Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Россия. Четвертый квартал 2025 года

23.04.2026

Версия 1.0

Россия

Актуальные угрозы

В рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, Россия занимает 10-е место. При этом регион находится на более высоких позициях в рейтингах по показателям угроз следующих категорий:

- майнеры – исполняемые файлы для ОС Windows – второе место;
- ресурсы в интернете из списка запрещенных – третье место;
- веб-майнеры – четвертое место;
- шпионские программы, вирусы и программы-вымогатели – девятое место.

Среди источников угроз выбиваются съемные носители: в рейтинге регионов по доле компьютеров АСУ, на которых блокировались угрозы при подключении съемных носителей, Россия находится на восьмом месте.

Основной источник угроз в России — интернет

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

Ресурсы в интернете из списка запрещенных

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 (C2). 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).

По доле компьютеров АСУ, на которых блокируются ресурсы из списка запрещенных в исследуемых отраслях, Россия среди регионов находится:

- на первом месте по показателю в автоматизации зданий;
- на втором месте по показателю в биометрических системах;
- на третьем месте по показателю в электроэнергетике.

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

Майнеры в отраслях

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, кроме производства. По показателям в производственной отрасли Россия находится на третьем месте в рейтинге по майнерам – исполняемым файлам и на четвертом – по веб-майнерам.

Программы-вымогатели

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

Угроза актуальна для всех отраслей. В рейтингах регионов по доле компьютеров АСУ, на которых блокируются программы-вымогатели в исследуемых отраслях, Россия занимает не ниже шестого места.

В рейтинге регионов по доле атакованных компьютеров в инфраструктуре биометрических систем в четвертом квартале 2025 года Россия находится на втором месте, в рейтингах регионов по показателю в электроэнергетической и нефтегазовой отраслях — на третьем.

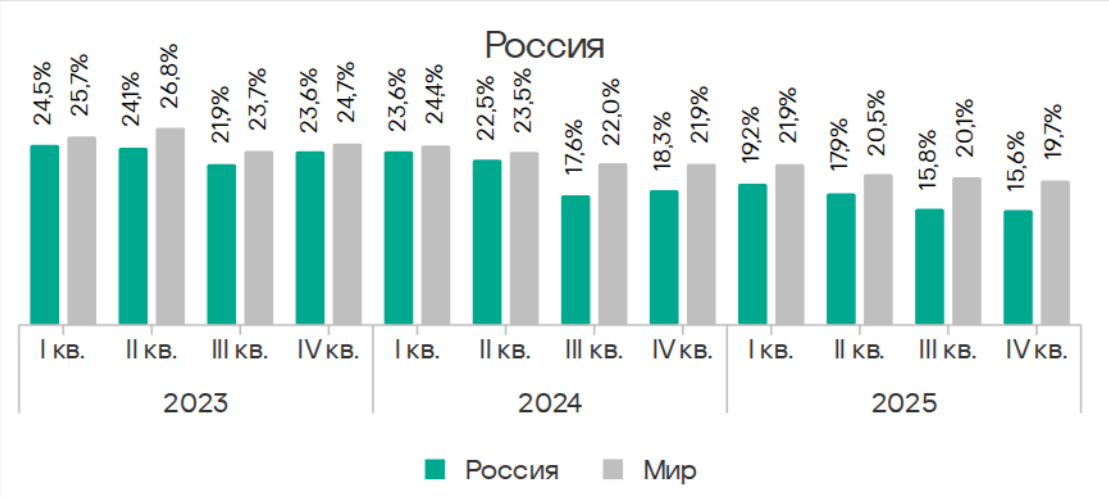
Угрозы на съемных носителях

По доле компьютеров АСУ, на которых угрозы блокируются при подключении съемных носителей, Россия занимает восьмое место среди регионов.

Статистика по всем угрозам

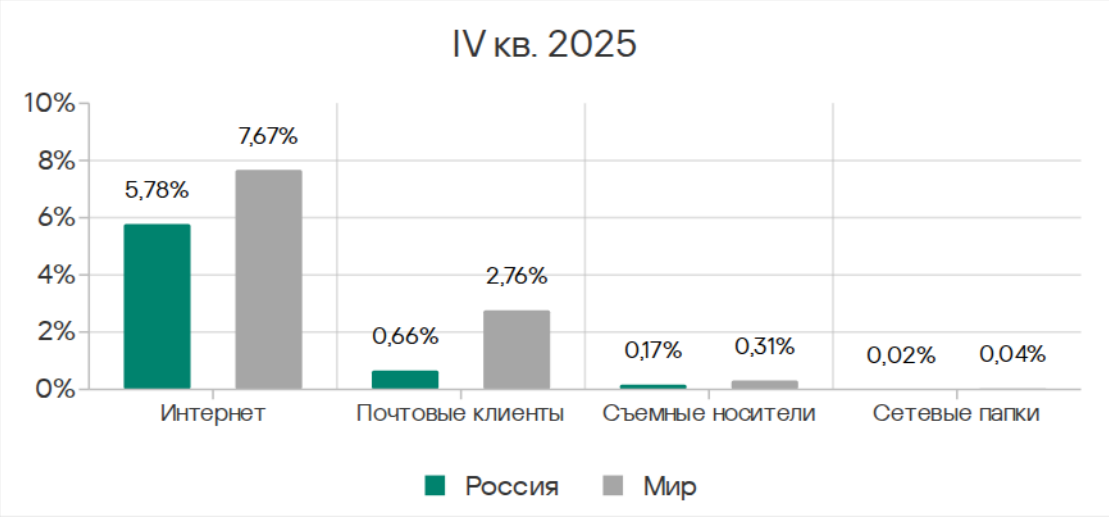
Россия занимает 10-е место в рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Показатель в регионе ниже среднемирового и уменьшается третий квартал подряд. В четвертом квартале 2025 года он оказался наименьшим за исследуемый период — 15,6%. Это в 1,8 раза больше, чем в Северной Европе, которая замыкает соответствующий рейтинг регионов.

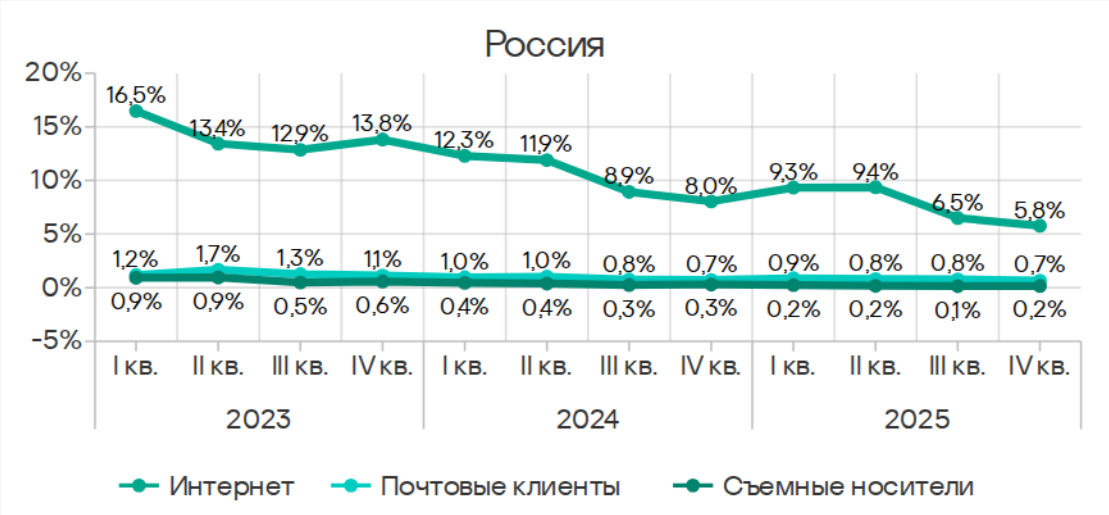


Источники угроз

В России доля компьютеров АСУ, на которых блокируются угрозы из разных источников, меньше среднемировых показателей у всех источников угроз.



Из всех источников угроз показатель за квартал увеличился только у съемных носителей.



