

# Ландшафт угроз для систем промышленной автоматизации

Южная и Северная Америка (Канада)

Четвертый квартал 2025 года

Южная Америка.....	4
Основные проблемы кибербезопасности в регионе .....	4
Статистика по всем угрозам.....	5
Источники угроз.....	7
Интернет.....	8
Почтовые клиенты .....	9
Съемные носители .....	11
Категории угроз .....	13
Вредоносные скрипты и фишинговые страницы .....	14
Вредоносные документы.....	16
Шпионские программы .....	18
Веб-майнеры .....	19
Черви .....	21
Отрасли.....	22
Источники и категории вредоносного ПО в отраслях: «горячие точки» .....	25
Особенности региона.....	26
Северная Америка (Канада).....	32
Основные проблемы кибербезопасности в регионе .....	32
Статистика по всем угрозам.....	32
Источники угроз.....	33
Интернет.....	34
Почтовые клиенты .....	35
Съемные носители .....	36
Сетевые папки.....	37
Категории угроз .....	38
Вредоносные скрипты и фишинговые страницы .....	39
Ресурсы в интернете из списка запрещенных .....	40
Шпионские программы .....	41
Вредоносные документы.....	41
Вирусы.....	42
Программы-вымогатели.....	43
Вредоносные программы для AutoCAD.....	43

Отрасли..... 44

Источники и категории вредоносного ПО в отраслях: «горячие точки» ..... 46

Методика подготовки статистики..... 50

# 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 1,9 раза. По этому показателю регион занимает второе место в мире.

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

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

По показателям угроз категорий вредоносные документы, вредоносные скрипты и фишинговые страницы Южная Америка находится на втором месте в соответствующих рейтингах регионов.

### Высокий показатель вредоносных документов

По доле компьютеров АСУ, на которых блокируются вредоносные документы, в четвертом квартале 2025 года Южная Америка на втором месте среди регионов. Показатель в регионе превышает среднемировой в 1,8 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.

### Высокий показатель вредоносных скриптов и фишинговых страниц

По доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы, Южная Америка среди регионов занимает второе место с показателем, который в 1,5 раза превышает среднемировой.

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 были заблокированы шпионские программы, Южная Америка находится на седьмом месте среди регионов. В региональном рейтинге категорий угроз шпионские программы занимают второе место.

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.

Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели.

### **Угрозы в отраслях**

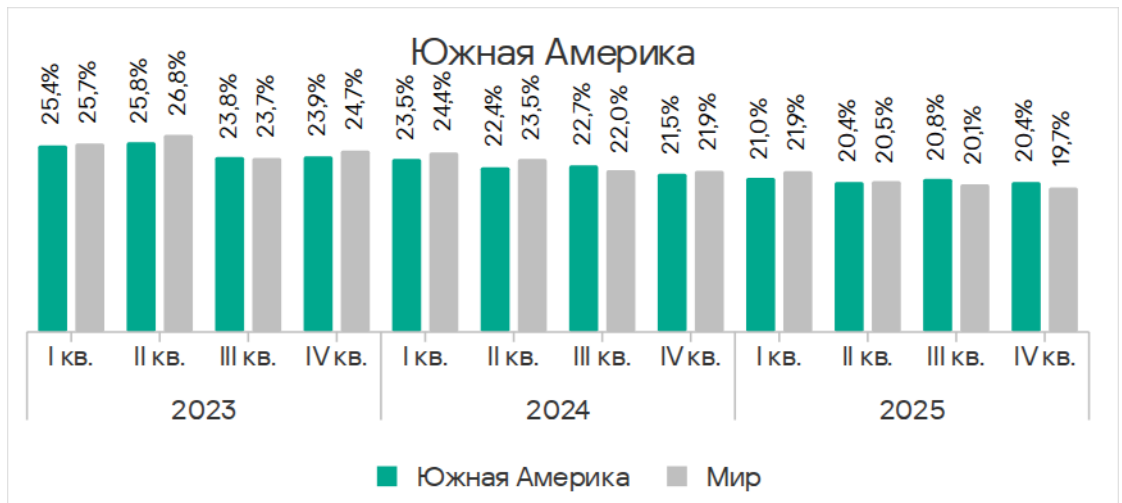
В рейтингах регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, Южная Америка попадает в топ-3 по показателям во всех отраслях, кроме производства. По показателям в нефтегазовой отрасли регион лидирует.

В большинстве отраслей также высокие показатели вредоносных документов. По этому показателю в нефтегазовой отрасли Южная Америка лидирует среди регионов.

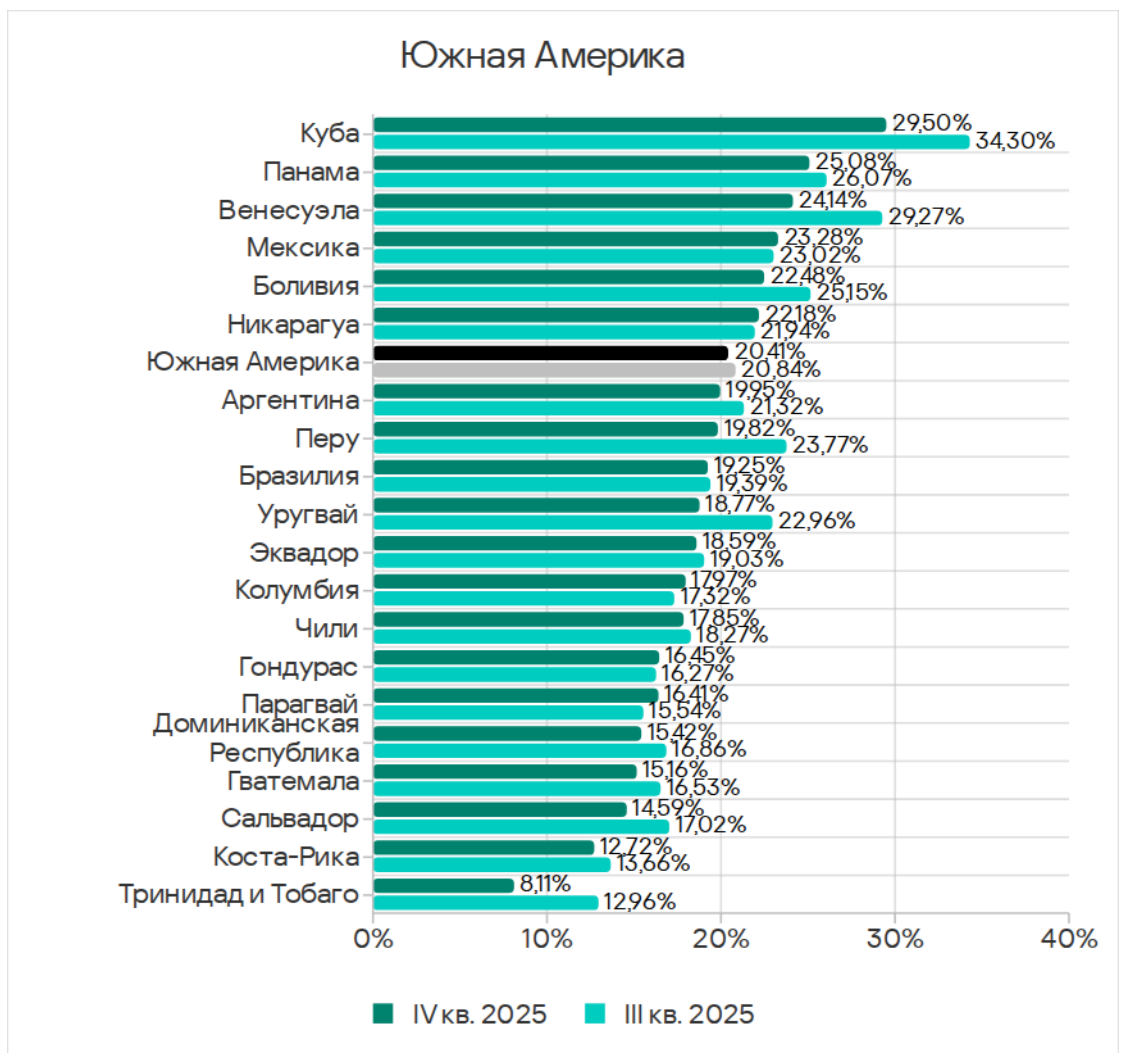
## **Статистика по всем угрозам**

Южная Америка в четвертом квартале 2025 года занимает шестое место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, с 20,4%. Это в 2,4 раза больше, чем в Северной Европе, где значение наименьшее из всех регионов.

В Южной Америке наблюдается нисходящий тренд. В четвертом квартале 2025 года после роста показателя в предшествующем квартале, доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, вернулась к значению второго квартала 2025 года.



Среди стран региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 8,11% в Тринидаде и Тобаго до 29,50% на Кубе.



## Источники угроз

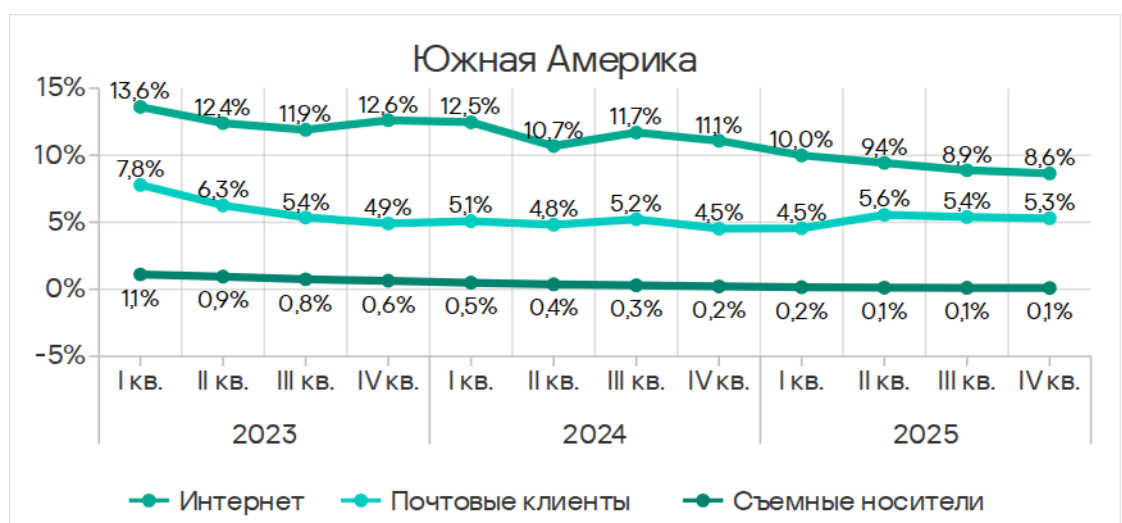
Вредоносные объекты в регионе распространяются преимущественно через интернет и почту.



В четвертом квартале 2025 года по сравнению с мировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы угрозы из следующих источников:

- интернет – в 1,1 раза;
- почтовые клиенты – в 1,9 раза.

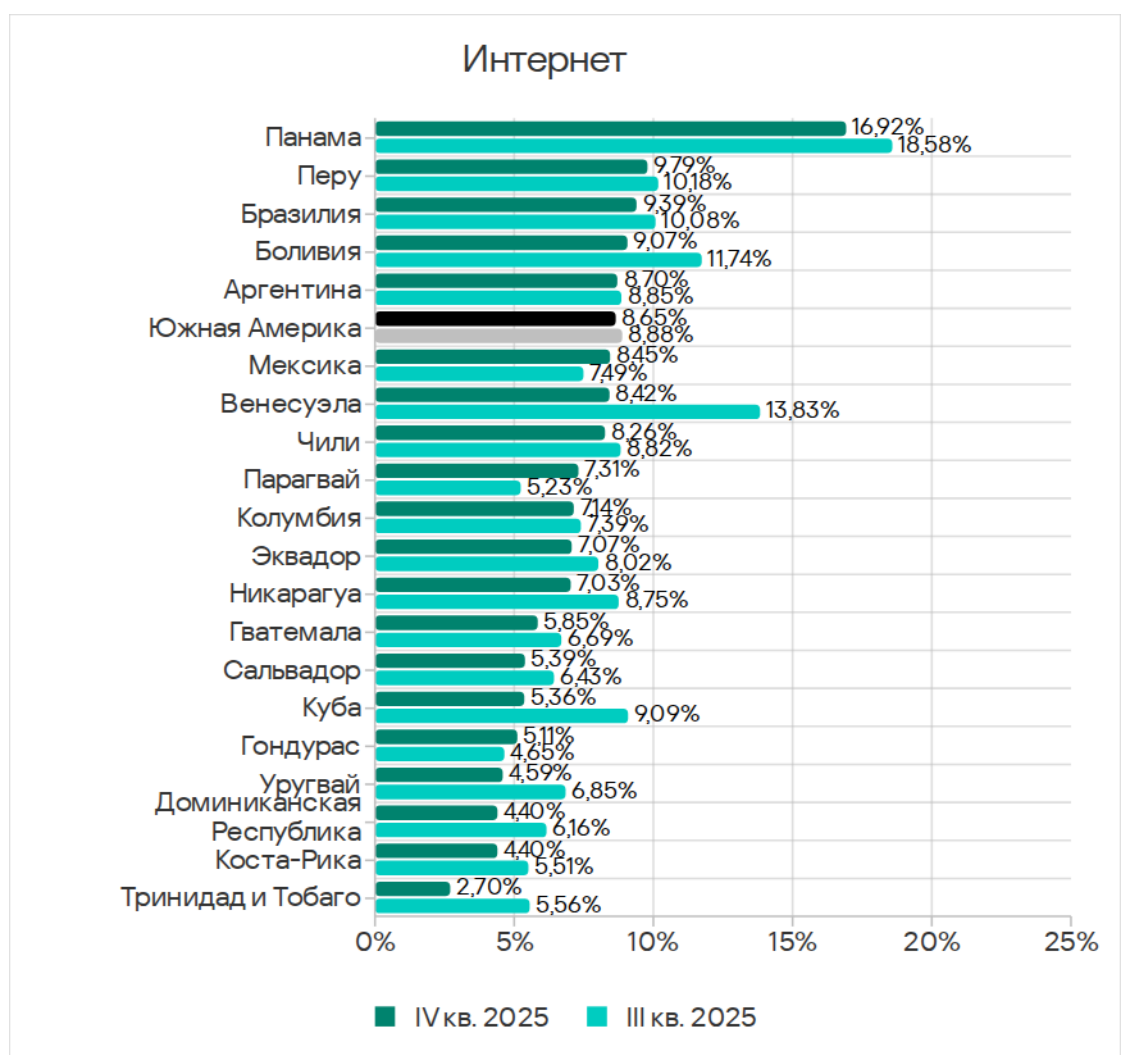
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась у всех источников угроз.



## Интернет

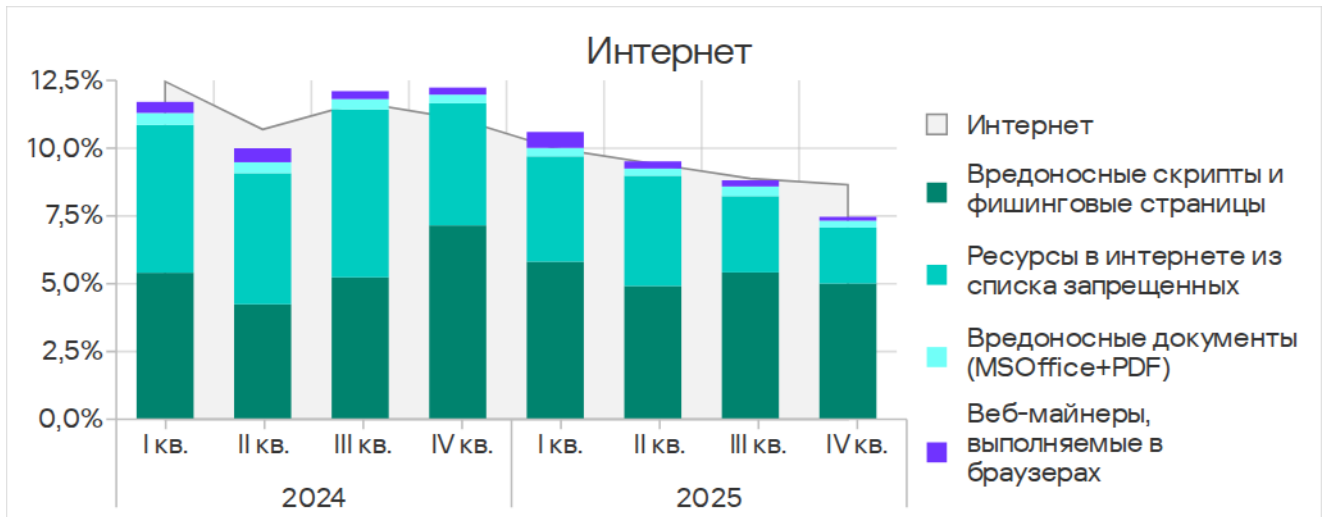
В четвертом квартале 2025 года в рейтинге регионов по доле компьютеров АСУ, на которых блокировались угрозы из интернета, Южная Америка находится на четвертом месте с 8,65%. Показатель в регионе в 2,2 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Показатели стран региона варьируют от 2,70% в Тринидаде и Тобаго до 16,92% в Панаме.



