%. Этот показатель в 1,8 раза больше, чем в Восточной Азии, где значение минимальное среди регионов.

Показатель в регионе растет третий квартал подряд. По его росту во втором квартале 2025 года Западная Европа заняла первое место среди регионов.



Среди стран региона в рейтинге по доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, лидирует Франция с 0,37%.



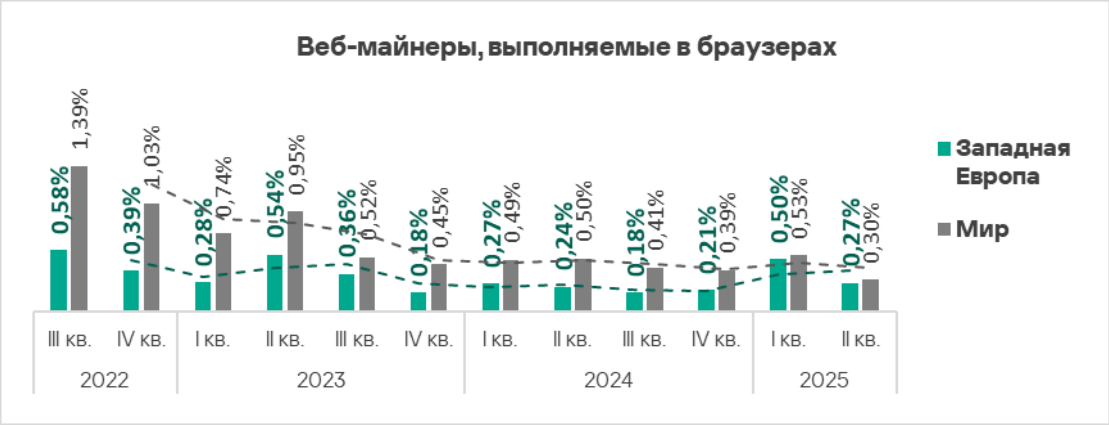
Майнеры — исполняемые файлы для ОС Windows в регионе распространяются преимущественно в интернете.

Отметим, что страны на верхних строчках этого рейтинга — Франция, Бельгия и Германия — лидируют и по показателям веб-майнеров.

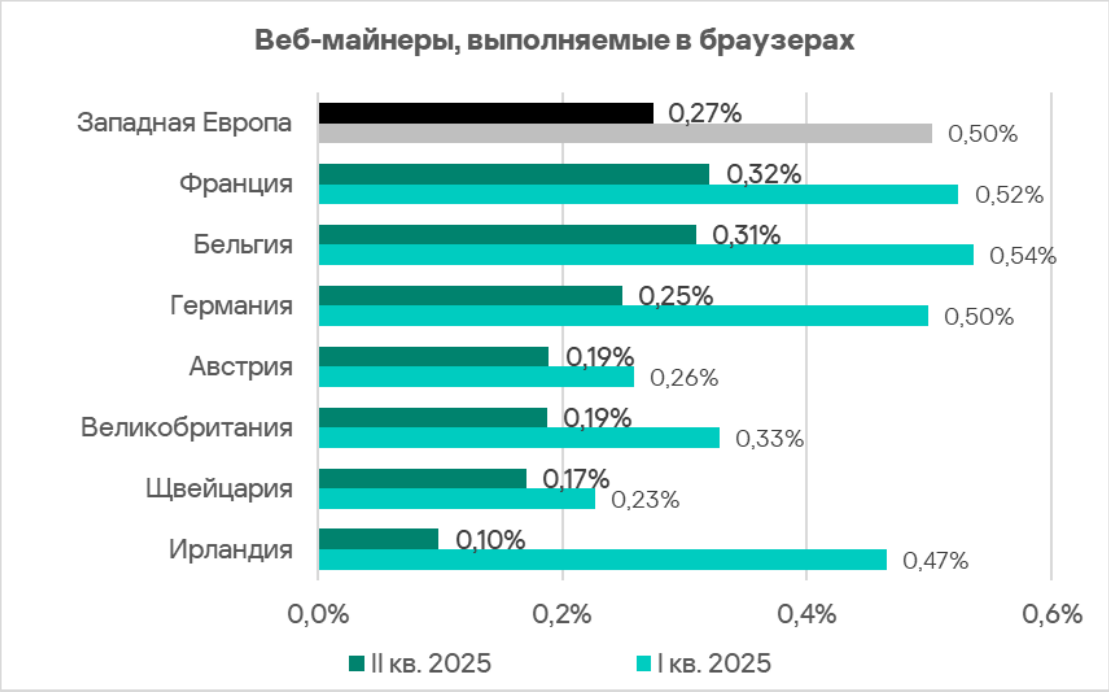
Веб-майнеры

В рейтингах по доле компьютеров АСУ, на которых блокируются различные категории угроз, самую высокую позицию Западная Европа занимает по показателю веб-майнеров — регион находится на восьмом месте с 0,27%. Это в 2,6 раза больше, чем в Восточной Азии, где минимальное значение среди регионов, и немного меньше среднемирового значения.

После роста в прошлом квартале показатель уменьшился во всех регионах, в том числе в Западной Европе.



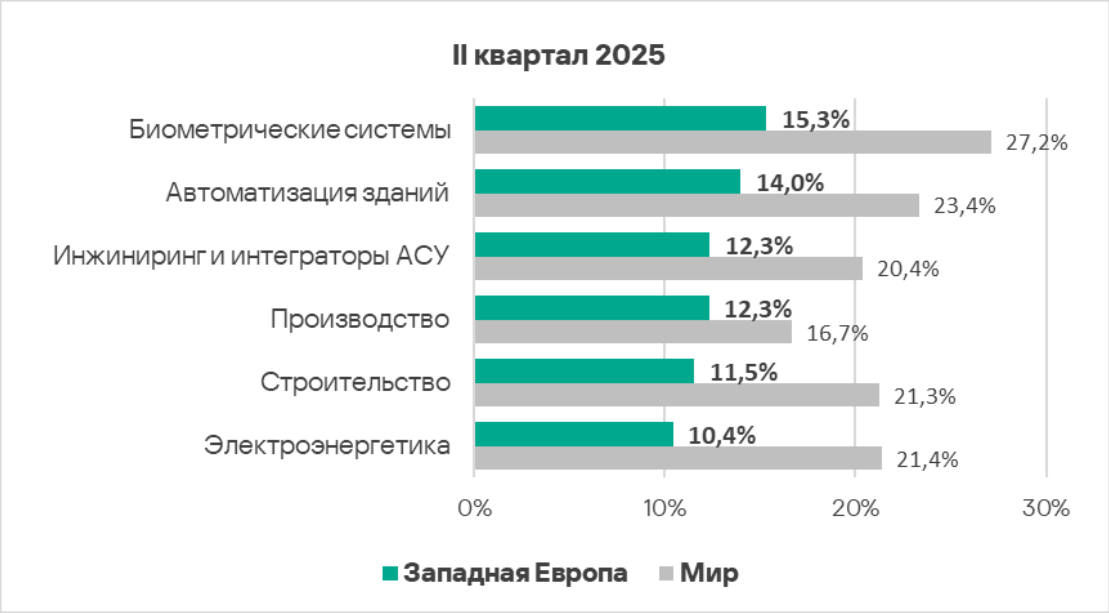
Среди стран региона в рейтинге по доле компьютеров АСУ, на которых блокируются веб-майнеры, лидирует Франция с 0,32%.