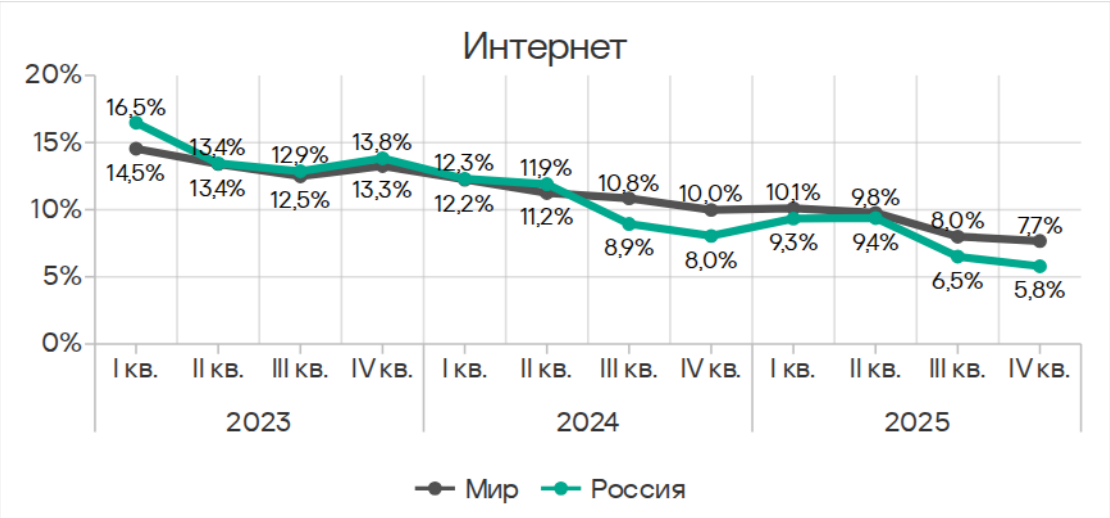
В рейтингах по доле компьютеров АСУ, на которых блокируются угрозы из разных источников, самая высокая позиция у России по показателю съемных носителей – регион занимает восьмое место.

Интернет

В рейтинге регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, Россия занимает 12-е место с 5,78%.

По сравнению с Северной Европой, которая замыкает этот рейтинг, показатель в России выше в 1,5 раза.

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, в России росла первые два квартала 2025 года и снижалась в третьем и четвертом кварталах. В четвертом квартале показатель оказался наименьшим за исследуемый период.



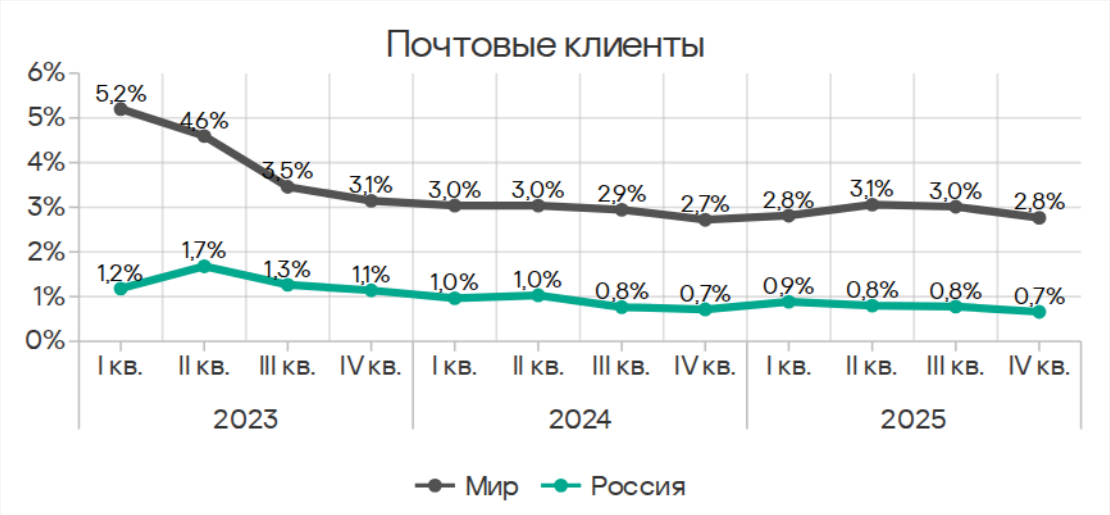
Основные категории угроз из интернета, которые блокируются на компьютерах АСУ: ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы.

По доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, Россия находится на третьем месте в соответствующем рейтинге регионов.

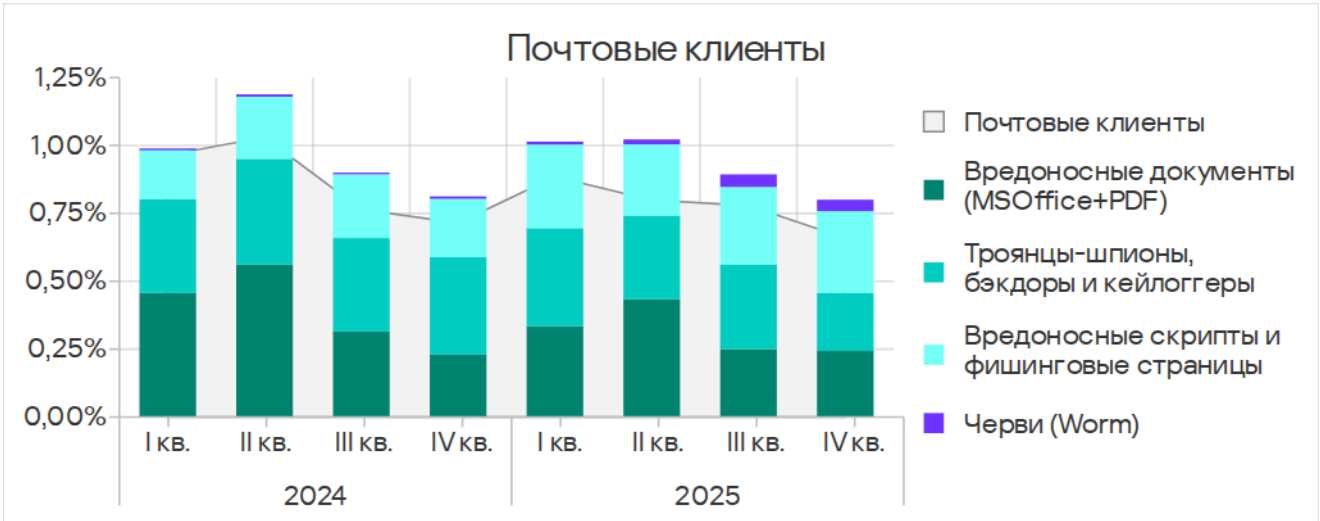
Вредоносные скрипты и фишинговые страницы распространяются как в интернете, так и в почте. В России в четвертом квартале 2025 года их источником был преимущественно интернет.

Почтовые клиенты

По доле компьютеров АСУ, на которых блокируются угрозы из почтовых клиентов, в четвертом квартале 2025 года Россия находится на предпоследнем, 13-м, месте с показателем 0,66%. Это значение чуть выше, чем в Северной Европе, где оно наименьшее из всех регионов.



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



Для вредоносных документов и шпионских программ электронная почта — основной канал распространения. Вредоносные скрипты

распространяются как в почте, так и в интернете. В четвертом квартале 2025 года интернет был основным источником этой угрозы.

В четвертом квартале 2025 года увеличилась доля компьютеров АСУ, на которых блокировались черви из почтовых клиентов. Это связано с очередной волной фишинговых кампаний, известных как Curriculum-vitae-catalina, атакам подверглись организации во всех регионах мира. В России пик атак пришелся на октябрь.

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

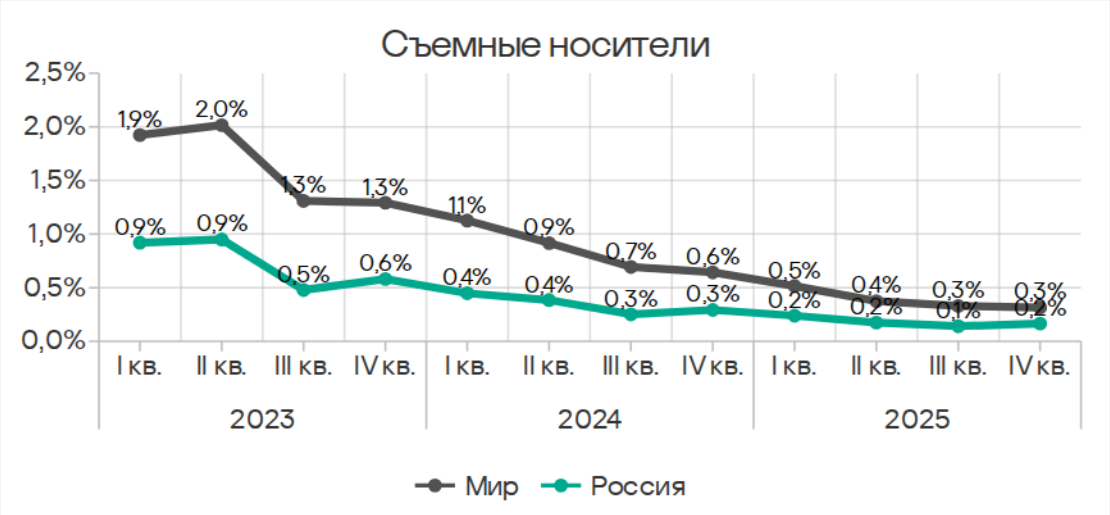
Как правило, такие кампании направлены на доставку вредоносного ПО для кражи данных, программ-шпионов или инструментов для удаленного управления (RAT).