В предыдущем квартале в Панаме показатель вырос в 2,4 раза из-за всплеска блокировок угрозы категории вредоносные скрипты и фишинговые страницы при попытке доступа к зараженным веб-сайтам. Хотя показатель в Панаме в четвертом квартале уменьшился, к прежним значениям он так и не вернулся.

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



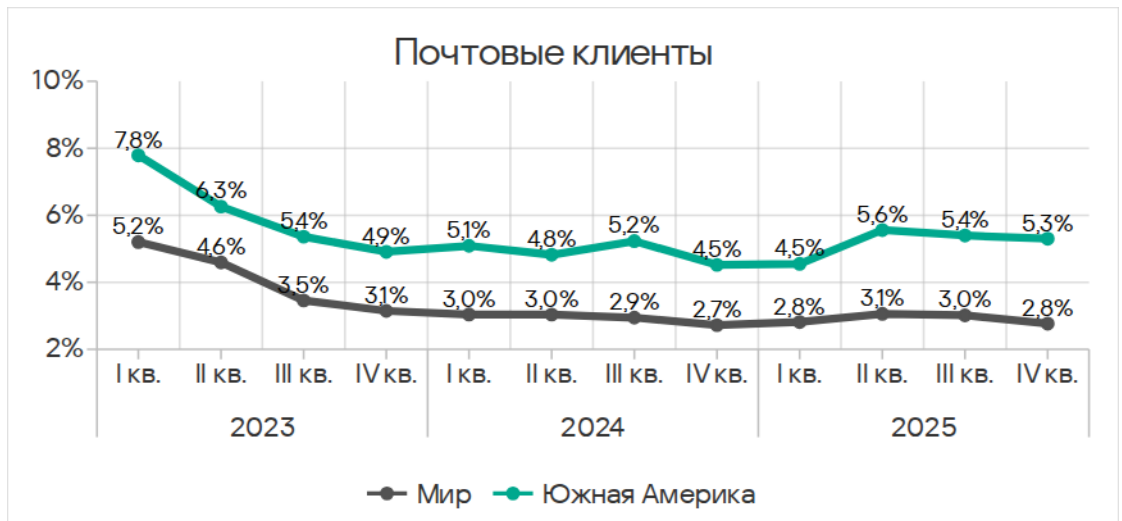
## Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в четвертом квартале 2025 года Южная Америка в соответствующем рейтинге регионов поднялась с третьего на второе место, уступая только Южной Европе.

Высокий показатель угроз из почтовых клиентов совместно с высоким показателем вредоносных скриптов и фишинговых страниц свидетельствует о высокой доступности систем, относящихся к ОТ-инфраструктуре, для целевых атак.

Показатель Южной Америки – 5,30% – в 8,3 раза выше, чем в Северной Европе, которая замыкает этот рейтинг.

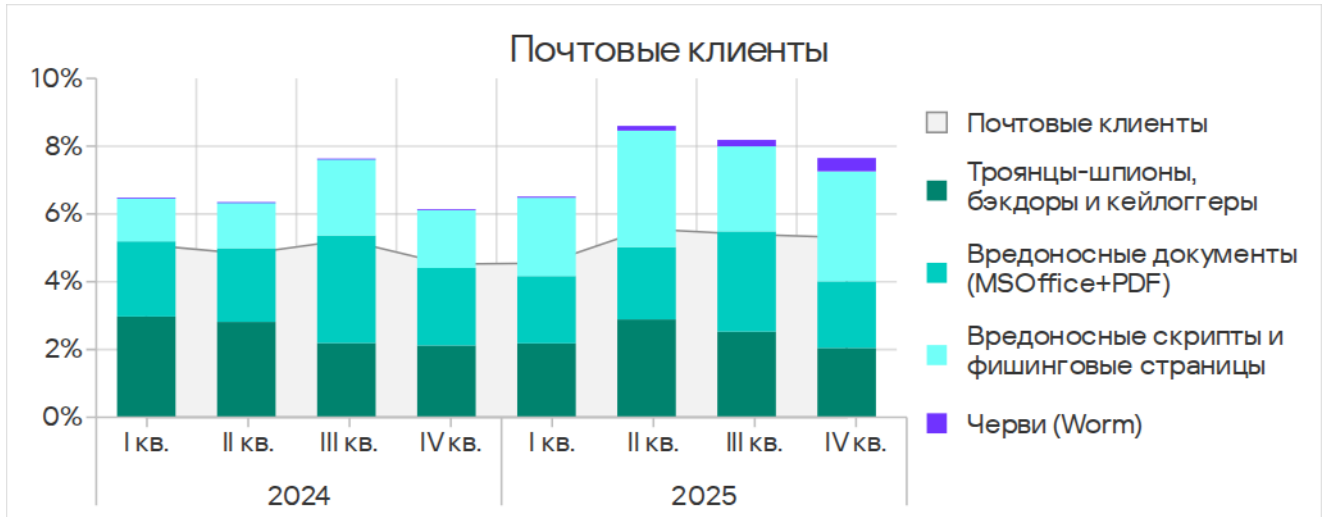
Показатель угроз из почтовых клиентов в регионе колеблется. Во втором – четвертом кварталах 2025 года значение было выше, чем в предыдущие полтора года.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, с отрывом лидируют Мексика с 9,51% и Уругвай с 8,56%. Показатели остальных стран варьируют от 1,35% в Тринидаде и Тобаго до 5,68% в Доминиканской республике.



Основные категории угроз из почтовых клиентов, которые были заблокированы на компьютерах АСУ: вредоносные скрипты и фишинговые страницы, шпионские программы и вредоносные документы.



В четвертом квартале 2025 года заметно увеличилась доля компьютеров АСУ, на которых были заблокированы черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, в ходе которых были атакованы все регионы мира. В Южной Америке пик атаки пришелся на октябрь.

Злоумышленники рассылали фишинговые письма, замаскированные под отклики на вакансии. Под видом резюме (Curriculum Vitae) такие письма содержали вредоносный исполняемый файл (червь-бэкдор для удаленного управления Backdoor.MSIL.XWorm). При запуске файла происходило заражение системы.

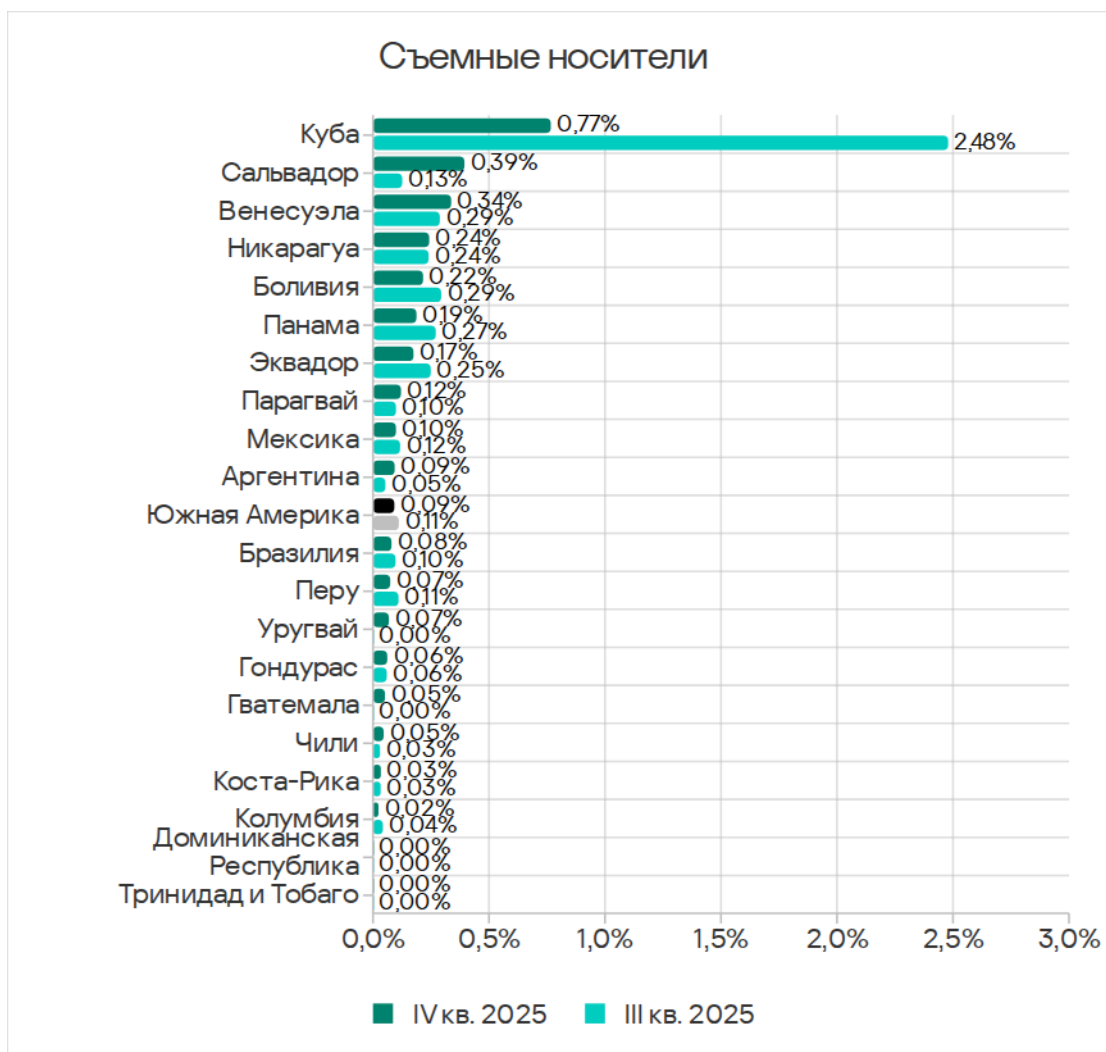
Как правило такие кампании направлены на доставку вредоносного ПО для кражи данных, программ-шпионов или инструментов для удаленного управления (RAT).

Страны-лидеры рейтинга по почтовым клиентам — Мексика и Уругвай — также занимают верхние строчки в рейтингах по показателям шпионских программ и вредоносных документов.

## Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, в четвертом квартале 2025 года Южная Америка занимает 10-е место среди регионов — с 0,09%. Это в 1,8 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.

Среди стран региона по доле компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, лидирует Куба с 0,77%.

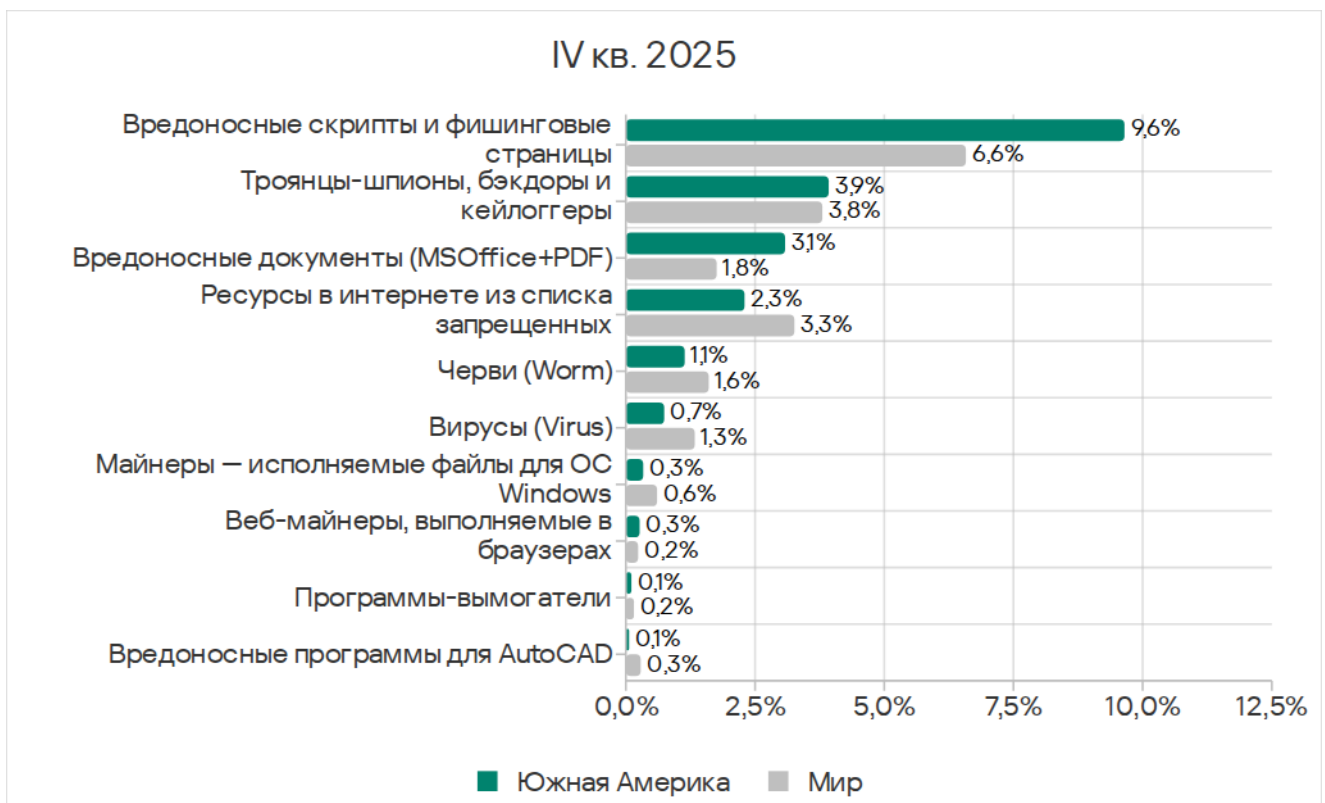


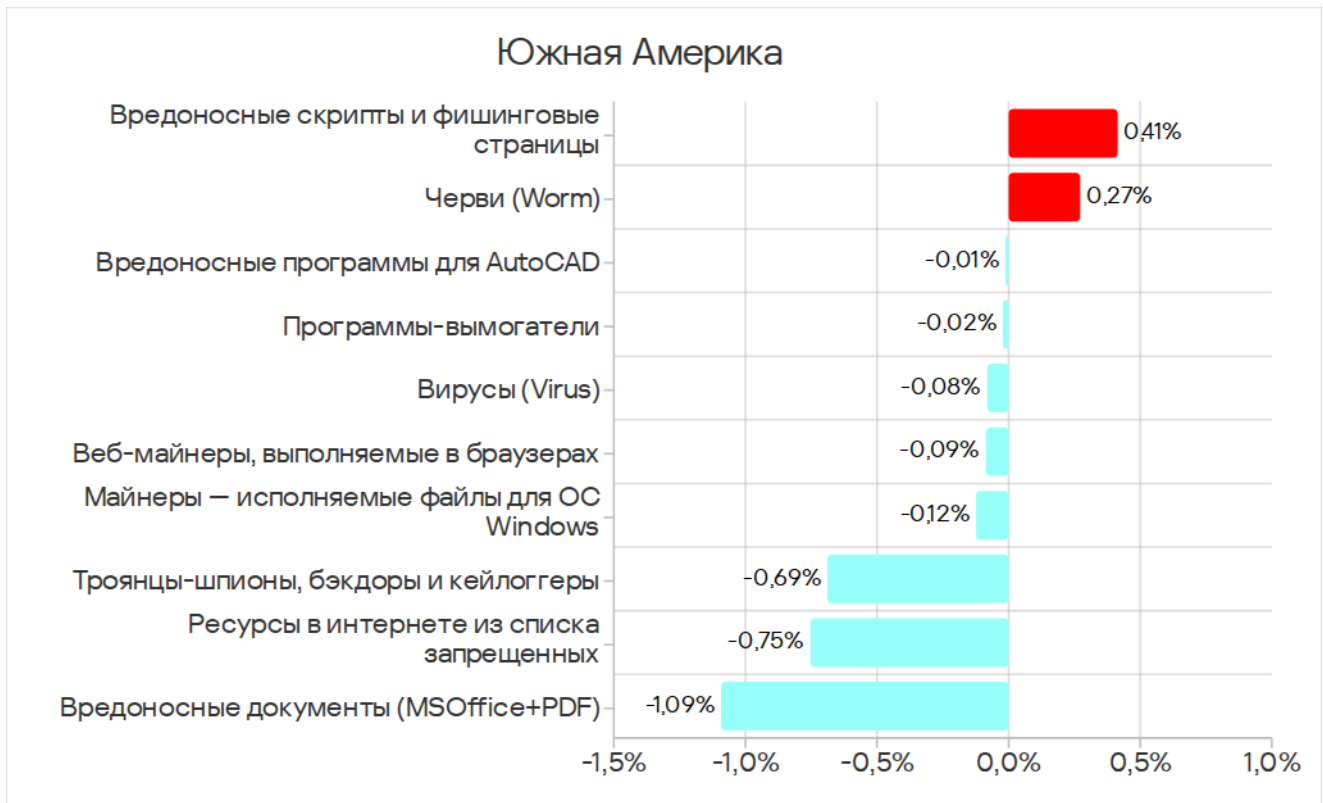
Основные категории угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ: черви, вирусы и шпионское ПО.



## Категории угроз

В региональном рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы, на втором и третьем местах находятся угрозы, которые распространяются преимущественно через почтовые клиенты: шпионское ПО и вредоносные документы. Вредоносные скрипты, которые возглавляют этот рейтинг, распространяются и в интернете, и по электронной почте.





