Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Второй квартал 2024

26.09.2024

Version 1.0

Цифры квартала

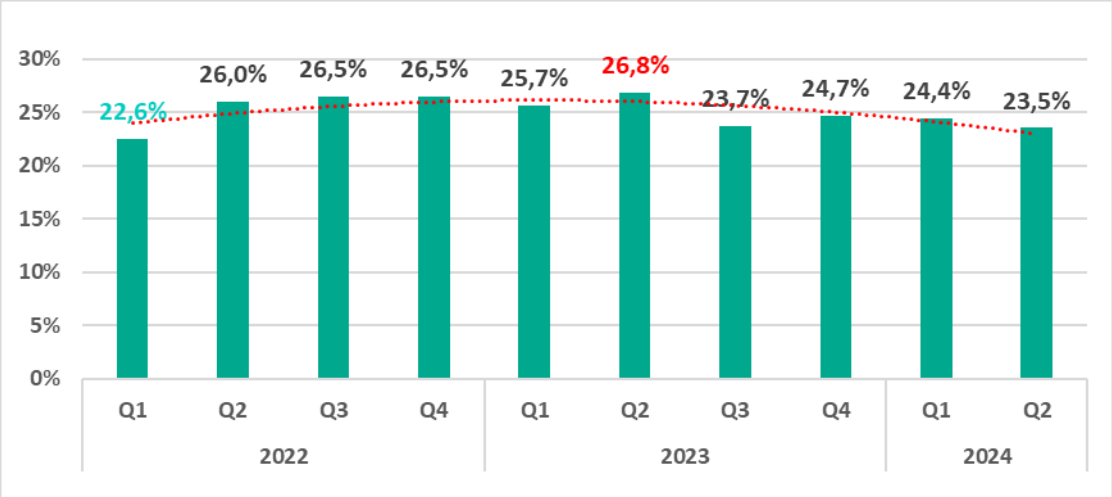
Показатель	Q1 2024	Q2 2024	Изменения за квартал
Процент атакованных компьютеров АСУ в мире	24,4%	23,5%	-0,9 п.п.
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Ресурсы в интернете из списка запрещённых	6,84%	6,63%	-0,21 п.п.
Вредоносные скрипты и фишинговые страницы (JS и HTML)	5,84%	5,69%	-0,15 п.п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,90%	4,08%	0,18 п.п.
Вредоносные документы (MSOffice+PDF)	1,72%	1,96%	0,24 п.п.
Вирусы (Virus)	1,56%	1,54%	-0,02 п.п.
Черви (Worm)	1,51%	1,48%	-0,03 п.п.
Майнеры — исполняемые файлы для ОС Windows	0,92%	0,89%	-0,03 п.п.
Веб-майнеры, выполняемые в браузерах	0,49%	0,50%	0,01 п.п.
Вредоносные программы для AutoCAD	0,41%	0,42%	0,01 п.п.
Программы-вымогатели	0,15%	0,18%	0,03 п.п.
Основные источники угроз			
Интернет	12,24%	11,25%	-0,99 п.п.
Почтовые клиенты	3,04%	3,04%	0 п.п.
Съемные носители	1,13%	0,92%	-0,21 п.п.
Сетевые папки	0,15%	0,13%	-0,02 п.п.

Статистика по всем угрозам

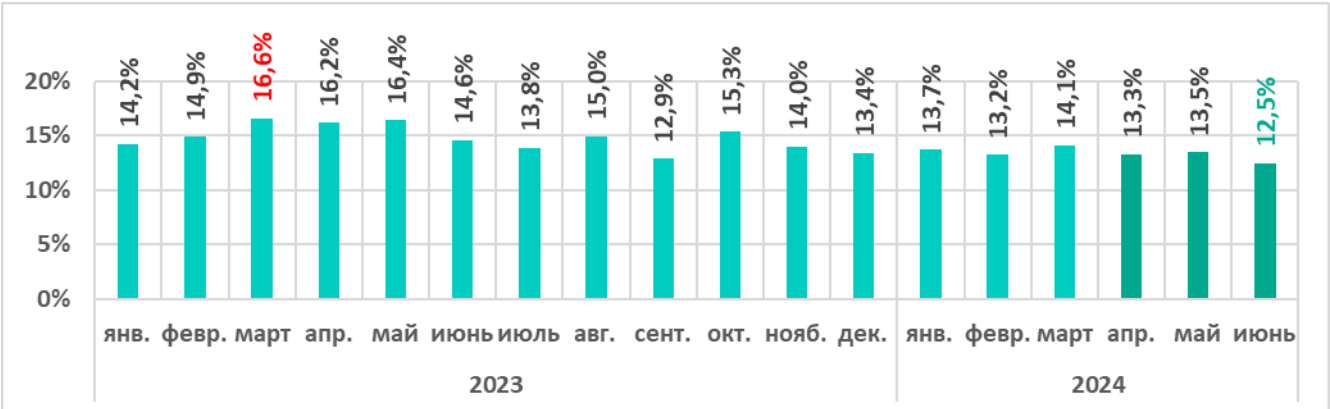
Во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с предыдущим кварталом на 0,9 п.п. и составил 23,5%.

