

# Ландшафт угроз для систем промышленной автоматизации

Россия. Третий квартал 2025 года

Россия.....	3
Актуальные угрозы.....	3
Статистика по всем угрозам.....	4
Источники угроз.....	5
Интернет.....	6
Почтовые клиенты .....	7
Съемные носители .....	8
Сетевые папки .....	8
Категории угроз.....	9
Ресурсы в интернете из списка запрещенных .....	11
Майнеры – исполняемые файлы для ОС Windows и черви .....	11
Троянцы-шпионы, бэкдоры и кейлоггеры .....	13
Программы-вымогатели.....	14
Отрасли .....	14
Источники и категории вредоносного ПО в отраслях: «горячие точки» .....	16
Методика подготовки статистики .....	22

# Россия

## Актуальные угрозы

### Основной источник угроз в России – интернет

Основные категории угроз из интернета, блокируемые на компьютерах АСУ, – это интернет-ресурсы из списка запрещенных, вредоносные скрипты и фишинговые страницы, а также майнеры.

Список запрещенных интернет-ресурсов используется для предотвращения попыток первичного заражения. С помощью этого списка на компьютерах АСУ блокируются преимущественно:

- известные вредоносные URL и IP-адреса, используемые злоумышленниками для размещения вредоносных нагрузок и конфигураций;
- подозрительные (ненадежные) веб-ресурсы с развлекательным и игровым контентом, часто используемые для доставки нежелательного программного обеспечения, криптомайнеров и вредоносных скриптов;
- узлы CDN, используемые злоумышленниками для распространения вредоносных скриптов на популярных веб-сайтах;
- сервисы обмена файлами и данными, включая репозитории, часто используемые злоумышленниками для размещения полезных нагрузок и конфигураций следующего этапа.

Интернет-ресурсы из списка запрещенных главным образом используются киберпреступниками для распространения вредоносного ПО, а также для фишинговых атак и в качестве инфраструктуры управления и контроля (С2). Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

Высокие значения параметра, как правило, свидетельствуют:

- о слабом контроле выполнения политик ИБ (компьютеры АСУ имеют так или иначе доступ к интернету);
- о недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным интернет-ресурсам).

### Майнеры – исполняемые файлы для ОС Windows и черви

Россия стабильно, с конца 2022 года, находится на втором месте среди регионов (выше – Средняя Азия и Закавказье) по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows.

Черви в третьем квартале 2025 года в рейтинге категорий угроз в России находятся на четвертом месте. Такая высокая позиция у этой категории угроз, кроме России, только в Средней Азии и Закавказье.

У этих двух категорий угроз динамика показателей в России очень схожая. Это объясняется тем, что 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.

Угроза майнеров актуальна для всех отраслей в регионе: Россия занимает не ниже четвертого места в рейтингах регионов по показателям майнеров обеих категорий во всех отраслях.

### **Программы-вымогатели**

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Россия занимает седьмое место среди регионов.

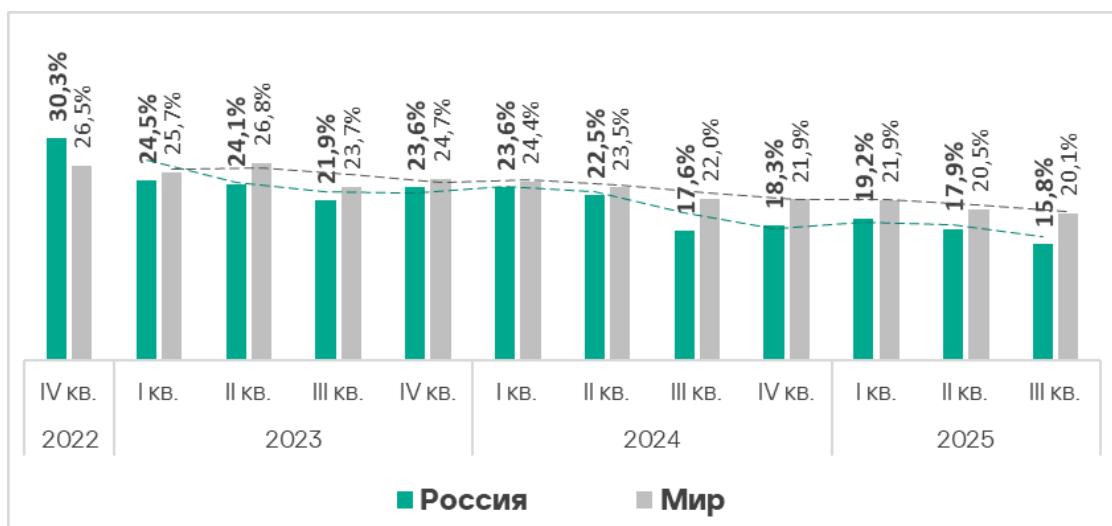
В третьем квартале 2025 года показатель этой угрозы в регионе заметно вырос, и по его росту Россия заняла второе место среди регионов.

