Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второй квартал 2025 года

11.09.2025

Версия 1.0

Цифры ... 3
Статистика по всем угрозам ... 4
Исследуемые отрасли ... 7
Разнообразие обнаруженных вредоносных объектов ... 9
Категории вредоносных объектов ... 11
Вредоносные объекты, используемые для первичного заражения ... 11
Ресурсы в интернете из списка запрещенных ... 11
Вредоносные документы (MSOffice+PDF) ... 15
Вредоносные скрипты и фишинговые страницы (JS и HTML) ... 18
Вредоносное ПО следующего этапа ... 21
Программы-шпионы ... 21
Программы-вымогатели ... 24
Майнеры — исполняемые файлы для ОС Windows ... 27
Веб-майнеры ... 31
Самораспространяющееся вредоносное ПО. Черви и вирусы ... 34
Черви ... 35
Вирусы ... 38
Вредоносные программы для AutoCAD ... 40
Основные источники угроз ... 44
Интернет ... 44
Почтовые клиенты ... 47
Съемные носители ... 50
Сетевые папки ... 53
Методика подготовки статистики ... 56

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Цифры

Показатель	I кв. 2025	II кв. 2025	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	21,9%%	20,5%	▼1,4 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	7,16%	6,49%	▼0,67 п. п.
Ресурсы в интернете из списка запрещенных	5,12%	5,91%	▲0,79 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	4,20%	3,84%	▼0,36 п. п.
Вредоносные документы (MSOffice+PDF)	1,85%	1,97%	▲0,12 п. п.
Вирусы (Virus)	1,53%	1,29%	▼0,24 п. п.
Черви (Worm)	1,31%	1,22%	▼0,09 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,78%	0,63%	▼0,15 п. п.
Веб-майнеры, выполняемые в браузерах	0,53%	0,30%	▼0,23 п. п.
Вредоносные программы для AutoCAD	0,34%	0,29%	▼0,05 п. п.
Программы-вымогатели	0,16%	0,14%	▼0,02 п. п.
Основные источники угроз			
Интернет	10,11%	9,76%	▼0,35 п. п.
Почтовые клиенты	2,81%	3,06%	▲0,25 п. п.
Съемные носители	0,52%	0,37%	▼0,15 п. п.
Сетевые папки	0,07%	0,05%	▼0,02 п. п.

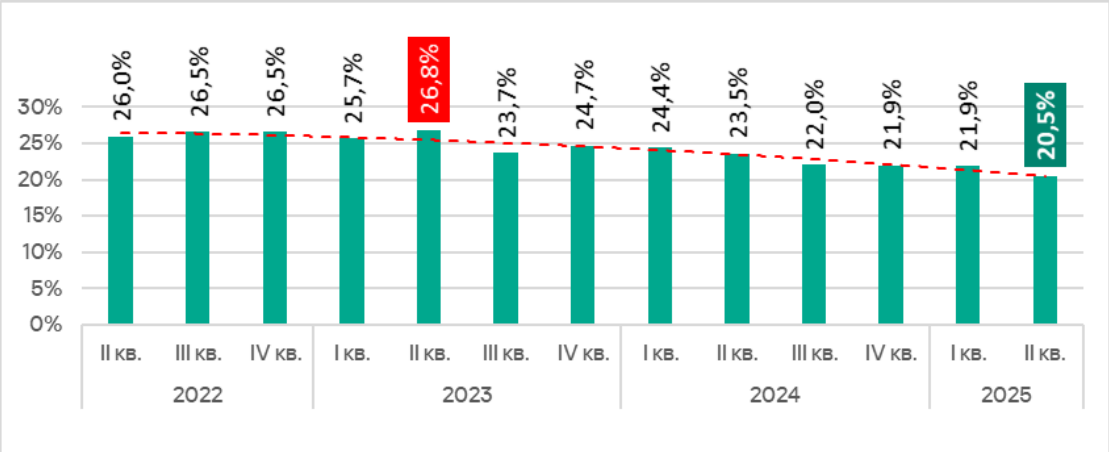
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Статистика по всем угрозам

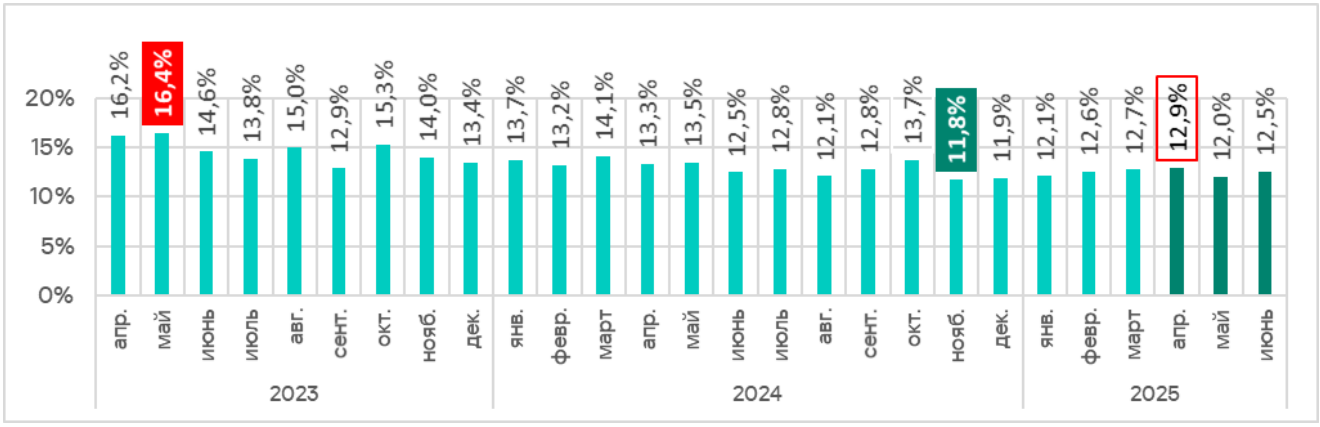
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, по сравнению с предыдущим кварталом уменьшилась на 1,4 п. п. и составила 20,5%.

По сравнению со вторым кварталом 2024 года доля атакованных компьютеров АСУ уменьшилась на 3,0 п. п.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, II квартал 2022 года — II квартал 2025 года



В течение второго квартала 2025 года самым высоким показатель был в апреле.



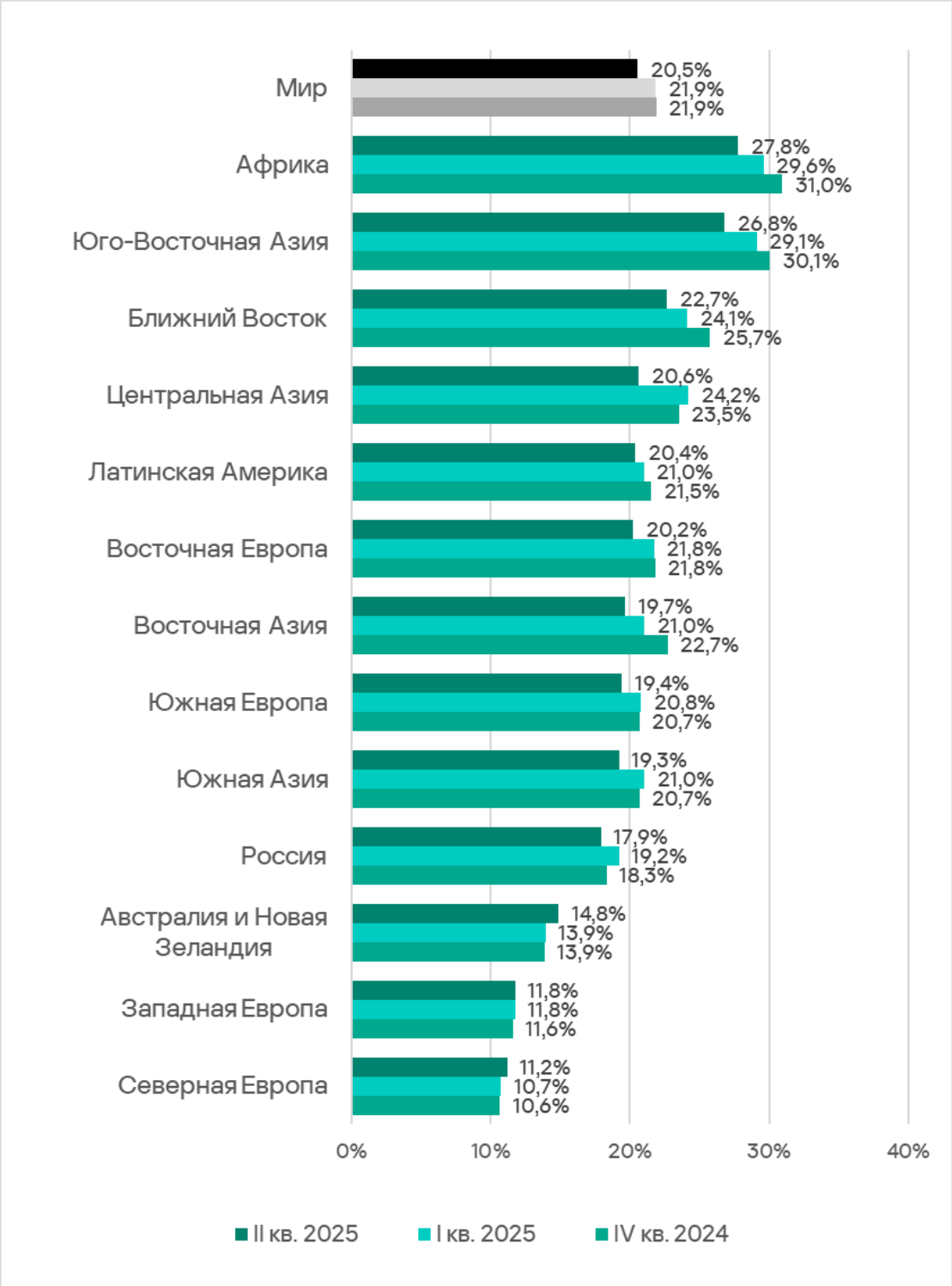
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых во втором квартале 2025 года были заблокированы вредоносные объекты, варьирует от 11,2% в Северной Европе до 27,8% в Африке.

Во большинстве регионов, рассматриваемых в этом отчете, показатель уменьшился по сравнению с предыдущим кварталом. Увеличился он только в Австралии и Новой Зеландии, а также в Северной Европе.

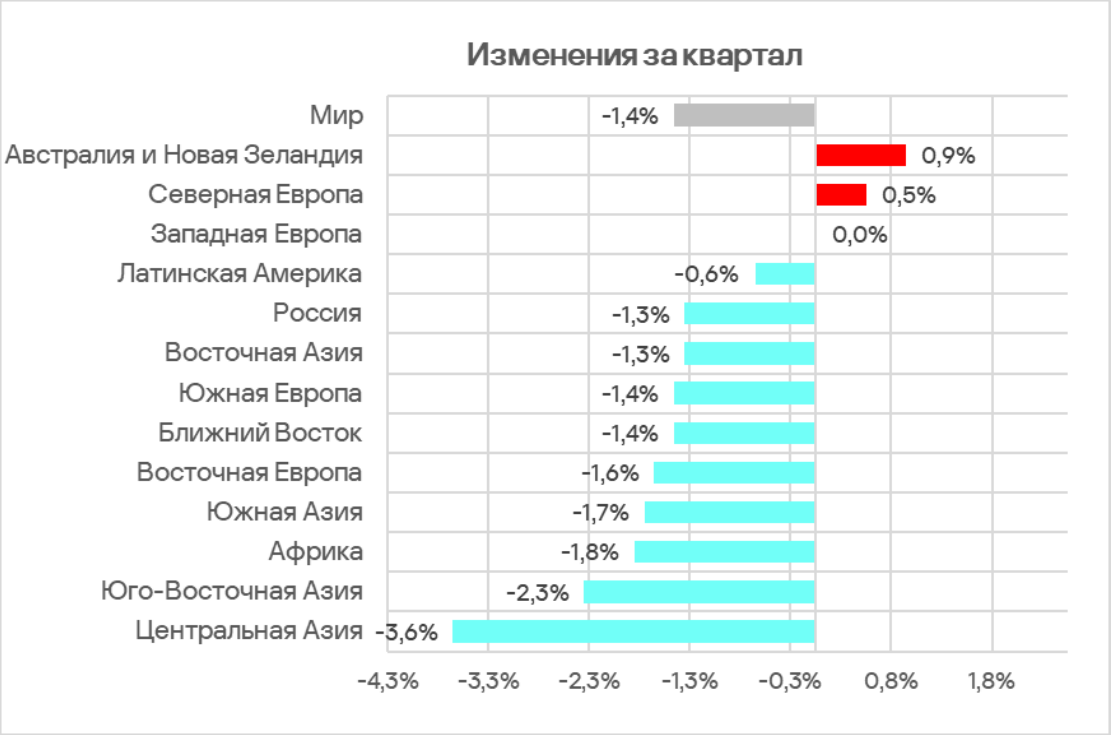
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле атакованных компьютеров АСУ, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты, II квартал 2025 года

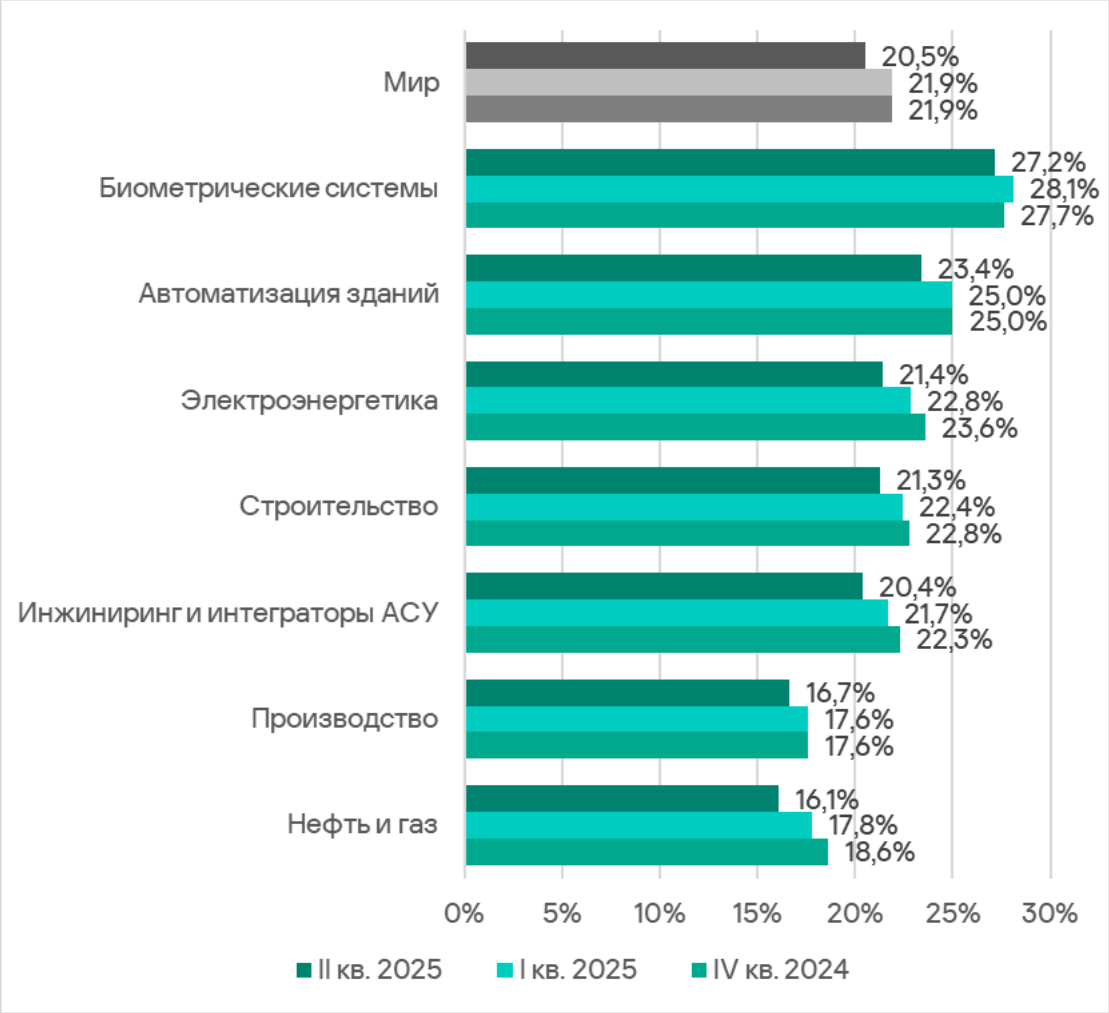


© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Исследуемые отрасли

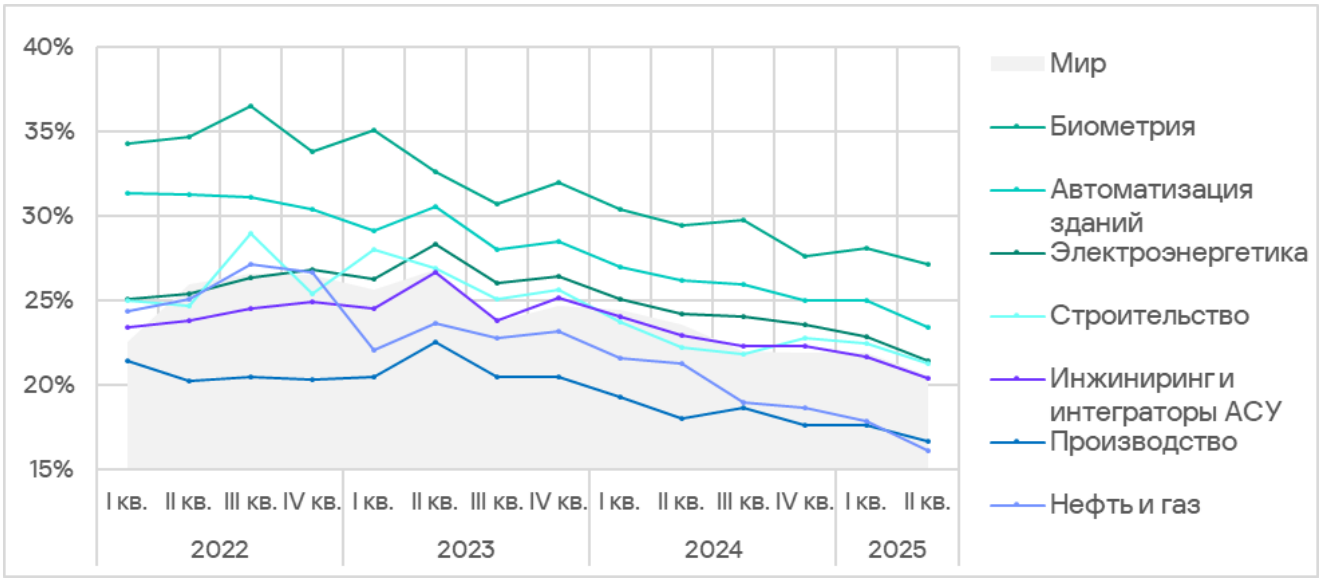
Во втором квартале 2025 года рейтинг исследуемых отраслей и типов OT-инфраструктур по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, традиционно возглавили биометрические системы.