По сравнению со вторым кварталом 2023 года процент уменьшился на 3,3 п.п.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по кварталам 2022–2024 годов



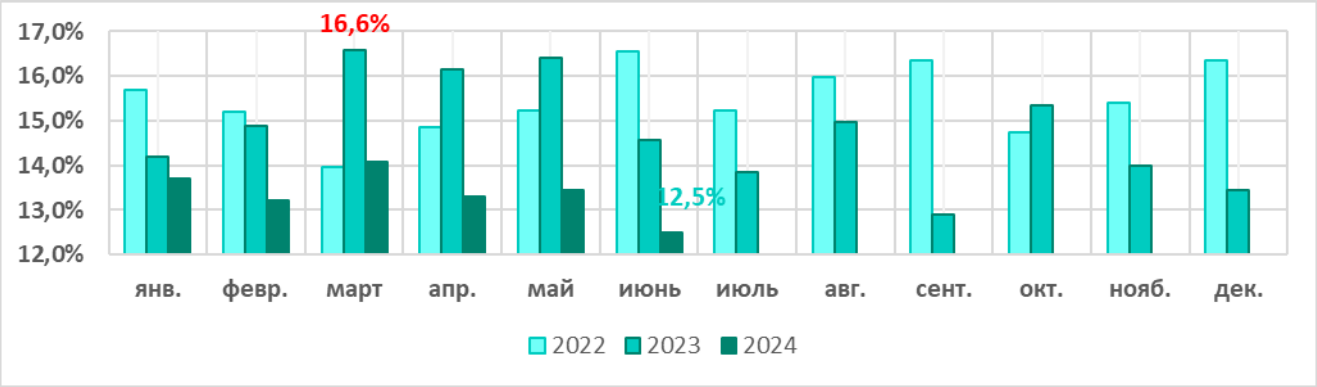
В течение второго квартала 2024 года самым высоким процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был в мае, самым низким — в июне.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 — июнь 2024

Проценты за три месяца второго квартала 2024 года заметно меньше, чем в те же месяцы предыдущего (2023) года.

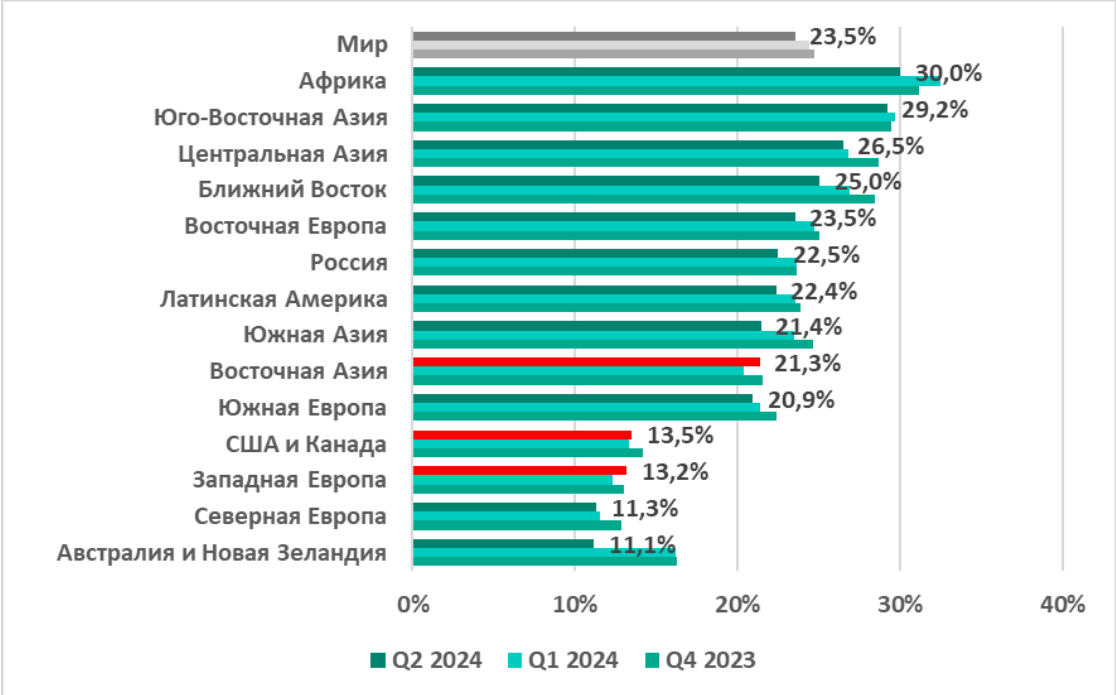
Более того, в июне 2024 года этот показатель был самым низким за период с 2022 года до конца первой половины 2024 года.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2022–2024 годов