Доля компьютеров АСУ, на которых блокировались черви, выросла во всех регионах, по росту этого показателя Россия на восьмом месте. В России, в отличие от остальных регионов, основным источником червей в четвертом квартале остались съемные носители, хотя в почте этой угрозы стало заметно больше.

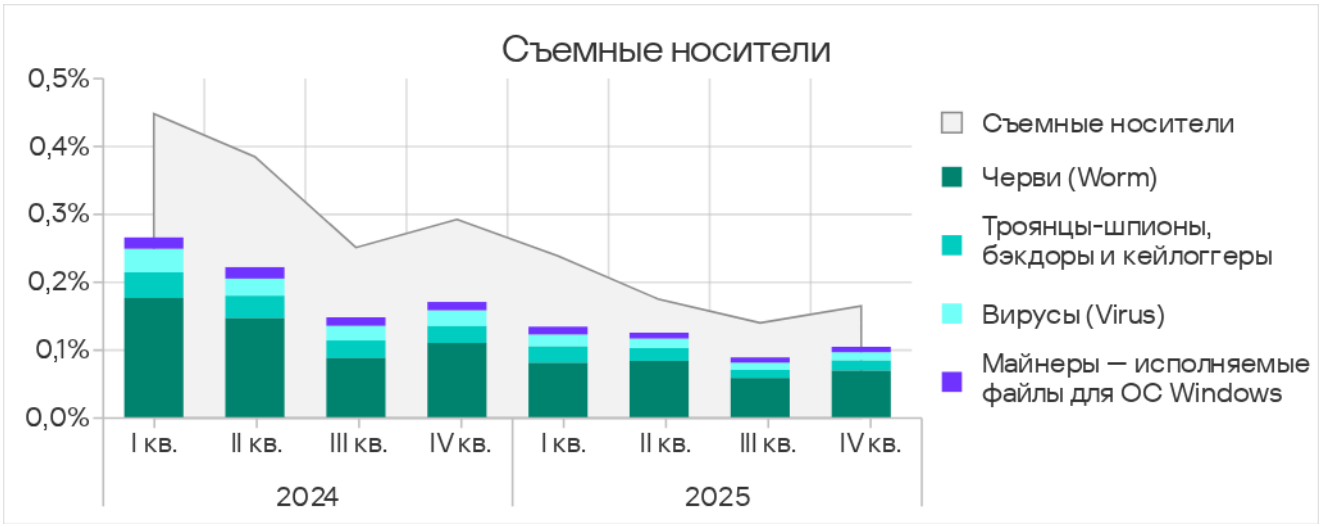
Съемные носители

По доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, Россия находится на восьмом месте в соответствующем рейтинге регионов. Эта самая высокая позиция региона в рейтингах по источникам угроз.

В четвертом квартале 2025 года показатель в Росси вырос до 0,17%. Это в 3,4 раза больше, чем в регионе Австралия и Новая Зеландия, который замыкает рейтинг.



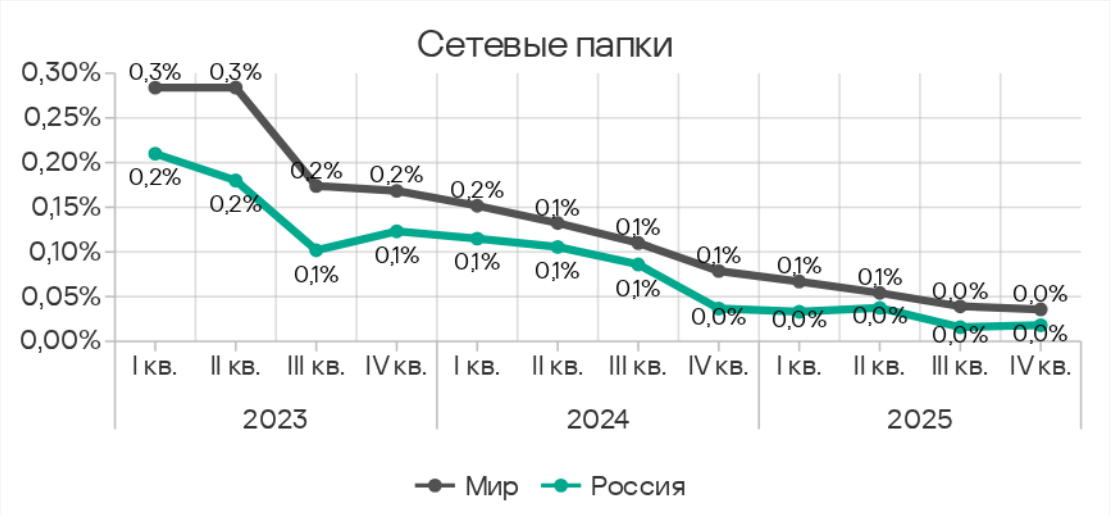
Основные категории угроз, которые блокируются в регионе при подключении съемных устройств к компьютерам АСУ: черви, шпионское ПО, вирусы и майнеры — исполняемые файлы для ОС Windows.



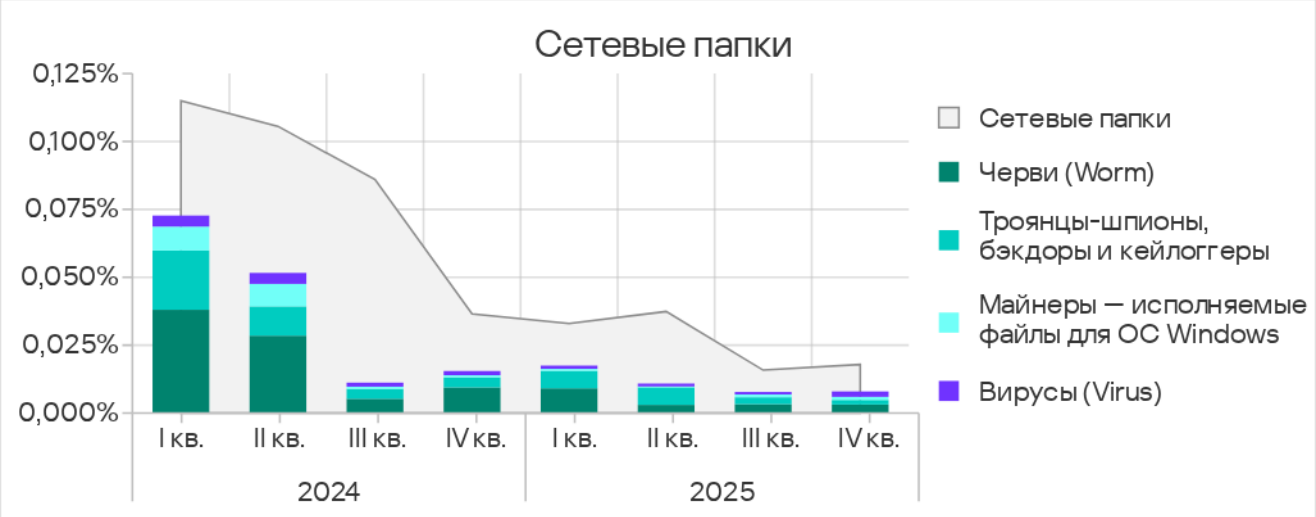
Для червей съемные носители — основной канал распространения. В отличие от остальных регионов, где из-за фишинговой кампании на компьютерах АСУ блокировалось больше червей из почтовых клиентов, чем на съемных носителях, в России съемные носители остались основным источником червей.

