kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2023

Kaspersky ICS CERT

13.09.2023 Version 1.0

Особенности полугодия

Цифры

Все угрозы

- В первом полугодии 2023 процент компьютеров АСУ, на которых были заблокированы вредоносные объекты (все угрозы), составил 34%. Это на 0,3 п.п. меньше, чем в предыдущем полугодии.
- Во втором квартале 2023 года в мире процент достиг максимального с 2022 года значения за квартал — 26,8%.
- В регионах показатель за полугодие варьирует от 40,3% в Африке до 14,7% в Северной Европе.
- В странах — от 53,3% в Эфиопии до 7,4% в Люксембурге.

Категории вредоносных объектов

- Вредоносные скрипты и фишинговые страницы были заблокированы на 12,7% компьютеров АСУ,
- Ресурсы в интернете из списка запрещенных — на 11,3%,
- Программы-шпионы — на 6%.
- Вредоносные документы — на 4%.
- Программы-вымогатели — на 0,32% компьютеров АСУ. Это минимальный процент с начала 2020 года.

Основные источники угроз

- Интернет был источником угроз, заблокированных на 19,3% компьютеров АСУ,
- Почтовые клиенты — на 6%,
- Съемные носители — на 3,4% компьютеров АСУ.

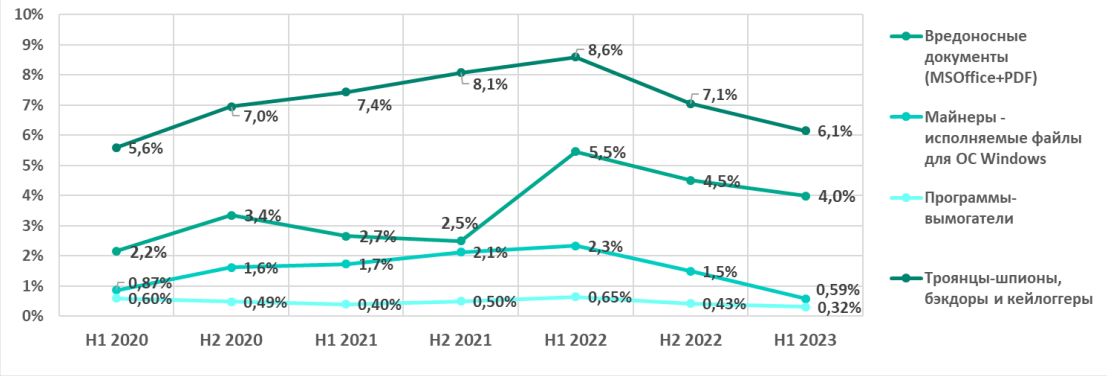
Хорошая новость

В первой половине 2022 года заметно вырос процент компьютеров АСУ, на которых были заблокированы:

- программы-шпионы,
- вредоносные документы,
- вредоносные майнеры — исполняемые файлы для ОС Windows,
- а также программы-вымогатели.

Это была новость плохая. Хорошая новость — со второго полугодия 2022 года проценты компьютеров АСУ, на которых блокировались все эти категории угроз, снижаются.

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



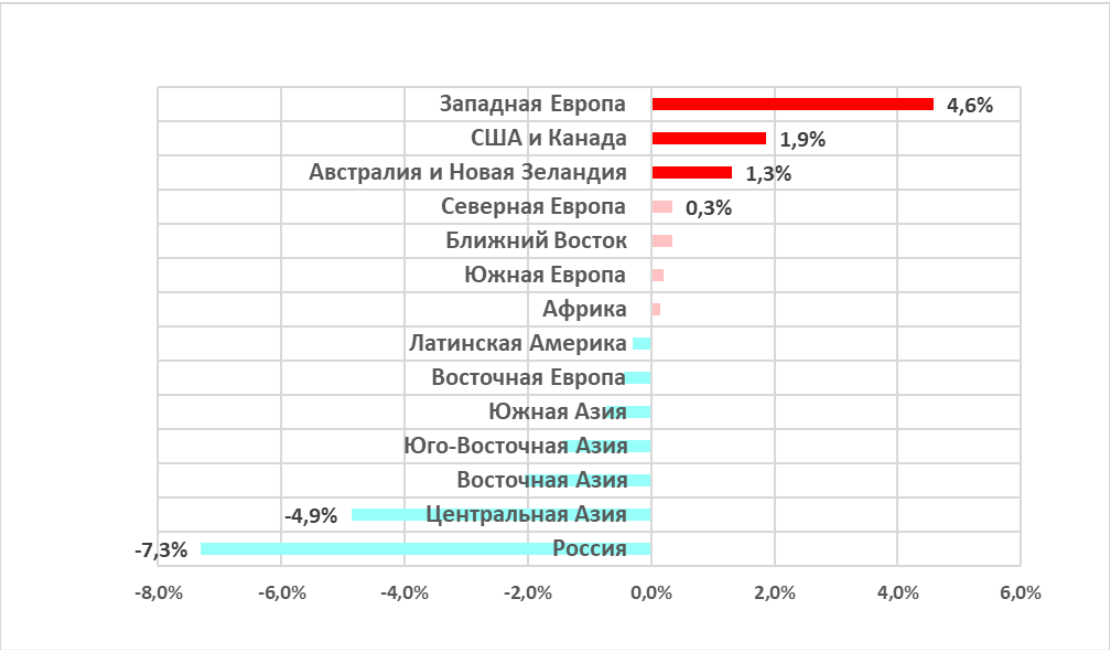
В первом полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы эти категории угроз, уменьшился почти во всех регионах. О неожиданных исключениях мы расскажем ниже.

Рейтинги неблагополучия, в которых лидируют благополучные регионы

Австралия и Новая Зеландия, США и Канада, Западная и Северная Европа — регионы, которые традиционно занимают последние места в рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Однако в первом полугодии 2023 года процент атакованных компьютеров АСУ вырос на максимальные величины (процентные пункты) именно в этих регионах.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, за первое полугодие 2023 года

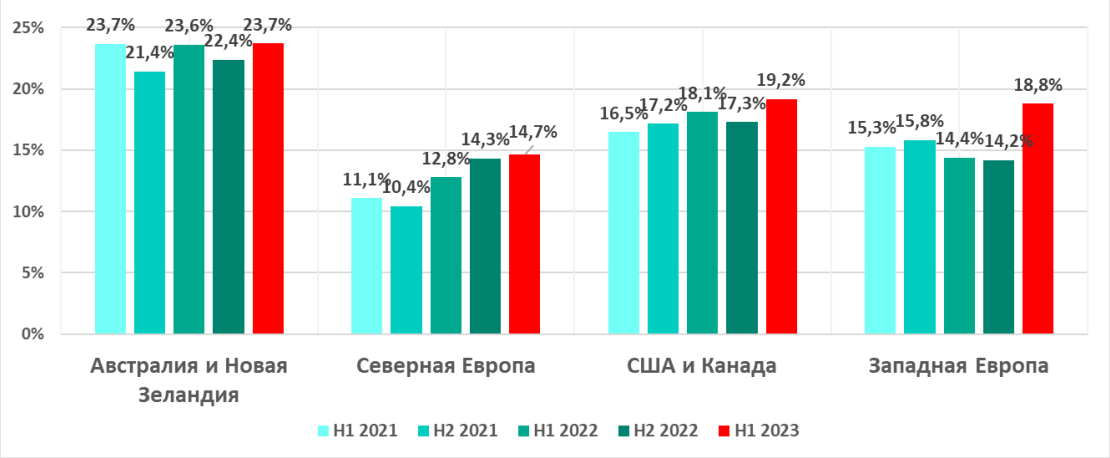


В Австралии и Новой Зеландии от полугодия к полугодию показатель колеблется, в первой половине 2023 года он не превысил значений предыдущих полугодий.

В Северной Европе, США и Канаде отмечена тенденция к увеличению процента атакованных компьютеров АСУ.

В Западной Европе процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, снижался в 2022 году, но в первом полугодии 2023 года резко вырос и превысил показатели полугодий предыдущих двух лет.

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

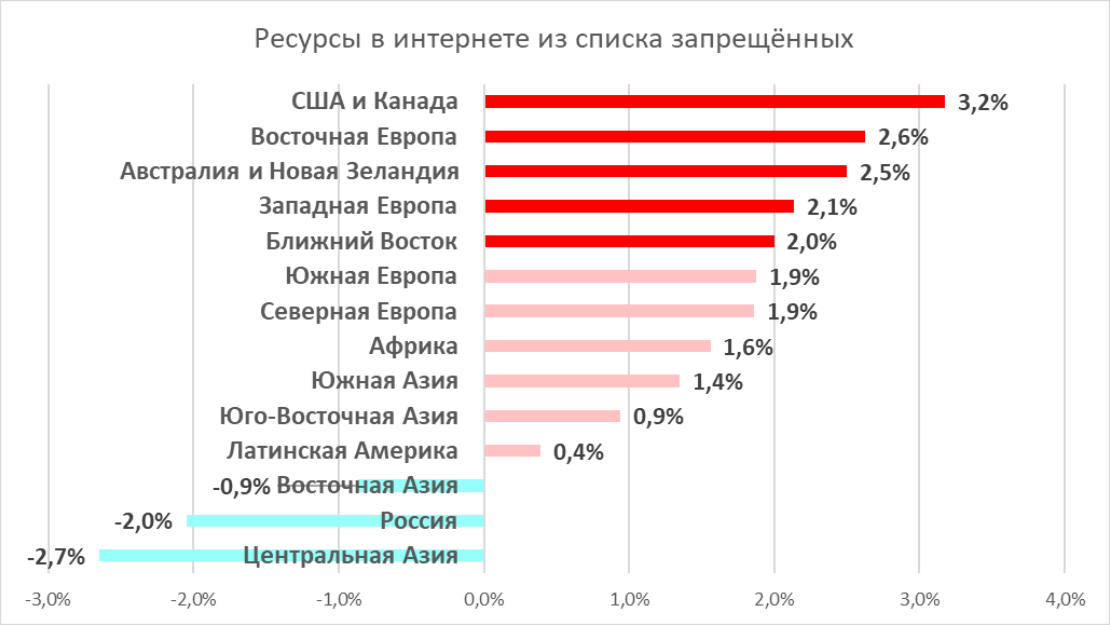


Сразу отметим, что, **несмотря на рост процента атакованных компьютеров, эти регионы не потеряли статуса регионов с минимальными процентами практически по всем критериям.**

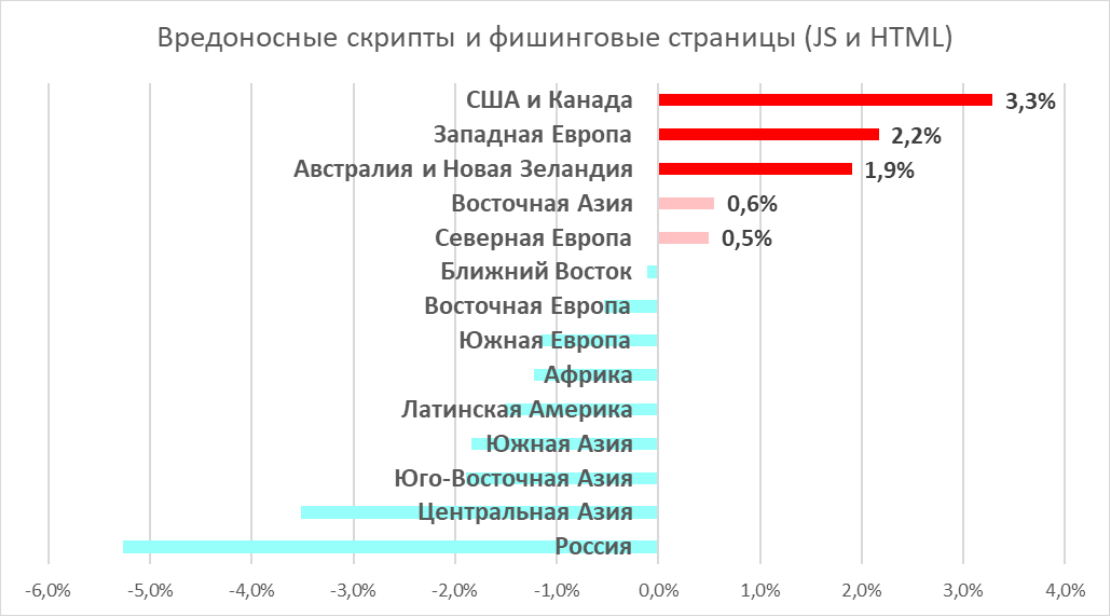
Однако если говорить об **увеличении процента за полугодие**, то в первом полугодии 2023 года эти регионы заняли лидирующие позиции во многих рейтингах.

Рост процента атакованных компьютеров АСУ в традиционно благополучных регионах обусловлен прежде всего увеличением процента компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, а также вредоносные скрипты и фишинговые страницы.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещённых, за первое полугодие 2023 года



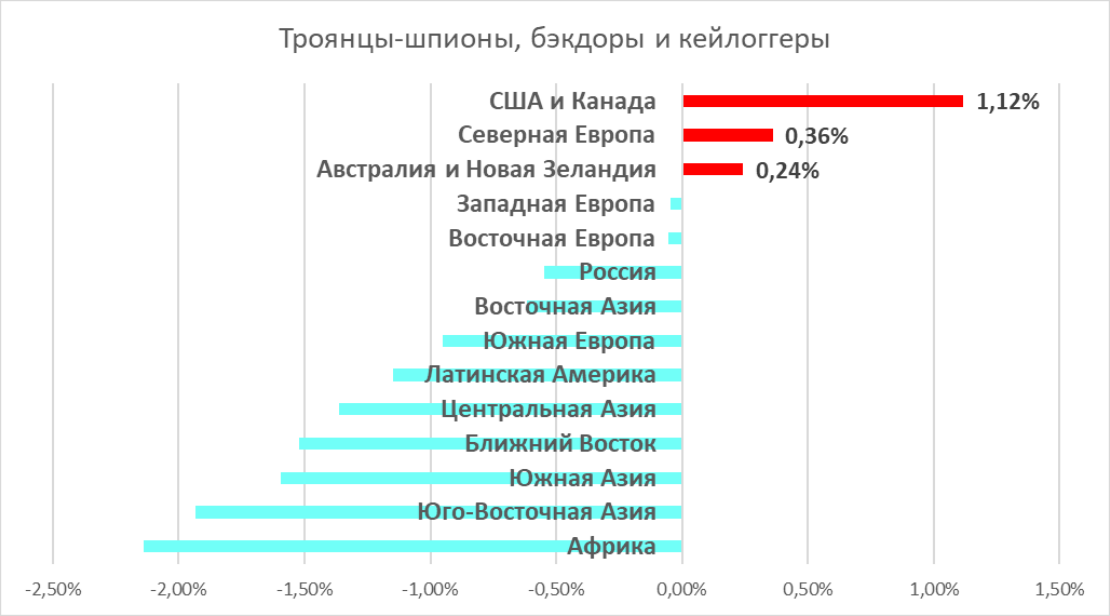
Изменение в регионах процента компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, за первое полугодие 2023 года



Обе эти угрозы распространяются в интернете, вредоносные скрипты и фишинговые страницы — и в интернете, и в почте. Процент компьютеров АСУ, на которых были заблокированы угрозы из этих двух источников, в США и Канаде и в Западной Европе также увеличился на максимальные среди регионов величины.

