kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2023

Kaspersky ICS CERT

19.03.2024 Version 1.0

2023 — цифры года

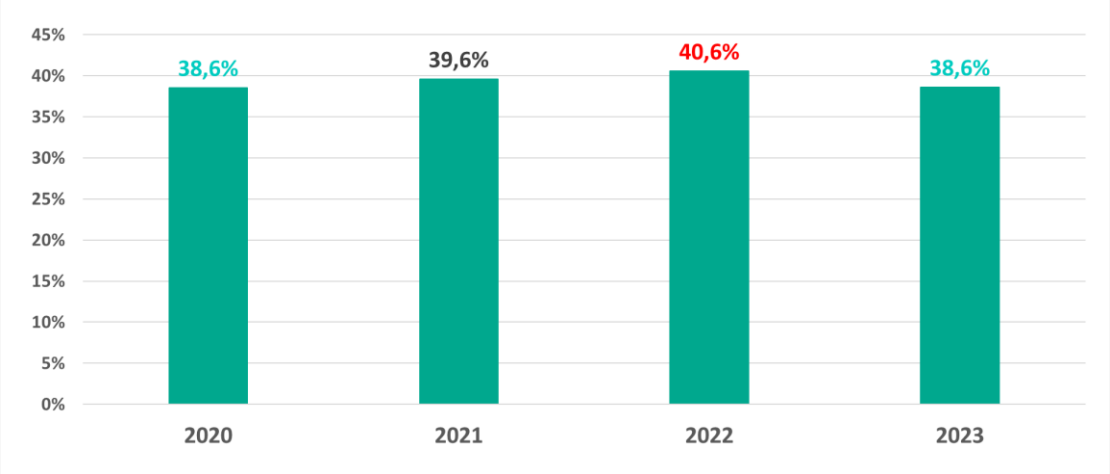
Показатель	H1 2023	H2 2023	2023
Процент атакованных компьютеров АСУ в мире	34,0%	31,9%	38,6%
Основные источники угроз			
Интернет	19,3%	18,1%	22,8%
Почтовые клиенты	6,0%	4,0%	5,4%
Съемные носители	3,4%	1,9%	3,2%
Сетевые папки	0,49%	0,25%	0,45%
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы (JS и HTML)	12,7%	10,9%	14,7%
Ресурсы в интернете из списка запрещённых	11,3%	10,1%	13,7%
Троянцы-шпионы, бэкдоры и кейлоггеры	6,1%	5,3%	7,1%
Вредоносные документы (MSOffice+PDF)	4,0%	2,9%	4,0%
Черви (Worm)	2,3%	2,1%	3,0%
Вирусы (Virus)	2,4%	2,1%	2,8%
Веб-майнеры, выполняемые в браузерах	1,3%	0,76%	1,3%
Майнеры — исполняемые файлы для ОС Windows	0,59%	0,85%	1,1%
Программы-вымогатели	0,32%	0,25%	0,37%

2023 год

Возврат к минимуму

После роста в 2021 и 2022 году процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился на 2 п.п. и вернулся к значениям 2020 года.

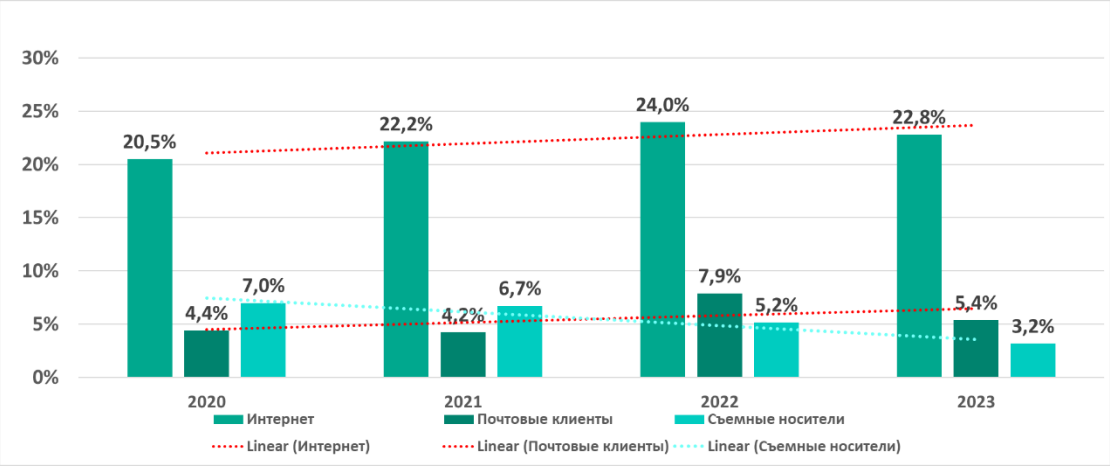
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, 2020 – 2023 годы



При этом в 2023 году по сравнению с 2020 годом изменились проценты по основным источникам угроз:

- увеличились проценты компьютеров АСУ, на которых были заблокированы угрозы из интернета и в почте,
- более чем вдвое уменьшился процент компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из разных источников, 2020 – 2023 годы

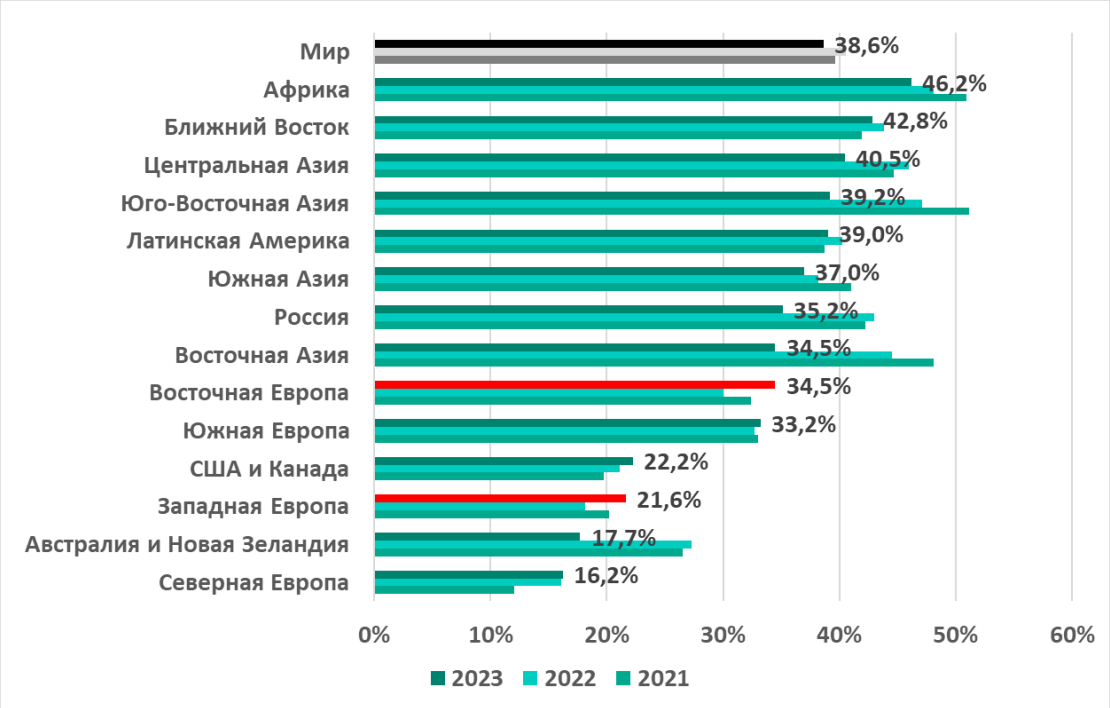


Красные линии 2023 года

По итогам 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился в двух регионах:

- в Восточной Европе – на 4,4 п.п.
- в Западной Европе – на 3,5 п.п.

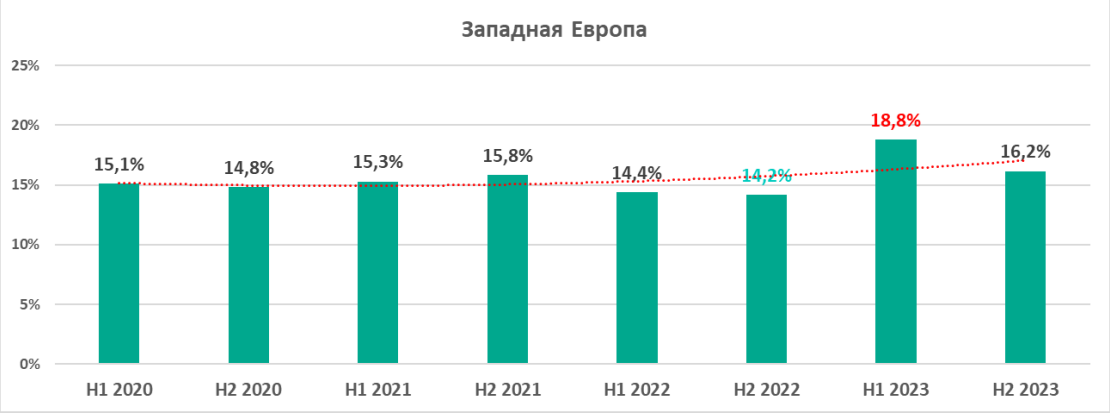
Регионы и мир. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, 2021, 2022 и 2023 год



Как видно на графиках ниже, ситуация в этих двух регионах заметно отличается.

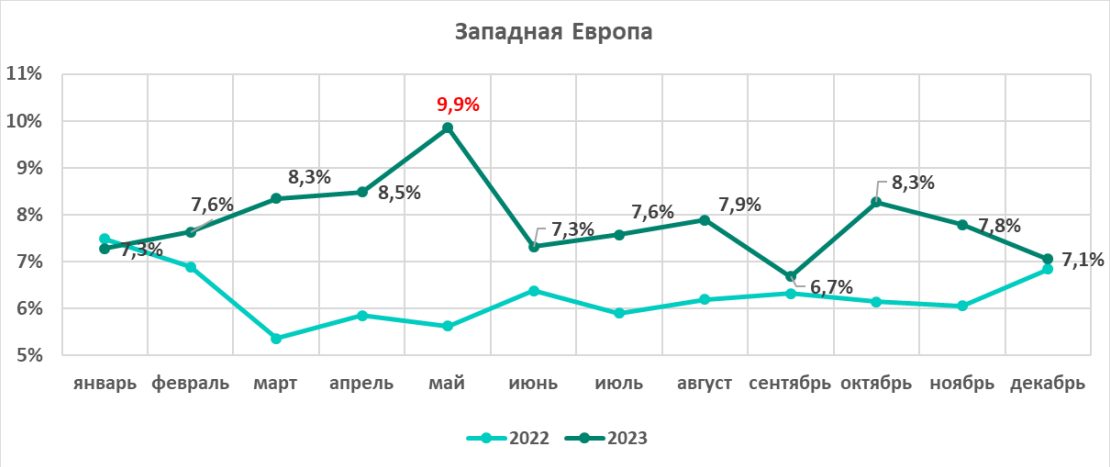
В Западной Европе первое полугодие 2023 года стало лидером по проценту атакованных компьютеров АСУ в период с 2020 по 2023 год. Второе полугодие 2023 года в этом рейтинге на втором месте.

Западная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям 2020 – 2023 года



Процент атакованных компьютеров АСУ в течение месяцев 2023 года (за исключением января) в Западной Европе был выше аналогичных показателей 2022 года. Максимум пришелся на май, когда в Европе был отмечен всплеск фишинговых атак, в том числе на промышленные организации.

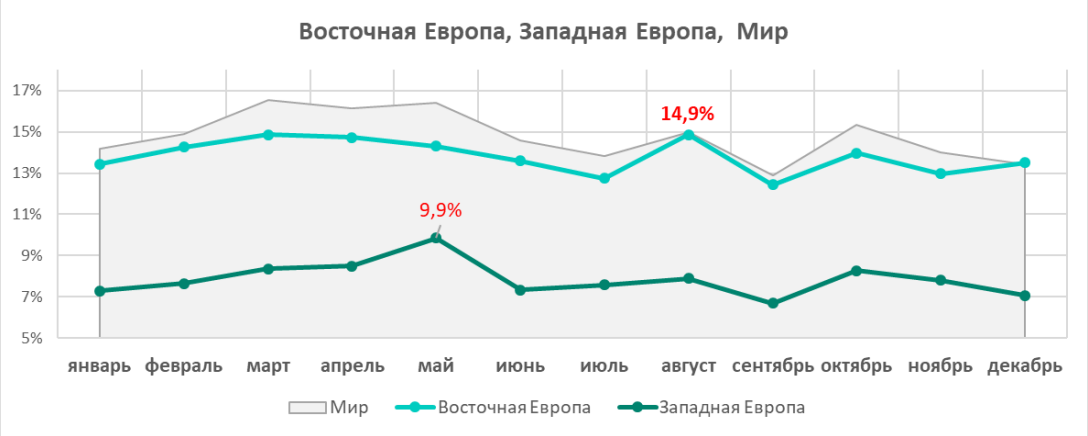
Западная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь – декабрь 2022 и 2023 года



В Восточной Европе первое полугодие 2023 года оказалось с минимальными показателями с 2020 года, а второе полугодие 2023 года стало лидером по проценту атакованных компьютеров АСУ в период с 2020 по 2023 год (30,9%). Основной вклад в рост процента за полугодие внесли вредоносные скрипты и фишинговые страницы.

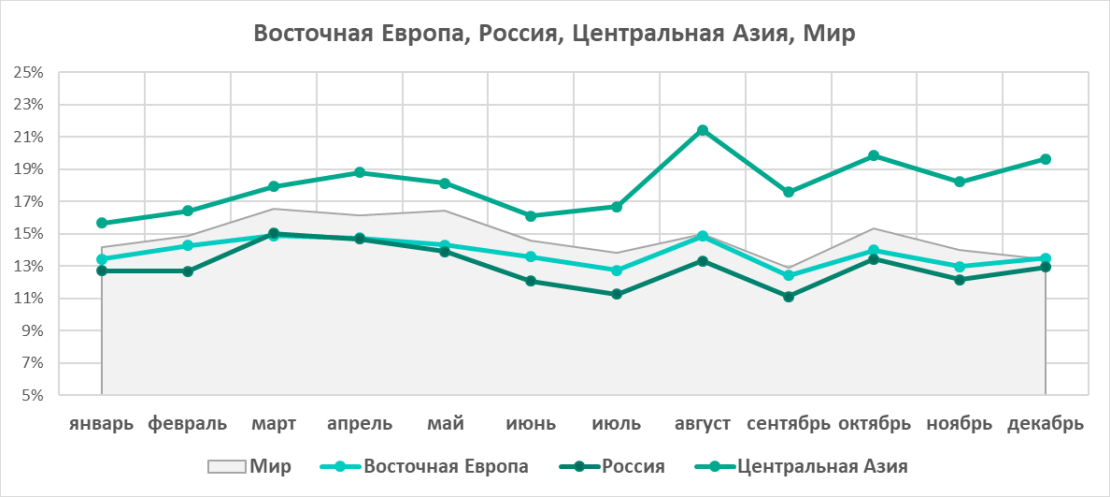
Статистика по месяцам в Восточной Европе отличается от Западной.

Западная Европа, Восточная Европа, мир. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь – декабрь 2022 и 2023 года



В то же время можно отметить определенные совпадения в изменениях процента (больше-меньше) в Восточной Европе, России и в Центральной Азии.

Восточная Европа, мир. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь – декабрь 2022 и 2023 года



Кроме того, в этих трех регионах заметно совпадение изменения процентов атакованных компьютеров АСУ за месяц (больше-меньше) с изменениями аналогичного показателя в мире.

Подробнее о регионе Восточная Европа — ниже, в статистике за второе полугодие 2023 года.

Второе полугодие 2023

Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с первым. Соответственно, по большинству позиций в статистике показатели также уменьшились. Однако есть нюансы, на которые мы хотели бы обратить внимание, поскольку они высвечивают опасные места на ландшафте киберугроз.

Красные линии полугодия

В мире

Процент компьютеров АСУ, где были заблокированы вредоносные объекты, **увеличился только у одной категории**:

- **Майнеры — исполняемые файлы для ОС Windows** — в 1,4 раза.