Угроза актуальна для отраслей автоматизация зданий, нефть и газ и строительство. По показателю программ-вымогателей в автоматизации зданий Россия лидирует, в нефтегазовой отрасли и строительстве занимает второе место в соответствующих рейтингах регионов.

## **Статистика по всем угрозам**

Россия занимает 10-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

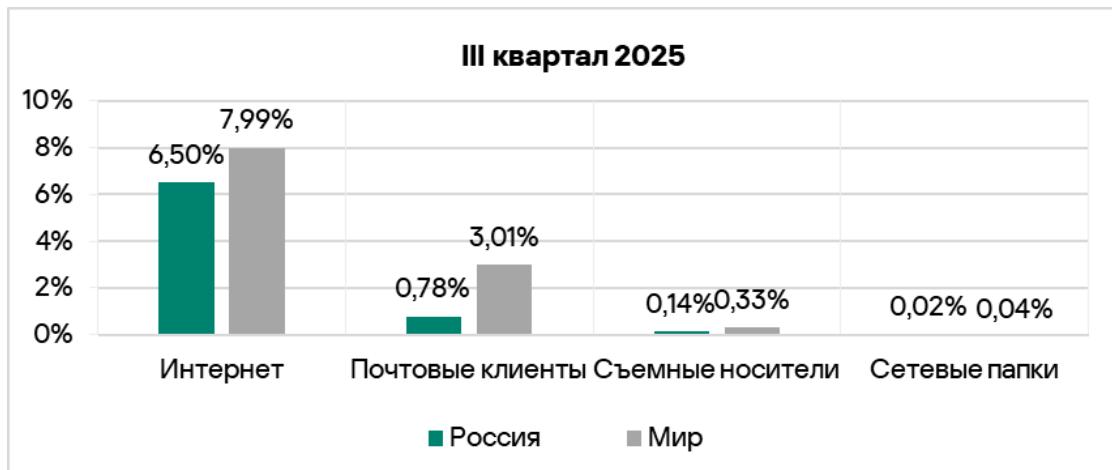
Показатель в регионе уменьшается второй квартал подряд. В третьем квартале 2025 года он оказался наименьшим за три года — 15,8%. Это в 1,7 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.



Значение этого показателя в регионе остается ниже среднемирового с начала 2023 года.

## Источники угроз

Значения доли компьютеров АСУ, на которых блокируются угрозы из разных источников, в России меньше среднемировых.



Показатель за квартал уменьшился у всех источников угроз.



## Интернет

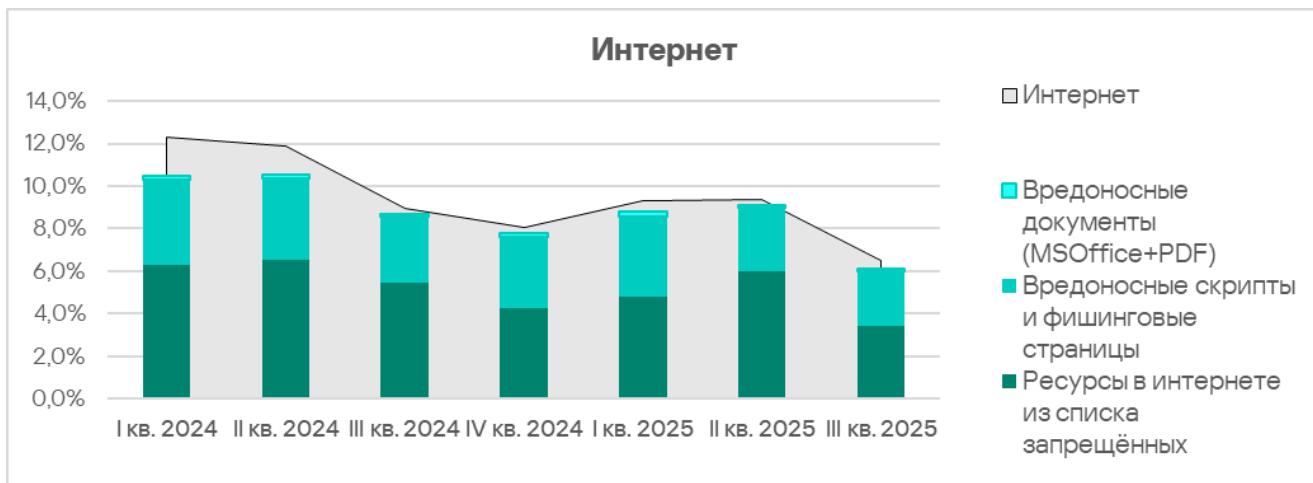
В рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Россия занимает 10-е место с 6,50%. По сравнению с регионом, который замыкает этот рейтинг, — Северной Европой, показатель в России выше в 1,4 раза.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, в России росла первые два квартала 2025 года. В третьем квартале показатель уменьшился на 2,87 п. п. до минимального за три года значения.