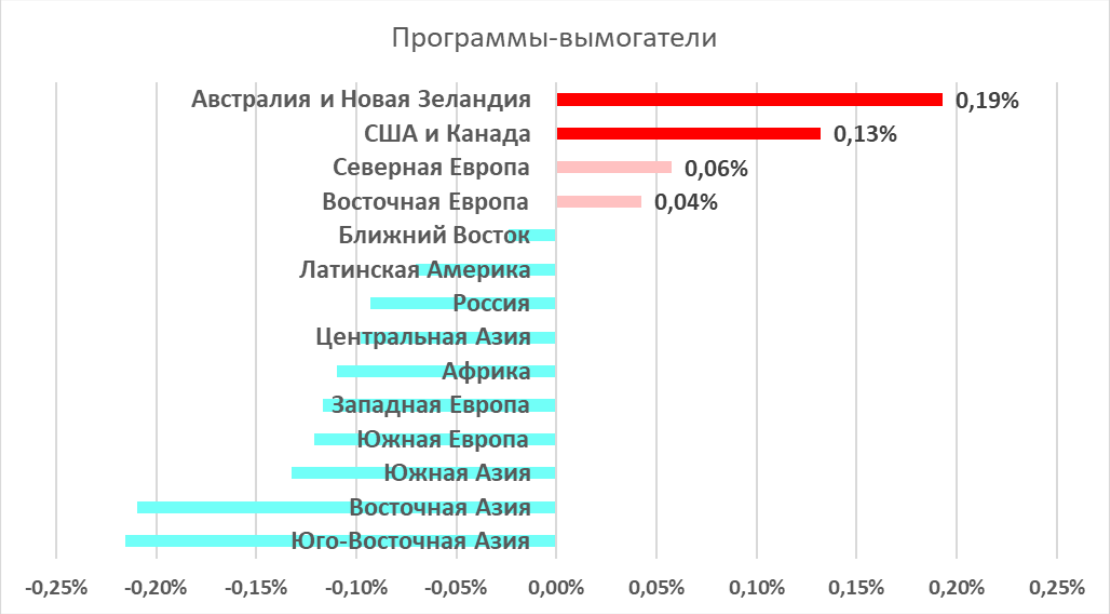
Однако этим лидерство регионов не ограничивается. В США и Канаде, Северной Европе и в Австралии и Новой Зеландии больше, чем в остальных регионах, вырос процент компьютеров, на которых были заблокированы шпионские программы.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы программы-шпионы, за первое полугодие 2023 года



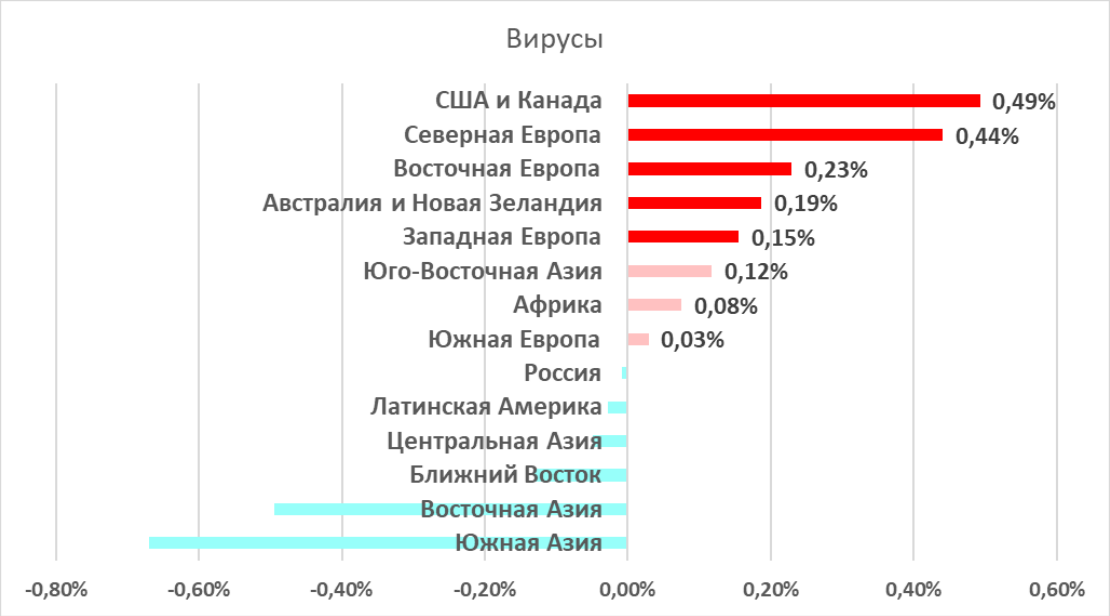
Отметим также, что процент атакованных программами-вымогателями компьютеров АСУ в первом полугодии увеличился в четырех регионах, в том числе в Австралии и Новой Зеландии, в США и Канаде — на заметные для этих регионов 0,19 п.п. и 0,13 п.п. соответственно, — а также в Северной Европе.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы программы-вымогатели, за первое полугодие 2023 года

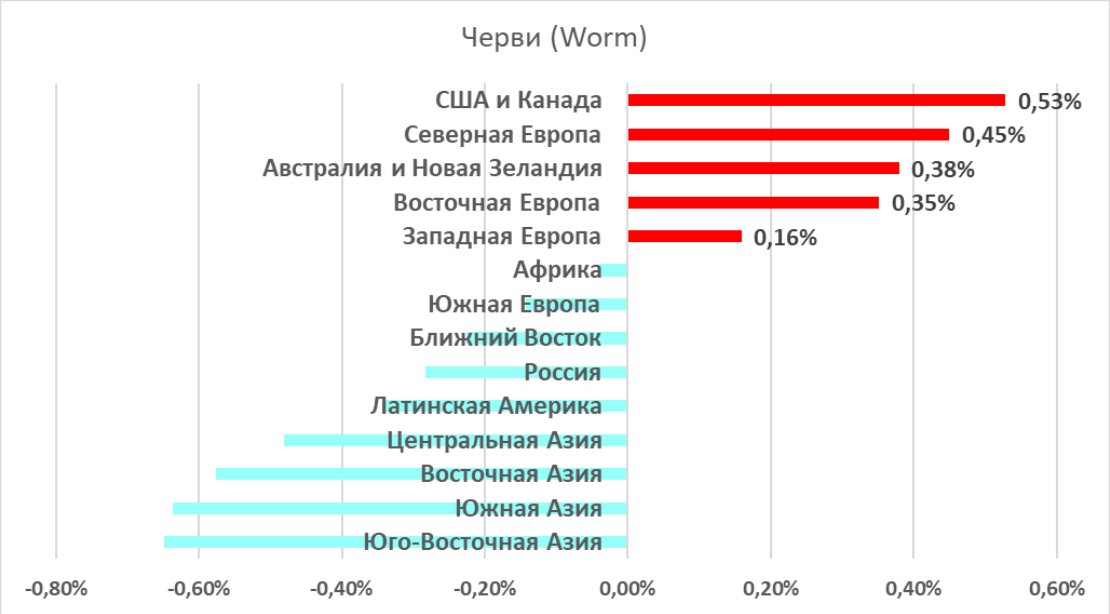


Неожиданные результаты и по проценту компьютеров АСУ, на которых были заблокированы вирусы и черви: среди пяти регионов, где эти показатели увеличились на максимальные величины — США и Канада, Северная Европа, Австралия и Новая Зеландия и Западная Европа.

Изменение в регионах процента компьютеров АСУ, на которых были заблокированы вирусы, за первое полугодие 2023 года



Изменение в регионах процента компьютеров АСУ, на которых были заблокированы черви, за первое полугодие 2023 года



В Австралии и Новой Зеландии при этом увеличился процент компьютеров АСУ, на которых угрозы были заблокированы при подключении съёмных носителей.

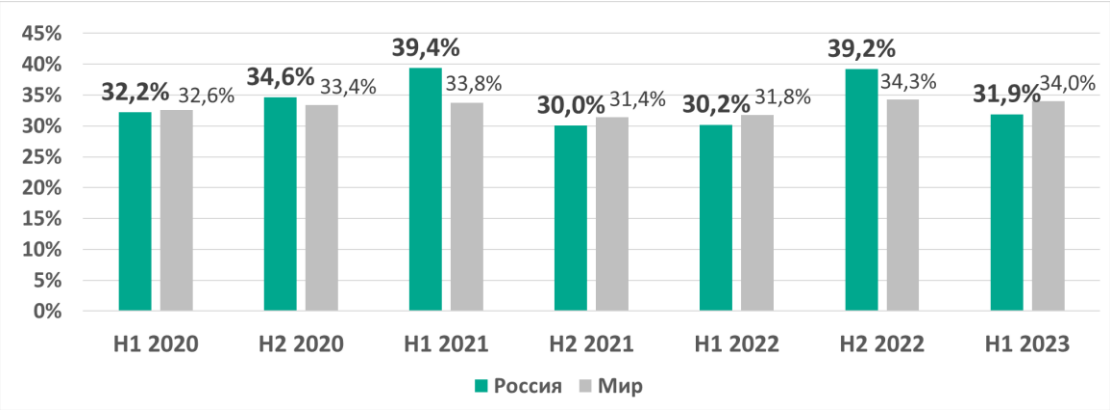
Изменение в регионах процента компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, за первое полугодие 2023 года

Россия в первом полугодии 2023

В первом полугодии 2023 года в России вредоносные объекты были заблокированы на 31,9% компьютеров АСУ. Это на 2,1 п.п. меньше, чем в среднем по миру.

В предыдущем полугодии в основном в результате массового заражения сайтов (в том числе промышленных организаций), использующих устаревшую версию одной из популярных российских CMS, процент атакованных компьютеров АСУ в России вырос на 9 п.п. В первом полугодии 2023 года — уменьшился на 8,3 п.п.

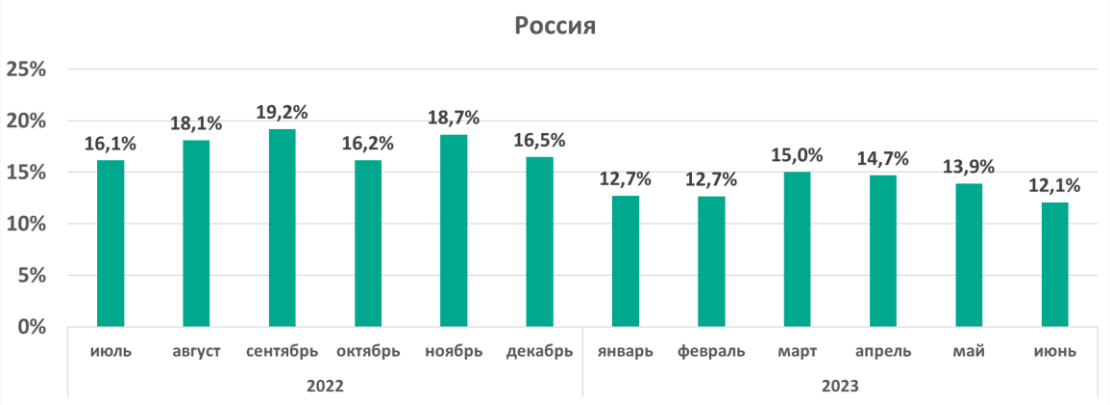
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



Самый высокий за первое полугодие 2023 года процент атакованных компьютеров АСУ отмечен в марте (15%), самый низкий — в июне (12,1%).

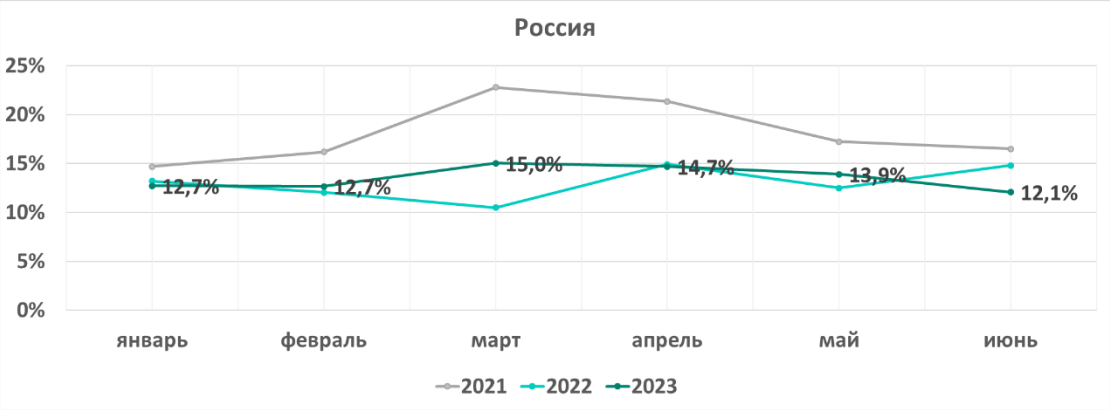
При этом даже мартовский максимум уступает показателям за месяцы предыдущего полугодия.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, июль 2022 — июнь 2023 года



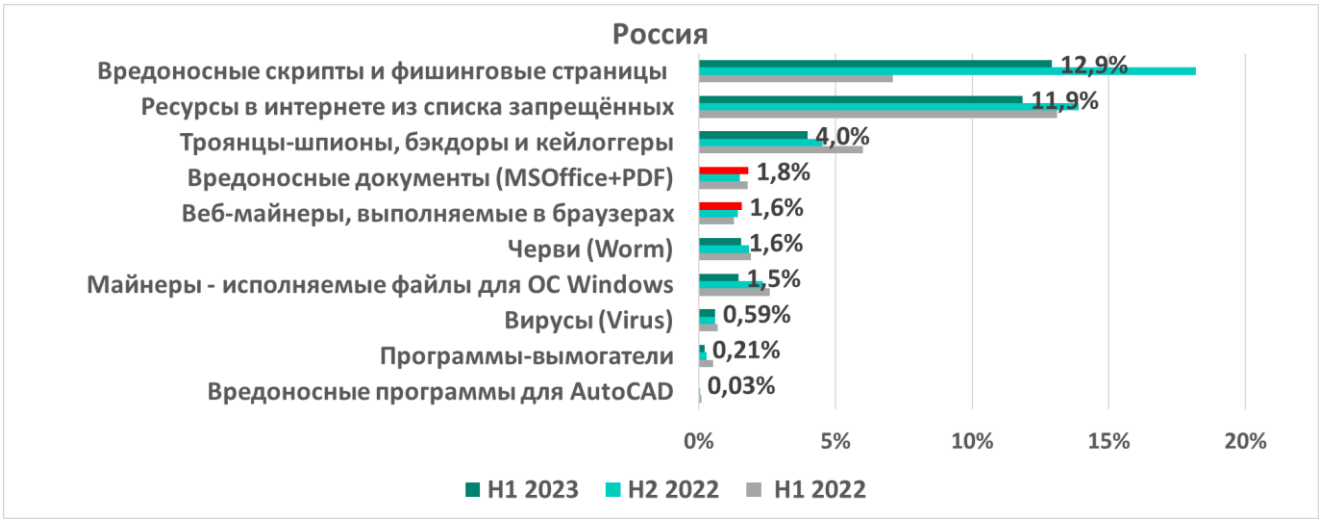
Изменения процента по месяцам первого полугодия 2023 года (больше — меньше) больше похожи на изменения по месяцам в аналогичный период 2021 года, чем на январь — июнь 2022 года.

