Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Южная и Северная Америка (Канада)

Второй квартал 2025 года

22.09.2025

Версия 1.0

Южная Америка

Основные проблемы кибербезопасности в регионе

Высокий риск целевых атак

В Южной Америке значительно выше среднемировых значений доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов — в 1,8 раза. По этому показателю регион занимает второе место в мире.

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Южная Америка лидирует среди регионов с показателем, который в 1,4 раза больше 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.

По доле компьютеров АСУ, на которых блокируются вредоносные документы, Южная Америка занимает второе место в мире. Показатель в регионе превышает среднемировой в 1,7 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.

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

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

Высокий показатель шпионских программ

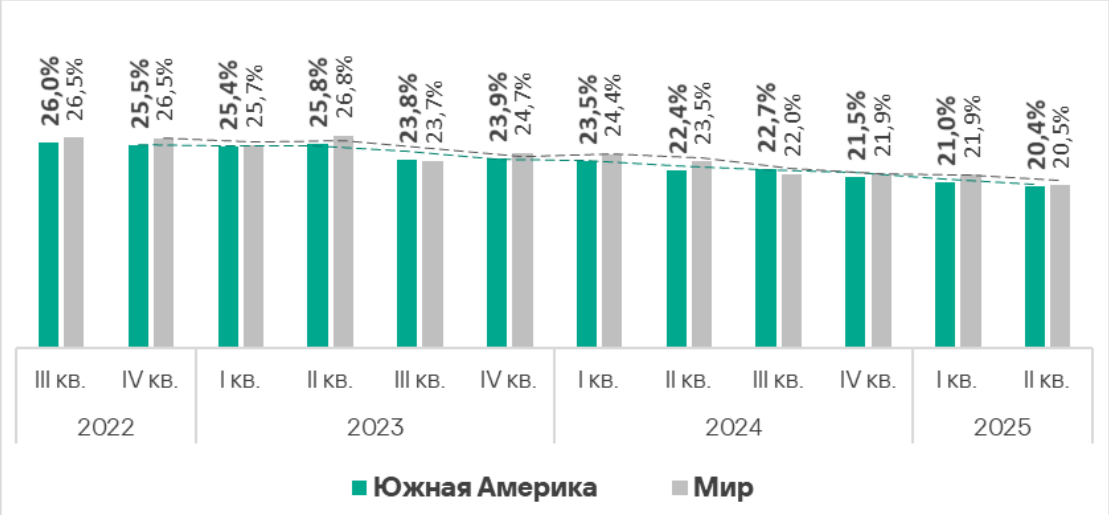
Доля компьютеров АСУ, на которых блокируются шпионские программы, в Южной Америке в 1,2 раза выше, чем в среднем в мире. В региональном рейтинге категорий угроз шпионские программы занимают второе место. По росту показателя этой категории угроз во втором квартале 2025 года регион лидирует.

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.

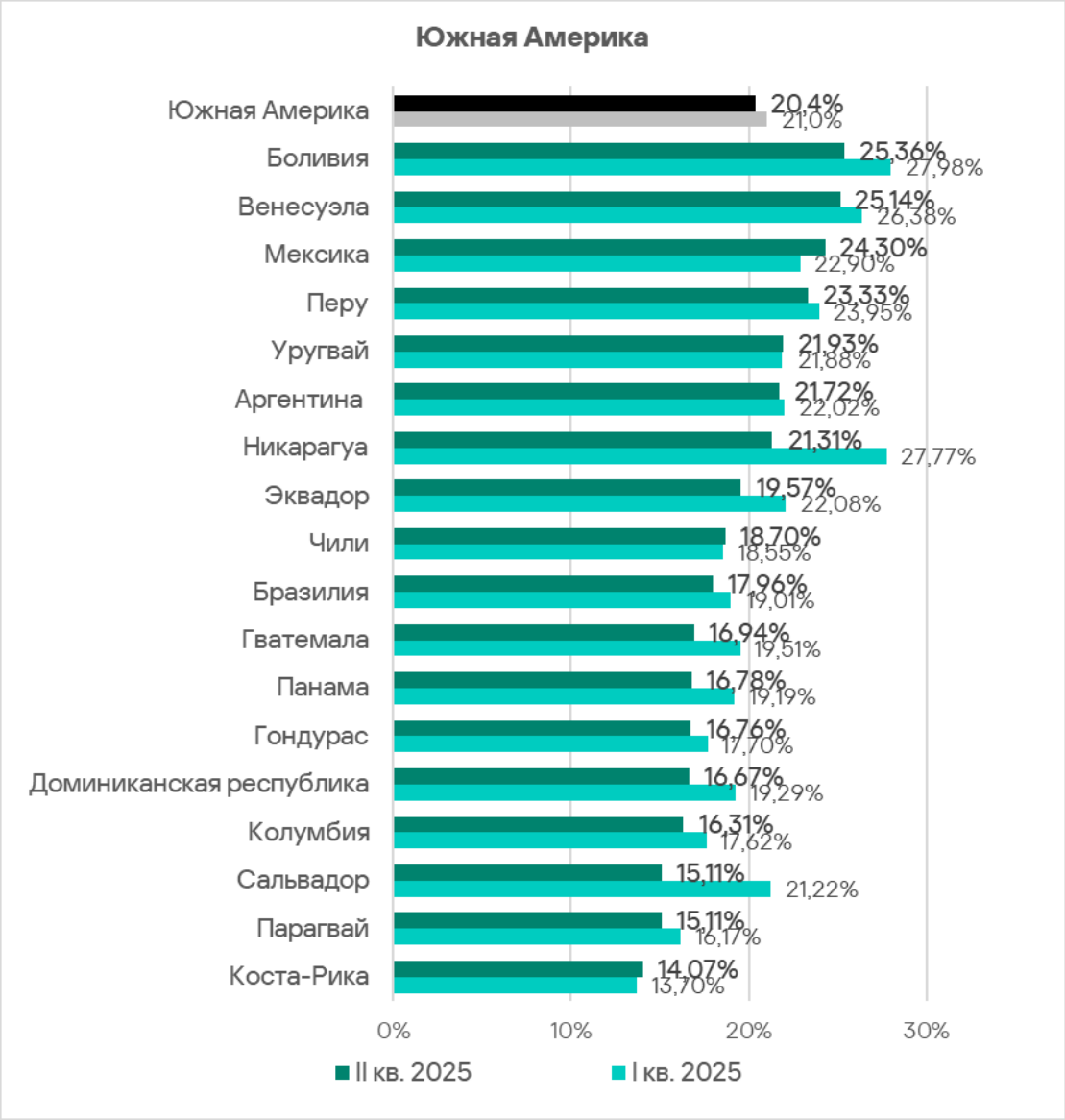
Статистика по всем угрозам

Южная Америка во втором квартале 2025 года поднялась с восьмого на пятое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Несмотря на это, показатель в регионе уменьшается третий квартал подряд. Во втором квартале 2025 года он опустился до 20,4% — это чуть ниже среднемирового значения и в 1,8 раза больше, чем в Северной Европе, где значение наименьшее из всех регионов.

В регионе наблюдается нисходящий тренд. Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Южной Америке наименьшая за период с третьего квартала 2022 года.



Среди стран региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 14,07% в Коста-Рике до 25,36% в Боливии.



Источники угроз

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

Вредоносные объекты в регионе распространяются преимущественно через интернет и почту.

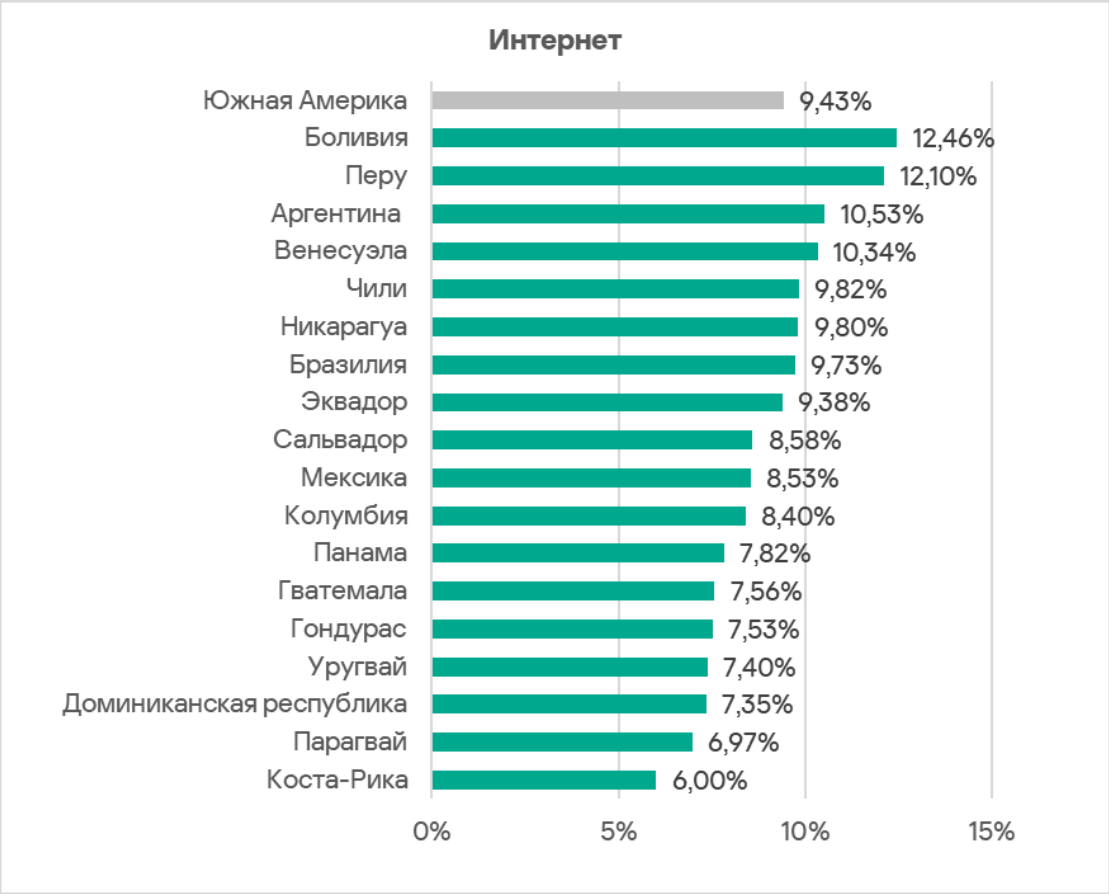
Южная Америка занимает второе место в рейтинге регионов по доле компьютеров АСУ, на которых заблокированы угрозы из почтовых клиентов, с превышением среднемирового значения в 1,8 раза.