Отрасли

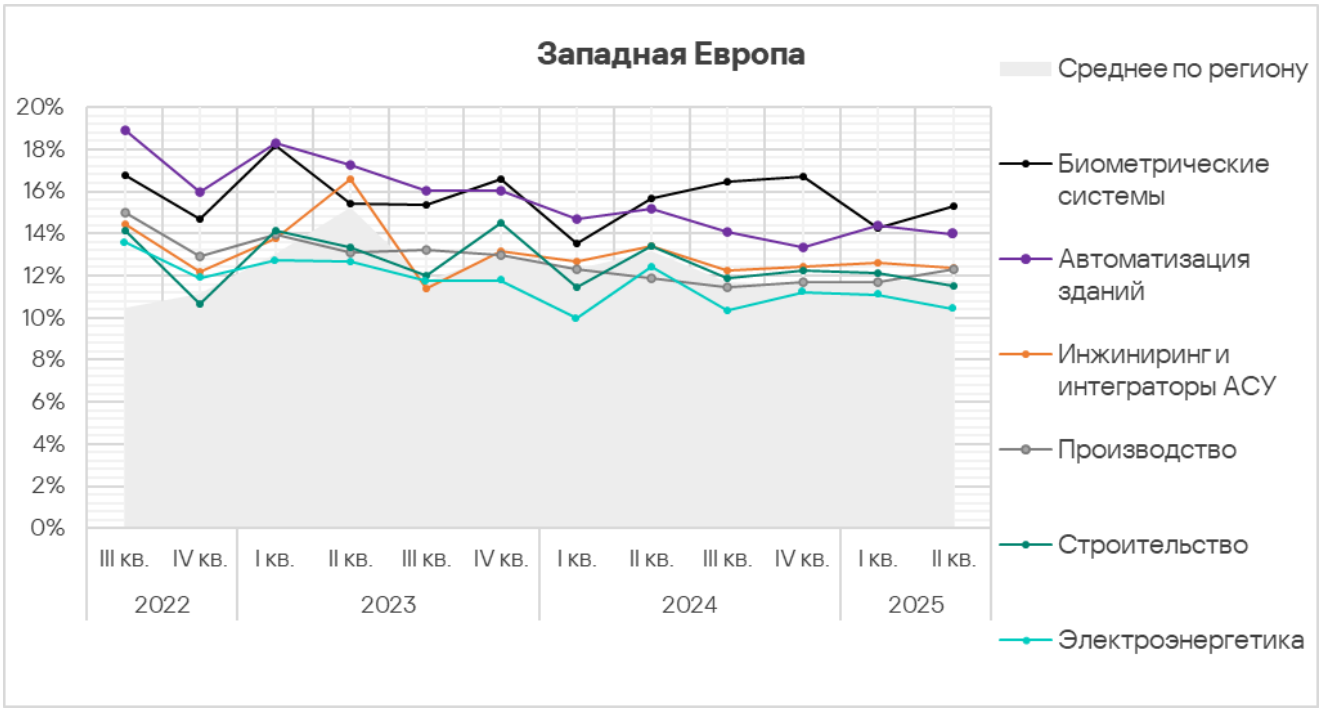
Доля компьютеров АСУ, на которых блокировались вредоносные объекты, во втором квартале 2025 года выше, чем у остальных рассмотренных в отчете отраслей, у OT-инфраструктуры биометрические системы.

Показатели во всех отраслях региона значительно ниже соответствующих среднемировых значений.



Во втором квартале 2025 года из рассмотренных отраслей региона показатель вырос у двух — биометрические системы и производство.

Показатели отраслей автоматизация зданий и биометрические системы по-прежнему заметно превышают среднее для региона значение.



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. В Западной Европе значения, наиболее приближенные к максимальным, наблюдается для совокупного показателя в сфере автоматизации зданий, а также в категории веб-майнеры в отрасли строительства.

Показатели источников угроз в отраслях в Западной Европе, 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	5,75%	6,67%	5,73%	7,59%	7,51%	6,54%	6,39%	6,82%
Почтовые клиенты	5,56%	4,18%	1,41%	1,73%	0,58%	2,11%	1,44%	1,89%
Съемные носители	0,00%	0,08%	0,17%	0,07%	0,29%	0,00%	0,25%	0,07%
Сетевые папки	0,00%	0,01%	0,02%	0,02%	0,00%	0,00%	0,00%	0,01%
Показатель отрасли в регионе	15,33%	13,96%	10,41%	12,34%	13,01%	11,51%	12,31%	

Показатели категорий угроз в отраслях в Западной Европе, 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	3,45%	3,93%	3,86%	4,77%	4,91%	3,82%	3,76%	4,31%
Вредоносные скрипты и фишинговые страницы	6,70%	5,84%	3,05%	4,42%	3,76%	4,97%	3,89%	4,15%
Троянцы-шпионы, бэкдоры и кейлоггеры	4,79%	2,51%	1,11%	1,43%	1,45%	1,03%	1,65%	1,38%
Черви (Worm)	0,38%	0,45%	0,28%	0,27%	0,29%	0,17%	0,72%	0,27%
Майнеры — исполняемые файлы для ОС Windows	0,19%	0,29%	0,33%	0,31%	0,58%	0,22%	0,25%	0,33%
Вредоносные документы (MSOffice+PDF)	3,64%	1,92%	0,78%	0,96%	0,58%	0,71%	0,85%	0,98%
Вирусы (Virus)	0,38%	0,26%	0,18%	0,16%	0,58%	0,24%	0,25%	0,16%
Программы-вымогатели	0,19%	0,12%	0,04%	0,06%	0,00%	0,00%	0,04%	0,07%
Веб-майнеры, выполняемые в браузерах	0,19%	0,26%	0,28%	0,26%	0,58%	0,22%	0,30%	0,27%
Вредоносные программы для AutoCAD	0,00%	0,00%	0,00%	0,01%	0,00%	0,10%	0,00%	0,01%
Показатель отрасли в регионе	15,33%	13,96%	10,41%	12,34%	13,01%	11,51%	12,31%	

«Горячие точки» отраслей

Биометрические системы

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах.
- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы следующие категории угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы и программы-вымогатели.
- Второе место среди отраслей региона по показателю вирусов.
- Третье место среди отраслей региона по показателю червей и вредоносных программ для AutoCAD.