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



Категории вредоносного ПО

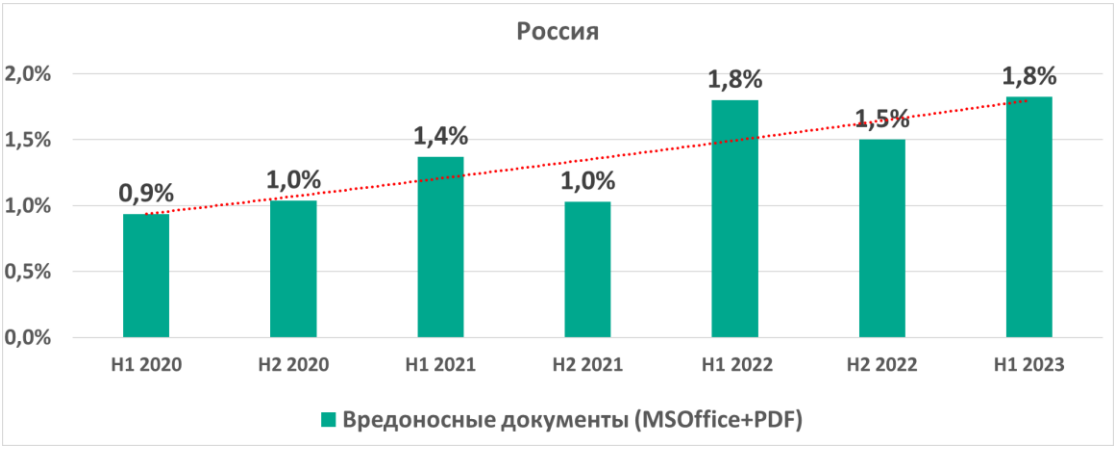
В первом полугодии 2023 года в России уменьшился процент атакованных компьютеров для большинства категорий угроз. Выросли только проценты компьютеров, на которых были заблокированы вредоносные документы (на 0,32 п.п.) и веб-майнеры (на 0,13 п.п.).



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

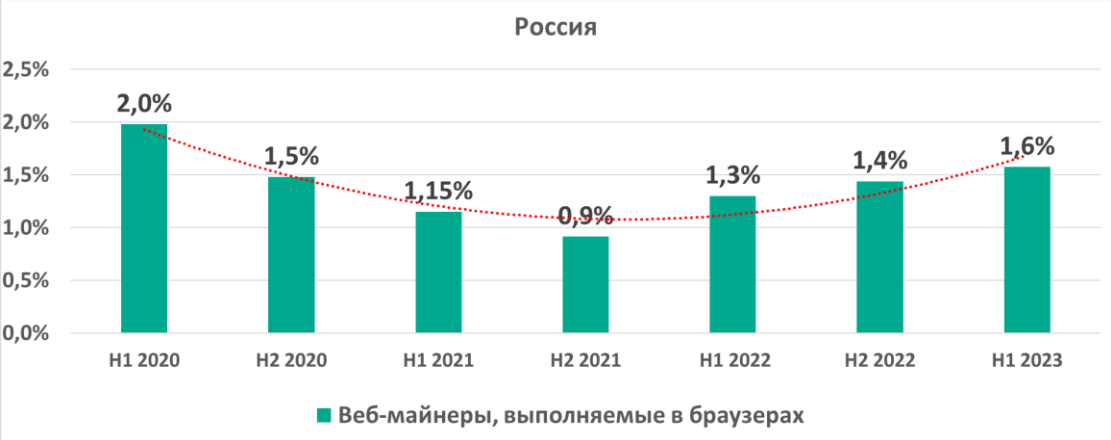
Тенденция по вредоносным документам в мире и в России противоположная: если в мире процент компьютеров, на которых заблокированы вредоносные документы, снижается с 2022 года, то в России процент таких компьютеров за три года вырос вдвое — с 0,9% в первом полугодии 2020 до 1,8% в первом полугодии 2023 года. Основной канал распространения таких угроз — электронная почта.

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



Показатель веб-майнеров в России в 2020 — 2021 годах уменьшался, а расти начал только в 2022 году. За полтора года он увеличился с 0,9% до 1,6% — т.е. в 1,8 раз.

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

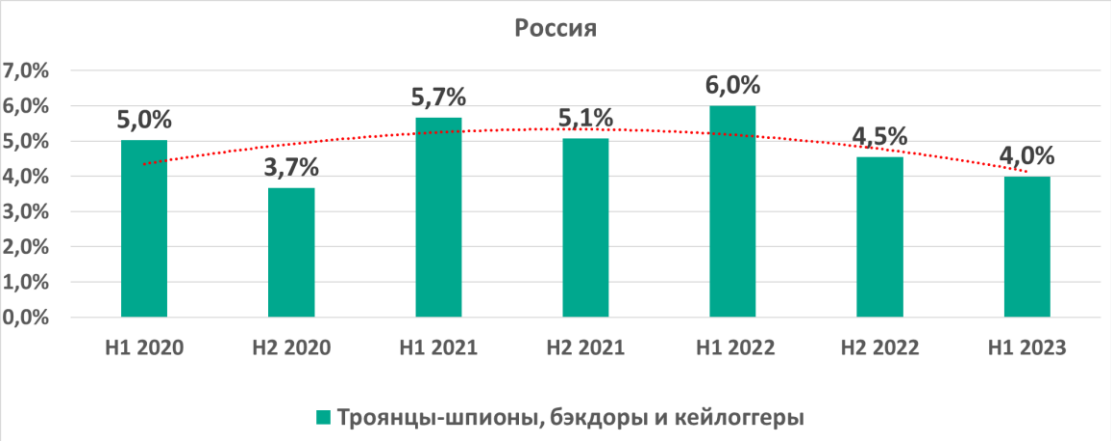


Со второго полугодия 2022 года в России уменьшается процент компьютеров АСУ, на которых были заблокированы:

- программы-шпионы,
- майнеры — исполняемые файлы для ОС Windows,
- вирусы,
- черви,
- вредоносное ПО для AutoCAD
- и программы-вымогатели.

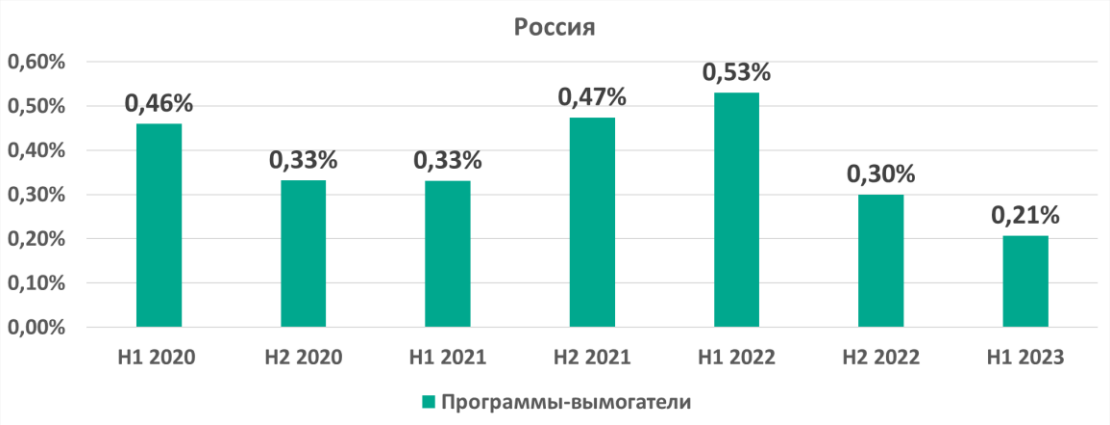
Отметим, что показатели программ-шпионов, майнеров — исполняемых файлов и программ-вымогателей в тот же период снижался и в среднем по миру.

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



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

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

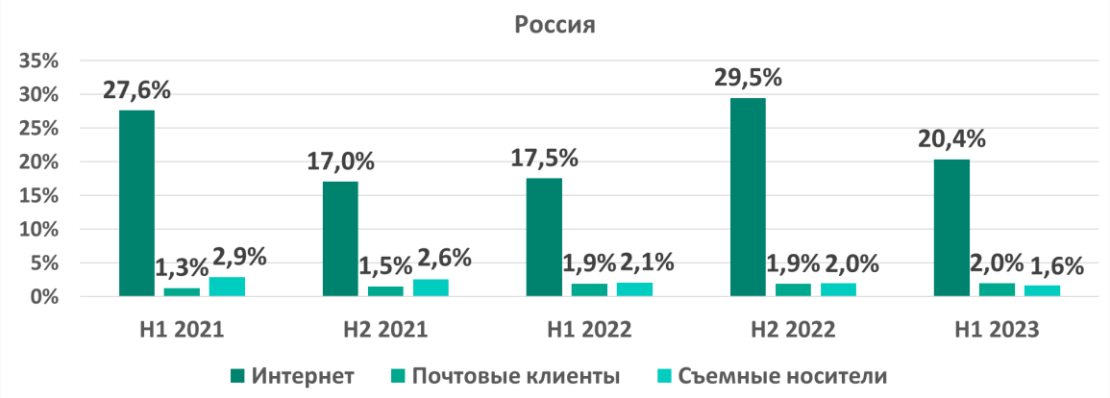


Источники угроз

Из основных источников угроз в России в первом полугодии 2023 года уменьшился процент компьютеров АСУ, на которых были заблокированы:

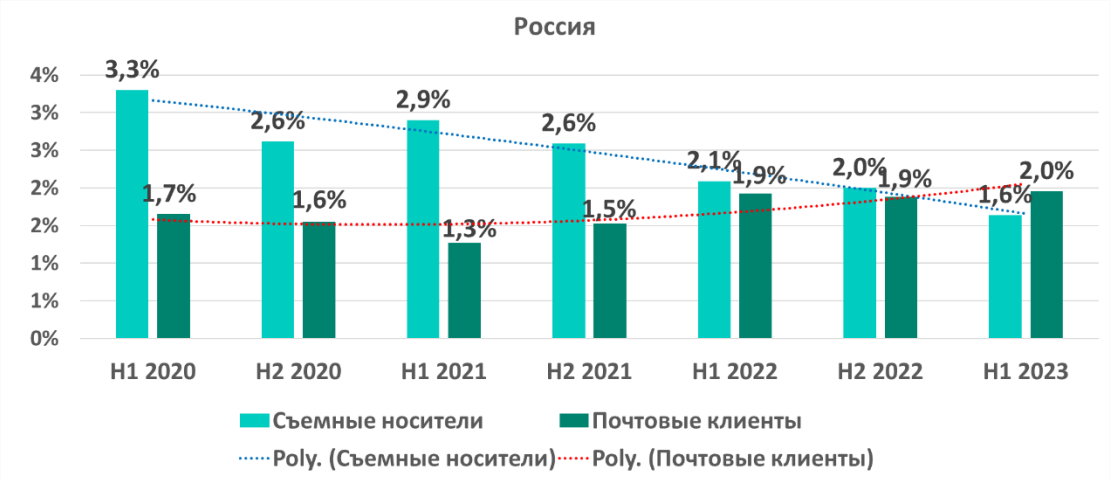
- угрозы из интернета — на 9,1 п.п.,
- угрозы, обнаруженные при подключении съемных носителей, — на 0,4 п.п.

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



В первом полугодии 2023 года почта впервые стала в России более значимым источником угроз для компьютеров АСУ, чем съемные носители. Процент компьютеров АСУ, источником угроз для которых были почтовые клиенты, растет со второго полугодия 2021 года. С этого же времени уменьшается показатель угроз на съемных носителях, и в первом полугодии 2023 года он оказался на 0,4 п.п. меньше, чем процент компьютеров АСУ, на которых были заблокированы угрозы из почты.

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

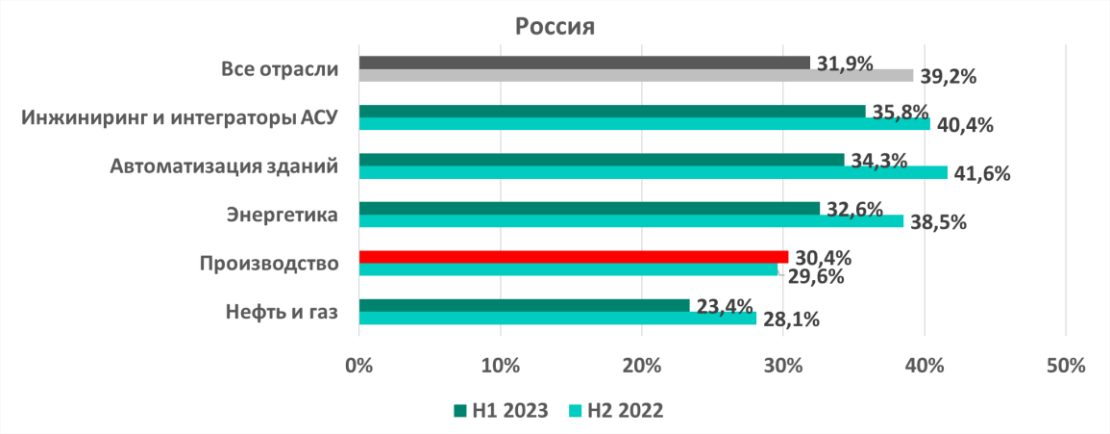


Процент компьютеров АСУ, на которых были заблокированы угрозы из сетевых папок, в первом полугодии 2023 года в России составил 0,40% — на 0,13 п.п. меньше, чем в предыдущем полугодии.

Некоторые отрасли

В первом полугодии 2023 года в России Производство — единственная из исследуемых отраслей, где процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился.