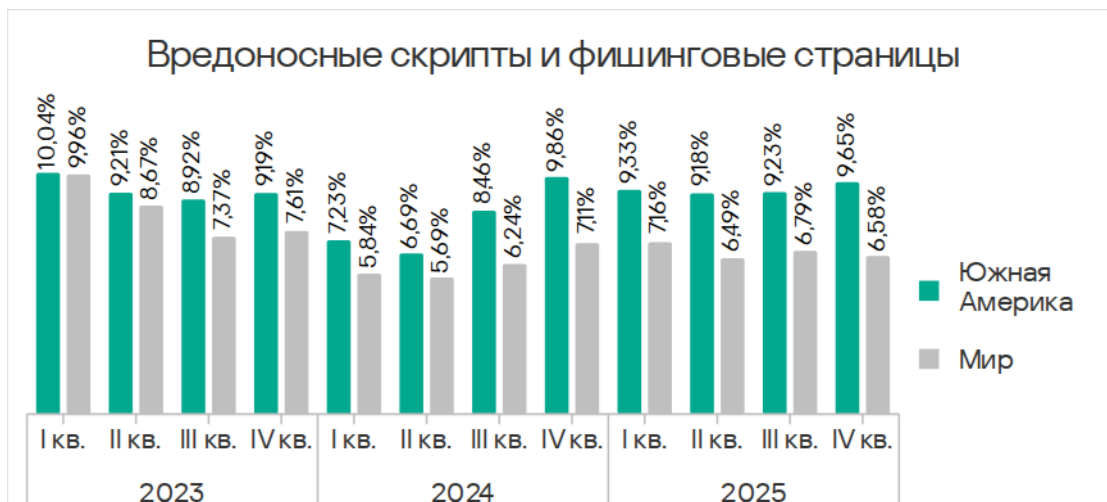
По сравнению с мировыми показателями в регионе выше доля компьютеров АСУ, на которых были заблокированы следующие категории угроз:

- вредоносные документы — в 1,8 раза, второе место среди регионов по доле компьютеров АСУ, на которых была заблокирована угроза;
- вредоносные скрипты и фишинговые страницы — в 1,5 раза, второе место среди регионов по доле компьютеров АСУ, на которых была заблокирована угроза, и по росту показателя;
- веб-майнеры — в 1,1 раза, второе место среди регионов;
- шпионские программы.

## Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, Южная Америка находится на втором месте в соответствующем рейтинге регионов с 9,65%. Это в 3,8 раза больше, чем в Северной Европе, где этот показатель — наименьший среди регионов.

Показатель в регионе растет второй квартал подряд и оказался самым высоким за 2025 год. Из четырех регионов, где значение за квартал увеличилось, Южная Америка занимает второе место по его росту.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, с отрывом от остальных лидирует Панама с 18,24%. В прошлом квартале показатель этой страны резко вырос в связи с попытками заражения популярных сайтов на движке WordPress, в частности – сайтов правительственных организаций. В четвертом квартале к прежнему уровню значение так и не вернулось.

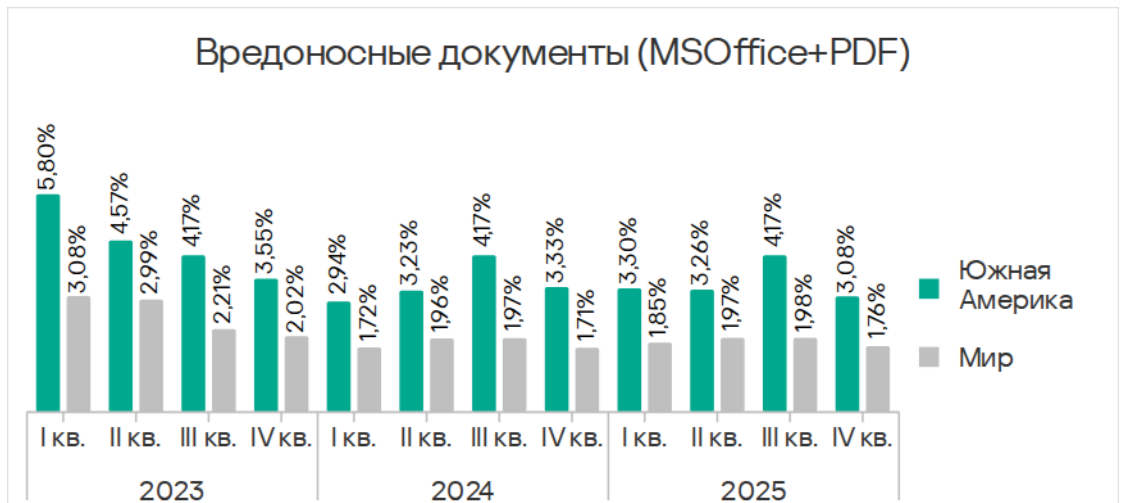


Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

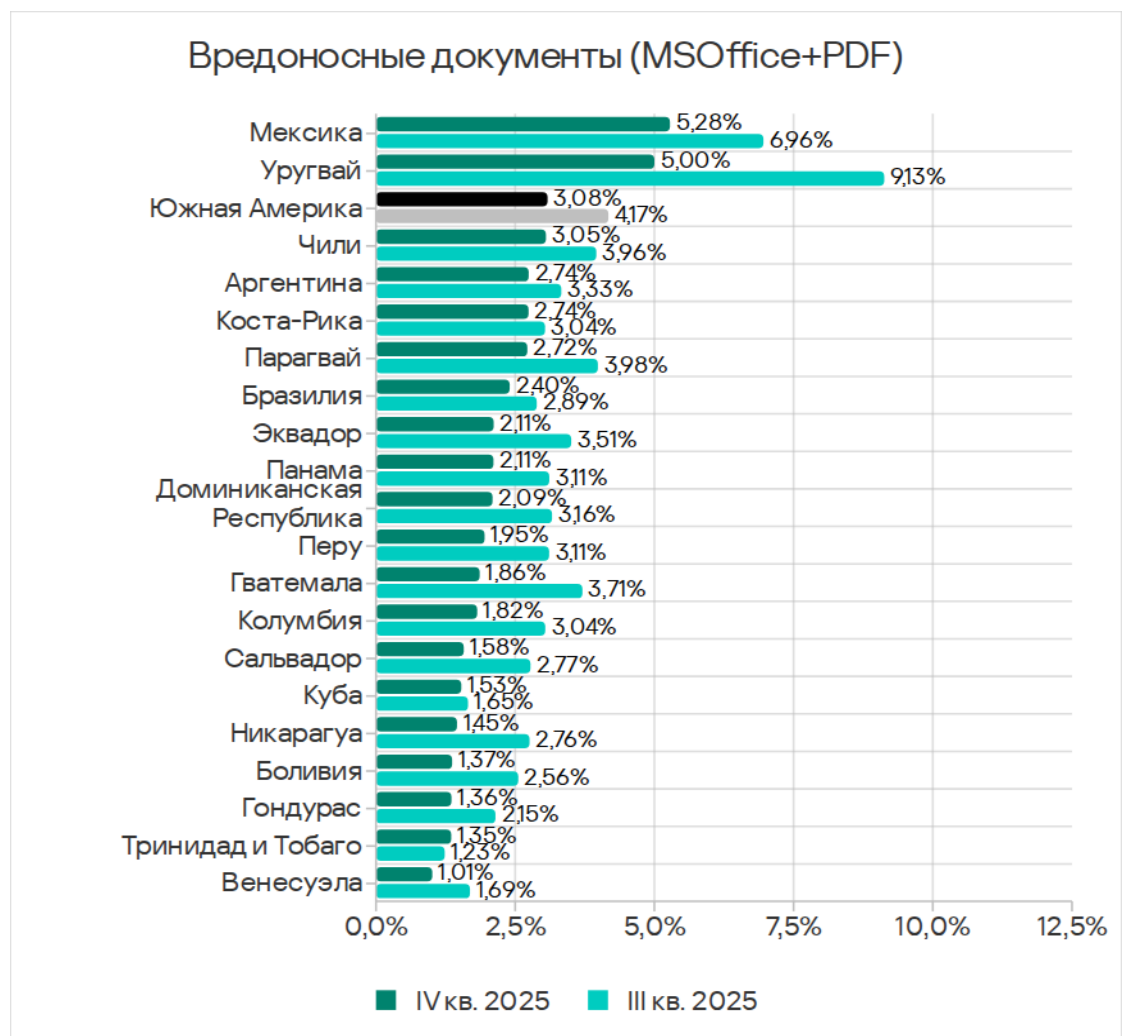
## Вредоносные документы

Южная Америка занимает второе место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, с 3,08%. Это в 6,7 раза больше, чем в Северной Европе, которая замыкает этот рейтинг.

Показатель в регионе колеблется, в четвертом квартале он уменьшился.



Среди стран региона по доле компьютеров АСУ, на которых блокируются вредоносные документы, с отрывом от остальных лидируют Мексика с 5,28% и Уругвай с 5,00%. После роста в предыдущем квартале показатель уменьшился во всех странах.

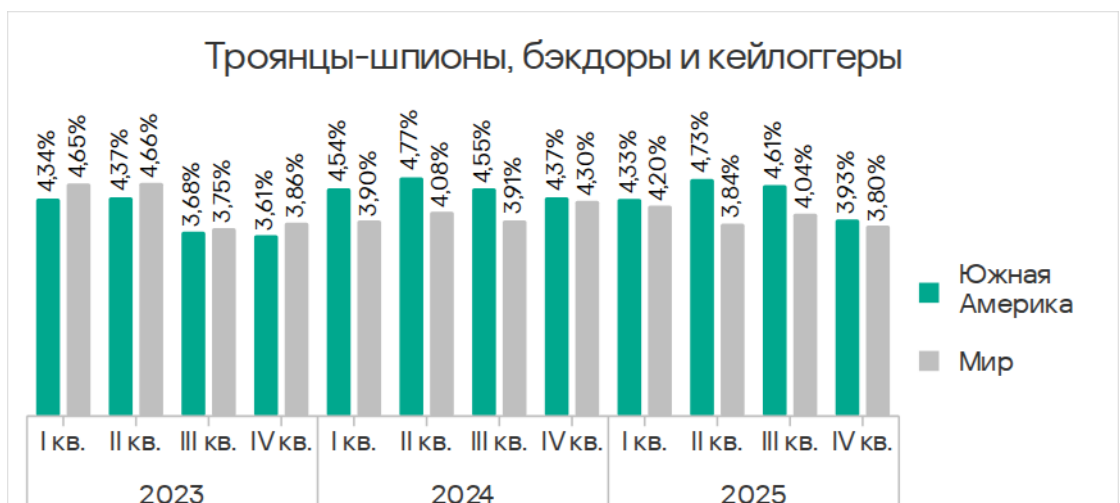


Вредоносные документы распространяются преимущественно по электронной почте. Мексика и Уругвай возглавляют также рейтинг стран региона по доле компьютеров АСУ, где угрозы были заблокированы в почтовых клиентах.

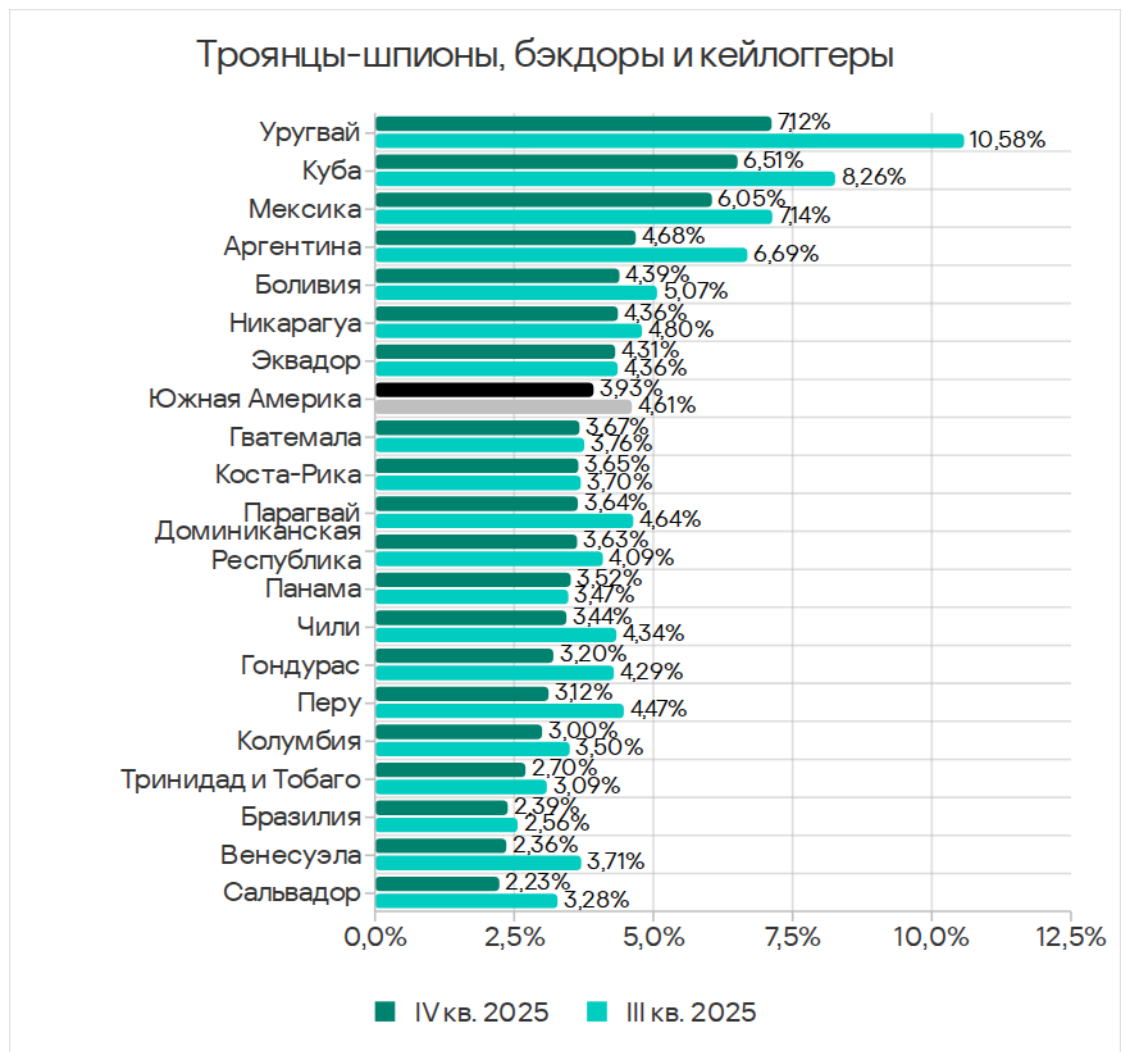
## Шпионские программы

По доле компьютеров АСУ, на которых были заблокированы шпионские программы, в соответствующем рейтинге регионов Южная Америка находится на седьмом месте с 3,93%. Это в 3,1 раза больше, чем в Северной Европе, где этот показатель наименьший.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в Южной Америке колеблется, в третьем и четвертом кварталах 2025 года этот показатель уменьшался.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы шпионские программы, лидирует Уругвай с 7,12%. Наименьший показатель – в Сальвадоре (2,23%). Значения уменьшились во всех странах, кроме Панамы.

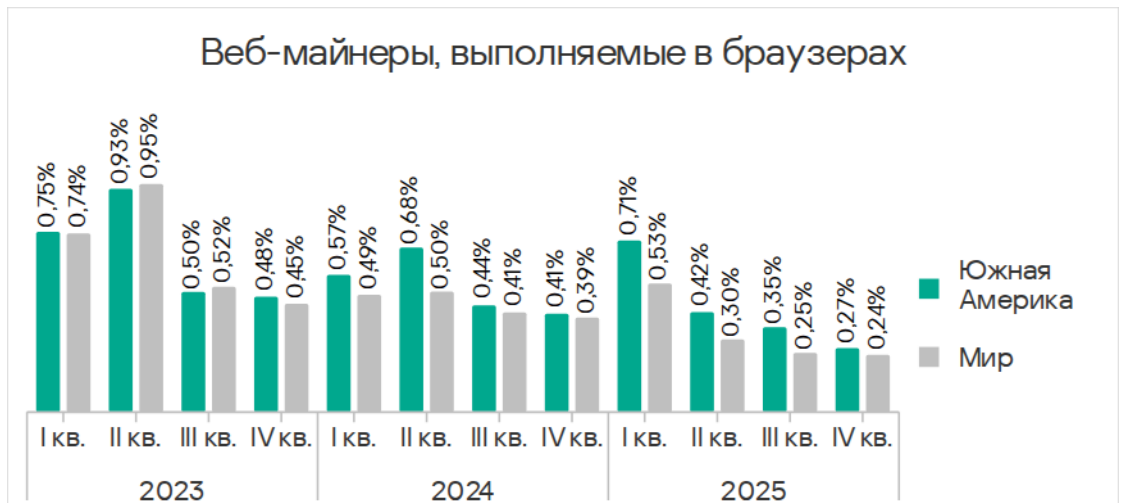


Шпионские программы в регионе блокируются преимущественно в почтовых клиентах. Уругвай и Мексика, лидирующие в рейтинге по показателю шпионских программ, оказались в числе лидеров и по угрозам из почтовых клиентов.