Сетевые папки

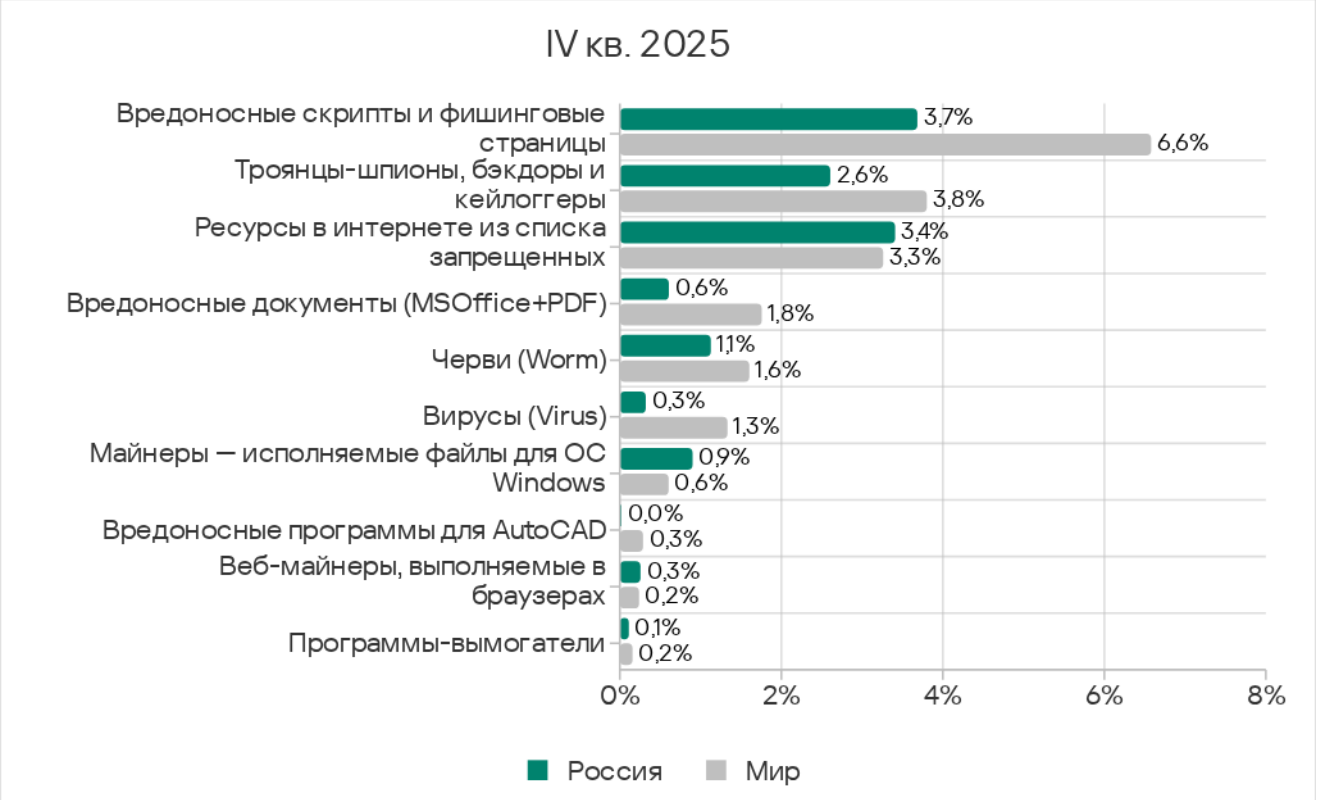
По доле компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, Россия занимает 11-е место в соответствующем рейтинге регионов с 0,018%. Этот показатель в 2,6 раза больше, чем в Северной Европе, где он наименьший из всех регионов.



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



Категории угроз



В России доля компьютеров АСУ, на которых были заблокированы вредоносные объекты трех категорий, выше среднемирового значения:

- ресурсы в интернете из списка запрещенных, третье место среди регионов по доле компьютеров АСУ, на которых блокировалась эта угроза,
- майнеры — исполняемые файлы для ОС Windows – в 1,5 раза, второе место среди регионов по этому показателю;
- веб-майнеры – в 1,1 раза, четвертое место среди регионов по этому показателю.

За квартал показатель увеличился у червей, майнеров обеих категорий, шпионских программ, вредоносных документов и вирусов.

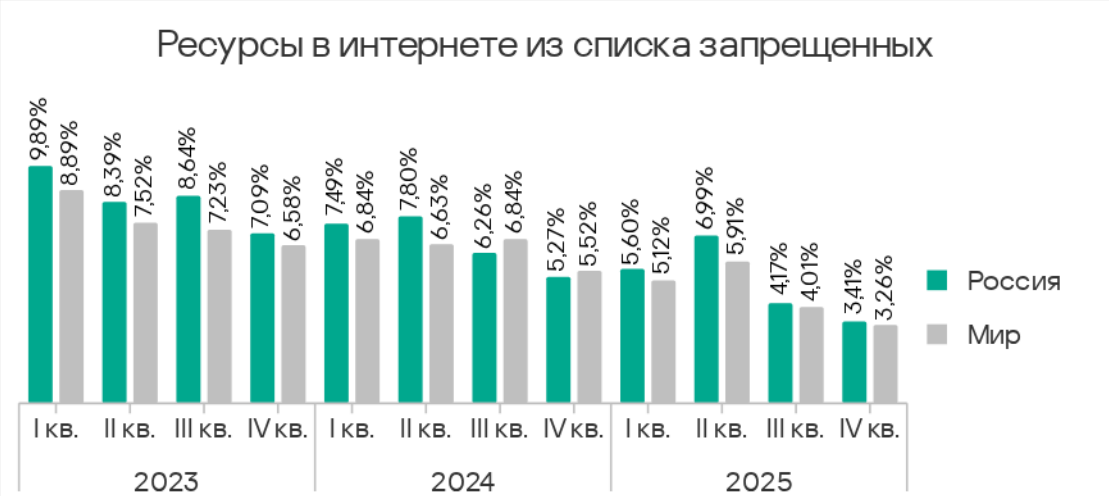
По росту показателя майнеров в формате исполняемых файлов Россия находится на первом месте среди регионов.

Ресурсы в интернете из списка запрещенных

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в четвертом квартале 2025 года Россия поднялась с четвертого на третье место.

В то же время в региональном рейтинге категорий угроз ресурсы в интернете из списка запрещенных уступили первое место вредоносным скриптам и фишинговым страницам, хотя по показателю скриптов Россия находится на 13-м месте в соответствующем рейтинге регионов.

Доля компьютеров АСУ, на которых блокируются ресурсы в интернете из списка запрещенных, в России, как и во всех регионах мира, постепенно снижается. В четвертом квартале показатель в России — 3,41% — в 2,0 раза больше, чем в Северной Европе, которая замыкает рейтинг.



Среди исследуемых отраслей в регионе наибольший показатель угрозы категории ресурсы в интернете из списка запрещенных — у электроэнергетики.

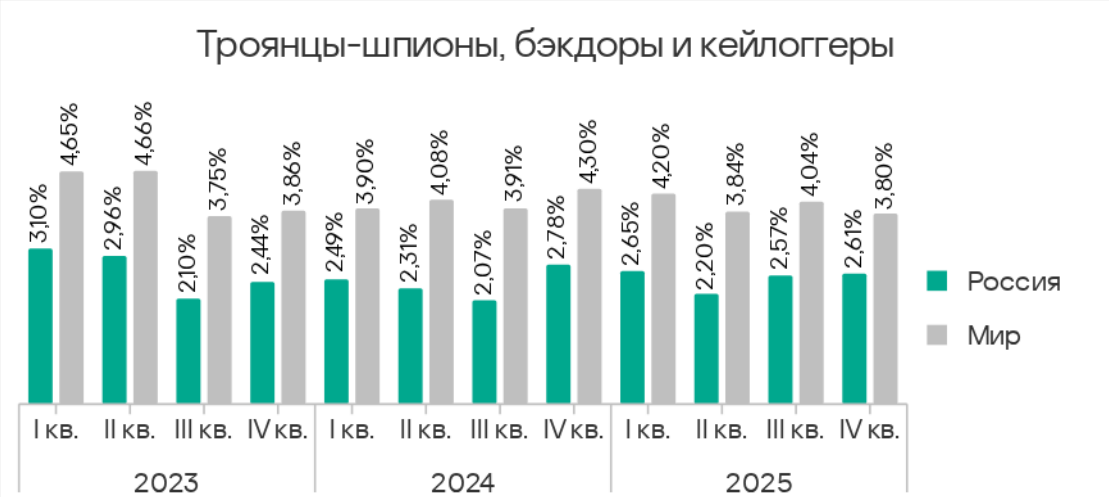
По доле компьютеров АСУ, на которых блокируются ресурсы из списка запрещенных в различных отраслях, Россия среди регионов находится:

- на первом месте по показателю в автоматизации зданий;
- на втором месте по показателю в биометрических системах;
- на третьем месте по показателю в электроэнергетике.

Троянцы-шпионы, бэкдоры и кейлоггеры

По доле компьютеров АСУ, на которых блокируются шпионские программы, в четвертом квартале 2025 года Россия заняла девятое место среди регионов.

Доля компьютеров АСУ, на которых блокируются шпионские программы, в России выросла до 2,61%. Этот показатель в 2,1 раза больше, чем в Северной Европе, где он наименьший среди регионов.