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

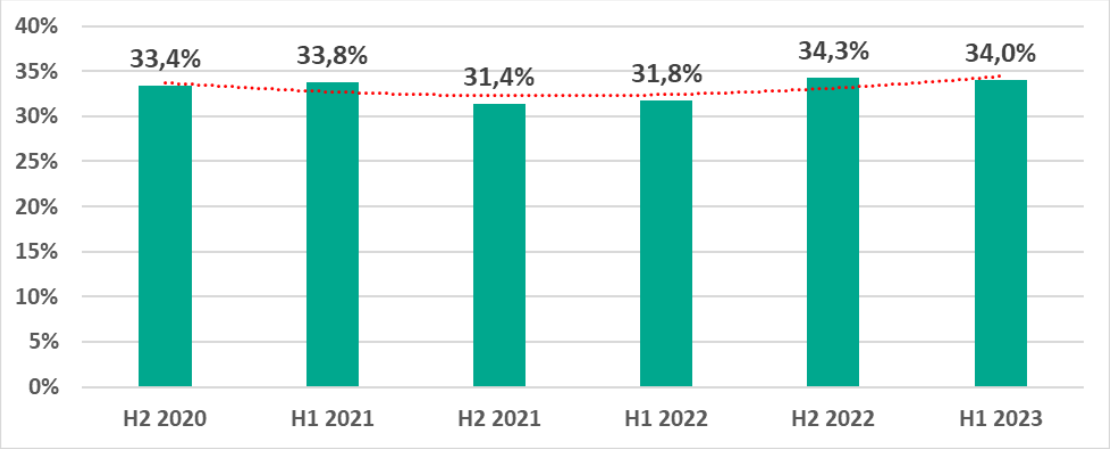


Уменьшение процента атакованных компьютеров АСУ в остальных исследуемых отраслях по сравнению со вторым полугодием 2022 года преимущественно связано со снижением показателей для интернет-угроз.

Глобальная статистика по всем угрозам

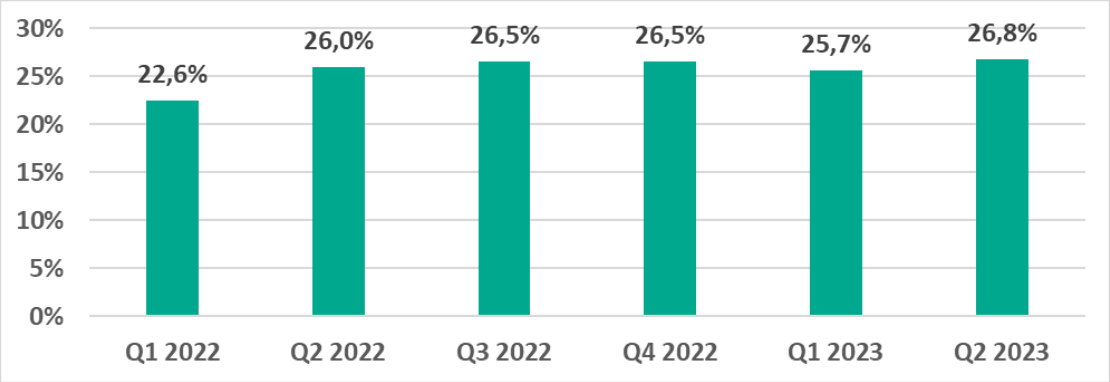
В первом полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с предыдущим полугодием всего на 0,3 п.п. и составил 34%.

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



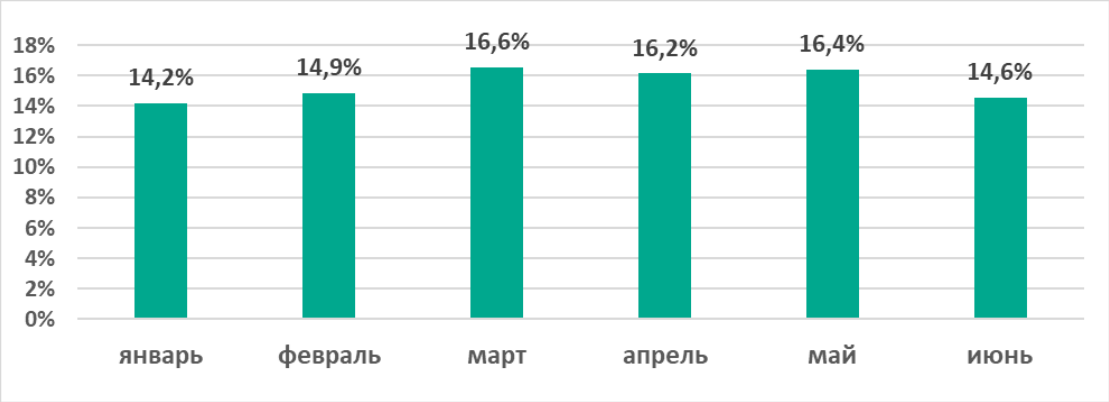
При этом в первом квартале 2023 года процент атакованных компьютеров АСУ уменьшился, а во втором вырос и достиг максимального с 2022 года значения за квартал.

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



В весенние месяцы (март — май) процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был выше, чем в остальные месяцы полугодия.

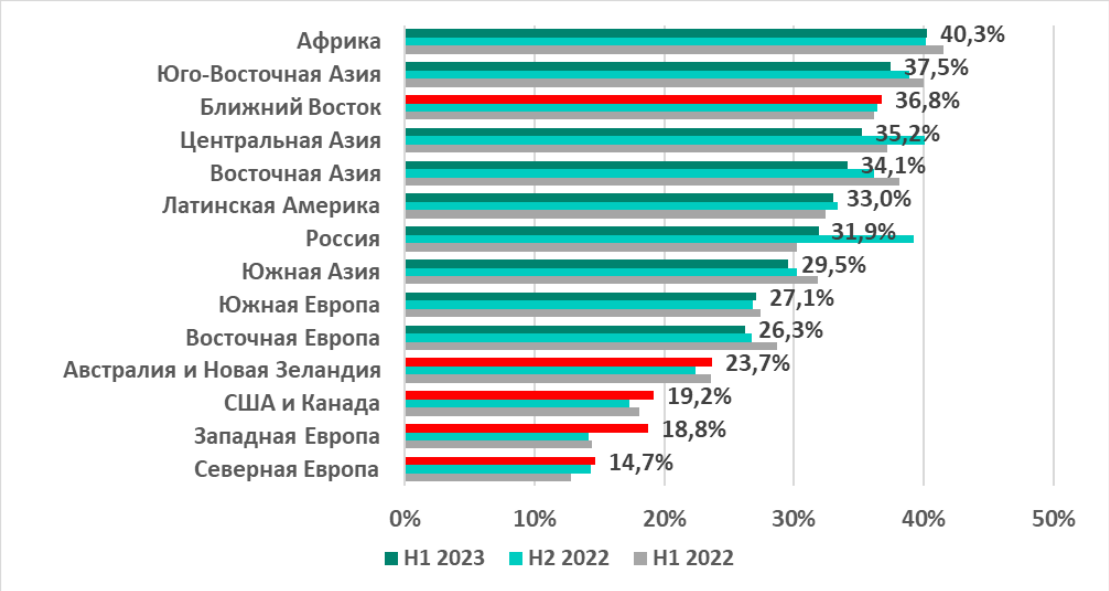
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — июнь 2023



Регионы

В регионах мира доля компьютеров АСУ, на которых была предотвращена вредоносная активность, варьирует от 40,3% в Африке до 14,7% в Северной Европе.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах

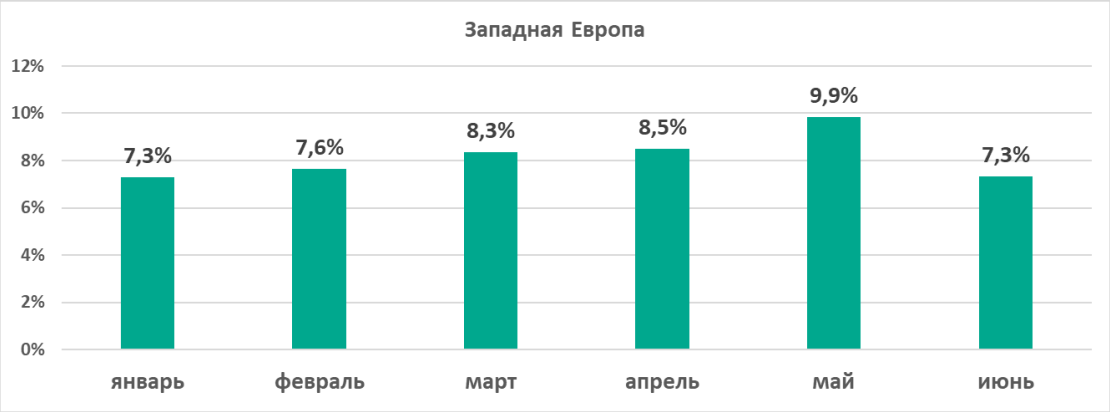


Напомним, что в России и в Центральной Азии в прошлом полугодии процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, заметно вырос в результате массового заражения сайтов (в том числе промышленных организаций), использующих устаревшую версию одной из популярных российских CMS. В первом полугодии 2023 года показатели обоих регионов вернулись к значениям, близким к первому полугодию 2022 года.

Как уже было сказано выше, наиболее значительный рост процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, отмечен в Западной Европе (+4,6 п.п.), США и Канаде (+1,9 п.п.), а также

в Австралии и Новой Зеландии (1,3 п.п.). Отметим также небольшой, но устойчивый рост процента в Северной Европе и на Ближнем Востоке (+0,3 п.п. в каждом регионе).

В Западной Европе, где прирост был максимальным среди всех регионов, в первом полугодии 2023 года процент атакованных компьютеров АСУ увеличивался от месяца к месяцу вплоть до мая, а в июне снизился до показателя января.

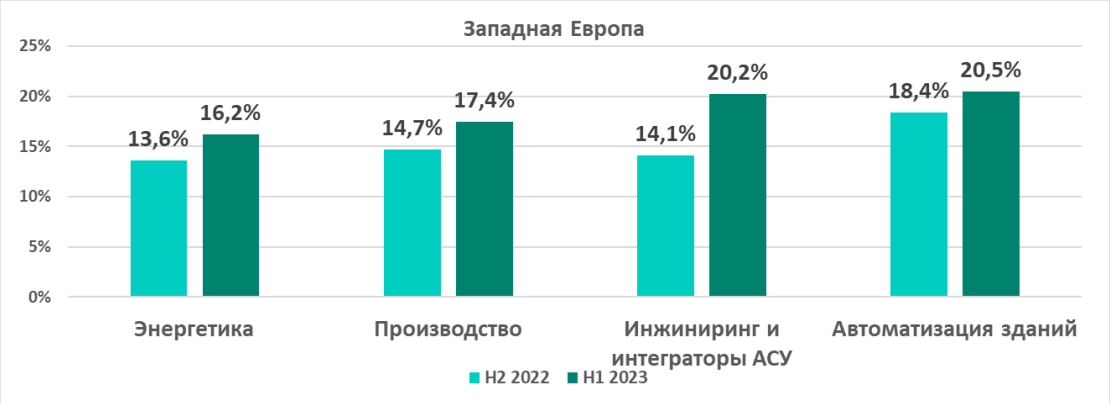


Западная Европа. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь — июнь 2023 года

По нашим данным, в первом полугодии 2023 г. злоумышленники вспомнили старый фишинговый метод, который впервые был использован в 2010 г. для атак на организации (в том числе промышленные) в Европе: сайт жертвы заражается вредоносным скриптом, который запускает всплывающее окно, внешне очень похожее на окно техподдержки Microsoft. В окне нет ссылок, вместо них пользователь видит фишинговое сообщение и местный номер телефона, по которому необходимо позвонить. На звонок отвечает злоумышленник, разговаривающий на региональном языке, и вынуждает ничего не подозревающего пользователя скачать и установить программу для удаленного доступа к компьютеру или многофункциональное шпионское ПО. Злоумышленники используют приемы социальной инженерии для обмана пользователей и получения несанкционированного доступа к их системам, что представляет серьезную угрозу для организаций, в том числе промышленных.

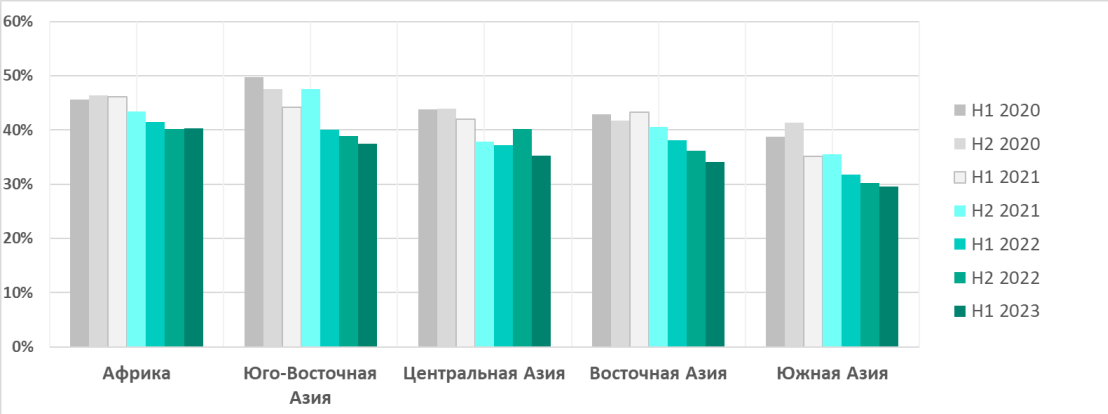
В этом регионе среди исследуемых отраслей наиболее значительно процент выпрос в отрасли Инжиниринг и интеграторы АСУ (+6,1 п.п.).

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



Большинство регионов, где в первом полугодии 2023 года отмечен рост процента атакованных компьютеров АСУ, — Северная и Западная Европа, США и Канада, Австралия и Новая Зеландия — это регионы, замыкающие рейтинг по этому показателю. В то же время в Африке и регионах Азии, где процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, традиционно высок, видна тенденция к его снижению.

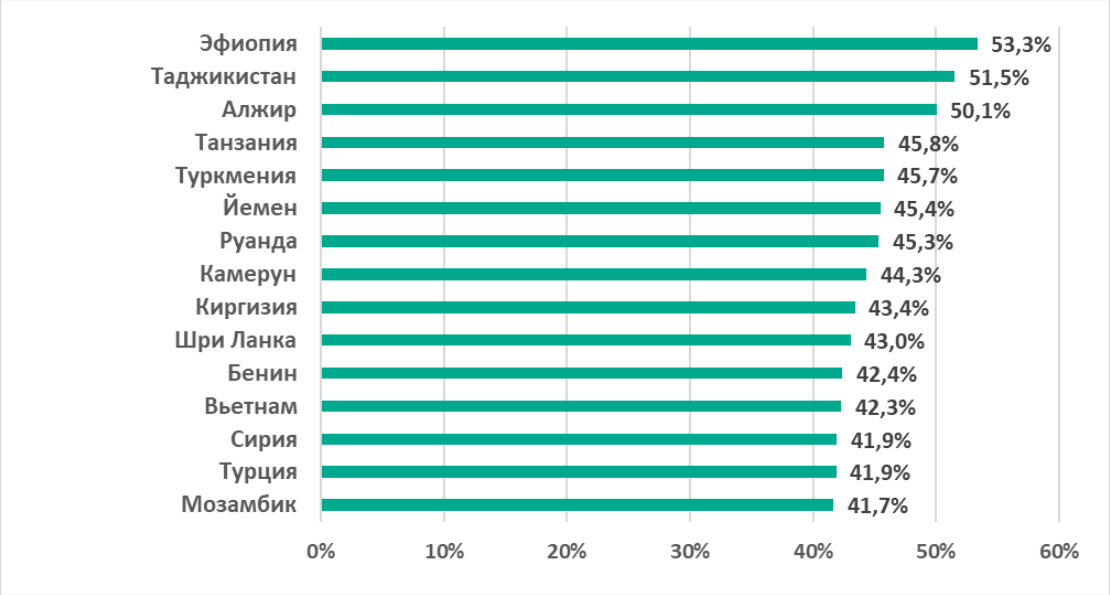
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Африке и регионах Азии



Страны

В разных странах процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, варьирует от 53,3% в Эфиопии до 7,4% в Люксембурге.