Автоматизация зданий

- Второе месте среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах. Третье место — по показателю угроз в интернете и сетевых папках.
- Второе место среди отраслей региона по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви, программы-вымогатели.
- Третье место среди отраслей региона по показателю следующих категорий: ресурсы в интернете из списка запрещенных и вирусы.

Нефть и газ

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей. Второе место — по показателю угроз из интернета.
- Первое место среди отраслей региона по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, майнеры обеих категорий и вирусы.

Инжиниринг и интеграторы АСУ

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и в сетевых папках.
- Второе место среди отраслей региона по показателю следующих категорий: ресурсы в интернете из списка запрещенных и вредоносные программы для AutoCAD.
- Третье место среди отраслей региона по показателю следующих категорий: вредоносные документы, майнеры — исполняемые файлы для ОС Windows, программы-вымогатели.

Производство

- Второе место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.
- Первое место среди отраслей региона по показателю червей.
- Второе место среди отраслей региона по показателю веб-майнеров.
- Третье место среди отраслей региона по показателю шпионских программ.

Строительство

- Третье место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах.
- Первое место среди отраслей региона по показателю вредоносных программ для AutoCAD.
- Третье место среди отраслей региона по показателю категории вредоносные скрипты и фишинговые страницы.

Электроэнергетика

- Второе место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках. Третье место — по показателю угроз на съемных носителях.
- Второе место среди отраслей региона по показателю категории майнеры — исполняемые файлы для ОС Windows.
- Третье место среди отраслей региона по показателю веб-майнеров.

Северная Европа

Основные проблемы кибербезопасности в регионе

Самый благополучный с точки зрения кибербезопасности регион, традиционно занимающий последнее, 14-е, место в рейтинге по доле компьютеров АСУ, на которых блокируются вредоносные объекты.

При этом Северная Европа — один из двух регионов, где этот показатель во втором квартале 2025 года вырос.

В Северной Европе во втором квартале 2025 года выросли показатели нескольких категорий угроз, наиболее значительный рост отмечен у следующих категорий:

- ресурсы в интернете из списка запрещенных — в 1,6 раза, первое место среди регионов по росту этого показателя;
- программы-вымогатели — в 1,3 раза, показатель растет второй квартал подряд, во втором квартале 2025 года регион занимает третье место по росту этого показателя;
- майнеры — исполняемые файлы для ОС Windows — в 1,1 раза, второе место по росту этого показателя.

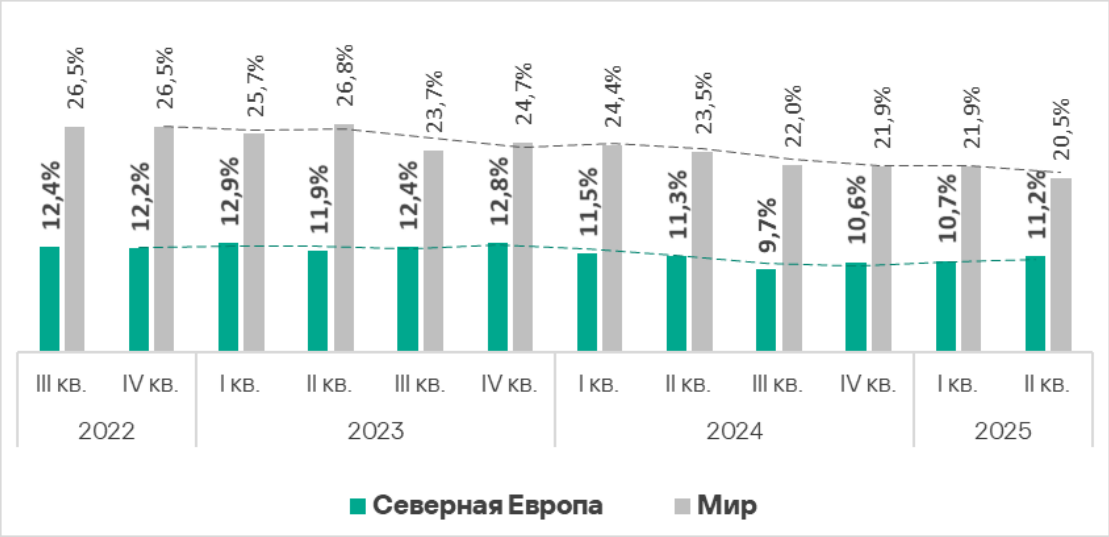
Основная причина роста связана с волнами заражений уязвимых ресурсов в интернете, которые используются для распространения майнеров обеих категорий, шпионского ПО и программ-вымогателей.

Статистика по всем угрозам

Северная Европа занимает 14-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Показатель в регионе значительно ниже среднемирового.

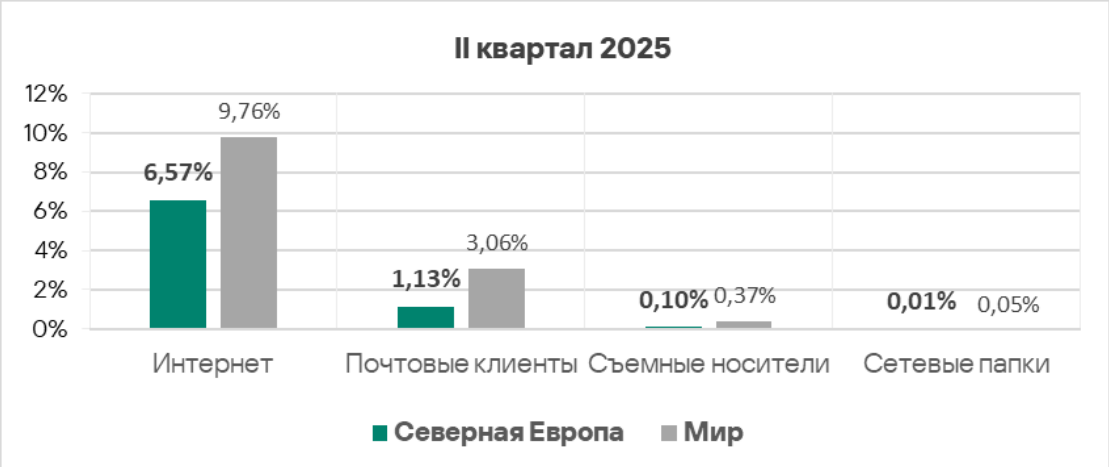
Северная Европа — один из двух регионов, где доля компьютеров АСУ, на которых блокировались вредоносные объекты, выросла во втором квартале 2025 года. Тем не менее, показатель региона — 11,2% — наименьший из всех регионов.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, лидирует Латвия с 12,77%. Наименьший показатель — в Люксембурге (7,35%).