  Россия, Восточная Европа и Южная Азия — регионы, где отмечено заметное увеличение процента компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для OS Windows.

  В рейтинге регионов по этому показателю лидирует **Центральная Азия, Россия** на втором месте.

Регионы

Африка

Африка лидирует среди регионов

- По проценту компьютеров АСУ, на которых были заблокированы **программы-шпионы**.
- По проценту компьютеров АСУ, на которых детектируются **черви**.
- По проценту компьютеров АСУ, на которых были заблокированы **веб-майнеры**.
- По проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении **съемных носителей**.

С уверенностью можно сказать, что регион продолжает занимать последнюю позицию в рейтинге регионов по уровню зрелости информационной безопасности промышленных предприятий.

Южная Европа

- **Лидирует** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **угрозы из почты — вредоносные почтовые вложения и фишинговые ссылки.** Это тревожный знак. Фишинг — один из излюбленных способов первоначальной компрометации у злоумышленников, сосредоточенных на целевых атаках, — APT, вымогательстве, BEC и атаках хактивистов.
- **На втором месте** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **вредоносные документы**.
- Один из двух регионов, где за полугодие увеличился процент компьютеров АСУ, на которых были заблокированы **программы-шпионы**. Вероятно, это привело к увеличению потока скомпрометированных данных аутентификации в технологических системах промышленных предприятий — что также увеличивает риски последующих целевых атак.

Восточная Европа

- Один из трех регионов, где во втором полугодии 2023 года по сравнению с предыдущим полугодием **увеличился процент** компьютеров АСУ, на которых были заблокированы вредоносные объекты — **на максимальные среди всех регионов 4,6 п.п.**

- За полугодие **в регионе увеличился процент** компьютеров АСУ, на которых были заблокированы:
  - **Вредоносные скрипты и фишинговые страницы** — на 2,9 п.п.;
  - **Майнеры — исполняемые файлы для ОС Windows** — на 0,9 п.п.;
  - **Черви** — на 0,43 п.п. (единственный регион, где этот процент увеличился);
  - **Ресурсы в интернете из списка запрещённых** — на 0,4 п.п. (единственный регион, где этот процент увеличился);
- **На втором месте** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы**.

Все эти изменения никак не могут свидетельствовать в пользу тенденции к увеличению общего уровня зрелости безопасности промышленных предприятий. Как мы видим, доступность ОТ-систем для различного типа угроз растет по причинам, связанным, в первую очередь, с человеческим фактором и с общим для региона недостатком финансирования ИБ промышленных объектов.

Россия

- **На втором месте** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows.**

Центральная Азия

- **Лидирует** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **ресурсы в интернете из списка запрещённых.**
- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **майнеры — исполняемые файлы для ОС Windows**.
- **На втором месте среди регионов** по проценту компьютеров АСУ, на которых были заблокированы **черви**.

Регион традиционно демонстрирует весьма низкую общую зрелость информационной безопасности. Промышленным организациям в регионе явно стоит уделять больше внимания обучению сотрудников.

Восточная Азия

- **Лидирует** среди регионов по проценту компьютеров АСУ, на которых было заблокировано **вредоносное ПО для AutoCAD**.
- **На втором месте среди регионов** по проценту компьютеров АСУ, на которых были заблокированы **вирусы**.
- **В регионе программы-шпионы на втором месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.

Юго-Восточная Азия

- **Лидирует** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **вирусы**.
- **В регионе вирусы на третьем месте** в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.

Промышленным организациям в регионе нужно лучше обеспечивать покрытие своих систем в технологической сети хотя бы минимальным набором защитных мер и средств.

Южная Азия

- **Делит с Ближним Востоком лидерство** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **программы-вымогатели**.

Ближний Восток

- **Лидирует (вместе с Южной Азией)** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **программы-вымогатели.** Промышленным организациям в регионе явно стоит учитывать риск вымогательства со стороны мелких малоизвестных групп и злоумышленников-одиночек — именно они вносят основной вклад в статистику обнаруженных угроз.
- **На втором месте** в рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы **программы-шпионы**.
- **На втором месте среди регионов** по проценту компьютеров АСУ, на которых были заблокированы **веб-майнеры**.

Латинская Америка

- **Лидирует** среди регионов по проценту компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы.** Промышленным организациям в регионе следует оценивать риск целевых атак на технологические сегменты сети как высокий.
- **Лидирует** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные документы**. По всей видимости это следствие высокого процента систем, столкнувшихся с фишингом. Вредоносные документы (например, приложенные к письму или доступные для скачивания по ссылке) — один из самых популярных у злоумышленников способов компрометации через фишинговые рассылки.
- **На втором месте** по проценту компьютеров АСУ, на которых были заблокированы **вредоносные почтовые вложения и фишинговые ссылки**.

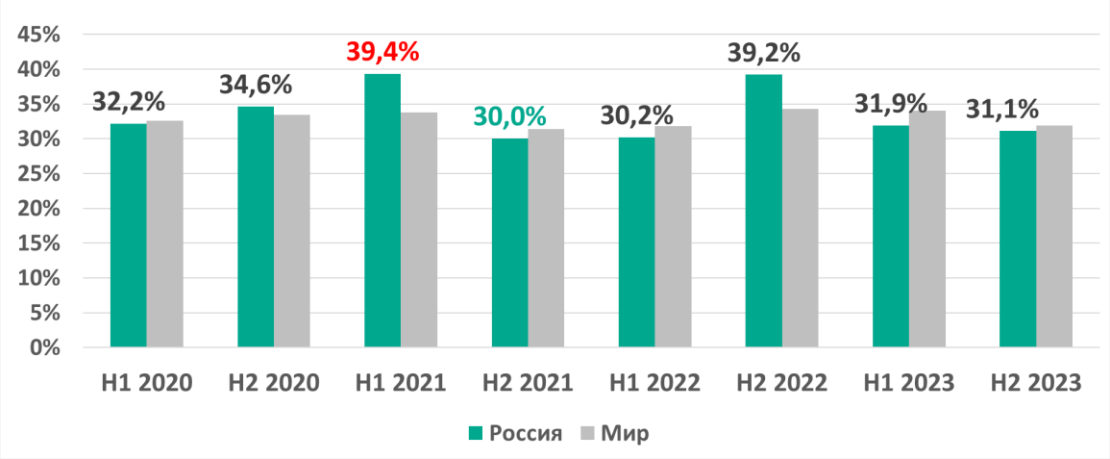
Австралия и Новая Зеландия

- Единственный регион, где за полугодие увеличился процент компьютеров АСУ, на которых были заблокированы **вредоносные документы.**

Россия во втором полугодии 2023

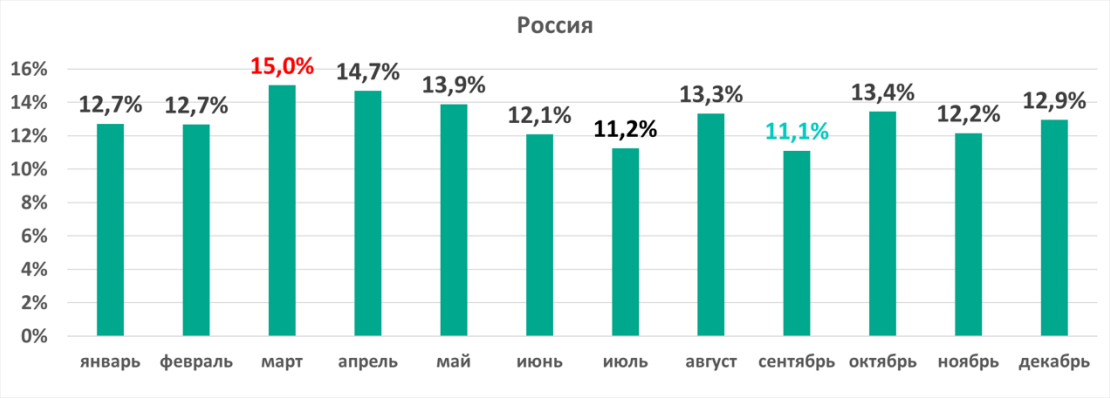
Во втором полугодии 2023 года в России вредоносные объекты были заблокированы на 31,1% компьютеров АСУ — на 0,8 п.п. меньше, чем в предыдущем полугодии и на столько же меньше, чем в среднем по миру.

Россия и мир. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



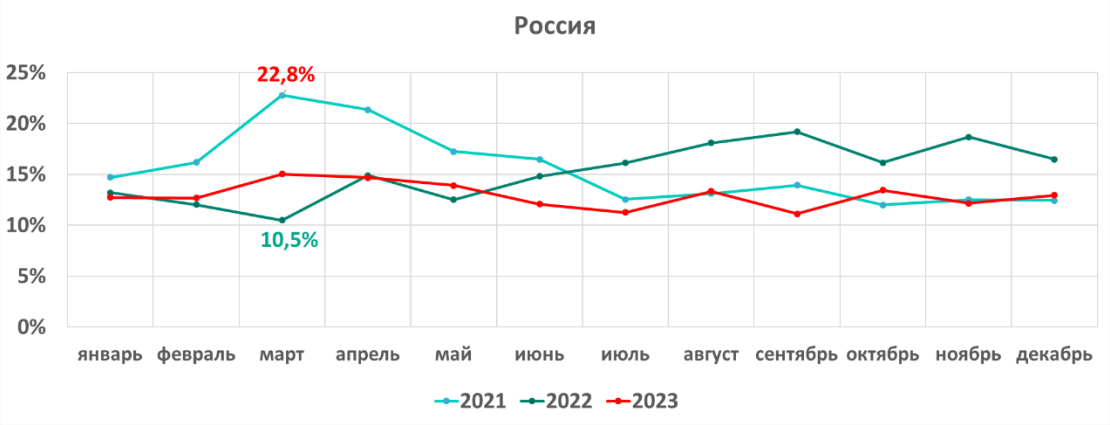
В России во втором полугодии 2023 года самым высоким процент атакованных компьютеров АСУ был в марте (15%), самым низким — в сентябре (11,1%).

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2023 года



Если рассматривать месячные показатели за последние три года, то и максимум, и минимум пришелся на март — 2021 и 2022 года соответственно.

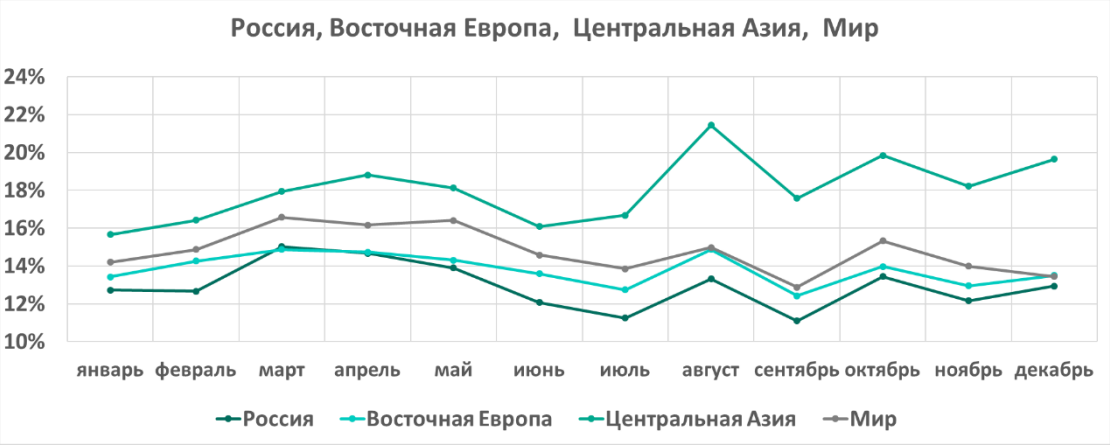
Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2021, 2022, 2023 годов



Как видно на графике выше, динамика изменений процента от месяца к месяцу (больше-меньше) в 2023 году не совпадает с предыдущими, хотя есть некоторое сходство с 2021 годом в первом полугодии.

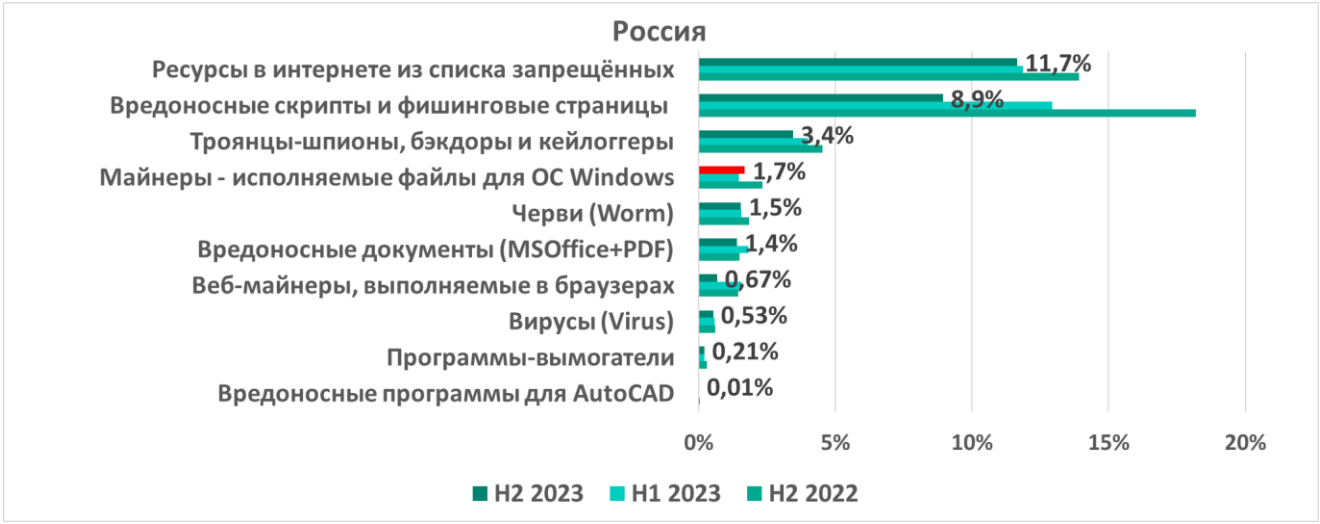
Зато на графике ниже видно явное сходство месячных изменений в 2023 году в России, в Центральной Азии и в среднем по миру. Менее близки к изменениям в России, но все же похожи, показатели Восточной Европы.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2023 года



Категории вредоносного ПО

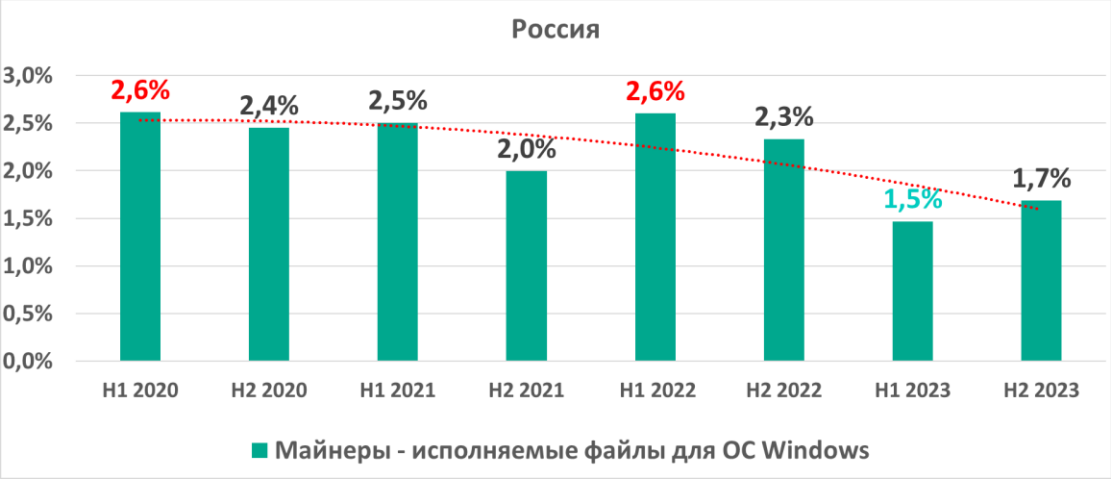
Во втором полугодии 2023 года в России среди категорий угроз, заблокированных на компьютерах АСУ, как и во всем мире лидируют Ресурсы в интернете из списка запрещенных, Вредоносные скрипты и фишинговые страницы и шпионское ПО. Основные источники распространения этих категорий вредоносных объектов — интернет и электронная почта.