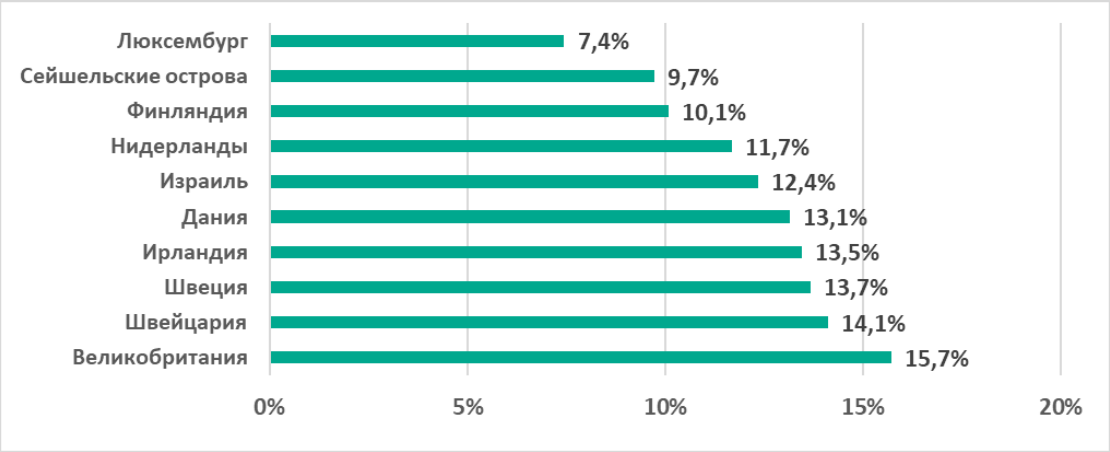
15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты в первом полугодии 2023



Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты, в первом полугодии 2023 года 7 африканских стран, по 3 страны из Ближнего Востока и Центральной Азии.

В десятке стран с наименьшими показателями половина стран из Северной Европы.

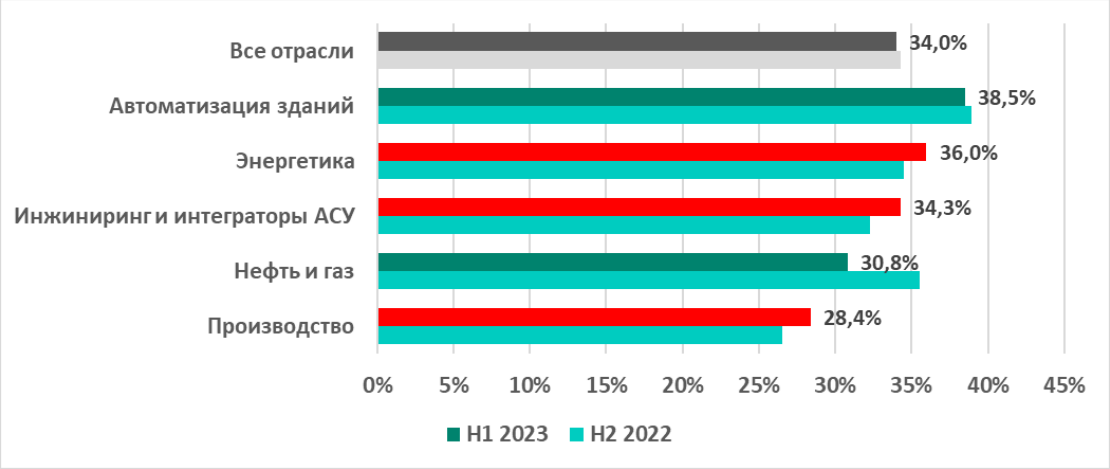
10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты в первом полугодии 2023



Некоторые отрасли

В первом полугодии 2023 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, увеличился в отраслях Инжиниринг и интеграторы АСУ (+2 п.п.), Производство (+1,9 п.п.) и Энергетика (+1,5 п.п.).

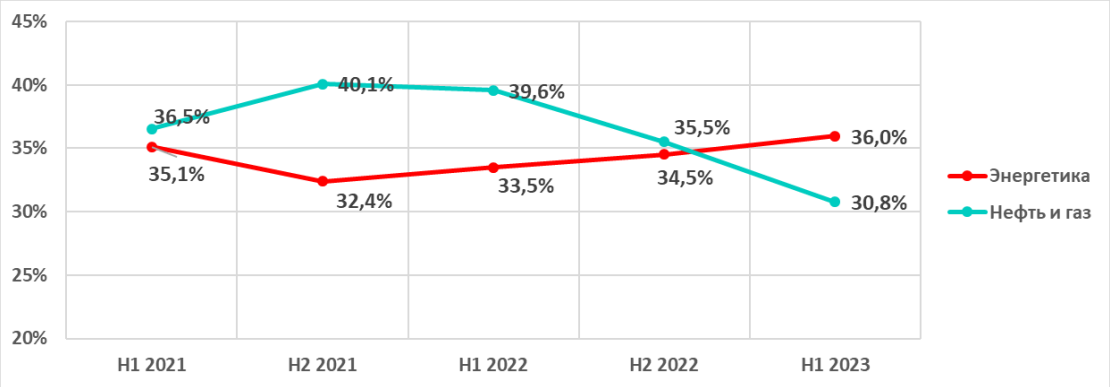
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях



Автоматизация зданий по-прежнему лидирует среди исследуемых отраслей.

С 2021 года динамика (больше — меньше) процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, в отраслях Энергетика и Нефть и газ противоположная.

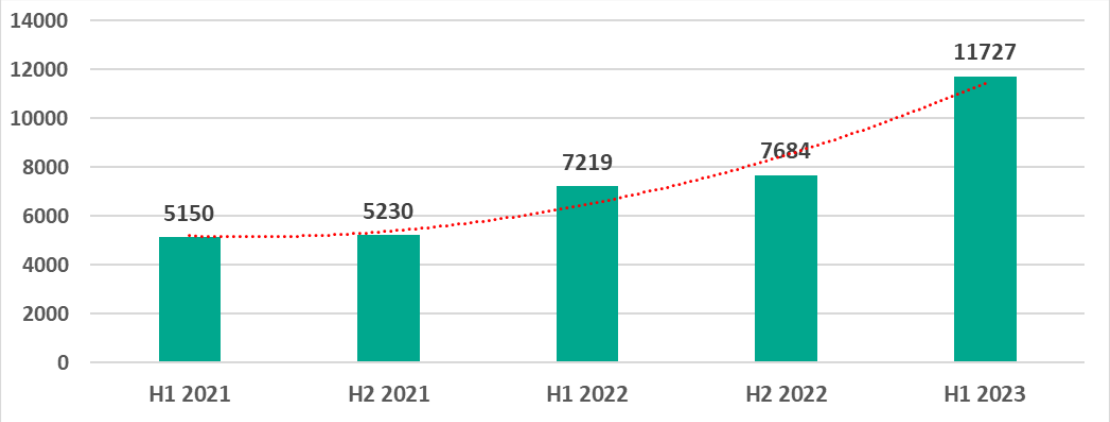
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях



Разнообразие обнаруженного вредоносного ПО

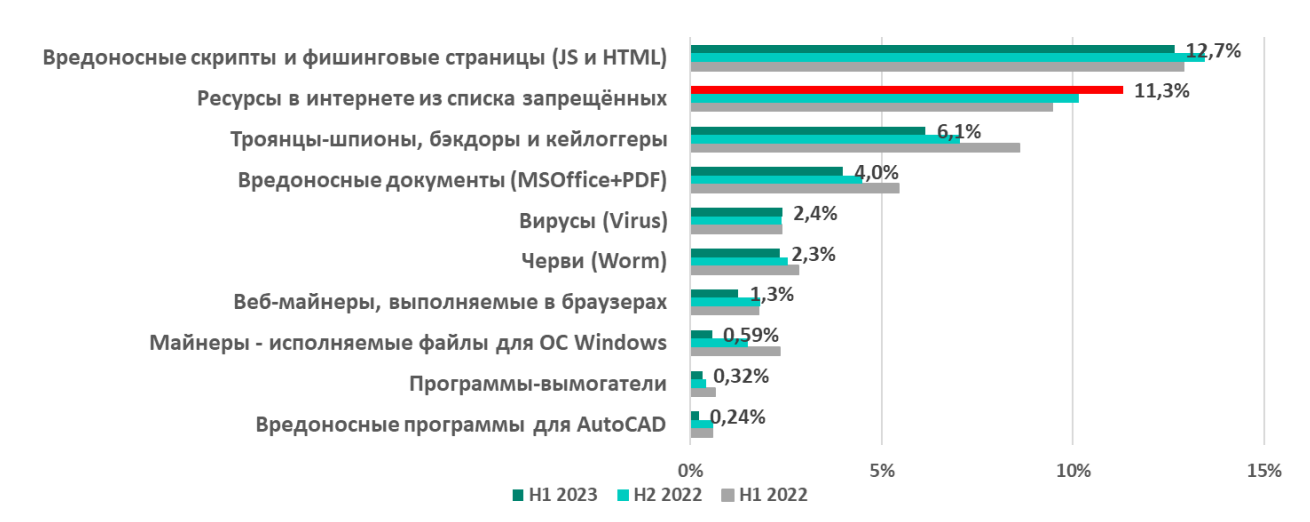
В первом полугодии 2023 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано вредоносное ПО из 11727 различных семейств.

Количество семейств вредоносного ПО, заблокированного на компьютерах АСУ



Категории вредоносных объектов

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Краткое описание каждого типа угроз представлено в отдельном документе.



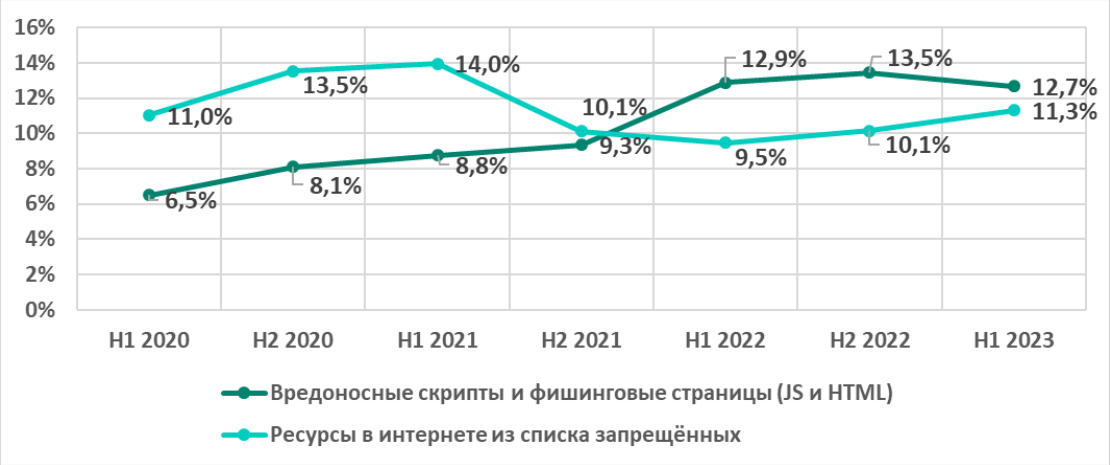
Процент компьютеров АСУ*, на которых была предотвращена активность вредоносных объектов различных категорий

** 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.*

В первом полугодии 2023 года увеличился показатель единственной из всех категорий вредоносных объектов — ресурсы из интернета из списка запрещённых. Процент компьютеров АСУ, на которых были заблокированы угрозы этой категории, растет уже второе полугодие подряд.

До 2022 года ресурсы из интернета из списка запрещённых лидировали в рейтинге категорий угроз. В 2022 году их потеснили вредоносные скрипты и фишинговые страницы, которые до сих пор удерживают первую позицию в рейтинге. Однако показатели по этим двум категориям угроз сближаются.

Процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы и ресурсы в интернете из списка запрещённых



Вредоносные скрипты и фишинговые страницы (JS и HTML)

Вредоносные скрипты и фишинговые страницы (JS и HTML) распространяются как в интернете, так и в письмах, рассылаемых в электронной почте. Для распространения вредоносных скриптов и фишинговых страниц используется значительная часть ресурсов из интернета из списка запрещённых.

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).

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, отмечен на Ближнем Востоке и в России. За полугодие этот показатель вырос в пяти регионах, больше всего прирост в США и Канаде (3,3 п.п.), в Западной Европе (2,2 п.п.) и в Австралии и Новой Зеландии (1,9 п.п.).

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

Среди стран по проценту компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, лидируют Киргизия (21%) и Афганистан (20,9%).

Ресурсы из интернета из списка запрещённых

Среди регионов самый высокий процент компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, отмечен в Африке. Как и следовало ожидать, этот же регион лидирует по проценту компьютеров АСУ, на которых были заблокированы угрозы, источником которых был интернет (см. ниже главу Основные источники угроз).

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

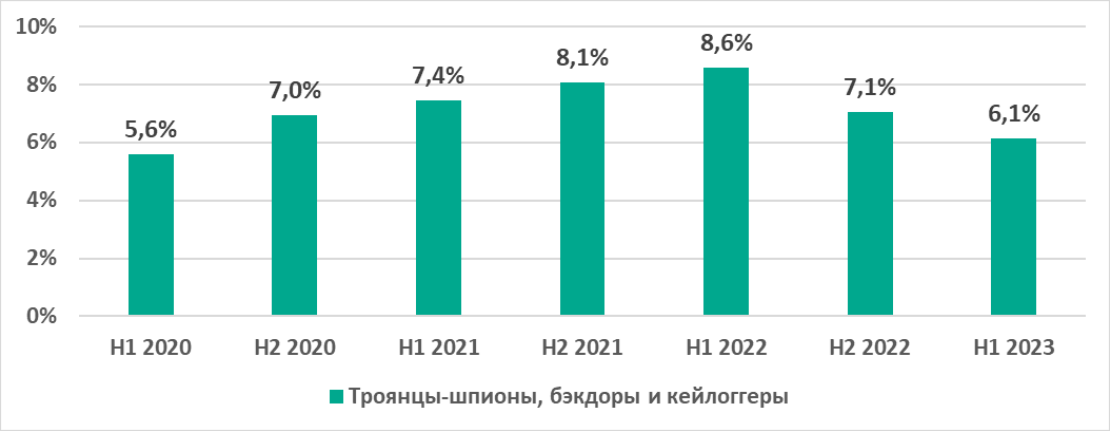
Как уже было сказано выше, ресурсы в интернете из списка запрещённых — единственная категория угроз, по которой в мире вырос процент компьютеров АСУ, на которых эти угрозы были заблокированы. Рост за полугодие отмечен в большинстве регионов. Самый большой — в США и Канаде (3,2 п.п.), Восточной Европе (2,6 п.п.), в Австралии и Новой Зеландии (2,5 п.п.).