Источники угроз

Показатели всех источников угроз в Северной Европе ниже среднемировых.

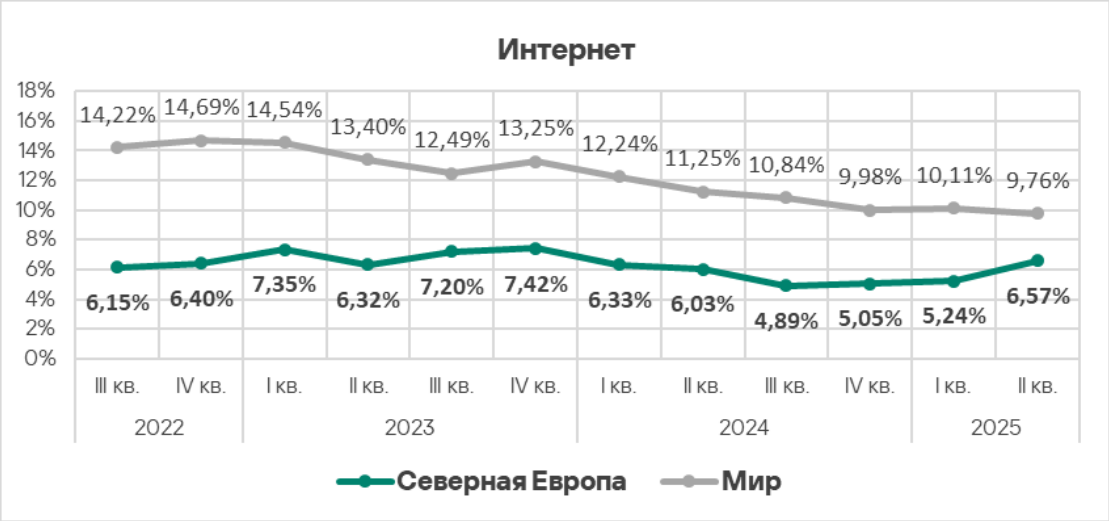


Доминирующие источники угроз в регионе — интернет и почта.

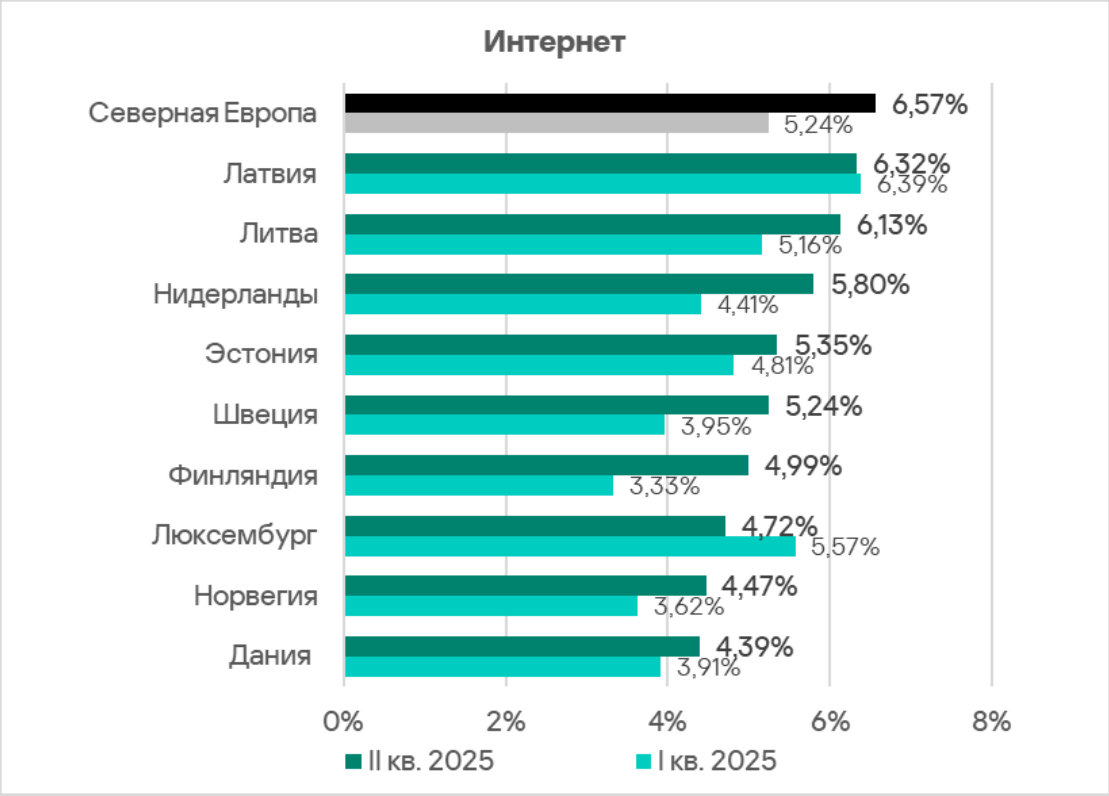
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась применительно к угрозам из всех источников. Северная Европа — единственный регион, где доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, во втором квартале 2025 года не уменьшилась.