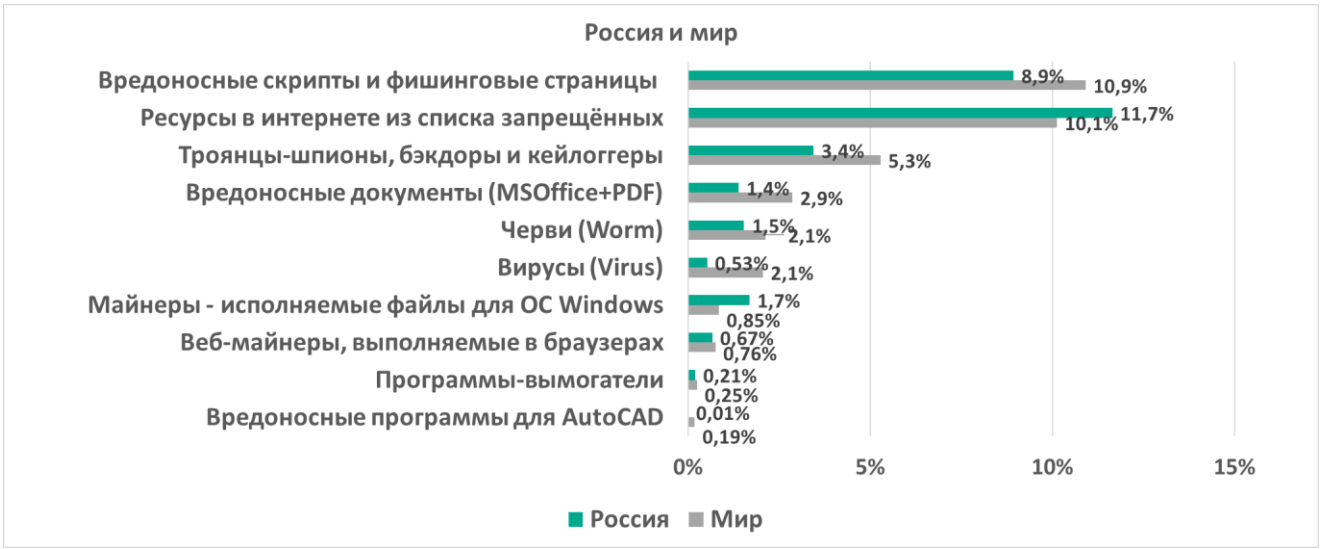
Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий

В России во втором полугодии 2023 года из всех категорий угроз вырос только показатель категории Майнеры — исполняемые файлы для ОС Windows (на 0,22 п.п.). При этом в предыдущем полугодии показатель был минимальным с 2020 года. По всем остальным категориям угроз показатели уменьшились.

Россия. Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows



В России в рейтинге угроз по проценту компьютеров АСУ, на которых они были заблокированы, майнеры — исполняемые файлы для ОС Windows оказались на четвертом месте. Для сравнения — в мире в аналогичном рейтинге эта категория угроз на седьмом месте с показателем 0,85%, что вдвое меньше, чем в России (1,7%). На графике ниже рейтинг категорий вредоносных объектов выстроен по показателям в мире.

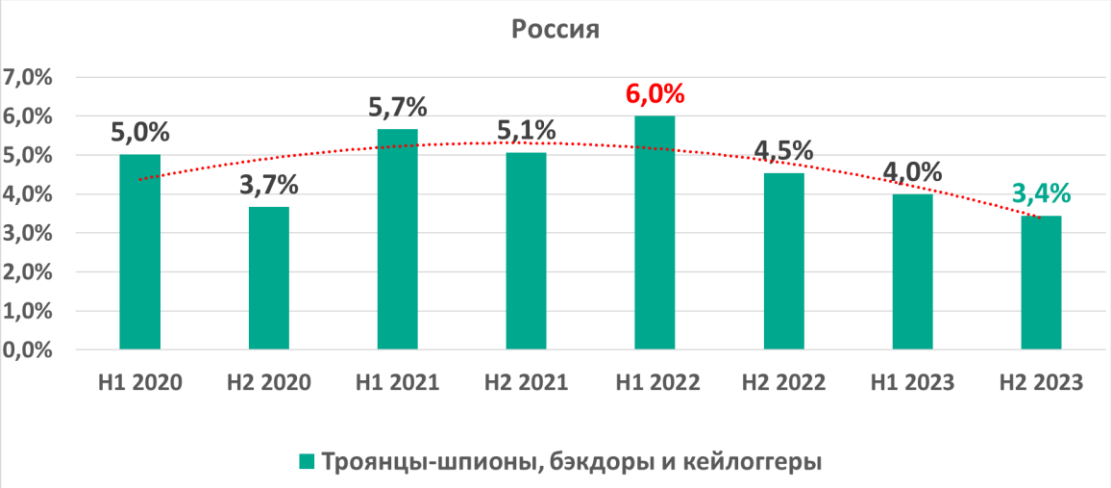


Россия и мир. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, первое полугодие 2023 года

Как видно по цифрам на графике, в России чаще, чем в среднем по миру, операторы и инженеры АСУ заходили на вредоносные и заражённые интернет-ресурсы — соответствующий показатель по России (11,7%) превышает общемировой на 1,6 п.п.

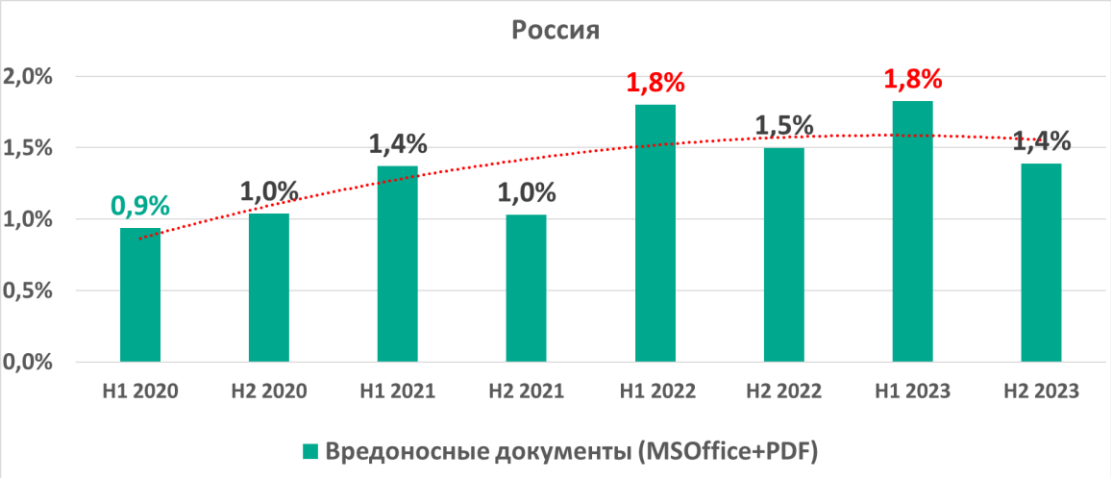
Процент компьютеров АСУ, на которых были заблокированы программы-шпионы, во втором полугодии 2023 года в России был минимальным с 2020 года.

Россия. Процент компьютеров АСУ, на которых было заблокированы шпионское ПО



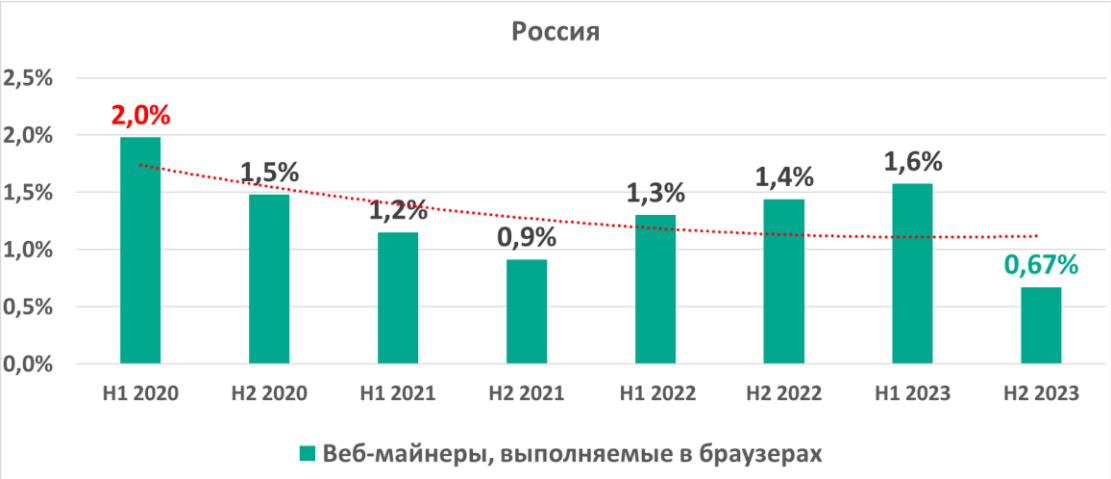
После заметного роста в предыдущие полугодия процент компьютеров АСУ, на которых были заблокированы вредоносные документы, во втором полугодии 2023 года снизился до уровня первого полугодия 2021 года.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные документы



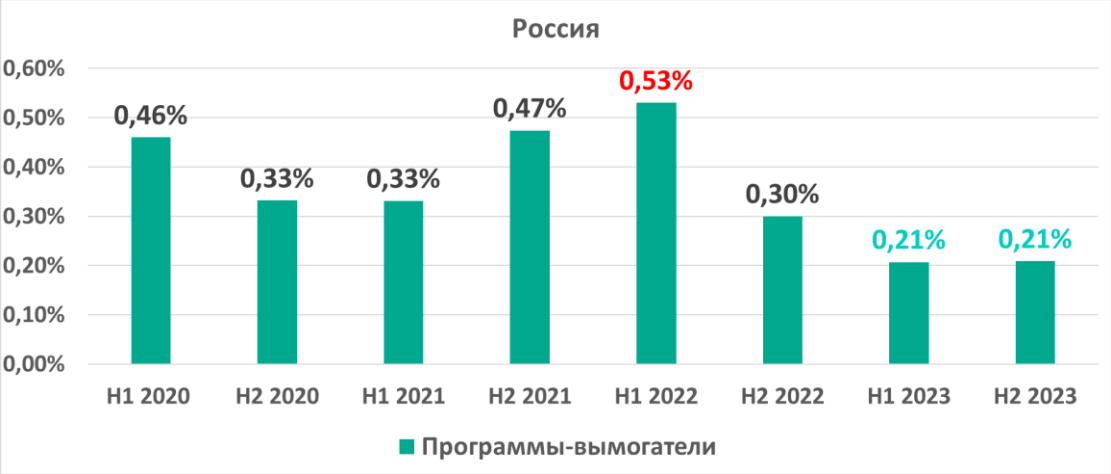
Показатель веб-майнеров, который в России вырос с 0,9% во втором полугодии 2021 до 1,6% в первом полугодии 2023, во втором полугодии 2023 года снизился до минимальных с 2020 года 0,67%.

Россия. Процент компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах



Процент компьютеров АСУ, на которых была предотвращена активность программ-вымогателей, в России и в первом, и во втором полугодиях 2023 года был минимальным с 2020 года.

Россия. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



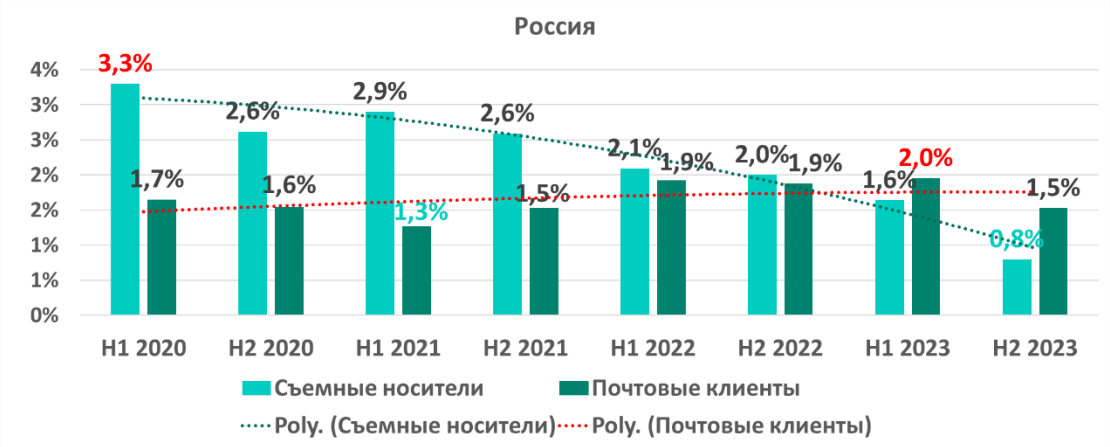
Источники угроз

В России во втором полугодии 2023 года уменьшился процент компьютеров АСУ, на которых были заблокированы угрозы из всех основных источников:

- угрозы из интернета — на 1,3 п.п.,
- угрозы, обнаруженные при подключении съемных носителей, — на 0,8 п.п.
- угрозы, источником которых стала почта, — на 0,4 п.п.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из интернета

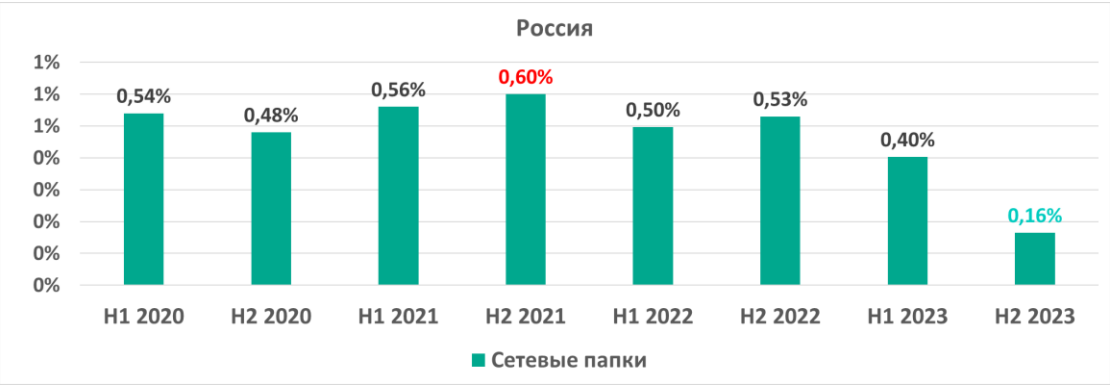
Россия. Процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей и угрозы из почты



Электронная почта в России впервые стала более значимым источником угроз для компьютеров АСУ, чем съемные носители, в первом полугодии 2023 года. Во втором полугодии 2023 года процент компьютеров АСУ, на которых заблокированы угрозы из почты, оказался почти вдвое (в 1,9 раз) больше, чем процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей.

Уменьшился также процент компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках.