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

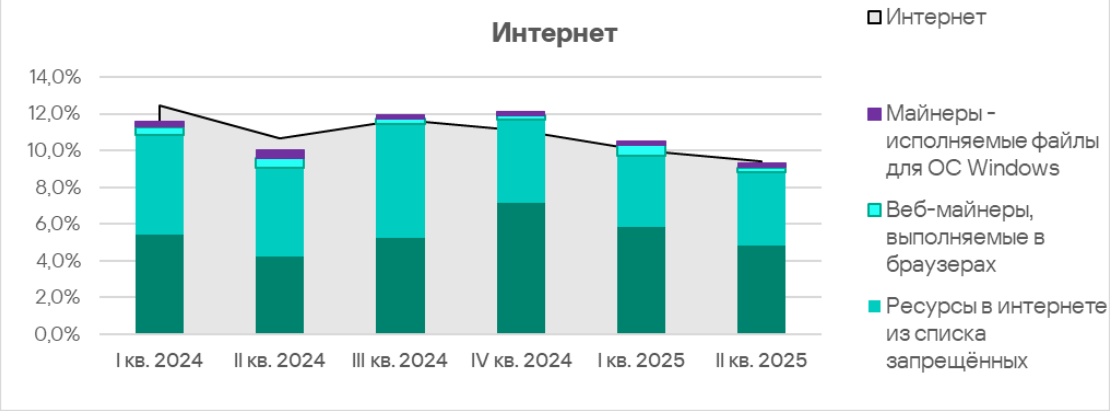
Интернет

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

Показатели стран региона варьируют от 6,00% в Коста-Рике до 12,46% в Боливии.



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



Почтовые клиенты

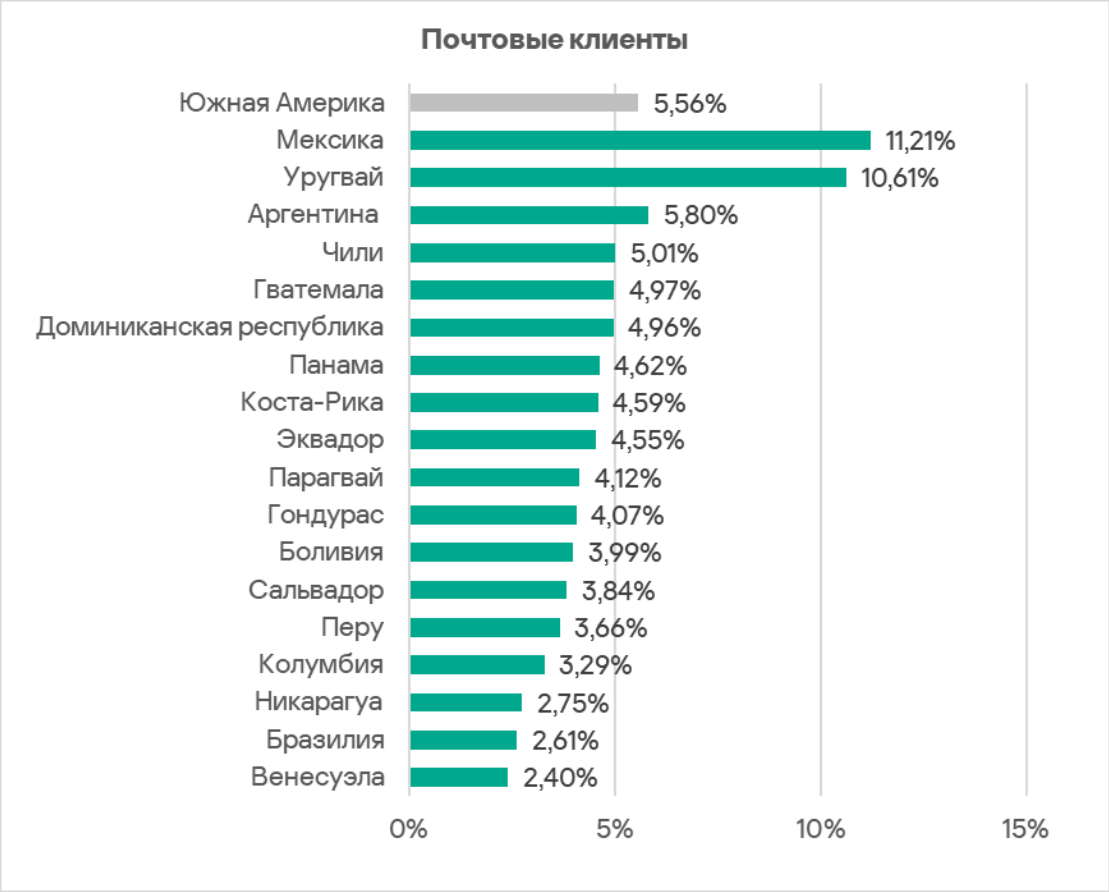
По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, во втором квартале 2025 года Южная Америка занимает второе место среди регионов, уступая только Южной Европе. Показатель Южной Америки в 7 раз выше, чем в России, которая замыкает этот рейтинг.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, выросла во всех регионах, кроме России. По росту этого показателя также лидирует Южная Америка.

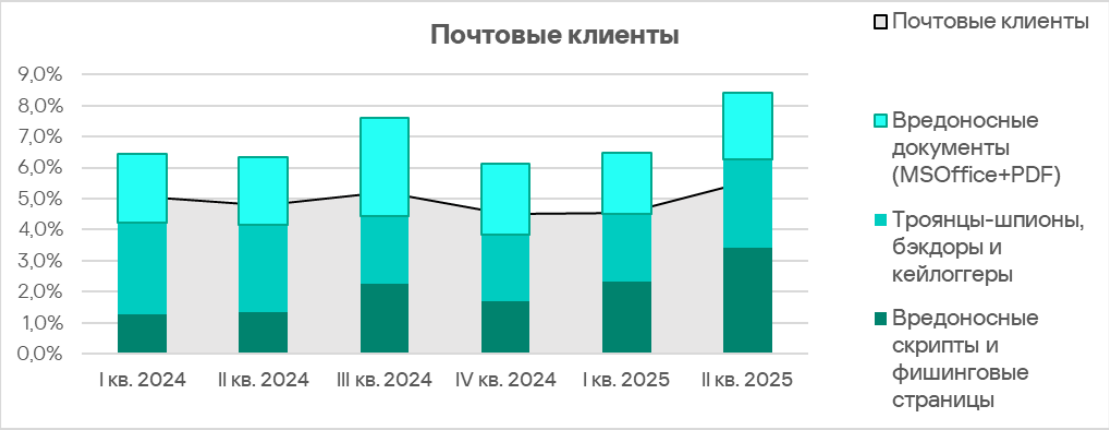
Совместно с высокими показателями скриптов и фишинговых страниц это свидетельствует о высокой доступности систем, относящихся к OT-инфраструктуре, для целевых атак.

Показатель почтовых клиентов в регионе растет второй квартал подряд, что соответствует динамике среднемирового значения.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, с отрывом лидируют Мексика с 11,21% и Уругвай с 10,61%. Показатели остальных стран варьируют от 2,40% в Венесуэле до 5,80% в Аргентине.