Интернет

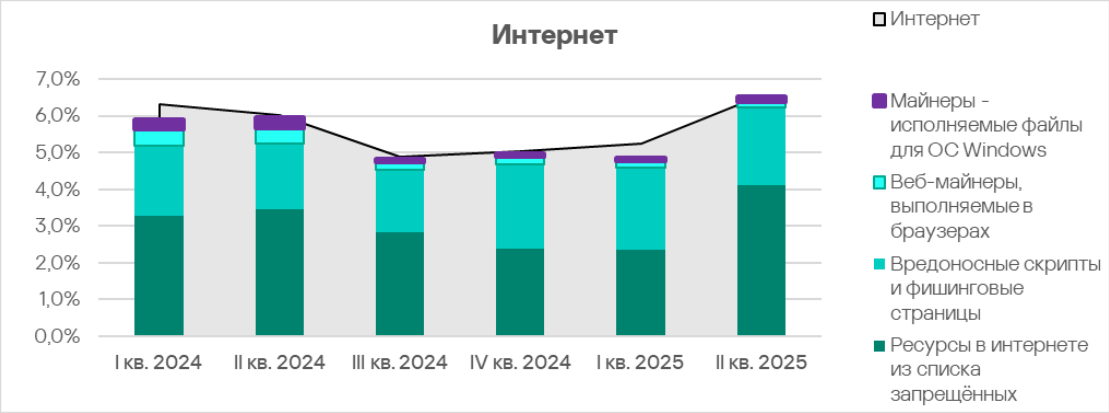
По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Северная Европа занимает 13-е место в рейтинге регионов с показателем 6,57%. Этот показатель растет в регионе третий квартал подряд. Во втором квартале 2025 года по его росту Северная Европа заняла первое место.



В странах региона доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, варьирует от 4,39% в Дании до 6,32% в Латвии.

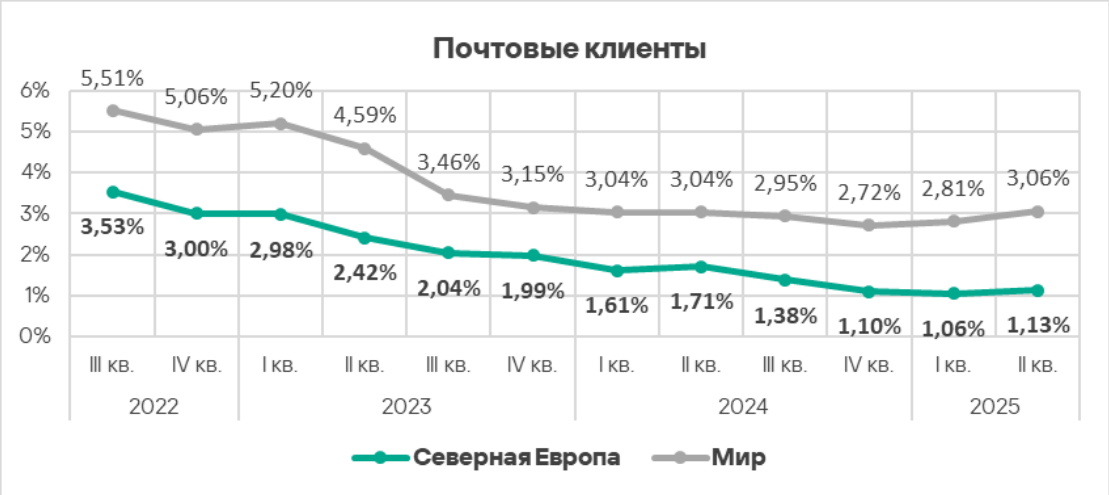


Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, майнеры обеих категорий.



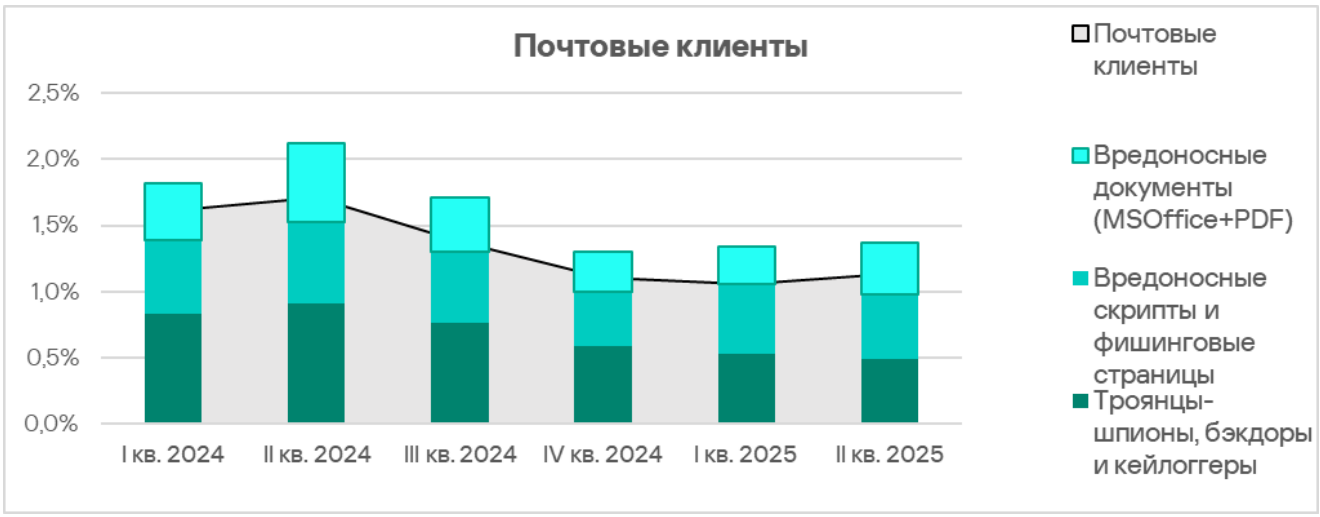
Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Северная Европа занимает 13-е место в рейтинге регионов с 1,13%. Этот показатель в 1,4 раза больше, чем в России, которая замыкает этот рейтинг.