Россия. Процент компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках

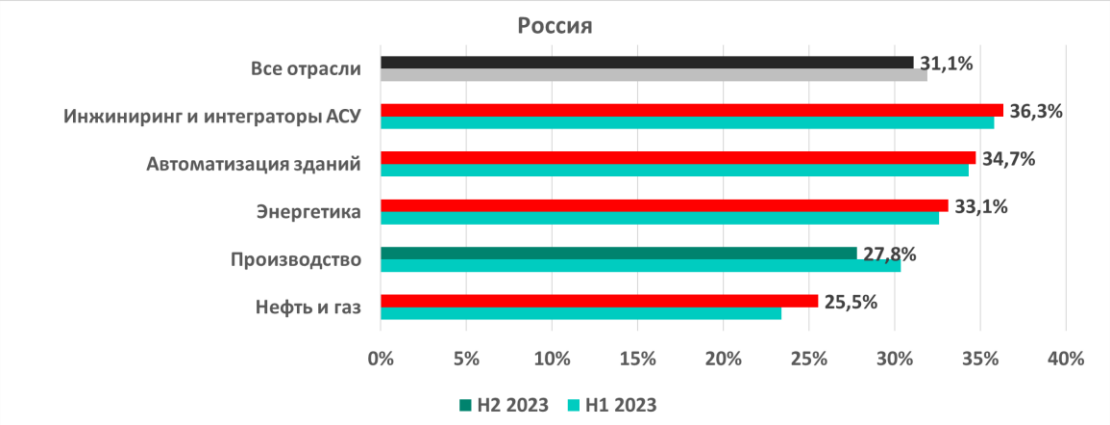


Снижение процента компьютеров АСУ, на которых блокируются угрозы, распространяемые через почту и сетевые папки, по всей видимости, свидетельствует об общем улучшении уровня зрелости информационной безопасности промышленных предприятия — и в части кибергигиены и осведомлённости персонала об угрозах, и в части покрытия технологической инфраструктуры автоматизированными средствами защиты.

Некоторые отрасли

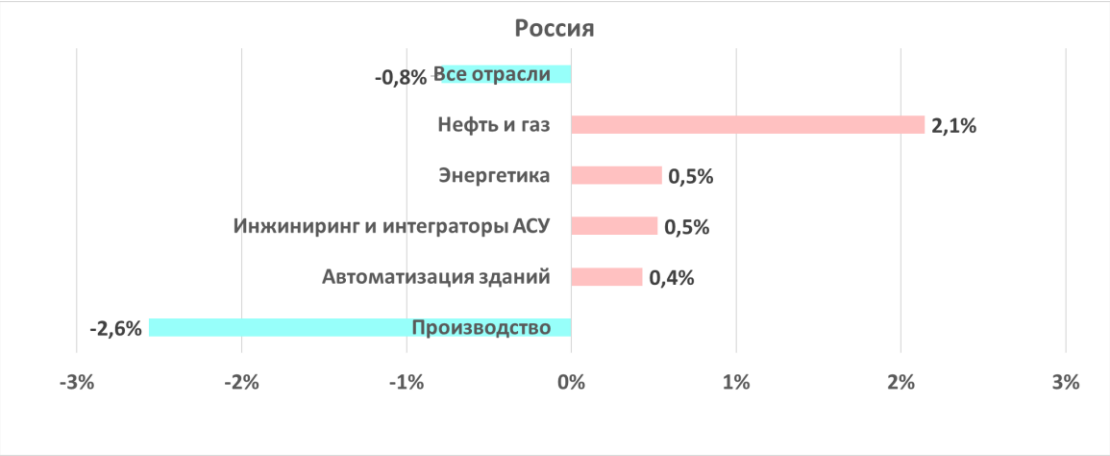
Во втором полугодии 2023 года в России Производство оказалось единственной из рассмотренных в данном исследовании отраслей, где процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился. В предыдущем полугодии ситуация была обратной — процент атакованных компьютеров АСУ увеличился только в этой отрасли.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях



Больше всего — на 2,1 п.п. — увеличился показатель отрасли Нефть и газ.

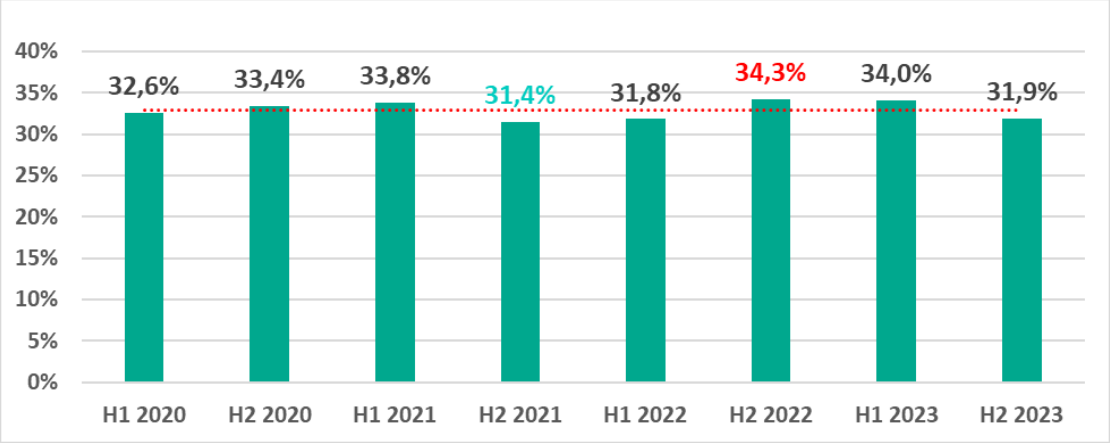
Россия. Изменение во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях



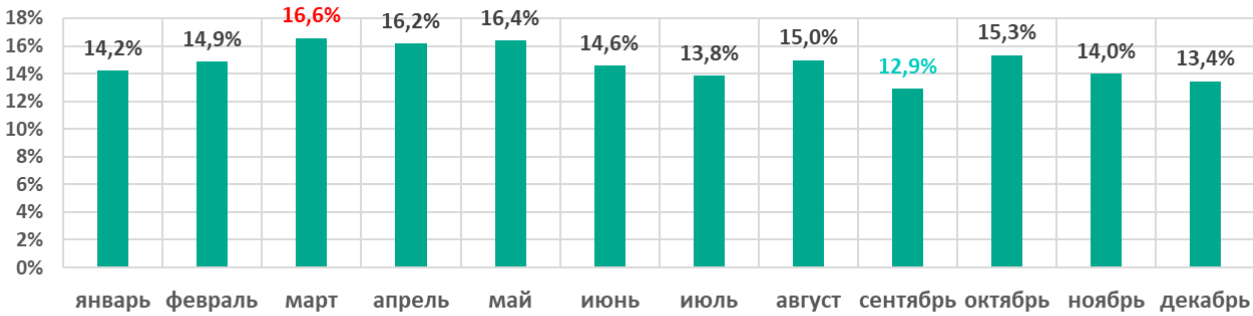
Глобальная статистика по всем угрозам

Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с предыдущим полугодием на 2,1 п.п. и составил 31,9%.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по полугодиям

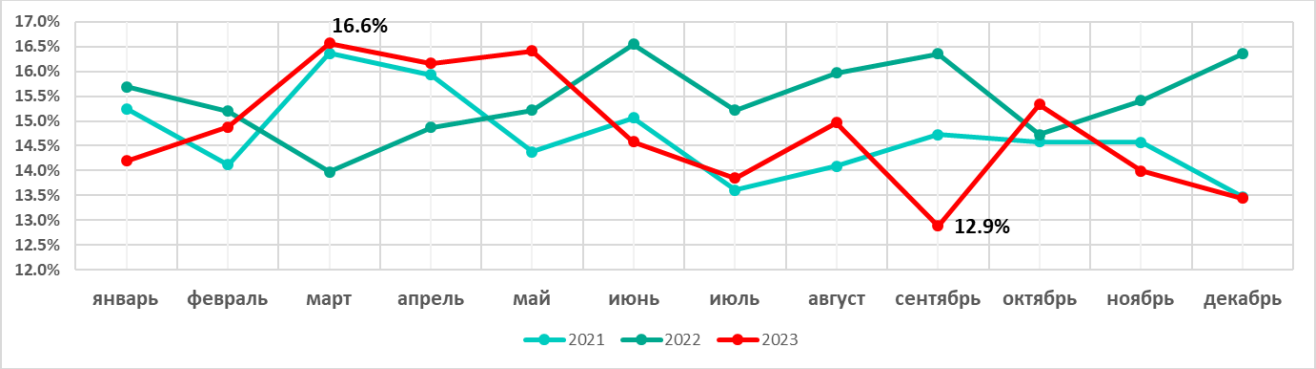


В течение 2023 года самым высоким процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был в марте, самым низким — в сентябре.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — декабрь 2023

Отметим, что в марте и сентябре проценты оказались рекордными не только для 2023 года, но и в сравнении с месячными показателями за три года — с 2021 по 2023.



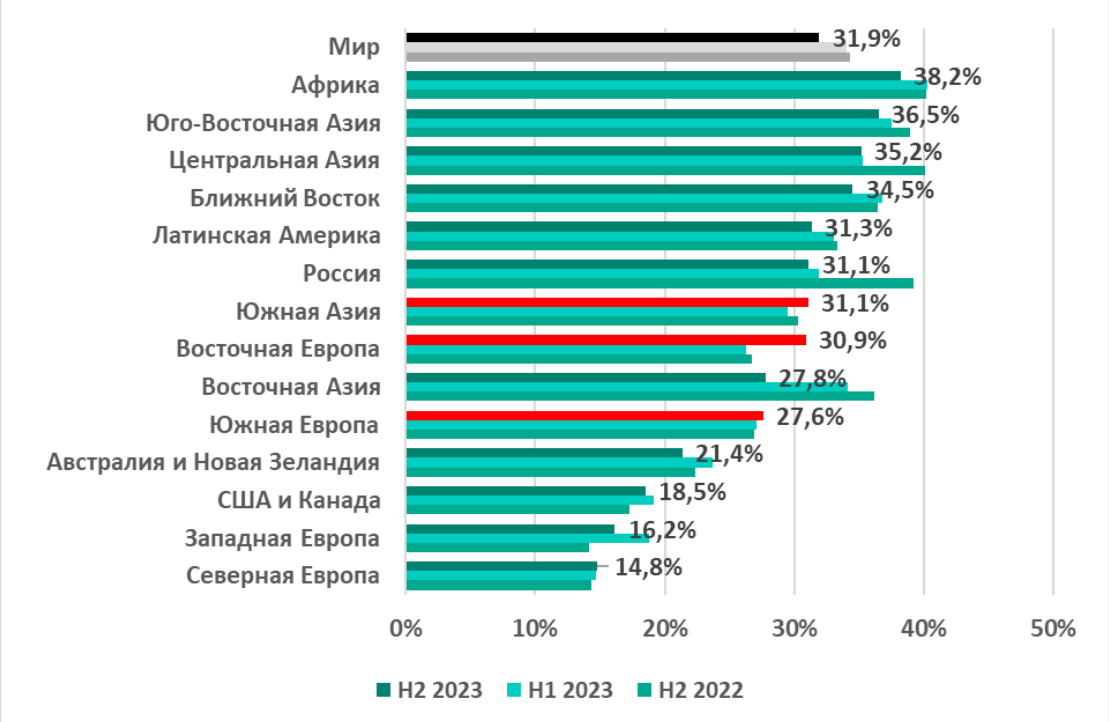
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2021, 2022 и 2023 годов

Что касается изменения процента от месяца к месяцу (больше — меньше), то 2023 год отличается от двух предыдущих, но все же ближе к 2021, чем к 2022 году.

Регионы

Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился по сравнению с первым полугодием в Южной Азии, Восточной и Южной Европе.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2023 года



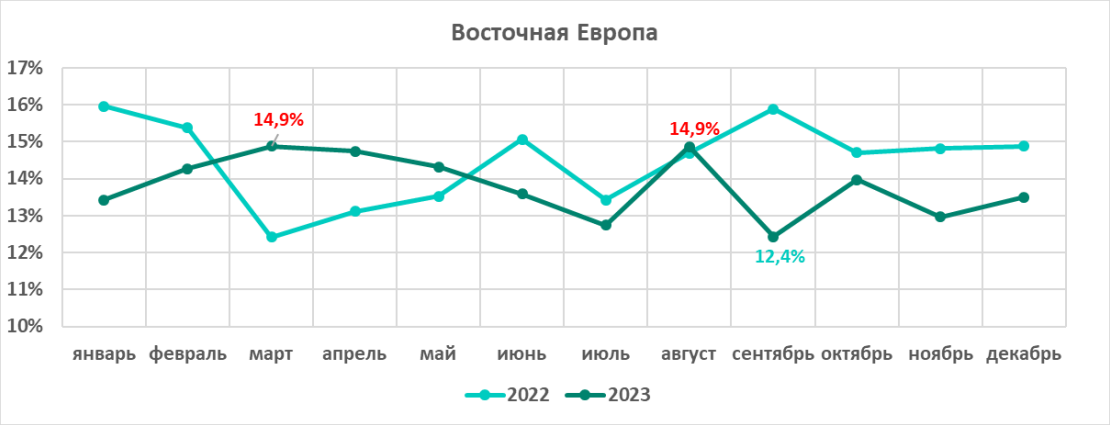
Регионы и мир. Изменение процента атакованных компьютеров за второе полугодие 2023 года

Наибольший рост во втором полугодии отмечен в Восточной Европе (на 4,6 п.п.). При этом в предыдущем полугодии процент в регионе был минимальным с 2020 года, а показатель за второе полугодие оказался самым высоким за четыре года.

Восточная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

Самым высоким процент атакованных компьютеров АСУ в Восточной Европе был в марте и в августе, самым низким — в сентябре. Динамика по месяцам 2022 года заметно отличается от 2023 года.

Восточная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь – декабрь 2022 и 2023 годов



Страны

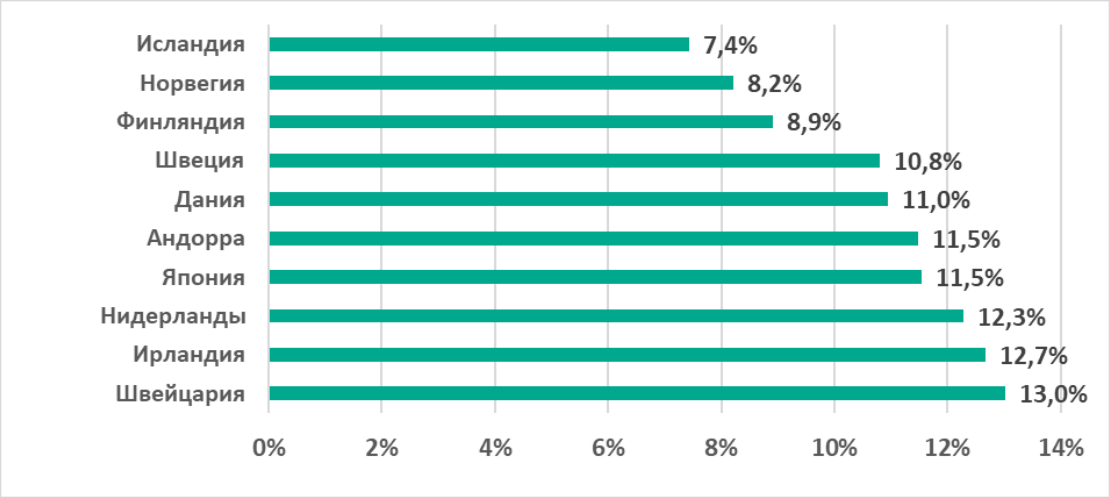
В разных странах процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 56,6% в Йемене до 7,4% в Исландии.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2023

Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором полугодии 2023 года пять стран — африканские, четыре — из Южной Азии.

Из 10 стран, в которых процент был самым маленьким, шесть стран — из Северной Европы.

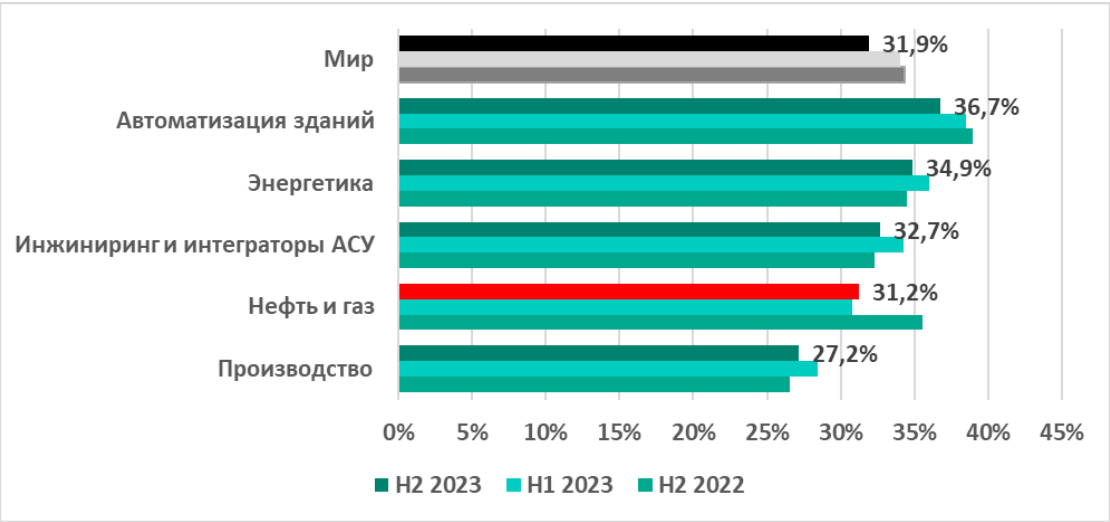
10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором полугодии 2023



Некоторые отрасли

Во втором полугодии 2023 года Автоматизация зданий по-прежнему лидирует среди исследуемых отраслей по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты.