Рейтинг исследуемых отраслей по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, II квартал 2025 года



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

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, в исследуемых отраслях

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Разнообразие обнаруженных вредоносных объектов

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, по способу распространения и назначению можно условно разделить на три группы.

1. Вредоносные объекты, используемые для первичного заражения.
   Чаще всего, это ресурсы в интернете из списка запрещенных, вредоносные скрипты и фишинговые страницы, вредоносные документы.
2. Вредоносное ПО следующего этапа.
   Как правило, это программы-шпионы, программы-вымогатели, майнеры — исполняемые файлы для ОС Windows и веб-майнеры.
3. Самораспространяющееся вредоносное ПО.
   Эта категория включает в себя вирусы и черви.

Вредоносные программы для AutoCAD распространяются разными способами, поэтому мы не относим их к конкретной группе по типу распространения.

Вредоносные объекты для первичного заражения компьютеров АСУ активно используются злоумышленниками, в результате они чаще остальных блокируются защитными решениями. Это отражается и в нашей статистике: в мире и почти во всех регионах вредоносные скрипты и фишинговые страницы, а также интернет-ресурсы из списка запрещенных занимают первые места в рейтингах категорий угроз по доле компьютеров АСУ, на которых они были заблокированы.

Следует заметить, что в небольшом проценте случаев категории угроз, которые мы относим к объектам первичного заражения, скажем, вредоносные ссылки, на самом деле могут использоваться на последующих этапах атаки. Так, например, иногда ссылка на вредоносный ресурс может быть обнаружена при сканировании реестра компьютера, где она появились, очевидно, в результате работы другого вредоносного ПО — до того момента, как оно было идентифицировано и заблокировано. Более строгое деление атакованных компьютеров АСУ по категориям заблокированного на них вредоносного ПО и по источникам его попадания на компьютер описано в специальной статье «Динамика внешних и внутренних угроз АСУ», открывающей новый цикл публикаций результатов более глубокого исследования ландшафта угроз АСУ ТП по данным статистики срабатывания защитных компонентов наших продуктов.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, II квартал 2025 года

Из всех исследуемых категорий во втором квартале 2025 года выросла доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных (по отношению к показателю предыдущего квартала в 1,2 раза) и вредоносные документы (в 1,1 раза).

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Категории вредоносных объектов

Во втором квартале 2025 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 10 408 семейств, относящихся к различным категориям.

Типовые атаки, блокируемые в сети АСУ, представляют собой многоступенчатый процесс, где каждый последующий шаг злоумышленников направлен на повышение привилегий и получение доступа к другим системам путем эксплуатации проблем безопасности промышленных предприятий, в том числе технологических инфраструктур.

Стоит отметить, что в ходе атаки злоумышленники часто повторяют одни и те же шаги (TTP), например, когда используют вредоносные скрипты и установленные каналы связи с инфраструктурой управления и контроля (C2) для горизонтального перемещения внутри сети и продвижения атаки.

Вредоносные объекты, используемые для первичного заражения

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-адреса 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.

Обнаруженный опасный интернет-ресурс не всегда может быть добавлен в список запрещенных, поскольку злоумышленники все чаще используют легитимные интернет-ресурсы и сервисы, например платформы доставки контента (CDN), мессенджеры и облачные хранилища. Подобные сервисы позволяют распространять вредоносный код по уникальным ссылкам на

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

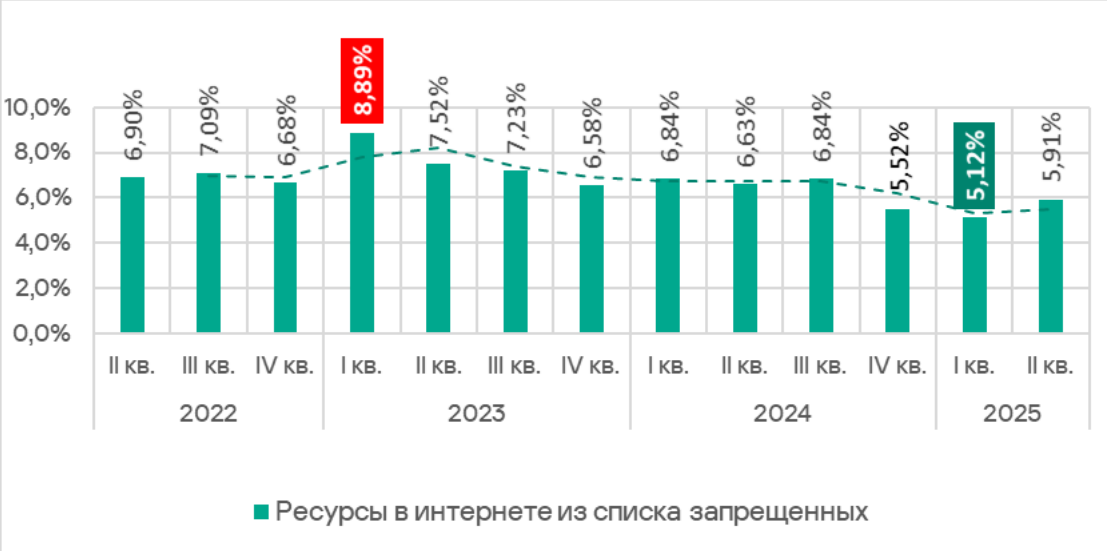
уникальный контент, затрудняя таким образом тактики блокировки по репутации. Настоятельно рекомендуем промышленным организациям предусмотреть блокировку подобных сервисов политикой, как минимум, для технологических сетей, где необходимость в таких сервисах крайне редко бывает обусловлена объективными причинами.

Интернет-ресурсы из списка запрещенных главным образом используются киберпреступниками для распространения вредоносного ПО и фишинговых атак, а также 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), недостатках защиты от фишинга (многие вредоносные ссылки доставляются в фишинговых сообщениях) и недостатках культуры информационной безопасности (сотрудники обращаются к небезопасным интернет-ресурсам и ссылкам из подозрительных писем и сообщений мессенджеров).

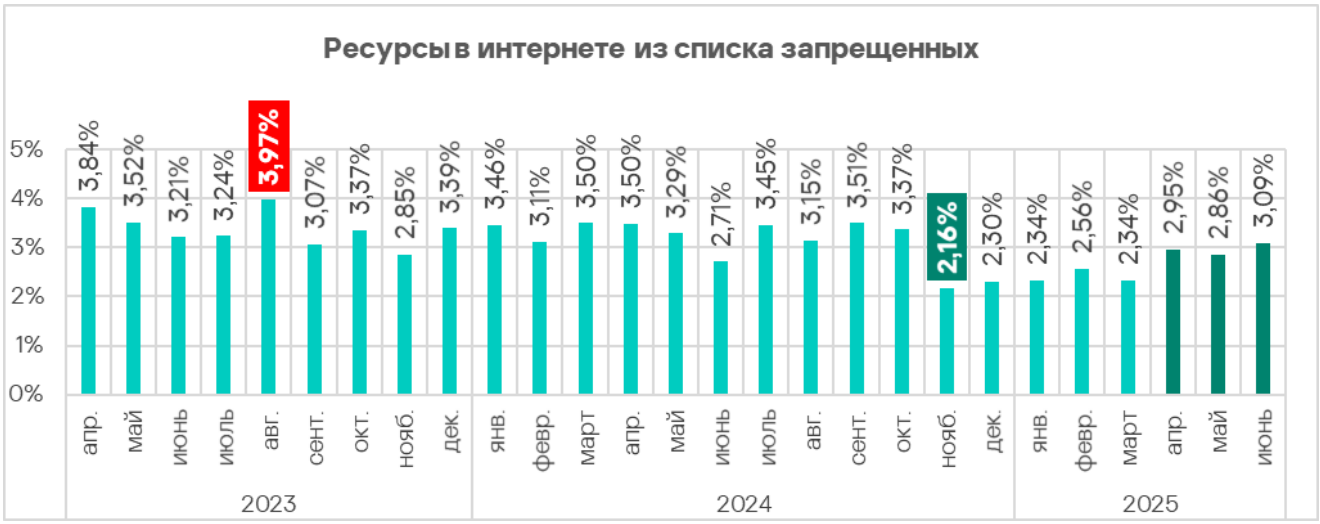
Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, выросла до 5,91%.

Доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, II квартал 2022 года — II квартал 2025 года



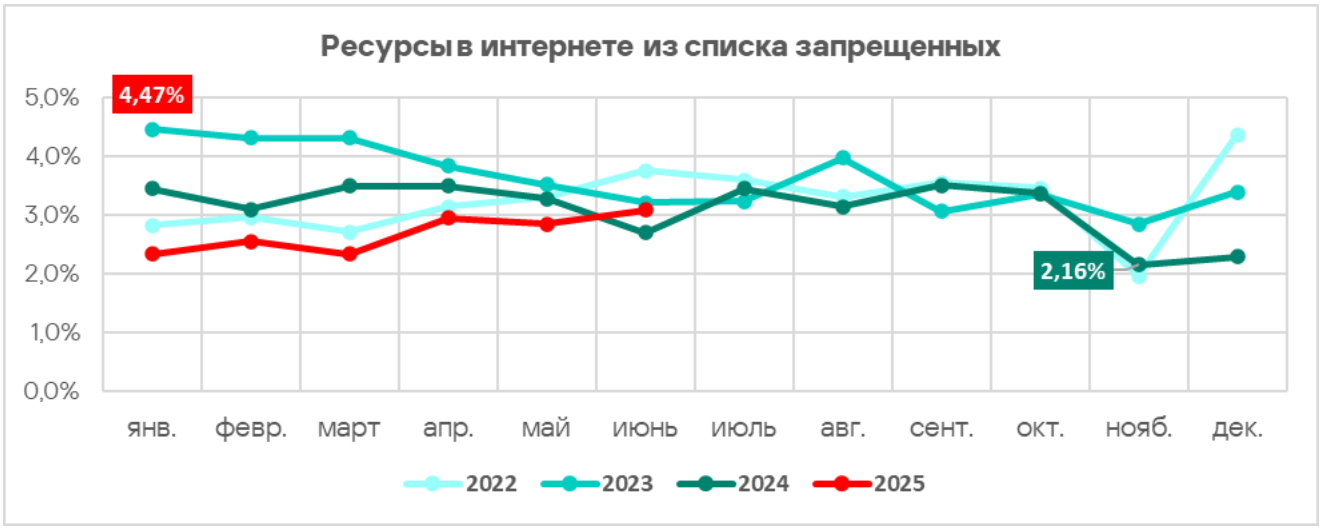
На диаграмме ниже показано ежемесячное значение этого показателя с апреля 2022 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, апрель 2023 года — июнь 2025 года

В первой половине 2025 года сформировалась тенденция к росту доли компьютеров АСУ, на которых в течение месяца были заблокированы ресурсы в интернете из списка запрещенных, после того как в ноябре 2024 года этот показатель достиг минимального значения за рассматриваемый период



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2022 ода — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, варьируют от 3,28% в Восточной Азии до 6,98% в Африке. В тройке лидеров по этому показателю также Россия и Восточная Европа.

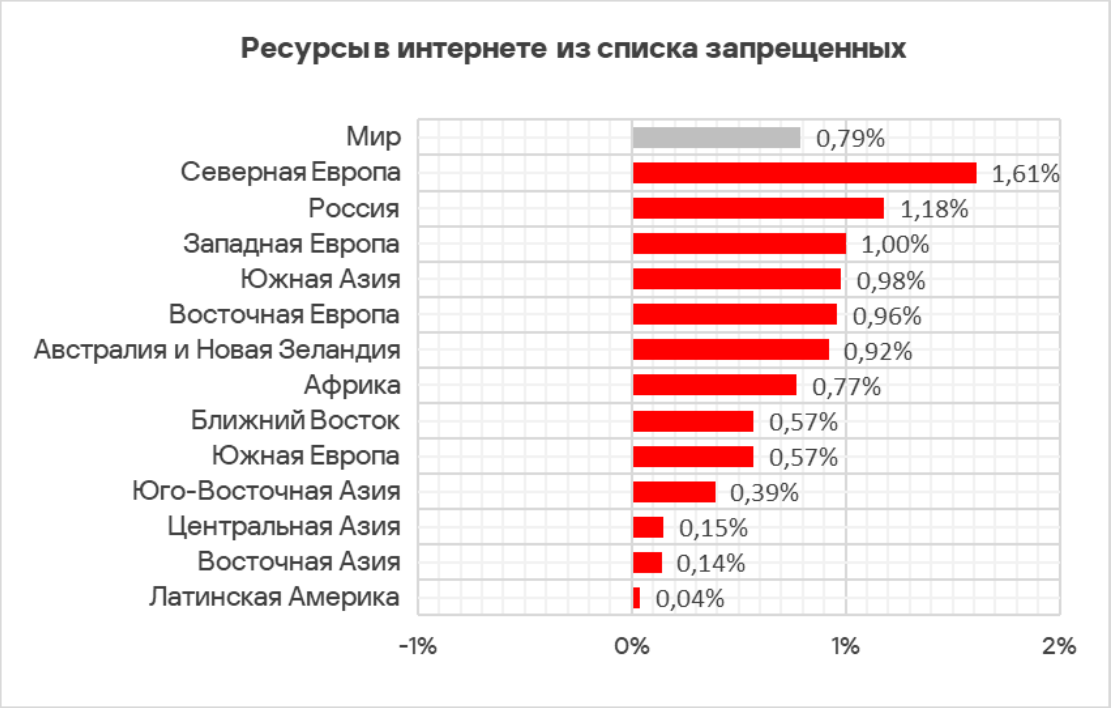
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, II квартал 2025 года

Во втором квартале 2025 года после снижения в предыдущем квартале показатель вырос во всех регионах. Рост показателя во всех регионах связан с добавлением прямых ссылок на вредоносный код, размещаемый на популярных публичных интернет-площадках и файловых сервисах.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, II квартал 2025 года

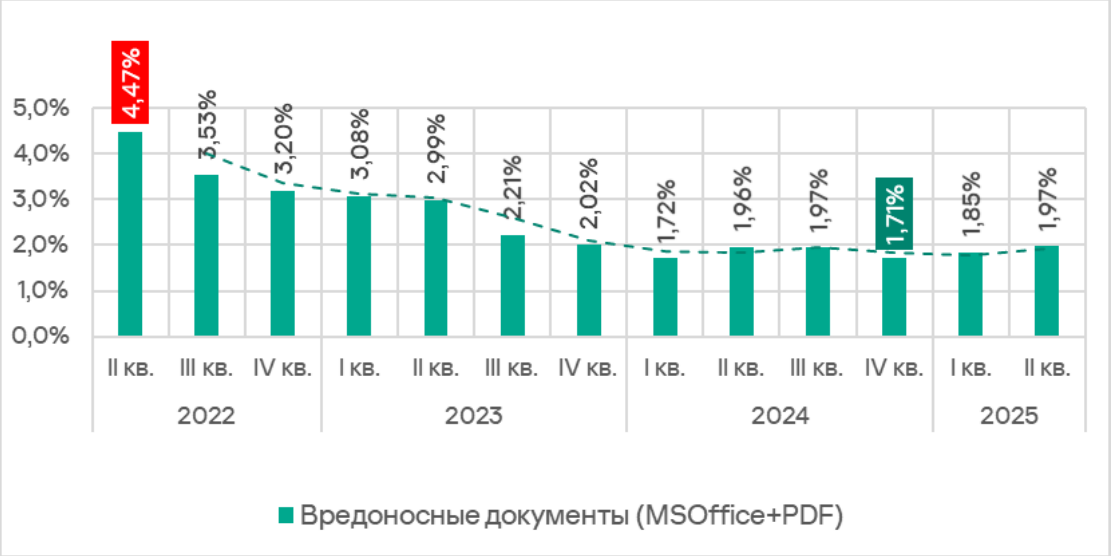


Вредоносные документы (MSOffice+PDF)

Вредоносные документы злоумышленники преимущественно 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.

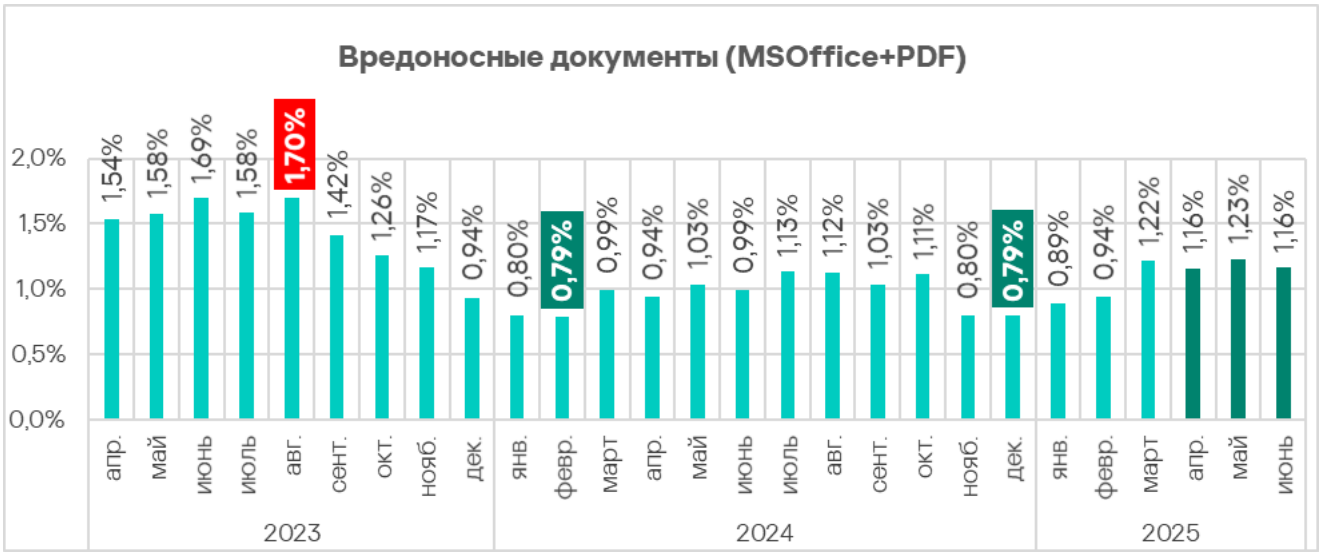
После снижения в конце 2024 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, растет второй квартал подряд и вернулась к значениям третьего квартала 2024 года.

Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, II квартал 2022 года — II квартал 2025 года

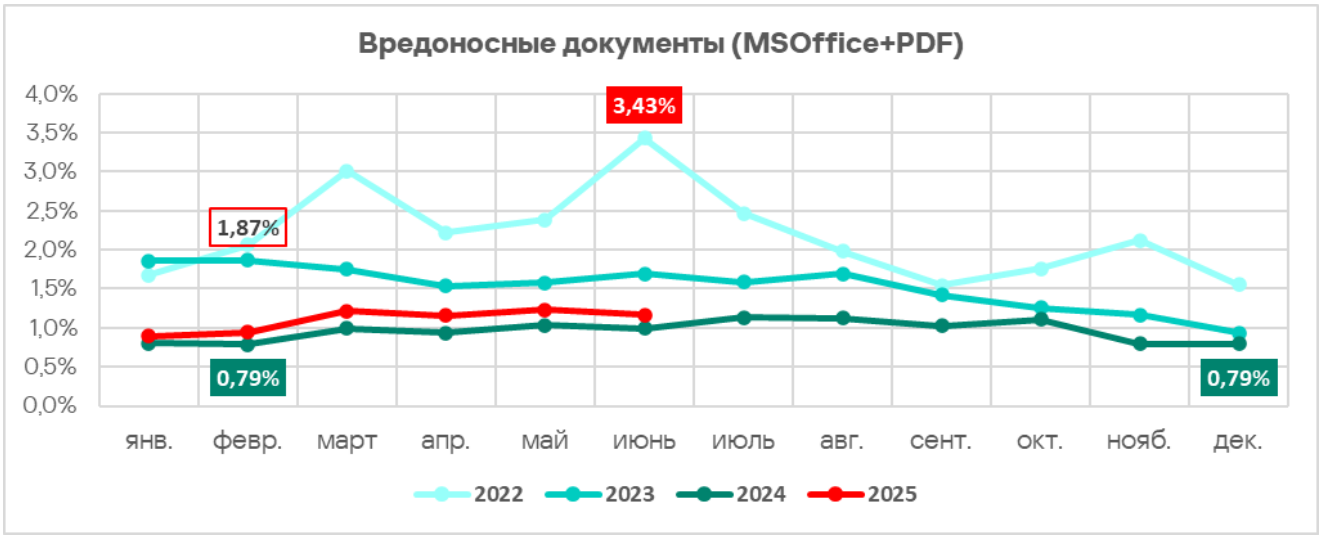


© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Месячные показатели за апрель – июнь 2025 года оказались выше, чем показатели за те же месяцы 2024 года.



Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, апрель 2023 года — июнь 2025 года



Доля компьютеров АСУ, на которых были заблокированы вредоносные документы, январь 2022 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные документы, варьирует от 0,64% в Северной Европе до 4,39% в Южной Европе. Тройка лидеров осталась неизменной: Южная Европа, Латинская Америка и Ближний Восток.

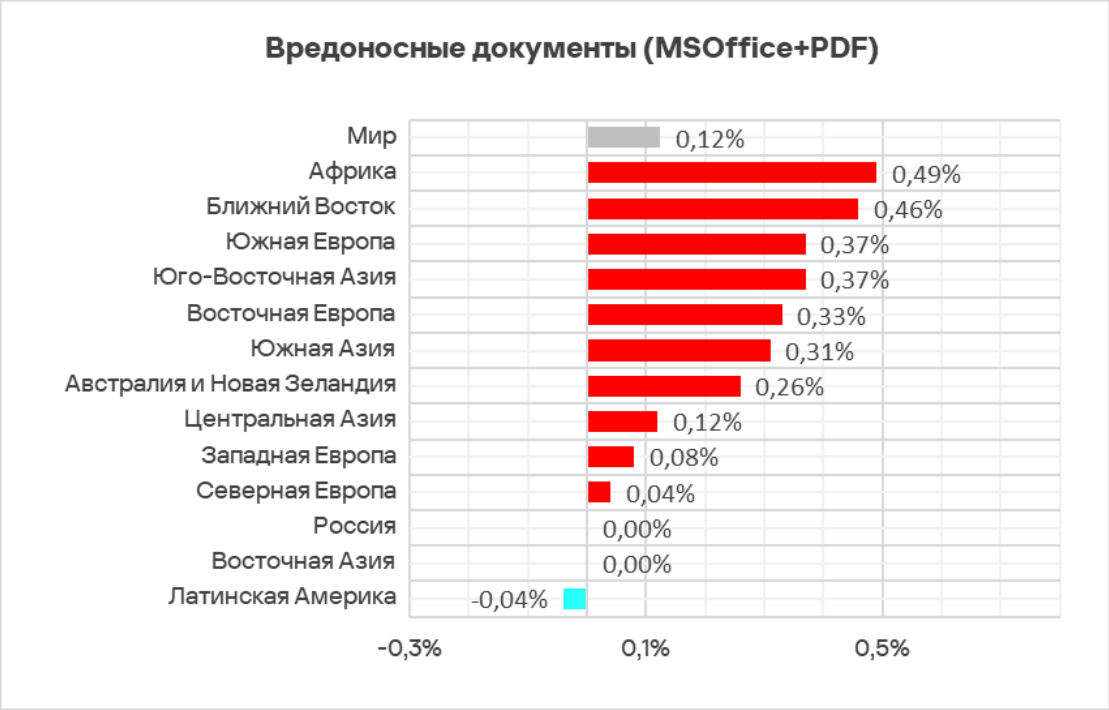
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные документы, II квартал 2025 года

Во втором квартале 2025 года показатель вырос во всех регионах, кроме Латинской Америки.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные документы, II квартал 2025 года



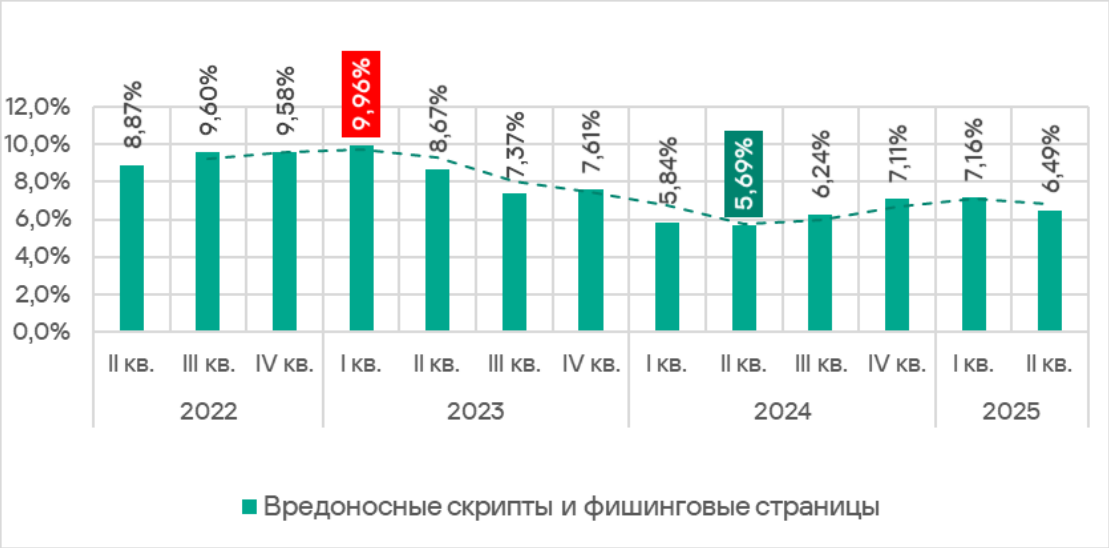
Вредоносные скрипты и фишинговые страницы (JS и HTML)

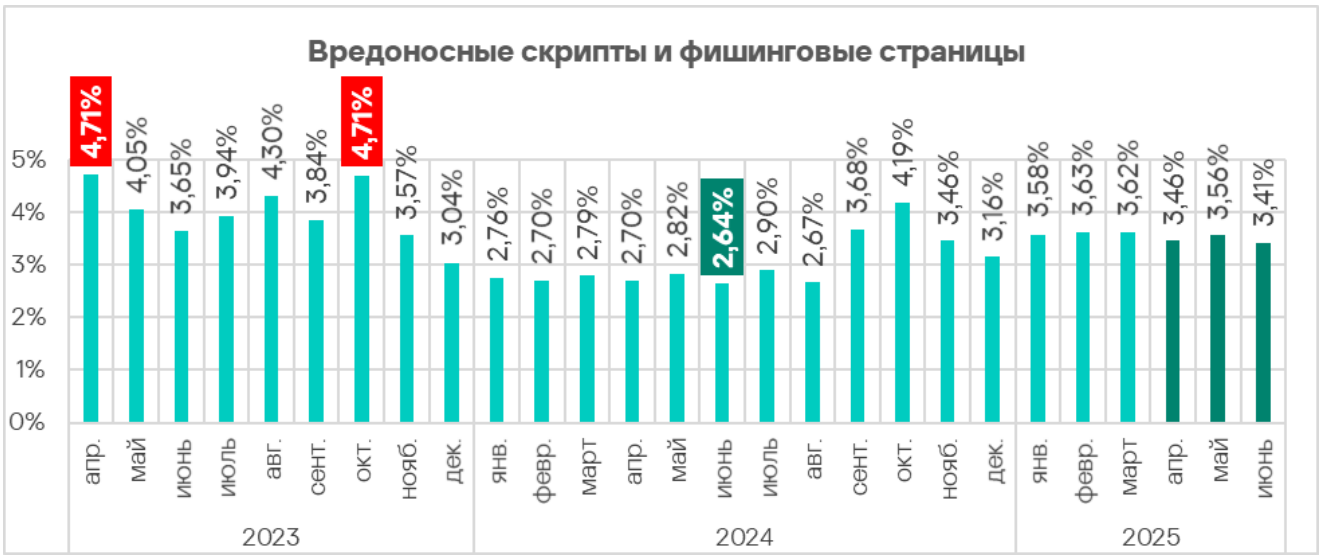
Вредоносные скрипты применяются злоумышленниками для выполнения широкого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, шпионского ПО, программ для скрытого майнинга криптовалюты, программ-вымогателей). Они распространяются как в интернете, так и в письмах, рассылаемых по электронной почте.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, уменьшилась.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, II квартал 2022 года — II квартал 2025 года





Доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, апрель 2023 года — июнь 2025 года

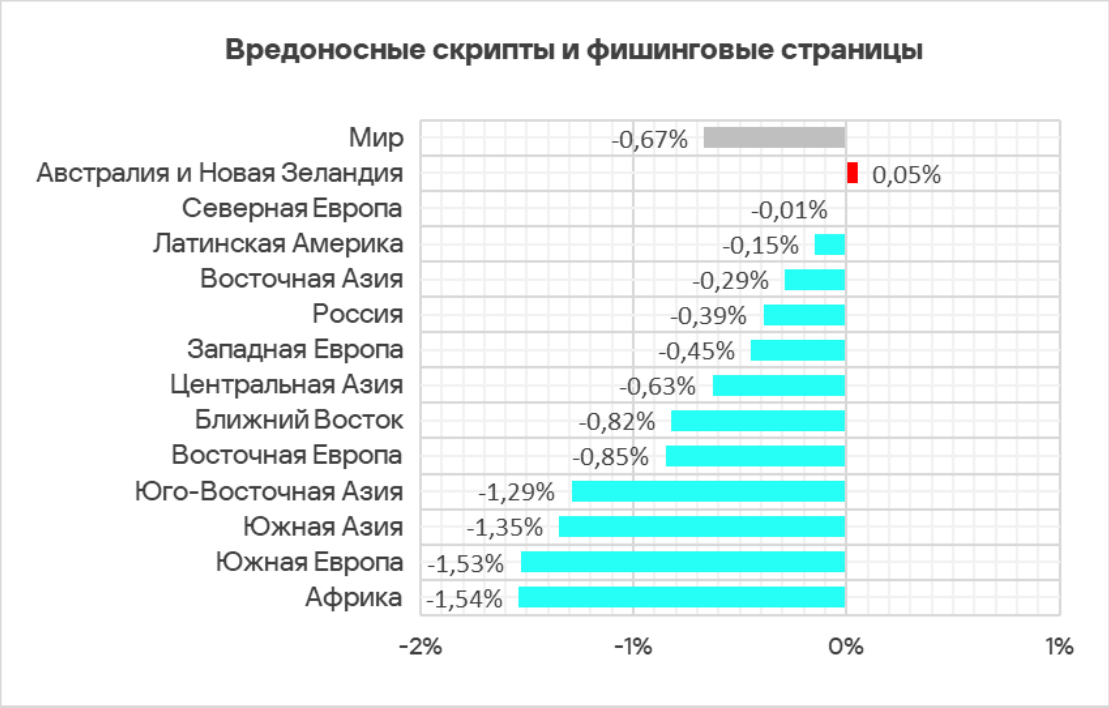
В регионах показатель варьирует от 3,06% в Северной Европе до 9,18% в Латинской Америке. В топ 3 регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вошли Латинская Европа, Южная Европа и Ближний Восток.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, II квартал 2025 года

В регионах показатель уменьшился везде, кроме региона Австралия и Новая Зеландия.

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Вредоносное ПО следующего этапа

Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа. Как правило, это шпионское ПО, программы-вымогатели и майнеры. Обычно, чем выше доля компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, тем выше этот показатель и для вредоносного ПО следующего этапа.

Программы-шпионы

Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО (троянцы, бэкдоры, кейлоггеры) — наиболее часто обнаруживаемый тип вредоносного ПО следующего этапа. Оно используется либо как инструментарий промежуточных этапов кибератаки (например, разведки и распространения по сети), либо как инструмент последнего этапа атаки, применяемый для кражи и вывода конфиденциальных данных. В большинстве случаев конечная цель атак с применением такого ПО — кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

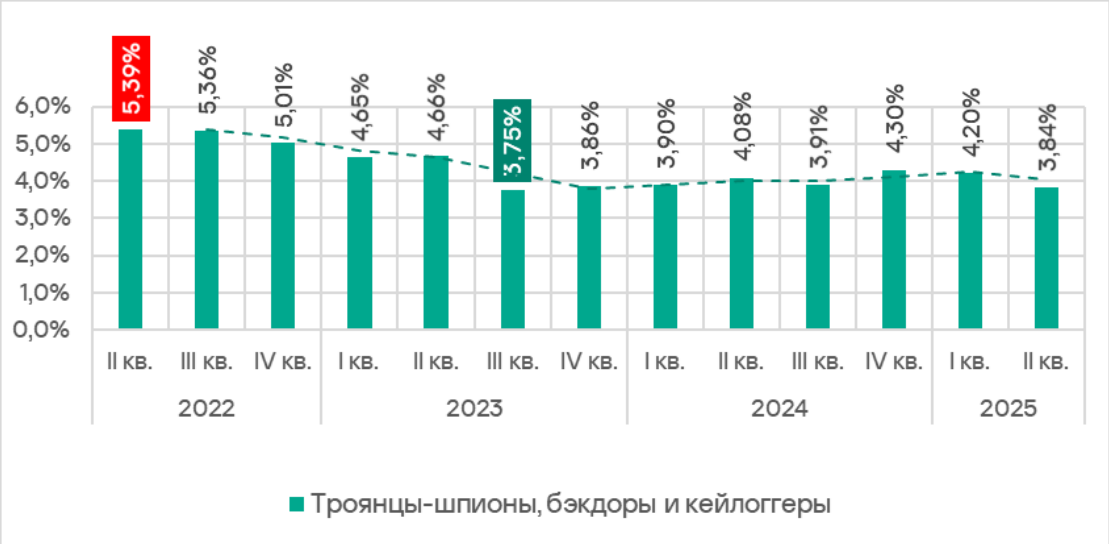
Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

Обнаружение шпионского ПО на компьютере АСУ обычно указывает на то, что вектор первоначального заражения сработал, будь то переход по вредоносной ссылке, открытие вложения из фишингового письма или подключение зараженного USB-накопителя. Это свидетельствует об отсутствии или о неэффективности мер защиты периметра технологической сети (таких как контроль безопасности сетевых коммуникаций и выполнения политики использования съемных носителей).

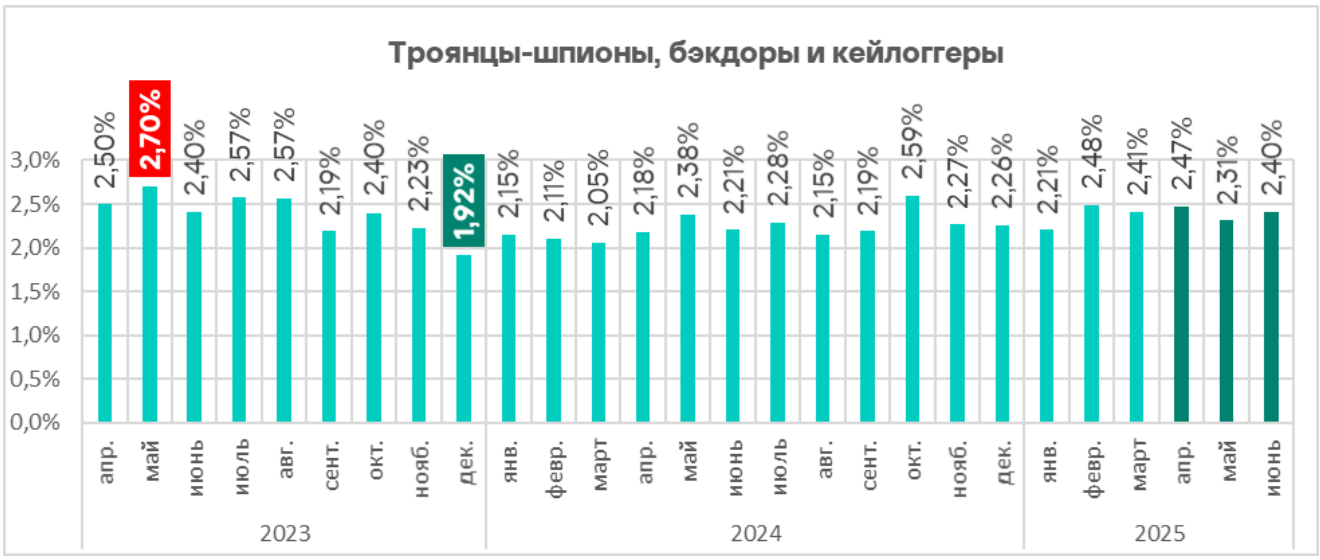
Во втором квартале 2025 года доля компьютеров АСУ, на которых было заблокировано шпионское ПО, уменьшилась по сравнению с предыдущим кварталом.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, II квартал 2022 года — II квартал 2025 года



Наибольшее значение месячного показателя за второй квартал 2025 года было отмечено в апреле.



Доля компьютеров АСУ, на которых были заблокированы программы-шпионы, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых было заблокировано шпионское ПО, варьирует от 1,38% в Западной Европе до 6,82% в Африке. В топ 3 регионов по этому показателю, как и в прошлом квартале, вошли Африка, Южная Европа и Юго-Восточная Азия.