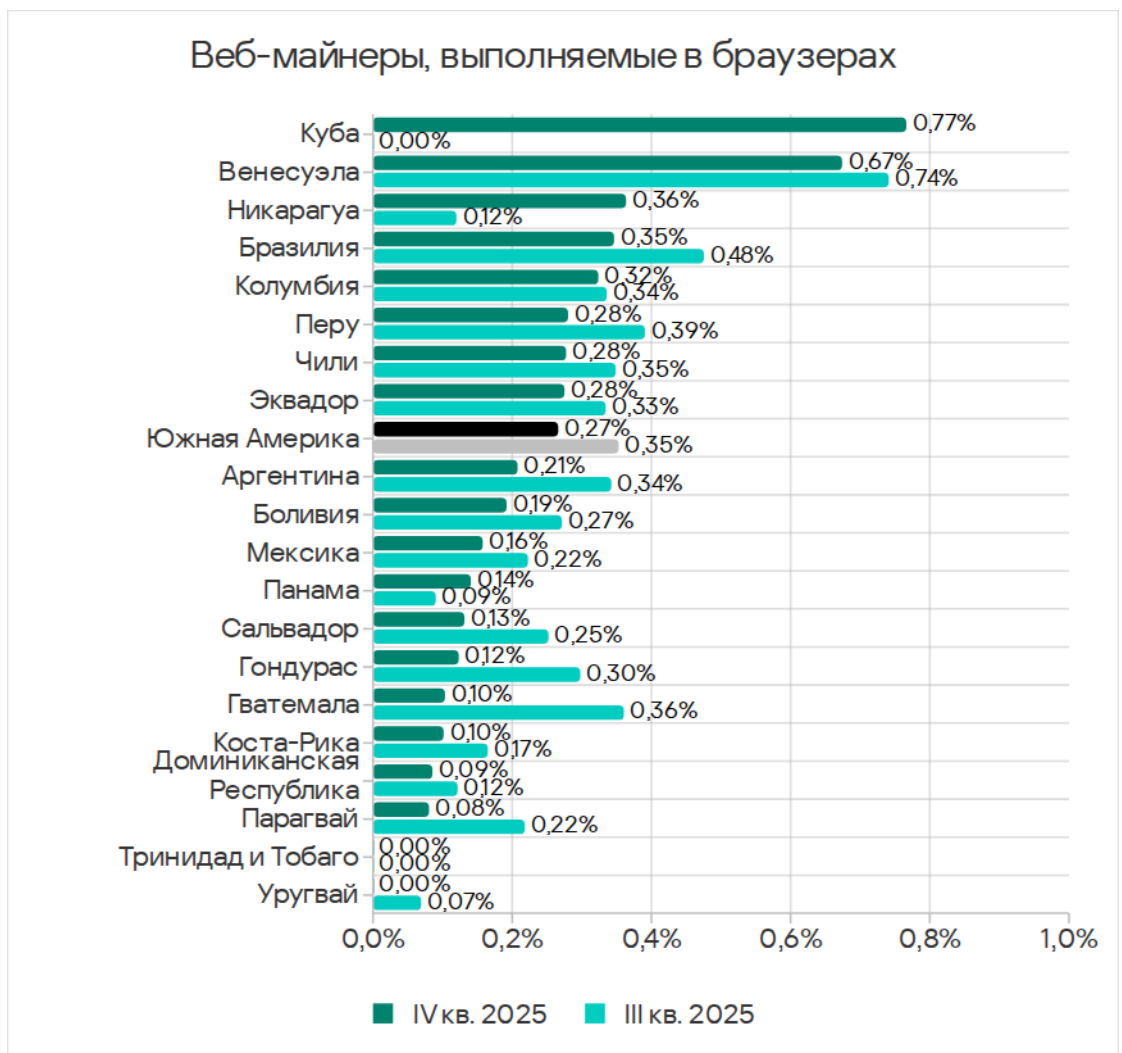
## Веб-майнеры

По доле компьютеров АСУ, на которых были заблокированы веб-майнеры, в четвертом квартале 2025 года Южная Америка занимает второе место среди регионов – с 0,27%. Это в 4,5 раза больше, чем в Восточной Азии, которая замыкает соответствующий рейтинг.

Показатель веб-майнеров в регионе уменьшается третий квартал подряд и в четвертом квартале 2025 года он оказался наименьшим за три года.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, с отрывом лидируют Куба с 0,77% и Венесуэла с 0,67%.

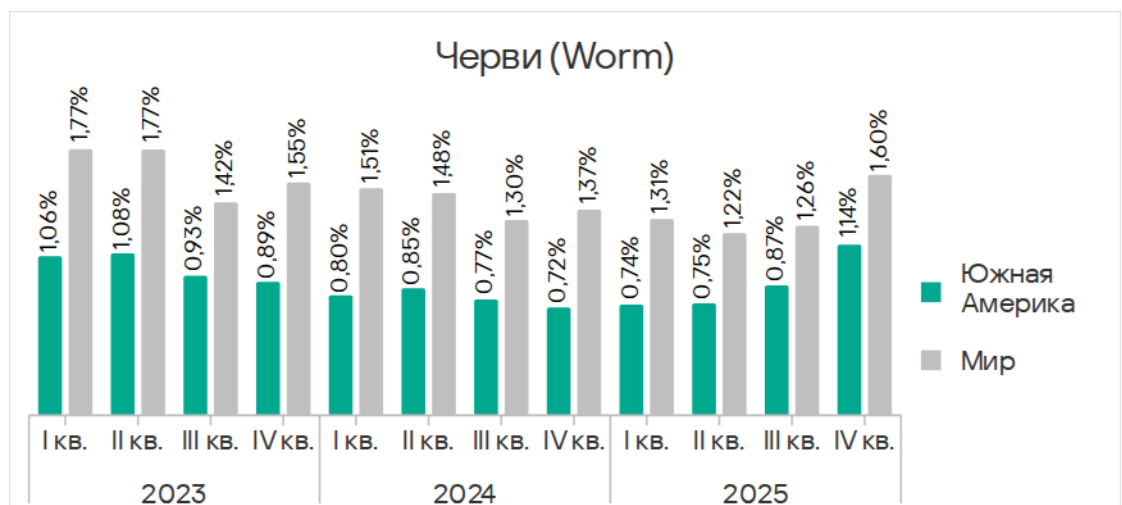


## Черви

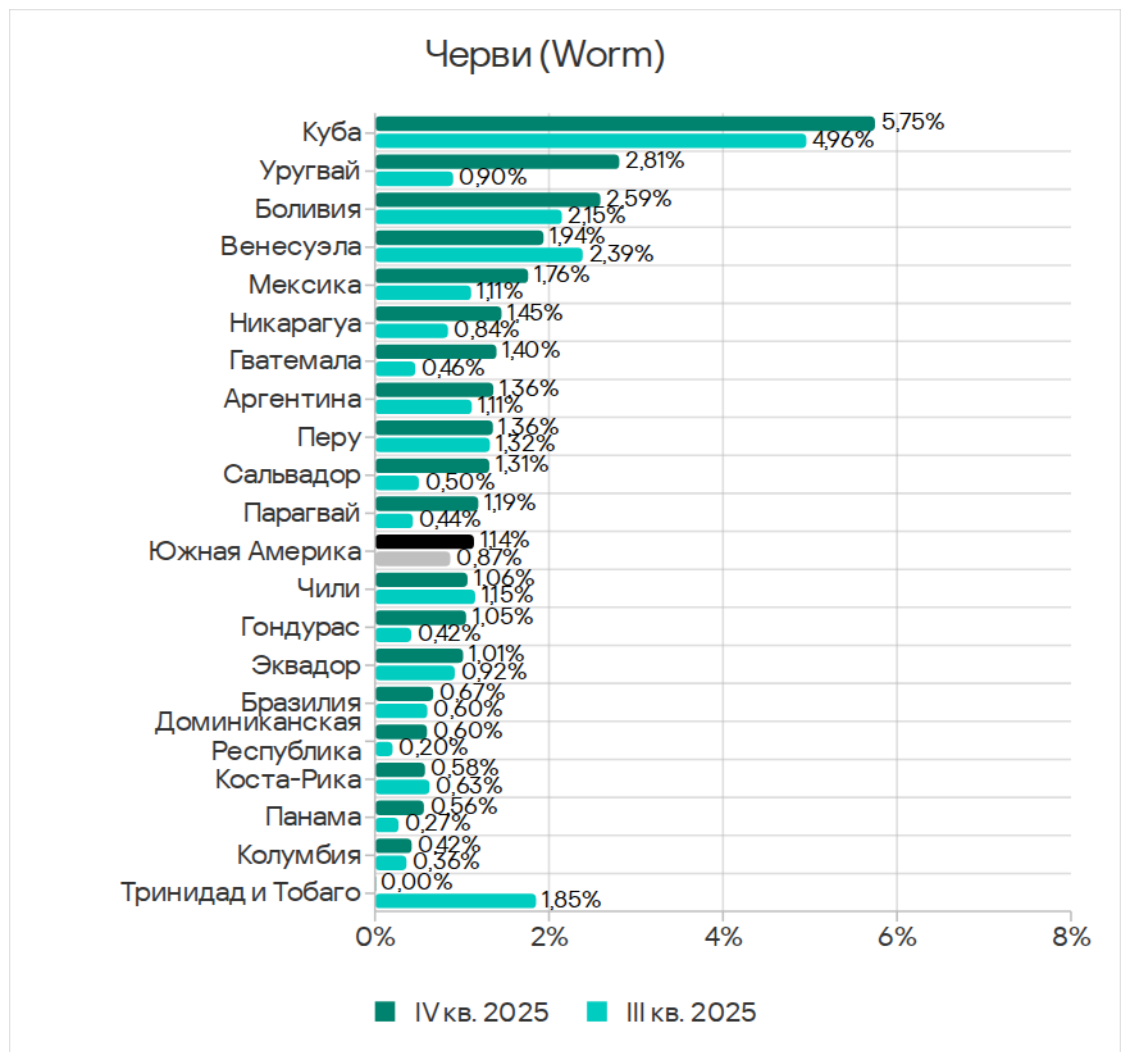
По доле компьютеров АСУ, на которых были заблокированы черви, Южная Америка занимает девятое место среди регионов.

В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие очередной волны фишинговых кампаний, известных как Curriculum-vitae-catalina, о которых мы рассказывали выше.

В Южной Америке показатель вырос до 1,14%. Это в 3,6 раза больше, чем в Северной Европе, где значение – наименьшее среди всех регионов.



Среди стран региона по доле компьютеров АСУ, на которых были заблокированы черви, с большим отрывом лидирует Куба с 5,75%. В Уругвае показатель за квартал увеличился в 3,1 раза. Значение выросло во всех странах региона, кроме Венесуэлы, Чили, Коста-Рики, Тринидада и Тобаго.

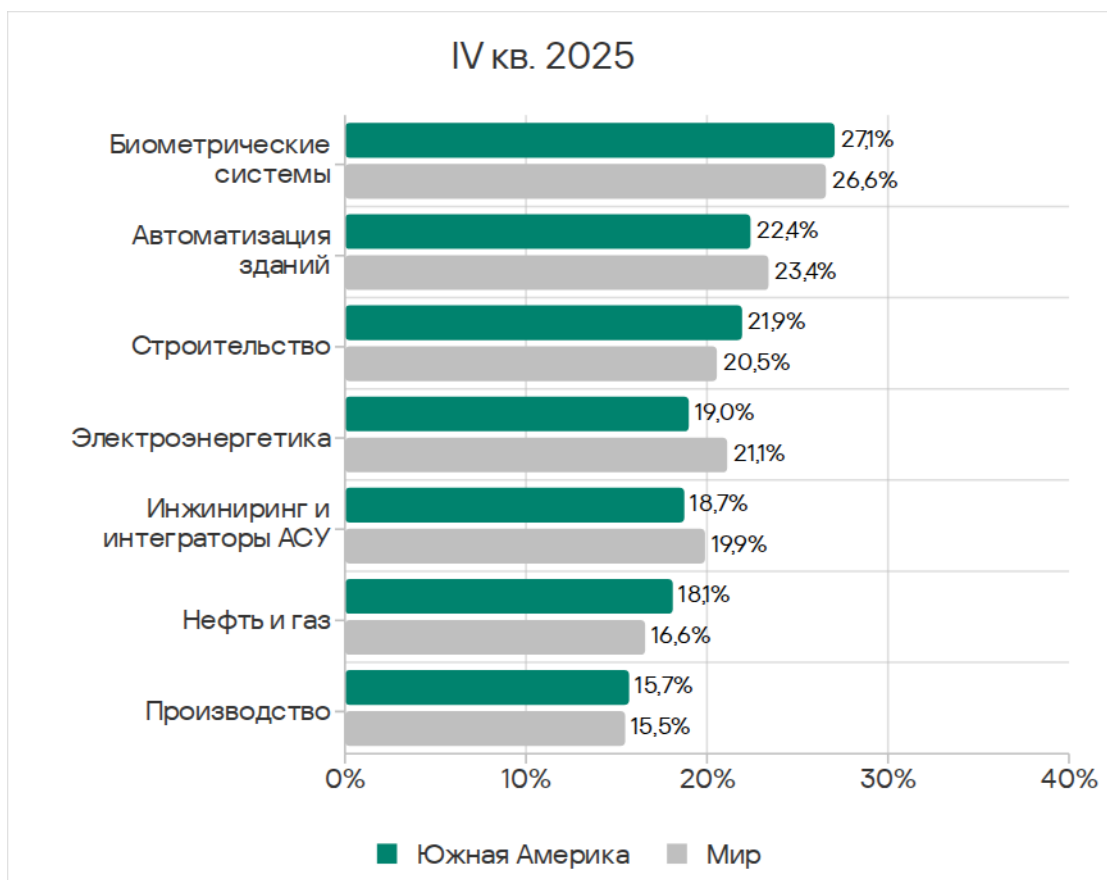


Распространяются черви через все источники, в четвертом квартале из-за фишинговых кампаний основным источником червей стала почта.

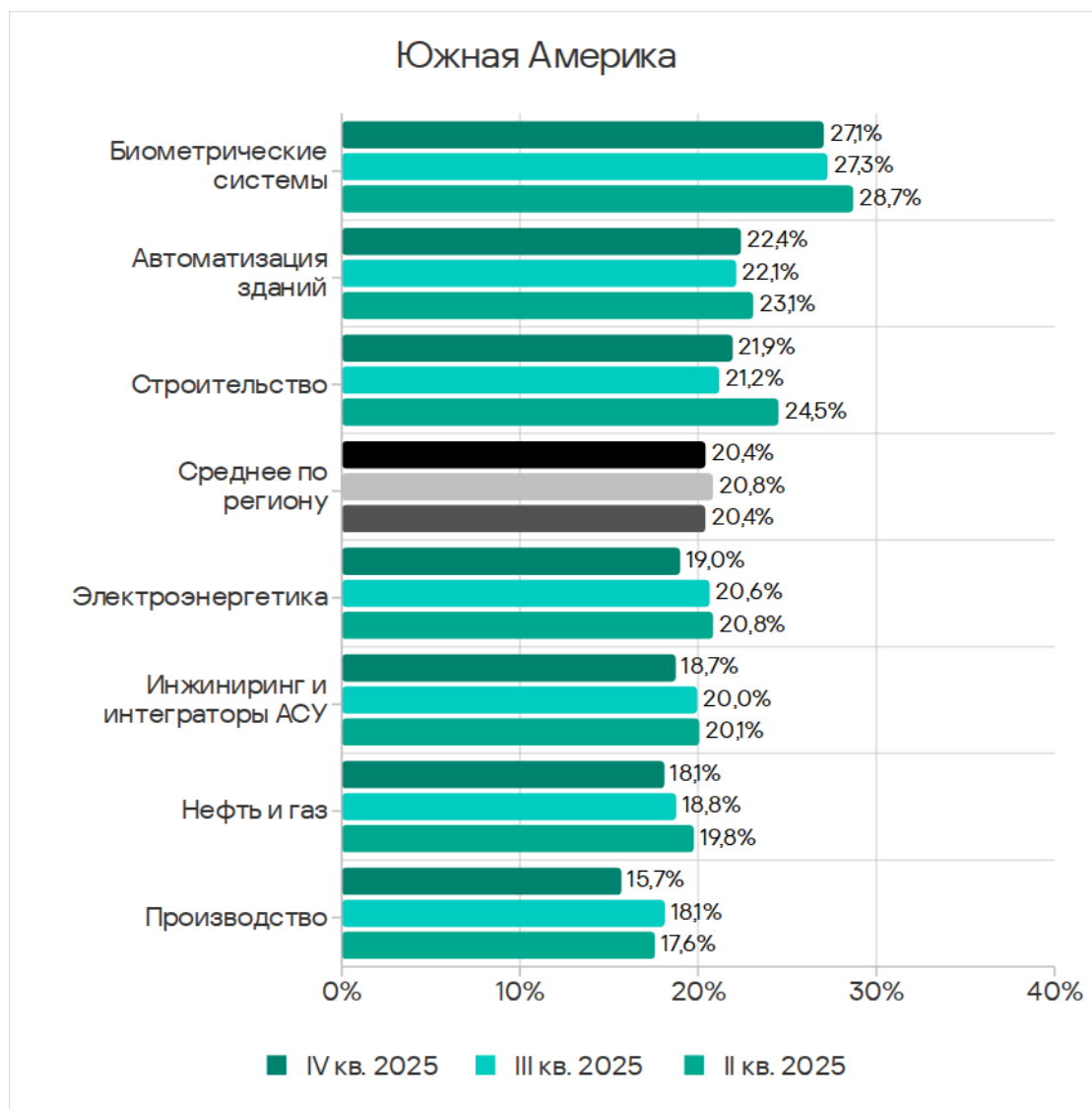
## Отрасли

В регионе из всех рассмотренных в отчете отраслей чаще всего вредоносные объекты блокировались в инфраструктуре биометрических систем.