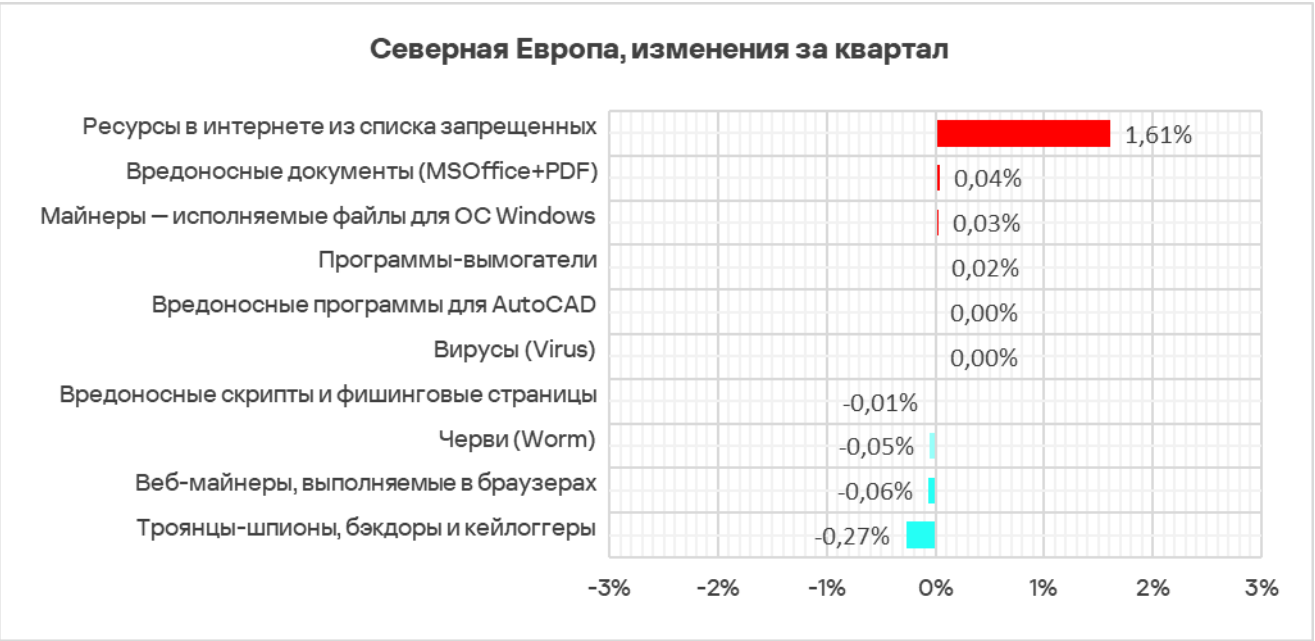


Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, лидирует Эстония с 2,57%. Наименьший показатель — в Финляндии (0,14%).

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



Категории угроз



Для всех категорий угроз показатели в регионе меньше среднемировых.

Рост за квартал отмечен у доли компьютеров АСУ, на которых были заблокированы следующие категории вредоносных объектов:

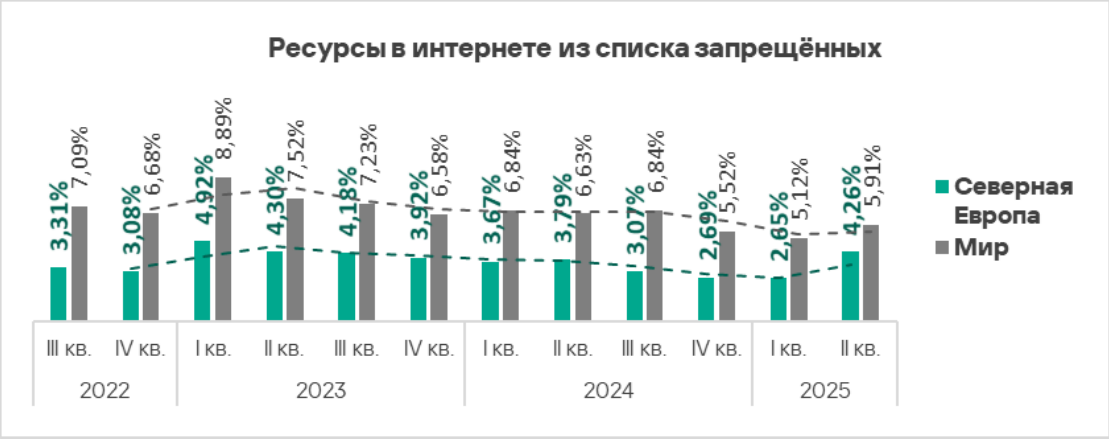
- ресурсы в интернете из списка запрещенных — в 1,6 раза, первое место среди регионов по росту этого показателя;
- программы-вымогатели — в 1,3 раза, третье место среди регионов по росту этого показателя;
- майнеры-исполняемые файлы для ОС Windows — в 1,1 раза, второе место среди регионов по росту этого показателя;
- вредоносные документы — в 1,1 раза.

Северная Европа — единственный регион, где во втором квартале 2025 года доля компьютеров АСУ, на которых блокируются вирусы, не уменьшилась.

Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Северная Европа занимает 10-е место в соответствующем рейтинге регионов с 4,26%. Это в 1,3 раза больше, чем в Восточной Азии, где этот показатель наименьший.

Во втором квартале 2025 года Северная Европа лидирует среди регионов по росту доли компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных.

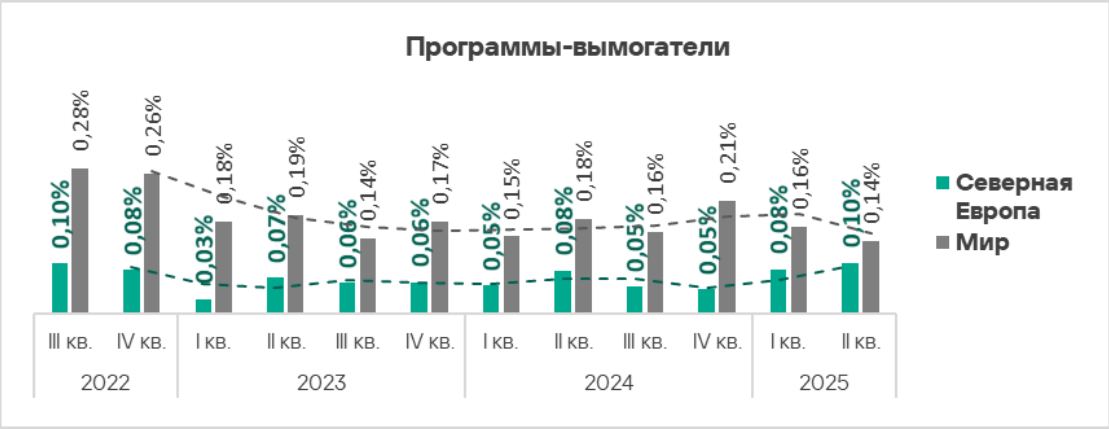


Среди стран региона по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, лидирует Латвия с 4,28%. Показатель за квартал вырос во всех странах региона.

Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, в соответствующем рейтинге регионов Северная Европа находится на 10-м месте с 0,10%. Это в 1,3 раза больше, чем в Западной Европе, где этот показатель наименьший.

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в регионе растет второй квартал подряд. Во втором квартале 2025 года Северная Европа занимает третье место среди регионов по его росту.