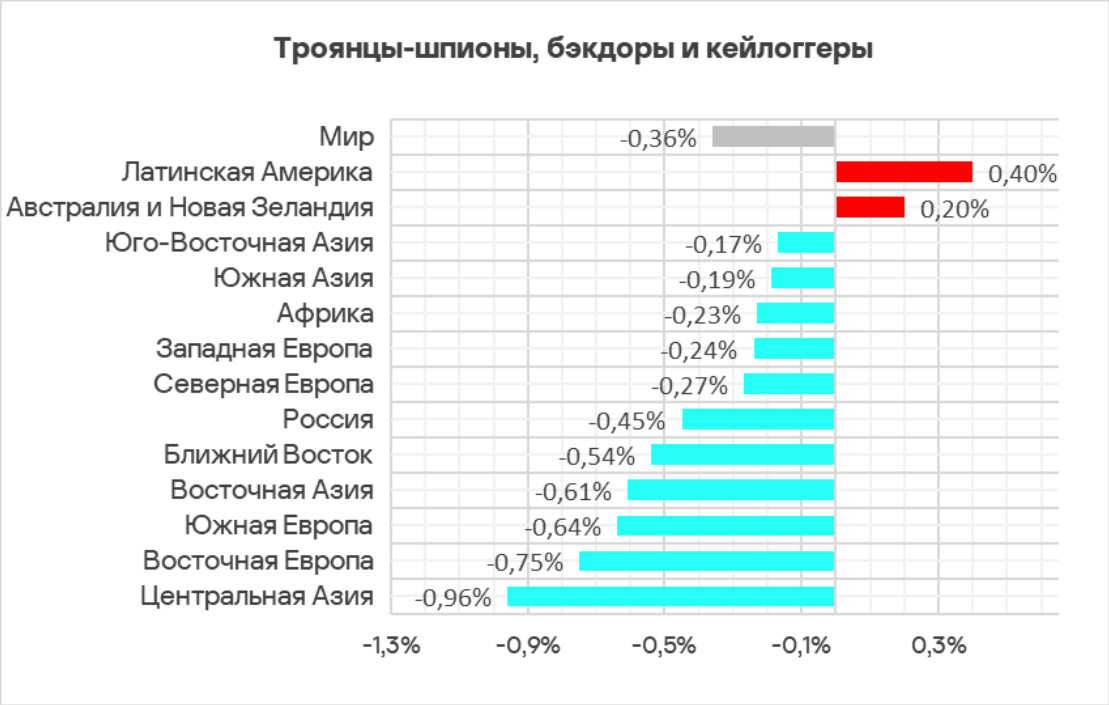
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы шпионские программы, II квартал 2025 года

За квартал доля компьютеров АСУ, на которых были заблокированы шпионские программы, выросла в Латинской Америке, а также Австралии и Новой Зеландии.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

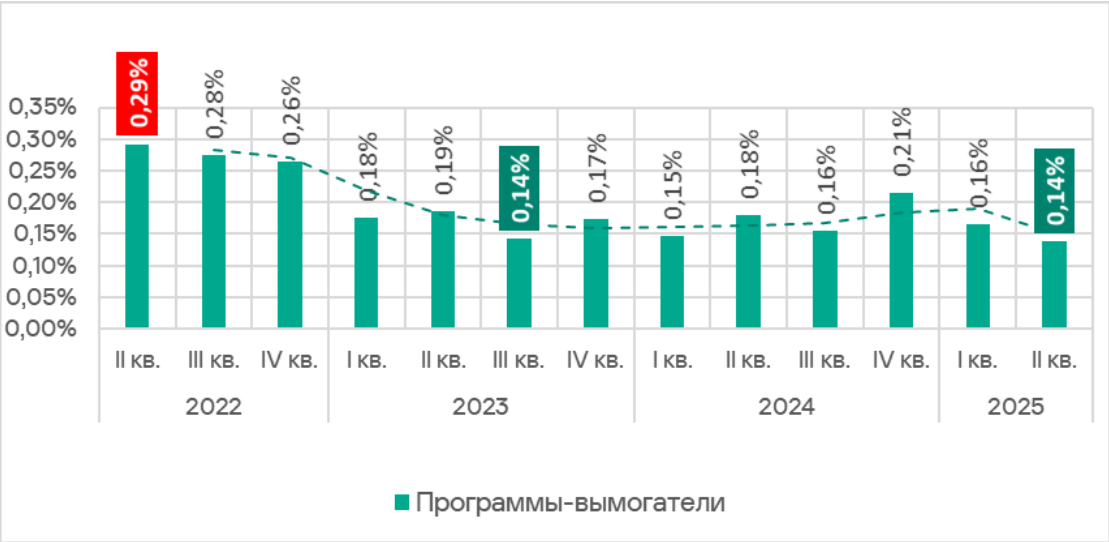
Изменение доли компьютеров АСУ, на которых были заблокированы шпионские программы, II квартал 2025 года



Программы-вымогатели

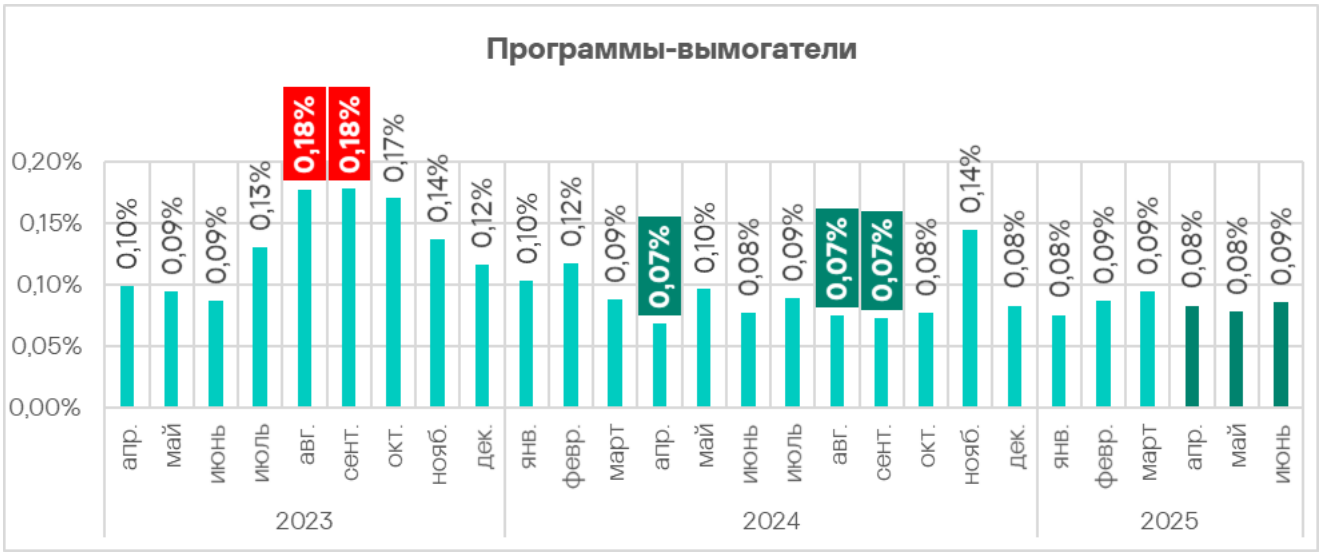
После роста в конце 2024 года доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, снижается уже второй квартал подряд.

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, II квартал 2022 года — II квартал 2025 года



Месячные показатели квартала сопоставимы с предыдущими месяцами 2025 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, апрель 2023 года — июль 2025 года

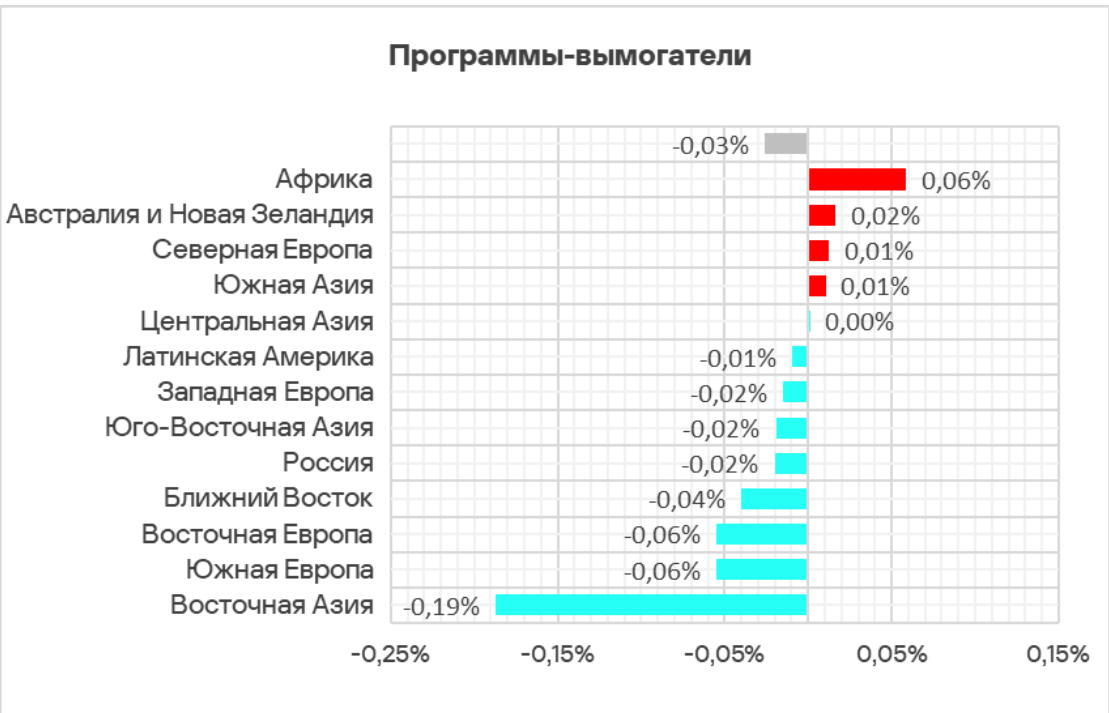
Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, в регионах варьирует от 0,07% в Западной Европе до 0,31% в Африке. В топ 3 регионов также входят Ближний Восток и Центральная Азия.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы программы-вымогатели, II квартал 2025 года

Африка лидирует среди регионов и по росту этого показателя.

Изменение доли компьютеров АСУ, на которых были заблокированы программы-вымогатели, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Майнеры — исполняемые файлы для ОС Windows

Наряду с «классическими» майнерами — приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют, — появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры криптовалют на компьютеры АСУ.

Значительная часть майнеров для ОС Windows, обнаруженных на компьютерах АСУ, представляет собой архивы, названия которых имитировали легальное программное обеспечение. Эти архивы не содержат реального программного обеспечения, но включают в себя файл формата Windows LNK, более известный как ярлык. Однако целевой объект (или путь), на который указывает LNK-файл, не является обычным приложением, а представляет собой команду, которая может выполнить вредоносный код, например, скрипт PowerShell. Злоумышленники все чаще выбирают PowerShell, с помощью которого код вредоносного ПО (в том числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом. Бесфайловое выполнение майнера делает проблематичным его обнаружение средствами защиты.

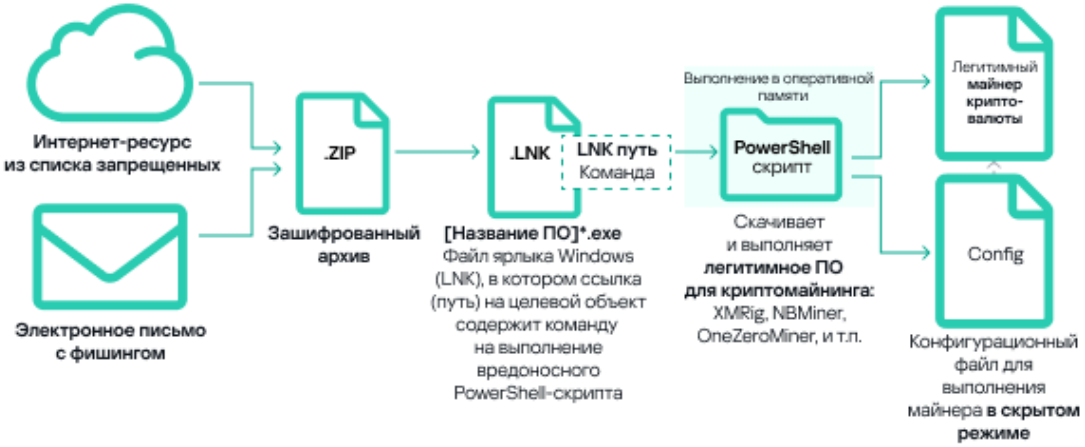
Цепочка атаки: пример бесфайлового исполнения в майнинговых атаках

Еще одним популярным методом внедрения майнеров в технологическую инфраструктуру является использование легитимных криптомайнеров, таких как XMRig, NBMiner, OneZeroMiner и т. д. Сами по себе эти майнеры не являются вредоносными, однако защитные системы классифицируют их как RiskTools. Злоумышленники используют такие майнеры

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

со специфическими файлами конфигурации, позволяющими скрыть активность майнера от пользователя.

Цепочка атаки: пример с использованием легитимных крипто-майнеров

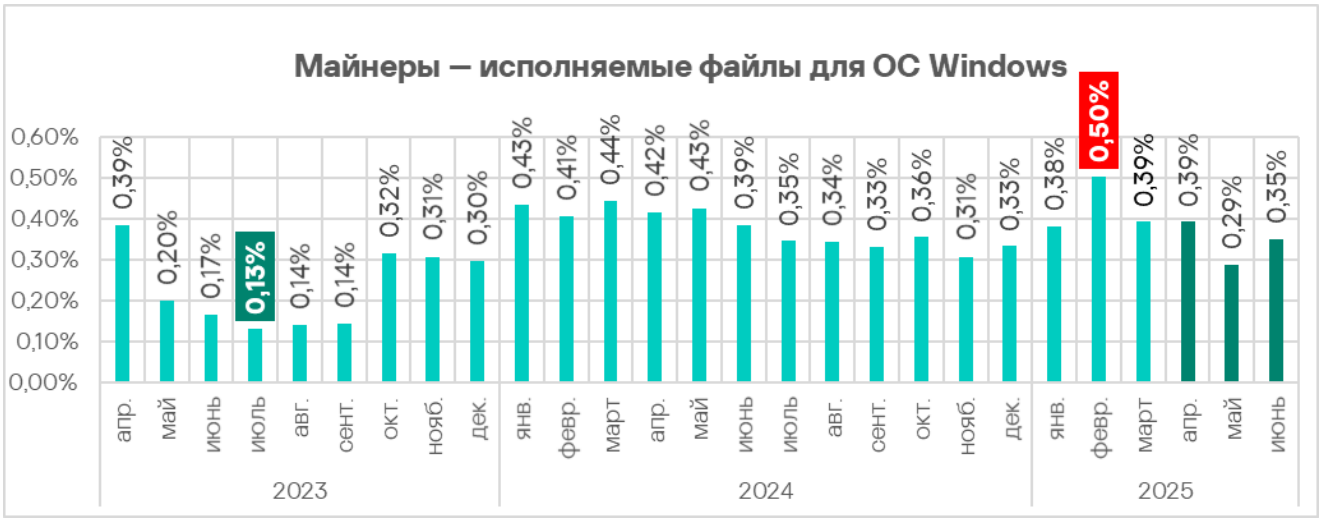


Во втором квартале 2025 года доля компьютеров АСУ, на которых были выявлены майнеры в формате исполняемых файлов для Windows, уменьшилась до 0,63%.

Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, II квартал 2022 года — II квартал 2025 года

Самым высоким за три месяца показатель был в апреле — 0,39%.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

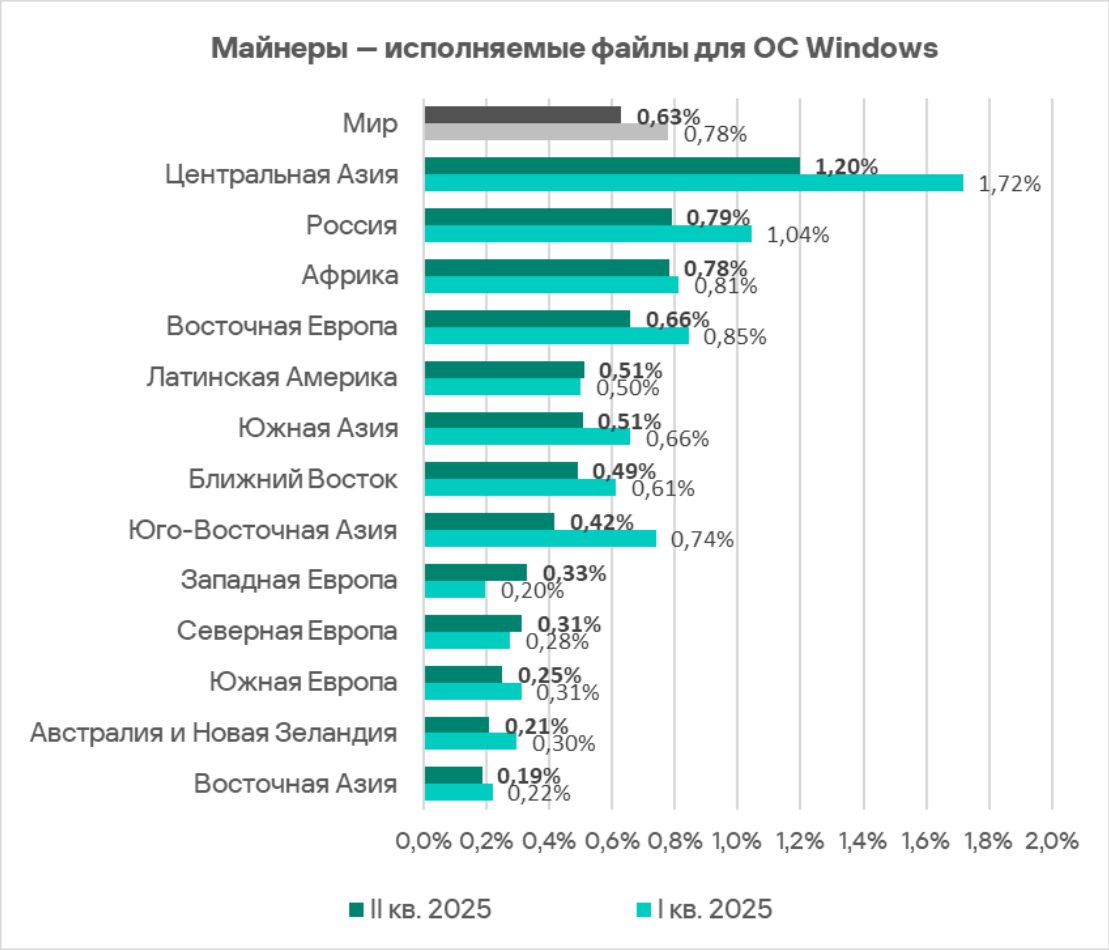


Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, варьирует от 0,19% в Восточной Азии до 1,20% в Центральной Азии. Лидируют по этому показателю Центральная Азия, Россия и Африка.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