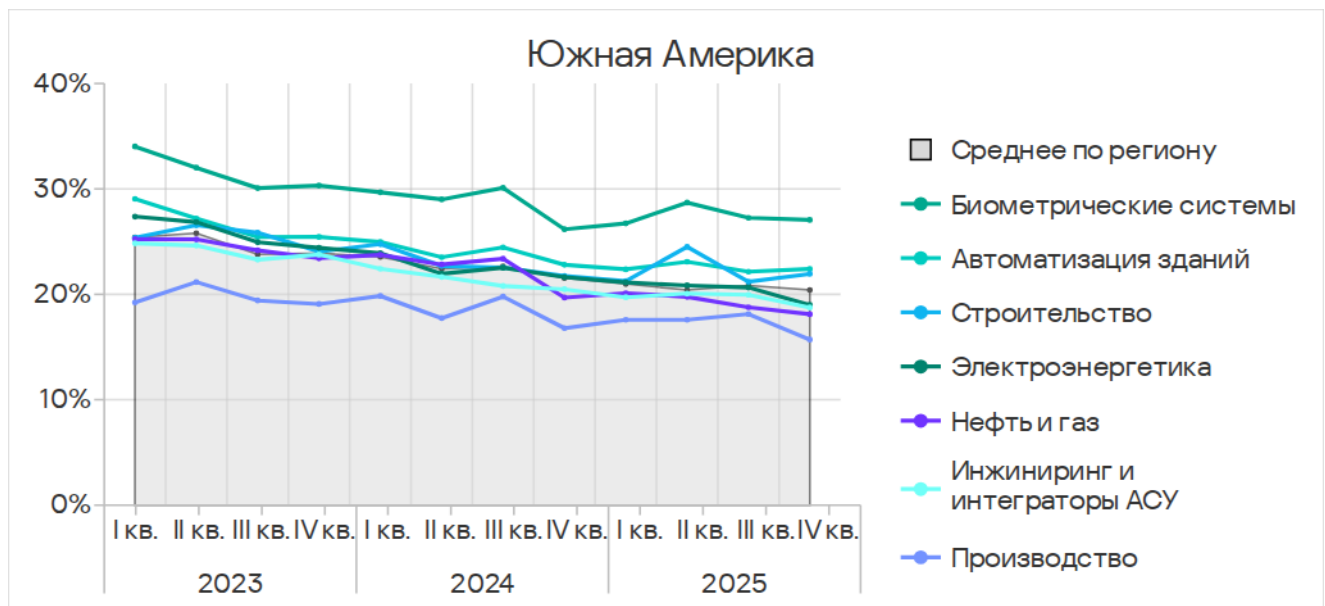
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превышает среднемировое значение в четырех отраслях: биометрические системы, строительство, нефть и газ, производство. Больше всего эта разница в показателях – у нефтегазовой отрасли, в регионе значение больше, чем в мире, в 1,1 раза.



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех отраслях, кроме автоматизации зданий и строительства.



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



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

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

### Показатели источников угроз в отраслях в Южной Америке, IV квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	8,35%	8,36%	9,17%	9,54%	8,67%	11,45%	7,06%	8,65%
Почтовые клиенты	12,07%	7,49%	2,96%	2,80%	3,56%	3,58%	2,31%	5,30%
Съемные носители	0,09%	0,09%	0,08%	0,13%	0,22%	0,14%	0,05%	0,09%
Сетевые папки	0,01%	0,01%	0,00%	—	—	—	0,01%	0,01%
<b>Показатель отрасли в регионе</b>	<b>27,05%</b>	<b>22,40%</b>	<b>18,75%</b>	<b>19,00%</b>	<b>18,11%</b>	<b>21,94%</b>	<b>15,70%</b>	

## Показатели категорий угроз в отраслях в Южной Америке, IV квартал 2025 года

Отрасль / Тип угрозы	Биометрические системы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	1,95%	2,21%	2,44%	2,73%	2,22%	3,01%	1,89%	2,30%
Вредоносные скрипты и фишинговые страницы	14,32%	11,49%	7,84%	8,14%	8,11%	9,70%	6,26%	9,65%
Вредоносные документы (MSOffice+PDF)	5,98%	4,03%	2,16%	2,22%	2,89%	2,26%	2,03%	3,08%
Троянцы-шпионы, бэкдоры и кейлоггеры	7,82%	5,20%	2,60%	2,64%	2,22%	3,23%	2,50%	3,93%
Программы-вымогатели	0,14%	0,14%	0,09%	0,16%	0,22%	0,08%	0,09%	0,11%
Майнеры — исполняемые файлы для ОС Windows	0,33%	0,35%	0,36%	0,33%	0,44%	0,43%	0,26%	0,34%
Веб-майнеры, выполняемые в браузерах	0,21%	0,28%	0,30%	0,26%	0,56%	0,35%	0,18%	0,27%
Вредоносные программы для AutoCAD	0,04%	0,04%	0,07%	0,06%	—	0,41%	0,02%	0,06%
Черви (Worm)	1,77%	1,49%	0,86%	1,08%	1,33%	0,79%	0,77%	1,14%
Вирусы (Virus)	1,00%	0,82%	0,65%	0,97%	0,44%	1,12%	0,64%	0,74%
<b>Показатель отрасли в регионе</b>	<b>27,05%</b>	<b>22,40%</b>	<b>18,75%</b>	<b>19,00%</b>	<b>18,11%</b>	<b>21,94%</b>	<b>15,70%</b>	

## Особенности региона

По доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, Южная Америка находится на втором месте в соответствующем рейтинге регионов.

По показателям в инфраструктуре биометрических систем Южная Америка также занимает второе место среди регионов по доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов.

В электронных письмах злоумышленники распространяют вредоносные документы и вредоносные скрипты и фишинговые страницы, которые применяются, в том числе, для загрузки в систему пользователя шпионских программ.

По показателям и вредоносных скриптов, и вредоносных документов Южная Америка находится на втором месте среди регионов, по показателю шпионских программ — на седьмом. Эти категории угроз актуальны для всех отраслей региона.

Отметим, что высокие показатели этих угроз — явные признаки высокой доступности технологических систем для продвинутых категорий злоумышленников.

Южная Америка попадает в топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, по показателям во всех отраслях, кроме производства:

- нефтегазовая отрасль – регион занимает первое место;
- биометрические системы, строительство и электроэнергетика – второе место;
- автоматизация зданий, инжиниринг и интеграторы АСУ – третье место.

При этом во многих случаях вредоносные скрипты нацелены напрямую на кражу данных аутентификации сотрудников в корпоративных сервисах.

Южная Америка попадает в топ-3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, по показателям в следующих отраслях:

- нефтегазовая отрасль – регион занимает первое место;
- биометрические системы, инжиниринг и интеграторы АСУ, производство – второе место;
- строительство, электроэнергетика – третье место.

В нефтегазовой отрасли Южная Америка находится на третьем месте среди регионов по показателю шпионских программ.

В четвертом квартале 2025 года почтовые клиенты стали источником червя-бэкдора, который рассылался в электронных письмах в ходе очередной волны фишинговых кампаний. Среди отраслей в Южной Америке по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, лидируют биометрические системы и автоматизация зданий. Они же занимают первое и второе места в

рейтингах отраслей региона по показателям вредоносных скриптов, вредоносных документов, шпионских программ и червей.

### **Биометрические системы**

Южная Америка находится на третьем месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в инфраструктуре биометрических систем.

Среди регионов по показателям в инфраструктуре биометрических систем Южная Америка занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

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

### **Автоматизация зданий**

Южная Америка находится на восьмом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в автоматизации зданий.

Среди регионов по показателям в отрасли Южная Америка занимает:

- третье место по доле компьютеров АСУ, на которых блокируются вредоносные скрипты и фишинговые страницы.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по доле компьютеров АСУ, на которых угрозы были заблокированы в почтовых клиентах и в сетевых папках;
- второе место по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы и черви;
- третье место по показателю программ-вымогателей.

## Строительство

Южная Америка находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

Среди регионов по показателям в отрасли Южная Америка занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы в интернете и угрозы из почтовых клиентов;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы;
- третье место по показателю вредоносных документов.

Среди отраслей в регионе строительство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- второе место по показателю угроз на съемных носителях;
- третье место по показателю угроз из почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, вирусы и вредоносные программы для AutoCAD;
- второе место по показателям майнеров обеих категорий;
- третье место по показателям вредоносных скриптов и шпионских программ.

## Электроэнергетика

Южная Америка находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

Среди регионов по показателям в отрасли Южная Америка занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы в интернете и угрозы из почтовых клиентов;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы;
- третье место по показателю вредоносных документов.

Среди отраслей в регионе электроэнергетика занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- третье место по показателю угроз на съемных носителях;

- второе место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных и программы-вымогатели;
- третье место по показателю вирусов и вредоносных программ для AutoCAD.

### **Инжиниринг и интеграторы АСУ**

Южная Америка находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли инжиниринг и интеграторы АСУ.

Среди регионов по показателям в отрасли Южная Америка занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы;
- третье место по показателям угроз категорий вредоносные скрипты и фишинговые страницы, веб-майнеры.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD;
- третье место по показателям ресурсов в интернете из списка запрещенных и майнеров обеих категорий.

### **Нефть и газ**

Южная Америка находится на третьем месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в нефтегазовой отрасли.

Среди регионов по показателям в отрасли Южная Америка занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и угрозы из почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, вредоносные скрипты и фишинговые страницы, веб-майнеры;
- третье место по показателям шпионских программ и майнеров в формате исполняемых файлов.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях;
- первое место по показателям майнеров обеих категорий и программ-вымогателей;
- третье место по показателям вредоносных документов и червей.

### **Производство**

Южная Америка находится на пятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди регионов по показателям в отрасли Южная Америка занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные документы.

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.

## 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, в четвертом 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 выше 10-й позиции:

- угрозы из сетевых папок – шестое место;
- угрозы из интернета – девятое место;
- угрозы из почтовых клиентов – девятое место;
- вредоносные скрипты и фишинговые страницы – девятое место.

По показателям вредоносных документов и вирусов регион занимает десятое место в соответствующих рейтингах.

В Северной Америке (Канаде) почтовый спам и фишинг, содержащий вредоносные скрипты и майнеры в виде исполняемых файлов, вероятнее всего, попадали на компьютеры в технологической сети через доступ к почтовому серверу в корпоративной сети, открытый для внешних рассылок.

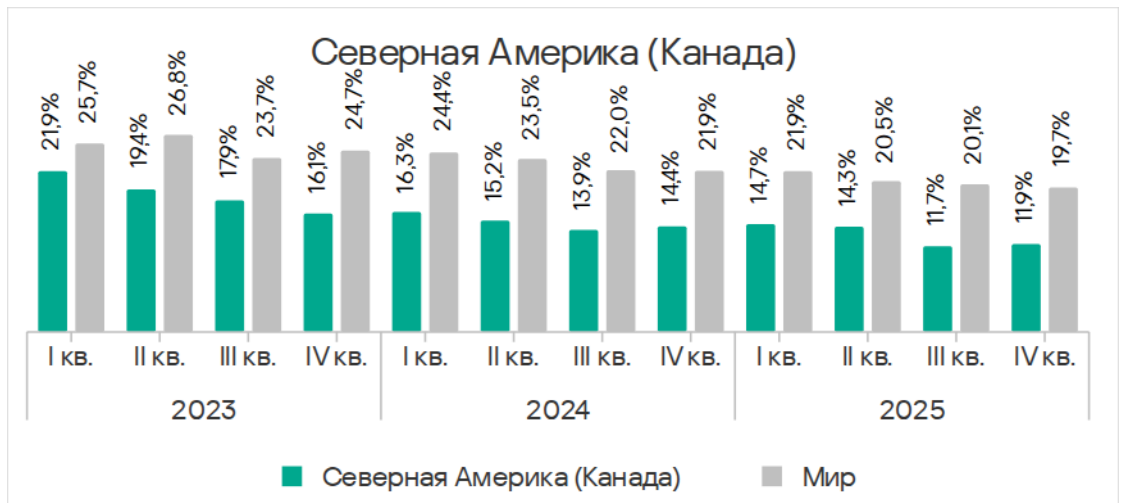
Относительно высокие показатели угроз, распространяющихся через почтовые клиенты (фишинг), вредоносных скриптов и майнеров обеих категорий могут быть признаками доступности технологических систем в регионе для продвинутых категорий злоумышленников.

### Статистика по всем угрозам

Северная Америка (Канада) занимает 12-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Показатель в регионе постепенно снижается с периодическими колебаниями.

В четвертом квартале 2025 года в регионе доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выросла до 11,9%. Это существенно ниже среднемирового значения, но в 1,4 раза выше, чем в Северной Европе, где показатель наименьший.



## Источники угроз

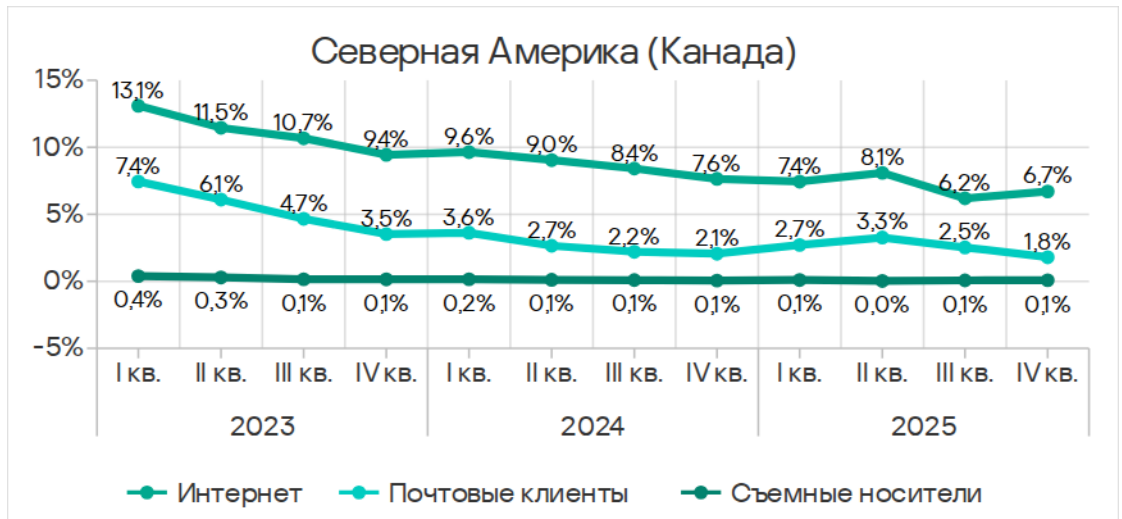
Показатели всех источников угроз в Северной Америке (Канаде) ниже, чем среднемировые.



Вредоносные объекты в регионе распространяются преимущественно через интернет и почту.

Неожиданно высокая позиция у региона оказалась в рейтинге по доле компьютеров АСУ, на которых угрозы были блокированы в сетевых папках: Северная Америка (Канада) заняла в нем шестое место. Это самая высокая позиция региона в рейтингах и по источникам, и по категориям угроз. Единственная отрасль в регионе, где отмечены такие угрозы, – инжиниринг и интеграторы АСУ.

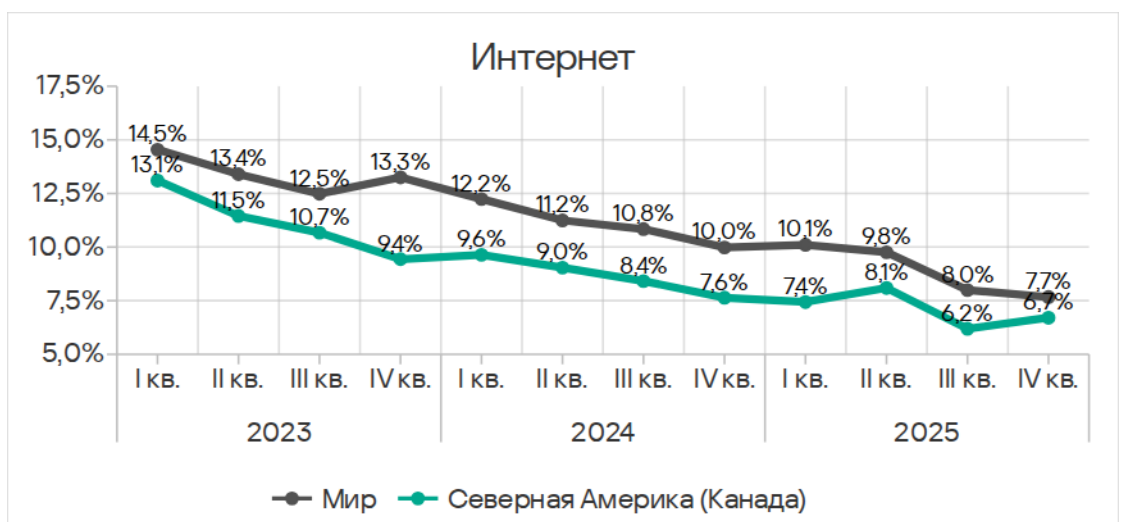
В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличилась у угроз из интернета и на съемных носителях.