Отметим, что в третьем квартале 2025 года доля компьютеров АСУ, на которых блокируются угрозы из интернета, уменьшилась во всех регионах, но Россия занимает первое место по изменению этого показателя.

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

И вредоносные скрипты и фишинговые страницы, и вредоносные документы распространяются как в интернете, так и в почте. В отличие от вредоносных писем, вредоносные скрипты и фишинговые страницы в третьем квартале 2025 года распространялись в России преимущественно через интернет.

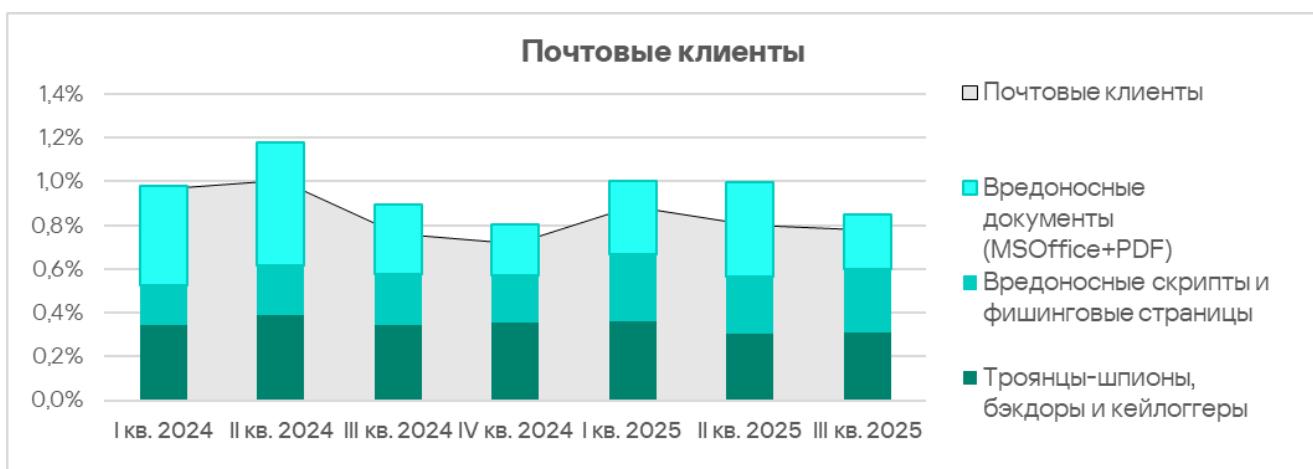


## Почтовые клиенты

Доля компьютеров АСУ, на которых блокируются угрозы в почтовых клиентах, в России в третьем квартале 2025 года оказалась наименьшей из всех регионов – 0,78%.

Основные категории угроз из почтовых клиентов, которые блокируются на компьютерах АСУ, – это шпионские программы, вредоносные скрипты и фишинговые страницы, вредоносные документы.

Для вредоносных документов и шпионских программ электронная почта – основной канал распространения. Вредоносные скрипты распространяются как в почте, так и в интернете. В третьем квартале 2025 года интернет был основным источником этой угрозы.