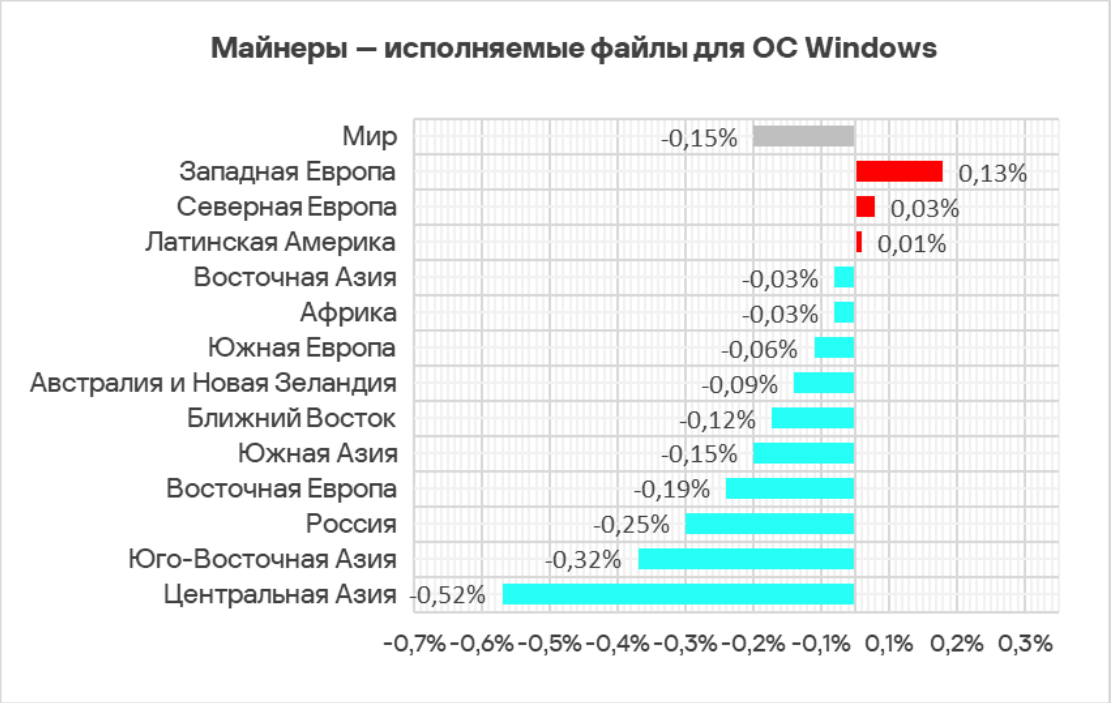
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, II квартал 2025 года



Доля компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, во втором квартале 2025 года больше всего выросла в Западной Европе.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

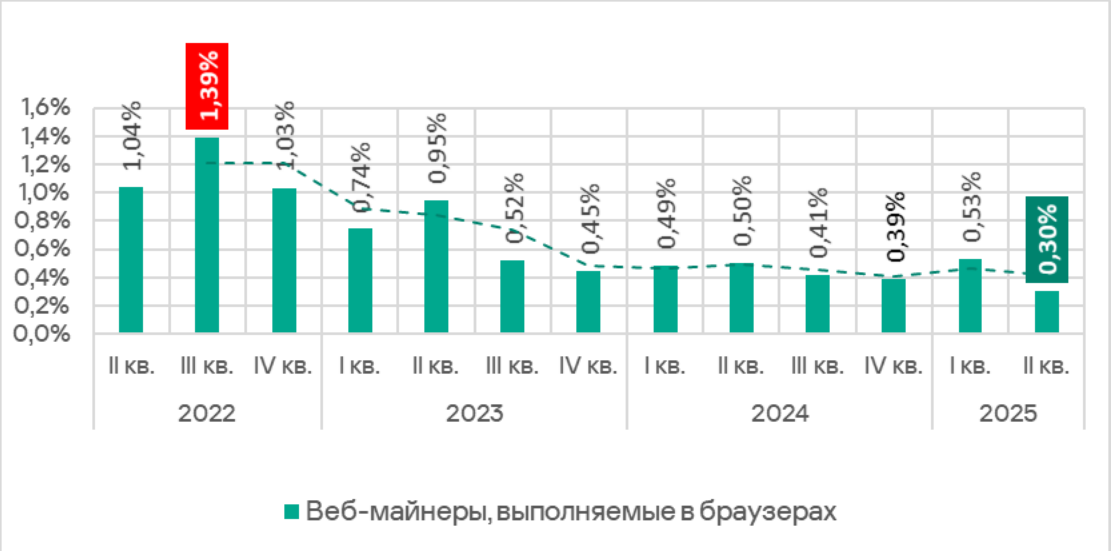
Изменение доли компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, II квартал 2025 года



Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, во втором квартале 2025 года уменьшилась до 0,30%. Это минимальное значение со второго квартала 2022 года.

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, II квартал 2022 года — II квартал 2025 года



В мае 2025 года был отмечен минимальный месячный показатель за период с апреля 2023 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, варьирует от 0,11% в Восточной Азии до 0,54% в Африке: Топ 3 регионов по этому показателю — Африка, Латинская Америка и Юго-Восточная Азия.

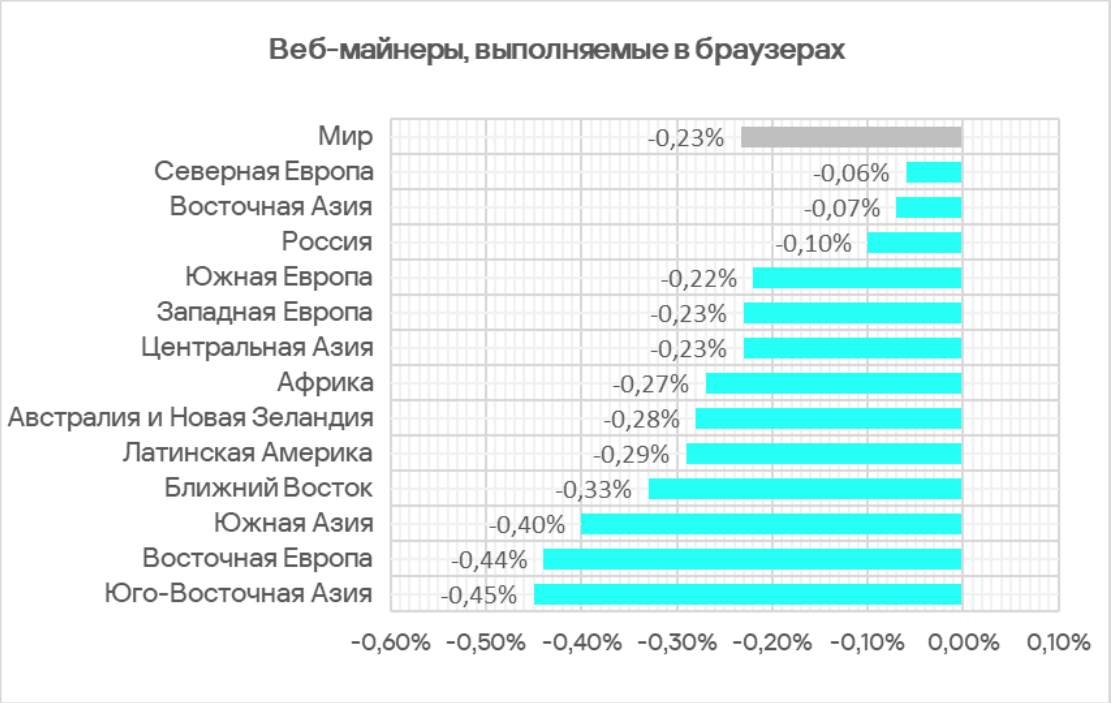
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, II квартал 2025 года

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы веб-майнеры, уменьшилась во всех регионах.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, II квартал 2025 года



Самораспространяющееся вредоносное ПО. Черви и вирусы

Самораспространяющееся вредоносное ПО — черви и вирусы — относится к отдельной категории. Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнетов, приобрели черты угроз следующего этапа.

Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

Среди распространяющихся вирусов и червей довольно много старых, их командные серверы уже отключены. Тем не менее, они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, — но также могут приводить к сбоям в работе ПО, отказам в обслуживании и т. п.

Высокие показатели обнаружения самораспространяющегося вредоносного ПО и ПО, которое распространяется через сетевые папки, на уровне отрасли, страны или региона, как правило, указывают на наличие незащищенной технологической инфраструктуры, в которой отсутствует даже базовая защита конечных устройств. Эти незащищенные компьютеры становятся источниками распространения вредоносного ПО. Ситуацию

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

может ухудшать и слабая сегментация сети предприятия, и отсутствие контроля использования съемных носителей информации.

Черви

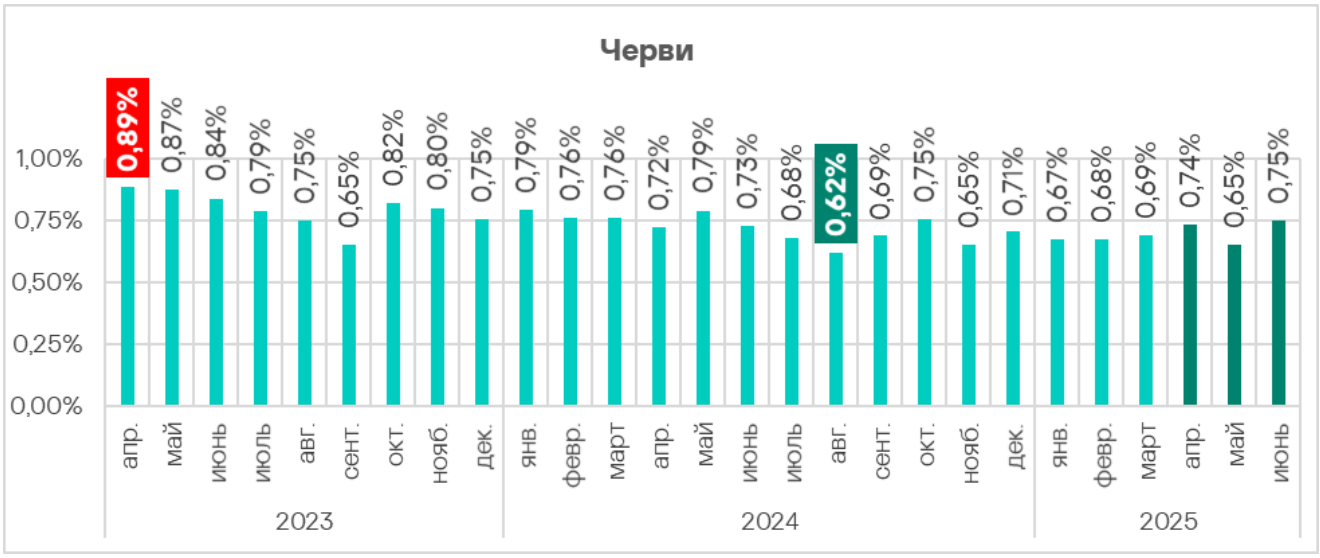
В сетях АСУ встречаются новые версии червей, используемые злоумышленниками для распространения шпионского ПО, программ-вымогателей и майнеров. Чаще всего эти черви используют эксплойты известных уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

Доля компьютеров АСУ, на которых были заблокированы черви, уменьшилась во втором квартале 2025 года до 1,22%. Это минимальный показатель со второго квартала 2022 года

Доля компьютеров АСУ, на которых были заблокированы черви, II квартал 2022 года — II квартал 2025 года

В течение квартала самым высоким показатель за месяц был в июне.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

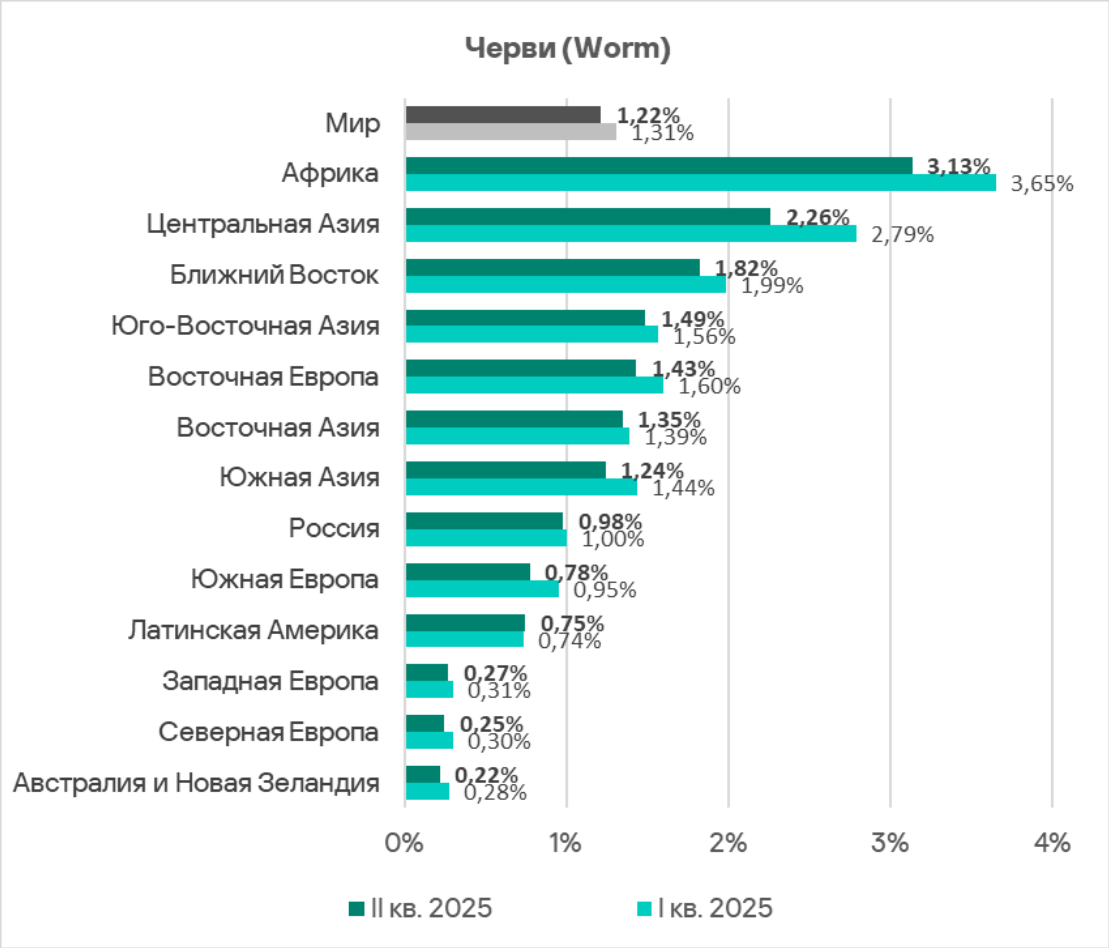


Доля компьютеров АСУ, на которых были заблокированы черви, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы черви, варьирует от 0,22% в Австралии и Новой Зеландии до 3,13% в Африке. Топ 3 регионов по этому показателю неизменен: Африка, Центральная Азия и Ближний Восток.

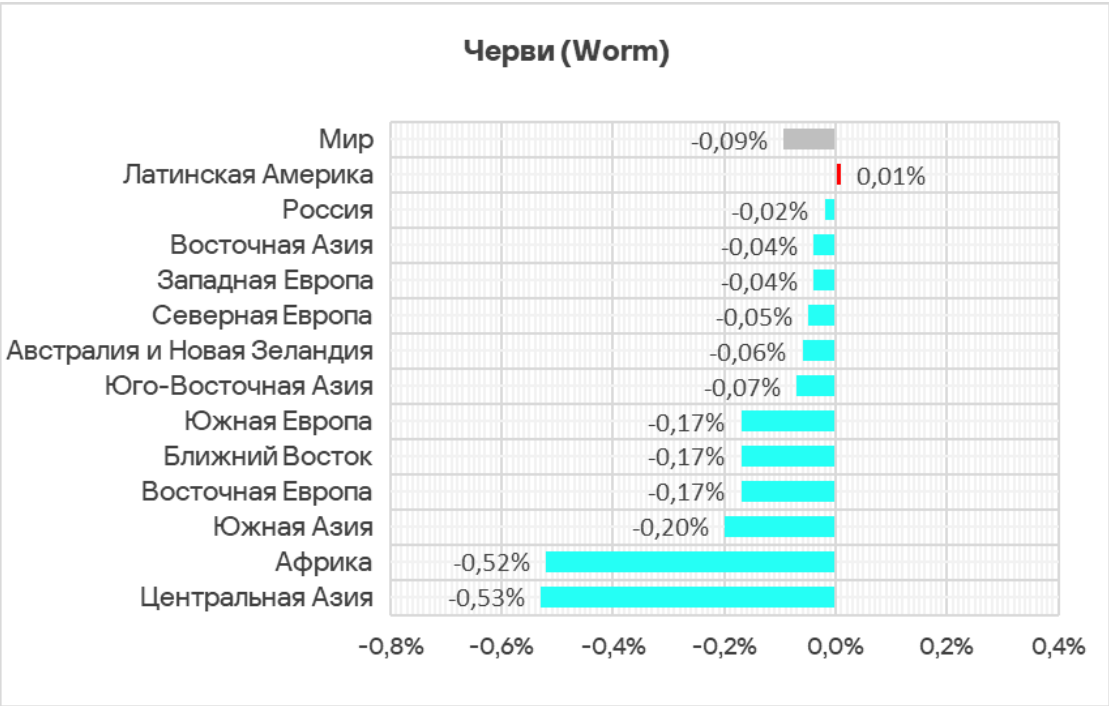
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы черви, II квартал 2025 года



Во всех регионах, кроме Латинской Америки, показатель уменьшился.