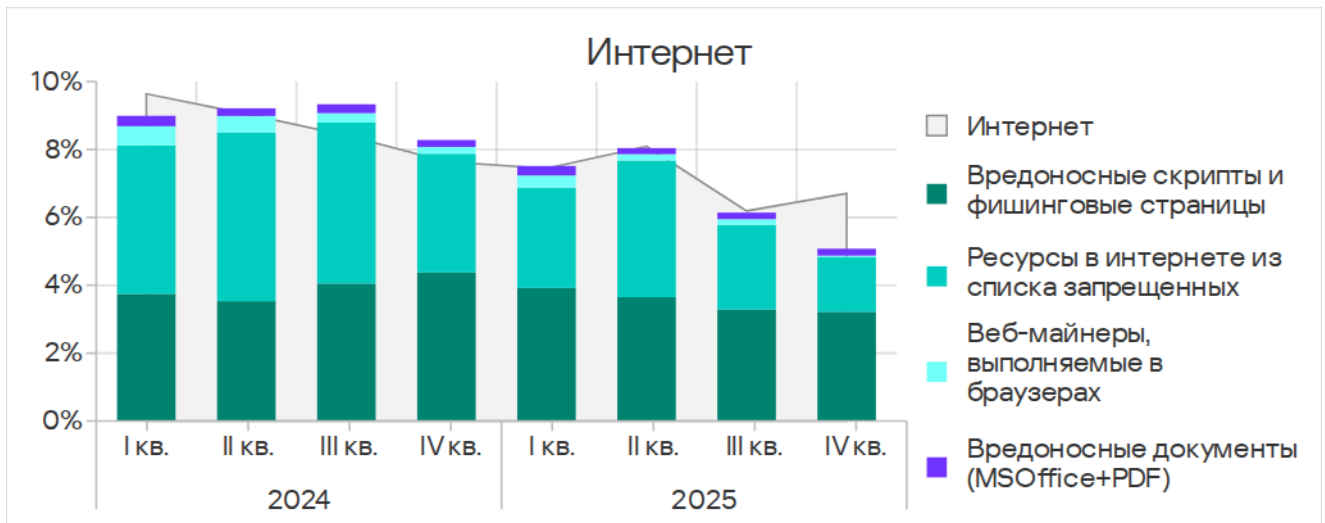
## Интернет

По доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Северная Америка (Канада) занимает девятое место с показателем 6,71%. Это выше минимального показателя регионов – у Северной Европы – в 1,7 раза.

Северная Америка (Канада) – один из пяти регионов, где в четвертом квартале 2025 доля угроз из интернета увеличилась.



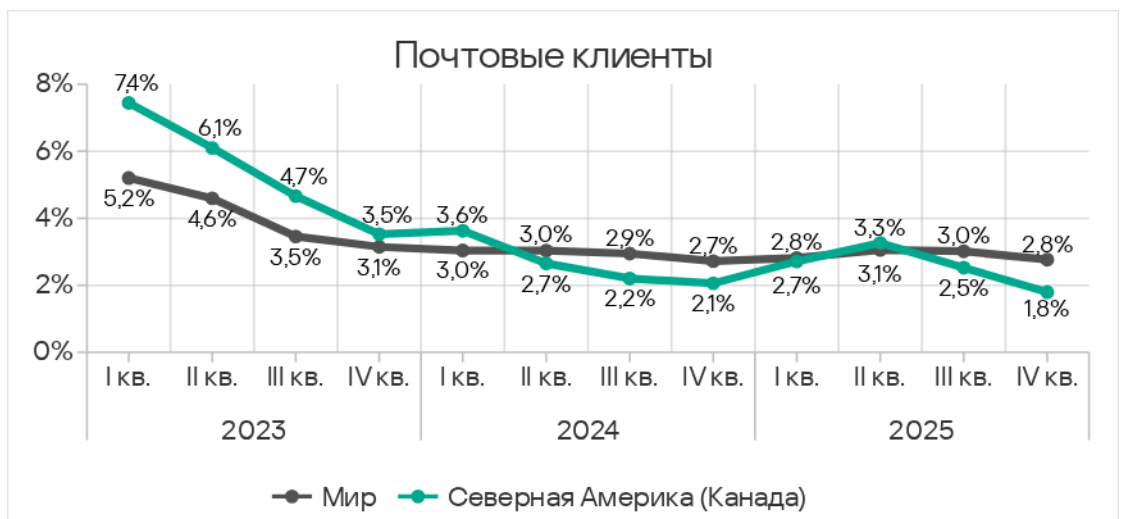
Основные категории угроз из интернета, заблокированные на компьютерах АСУ в регионе: вредоносные скрипты и фишинговые страницы, ресурсы в интернете из списка запрещенных.



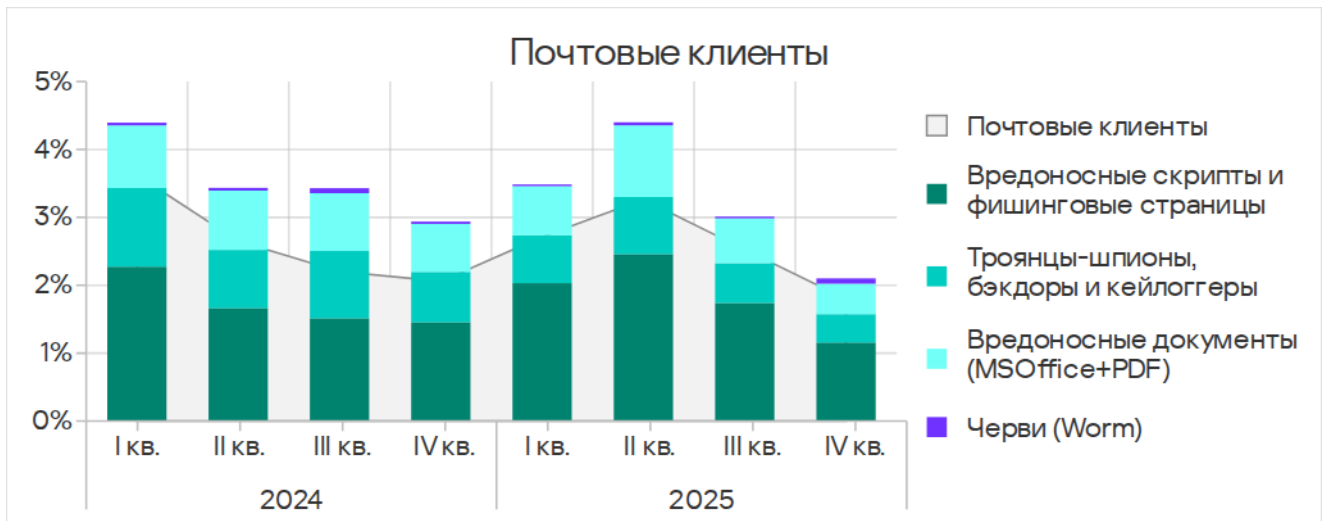
## Почтовые клиенты

По доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, в четвертом квартале 2025 года Северная Америка (Канада) заняла девятое место.

Показатель в Северной Америке (Канада) за квартал уменьшился до 1,79%. Это в 2,8 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.



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



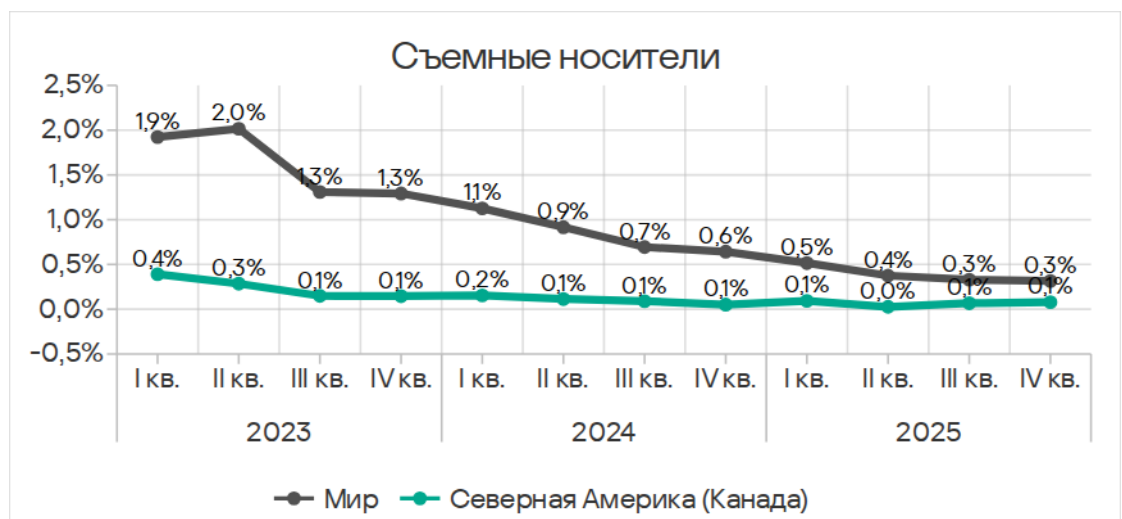
В четвертом квартале 2025 года во всех регионах увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это связано с новой волной фишинговых кампаний Curriculum-vitae-catalina. В Северной Америке (Канада) пик атак пришелся на октябрь.

Северная Америка (Канада), Западная Европа и Австралия вошли в топ-3 регионов с наименьшим ростом показателя червей за квартал.

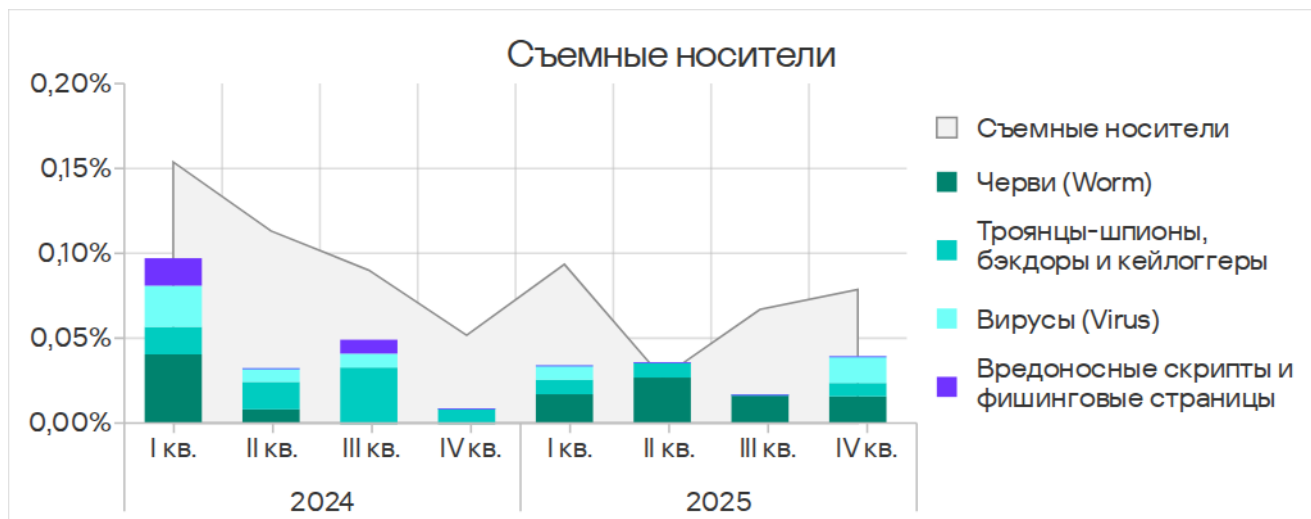
## Съемные носители

По доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, в четвертом квартале 2025 года Северная Америка (Канада) заняла 11-е место с 0,08%. Это в 1,7 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.

Показатель в регионе колеблется. Северная Америка (Канада) – один из трех регионов, где в четвертом квартале 2025 года он подрос.



Основные категории угроз, которые блокируются на компьютерах АСУ при подключении съемных носителей: черви и вирусы. В четвертом квартале 2025 года на съемных носителях блокировалось также шпионское ПО и майнеры в формате исполняемых файлов.

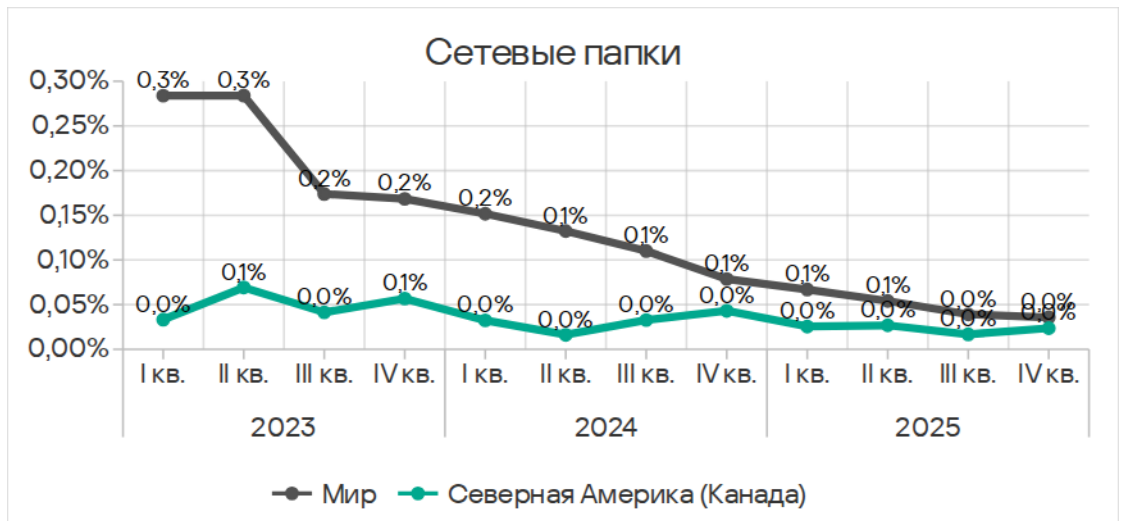


## Сетевые папки

По доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, в четвертом квартале 2025 года Северная Америка (Канада) заняла шестое место. Это самая высокая позиция региона во всех рейтингах – и по источникам, и по категориям угроз.

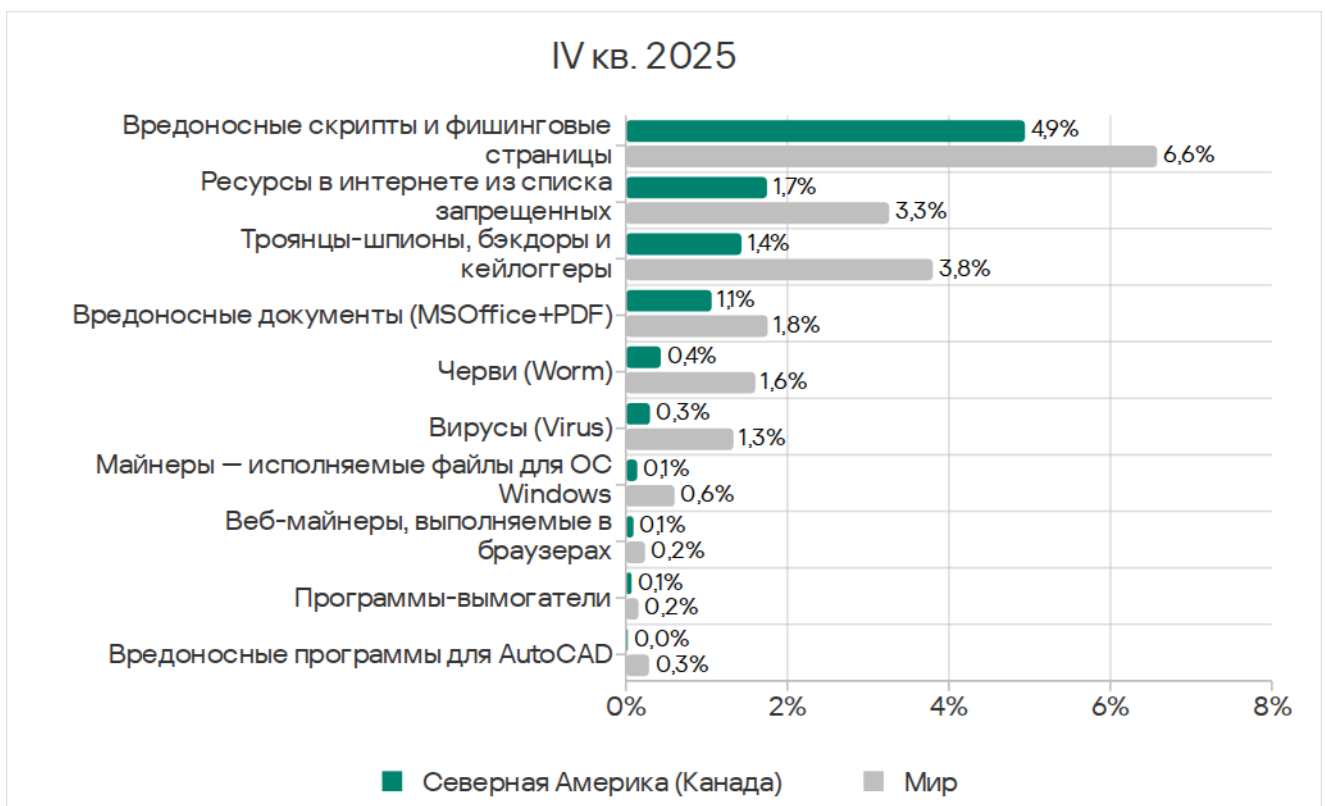
Показатель в регионе – с 0,024% – в 3,4 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