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

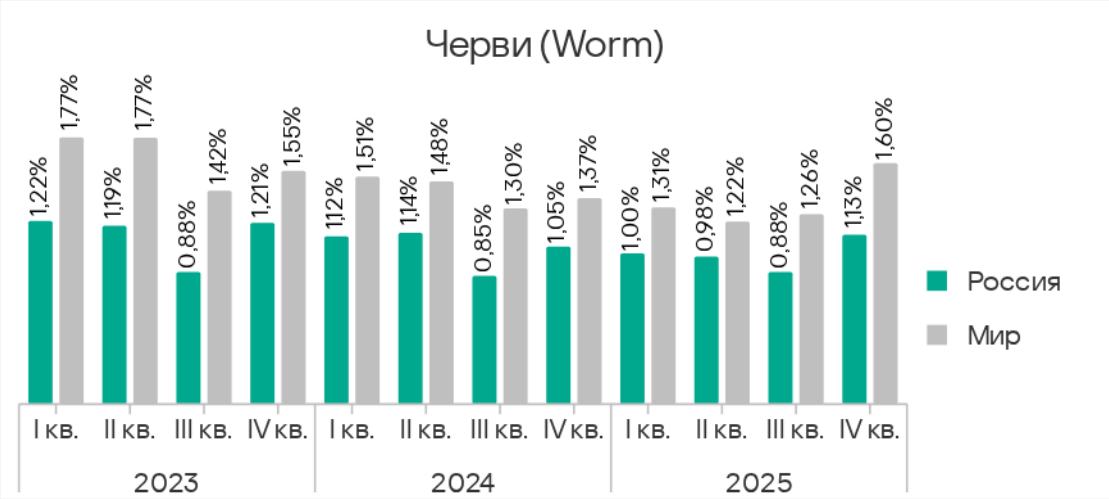
Россия — один из двух регионов, где показатель шпионских программ за квартал вырос.

Доля компьютеров АСУ, на которых блокируются шпионские программы, увеличилась в четырех из исследуемых отраслей региона: нефтегазовой, строительстве, электроэнергетике и отрасли инжиниринг и интеграторы АСУ. По росту показателя на первом месте находится нефтегазовая отрасль.

Черви

В России в региональном рейтинге категорий угроз черви занимают четвертое место. Кроме России на такой высокой позиции в региональных рейтингах черви находятся только в Африке, Южной Азии и в Средней Азии и Закавказье.

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются черви, Россия занимает 10-е место. Показатель в России — 1,13% — в 3,5 раза больше, чем в Северной Европе, где он наименьший среди регионов.



Для червей съемные носители — основной канал распространения.

В четвертом квартале 2025 года показатель червей вырос во всех регионах вследствие массовых фишинговых атак Curriculum-vitae-catalina, о которых мы рассказывали выше. В отличие от остальных регионов, где из-за фишинговых кампаний на компьютерах АСУ блокировалось больше червей из почтовых клиентов, чем на съемных носителях, в России съемные носители остались основным источником червей.

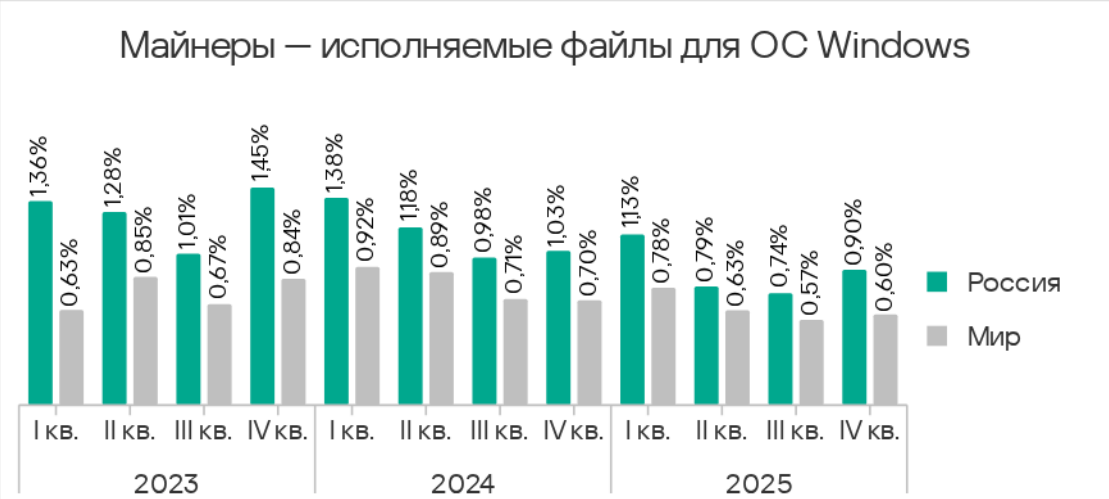
Доля компьютеров АСУ, на которых блокируются черви, выросла во всех исследуемых отраслях региона, кроме производства и инфраструктуры биометрических систем. Лидер по росту этого показателя – автоматизация зданий.

Майнеры — исполняемые файлы для ОС Windows

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

Россия – один из четырех регионов, где выросла доля компьютеров АСУ, на которых блокируются майнеры этой категории. По росту показателя Россия находится на первом месте.

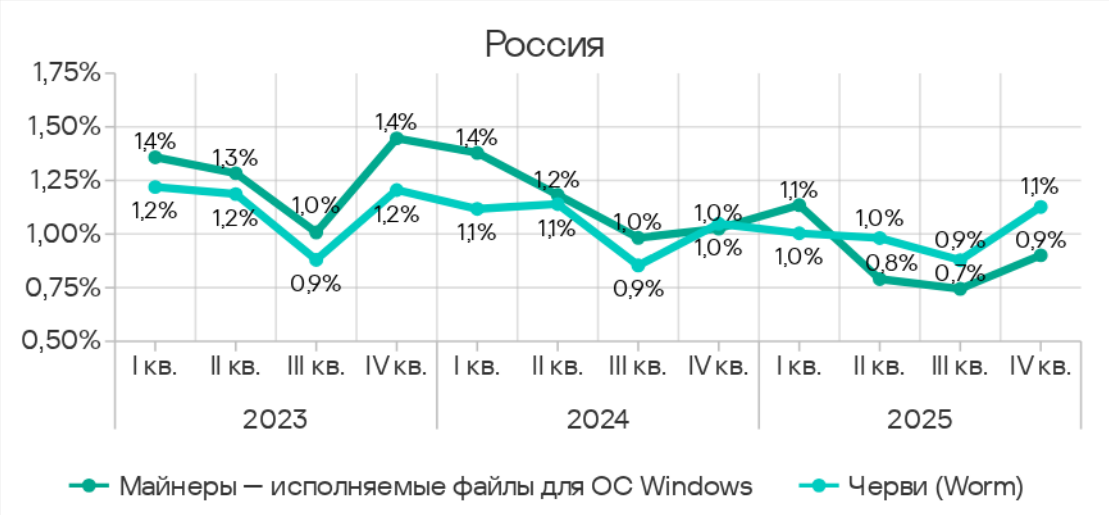
Показатель майнеров в формате исполняемых файлов для ОС Windows в России в четвертом квартале 2025 года увеличился до 0,90%. Это значение в 6,4 раза больше, чем в Северной Америке (Канаде), где оно наименьшее среди регионов.



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы, выросла во всех исследуемых отраслях региона. По росту показателя лидируют производство и электроэнергетика.

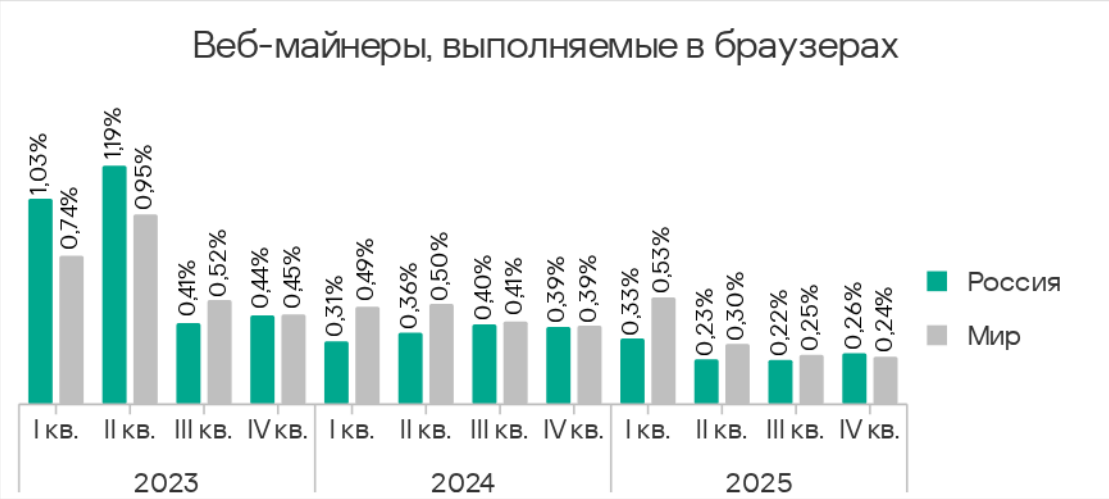
В России майнеры для ОС Windows активно используют модули и компоненты, которые по сути являются червями и служат для доставки майнера на другие компьютеры в сети – автоматизированный lateral movement.