Изменение доли компьютеров АСУ, на которых были заблокированы черви, II квартал 2025 года

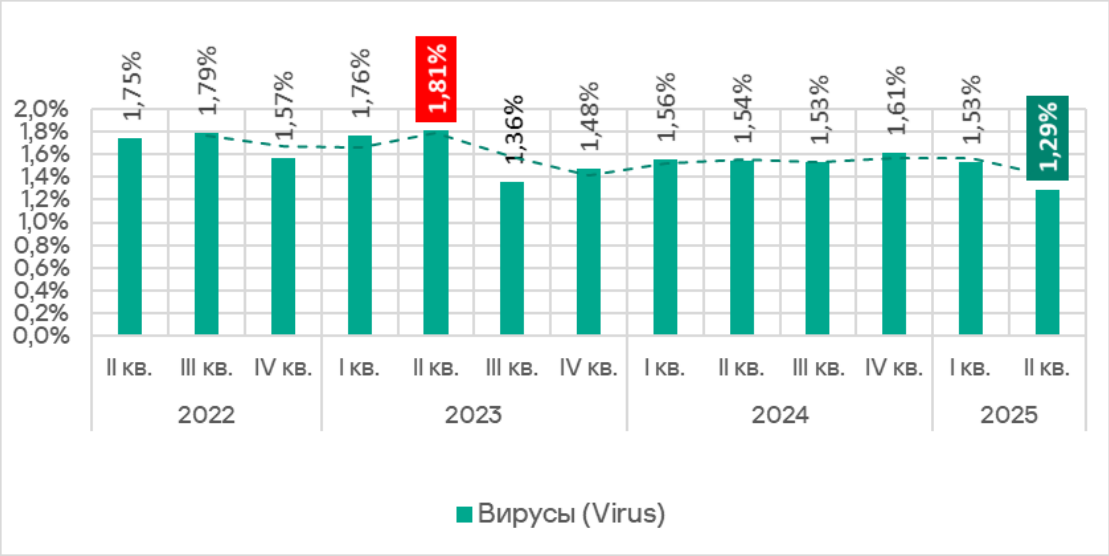


© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

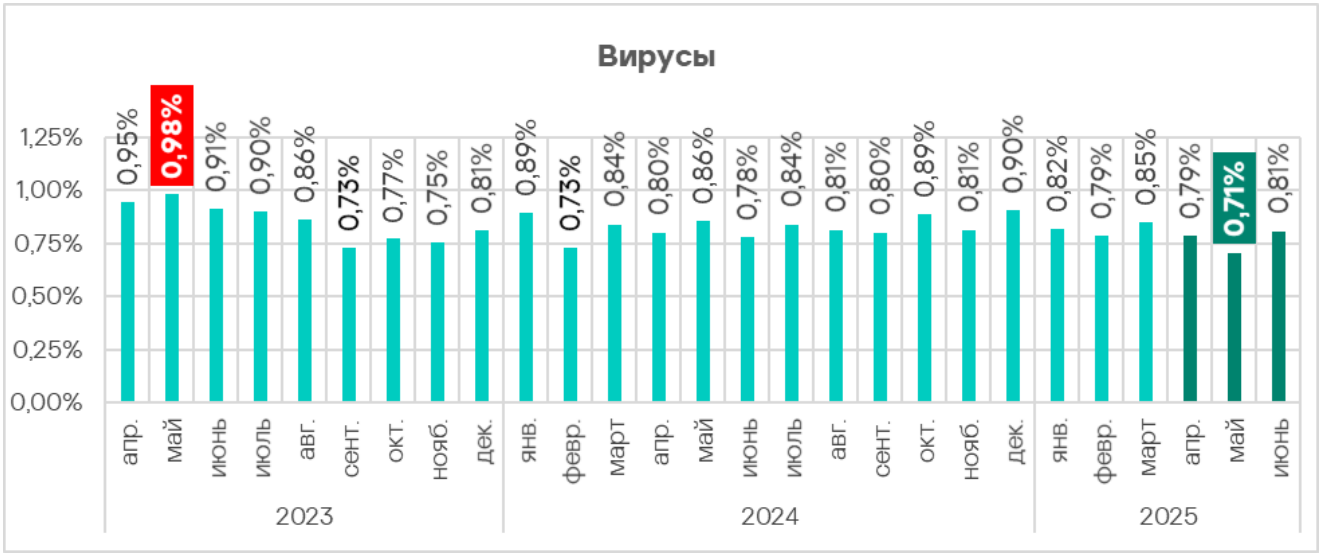
Вирусы

Доля компьютеров АСУ, на которых были заблокированы вирусы, во втором квартале 2025 года, как и у червей, уменьшилась до минимального со второго квартала 2022 года значения (1,29%).

Доля компьютеров АСУ, на которых были заблокированы вирусы, II квартал 2022 года — II квартал 2025 года



Минимальное месячное значение показателя в период с апреля 2023 года пришлось на май 2025 года.



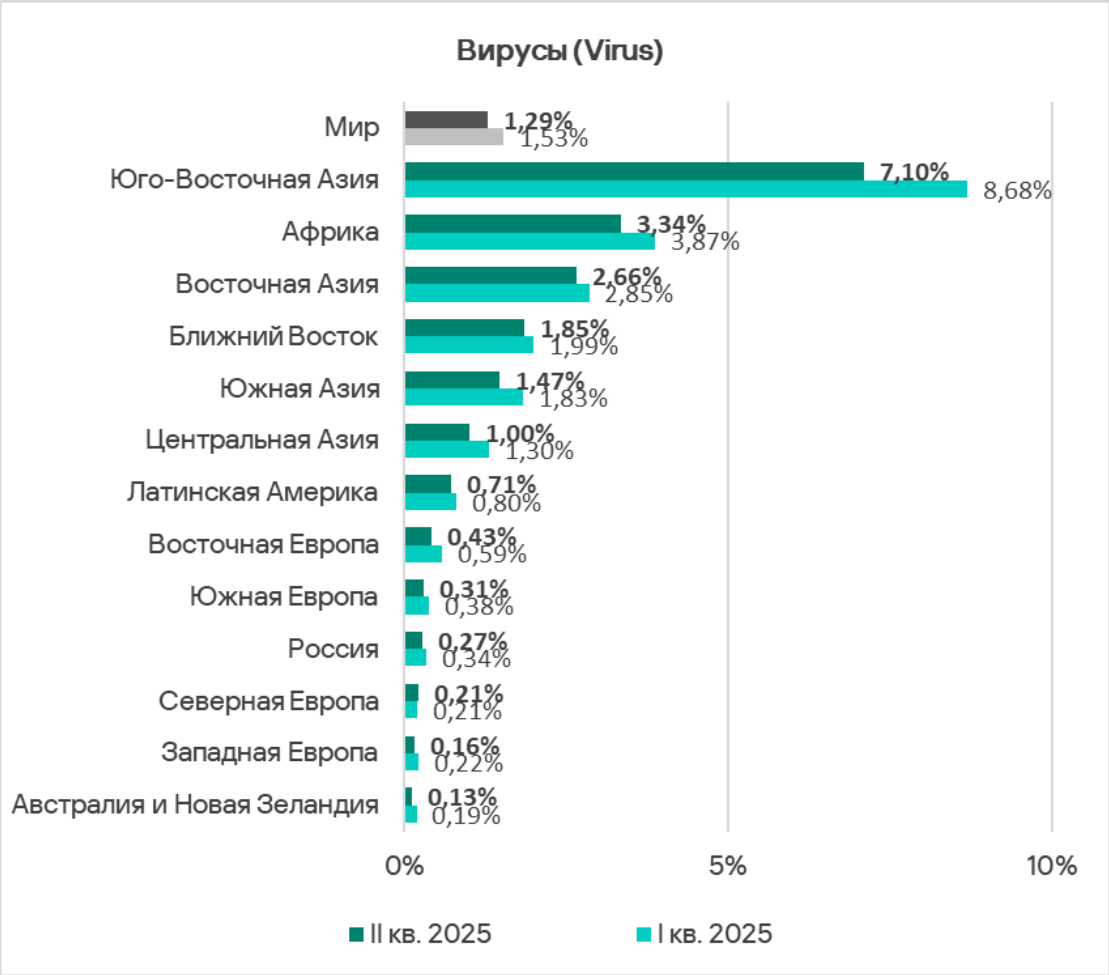
Доля компьютеров АСУ, на которых были заблокированы вирусы, апрель 2023 года — июнь 2025 года

В регионах доля компьютеров АСУ, на которых были заблокированы вирусы, варьирует от 0,13% в Австралии и Новой Зеландии до 7,10% в Юго-Восточной Азии. Топ 3 регионов по этому показателю, как и в случае

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

вредоносных программ для AutoCAD, не меняется: Юго-Восточная Азия, Африка и Восточная Азия.

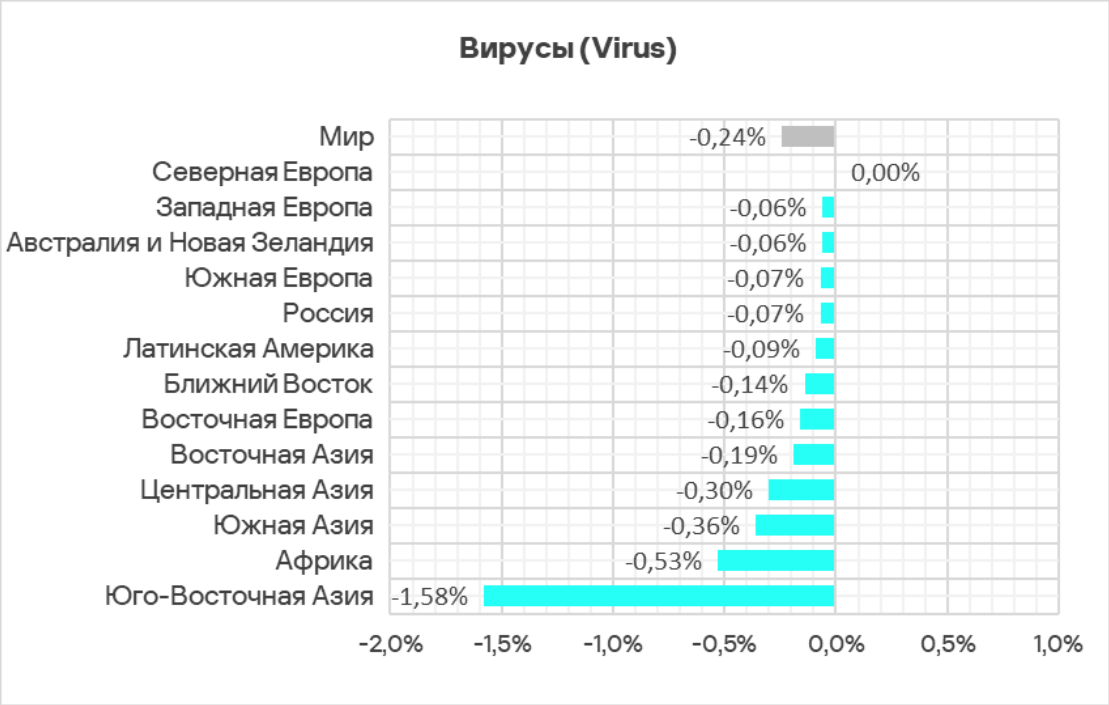
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вирусы, II квартал 2025 года



Доля компьютеров АСУ, на которых были заблокированы вирусы, во втором квартале 2025 года уменьшилась во всех регионах, кроме Северной Европы.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы вирусы, II квартал 2025 года



Вредоносные программы для AutoCAD

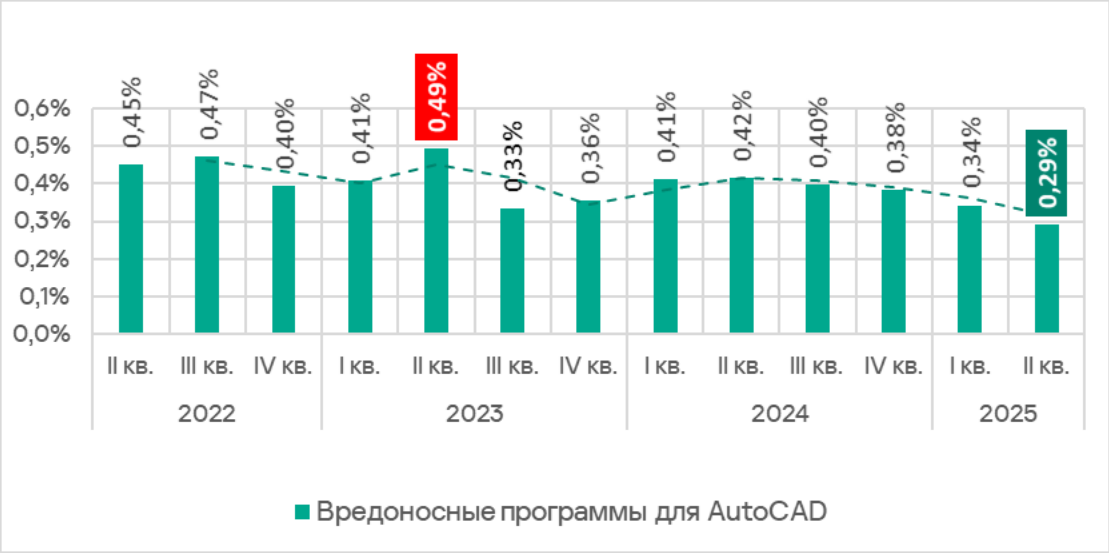
Эта категория вредоносного ПО может распространяться по-разному, поэтому не относится к конкретной группе.

Как правило, вредоносные программы для AutoCAD — минорная угроза, которая в рейтинге категорий вредоносных объектов по доле компьютеров АСУ, на которых она была заблокирована, занимает последние места.

Во втором квартале 2025 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, продолжила снижаться. Показатель был минимальным в период со второго квартала 2022 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, II квартал 2022 года — II квартал 2025 года



В регионах доля компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, варьирует от 0,01% в Северной и Западной Европе до 2,30% в Юго-Восточной Азии. Лидируют по этому показателю те же регионы, что и в рейтинге по вирусам: Юго-Восточная Азия, Восточная Азия и Африка.

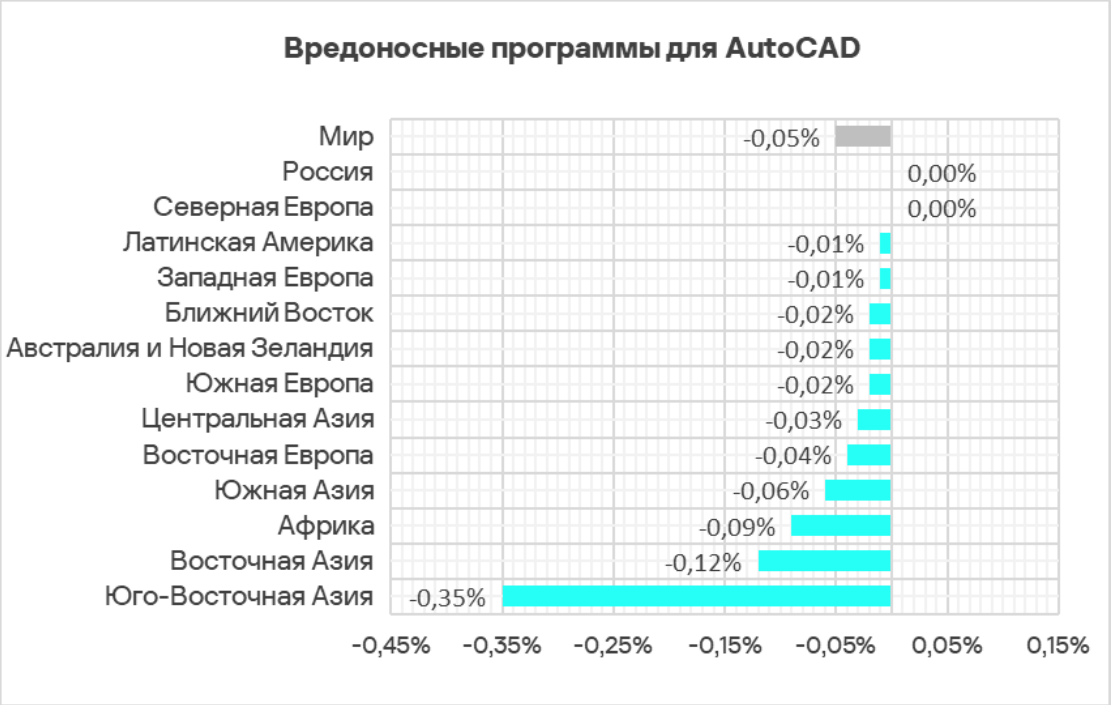
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, II квартал 2025 года

Как и в случае вирусов, показатель вредоносных программ для AutoCAD во втором квартале 2025 года уменьшился во всех регионах.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные программы для AutoCAD, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Основные источники угроз

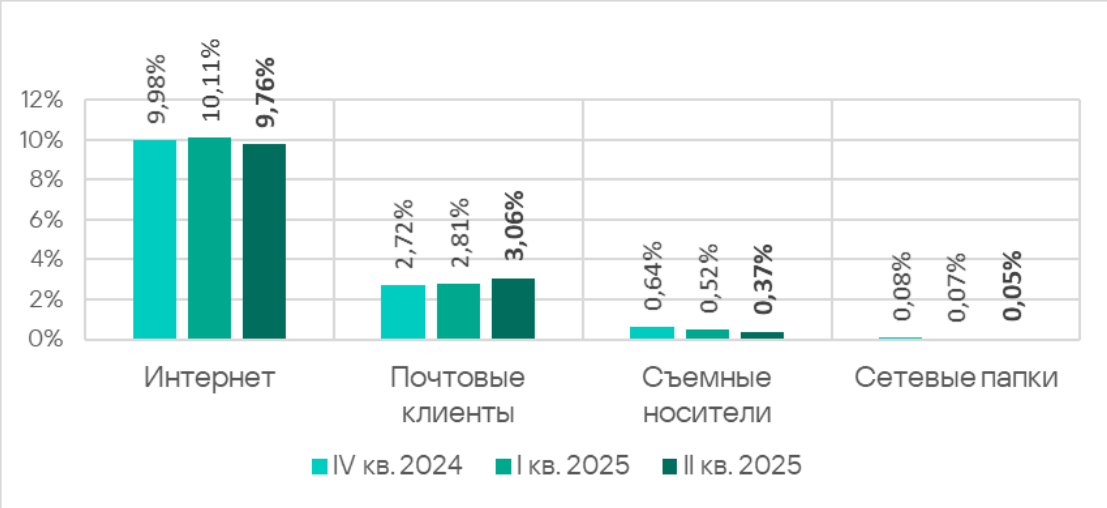
В зависимости от сценария обнаружения и блокирования угрозы не всегда возможно надежно определить ее источник. Косвенным признаком того или иного источника может быть вид (категория) заблокированной угрозы.

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет (обращения к вредоносным или скомпрометированным интернет-ресурсам; вредоносный контент, распространяемый через мессенджеры; облачные сервисы хранения и обработки данных и CDN), почтовые клиенты (фишинговые рассылки) и съемные носители.

Во втором квартале 2025 года продолжила расти доля компьютеров АСУ, на которых в течение квартала были заблокированы угрозы, распространяемые через почту. Этот показатель за квартал вырос во всех регионах, кроме России.