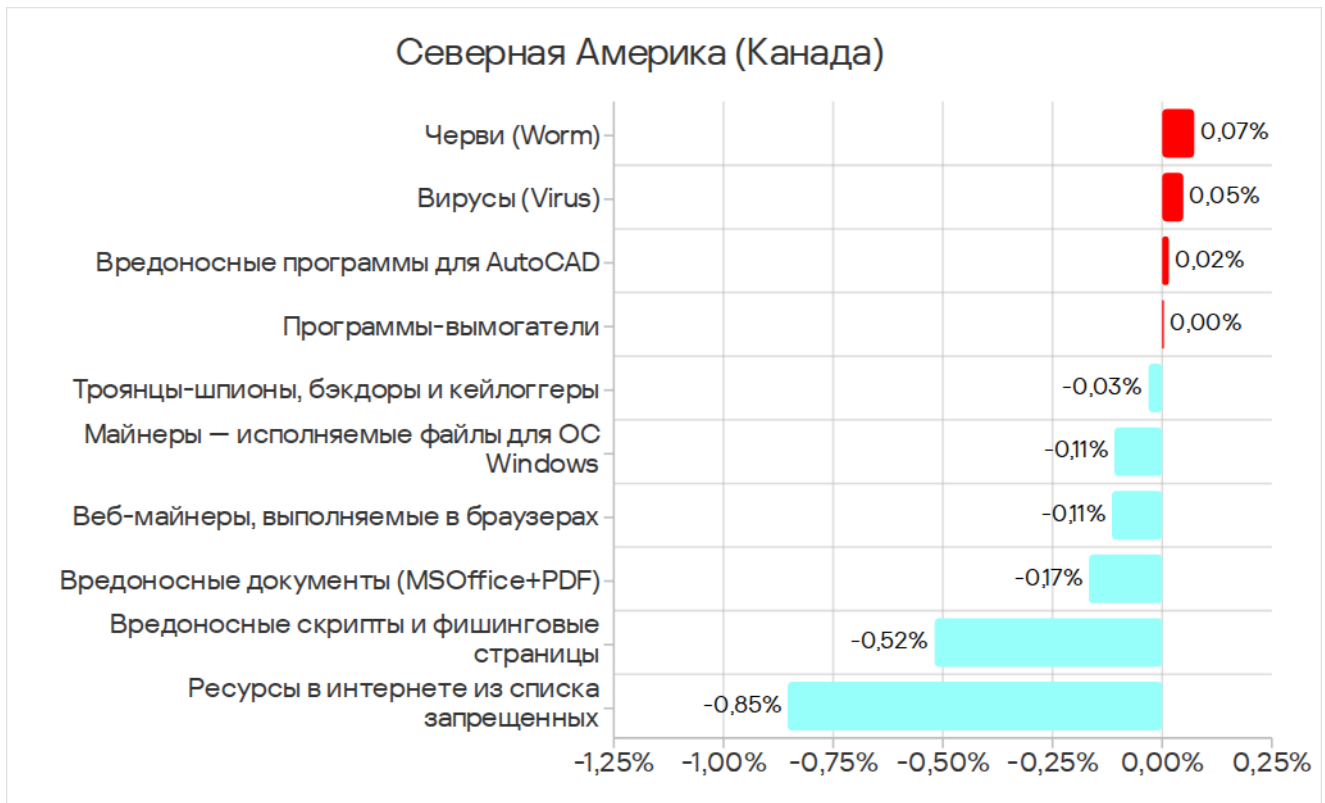
В то время как среднемировой показатель угроз из сетевых папок неуклонно снижается, значение в регионе колеблется. Северная Америка (Канада) – один из четырех регионов, где в четвертом квартале 2025 года показатель сетевых папок вырос.



В четвертом квартале через сетевые папки распространялись преимущественно шпионские программы. Угрозы из сетевых папок блокировались в отрасли инжиниринг и интеграторы АСУ.

## Категории угроз





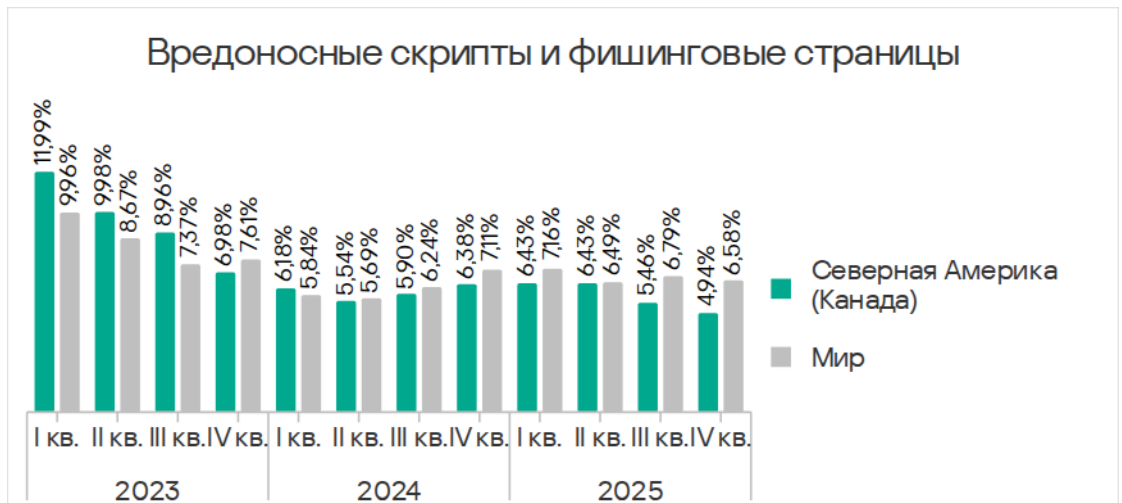
В Северной Америке (Канаде) показатели всех категорий ниже среднемировых. В четвертом квартале 2025 года уменьшились показатели угроз всех категорий, кроме червей, вирусов, программ для AutoCAD и программ-вымогателей.

Самая высокая позиция в рейтингах регионов по показателям угроз различных категорий у Северной Америки (Канады) оказалась в рейтинге по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, — девятое место.

## Вредоносные скрипты и фишинговые страницы

По доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, Северная Америка (Канада) заняла девятое место с 4,94%. Этот показатель в 2,0 раза выше, чем в Северной Европе, где он — наименьший из всех регионов.

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, в регионе уменьшился второй квартал подряд.



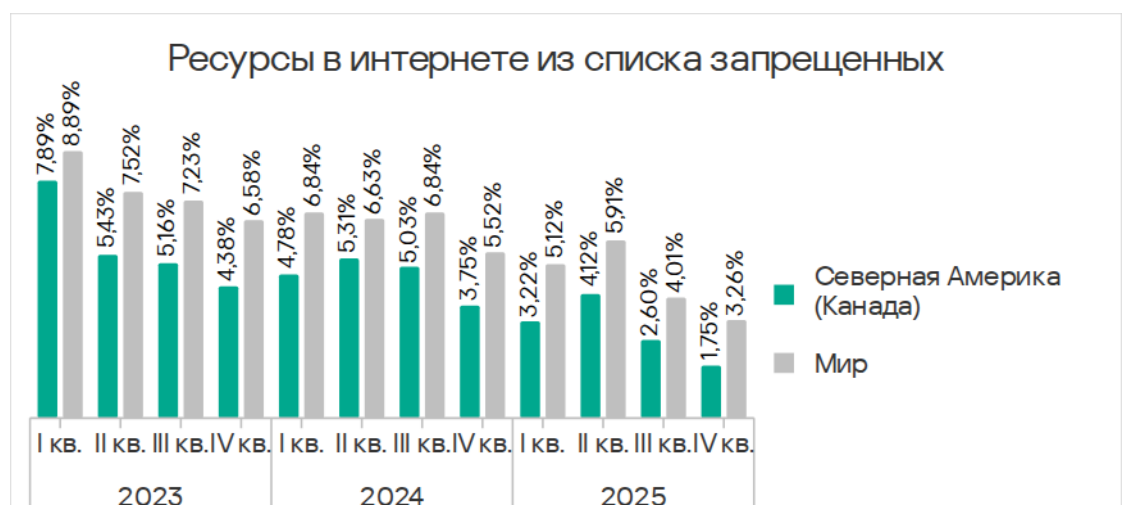
Распространяются вредоносные скрипты и фишинговые страницы как в интернете, так и по электронной почте.

## Ресурсы в интернете из списка запрещенных

По доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, Северная Америка (Канада) заняла 13-е место в соответствующем рейтинге регионов – с 1,75%.

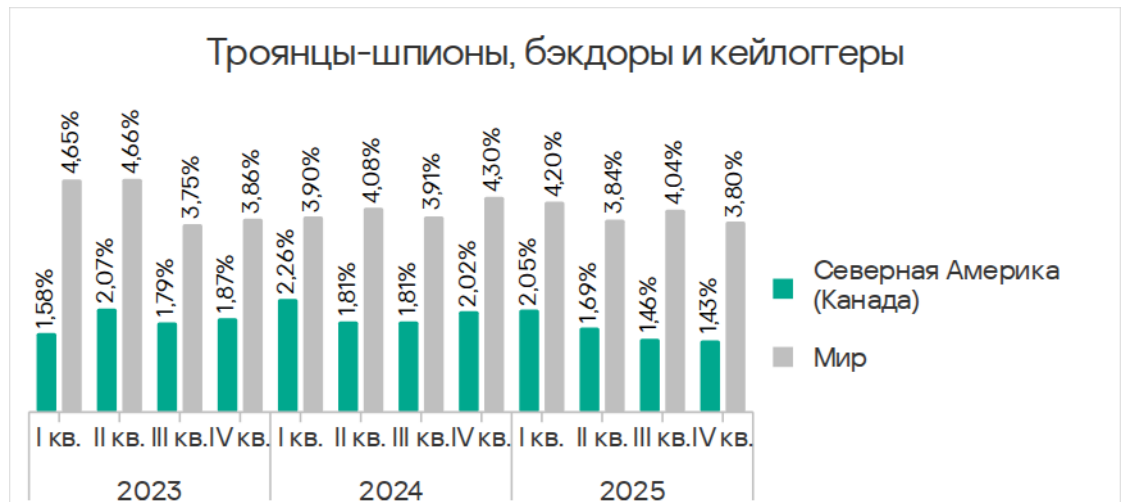
Ресурсы в интернете из списка запрещенных находятся на втором месте (после вредоносных скриптов) в региональном рейтинге категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

Показатель в регионе уменьшился второй квартал подряд и в четвертом квартале был минимальным за три года.



## Шпионские программы

По доле компьютеров АСУ, на которых были заблокированы шпионские программы, в соответствующем рейтинге регионов Северная Америка (Канада) заняла 12-е место с 1,43%. Показатель в регионе уменьшился третий квартал подряд.

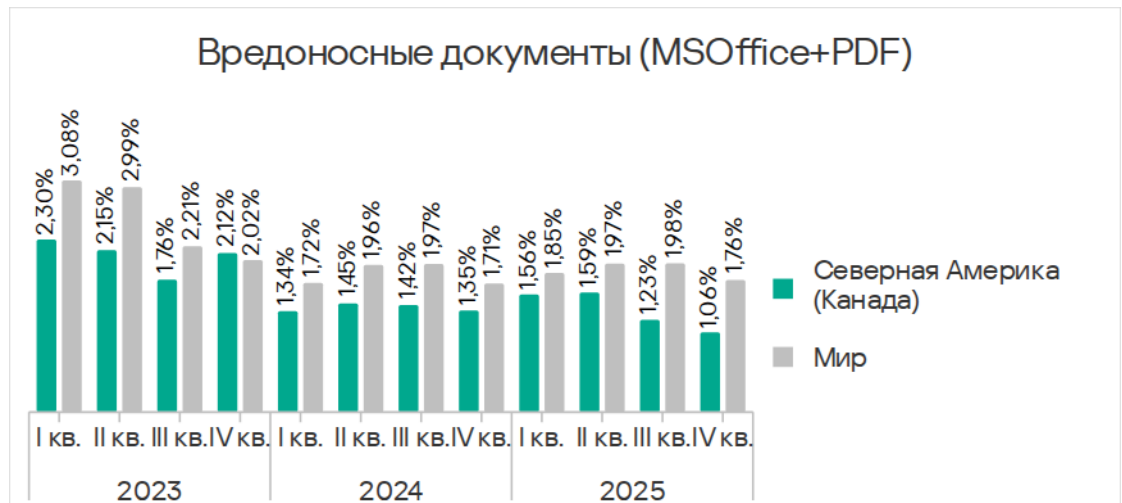


Шпионские программы в регионе блокируются во всех источниках угроз, преимущественно в почтовых клиентах.

## Вредоносные документы

Северная Америка (Канада) заняла 10-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы. Показатель в регионе — 1,06% — в 2,3 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, в регионе колеблется. В четвертом квартале 2025 года она снизилась до значения, наименьшего за три года.

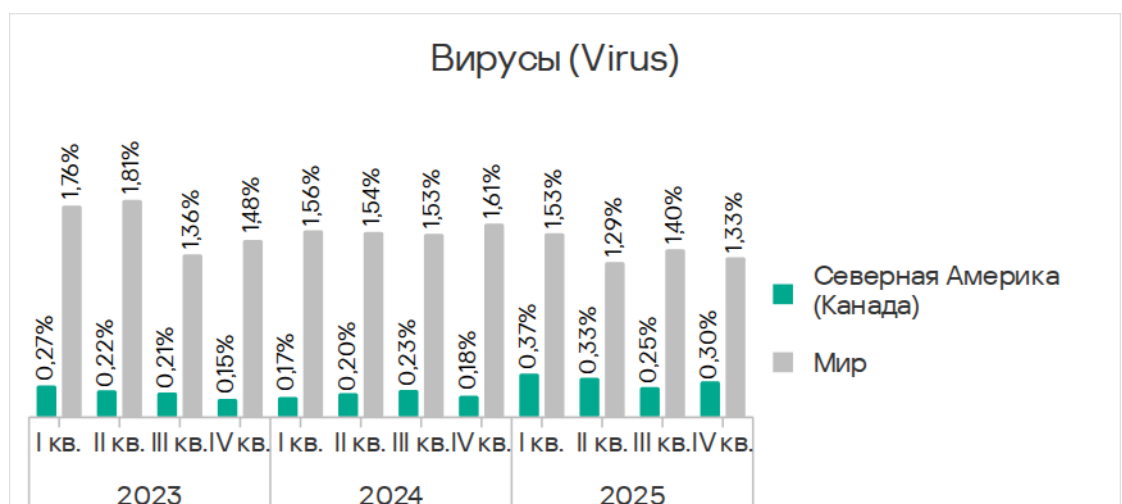


Распространяются вредоносные документы преимущественно по электронной почте.

## Вирусы

По доле компьютеров АСУ, на которых были заблокированы вирусы, Северная Америка (Канада) заняла 10-е место с показателем 0,30%, который существенно ниже среднемирового, но в 2,0 раза больше, чем у замыкающей соответствующий рейтинг Западной Европы.

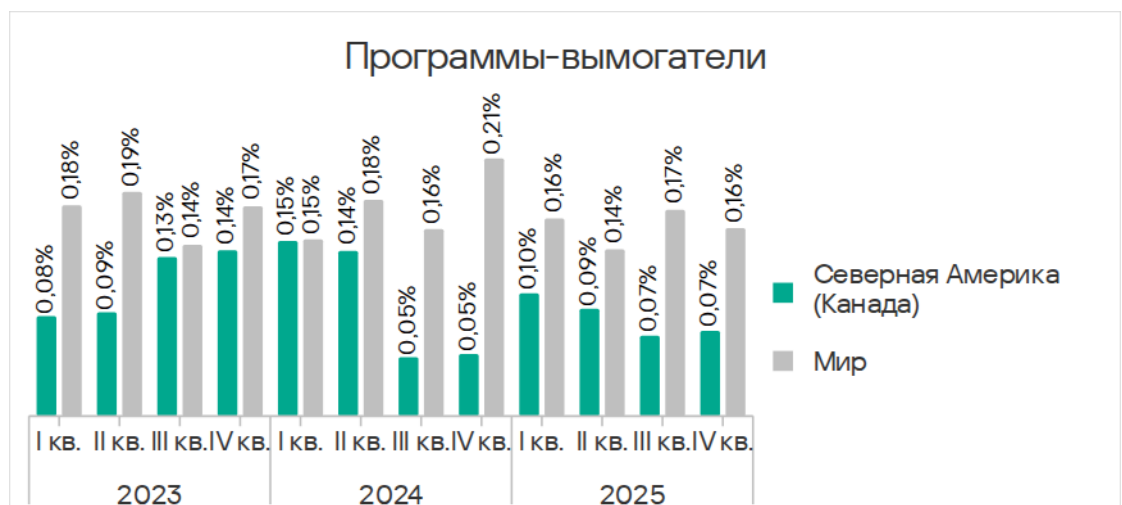
Северная Америка (Канада) – один из четырех регионов, где показатель вирусов за квартал вырос. Отметим, что в 2025 году значения были выше, чем в предыдущие два года (за исключением первого квартала 2023 года).