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.



Веб-майнеры

По доле компьютеров АСУ, на которых блокируются веб-майнеры, Россия находится на четвертом месте среди регионов с 0,26%. Этот показатель в 4,3 раза превышает показатель в Восточной Азии, которая замыкает соответствующий рейтинг.

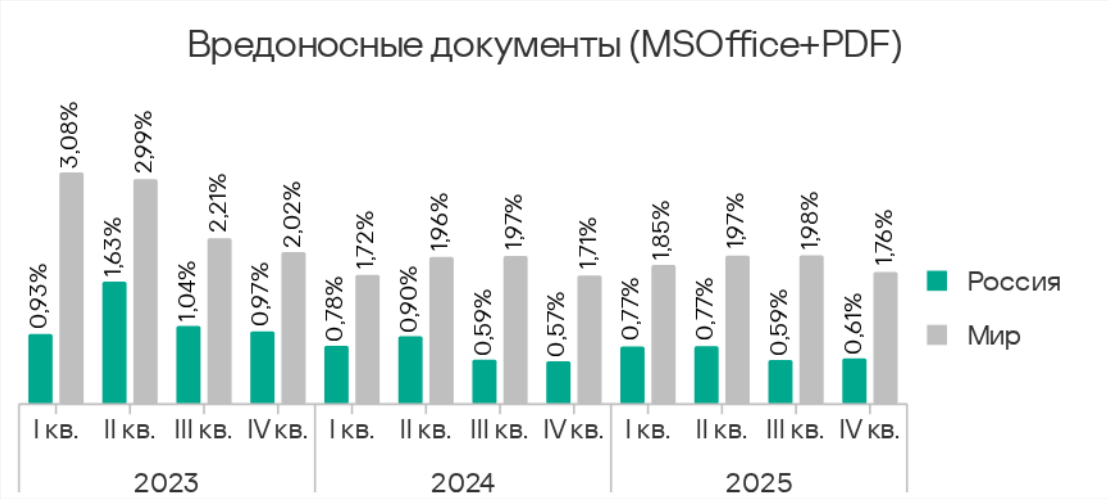


Россия – один из трех регионов, где в четвертом квартале 2025 года доля компьютеров АСУ, на которых блокируются веб-майнеры, увеличилась.

Показатель этой угрозы вырос в четырех из исследуемых отраслей региона – производственной, нефтегазовой, автоматизации зданий, а также инфраструктуры биометрических систем. По росту показателя на первом месте находится производство.

Вредоносные документы

В рейтинге регионов по доле компьютеров АСУ, на которых блокируются вредоносные документы, Россия занимает 13-е место с 0,61%. Этот показатель в 1,3 раза превышает показатель в Северной Европе, которая замыкает соответствующий рейтинг.



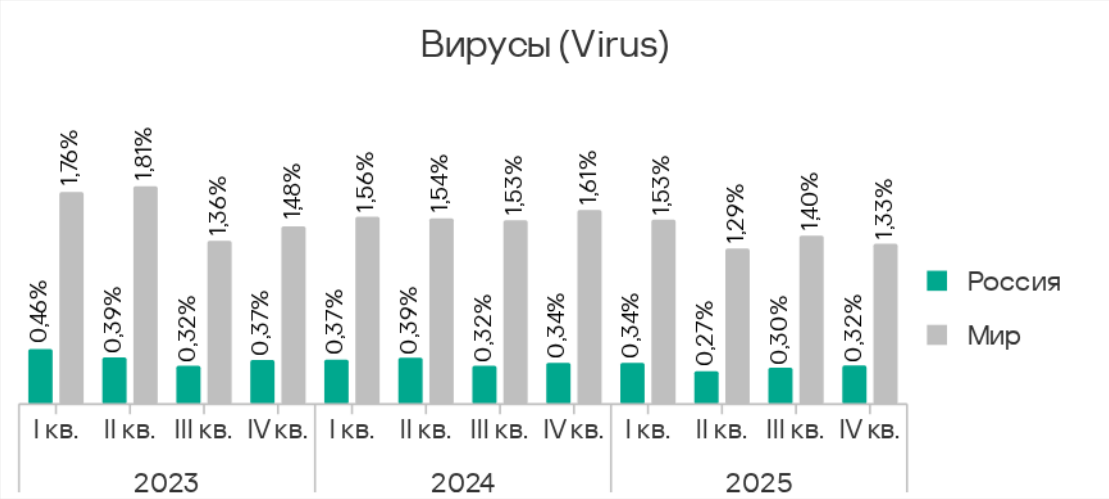
Россия – один из трех регионов, где доля компьютеров АСУ, на которых блокируются вредоносные документы, за квартал увеличилась.

Показатель вырос в двух из исследуемых отраслей региона – нефтегазовой и электроэнергетике.

Основные источники вредоносных документов – почтовые клиенты (преимущественно) и интернет.

Вирусы

По доле компьютеров АСУ, на которых блокируются вирусы, Россия занимает девятое место среди регионов с 0,14%. Этот показатель в 2,1 раза больше показателя в Западной Европе, которая замыкает соответствующий рейтинг регионов.



Россия – один из четырех регионов, где в четвертом квартале 2025 года доля компьютеров АСУ, на которых блокируются вирусы, увеличилась.

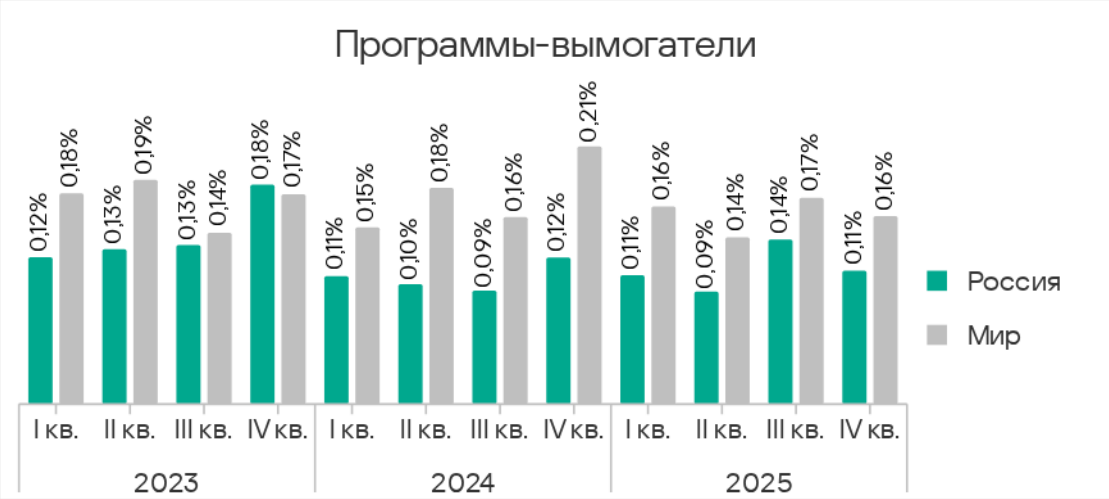
Показатель вирусов вырос во всех исследуемых отраслях региона, кроме строительства и производства. Лидирует по его росту инфраструктура биометрических систем.

В четвертом квартале 2025 года вирусы распространялись в России через все источники, чаще всего – через интернет.

Программы-вымогатели

По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Россия занимает девятое место среди регионов с 0,11%. Это значение в 2,2 раза превышает показатель в Северной Европе, которая замыкает соответствующий рейтинг.

Показатель в регионе колеблется. После роста в третьем квартале 2025 года, в четвертом квартале он уменьшился.



В рейтингах регионов по доле компьютеров АСУ, на которых блокируются программы-вымогатели в исследуемых отраслях, Россия занимает не ниже шестого места. По показателям в инфраструктуре биометрических систем Россия находится на втором месте, в электроэнергетической и нефтегазовой отраслях — на третьем.