Показатели остальных источников угроз в среднем по миру уменьшились.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников



Интернет

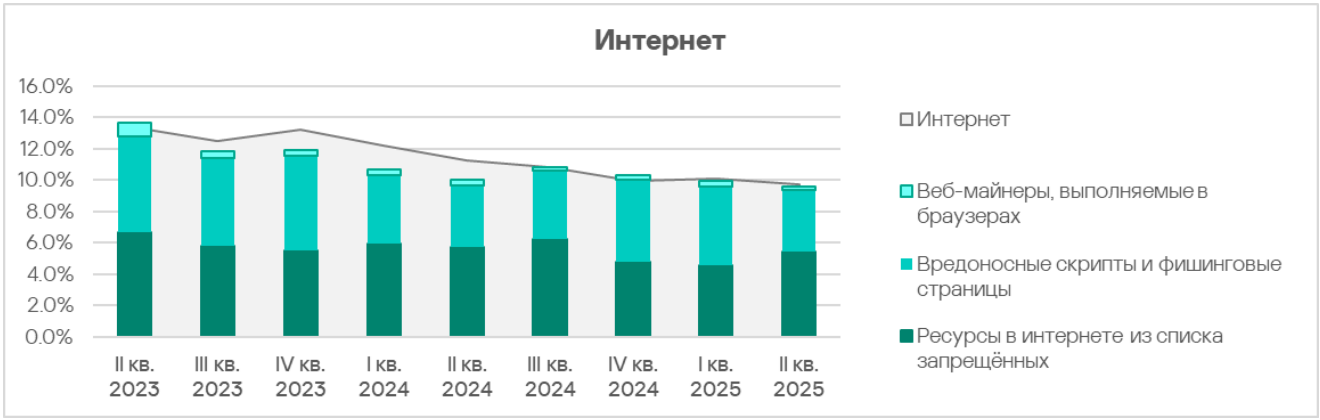
Обнаружение и блокирование угроз из интернета на компьютерах АСУ, защищенных решением «Лаборатории Касперского», означает, что на момент обнаружения с них был разрешен доступ к внешним сервисам.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, уменьшилась до 9,76% — это минимальный показатель в период со второго квартала 2022 года.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, II квартал 2022 года — II квартал 2025 года

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



Угрозы из интернета и основные категории угроз из интернета, II квартал 2023 года — II квартал 2025 года

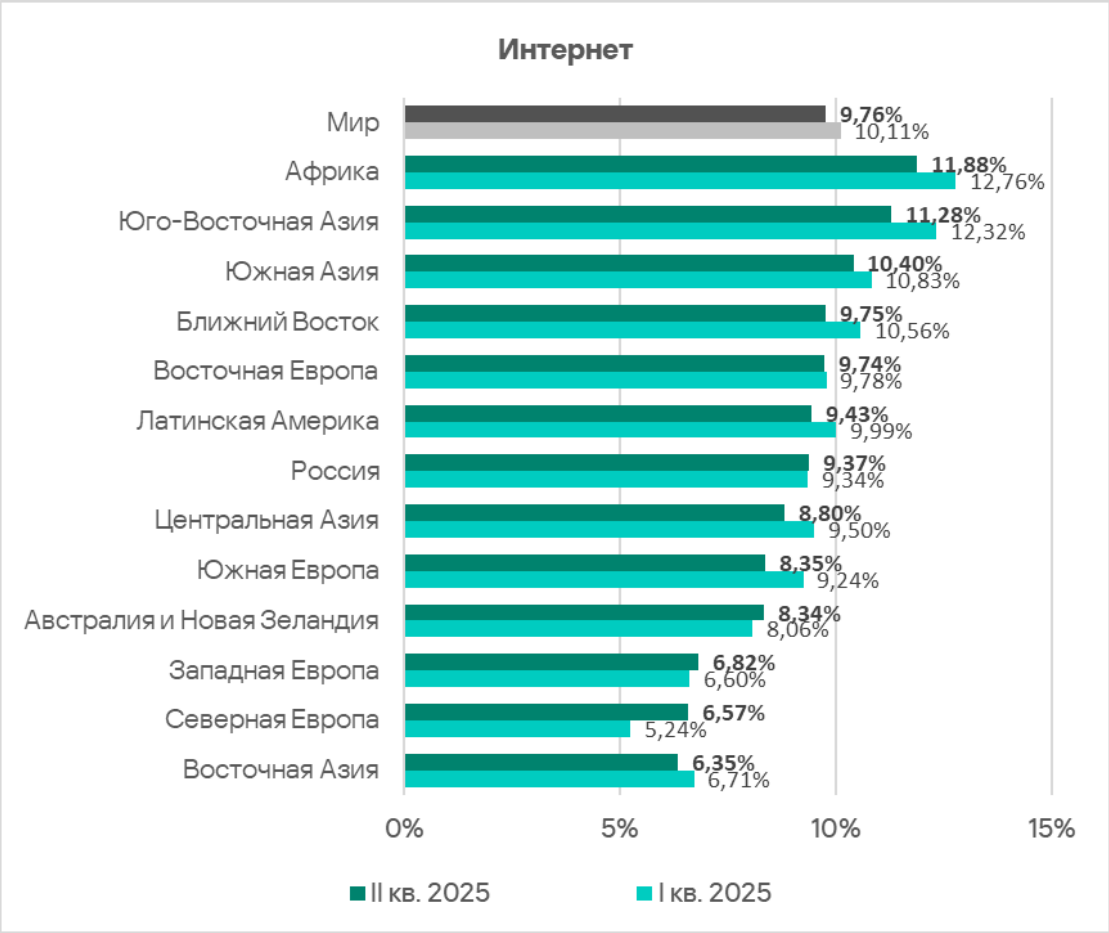
Напомним, что один и тот же компьютер в течение квартала может быть атакован несколькими категориями вредоносного ПО, которое распространяется из одного источника. Такой компьютер будет учтен при подсчете процента атакованных компьютеров для каждой категории угроз, но для источника угроз будет учитываться лишь один раз (мы считаем уникальные атакованные компьютеры). К тому же, однозначно определить первоначальной попытки заражения не всегда представляется возможным. Поэтому суммарная доля компьютеров АСУ, на которых были заблокированы различные категории угроз из определенного источника, превышает долю угроз из самого источника.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы из интернета, варьирует от 6,35% в Восточной Азии до 11,88% в Африке.

Топ 3 регионов по доле компьютеров АСУ, на которых во втором квартале 2025 года были заблокированы угрозы из интернета: Африка, Юго-Восточная Азия и Южная Азия.

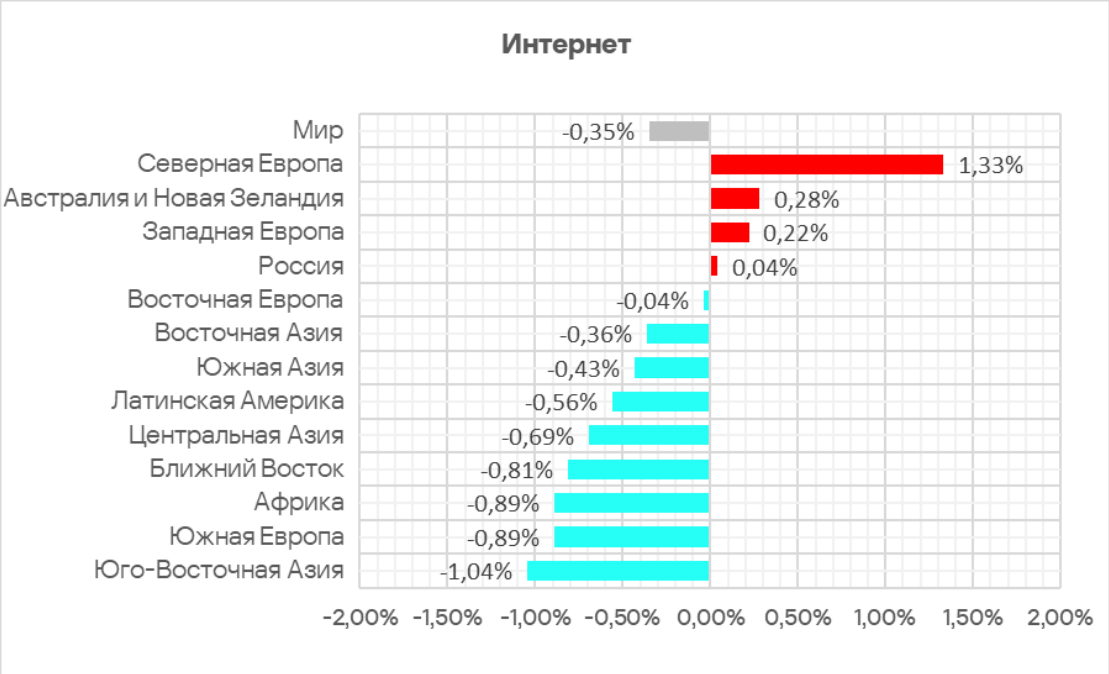
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из интернета, II квартал 2025 года



Во втором квартале 2025 показатель угроз из интернета увеличился в четырех регионах, больше всего — в Северной Европе.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из интернета, II квартал 2025 года



Почтовые клиенты

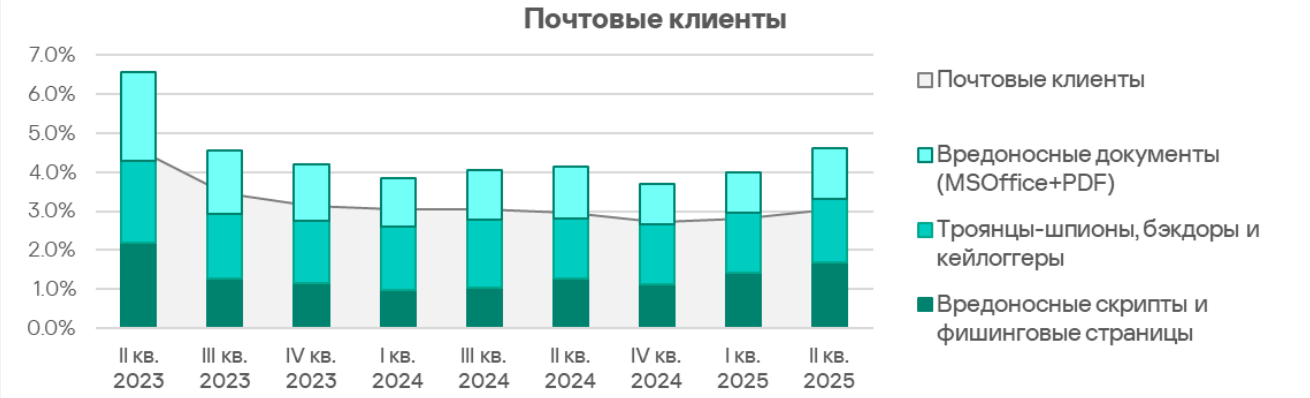
Некоторые из обнаруженных и заблокированных угроз были доставлены на защищенный компьютер системой доставки почты и/или пытались получить доступ через клиентское приложение электронной почты.

Во втором квартале 2025 года доля компьютеров АСУ, на которых были заблокированы такие угрозы, снова увеличилась.

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, II квартал 2022 года — II квартал 2025 года

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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



Угрозы из почтовых клиентов и основные категории угроз из почтовых клиентов, II квартал 2023 года — II квартал 2025 года

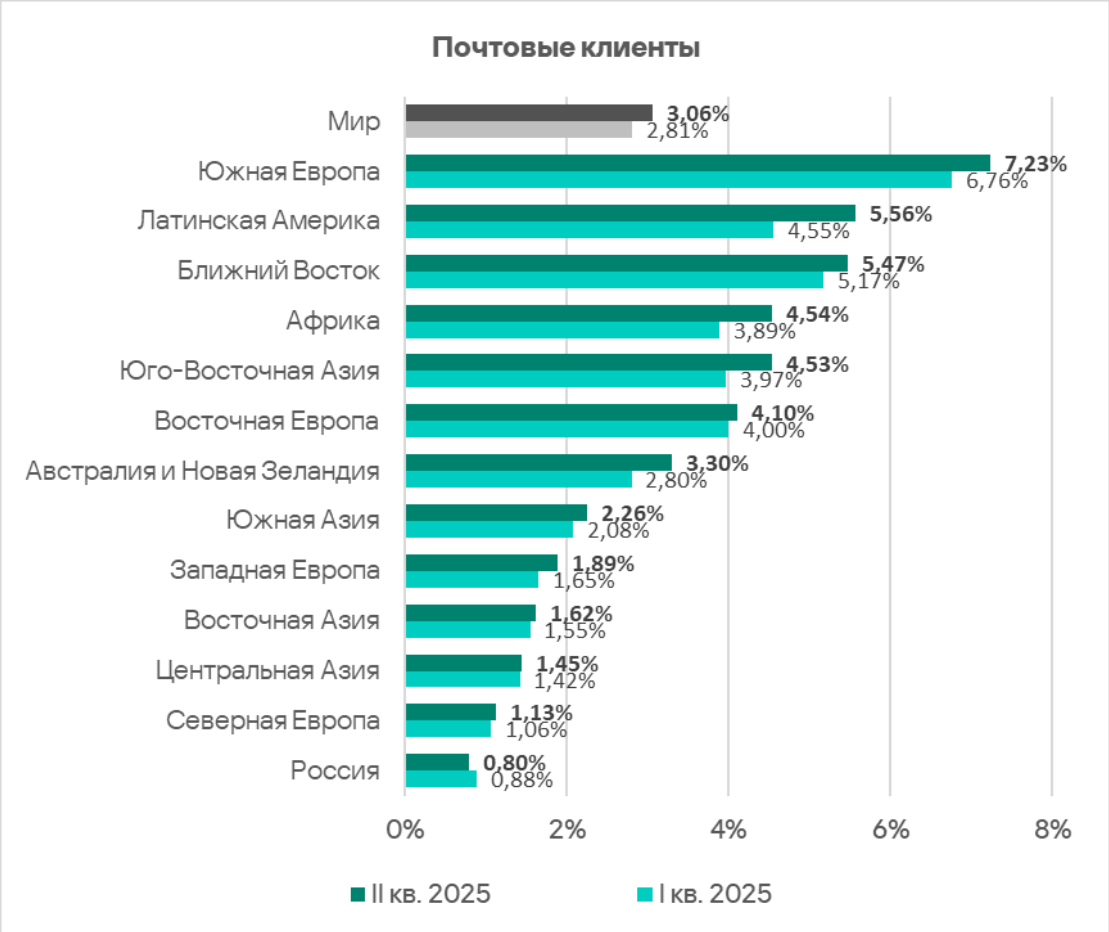
Чтобы избежать обнаружения, большинство шпионских программ, обнаруженных в фишинговых письмах, доставлялись в форме архива или многослойного скрипта, либо в виде отдельного файла, либо встроенного в форматы офисных документов.

В регионах доля компьютеров АСУ, на которых были заблокированы угрозы, распространяемые через электронную почту, варьирует от 0,80% в России до 7,23% в Южной Европе.

Топ 3 регионов по уровню угроз из почтовых клиентов: Южная Европа, Латинская Америка и Ближний Восток.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

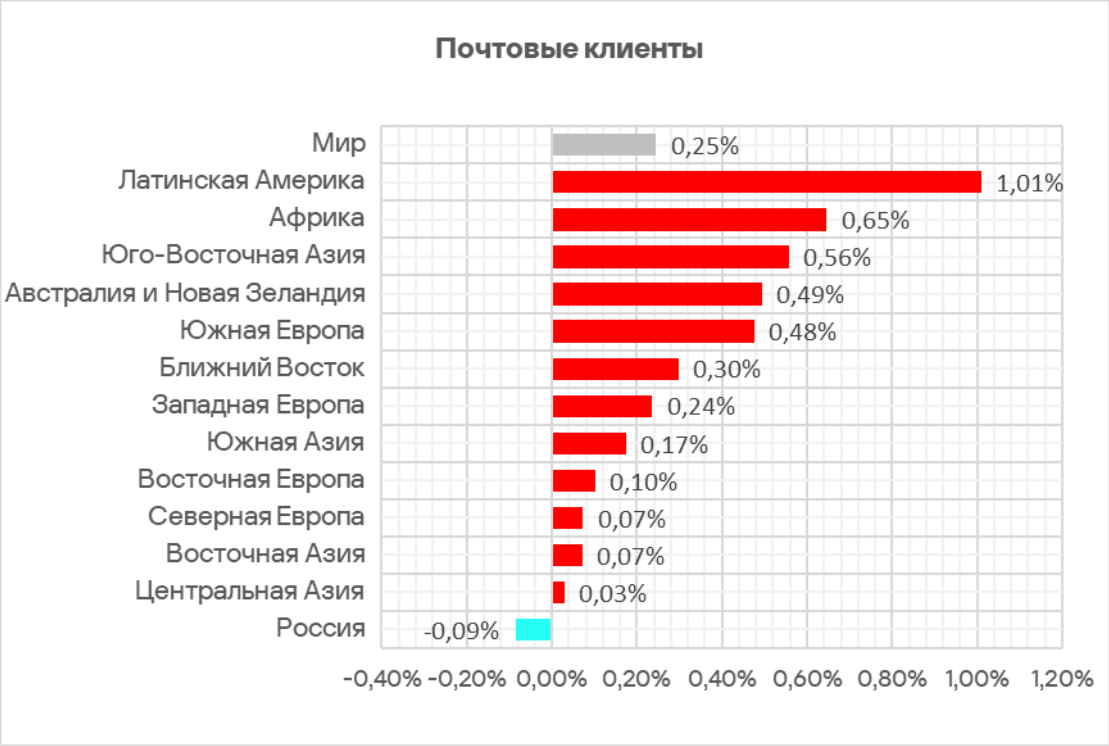
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, II квартал 2025 года



Во втором квартале 2025 показатель угроз из почтовых клиентов увеличился во всех регионах, кроме России, больше всего — в Латинской Америке.