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



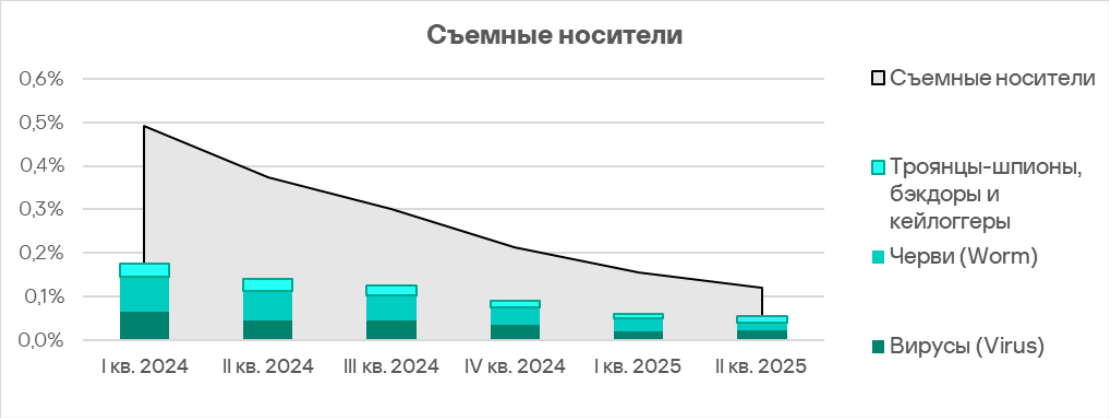
Страны в тройке лидеров рейтинга по почтовым клиентам — Мексика, Уругвай и Аргентина — занимают верхние строчки и в рейтинге по показателям шпионских программ. Мексика и Аргентина также лидируют в рейтинге по показателю вредоносных скриптов и фишинговых страниц, Уругвай и Мексика — по показателю вредоносных документов.

Съемные носители

По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, во втором квартале 2025 года Южная Америка занимает девятое место среди регионов. В Северной Америке (Канаде), которая занимает последнее место в рейтинге, показатель меньше в 4,5 раза.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, с большим отрывом лидирует Венесуэла с 0,47%.

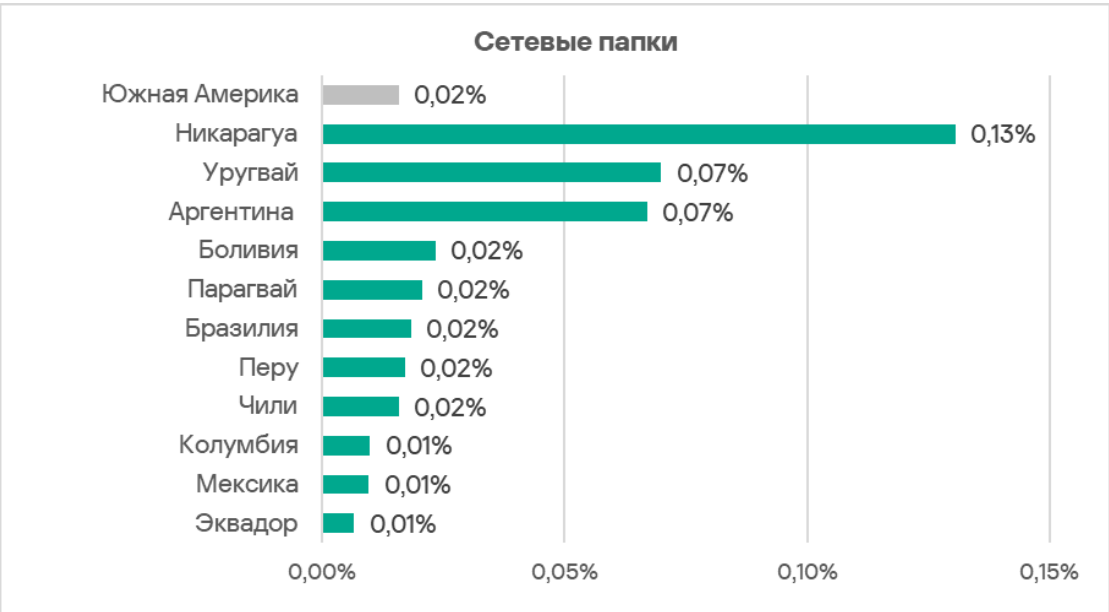
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: вирусы, черви и шпионское ПО.



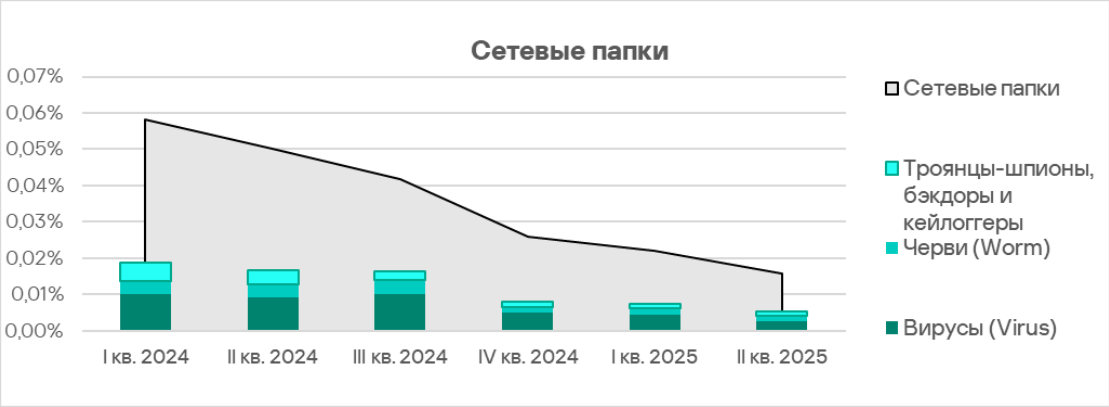
Сетевые папки

Южная Америка занимает девятое место среди регионов по доле компьютеров АСУ, на которых угрозы блокируются в сетевых папках, с 0,02%. С Северной Европой, которая занимает последнее место в рейтинге, показатели отличаются в 1,6 раза.

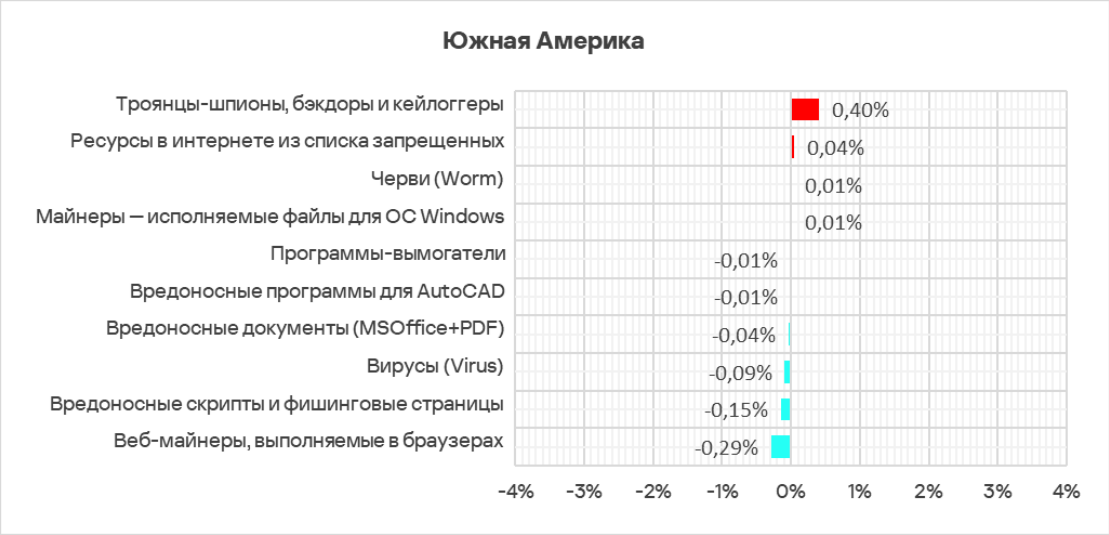
Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, с отрывом лидирует Никарагуа с 0,13%.



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



Категории угроз



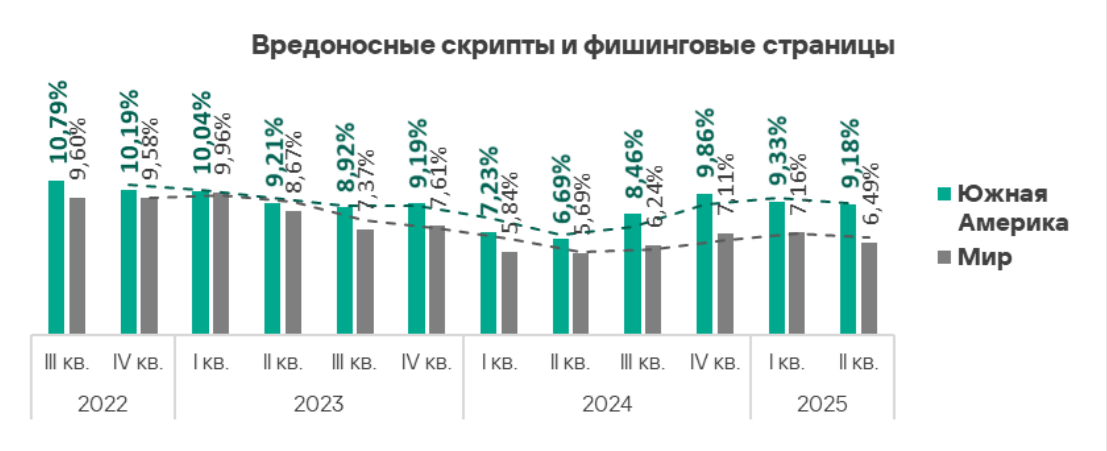
По сравнению с мировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- вредоносные документы — в 1,7 раза, второе место среди регионов;
- вредоносные скрипты и фишинговые страницы — в 1,4 раза, первое место среди регионов;
- веб-майнеры — в 1,4 раза, второе место среди регионов;
- шпионские программы — в 1,2 раза, по росту показателя за квартал первое место среди регионов.

Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Южная Америка лидирует в соответствующем рейтинге регионов с 9,18%. Это в 3 раза больше, чем в Северной Европе, где этот показатель наименьший.

Показатель в регионе уменьшается второй квартал подряд.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Мексика с 13,80%. Наименьший показатель в Гондурасе — 4,80%.

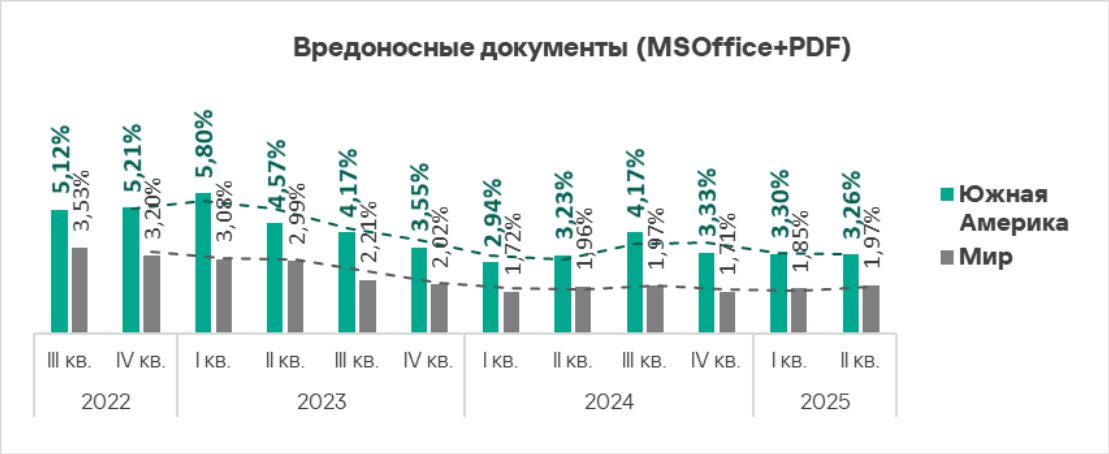
Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

Лидеры по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, — Мексика и Аргентина — также занимают верхние строчки в рейтингах по показателям шпионских программ и по доле компьютеров АСУ, где угрозы были заблокированы в почтовых клиентах.

Вредоносные документы

Вредоносные документы распространяются преимущественно по электронной почте. Южная Америка занимает второе место в обоих рейтингах регионов — и по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, и по показателю вредоносных документов.

В Южной Америке доля компьютеров АСУ, на которых блокируются вредоносные документы, уменьшается третий квартал подряд. Показатель в регионе (3,26%) — в 5,1 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.



Среди стран региона по этому показателю лидируют Уругвай с 7,61% и Мексика с 4,99%. Показатели остальных стран варьируют от 1,65% в Панаме до 3,17% в Чили.

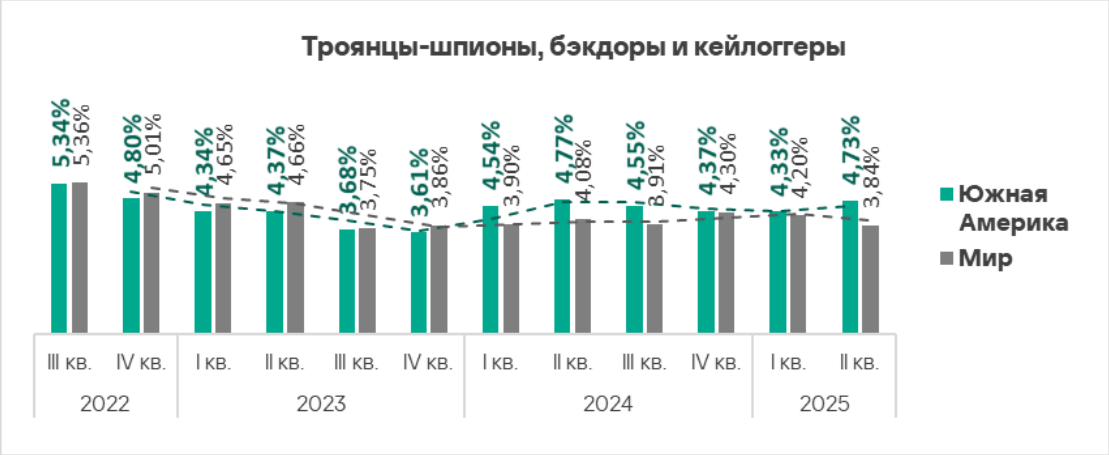
Уругвай и Мексика также возглавляют рейтинг стран региона по доле компьютеров АСУ, где угрозы были заблокированы в почтовых клиентах.

Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, в соответствующем рейтинге регионов Южная Америка находится на пятом месте с 4,73%. Это в 3,4 раза больше, чем в Западной Европе, где этот показатель наименьший.

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

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



Среди стран региона по доле компьютеров АСУ, на которых заблокированы шпионские программы, с отрывом от остальных стран лидирует Уругвай с 11,45%. В Бразилии показатель наименьший — 2,40%.

Во втором квартале 2025 года доля компьютеров АСУ, на которых блокируются шпионские программы, выросла только в двух регионах, и Южная Америка лидирует по росту этого показателя. Среди стран региона больше всего показатель вырос в Уругвае, Мексике и Гватемале.

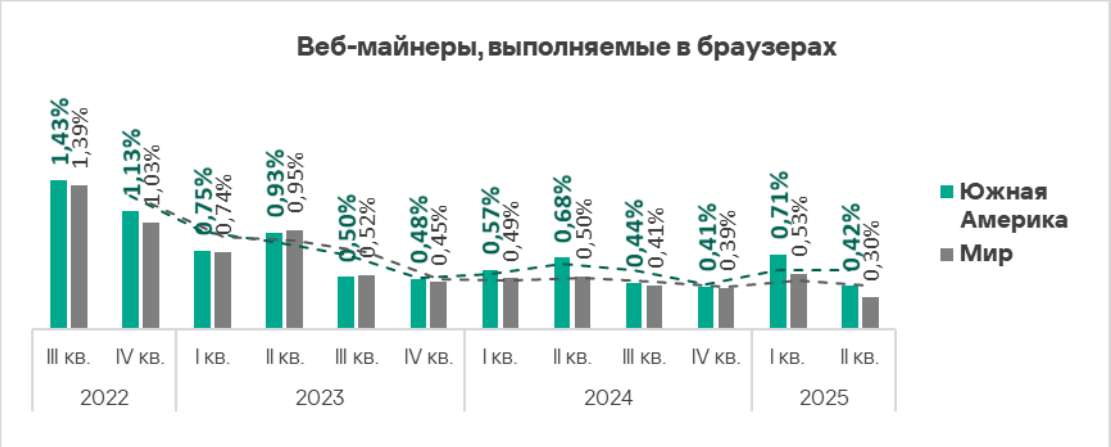
Шпионские программы в регионе блокируются во всех источниках угроз, преимущественно в почтовых клиентах.

Первые три страны в рейтинге по шпионским программам оказались и в числе лидеров региона по угрозам из почтовых клиентов.

Веб-майнеры

По доле компьютеров АСУ, на которых блокируются веб-майнеры, Южная Америка занимает второе место среди регионов с 0,42%. Это в 4 раза больше, чем в Восточной Азии, где показатель наименьший среди регионов.

Показатель веб-майнеров в регионе с третьего квартала 2023 года колеблется в диапазоне от 0,41% до 0,71%.



Среди стран региона по доле компьютеров АСУ, на которых блокируются веб-майнеры, лидирует Гондурас с 0,67%. Наименьший показатель в Панаме — 0,18%.