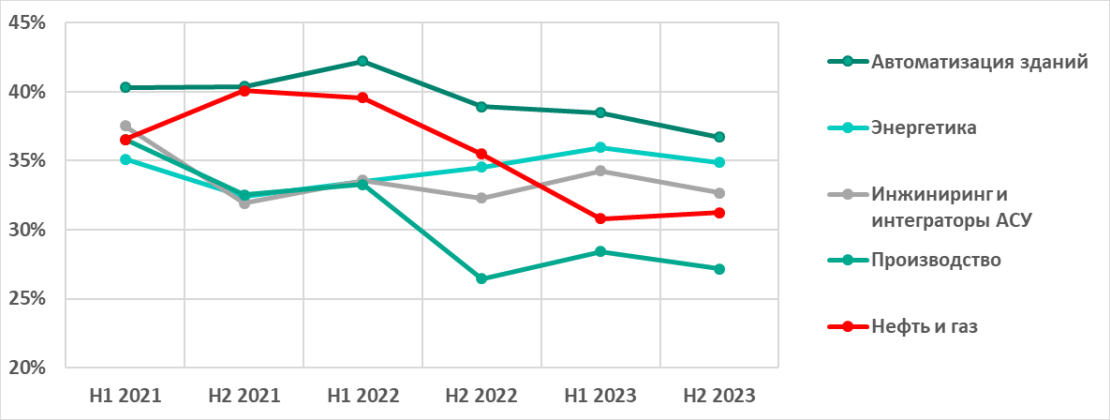
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях



На втором месте — Энергетика. Процент атакованных компьютеров АСУ в этой отрасли увеличивался три полугодия подряд — с первого полугодия 2022 года — и лишь во втором полугодии 2023 года уменьшился на 1,1 п.п.

В отрасли Нефть и Газ ситуация обратная — с 2022 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в отрасли уменьшался, а во втором полугодии 2023 года немного увеличился (на 0,5 п.п.). Это единственная отрасль, где показатель за полугодие вырос.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях

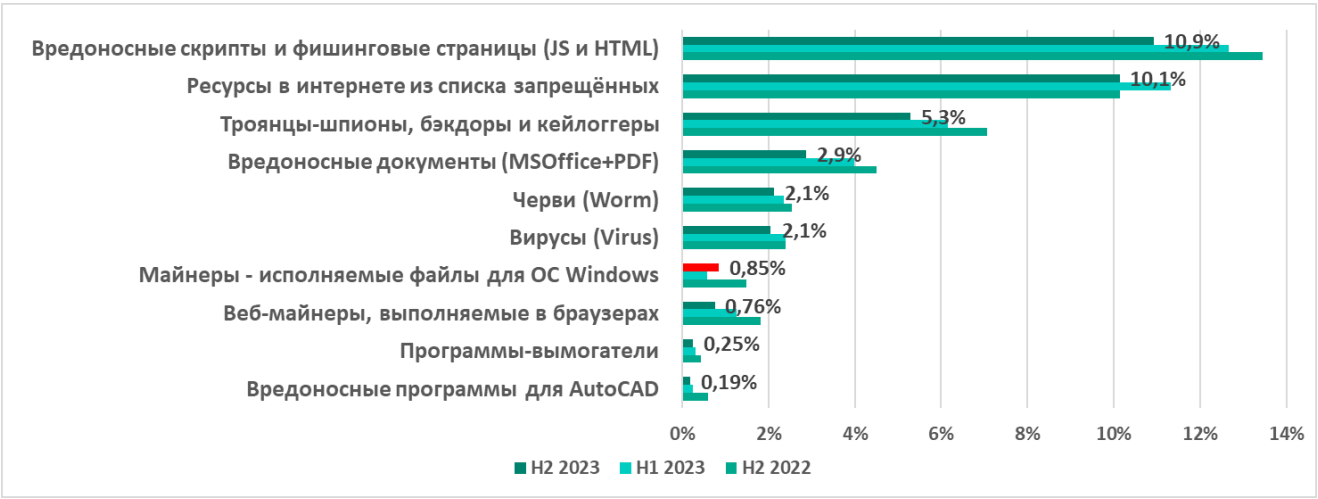


Разнообразие обнаруженного вредоносного ПО

Во втором полугодии 2023 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано вредоносное ПО из 12618 различных семейств.

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям.

Во втором полугодии 2023 года по сравнению с первым полугодием увеличился показатель только одной категории вредоносных объектов: процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, вырос в 1,4 раза.



Процент компьютеров АСУ[1], на которых была предотвращена активность вредоносных объектов различных категорий

[1] Заметим, что получившиеся проценты некорректно суммировать, потому что во многих случаях на одном компьютере за отчётный период могли быть заблокированы угрозы двух и более типов.

Далее мы сгруппировали статистику по вредоносным объектам, условно разделив их по способу распространения и назначению на три группы:

1. Вредоносные объекты, используемые для первичного заражения;
2. Вредоносное ПО следующего этапа;
3. Самораспространяющееся вредоносное ПО.

Вредоносные объекты, которые используются для первичного заражения компьютеров, — опасные веб-ресурсы, вредоносные скрипты и вредоносные документы. Они напрямую связаны с доставляемым ими на компьютер жертвы вредоносным ПО следующего этапа — шпионским ПО, вымогателями и майнерами. В большинстве случаев источником таких угроз становится интернет или электронная почта.

В тех регионах и странах, где процент компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, высок, можно наблюдать и высокий процент для вредоносно ПО следующего этапа.

Самораспространяющееся вредоносное ПО — черви и вирусы — относится к отдельно категорий. Изначально черви и зараженные вирусами файлы использовались для первичного заражения компьютеров, но позднее, с развитием функциональности ботнет-сетей, приобрели черты угроз следующего этапа.

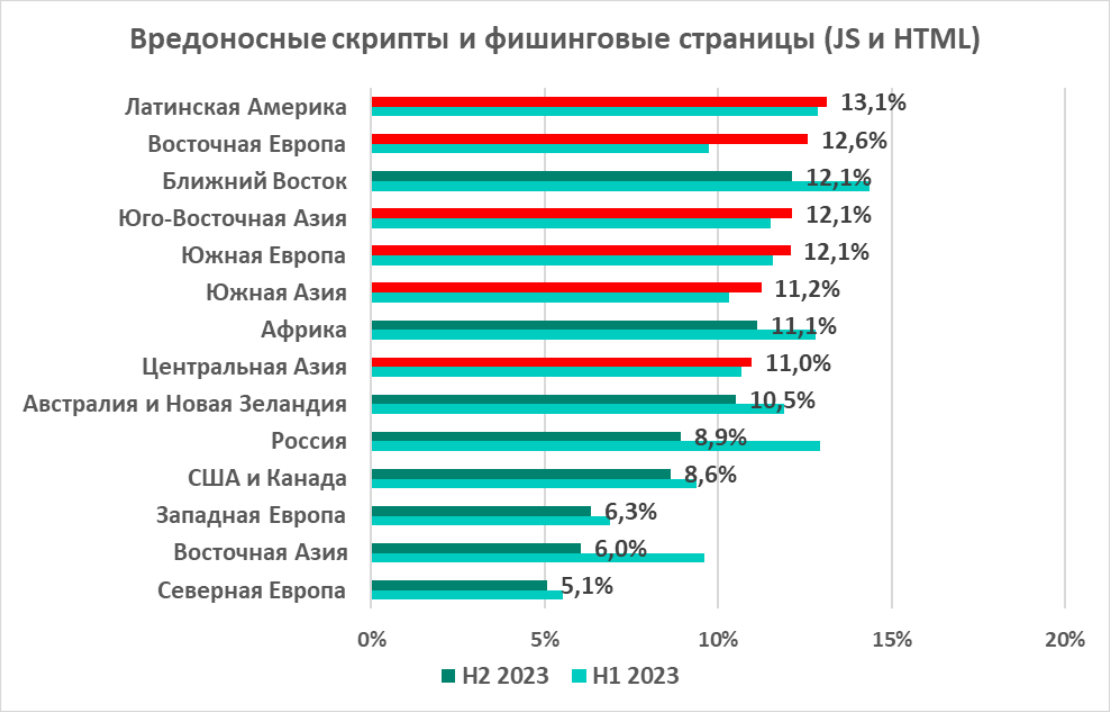
Вредоносные объекты, используемые для первичного заражения

Вредоносные скрипты и фишинговые страницы (JS и HTML)

Вредоносные скрипты применяются злоумышленниками для выполнения большого 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 и/или программ для скрытого майнинга криптовалюты). Они распространяются как в интернете, так и в письмах, рассылаемых в электронной почте.

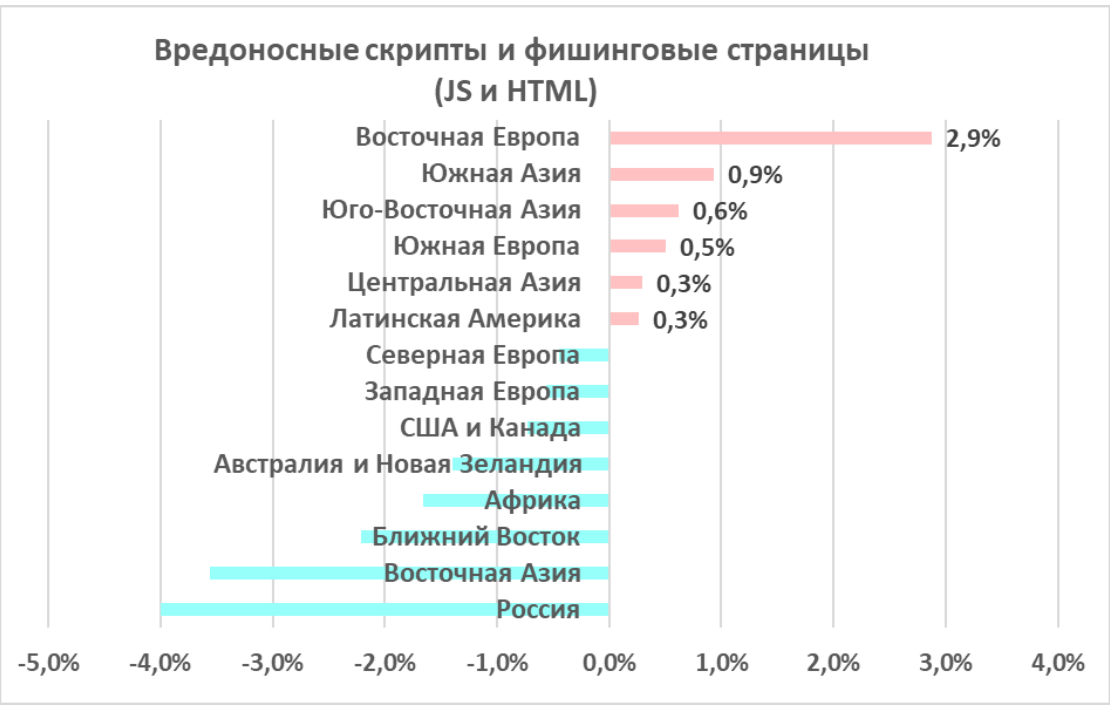
Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, отмечен в Латинской Америке и в Восточной Европе.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, второе полугодие 2023 года



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты этой категории, за полугодие вырос в шести регионах, больше всего — в Восточной Европе (на 2,9 п.п.).

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы (JS и HTML), за второе полугодие 2023 года



Среди стран по проценту компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидирует Киргизия (21,2%). На втором месте — Северная Македония (20,7%), на третьем — Греция (19,8%).

Ресурсы из интернета из списка запрещённых

Ресурсы в интернете из списка запрещённых связаны с распространением или управлением каким-либо вредоносным ПО. Значительная часть таких ресурсов используется для распространения вредоносных скриптов и фишинговых страниц (HTML).

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, отмечен в Центральной Азии.

Единственный регион, в котором процент по этой угрозе немного вырос — Восточная Европа (на 0,4 п.п.).

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, второе полугодие 2023 года

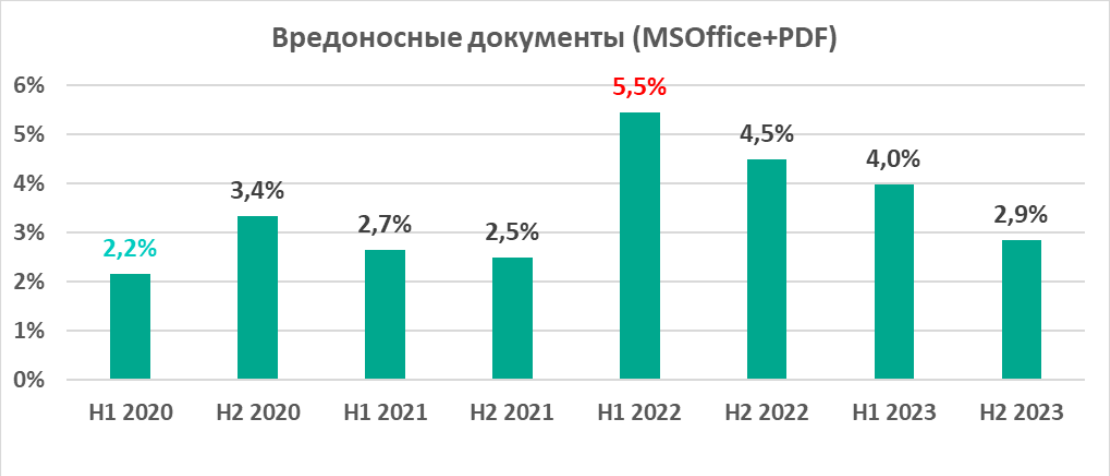
Среди стран по проценту компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, лидируют Таджикистан (18,2%) и Йемен (16,6%).

Вредоносные документы (MSOffice+PDF)

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. Как правило, вредоносные документы содержат эксплойты, вредоносные макросы и зловредные ссылки.

В мире процент компьютеров АСУ, на которых были заблокированы угрозы этой категории, снижается со второго полугодия 2022 года. Во втором полугодии 2023 года он уменьшился на 1,1 п.п. по сравнению с предыдущим полугодием.