Среди стран по проценту компьютеров АСУ, на которых были заблокированы ресурсы из интернета из списка запрещённых, лидируют Алжир (21,8%) и Афганистан (20,2%).

Программы-шпионы

Продолжает уменьшаться процент компьютеров АСУ, на которых блокируются программы-шпионы. Рост этого показателя мы наблюдали с 2020 года до первого полугодия 2022 года включительно.

Процент компьютеров АСУ, на которых были заблокированы программы-шпионы



Максимальный среди всех регионов процент компьютеров АСУ, на которых в первом полугодии 2023 года были заблокированы программы-шпионы, в Африке. Высок также этот показатель на Ближнем Востоке и в Юго-Восточной Азии.

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

Среди стран и территорий по этому показателю лидируют Таджикистан (18,9%), Алжир (16,7%) и Афганистан (16,6%).

Вредоносные документы (MSOffice+PDF)

Вредоносные документы злоумышленники рассылают в фишинговых сообщениях и применяют в атаках, целью которых является первичное заражение компьютеров. В мире процент компьютеров АСУ, на которых были заблокированы угрозы этой категории, вырос более чем вдвое

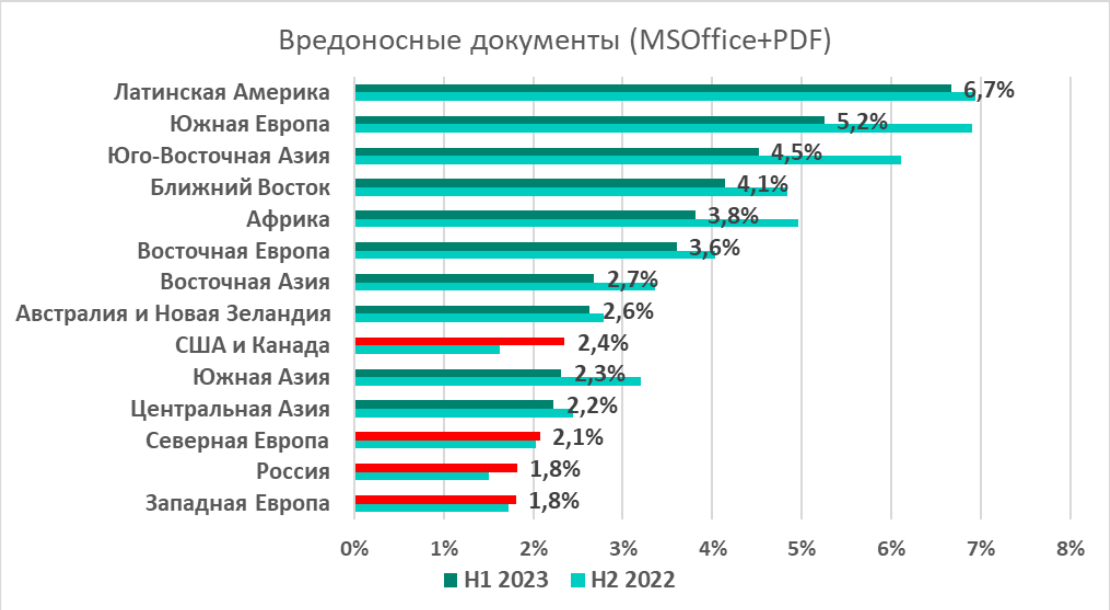
в первом полугодии 2022 года — и с тех пор снижается. Тем не менее, в первом полугодии 2023 года он все еще выше, чем в 2020 — 2021 годах.

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

Среди регионов самый высокий показатель — в Латинской Америке и в Южной Европе. Эти же регионы лидируют по проценту компьютеров АСУ, на которых были заблокированы угрозы из почты.

Больше всего за полугодие процент компьютеров АСУ, на которых были заблокированы вредоносные документы, увеличился в США и Канаде (на 0,72 п.п.).

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



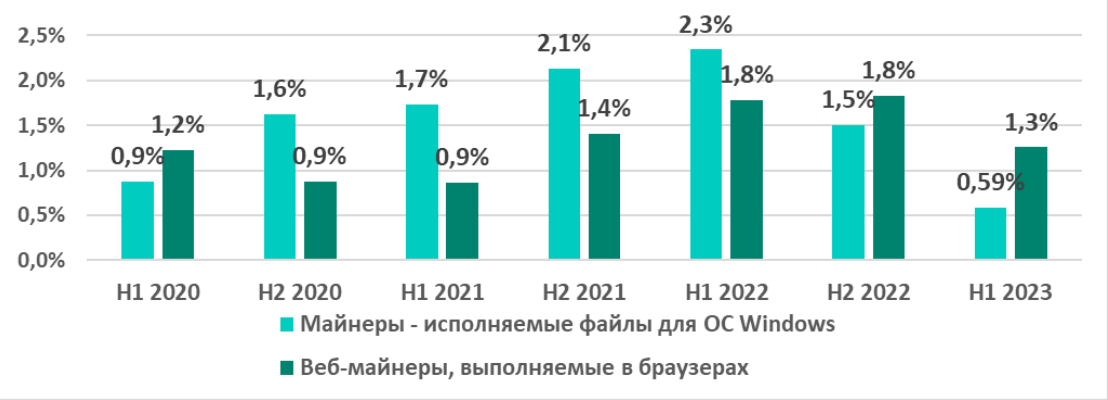
Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные документы, лидируют Алжир (16,7%) и Афганистан (16,6%).

Вредоносные программы для скрытого майнинга криптовалюты

Майнеры часто распространяются на сайтах, на которые пользователей перенаправляют вредоносные скрипты, размещённые злоумышленниками на различных медиаресурсах и сайтах с пиратским контентом.

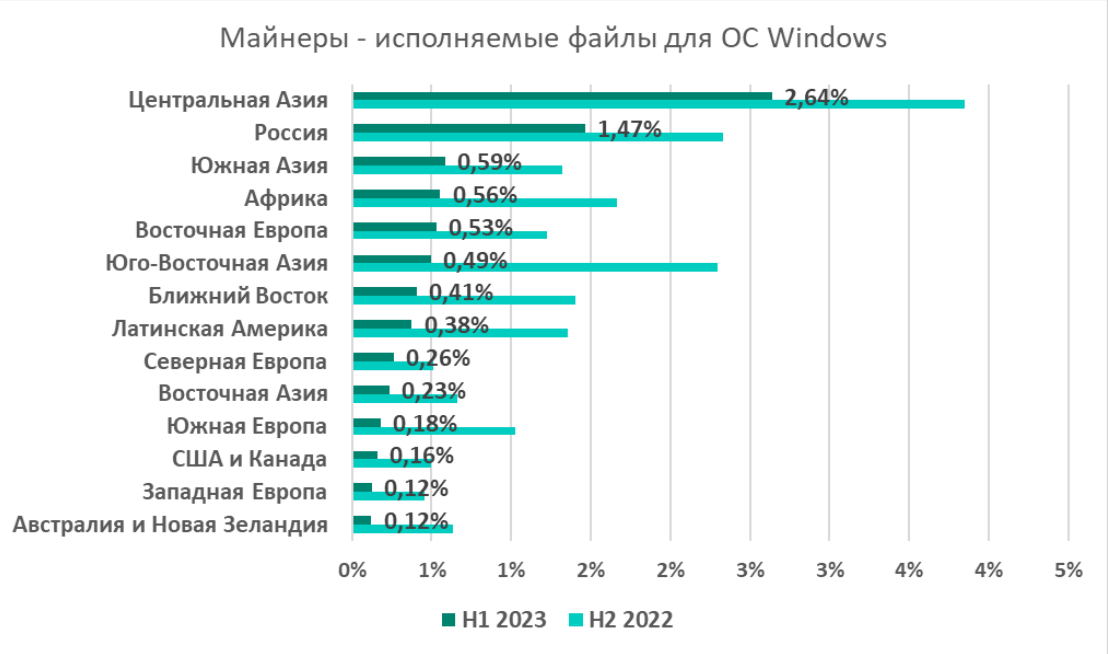
Процент компьютеров АСУ в мире, на которых были заблокированы вредоносные майнеры — как исполняемые файлы для ОС Windows, так и веб-майнеры, — в первом полугодии 2023 года уменьшился.

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



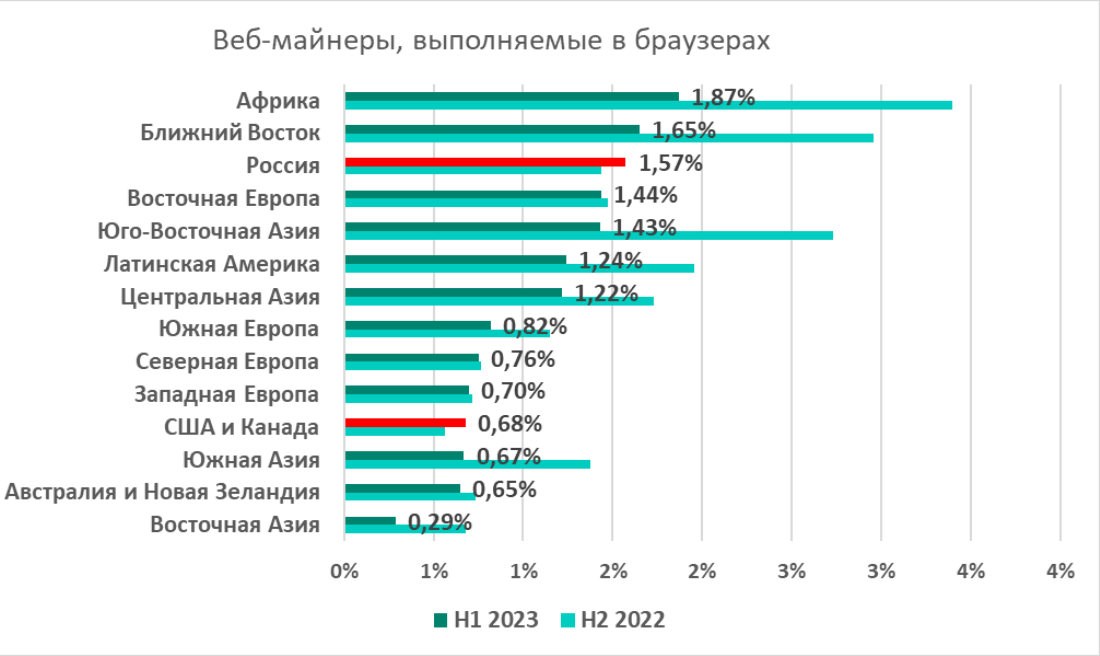
По проценту компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, среди регионов в первом полугодии 2023 года лидирует Центральная Азия. Среди стран и территорий — Таджикистан (7,9%) и Туркменистан (7,4%).

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



По проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, среди регионов лидирует Африка. За полугодие увеличился процент в России и в США и Канаде — на 0,13 и 0,12 п.п. соответственно.

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



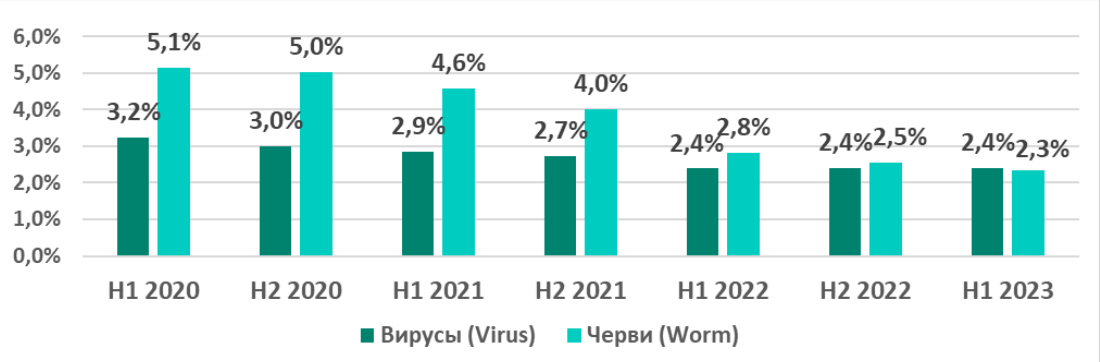
Среди стран и территорий по проценту компьютеров АСУ, на которых были заблокированы веб-майнеры, на первом месте Сербия (6,4%).

Вирусы и черви

В мире продолжает уменьшаться процент компьютеров АСУ, на которых были заблокированы черви. Мы полагаем, что это косвенно свидетельствует о планомерной работе по развёртыванию защитных решений в OT-инфраструктурах, что устраняет очаги заражения и препятствует распространению самораспространяющегося вредоносного ПО.

Процент компьютеров АСУ, на которых были заблокированы вирусы, за полугодие не изменился.

Процент компьютеров АСУ, на которых были заблокированы вирусы и черви



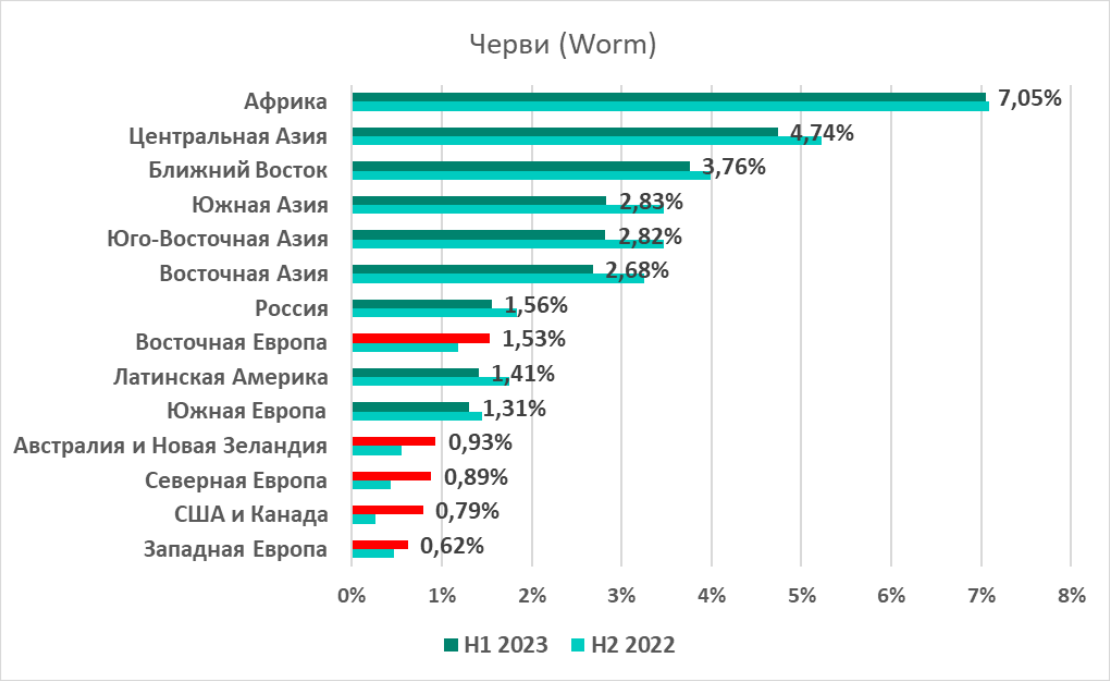
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

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.