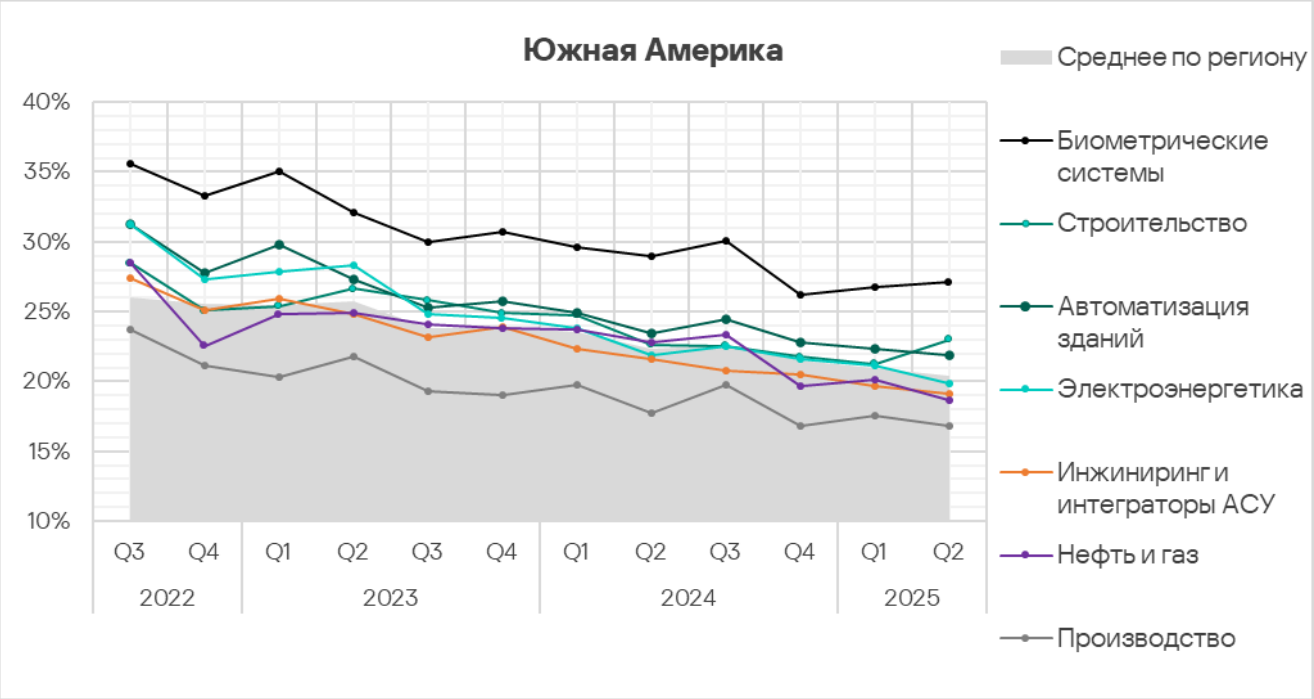
Отрасли

В регионе из всех рассмотренных в отчете отраслей чаще всего вредоносные объекты блокируются в OT-инфраструктуре биометрические системы.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает среднемировое значение в трех отраслях — нефтегазовой, строительстве и производстве.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, немного увеличилась в OT-инфраструктуре биометрические системы и в отрасли строительство.

Рассмотренные отрасли, несмотря на колебания, демонстрируют преимущественно позитивную динамику долгосрочных трендов начиная с третьего квартала 2023 года.



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

При оценке проблем отраслей мы используем тепловые карты. На них ячейки окрашиваются в цвета в диапазоне от красного к зеленому, где красный цвет указывает на максимальное значение индустрии в регионе, источника или категории угроз среди всех регионов и индустрий. В Южной Америке близкие к максимальным значения наблюдаются для интернет-угроз в строительстве, а также показателей в категориях веб-майнеры — в нефтегазовой сфере и вредоносные скрипты и фишинговые страницы — в биометрических системах.

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

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

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	8,55%	8,89%	11,06%	10,16%	10,70%	12,98%	7,83%	9,43%
Почтовые клиенты	12,55%	7,73%	3,08%	3,25%	3,71%	3,85%	2,78%	5,56%
Съемные носители	0,14%	0,12%	0,11%	0,11%	0,11%	0,08%	0,07%	0,12%
Сетевые папки	0,02%	0,02%	0,00%	0,01%	0,00%	0,00%	0,00%	0,02%
Показатель отрасли в регионе	27,10%	21,86%	19,86%	19,11%	18,67%	23,00%	16,78%	

Показатели категорий угроз в отраслях в Южной Америке, 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	3,50%	3,85%	5,59%	4,62%	6,88%	5,77%	3,76%	4,23%
Вредоносные скрипты и фишинговые страницы	14,23%	10,53%	8,05%	7,77%	6,88%	9,94%	7,24%	9,18%
Троянцы-шпионы, бэкдоры и кейлоггеры	9,77%	6,23%	3,30%	3,03%	3,28%	4,18%	3,61%	4,73%
Черви (Worm)	1,17%	0,88%	0,97%	0,60%	1,53%	0,79%	0,66%	0,75%
Майнеры — исполняемые файлы для ОС Windows	0,44%	0,49%	0,80%	0,55%	1,31%	0,95%	0,42%	0,51%
Вредоносные документы (MSOffice+PDF)	5,91%	4,47%	2,09%	2,15%	1,86%	1,97%	2,02%	3,26%
Вирусы (Virus)	0,87%	0,80%	0,91%	0,55%	0,76%	1,45%	0,69%	0,71%
Программы-вымогатели	0,17%	0,12%	0,15%	0,09%	0,22%	0,21%	0,03%	0,10%
Веб-майнеры, выполняемые в браузерах	0,35%	0,38%	0,66%	0,44%	0,98%	0,79%	0,36%	0,42%
Вредоносные программы для AutoCAD	0,03%	0,04%	0,13%	0,08%	0,11%	0,62%	0,08%	0,07%
Показатель отрасли в регионе	27,10%	21,86%	19,86%	19,11%	18,67%	23,00%	16,78%	

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

«Горячие точки» отраслей

Биометрические системы

- Лидер в регионе по показателям угроз из почтовых клиентов, на съемных носителях и в сетевых папках.

- Лидер среди отраслей в регионе по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы.
- Второе место среди отраслей во всех регионах по доле компьютеров, на которых были заблокированы вредоносные скрипты и фишинговые страницы.
- Второе место среди отраслей региона по показателю червей.
- Третье место в регионе по показателям вирусов и программ-вымогателей.

Строительство

- Первое место в регионе среди отраслей по показателю угроз из интернета, третье — по показателю угроз из почтовых клиентов.
- Первое место среди отраслей региона по показателям вирусов и вредоносных программ для AutoCAD.
- Второе место среди отраслей во всех регионах по показателю веб-майнеров.
- Второе место среди отраслей региона по показателям следующих категорий угроз: ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы и программы-вымогатели.
- Третье место в регионе по показателю категорий следующих угроз: вредоносные скрипты и фишинговые страницы, а также шпионские программы.

Автоматизация зданий

- Второе место среди отраслей региона по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах, на съемных носителях и в сетевых папках.
- Второе место в регионе среди отраслей по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионские программы, вредоносные документы.
- Четвертое место в регионе по показателям червей и вирусов.

Электроэнергетика

- Второе место среди отраслей региона по показателю угроз из интернета, третье место по показателю угроз на съемных носителях, четвертое место по показателю угроз в сетевых папках.
- Второе место среди отраслей региона по показателям вирусов и вредоносных программ для AutoCAD.
- Третье место в регионе по показателю следующих категорий: ресурсы в интернете из списка запрещенных, черви, майнеры обеих категорий.

- Четвертое место в регионе по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы и программы-вымогатели.

Инжиниринг и интеграторы АСУ

- Третье место среди отраслей региона по показателю угроз в сетевых папках. Четвертое место среди отраслей региона по показателю угроз из интернета.
- Третье место в регионе среди отраслей по показателю вредоносных документов.
- Четвертое место среди отраслей в регионе по показателям следующих категорий: ресурсы в интернете из списка запрещенных, майнеры обеих категорий, вредоносные программы для AutoCAD.

Нефтегазовая отрасль

- Третье место в регионе среди отраслей по показателю угроз из интернета. Четвертое место по показателю угроз в почтовых клиентах и на съемных носителях.
- Лидер среди отраслей в регионе по показателям категорий: ресурсы в интернете из списка запрещенных, черви, майнеры обеих категорий, программы-вымогатели.
- Третье место в регионе среди отраслей по показателю вредоносных программ для AutoCAD.

Производство

- Четвертое место среди отраслей региона по доле компьютеров АСУ, на которых блокировались шпионские программы.

Северная Америка (Канада)

Основные проблемы кибербезопасности в регионе

Один из наиболее благополучных с точки зрения кибербезопасности регионов. По доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором квартале 2025 года Северная Америка (Канада) занимает в рейтинге регионов 12-е место.

При этом по показателям некоторых источников и категорий угроз регион в соответствующих рейтингах занимает более высокие позиции:

- веб-майнеры — седьмое место;
- угрозы из почтовых клиентов — восьмое место;
- вредоносные скрипты и фишинговые страницы — восьмое место;
- вирусы — восьмое место;
- майнеры — исполняемые файлы — девятое место.

Очевидно, что компьютеры, на которых были заблокированы веб-майнеры (исполняемые в веб-браузере), с высокой вероятностью имеют незащищенное подключение к интернету. Также очевидно, что компьютеры, на которых блокировались угрозы из почтовых клиентов, имеют доступ к незащищенному почтовому сервису — в Северной Америке (Канаде) почтовый спам и фишинг, содержащий вредоносные скрипты и майнеры в виде исполняемых файлов, вероятнее всего попадал на компьютеры в технологической сети через доступ к почтовому серверу в корпоративной сети, открытый для внешних рассылок.

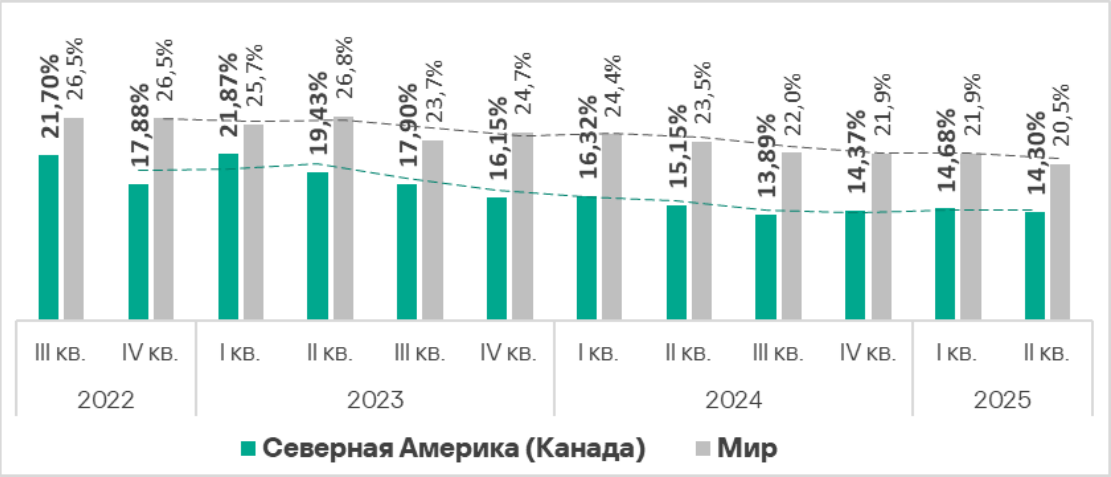
Северная Америка (Канада) — это один из пяти регионов, где во втором квартале выросла доля интернет-угроз (второе место в рейтинге), а также один из трех регионов, где наблюдался небольшой рост доли угроз в сетевых папках, на фоне общего снижения.