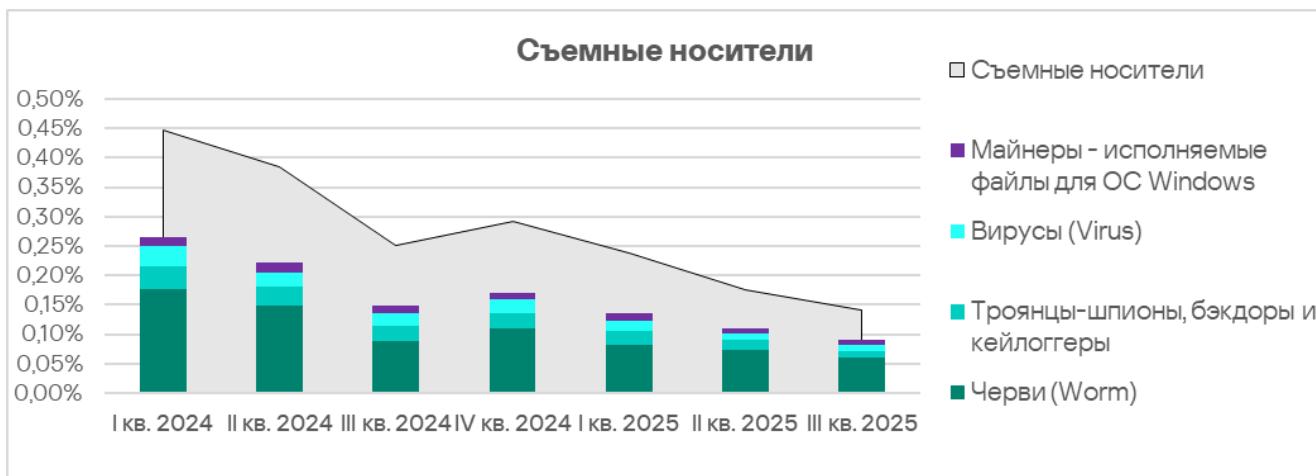


## Съемные носители

По доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, Россия находится на восьмом месте в соответствующем рейтинге регионов с 0,14%. Этот показатель в 2,8 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает рейтинг.

Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ: черви, шпионское ПО, вирусы и майнеры – исполняемые файлы для ОС Windows.

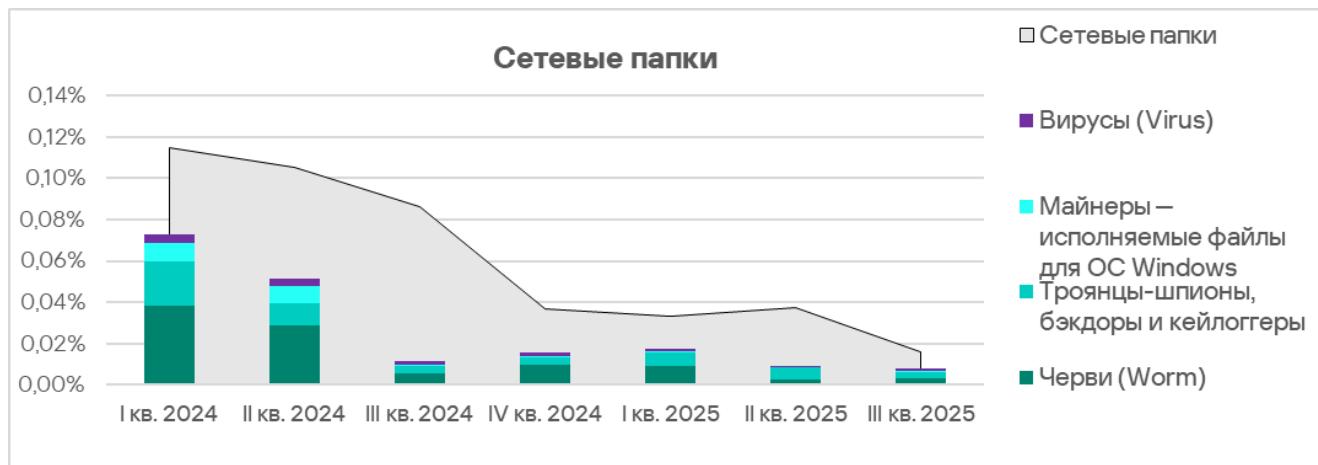
Для червей съемные носители – основной способ распространения.



## Сетевые папки

По доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, Россия занимает 10-е место в соответствующем рейтинге регионов с 0,016%. Этот показатель в 2,7 раза больше, чем в Северной Европе, где он наименьший из всех регионов.

Основные категории угроз, которые блокировались в сетевых папках в третьем квартале 2025 года: черви, шпионские программы, вирусы и майнеры – исполняемые файлы для ОС Windows.



## Категории угроз





В России у двух категорий угроз доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, выше среднемирового значения: ресурсы в интернете из списка запрещенных и майнеры – исполняемые файлы для ОС Windows.

Показатель первой категории соизмерим со среднемировым. Доля компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows, в 1,3 раза превышает среднемировое значение. Россия занимает второе место в рейтинге регионов по этому показателю.

За квартал показатель увеличился у трех категорий угроз: шпионские программы, программы-вымогатели и вирусы.

По росту показателей шпионских программ и программ-вымогателей в третьем квартале 2025 года Россия заняла второе место в соответствующих рейтингах регионов.

Больше всего за квартал уменьшился показатель категории ресурсы в интернете из списка запрещенных. Как и в случае угроз из интернета, по изменению (уменьшению) этого показателя Россия лидирует среди регионов – при том, что доля компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных, уменьшилась во всех регионах.

Несмотря на это, Россия занимает четвертое место в рейтинге регионов по доле компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных. Эта категория угроз сохранила лидирующую позицию в рейтинге категорий угроз внутри региона.