Процент компьютеров АСУ, на которых детектируются черви, по-прежнему весьма высок в Африке, которая, как следствие, лидирует среди регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей. За полугодие больше всего показатель по червям увеличился в США и Канаде (на 0,53 п.п.) и в Северной Европе (на 0,45 п.п.).

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

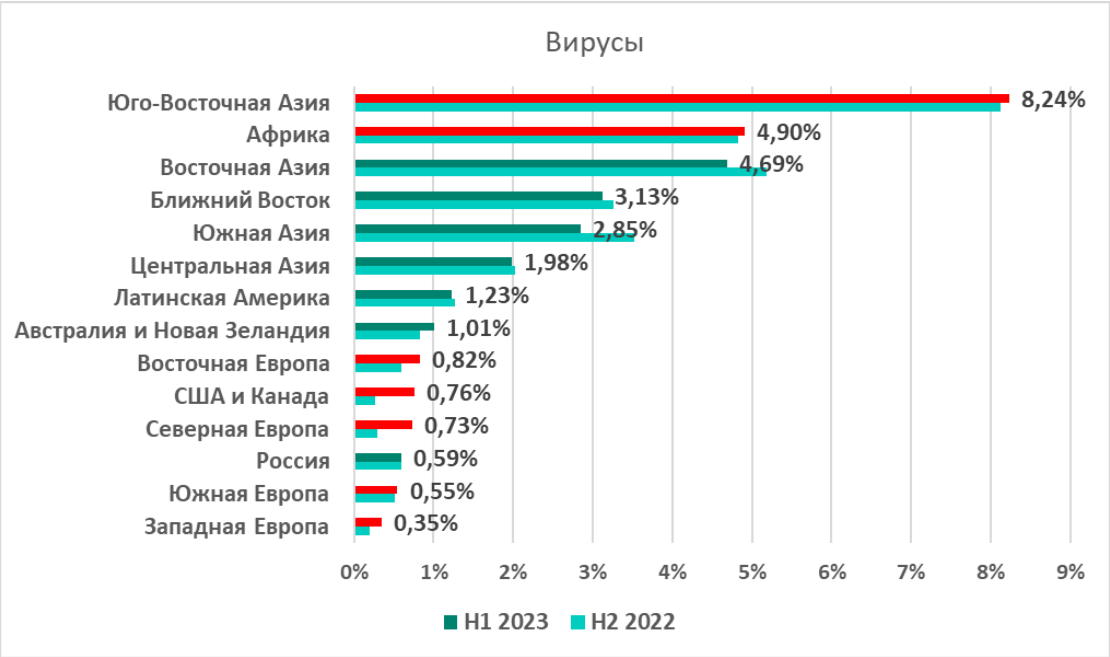


В лидирующей по этому показателю стране — Мали — процент компьютеров АСУ, на которых детектируются черви, достигает 20,8%. Отметим также, что

в пятерку стран-лидеров по этому показателю помимо африканских стран попала Туркмения с 18%.

Вирусы остаются актуальной проблемой для Юго-Восточной Азии. Процент компьютеров АСУ, на которых были заблокированы вирусы, вырос во многих регионах, больше всего — в США Канаде (на 0,49 п.п.) и в Северной Европе (на 0,44 п.п.).

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

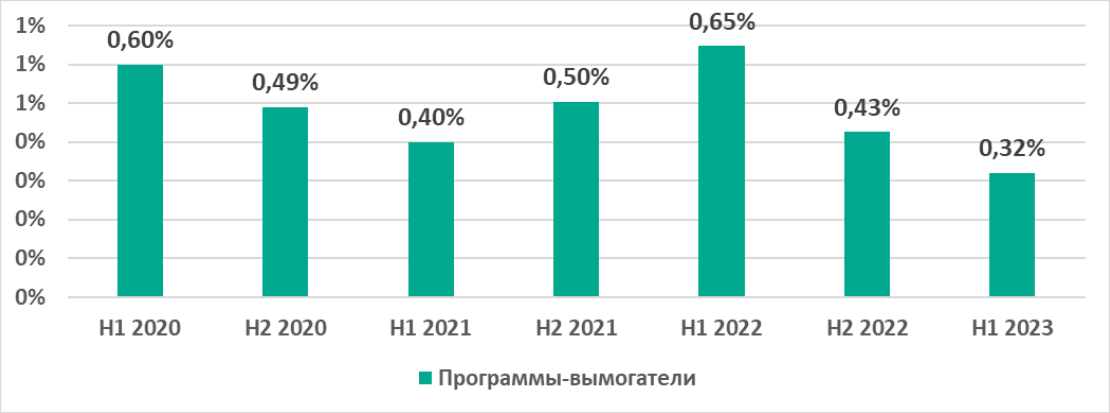


Среди стран и территорий самый высокий процент компьютеров АСУ, на которых блокируются вирусы, в Афганистане (16,6%), во Вьетнаме (14,1%) и в Йемене (13,8%).

Программы-вымогатели

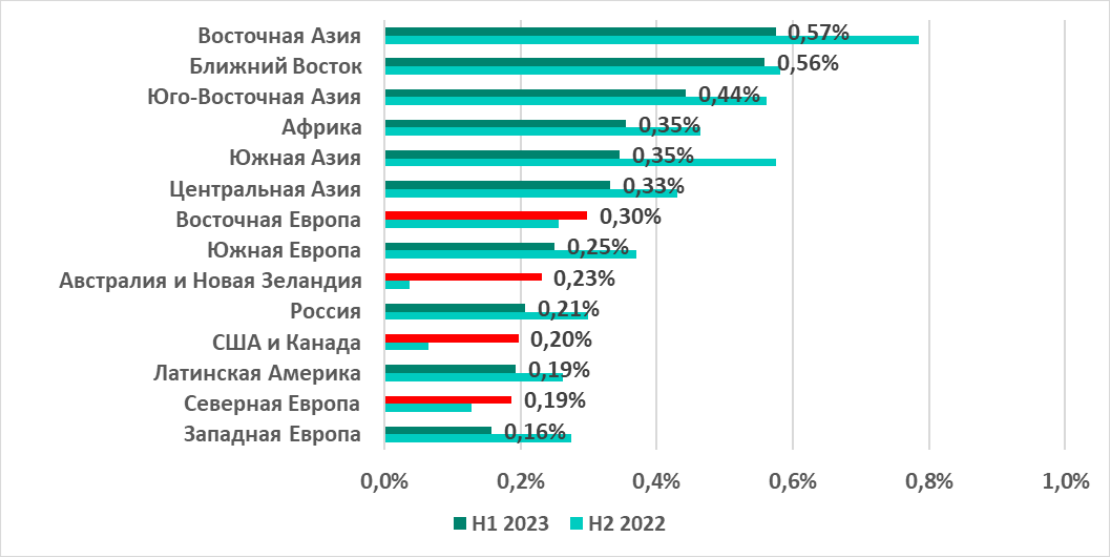
После увеличения в первом полугодии 2022 года процента компьютеров АСУ, на которых были заблокированы программы-вымогатели, снижается и в первом полугодии 2023 достиг минимума с 2020 года.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



Среди регионов в первом полугодии 2023 года по проценту атакованных вымогателями компьютеров АСУ лидируют Восточная Азия и Ближний Восток.

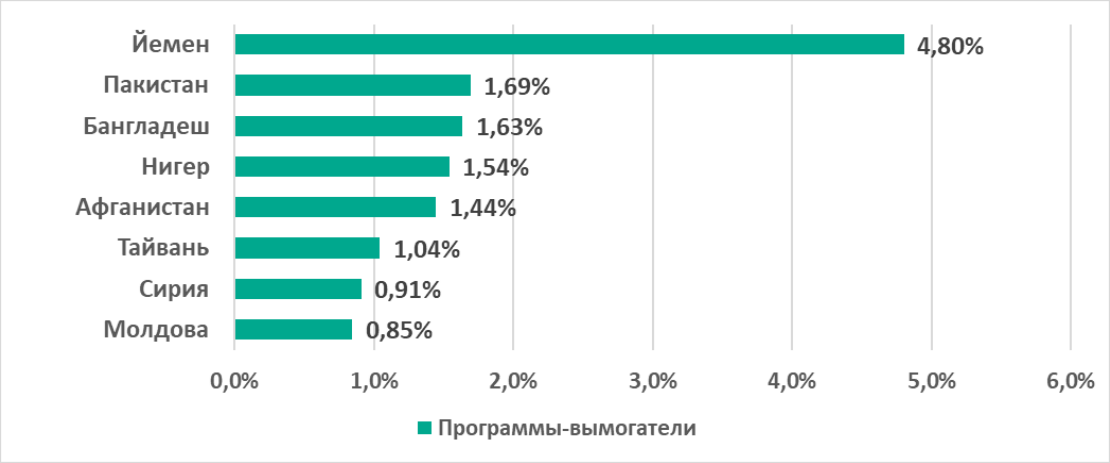
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, первое полугодие 2023



В большинстве регионов мира процент компьютеров АСУ, атакованных программами-вымогателями, уменьшился. Однако он вырос в Австралии и Новой Зеландии, в США и Канаде — на 0,19 п.п. и 0,13 п.п. соответственно — и немножко подрос в Северной и Восточной Европе.

Среди стран и территорий в первом полугодии 2023 года по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, с большим отрывом лидирует Йемен.

10 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы программы-вымогатели, первое полугодие 2023



Отметим, что по итогам полугодия в десятку неожиданно вошла одна европейская страна — Молдова.

Вредоносные программы для AutoCAD

По проценту компьютеров АСУ, на которых заблокировано вредоносное ПО для AutoCAD, в частности вирусы, лидирует Восточная Азия (3,1%). 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 (2,6%) и Вьетнам (1,5%).

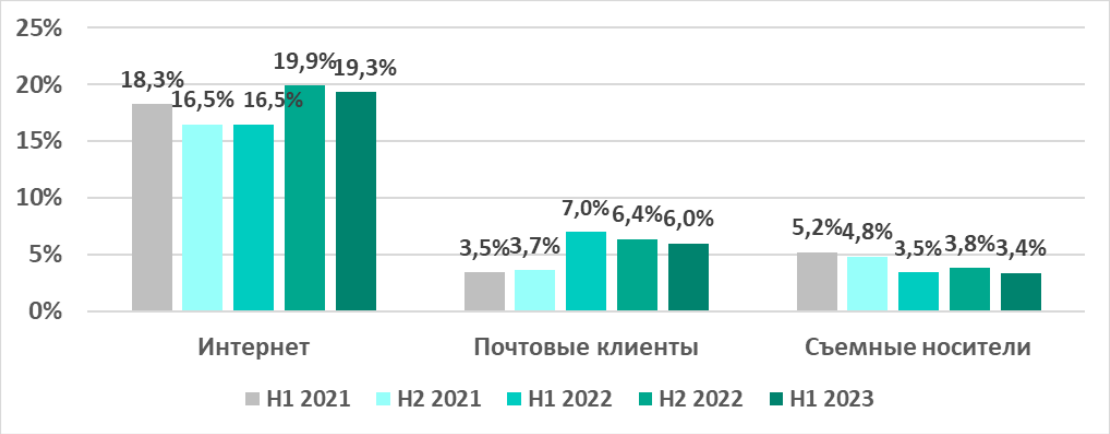
Основные источники угроз

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.

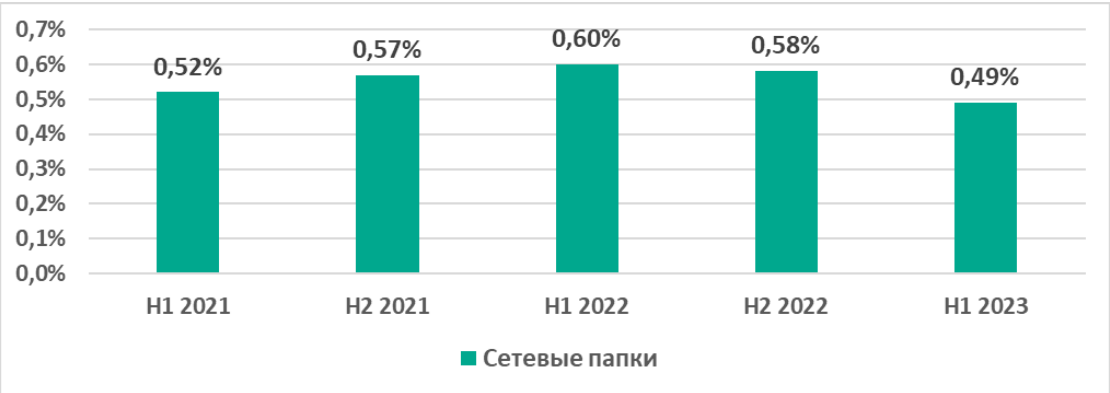
Мир

В первом 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



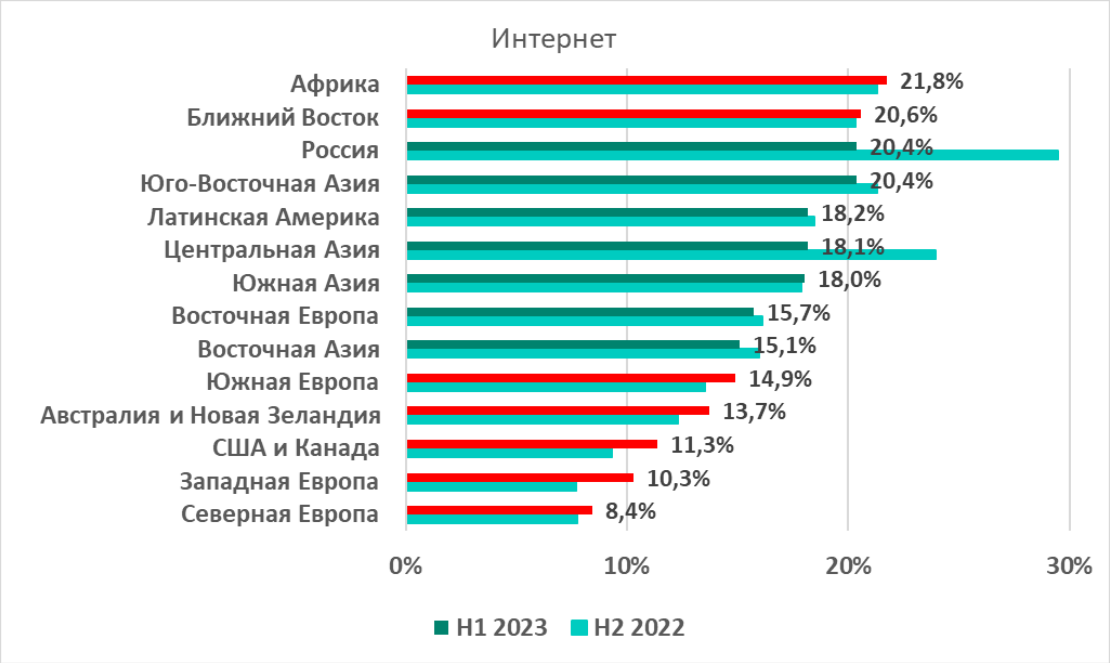
Как и в случае с общей статистикой по всем угрозам, процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, отличается в разных регионах и странах.