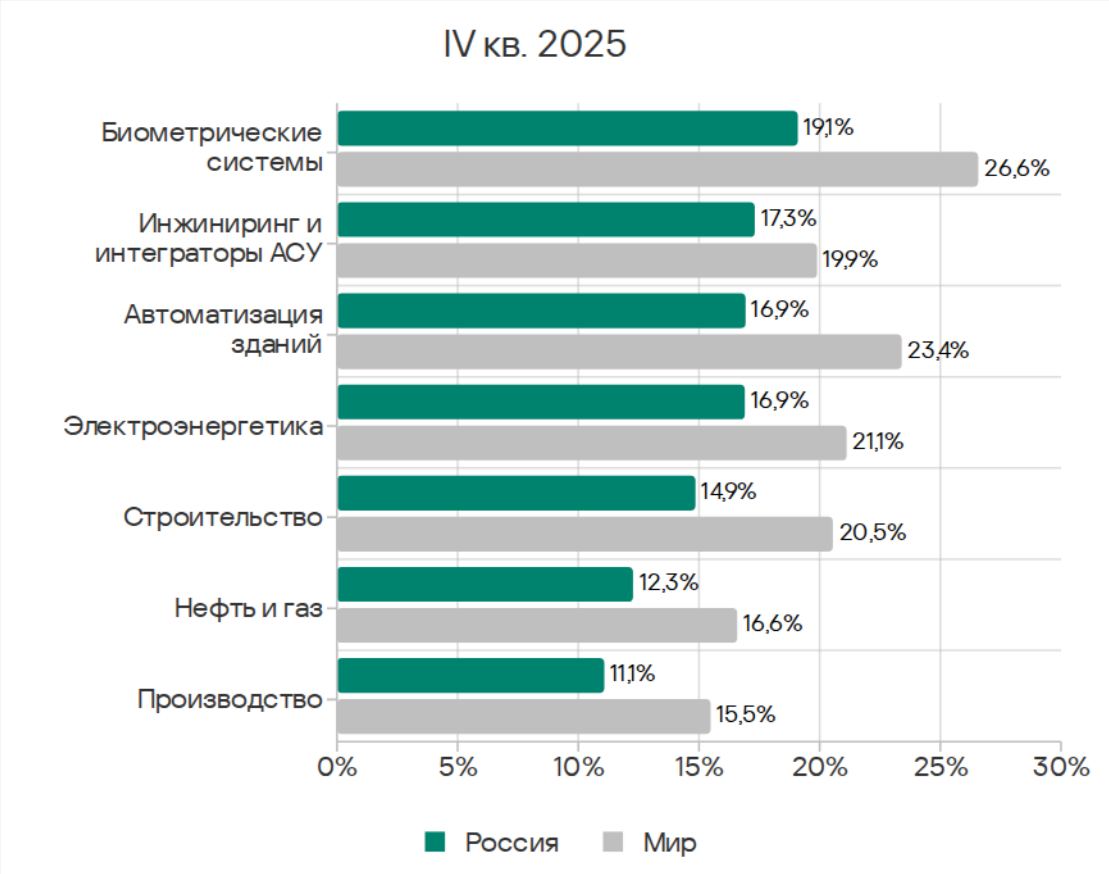
Несмотря на уменьшение в четвертом квартале среднего по России показателя, доля компьютеров АСУ, на которых блокируются программы-вымогатели, выросла во всех исследуемых отраслях региона, кроме строительства и автоматизации зданий. По росту показателя лидирует инфраструктура биометрических систем.

В четвертом квартале 2025 года программы-вымогатели распространялись в России через интернет и почту.

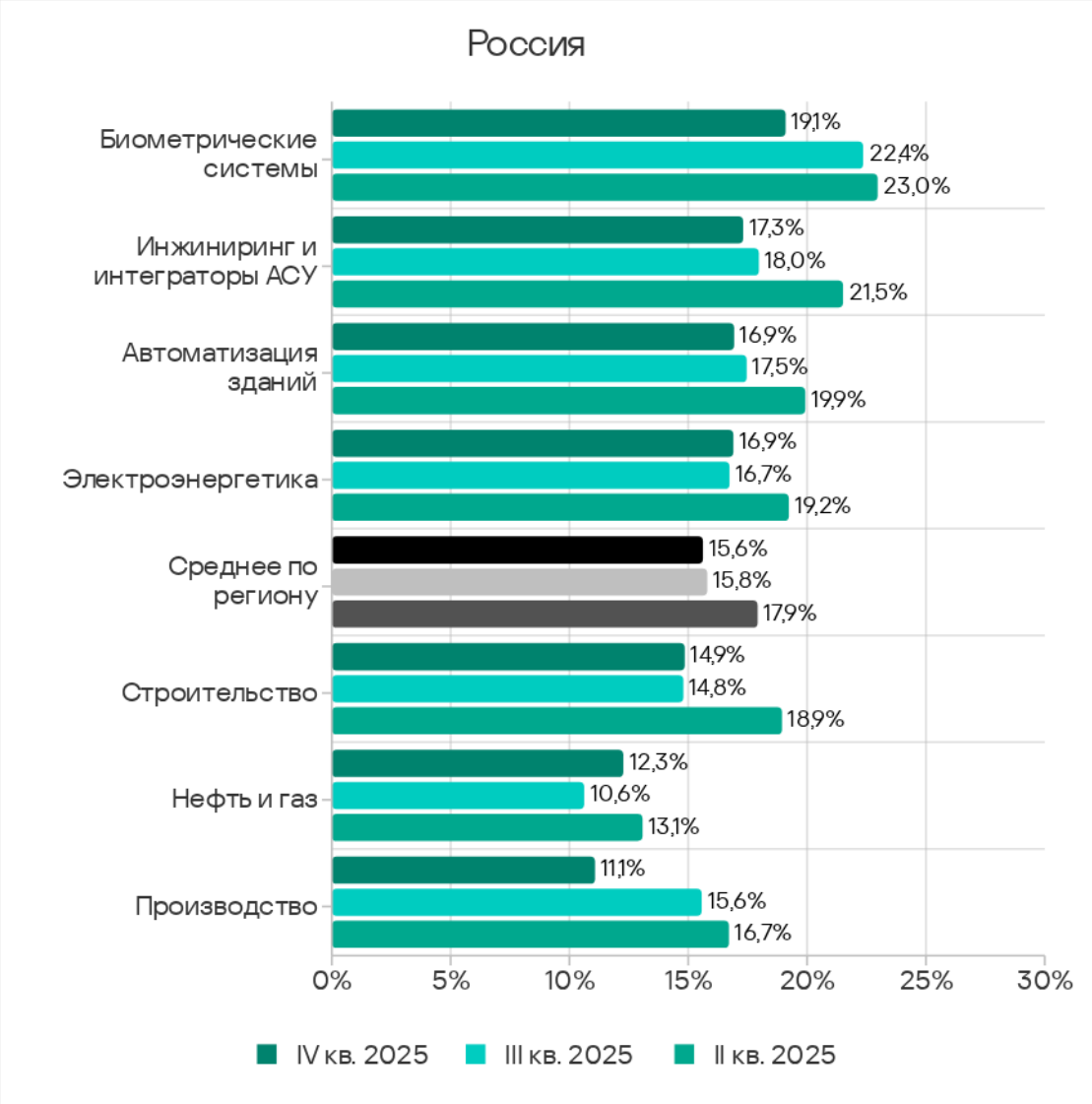
Отрасли

В России из всех рассмотренных в отчете отраслей чаще всего вредоносные объекты блокируются в инфраструктуре биометрических систем.