## Ресурсы в интернете из списка запрещенных

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Россия опустилась со второго на четвертое место.

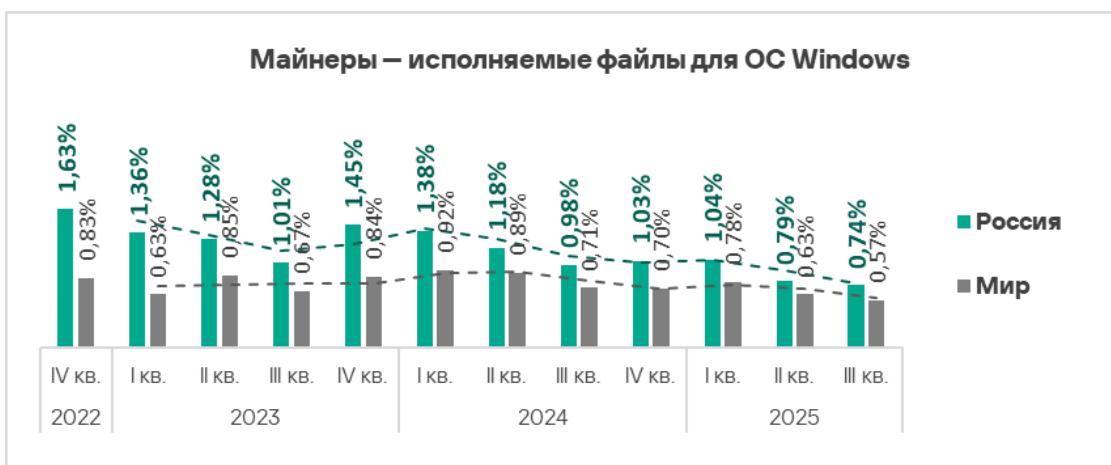
Ресурсы в интернете из списка запрещенных сохранили позицию лидера в рейтинге категорий угроз в регионе, несмотря на значительное уменьшение показателя в третьем квартале 2025 года – до 4,17%. Значение в России превышает показатель региона Австралия и Новая Зеландия, который замыкает соответствующий рейтинг, в 1,8 раза.



## Майнеры – исполняемые файлы для ОС Windows и черви

Среди регионов Россия находится на втором месте по доле компьютеров АСУ, на которых были заблокированы майнеры – исполняемые файлы для ОС Windows, уступая только Средней Азии и Закавказью.

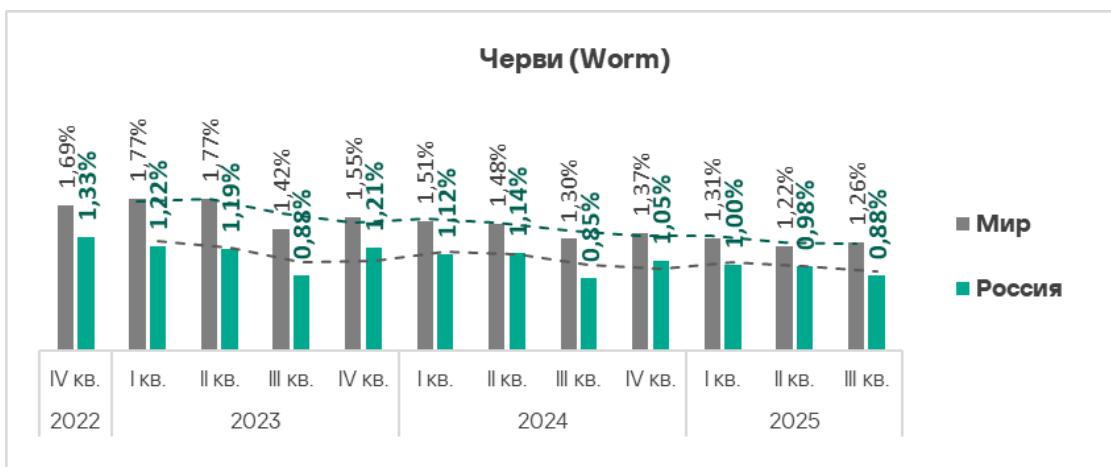
Показатель майнеров в формате исполняемых файлов для ОС Windows в России, как и во всех регионах, в третьем квартале 2025 года уменьшился. Значение в России оказалось минимальным за три года – 0,74%. Это в 5,7 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает соответствующий рейтинг.



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*.

Черви в третьем квартале 2025 года в рейтинге категорий угроз в регионе заняли четвертое место. На такой высокой позиции в региональном рейтинге эта категория угроз, кроме России, находится только в Средней Азии и Закавказье. В рейтинге регионов по этому показателю Россия на восьмом месте.