Регионы и страны

Интернет

В первом полугодии 2023 года среди регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, лидируют Африка, Ближний Восток и Россия.

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

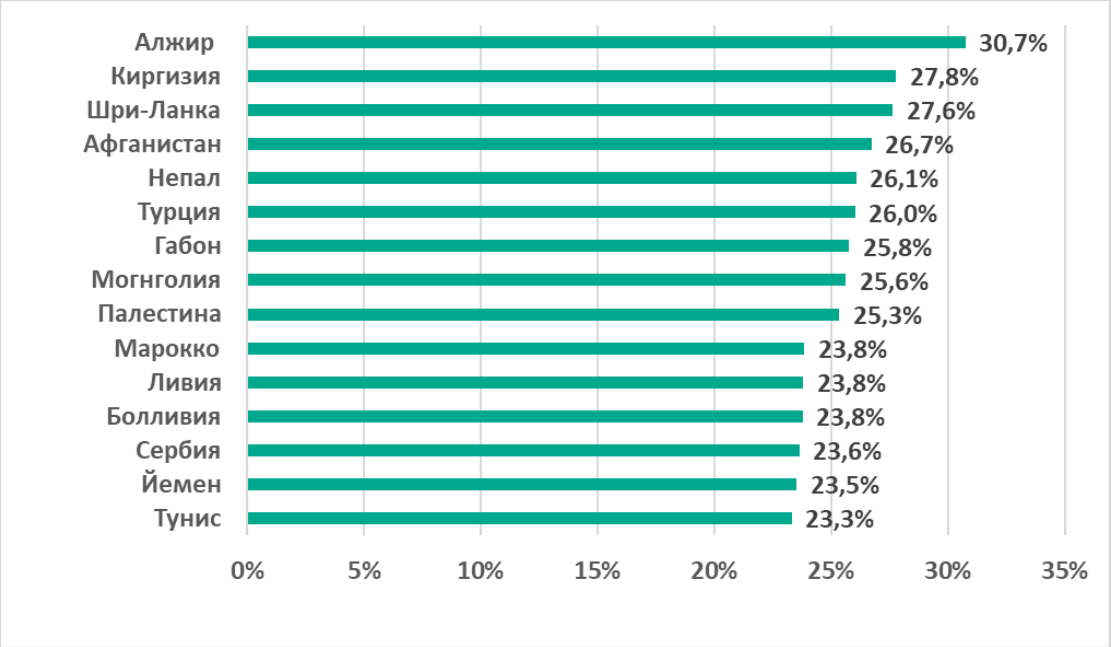


Наибольший рост процента компьютеров АСУ, на которых были заблокированы угрозы из интернета, в первом полугодии 2023 года отмечен в самых благополучных по этому критерию регионах — в Западной Европе (+2,6 п.п.), в США и Канаде (+2 п.п.) и в Австралии и Новой Зеландии (+1,4 п.п.).

Заметно снизились показатели России и Центральной Азии. В предыдущем полугодии в этих регионах процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, резко вырос. Этот рост был обусловлен массовым заражением сайтов, в том числе промышленных организаций, использующих устаревшую версию одной из популярных CMS.

В топе 15 стран и территорий по этому показателю по-прежнему одна европейская страна — Сербия.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы угрозы из интернета, первое полугодие 2023

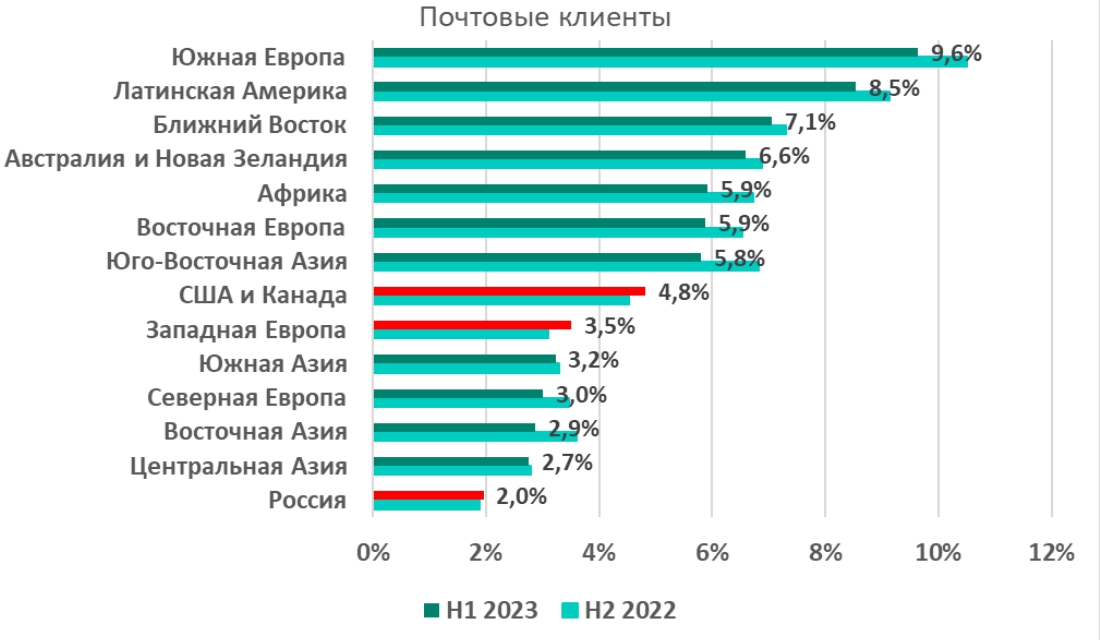


Почтовые клиенты

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.

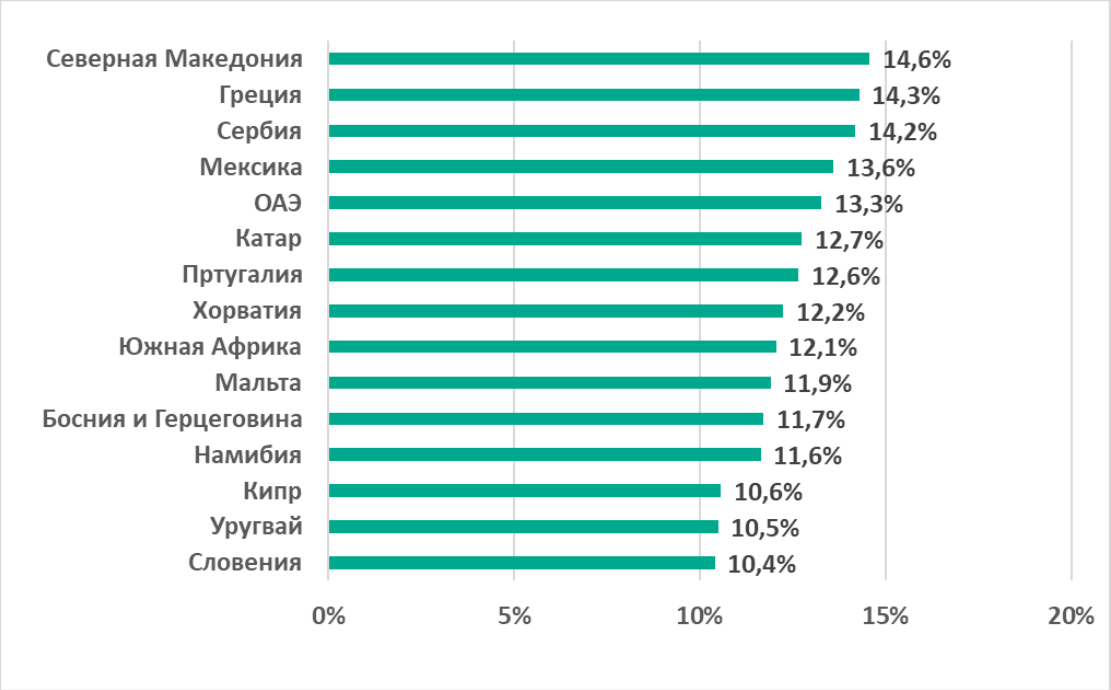
В первом полугодии 2023 года процент компьютеров АСУ, на которых блокировались угрозы из почты, вырос в регионах США и Канада (+0,3 п.п.), Западная Европа (+0,4 п.п.) и Россия (+0,1 п.п.).

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



В списке 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, преобладают страны из Южной и Восточной Европы.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки, первое полугодие 2023

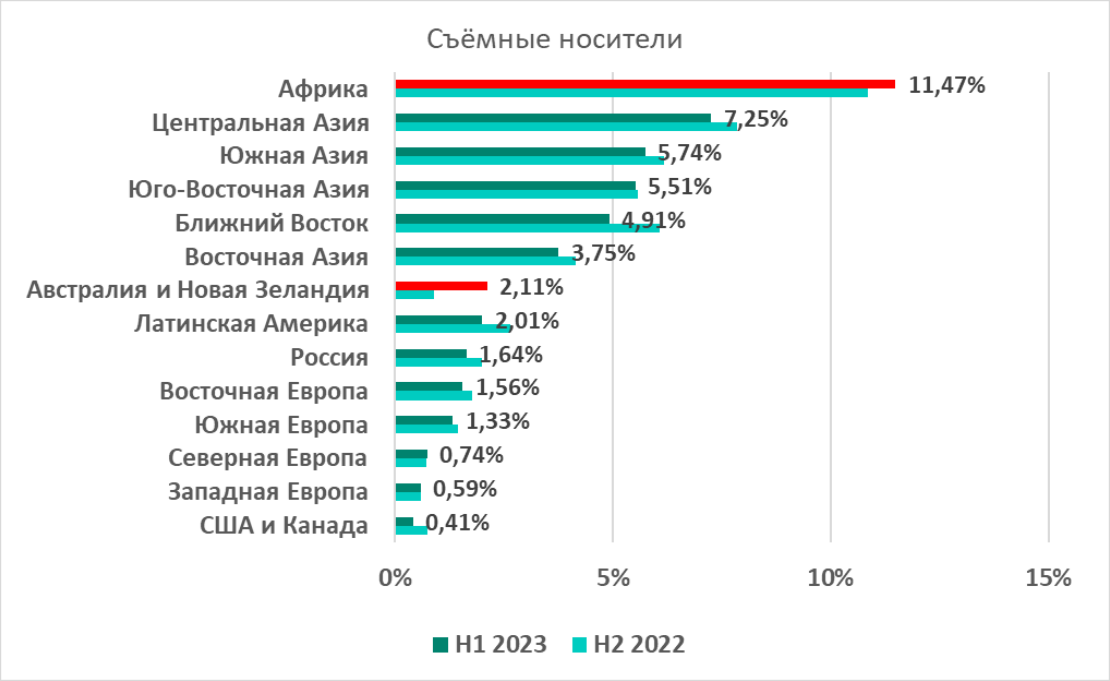


Мы рекомендуем специалистам по безопасности в этих странах обратить особое внимание на защиту сотрудников предприятий от фишинговых рассылок.

Съёмные носители

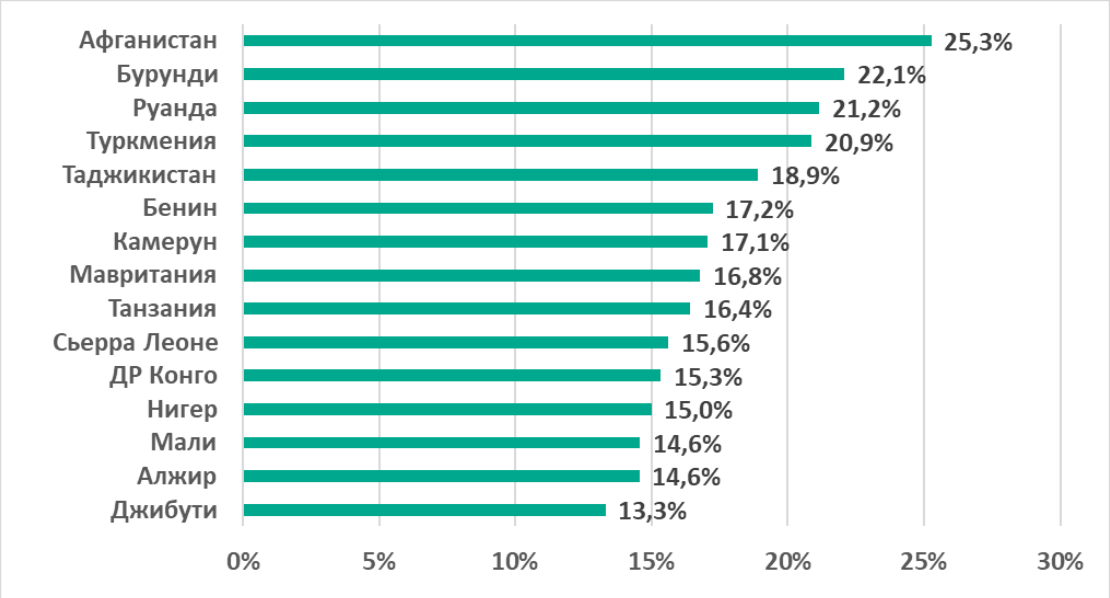
Рейтинг регионов по проценту компьютеров АСУ, на которых при подключении съемных носителей было заблокировано вредоносное ПО, традиционно возглавляет Африка и регионы Азии. В первом полугодии 2023 года этот показатель немного увеличился в Африке (+0,63 п.п.) и более чем вдвое — в Австралии и Новой Зеландии (+1,2 п.п.).

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



Среди 15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, преобладают страны Африки.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, первое 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, Юго-Восточной и Центральной Азии. В Австралии и Новой Зеландии за полугодие показатель увеличился вдвое, и регион оказался на четвертом месте в этом рейтинге.

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

Среди стран и территорий, как и в прошлом полугодии, лидирует Туркмения.

15 стран и территорий с наибольшим процентом компьютеров АСУ, на которых вредоносные объекты были заблокированы в сетевых папках, первое 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[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 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.

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.

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

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