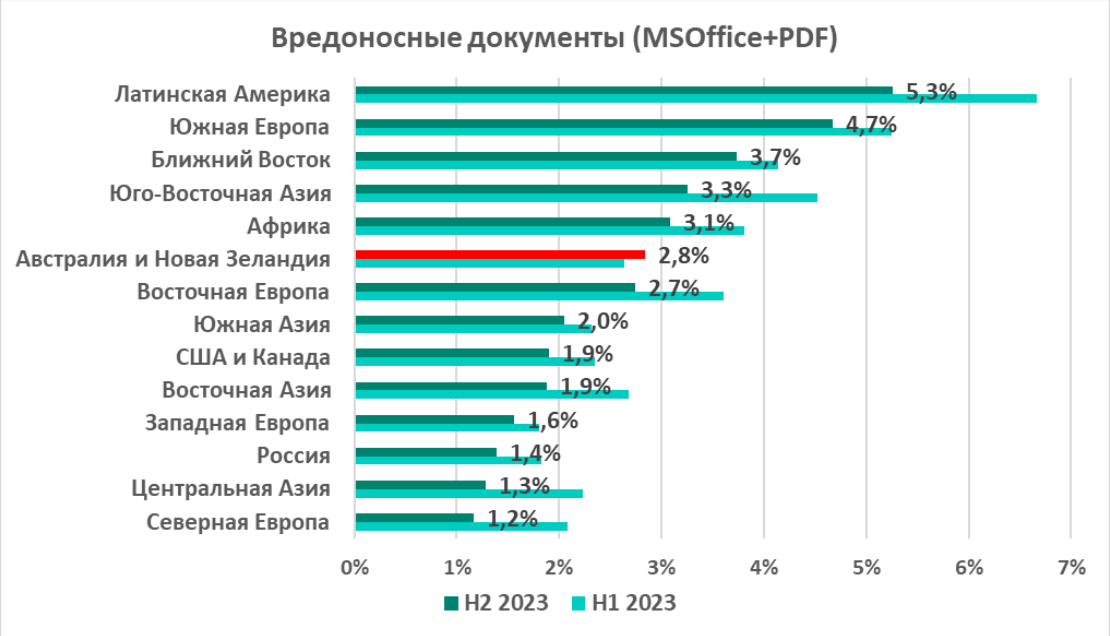
Процент компьютеров АСУ, на которых были заблокированы вредоносные документы (MSOffice и PDF)



В рейтинге регионов первые три позиции по-прежнему занимают Латинская Америка, Южная Европа и Ближний Восток. Эти же регионы лидируют по проценту компьютеров АСУ, на которых были заблокированы угрозы из почты.

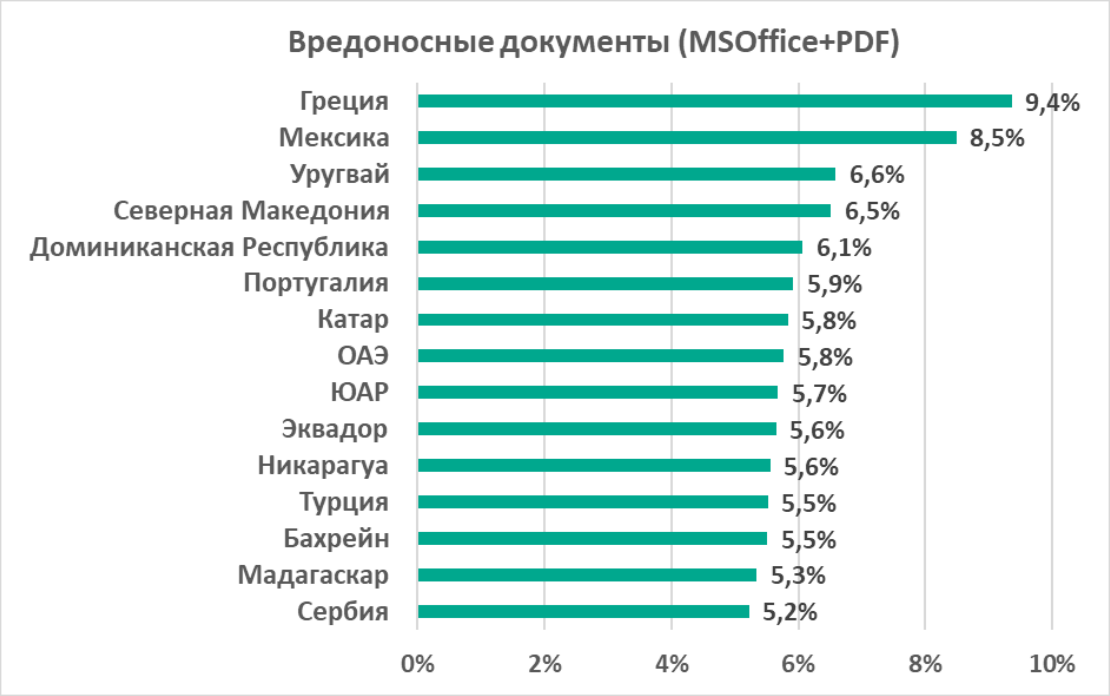
За полугодие показатель немного вырос только в Австралии и Новой Зеландии (на 0,2 п.п.).

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные документы, второе полугодие 2023 года



Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные документы, лидируют Греция (9,4%) и Мексика (8,5%).

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные документы, второе полугодие 2023 года



Треть стран в топ 15 из Латинской Америки, четыре страны — с Ближнего Востока, три — из Южной Европы.

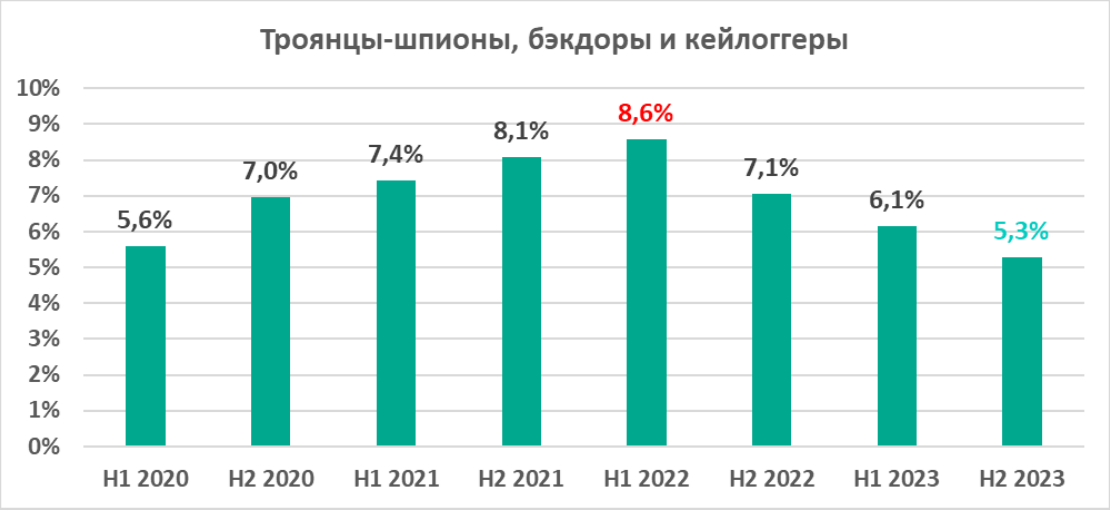
Вредоносное ПО следующего этапа

Программы-шпионы

Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО используется для несанкционированного удаленного доступа и кражи конфиденциальной информации. В большинстве случаев конечная цель атак с применением такого ПО — кража денег, но используются программы-шпионы и в целевых атаках, для кибершпионажа.

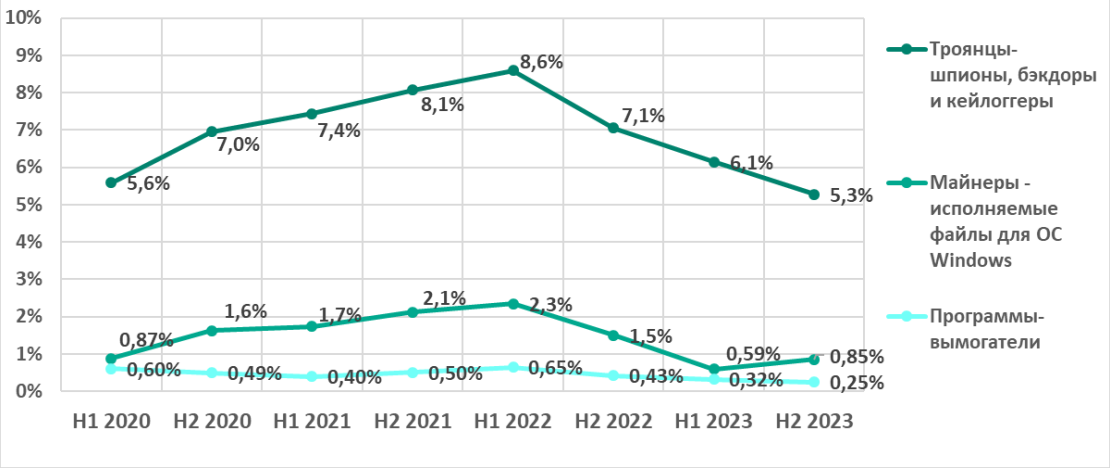
Во втором полугодии 2023 года в мире процент компьютеров АСУ, на которых были заблокированы программы-шпионы, был минимальным с 2020 года — 5,3%.

Процент компьютеров АСУ, на которых были заблокированы программы-шпионы



Отметим, что 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. Как правило, изменение процента компьютеров, на которых блокируются программы-шпионы (больше-меньше), влияет на риск целевых атак и приводит к соответствующему изменению процента компьютеров, атакованных майнерами или вымогателями.

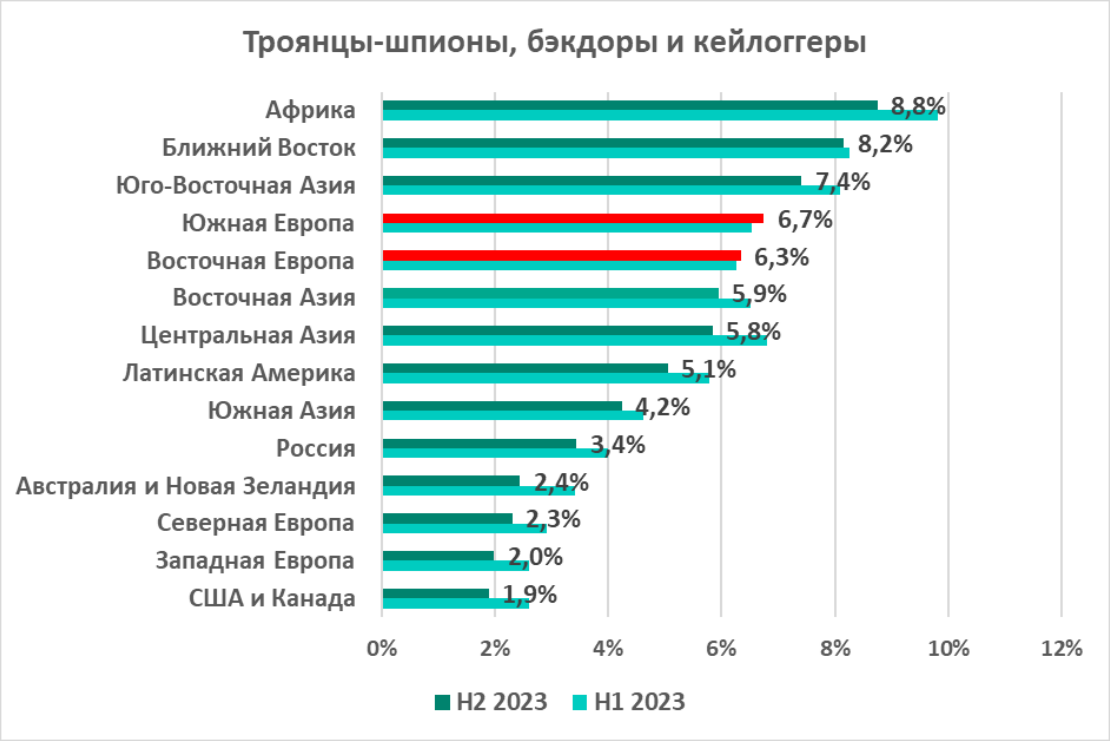
Процент компьютеров АСУ, на которых были заблокированы программы-шпионы, вредоносные майнеры и программы-вымогатели



Как и прежде, максимальный среди регионов процент компьютеров АСУ, на которых были заблокированы программы-шпионы, в Африке. И по-прежнему этот показатель высок на Ближнем Востоке и в Юго-Восточной Азии.

На фоне снижения в мире процента компьютеров АСУ, на которых были заблокированы программы-шпионы, во втором полугодии 2023 года он немного вырос в Южной Европе (на 0,2 п.п.) и в Восточной Европе (на незначительные 0,07 п.п.). Южная Европа в рейтинге регионов по этому показателю оказалась на четвертом месте, Восточная Европа — на пятом.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-шпионы, второе полугодие 2023 года



Отметим, что в Восточной Азии программы-шпионы находятся на втором месте в рейтинге категорий вредоносного ПО по проценту компьютеров АСУ, на которых оно было заблокировано.

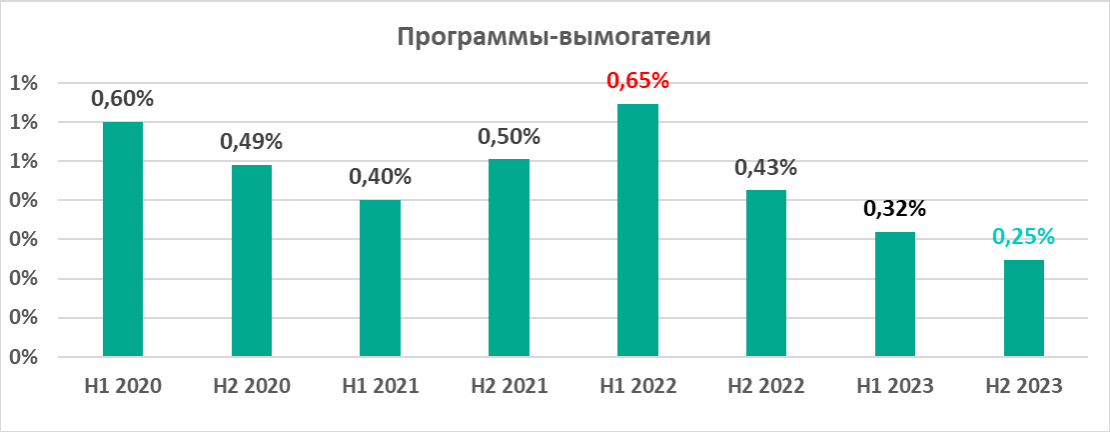
Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы программы-шпионы, лидируют Северная Македония, Йемен и Алжир.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-шпионы, второе полугодие 2023

Программы-вымогатели

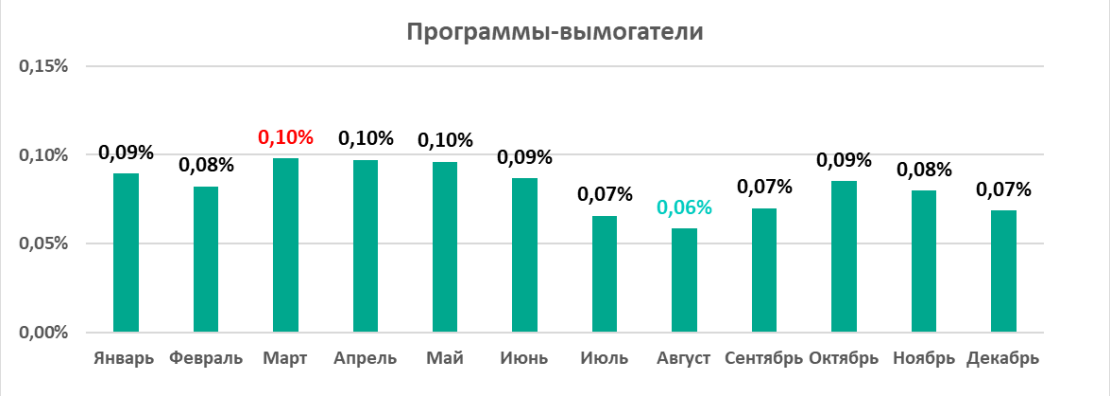
Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, снизился до минимального за четыре года значения — 0,25%.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, по полугодиям 2020 — 2023 годов