## Программы-вымогатели

По доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, Северная Америка (Канада) заняла предпоследнее, 13-е место с показателем 0,07%, который в 1,4 раза больше, чем у замыкающей соответствующий рейтинг Северной Европы.

Показатель в регионе колеблется, в четвертом квартале 2025 года он не изменился.

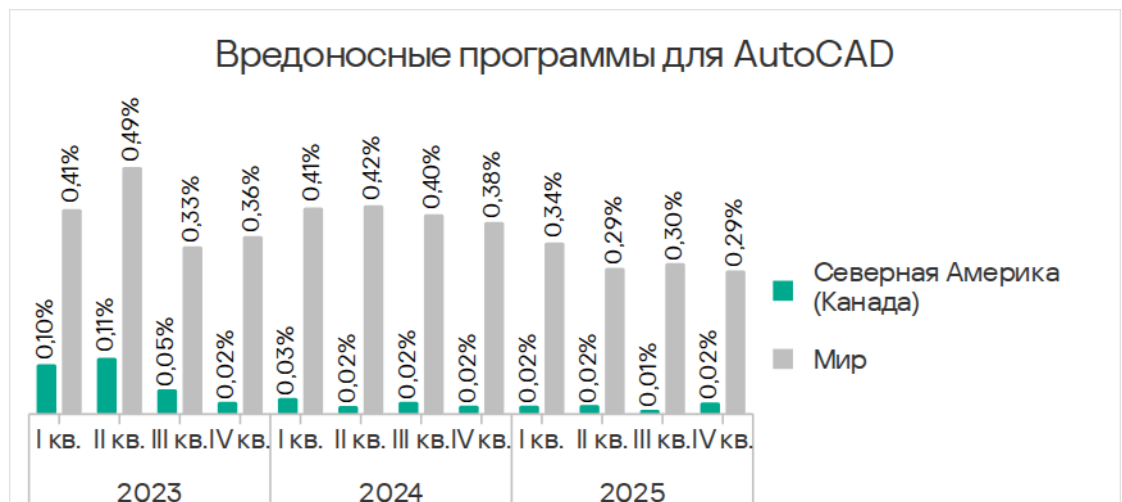


## Вредоносные программы для AutoCAD

По доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, Северная Америка (Канада) заняла 11-е место с показателем 0,02%, который более, чем в 14,5 раза меньше среднемирового, но в 2,0 раза больше, чем у замыкающей соответствующий рейтинг Северной Европы.

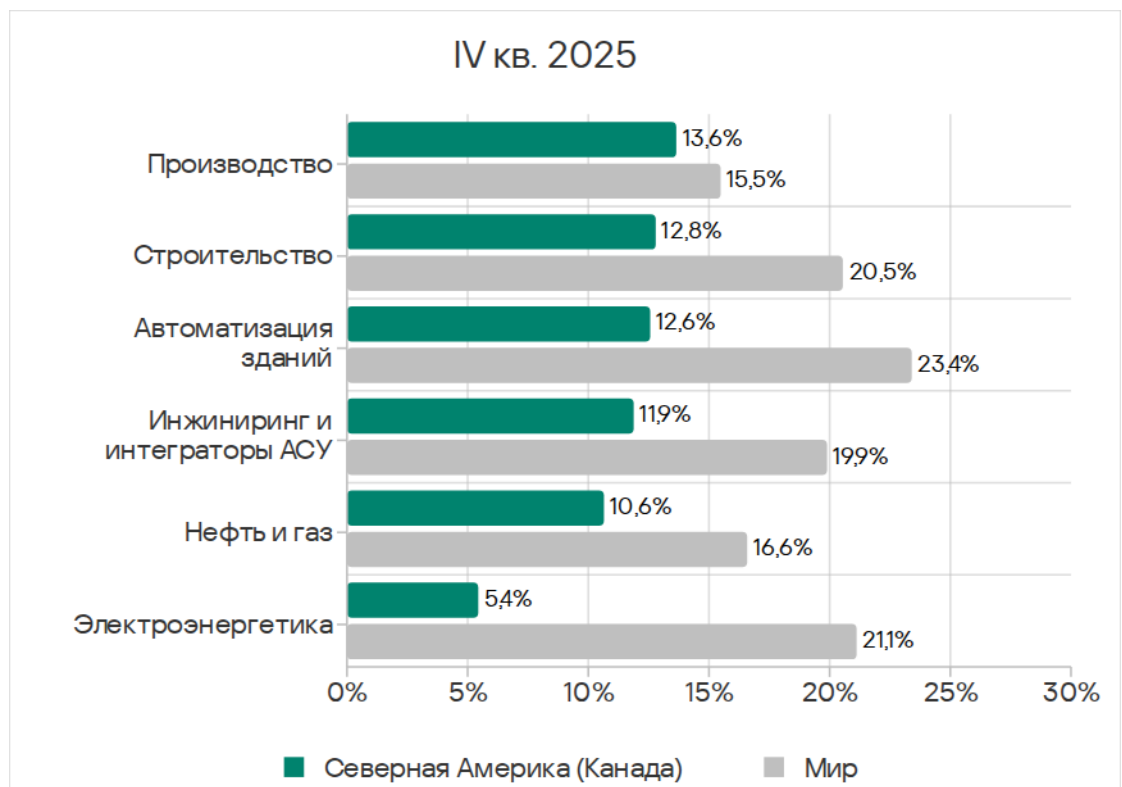
В четвертом квартале 2025 года эта угроза была актуальна лишь для одной из исследуемых отраслей – строительство.

Северная Америка (Канада) – один из четырех регионов, где показатель вредоносных программ для AutoCAD за квартал увеличился.



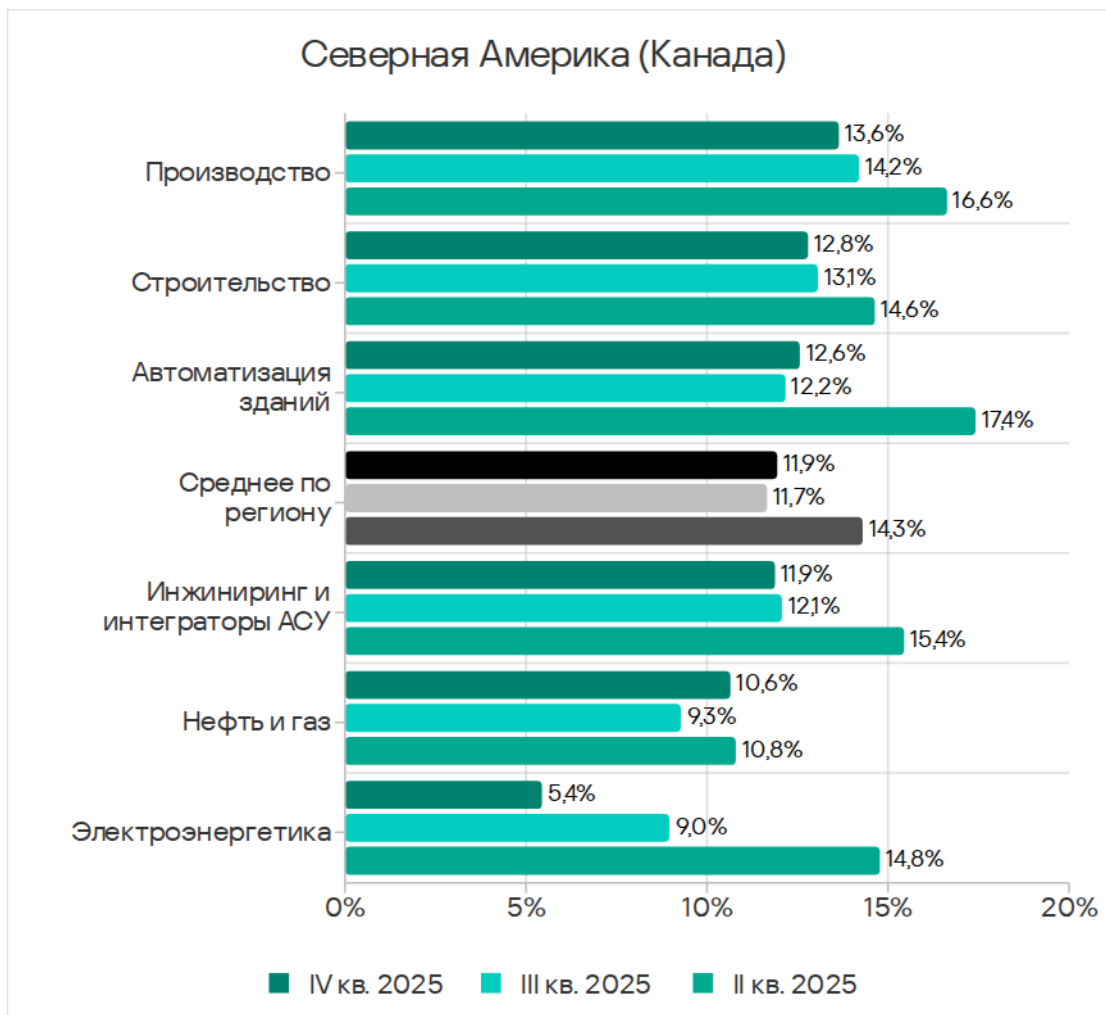
## Отрасли

Среди рассмотренных в отчете отраслей наибольшая доля компьютеров АСУ, на которых были заблокированы вредоносные объекты в Северной Америке (Канаде), – у производственного сектора.

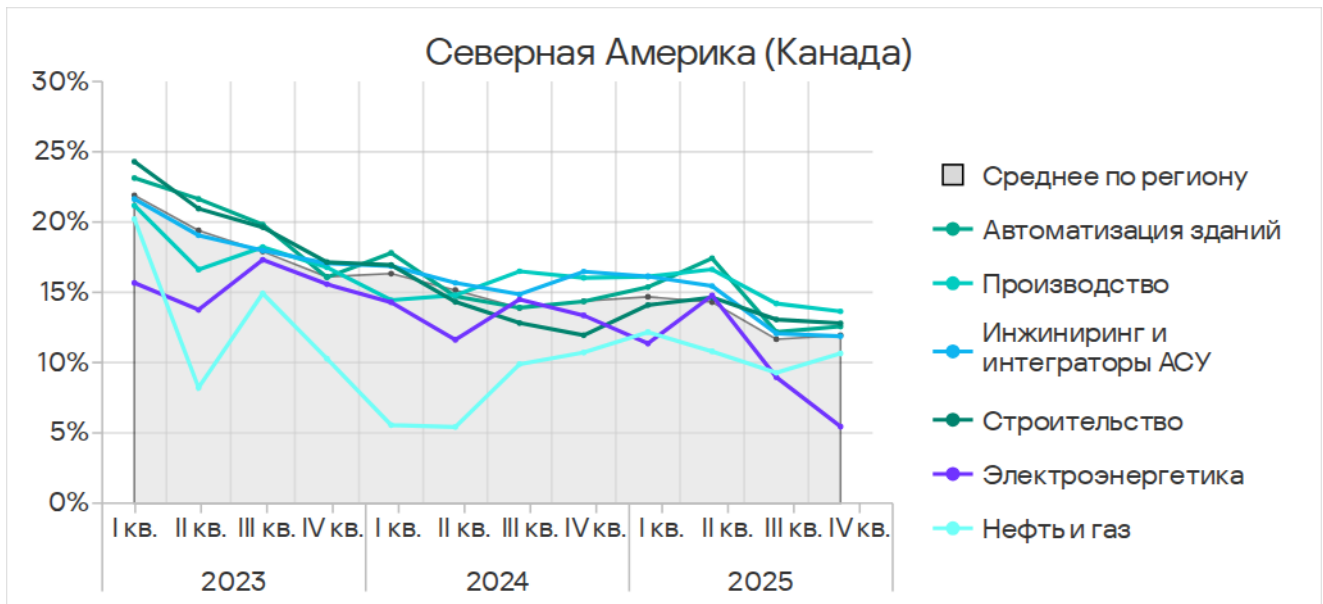


Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, второй квартал подряд снижается во всех отраслях, кроме нефтегазовой отрасли и автоматизации зданий. Особенно значительны

изменения в электроэнергетике, где показатель за полгода уменьшился в 2,7 раза.



Показатели всех исследуемых отраслей, кроме электроэнергетики, близки к показателям региона в целом. В электроэнергетической отрасли значения за большинство кварталов ниже региональных.



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

При оценке проблем отраслей в регионах мы используем тепловые карты. Цвет на карте определяет положение показателя в глобальном рейтинге отраслей в регионах (отдельно по каждой категории угроз или каждому источнику). Красный цвет указывает на то, что значение близко к максимальному.

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

Отрасль / Источник угрозы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Интернет	5,76%	7,09%	2,59%	2,31%	7,92%	8,26%	6,71%
Почтовые клиенты	3,28%	1,40%	0,78%	1,39%	2,25%	0,90%	1,79%
Съемные носители	0,20%	0,10%	—	—	0,05%	—	0,08%
Сетевые папки	—	0,02%	—	—	—	—	0,02%
<b>Показатель отрасли в регионе</b>	<b>12,57%</b>	<b>11,88%</b>	<b>5,44%</b>	<b>10,65%</b>	<b>12,79%</b>	<b>13,64%</b>	

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

Отрасль / Тип угрозы	Автоматизация зданий	Инжиниринг и интеграторы АСУ	Электроэнергетика	Нефть и газ	Строительство	Производство	Показатель категории в регионе
Ресурсы в интернете из списка запрещенных	1,36%	1,94%	1,04%	0,93%	1,55%	2,87%	1,75%
Вредоносные скрипты и фишинговые страницы	6,08%	4,74%	1,30%	2,31%	5,90%	3,95%	4,94%
Вредоносные документы (MSOffice+PDF)	2,00%	0,80%	—	0,93%	1,45%	0,54%	1,06%
Троянцы-шпионы, бэкдоры и кейлоггеры	2,24%	1,33%	1,04%	0,93%	1,08%	1,26%	1,43%
Программы-вымогатели	0,16%	0,07%	—	—	—	0,18%	0,07%
Майнеры — исполняемые файлы для ОС Windows	0,28%	0,15%	—	—	0,14%	—	0,14%
Веб-майнеры, выполняемые в браузерах	0,24%	0,10%	—	—	0,05%	—	0,09%
Вредоносные программы для AutoCAD	—	—	—	—	0,05%	—	0,02%
Черви (Worm)	0,80%	0,34%	0,26%	0,46%	0,28%	—	0,43%
Вирусы (Virus)	0,32%	0,12%	—	0,46%	0,52%	0,54%	0,30%
<b>Показатель отрасли в регионе</b>	<b>12,57%</b>	<b>11,88%</b>	<b>5,44%</b>	<b>10,65%</b>	<b>12,79%</b>	<b>13,64%</b>	

#### Производство

Северная Америка (Канада) находится на шестом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли. Это самая высокая позиция региона в рейтингах по доле атакованных компьютеров в отраслях.

Среди регионов по показателям в отрасли Северная Америка (Канада) занимает третье место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных.

Среди отраслей в регионе производство занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета;
- первое место по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных; вирусы и программы-вымогатели;
- третье место по показателю шпионских программ.

### **Строительство**

Северная Америка (Канада) находится на 12-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди отраслей в регионе строительство занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и из почтовых клиентов;
- третье место по показателю угроз на съемных носителях;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD (это единственная отрасль в регионе, где блокировались такие угрозы);
- второе место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вредоносные документы, вирусы;
- третье место по показателям угроз следующих категорий: ресурсы в интернете из списка запрещенных, черви, майнеры обоих видов.

### **Автоматизация зданий**

Северная Америка (Канада) находится на 13-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди отраслей в регионе автоматизация зданий занимает:

- первое место по доле компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах и при подключении съемных носителей;
- первое место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, черви, майнеры обеих категорий;
- второе место по показателю программ-вымогателей;
- третье место по показателю вирусов.

### **Инжиниринг и интеграторы АСУ**

Северная Америка (Канада) находится на 13-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- первое место по угрозам в сетевых папках (это единственная отрасль в регионе, где блокировались такие угрозы);
- второе место по показателю угроз на съемных носителях;
- третье место по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета и из почтовых клиентов;
- второе место по показателю угроз следующих категорий: ресурсы в интернете из списка запрещенных, шпионское ПО, черви, майнеры обеих категорий;
- третье место по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вредоносные документы, программы-вымогатели.

### **Электроэнергетика**

Северная Америка (Канада) находится на последнем, 14-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в этой отрасли.

## Методика подготовки статистики

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

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

*Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT<sup>1</sup>.*

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,

---

<sup>1</sup> 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](mailto:ics-cert@kaspersky.com)