Показатель червей в России за квартал уменьшился до 0,88%. Это в 4 раза больше, чем в Северной Европе, где показатель наименьший.



Майнеры – исполняемые файлы для ОС Windows распространяются преимущественно через интернет, а также через съемные носители и сетевые папки, используя функциональность червей. Поэтому динамика показателей у майнеров – исполняемых файлов и червей в России схожая.

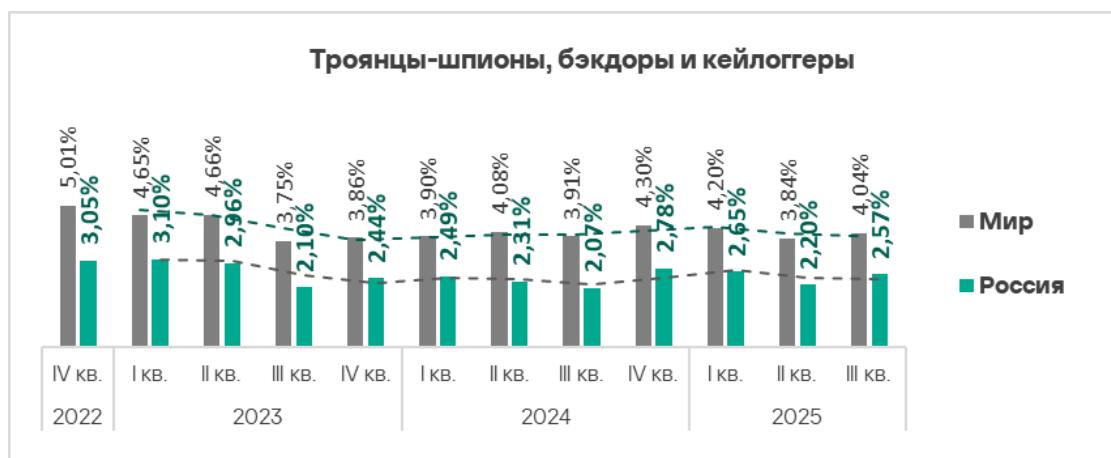


## Троянцы-шпионы, бэкдоры и кейлоггеры

По доле компьютеров АСУ, на которых блокируются шпионские программы, в третьем квартале Россия заняла 10-е место среди регионов.

Шпионские программы – одна из трех категорий угроз в регионе, показатель которой за квартал вырос. По его росту Россия заняла второе место в мире.

В России доля компьютеров АСУ, на которых блокируются шпионские программы (2,57%) – в 1,8 раза больше, чем в Северной Европе, где этот показатель наименьший среди регионов.



Распространяются шпионские программы через все источники угроз. Чаще всего – через почту и интернет.

## Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Россия занимает седьмое место среди регионов.

В третьем квартале 2025 года показатель этой угрозы в регионе заметно вырос — до 0,14%. По его росту Россия заняла второе место среди регионов.

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, в России в 2,8 раза превышает показатель в Северной Европе, которая замыкает соответствующий рейтинг.



В третьем квартале 2025 года программы-вымогатели распространялись в России через интернет и почту. Но в почтовых клиентах эти угрозы блокировались вдвое чаще, чем из интернета.

## Отрасли

В России из всех рассмотренных в отчете отраслей и ОТ-инфраструктур чаще всего вредоносные объекты блокируются в биометрических системах.