Северная Америка (Канада) — второй из четырех регионов по росту доли компьютеров во втором квартале 2025 года, на которых блокировались майнеры — исполняемые файлы, в то время как в большинстве регионов доля этой категории угроз снизилась.

Относительно высокие показатели угроз, распространяющихся через почтовые клиенты (фишинг), вредоносных скриптов и майнеров обеих категорий могут быть признаками доступности технологических систем в регионе для продвинутых категорий злоумышленников.

Статистика по всем угрозам

Северная Америка (Канада) занимает 12-е место по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты. Значение показателя — 14,3% — существенно ниже среднемирового, но в 1,3 раза выше, чем в Северной Европе, которая замыкает этот рейтинг.

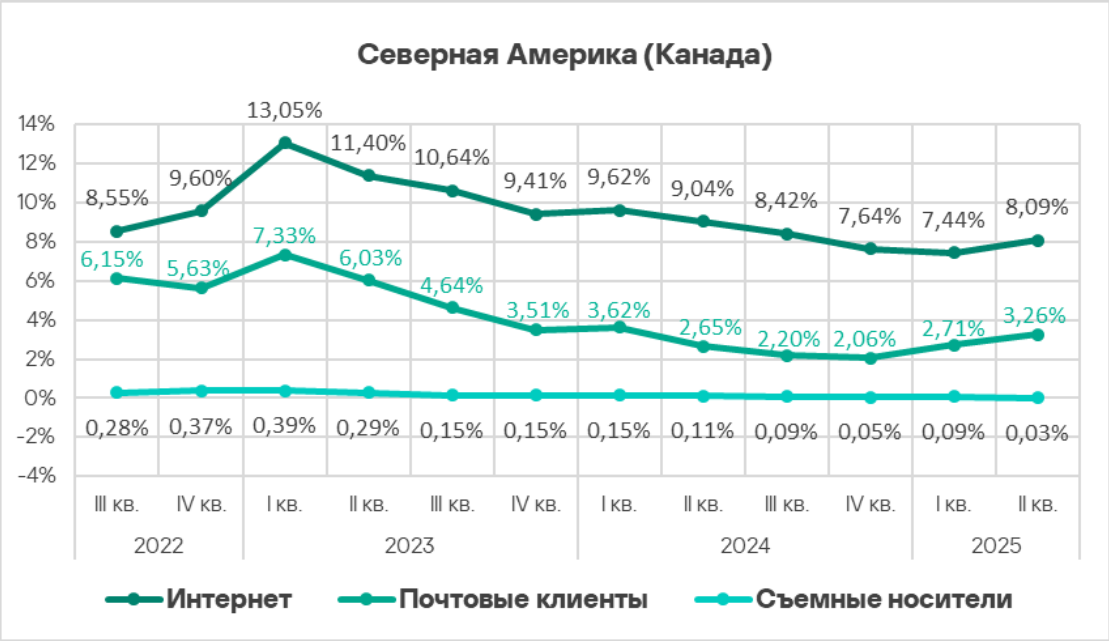


Источники угроз

Показатели всех источников угроз, кроме почтовых клиентов, в Северной Америке (Канаде) ниже, чем среднемировые. Доля компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, в регионе в 1,1 раза выше среднемирового показателя.

Вредоносные объекты в регионе распространяются преимущественно через интернет и почту. В рейтинге по доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, Северная Америка (Канада) занимает последнее место.

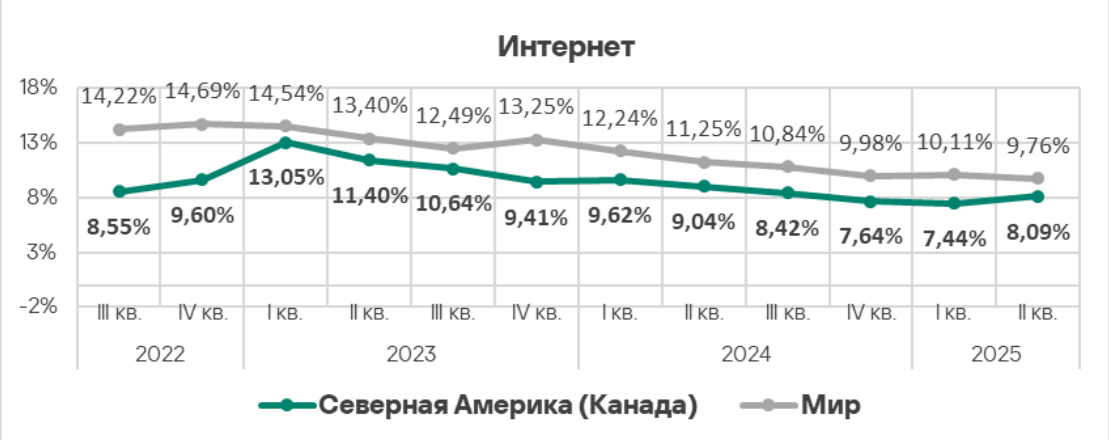
Во втором квартале 2025 года из всех источников угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась у интернета и почтовых клиентов. По росту показателя угроз из интернета Северная Америка (Канада) находится на втором месте среди регионов.



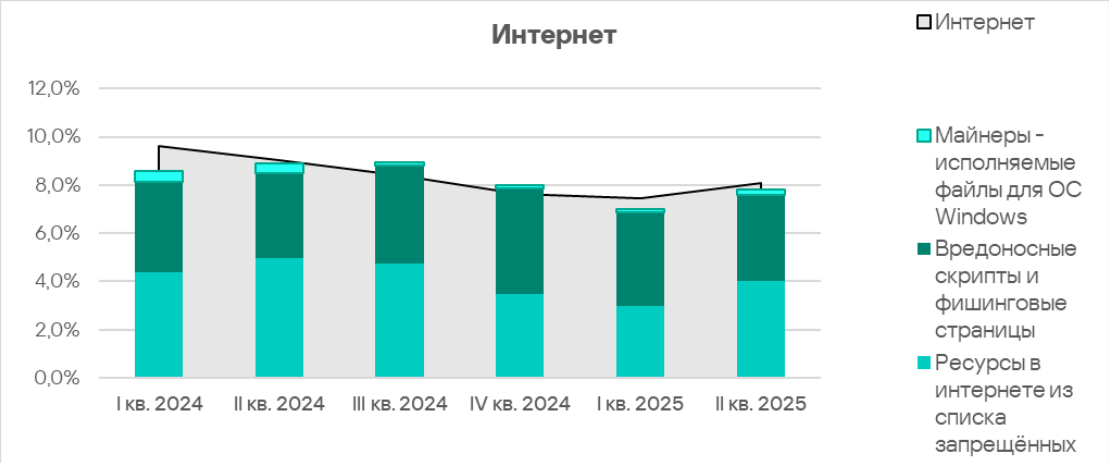
Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Северная Америка (Канада) занимает 11-е место с показателем 8,09%. Это выше минимального показателя регионов — у Восточной Азии — в 1,3 раза.

Во втором квартале 2025 доля интернет-угроз в регионе выросла, на фоне снижения среднемирового показателя, завершив последовательное снижение в течении предыдущих четырех кварталов.



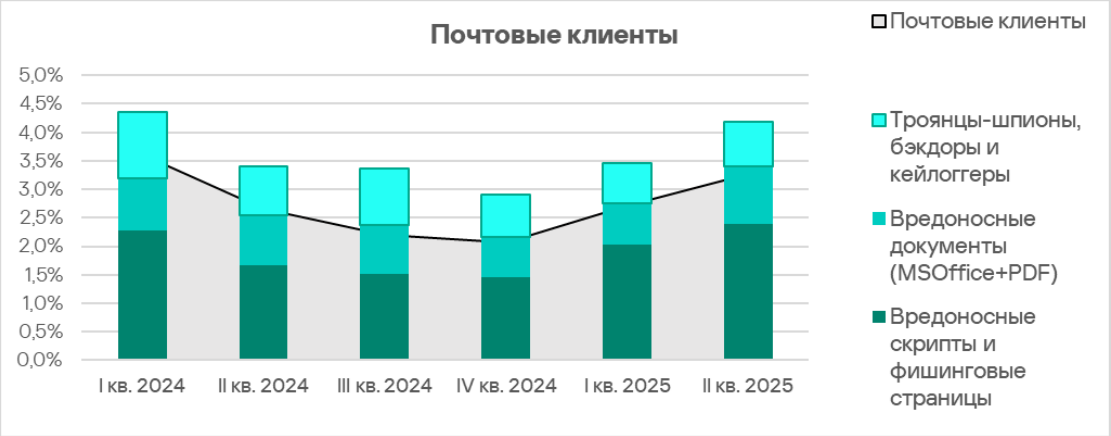
Основные категории угроз из интернета, блокируемые на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.