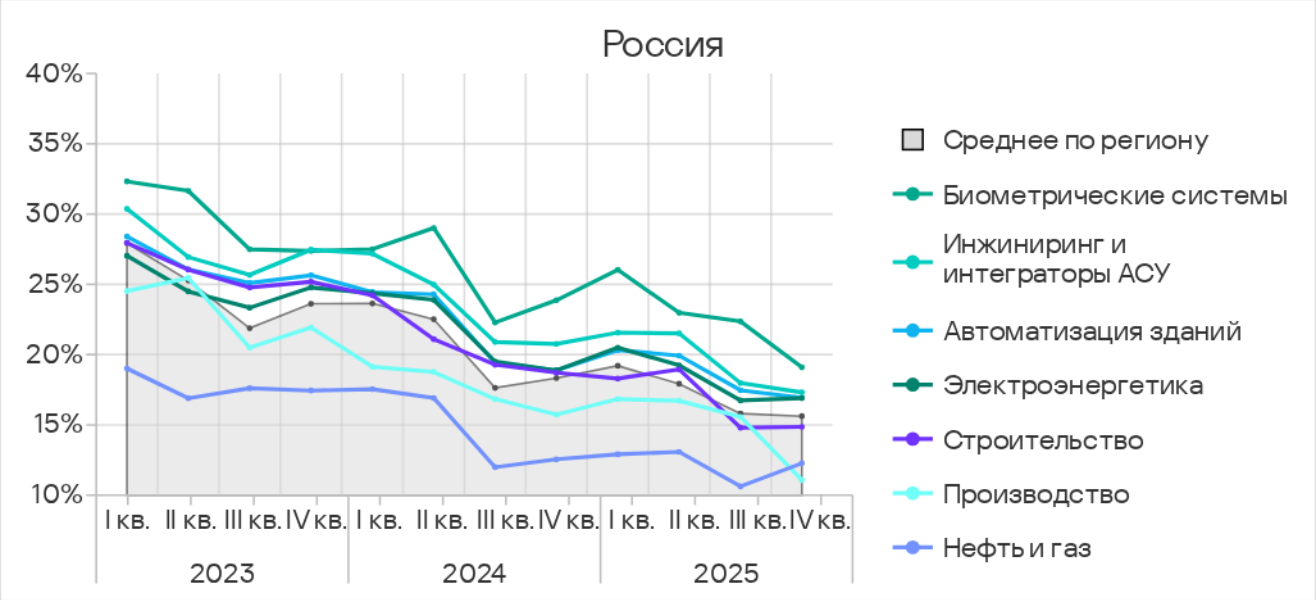
Во всех отраслях региона доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, ниже соответствующих среднемировых показателей.



В четвертом квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, из всех рассмотренных отраслей региона увеличилась в электроэнергетике, строительстве и нефтегазовой отрасли.



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, 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	5,92%	6,24%	6,55%	6,77%	4,28%	6,37%	3,62%	5,78%
Почтовые клиенты	2,57%	1,54%	0,73%	1,14%	0,94%	0,74%	0,49%	0,66%
Съемные носители	0,55%	0,23%	0,21%	0,39%	0,25%	0,36%	0,23%	0,17%
Сетевые папки	0,08%	0,04%	0,01%	0,03%	0,06%	0,03%	—	0,02%
Показатель отрасли в регионе	19,10%	16,93%	17,31%	16,90%	12,27%	14,85%	11,08%	

Показатели категорий угроз в отраслях в России, 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	4,21%	3,94%	3,77%	4,61%	2,92%	4,06%	2,66%	3,41%
Вредоносные скрипты и фишинговые страницы	5,38%	4,33%	4,15%	4,40%	3,00%	4,41%	2,36%	3,68%
Вредоносные документы (MSOffice+PDF)	1,56%	1,23%	0,77%	1,42%	1,19%	0,67%	0,68%	0,61%
Троянцы-шпионы, бэкдоры и кейлоггеры	3,82%	3,47%	2,80%	3,16%	2,10%	2,61%	1,83%	2,61%
Программы-вымогатели	0,78%	0,32%	0,14%	0,34%	0,29%	0,21%	0,13%	0,11%
Майнеры — исполняемые файлы для ОС Windows	1,09%	1,06%	1,11%	1,58%	0,78%	1,21%	0,89%	0,90%
Веб-майнеры, выполняемые в браузерах	0,55%	0,39%	0,34%	0,61%	0,38%	0,62%	0,45%	0,26%
Вредоносные программы для AutoCAD	0,08%	0,02%	0,04%	0,03%	0,12%	0,10%	0,08%	0,02%
Черви (Worm)	1,56%	1,57%	1,04%	1,69%	1,32%	1,24%	1,15%	1,13%
Вирусы (Virus)	0,94%	0,50%	0,50%	1,03%	0,59%	0,59%	0,49%	0,32%
Показатель отрасли в регионе	19,10%	16,93%	17,31%	16,90%	12,27%	14,85%	11,08%	

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.

По доле компьютеров АСУ, на которых блокируются **ресурсы в интернете из списка запрещенных** в различных отраслях, Россия среди регионов находится:

- на первом месте по показателю в автоматизации зданий;
- на втором месте по показателю в биометрических системах;

- на третьем месте по показателю в электроэнергетике.

Высокие показатели майнеров. Россия занимает не ниже третьего места в рейтингах регионов по показателям майнеров обеих категорий во всех отраслях, кроме производства.

В производственной отрасли Россия находится на третьем месте по показателю майнеров – исполняемых файлов для ОС Windows и на четвертом – по показателю веб-майнеров.

Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы, за квартал выросла во всех исследуемых отраслях региона, больше всего – в производственной отрасли.

Высокие показатели программ-вымогателей. По доле компьютеров АСУ, на которых блокируются программы-вымогатели, Россия в рейтингах регионов занимает:

- второе место по показателю в инфраструктуре биометрических систем;
- третье место по показателям в электроэнергетической и нефтегазовой отраслях,
- четвертое место по показателям в отраслях автоматизация зданий и строительство;
- пятое место по показателю в отрасли инжиниринг и интеграторы АСУ.

По показателю программ-вымогателей в отрасли производство Россия на шестом месте.

Доля компьютеров АСУ, на которых блокируются программы-вымогатели, за квартал выросла во всех исследуемых отраслях региона, кроме строительства и автоматизации зданий.

Биометрические системы

Россия находится на девятом 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 Россия занимает:

- второе место по доле компьютеров АСУ, на которых блокировались угрозы следующих категорий: ресурсы в интернете из списка запрещенных, майнеры обеих категорий и программы-вымогатели.

Среди отраслей в регионе инфраструктура биометрических систем занимает:

- первое место по показателям всех источников угроз, кроме интернета;
- первое место по доле компьютеров АСУ, на которых блокировались угрозы следующих категорий: вредоносные скрипты и фишинговые страницы, вредоносные документы, шпионские программы, программы-вымогатели;
- второе место по показателям угроз категорий ресурсы в интернете из списка запрещенных и вирусы;
- третье место по показателям червей, веб-майнеров и вредоносных программ для AutoCAD.

Инжиниринг и интеграторы АСУ

Россия находится на восьмом 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:

- первое место по доле компьютеров АСУ, на которых блокировались майнеры – исполняемые файлы для ОС Windows;
- второе место по показателю веб-майнеров.

Среди отраслей в регионе отрасль инжиниринг и интеграторы АСУ занимает:

- второе место по угрозам из интернета;
- третье место по доле компьютеров АСУ, на которых блокировались майнеры – 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.

Среди регионов по показателям отрасли Россия занимает:

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

Среди отраслей в регионе автоматизация зданий занимает:

- второе место по угрозам из почты;
- третье место по угрозам в сетевых папках;
- второе место по доле компьютеров АСУ, на которых блокировались шпионские программы и черви;
- третье место по показателям угроз категорий вредоносные документы и программы-вымогатели.

Электроэнергетика

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

Среди регионов по показателям в отрасли Россия занимает:

- второе место по доле компьютеров АСУ, на которых блокировались майнеры обеих категорий;
- третье место по доле компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных и программы-вымогатели.

Среди отраслей в регионе электроэнергетика занимает:

- первое место доле компьютеров АСУ, на которых блокировались угрозы из интернета;
- второе место по показателю съемных носителей;
- третье место по показателю угроз из почтовых клиентов;
- первое место по доле компьютеров АСУ, на которых блокировались ресурсы в интернете из списка запрещенных, черви, вирусы и майнеры в формате исполняемых файлов;
- второе место по показателям угроз следующих категорий: вредоносные документы, веб-майнеры и программы-вымогатели;
- третье место по показателям угроз категорий вредоносные скрипты и фишинговые страницы, а также шпионские программы.

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 майнеры обеих категорий.

Среди отраслей в регионе строительство занимает:

- третье место по доле компьютеров АСУ, на которых блокировались угрозы из интернета и на съемных носителях;
- первое место по доле компьютеров АСУ, на которых блокировались веб-майнеры;
- второе место по показателям угроз следующих категорий: вредоносные скрипты и фишинговые страницы, майнеры в формате исполняемых файлов и вредоносные программы для AutoCAD;
- третье место по показателям ресурсов в интернете из списка запрещенных и вирусов.

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:

- первое место по показателю угроз в сетевых папках — это единственный регион, где в нефтегазовой отрасли на компьютерах АСУ блокировались такие угрозы;
- второе место по доле компьютеров АСУ, на которых блокировались вредоносные документы и майнеры обеих категорий;
- третье место по доле компьютеров АСУ, на которых блокировались программы-вымогатели.

Среди отраслей в регионе нефтегазовая отрасль занимает:

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

Производство

Россия находится на 11-м 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 блокировались майнеры – исполняемые файлы для ОС Windows, четвертое место по показателям веб-майнеров.

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