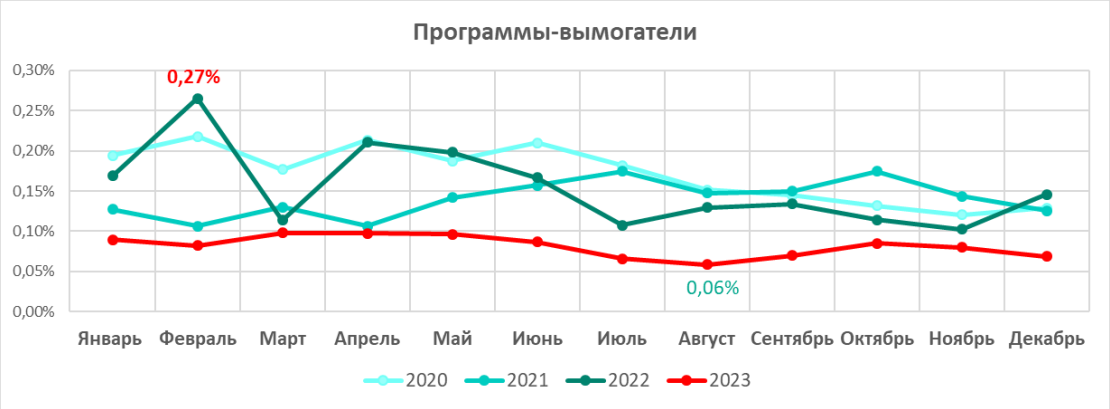
Самый высокий за месяцы 2023 года процент компьютеров АСУ, атакованных программами-вымогателями, отмечен в марте, самый низкий — в августе.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — декабрь 2023 года



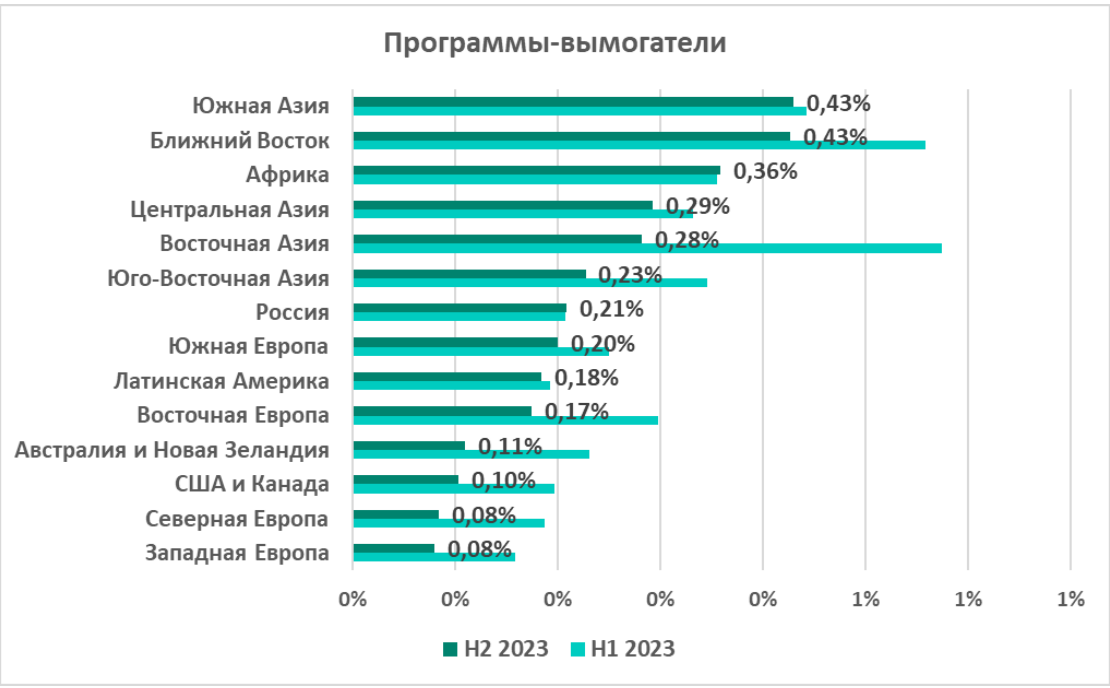
Все 12 месяцев 2023 года проценты были ниже соответствующих показателей предыдущих трех лет. Соответственно, на август пришелся месячный минимум не только за 2023, но и за все годы, начиная с 2020. Максимальный процент за этот же период был отмечен в феврале 2022 года.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, по месяцам 2020 — 2023 годов



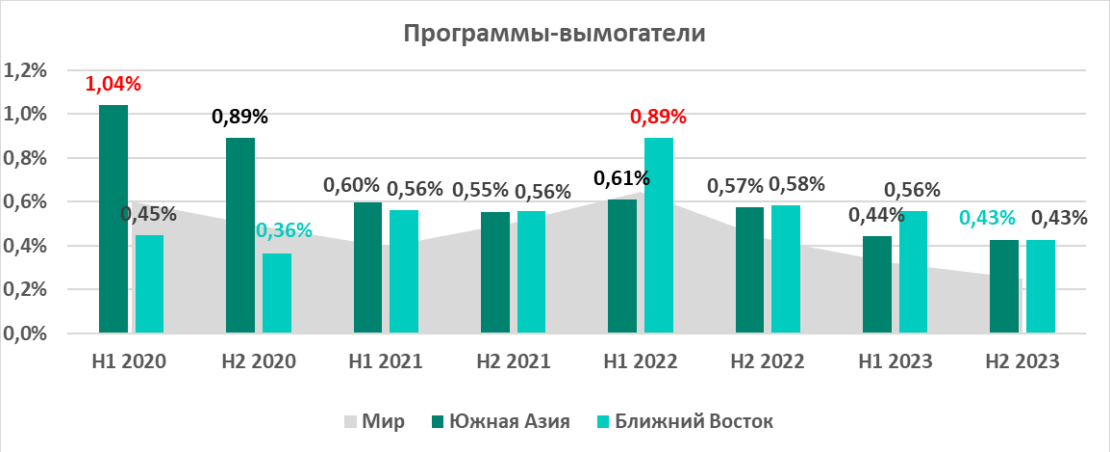
Среди регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, лидируют Южная Азия и Ближний Восток.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2023



В этом рейтинге Ближний Восток постепенно поднялся с седьмого места в первом полугодии 2020 года до первого места во втором полугодии 2023 года. По проценту атакованных вымогателями компьютеров АСУ рекордным для Ближнего Востока с 2020 года стало первое полугодие 2022 года (0,89%). За этот же период максимальный для всех регионов процент — 1,3% — был отмечен у Юго-Восточной Азии во втором полугодии 2021 года.

Южная Азия, Ближний Восток и мир. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, по полугодиям



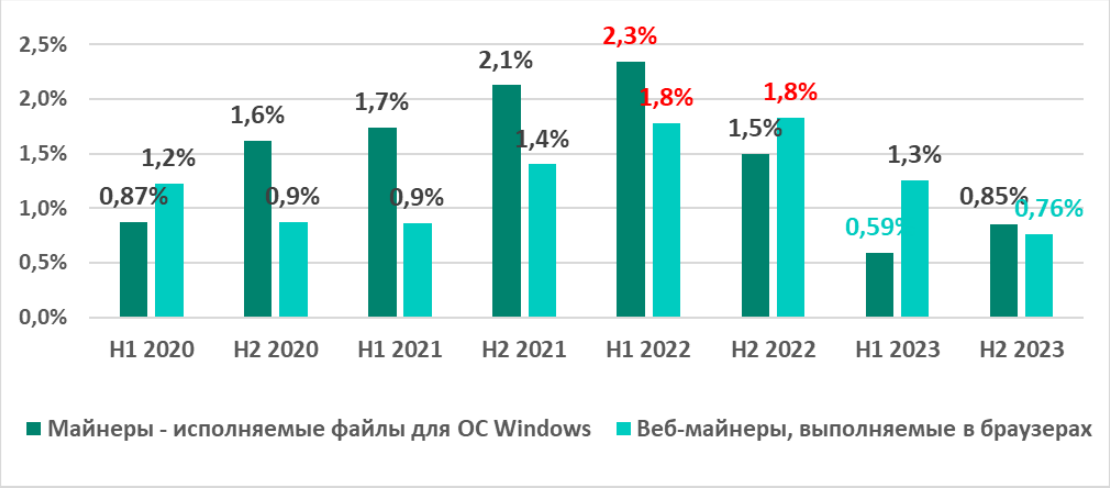
В список из 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, попали по четыре страны из лидирующих в рейтинге регионов — Южной Азии, Африки и Ближнего Востока.

Вредоносные программы для скрытого майнинга криптовалюты

Во втором полугодии 2023 года в мире процент компьютеров АСУ, на которых были заблокированы веб-майнеры, оказался минимальным с 2020 года.

Процент компьютеров АСУ, на которых были заблокированы вредоносные майнеры — исполняемые файлы для ОС Windows, за этот же период был наименьшим в первом полугодии 2023 года, во втором полугодии он подрос. Напомним, что в мире во втором полугодии 2023 года это была единственная категория вредоносного ПО, по которой увеличился процент атакованных компьютеров.

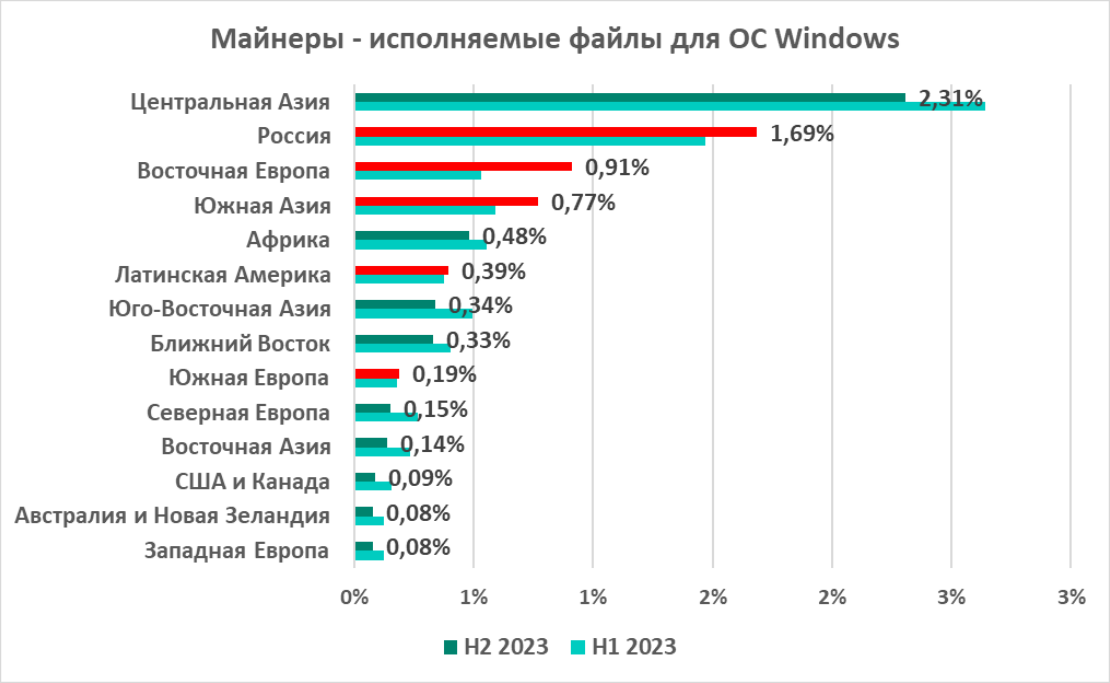
Процент компьютеров АСУ, на которых были заблокированы вредоносные программы для скрытого майнинга криптовалюты



Майнеры – исполняемые файлы для ОС Windows

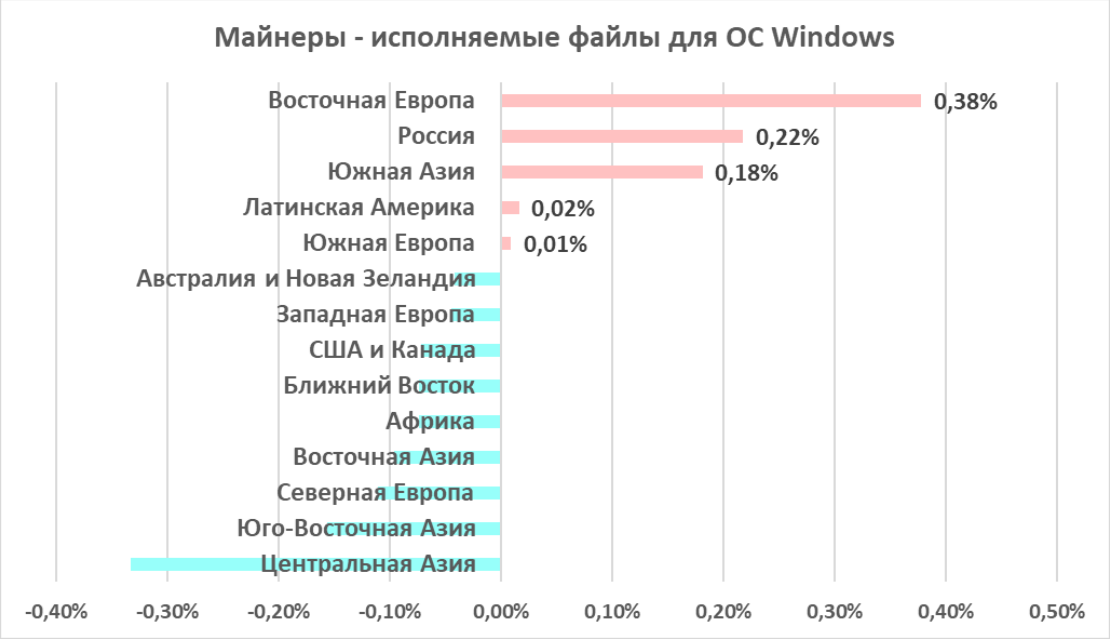
По проценту компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, среди регионов во втором полугодии 2023 года лидируют Центральная Азия и Россия.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные майнеры — исполняемые файлы, второе полугодие 2023 года



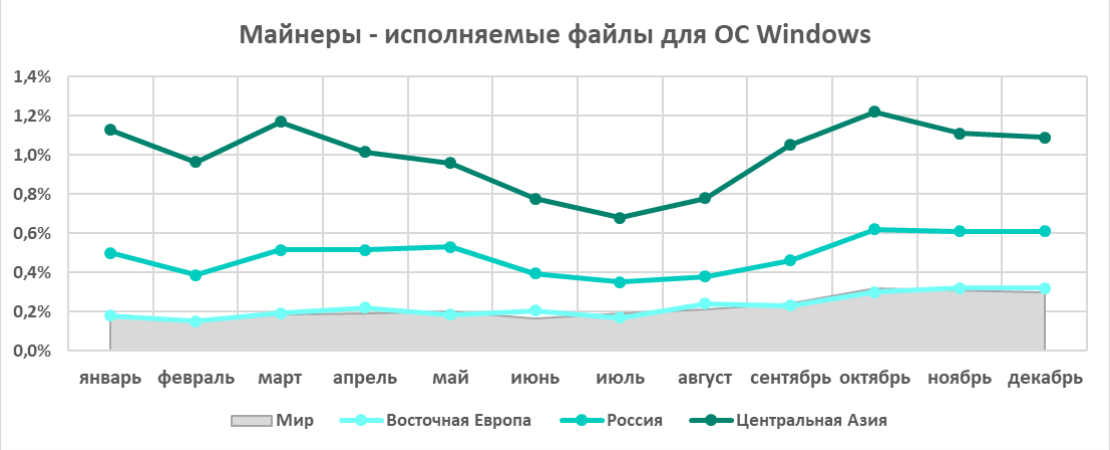
В пяти регионах по сравнению с предыдущим полугодием процент увеличился, больше всего в Восточной Европе — на 0,38 п.п. В лидирующей Центральной Азии процент уменьшился.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, за второе полугодие 2023 года



Выше, когда речь шла о проценте компьютеров АСУ, на которых были заблокированы вредоносные объекты всех категорий, мы уже отмечали сходство изменений (больше-меньше) процентов за месяц у Восточной Европы, Росси и Центральной Азии. В случае с майнерами — исполняемыми файлами это сходство также заметно, особенно у России и Центральной Азии.

Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, январь — декабрь 2023 года

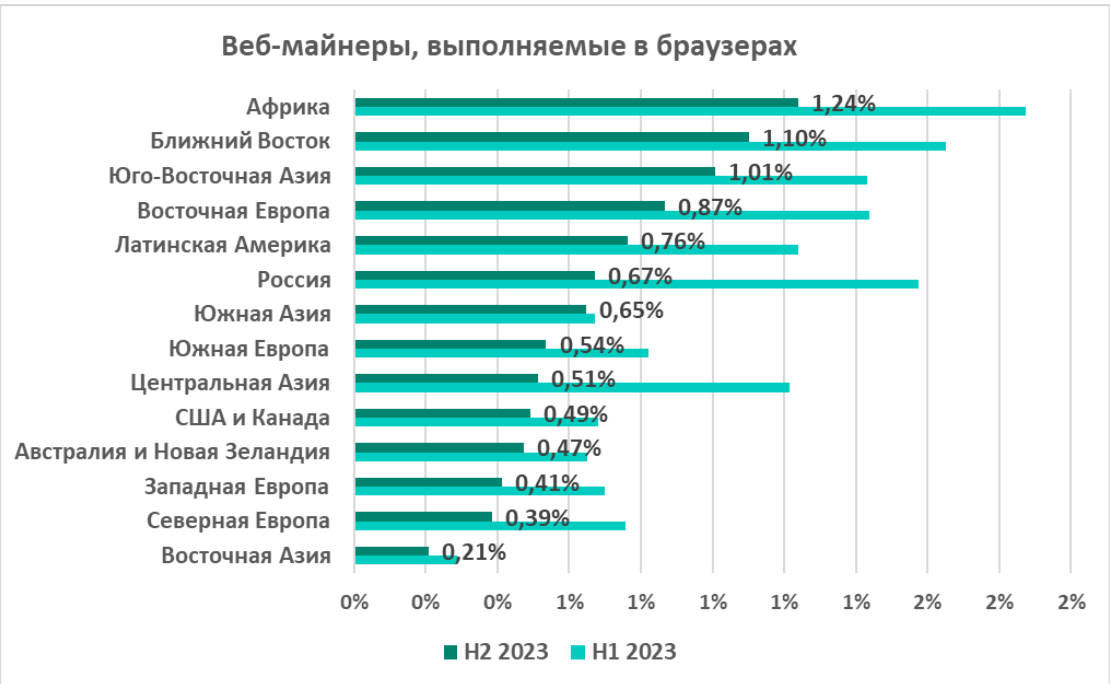


Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, с заметным отрывом от других стран лидируют Таджикистан (7,1%) и Туркмения (6,3%).

Веб-майнеры

В рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, лидируют Африка и Ближний Восток.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, выполняемые в браузерах, второе полугодие 2023 года



Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, на первом месте Йемен (3,9%), на втором — Сербия (3,5%).

Самораспространяющееся вредоносное ПО. Вирусы и черви

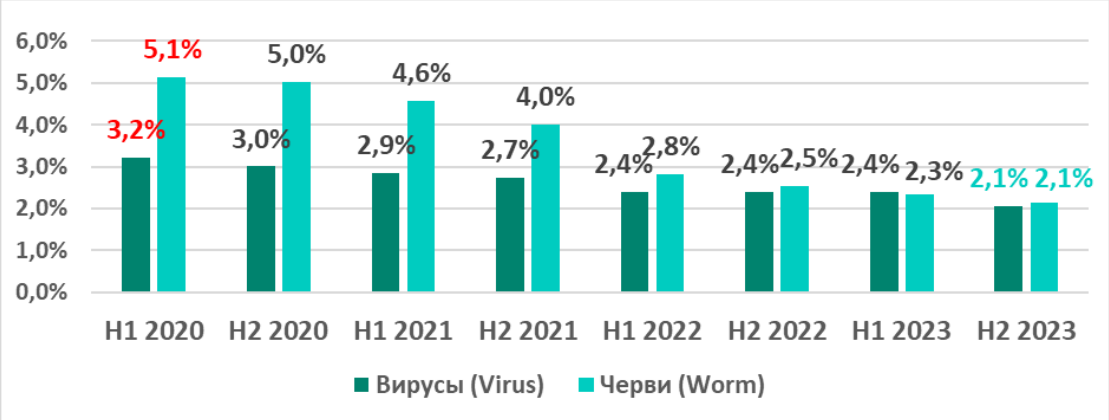
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

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

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

В мире процент компьютеров АСУ, на которых были заблокированы вирусы и черви, продолжает уменьшаться. Во втором полугодии 2023 года для каждой из этих угроз процент оказался минимальным с 2020 года.

Процент компьютеров АСУ, на которых были заблокированы вирусы и черви

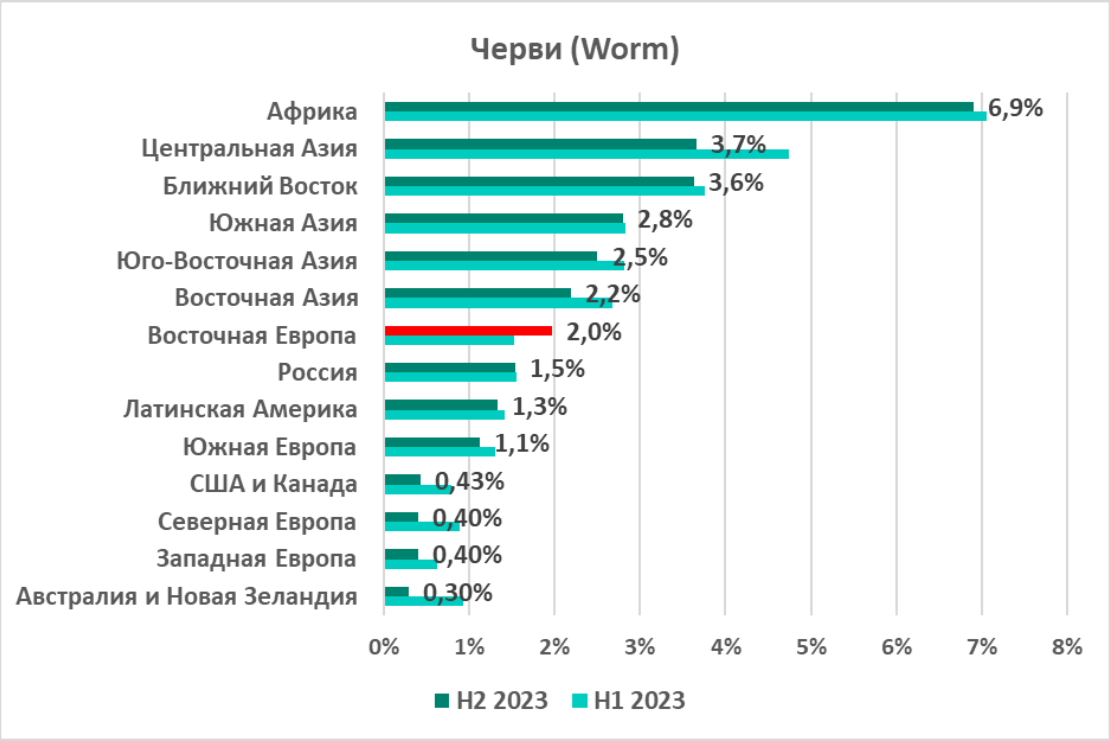


Черви

Африка по-прежнему лидирует среди регионов по проценту компьютеров АСУ, на которых детектируются черви. В регионе блокируются в том числе черви на Python, которые злоумышленники используют для распространения вредоносных майнеров. Регион с большим отрывом лидирует и по проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, на которых черви могут распространяться.

Из всех регионов за полугодие процент по червям вырос только в Восточной Европе — на 0,43 п.п.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы черви (worm), второе полугодие 2023 года



12 из 15 лидирующих по этому показателю стран — африканские. Две страны — из Центральной Азии, одна из них — Туркмения (19,7%) — на первом месте.

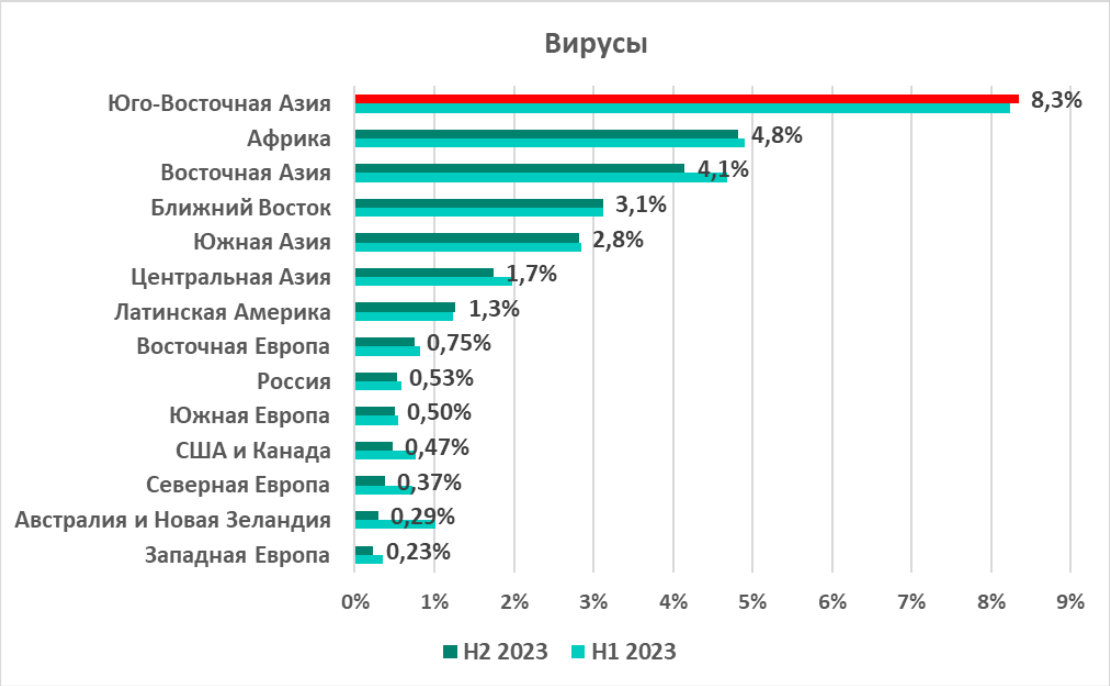
Вирусы

Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вирусы, вырос в лидирующей в рейтинге Юго-Восточной Азии — на 0,11 п.п.

Для Юго-Восточной Азии вирусы остаются актуальной проблемой. В этом регионе во втором полугодии 2023 года вирусы оказались

на третьем месте среди всех категорий вредоносного ПО в рейтинге по проценту компьютеров АСУ, на которых оно было заблокировано.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вирусы (virus), второе полугодие 2023 года



Среди стран и территорий самый высокий процент компьютеров АСУ, на которых блокируются вирусы, в Йемене (17,4%) и во Вьетнаме (14,3%).

Вредоносные программы для AutoCAD

По проценту компьютеров АСУ, на которых заблокировано вредоносное ПО для AutoCAD, в частности вирусы, лидирует Восточная Азия (1,2%). Эта категория угроз блокируется на компьютерах технологических сетей, в том числе в сетевых папках и на рабочих станциях инженеров.

Среди стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, лидируют Китай (7,84%), Вьетнам (1,4%) и Эфиопия (1,32%).

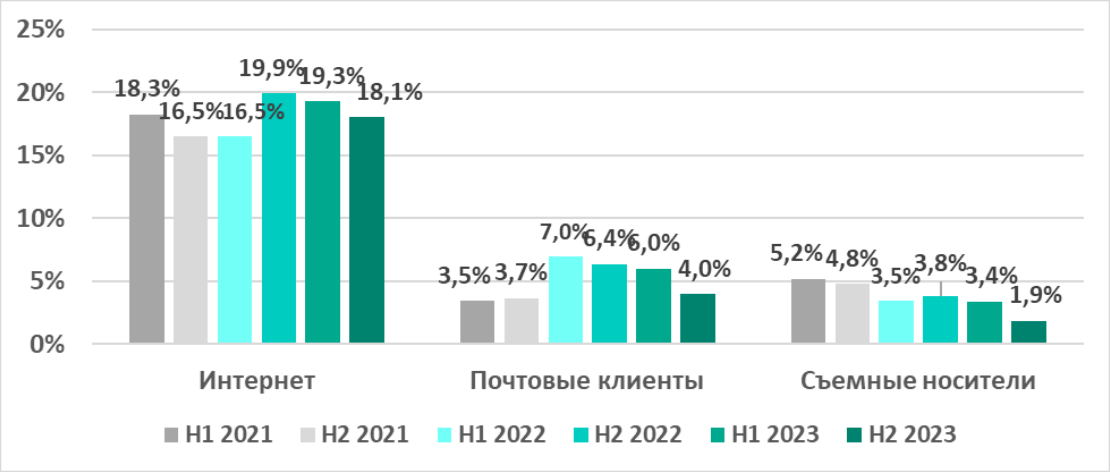
Основные источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, почтовые клиенты и съемные носители. Отметим, что источники заблокированных угроз надёжно установить удается не во всех случаях.

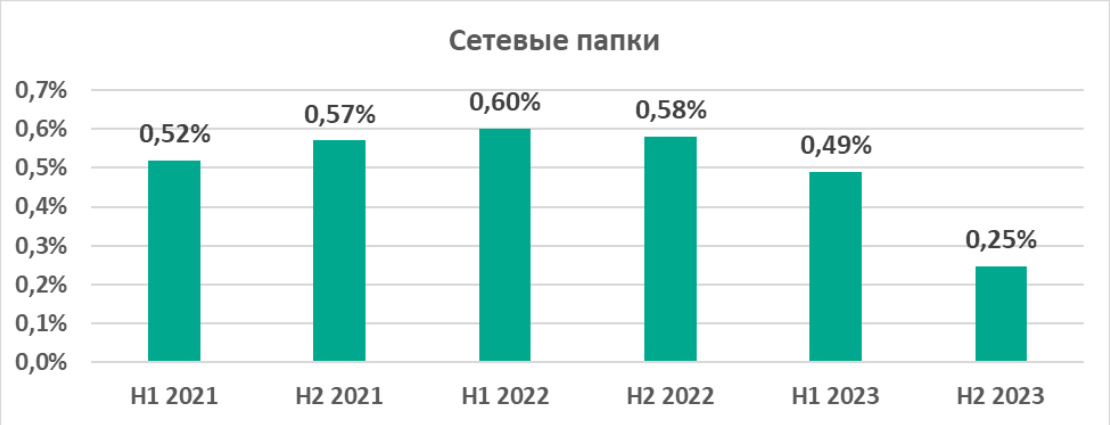
Мир

Во втором полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился для угроз из всех основных источников.

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



Процент компьютеров АСУ, на которых были заблокированы угрозы из сетевых папок



Как и в случае со статистикой по всем угрозам, процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, отличается в разных регионах.

Регионы

Интернет

Во втором полугодии 2023 года среди регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, лидируют Юго-Восточная Азия, Россия и Восточная Европа.

Процент вырос в четырех регионах, больше всего процент за полугодие вырос в Восточной Европе — на 3,2 п.п.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2023

Почтовые клиенты

Южная Европа сохраняет лидирующую позицию в рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, с первого полугодия 2022 года. С этого же времени на втором месте — Латинская Америка. Ближний Восток на третьем месте со второго полугодия 2022 года.

Во втором полугодии 2023 года процент компьютеров АСУ, на которых блокировались угрозы из почты, уменьшился во всех регионах.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, второе полугодие 2023

Съёмные носители

Рейтинг регионов по проценту компьютеров АСУ, на которых при подключении съёмных носителей было заблокировано вредоносное ПО, традиционно возглавляет Африка. Этот же регион с заметным отрывом лидирует по проценту компьютеров АСУ, на которых были заблокированы черви.

Во втором полугодии 2023 года процент компьютеров АСУ, на которых блокировались угрозы при подключении съёмных носителей, уменьшился во всех регионах.

Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2023

Сетевые папки

Сетевые папки — один из минорных источников вредоносных объектов. Больше всего процент компьютеров АСУ, на которых угрозы блокируются в сетевых папках, в Восточной и Юго-Восточной Азии.

Рейтинг регионов по проценту компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках, второе полугодие 2023

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 даёт нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счёт обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за её объёма и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные в значительной мере не только помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[2].

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 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;
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации.

[2] Организациям, в отношении любых данных которых наложены ограничения на их передачу во вне периметра организации, рекомендуем рассмотреть вариант использования сервиса Kaspersky Private Security Network.

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 процента 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», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com