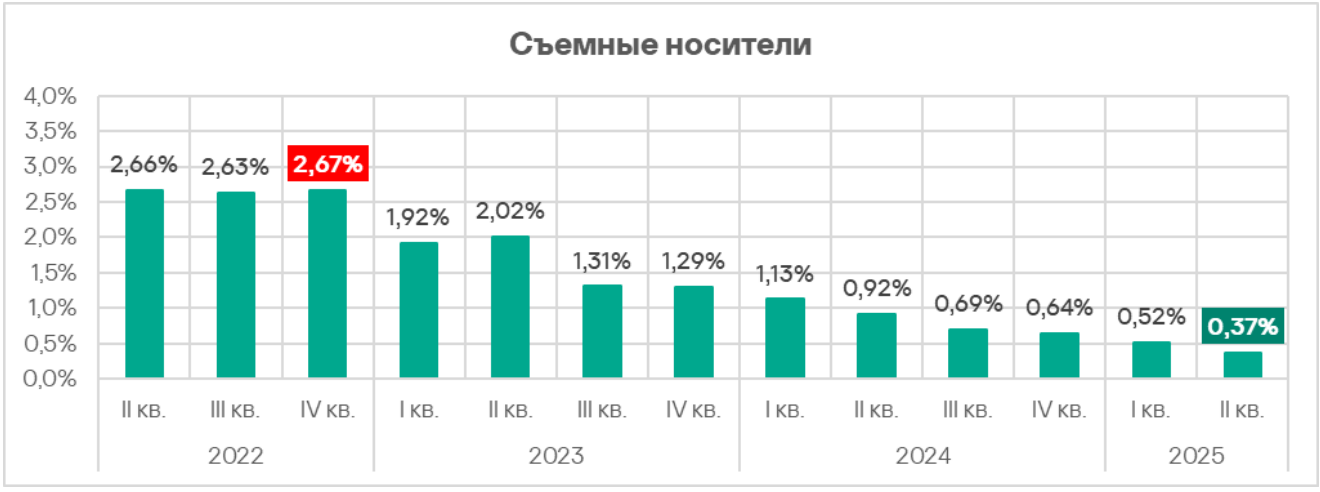
© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, II квартал 2025 года



Съемные носители

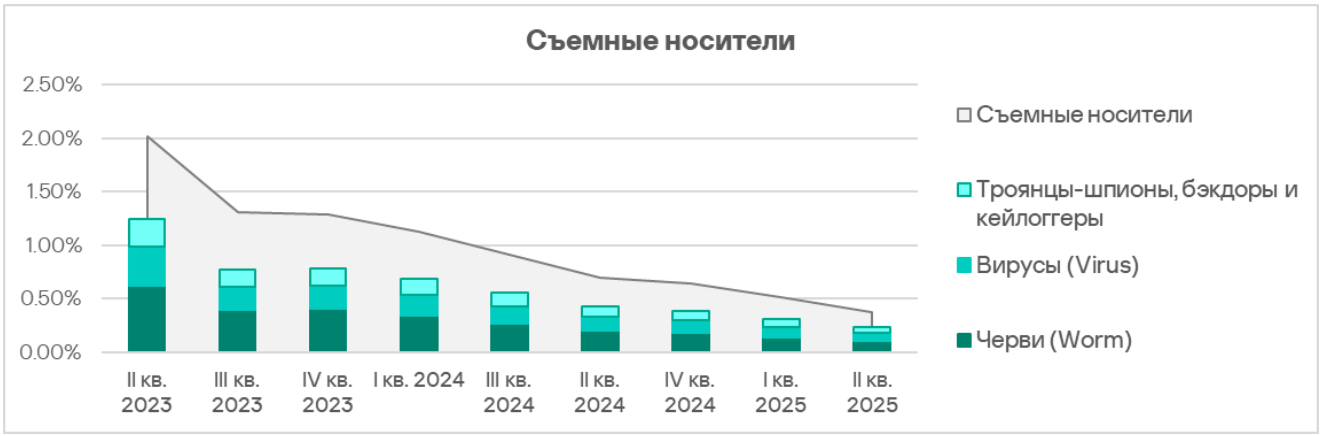
Доля компьютеров АСУ, на которых угрозы были обнаружены при подключении съемных носителей, продолжила снижаться и достигла минимальных значений с начала 2022 года.



Доля компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, II квартал 2022 года — II квартал 2025 года

Основными категориями угроз, которые блокируются при подключении съемных устройств к компьютерам АСУ, являются черви, вирусы и шпионское ПО.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»



Угрозы на съемных носителях и основные категории угроз на съемных носителях, II квартал 2023 года — II квартал 2025 года

Большинство червей и вирусов, обнаруживаемых на съемных носителях, представляют собой либо варианты устаревших полиморфных угроз (возникших около 2010 года), либо современные модульные криптомайнеры. Эти современные криптомайнеры способны распространяться по локальным сетям, используя кражу учетных данных с зараженных хостов, эксплуатируя уязвимости (известные, но еще не закрытые) и выполняя атаки на сетевые службы методом перебора (брутфорс).

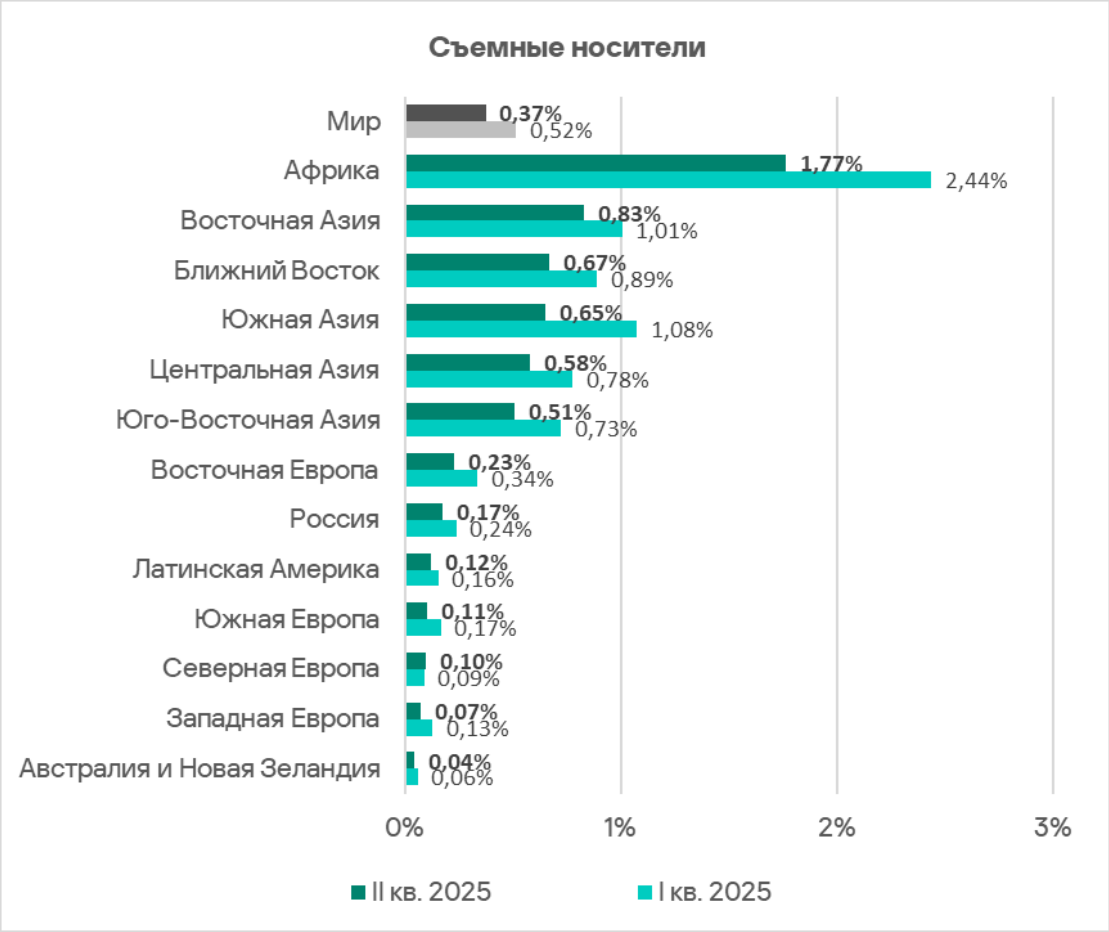
Большинство шпионских программ, обнаруженных на съемных носителях, состояли из универсальных компонентов как современных, так и устаревших червей, таких как стилеры, загрузчики, AV-киллеры.

В регионах доля компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей, варьирует от 0,04% в Австралии и Новой Зеландии до 1,77% в Африке.

Топ 3 регионов по доле компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей: Африка, Восточная Азия и Ближний Восток.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, II квартал 2025 года



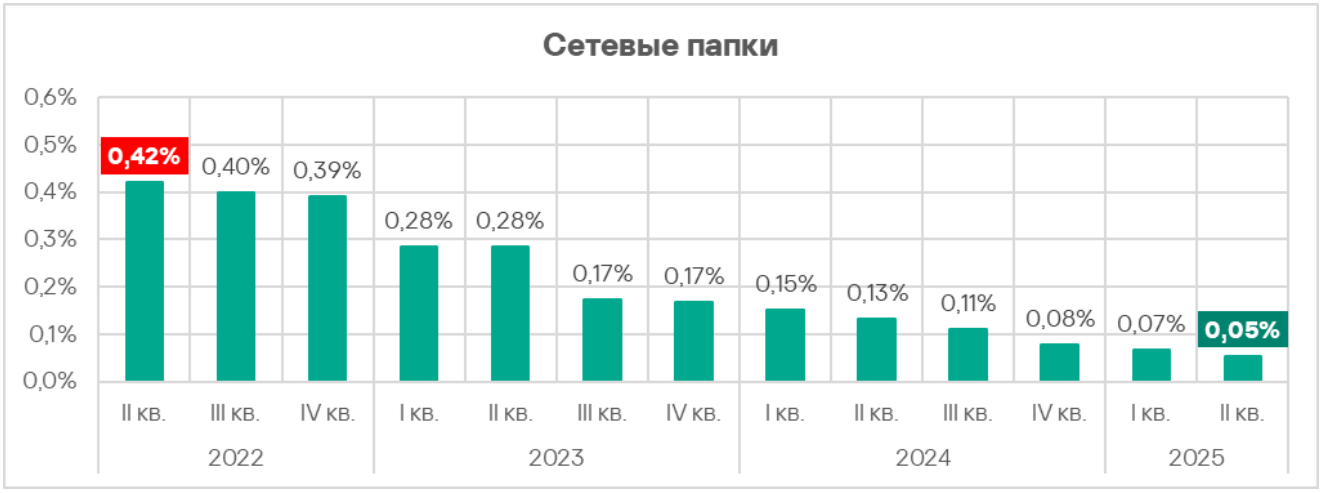
Во втором квартале 2025 показатель угроз со съемных носителей уменьшился во всех регионах, кроме Северной Европы.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, II квартал 2025 года

Сетевые папки

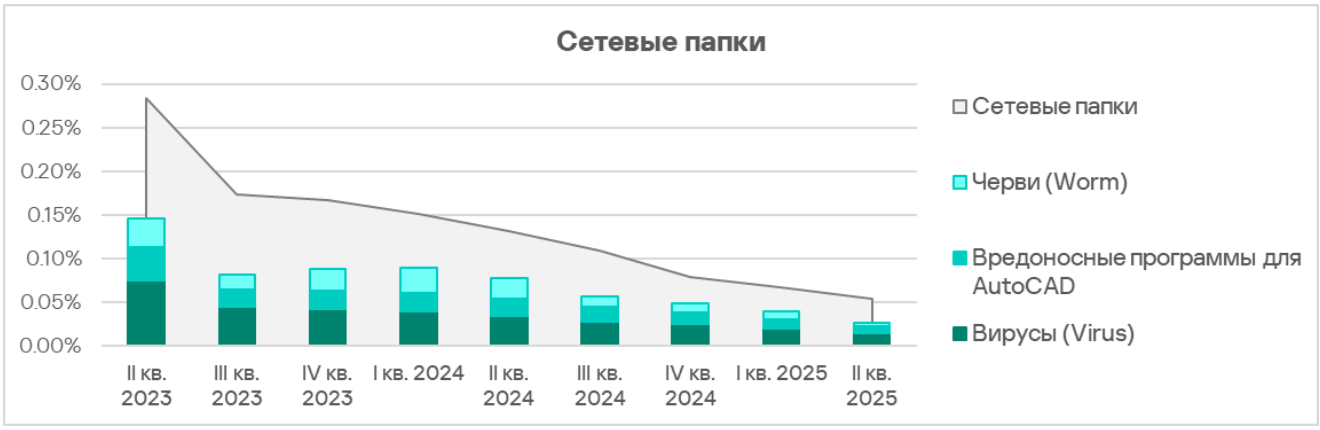
Показатели по сетевым папкам достигли минимальных значений в период со второго квартала 2022 года. Это минорный источник угроз, однако не стоит его недооценивать — через сетевые папки распространяются черви, вирусы и вредоносное ПО для AutoCAD.



Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, II квартал 2022 года — II квартал 2025 года

Основными категориями угроз, которые распространяются через сетевые папки, являются черви, вирусы и вредоносное ПО для AutoCAD.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

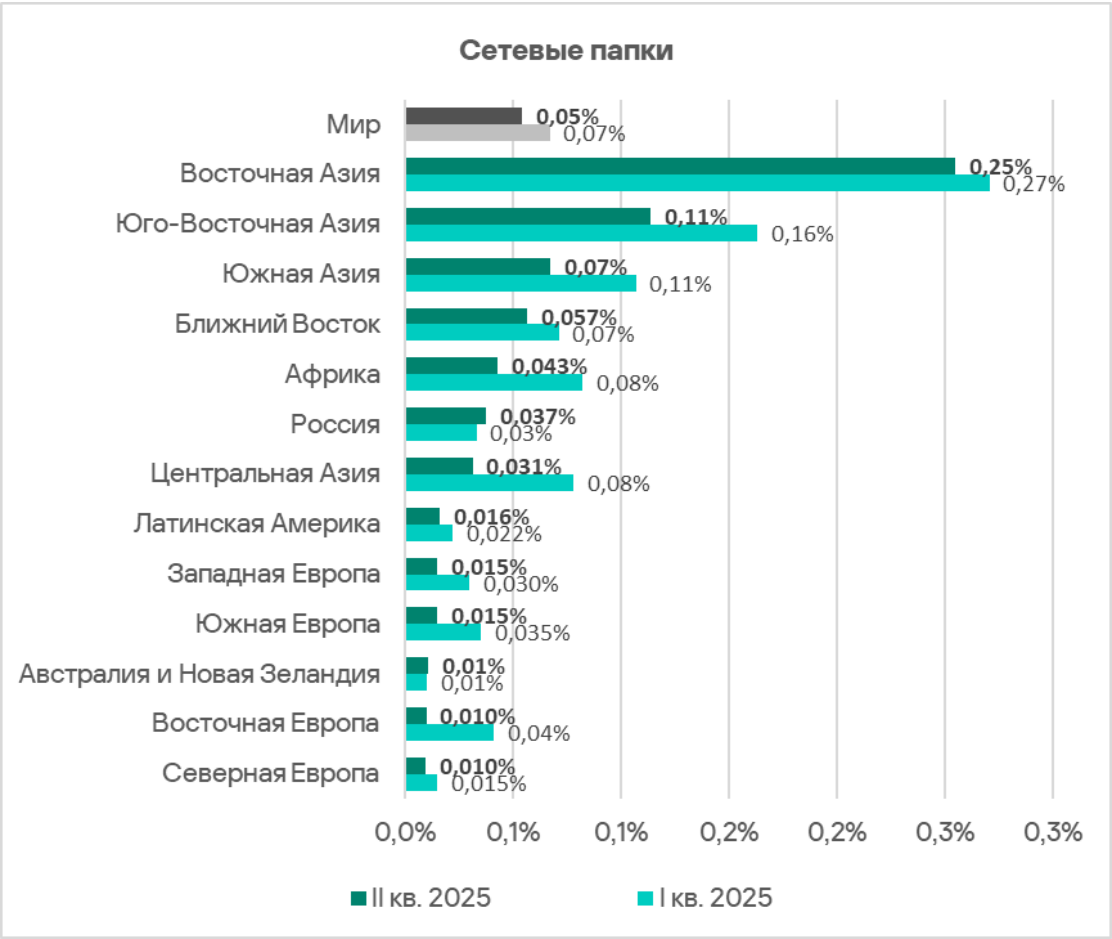


Угрозы в сетевых папках и основные категории угроз в сетевых папках, II квартал 2023 года — II квартал 2025 года

В регионах доля компьютеров АСУ, на которых угрозы были заблокированы в сетевых папках, варьирует от 0,01% в Северной Европе до 0,25% в Восточной Азии.

Топ 3 регионов по уровню угроз в сетевых папках: Восточная, Юго-Восточная и Южная Азия.

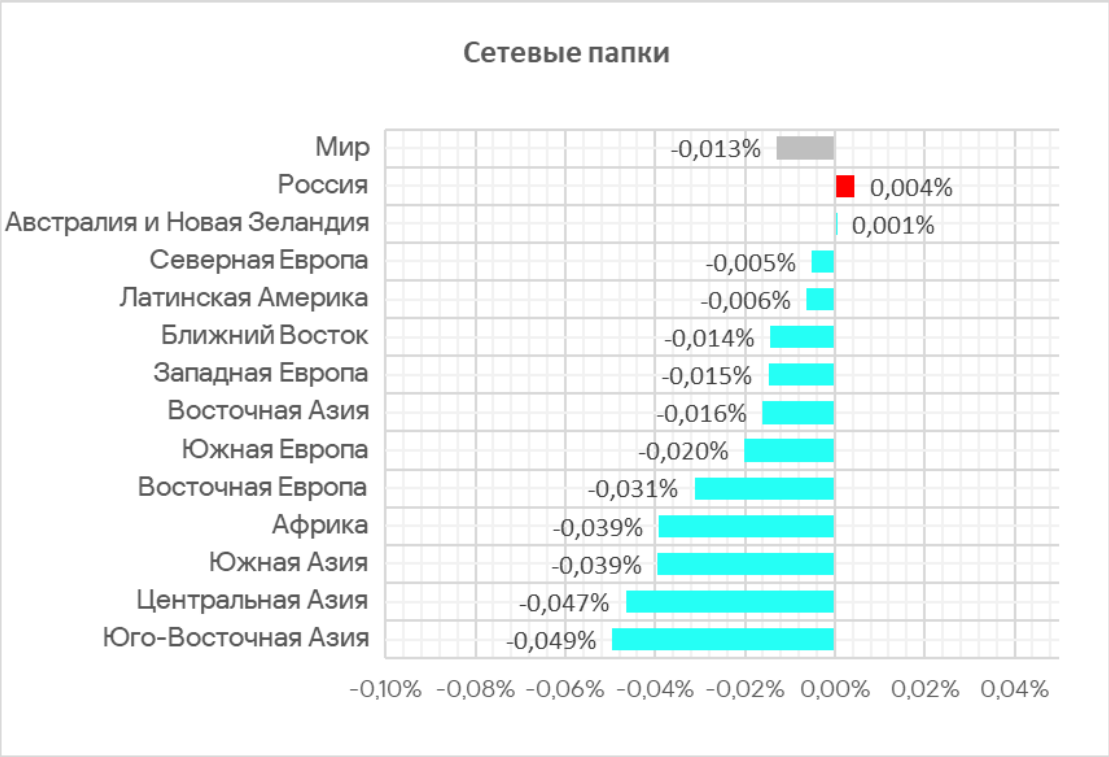
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Во втором квартале 2025 показатель угроз в сетевых папках уменьшился во всех регионах, кроме России и Австралии и Новой Зеландии.

Изменение доли компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, II квартал 2025 года



© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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.

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

© 2025 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»