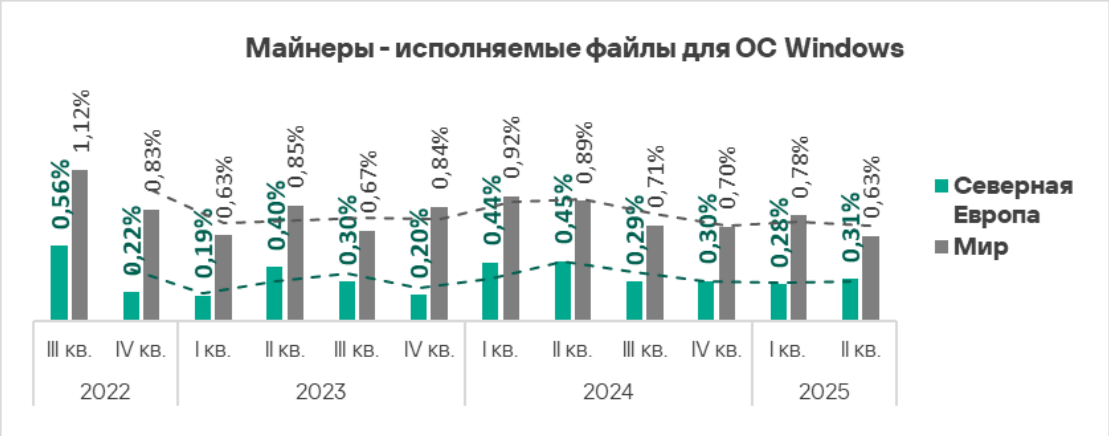
Среди стран региона по доле компьютеров АСУ, на которых блокировались программы-вымогатели, лидирует Эстония, где за квартал показатель резко вырос до 0,25%.

Программы-вымогатели в регионе распространяются через интернет и электронную почту.

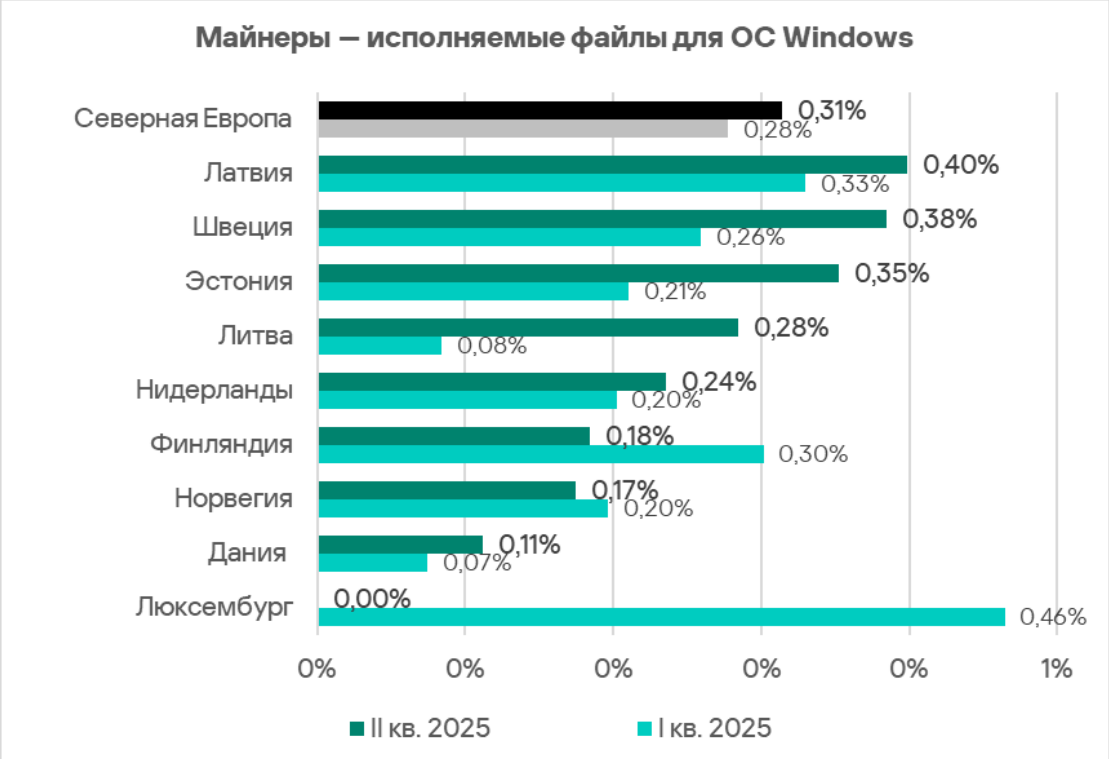
Майнеры — исполняемые файлы для ОС Windows

По доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, Северная Европа находится на 11-м месте в соответствующем рейтинге с 0,31%. Этот показатель в 1,7 раза больше, чем в Восточной Азии, где значение минимальное среди регионов.

Показатель в регионе колеблется. По его росту во втором квартале 2025 года Северная Европа заняла второе место среди регионов.



Среди стран региона в рейтинге по доле компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, лидирует Латвия с 0,40%.



* По Люксембургу нет данных за II квартал 2025 года.

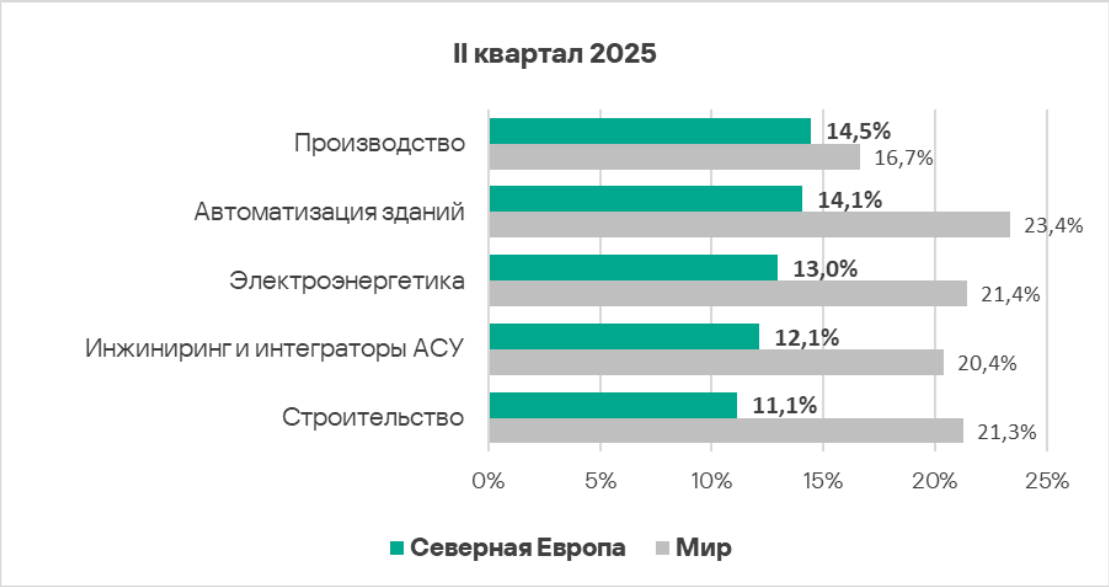
Майнеры — исполняемые файлы для ОС Windows в регионе распространяются преимущественно в интернете.