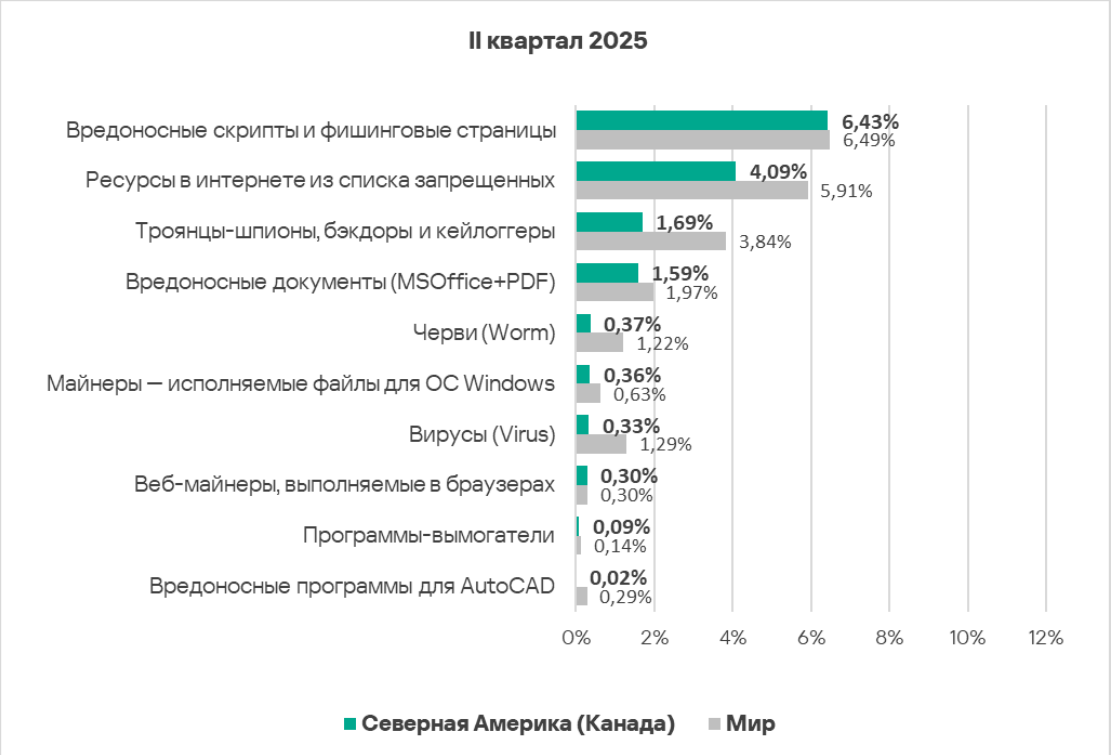
Почтовые клиенты

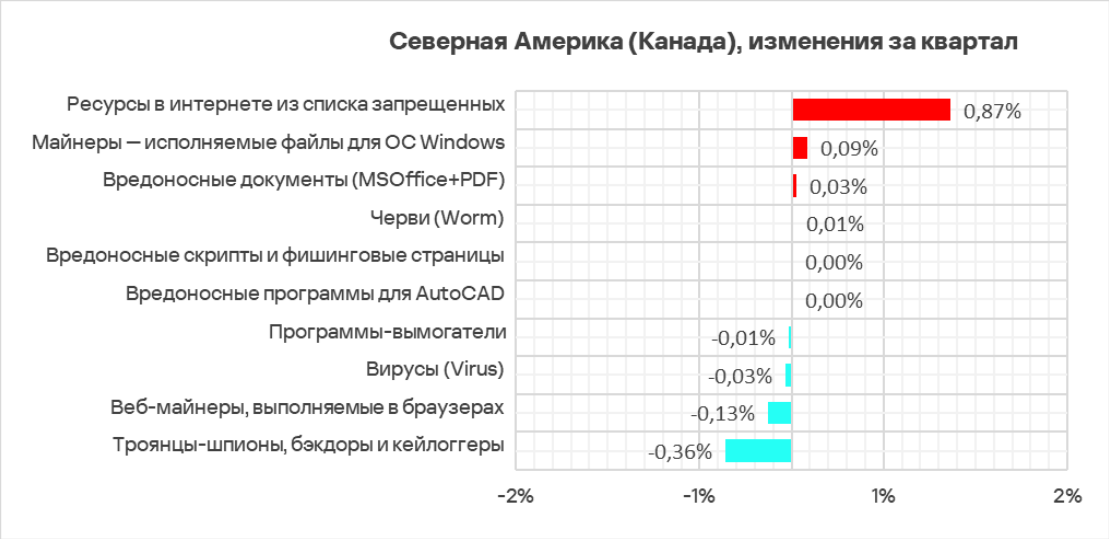
По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, во втором квартале 2025 года Северная Америка (Канада) занимает восьмое место с показателем 3,30%. Это в 4,1 раза больше, чем в России, которая замыкает соответствующий рейтинг.

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



Категории угроз





В Северной Америке (Канаде) среди категорий угроз все показатели ниже среднемировых.

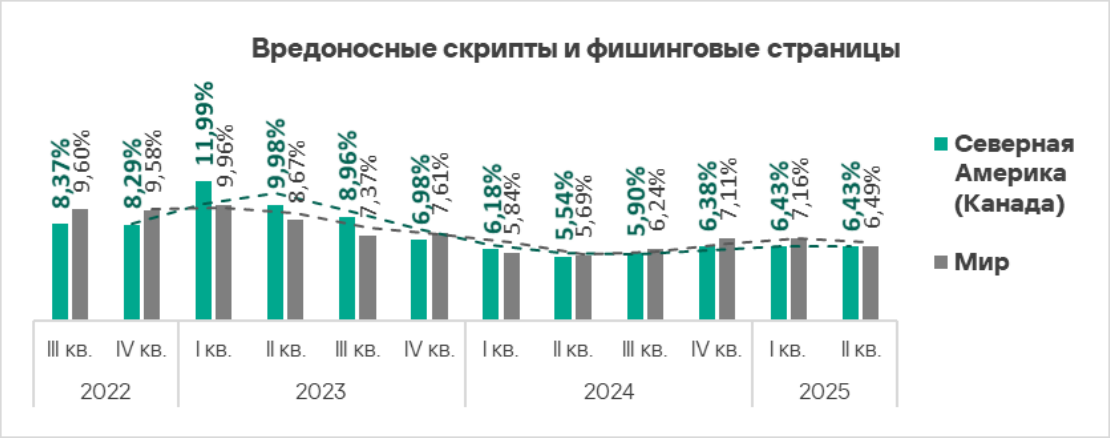
Рост за квартал в регионе наблюдался для угроз из четырех категорий, но существенное изменение можно отметить лишь для двух из них:

- ресурсы в интернете из списка запрещенных — в 1,3 раза;
- майнеры — исполняемые файлы — в 1,3 раза.

Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Северная Америка (Канада) занимает восьмое место с 6,43%. Этот показатель в 2,1 раза выше, чем в Северной Европе, где он наименьший из всех регионов.

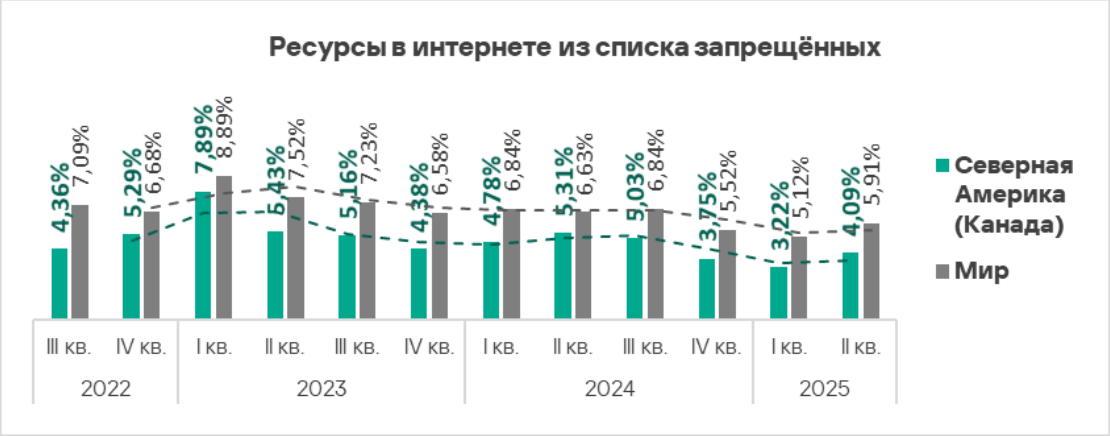
Во втором квартале 2025 года доля компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, уменьшилась во всех регионах, кроме двух — Северной Америки (Канады) и Австралии и Новой Зеландии.



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

Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Северная Америка (Канада) занимает третье с конца место в соответствующем рейтинге регионов с 4,09%. Однако по росту этого показателя регион оказался на седьмом месте — за квартал значение выросло в 1,3 раза.