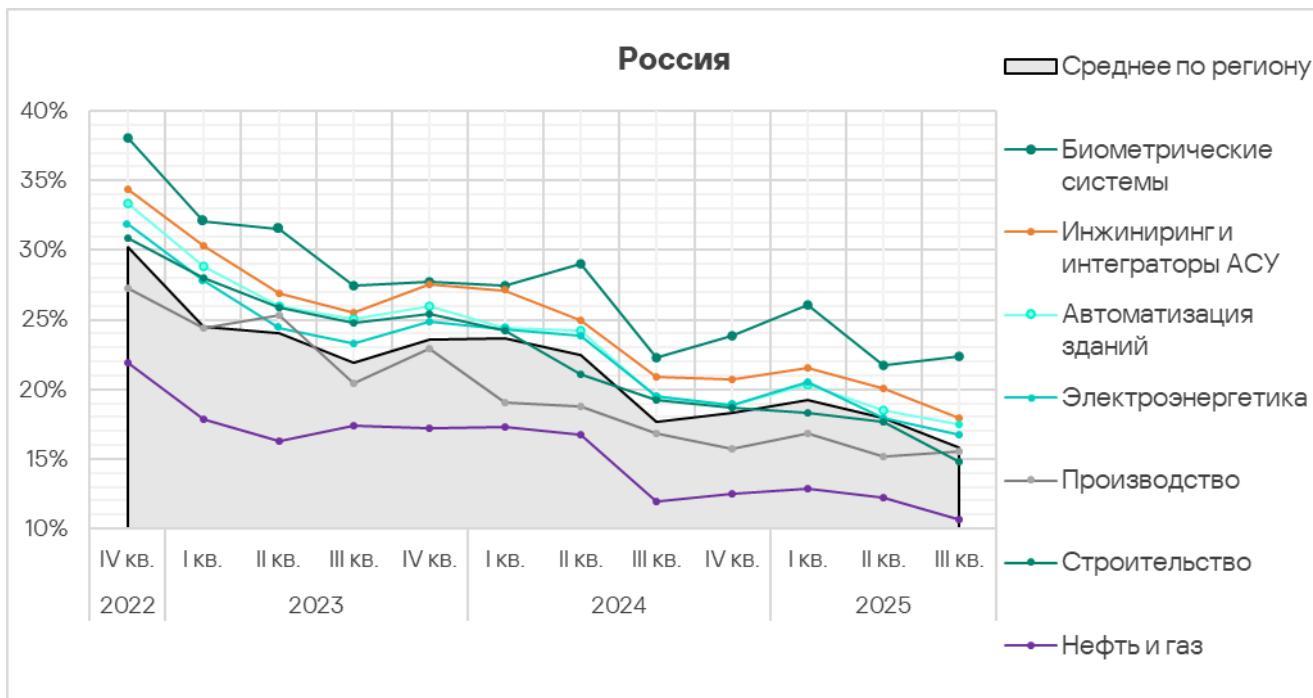
Во всех отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, ниже соответствующих среднемировых показателей.



В третьем квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась во всех рассмотренных отраслях региона, кроме ОТ-инфраструктуры биометрические системы и производства.



Во всех рассмотренных отраслях показатели с периодическими колебаниями постепенно снижаются.



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

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

### Показатели источников угроз в отраслях в России, III квартал 2025 года

Отрасль / Источник угрозы	Биометрические системы	Автоматизация зданий	Электроэнергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Интернет	8,10%	6,76%	7,64%	7,91%	4,06%	7,05%	5,24%	6,50%
Почтовые клиенты	2,70%	1,84%	1,18%	0,88%	0,88%	0,66%	0,69%	0,78%
Съемные носители	0,31%	0,21%	0,38%	0,19%	0,20%	0,43%	0,28%	0,14%
Сетевые папки	0,08%	0,03%	0,05%	0,02%	0,05%	0,04%	0,05%	0,02%
Показатель отрасли в регионе	22,36%	17,46%	16,74%	17,97%	10,62%	14,80%	15,57%	

### Показатели категорий угроз в отраслях в России, III квартал 2025 года

Отрасль / Категории вредоносного ПО	Биометрические системы	Автоматизация зданий	Электро-энергетика	Инжиниринг и интеграторы АСУ	Нефть и газ	Строительство	Производство	Показатель категорий в регионе
Ресурсы в интернете из списка запрещенных	5,01%	4,49%	5,66%	5,03%	3,08%	4,75%	3,48%	4,17%
Вредоносные скрипты и фишинговые страницы	5,78%	4,41%	4,27%	4,39%	2,72%	4,08%	3,15%	3,77%
Троянцы-шпионы, бэкдоры и кейлоггеры	5,86%	3,89%	3,02%	2,76%	1,69%	2,32%	3,06%	2,57%
Черви (Worm)	2,24%	1,21%	1,49%	0,93%	1,23%	1,01%	1,21%	0,88%
Майнеры - исполняемые файлы для ОС Windows	0,93%	0,92%	1,38%	0,99%	0,64%	1,18%	0,59%	0,74%
Вредоносные документы (MSOffice + PDF)	2,08%	1,27%	1,11%	0,78%	0,81%	0,78%	0,90%	0,59%
Вирусы (Virus)	0,69%	0,46%	0,88%	0,48%	0,58%	0,68%	0,95%	0,30%
Программы-вымогатели	0,39%	0,57%	0,14%	0,12%	0,14%	0,24%	0,12%	0,14%
Веб-майнеры, выполняемые в браузерах	0,46%	0,37%	0,74%	0,36%	0,26%	0,63%	0,28%	0,22%
Вредоносные программы для AutoCAD	0,00%	0,03%	0,08%	0,05%	0,11%	0,26%	0,19%	0,02%
<b>Показатель отрасли в регионе</b>	<b>22,36%</b>	<b>17,46%</b>	<b>16,74%</b>	<b>17,97%</b>	<b>10,62%</b>	<b>14,80%</b>	<b>15,57%</b>	

Для всех отраслей основной источник угроз – интернет. Как следствие, актуальны такие категории угроз как опасные ссылки из списка запрещенных, вредоносные скрипты и фишинговые страницы и программы-шпионы, которые распространяются через этот источник угроз.