Отрасли

Во втором квартале 2025 года доля компьютеров АСУ, на которых блокировались вредоносные объекты, выше, чем в остальных

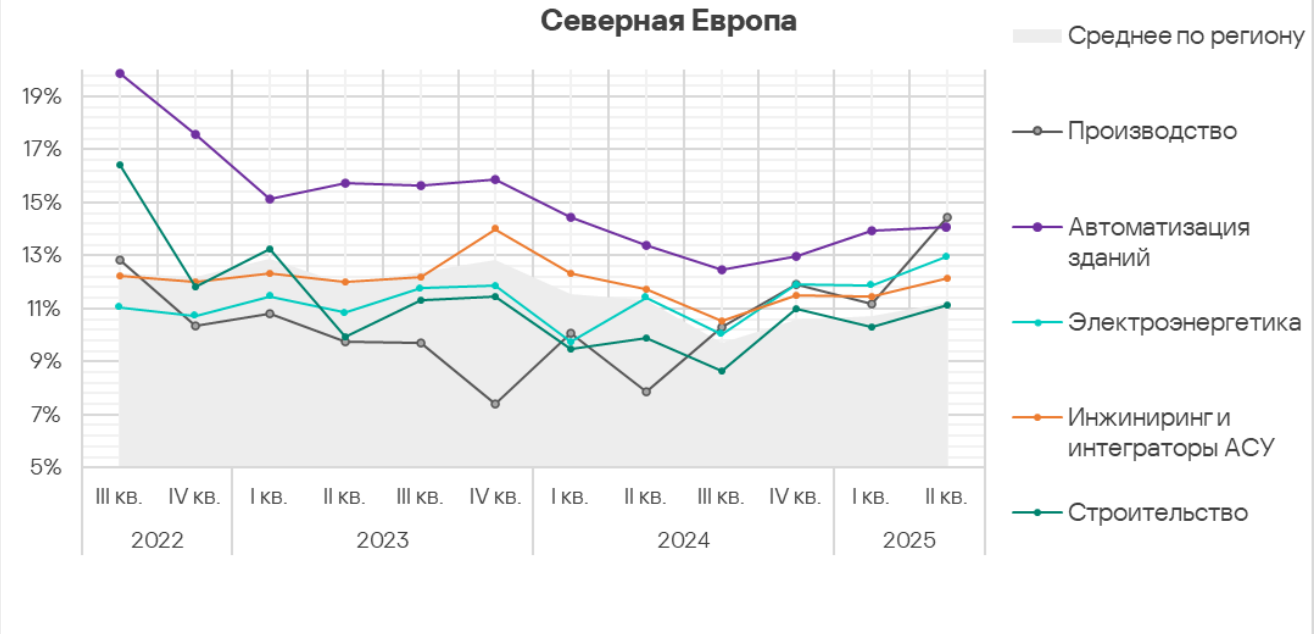
рассматриваемых отраслях, в производственной отрасли. Этот показатель вырос за квартал в 1,3 раза, и отрасль поднялась в рейтинге с третьего места на первое.

Показатели во всех отраслях региона по-прежнему остаются значительно ниже соответствующих среднемировых значений.



Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла во всех рассматриваемых отраслях.

Тренд автоматизации зданий остается заметно выше среднего регионального.



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. В Северной Европе в основном наблюдаются значения, близкие к минимальным. Наибольший показатель в регионе — у угроз из категории ресурсы в интернете из списка запрещенных, заблокированных на компьютерах в сфере электроэнергетики. Электроэнергетика занимает 30-е место из 98 в рейтинге отраслей всех регионов по доле угроз из этой категории.

Показатели источников угроз в отраслях в Северной Европе, II квартал 2025 года

Отрасль / Источник угрозы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Интернет	6,77%	8,09%	7,76%	6,86%	8,26%	6,57%
Почтовые клиенты	3,36%	0,55%	0,72%	1,57%	1,24%	1,13%
Съемные носители	0,12%	0,16%	0,11%	0,31%	0,00%	0,10%
Сетевые папки	0,00%	0,00%	0,01%	0,00%	0,00%	0,01%
Показатель отрасли в регионе	14,07%	12,96%	12,13%	11,14%	14,46%	

Показатели категорий угроз в отраслях в Северной Европе, II квартал 2025 года

Отрасль / Категории вредоносного ПО	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	4,53%	6,13%	4,96%	4,41%	5,58%	4,26%
Вредоносные скрипты и фишинговые страницы	4,20%	3,38%	3,65%	3,27%	5,58%	3,06%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,31%	1,41%	1,42%	1,51%	1,86%	1,44%
Черви (Worm)	0,52%	0,55%	0,32%	0,38%	1,03%	0,25%
Майнеры — исполняемые файлы для ОС Windows	0,30%	0,39%	0,35%	0,25%	0,41%	0,31%
Вредоносные документы (MSOffice+PDF)	1,69%	0,47%	0,48%	0,50%	0,83%	0,64%
Вирусы (Virus)	0,49%	0,47%	0,17%	0,38%	0,21%	0,21%
Программы-вымогатели	0,21%	0,31%	0,11%	0,19%	0,00%	0,10%
Веб-майнеры, выполняемые в браузерах	0,18%	0,31%	0,24%	0,19%	0,21%	0,18%
Вредоносные программы для AutoCAD	0,00%	0,00%	0,00%	0,13%	0,00%	0,01%
Показатель отрасли в регионе	14,07%	12,96%	12,13%	11,14%	14,46%	

«Горячие точки» отраслей

Производство

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета.
- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, программы-вымогатели.
- Второе место среди отраслей региона по показателям вирусов и веб-майнеров.

Автоматизация зданий

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах.
- Первое место среди отраслей региона по показателю вирусов.
- Второе место среди отраслей региона по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы, черви, программы-вымогатели.

Электроэнергетика

- Второе место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и на съемных носителях.
- Первое место среди отраслей региона по доле компьютеров АСУ, на которых были заблокированы угрозы следующих категорий: ресурсы в интернете из списка запрещенных, майнеры обеих категорий и черви.

Инжиниринг и интеграторы АСУ

- Первое место среди отраслей по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.
- Второе место среди отраслей региона по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы для ОС Windows, вредоносные программы для AutoCAD.

Строительство

- Первое место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных

носителей. Второе — по показателям угроз в почтовых клиентах и сетевых папках.

- Первое место среди отраслей региона 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