Вредоносные документы

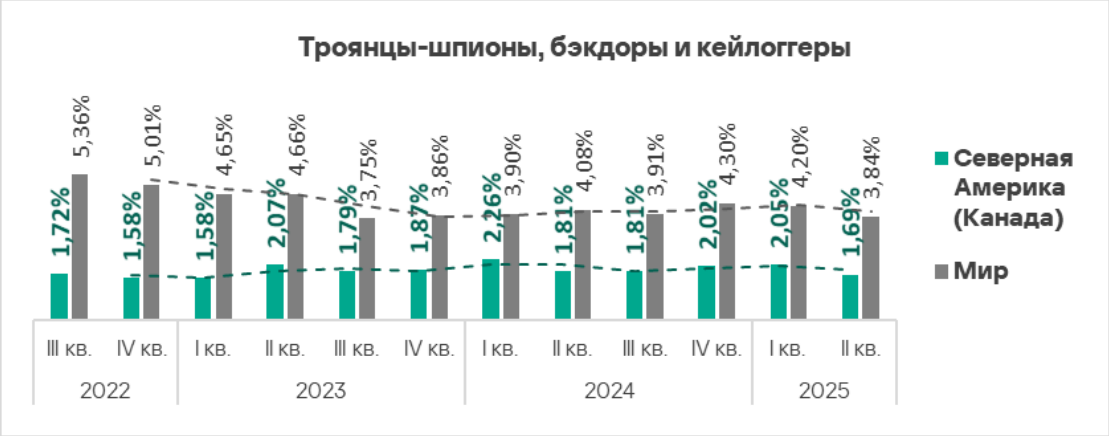
Северная Америка (Канада) занимает девятое место в рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы. Показатель в регионе — 1,59% — в 2,5 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых блокируются вредоносные документы, в регионе колеблется.

Распространяются вредоносные документы преимущественно по электронной почте.

Шпионские программы

По доле компьютеров АСУ, на которых блокируются шпионские программы, в соответствующем рейтинге регионов Северная Америка (Канада) находится на 12-м месте с 1,69%. Это в 1,2 раза больше, чем в Западной Европе, где значение наименьшее.

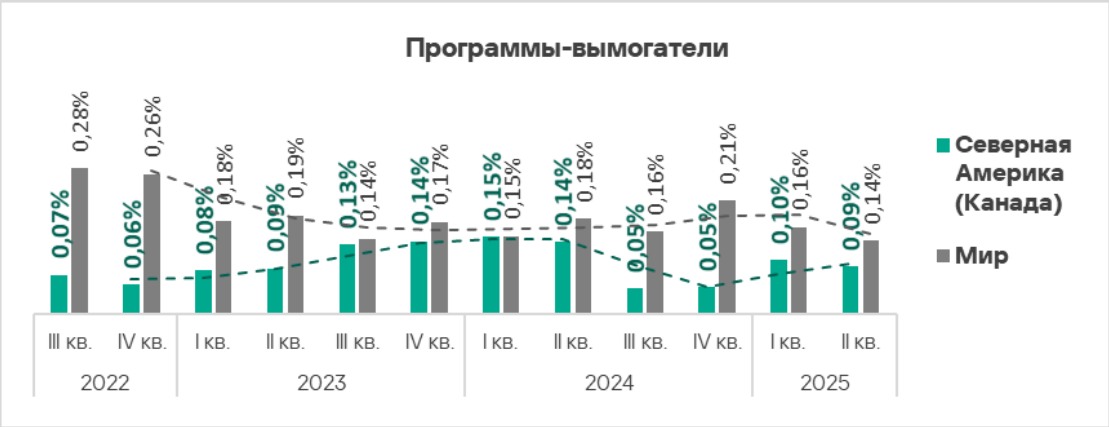


Шпионские программы в регионе блокируются во всех источниках угроз, преимущественно в почтовых клиентах.

Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Северная Америка (Канада) находится на предпоследнем, 13-м, месте с показателем 0,09%, который немногим больше, чем у замыкающей соответствующий рейтинг Западной Европы.

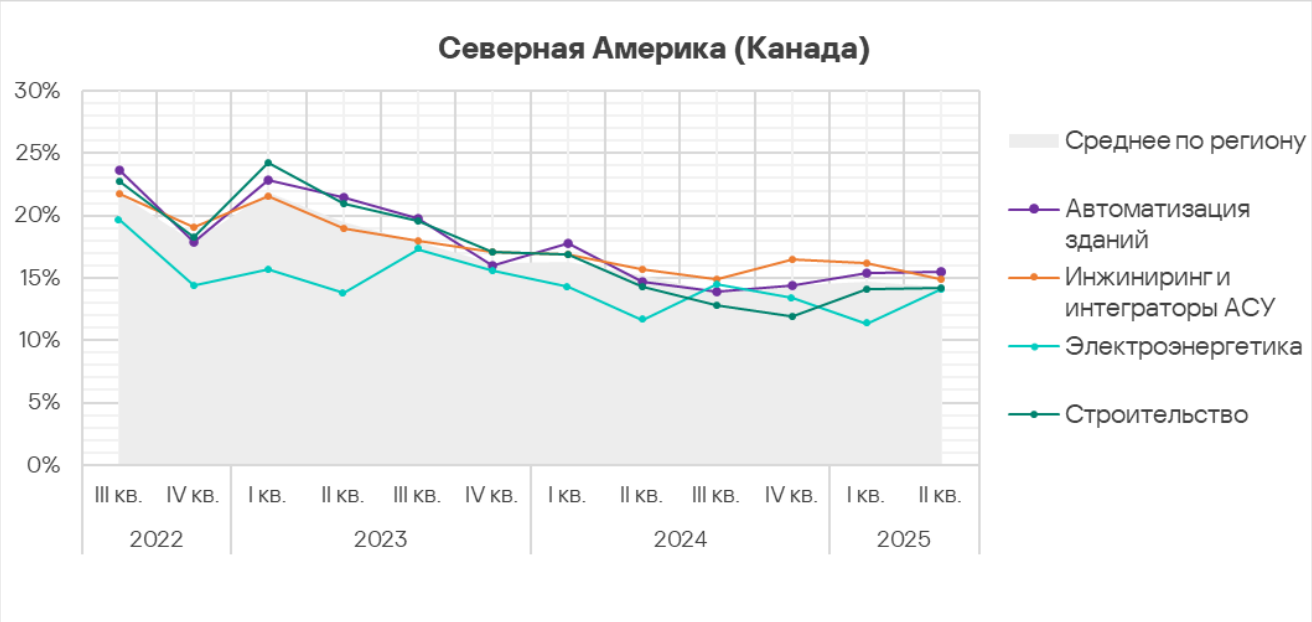
Показатель в регионе снова растет после заметного снижения во второй половине 2024 года.



Отрасли

Среди рассмотренных в отчете отраслей наибольшую долю компьютеров в Северной Америке (Канаде), на которых блокировались вредоносные объекты, представляет сектор производства.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, существенно увеличилась только в секторе электроэнергетики и снизилась в отрасли инжиниринг и интеграция АСУ. В остальных секторах заметных изменений не наблюдалось.



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 Америке (Канаде) значения, близкие к максимальным, наблюдаются для интернет-угроз в OT-инфраструктуре инжиниринг и интеграторы АСУ.

Показатели источников угроз в отраслях в Северной Америке (Канаде), II квартал 2025 года

Отрасль / Источник угрозы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Показатель категорий в регионе
Интернет	6,68%	8,59%	9,27%	7,50%	8,09%
Почтовые клиенты	6,59%	2,06%	2,11%	4,15%	3,26%
Съемные носители	0,00%	0,00%	0,08%	0,00%	0,03%
Сетевые папки	0,05%	0,00%	0,00%	0,00%	0,03%
Показатель отрасли в регионе	15,48%	14,09%	14,91%	14,23%	

Показатели категорий угроз в отраслях в Северной Америке (Канаде), II квартал 2025 года

Отрасль / Категории вредоносного ПО	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Строительство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	2,98%	5,84%	4,68%	3,57%	4,09%
Вредоносные скрипты и фишинговые страницы	8,80%	5,50%	6,54%	6,51%	6,43%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,29%	1,37%	1,16%	1,25%	1,69%
Черви (Worm)	0,63%	0,34%	0,25%	0,36%	0,37%
Майнеры — исполняемые файлы для ОС Windows	0,18%	0,69%	0,48%	0,27%	0,36%
Вредоносные документы (MSOffice+PDF)	3,29%	0,69%	1,21%	1,34%	1,59%
Вирусы (Virus)	0,50%	0,69%	0,11%	0,45%	0,33%
Программы-вымогатели	0,23%		0,03%	0,09%	0,09%
Веб-майнеры, выполняемые в браузерах	0,18%	0,34%	0,39%	0,27%	0,30%
Вредоносные программы для AutoCAD			0,03%		0,02%
Показатель отрасли в регионе	15,48%	14,09%	14,91%	14,23%	

«Горячие точки» отраслей

Автоматизация зданий

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

Инжиниринг и интеграторы АСУ

- Первое место в регионе среди отраслей по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и на съемных носителях.
- Первое место среди отраслей в регионе по доле веб-майнеров.
- Второе место в регионе среди отраслей по показателю следующих категорий угроз: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных, майнеры — исполняемые файлы.

Электроэнергетика

- Первое место среди отраслей региона по показателю следующих категорий угроз: ресурсы в интернете из списка запрещенных, вирусы, майнеры — исполняемые файлы.
- Второе место среди отраслей региона по показателям шпионских программ и веб-майнеров.

Строительство

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

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