Для всех отраслей актуальна угроза майнеров: Россия занимает не ниже четвертого места в рейтингах регионов по показателям майнеров обеих категорий во всех отраслях.

В отраслях автоматизация зданий, нефть и газ и в отрасли строительство высокие показатели программ-вымогателей. По этому показателю в отрасли автоматизация зданий Россия лидирует, в нефтегазовой отрасли и строительство – занимает второе место в соответствующих рейтингах регионов.

#### Биометрические системы

Россия находится на восьмом месте в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в ОТ-инфраструктуре биометрические системы.

Среди регионов по показателям ОТ-инфраструктуры биометрические системы Россия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и майнерах обеих категорий.

Среди отраслей в регионе ОТ-инфраструктура биометрические системы занимает:

- первое место по показателям всех источников угроз, кроме съемных носителей;
- третье место по показателю съемных носителей;
- первое место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, черви;
- второе место по показателю программ-вымогателей;
- третье место по показателям следующих категорий: ресурсы в интернете из списка запрещенных, вирусы и веб-майнера.

### **Инжиниринг и интеграторы АСУ**

Россия находится на девятом 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 Россия занимает:

- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных;
- третье место по доле компьютеров АСУ, на которых блокируются майнера – исполняемые файлы для ОС Windows;
- пятое место по показателю веб-майнеров.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- второе место по угрозам из интернета;
- второе место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных;
- третье место по показателям следующих категорий: вредоносные скрипты и фишинговые страницы, майнера – исполняемые файлы для ОС Windows.

### **Автоматизация зданий**

Россия находится на 10-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в отрасли автоматизация зданий.

В глобальном рейтинге по индустриям во всех регионах автоматизация зданий в России занимает:

- второе место по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели.

Среди регионов по показателям отрасли Россия занимает:

- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и программы-вымогатели;
- второе место по доле компьютеров АСУ, на которых блокируются майнеры – исполняемые файлы для ОС Windows;
- третье место по показателю веб-майнеров.

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по угрозам из почты;
- первое место по доле компьютеров АСУ, на которых блокируются программы-вымогатели;
- второе место по показателям следующих категорий угроз: вредоносные скрипты и фишинговые страницы, шпионское ПО, вредоносные документы.

## Электроэнергетика

Россия находится на девятом месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в электроэнергетической отрасли.

В глобальном рейтинге по индустриям во всех регионах электроэнергетика в России занимает:

- третье место по доле компьютеров АСУ, на которых были заблокированы веб-майнеры.

Среди регионов по показателям в отрасли Россия занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокируются майнеры обеих категорий;

- четвертое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных.

Среди отраслей в регионе электроэнергетика занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях;
- третье место по показателям угроз из интернета, почтовых клиентов и в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных и майнерах обеих категорий;
- второе место по показателям червей и вирусов;
- третье место по показателю вредоносных документов.

### Производство

Россия находится на седьмом месте по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в производственной отрасли.

Среди регионов по показателям в отрасли Россия занимает:

- третье место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- третье место по доле компьютеров АСУ, на которых блокируются майнерах обеих категорий.

Среди отраслей в регионе производство занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- первое место по доле компьютеров АСУ, на которых блокируются вирусы;
- второе место по показателю вредоносных программ для AutoCAD;
- третье место по показателю шпионских программ.

### Строительство

Россия находится на 10-м месте среди регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в строительной отрасли.

Среди регионов по показателям в отрасли Россия занимает:

- второе место по доле компьютеров АСУ, на которых блокируются майнера — исполняемые файлы для ОС Windows и программы-вымогатели;

- четвертое место по доле компьютеров АСУ, на которых блокируются веб-майнеры.

Среди отраслей в регионе строительство занимает:

- первое место по доле компьютеров АСУ, на которых блокируются угрозы на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокируются вредоносные программы для AutoCAD;
- второе место по показателям майнеров обеих категорий;
- третье место по показателю программ-вымогателей.

## Нефть и газ

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

Среди регионов по показателям в отрасли Россия занимает:

- второе место по доле компьютеров АСУ, на которых блокируются угрозы в сетевых папках;
- третье место по показателю почтовых клиентов;
- второе место по доле компьютеров АСУ, на которых блокируются программы-вымогатели;
- четвертое место по показателям следующих категорий угроз: вредоносные документы, майнеры обеих категорий, черви и вредоносные программы для AutoCAD.

Среди отраслей в регионе нефтегазовая отрасль занимает:

- третье место по доле компьютеров АСУ, на которых блокируются черви и вредоносные программы 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<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)