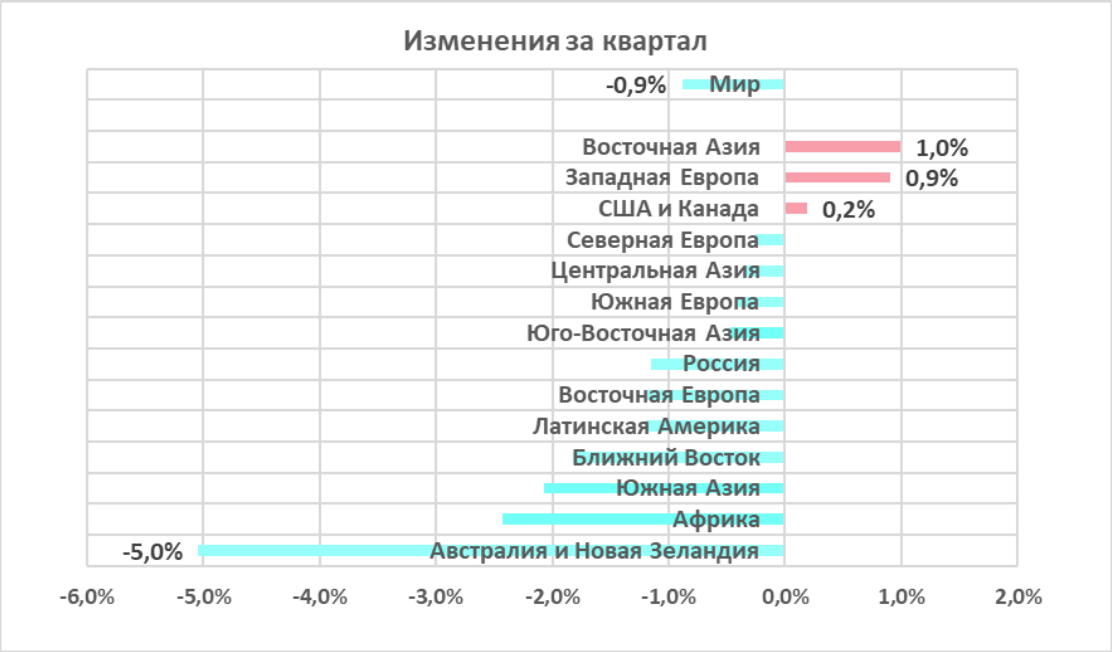
В регионах процент компьютеров АСУ, на которых в течение квартала были заблокированы вредоносные объекты, варьировался от 11,3% в Северной Европе до 30% в Африке.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты во втором квартале 2024 года



В четырех регионах — Восточной Азии, Австралии и Новой Зеландии, США и Канаде, а также Западной Европе — показатели увеличились по сравнению с предыдущим кварталом.

Регионы и мир. Изменение процента атакованных компьютеров за второй квартал 2024 года

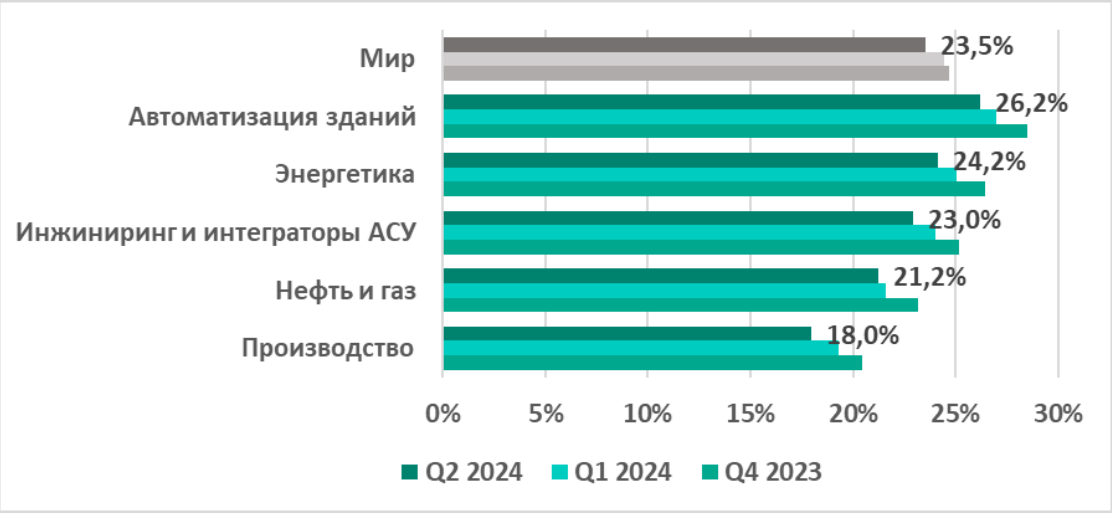


Подробнее о региональной статистике мы рассказываем в отчете по регионам.

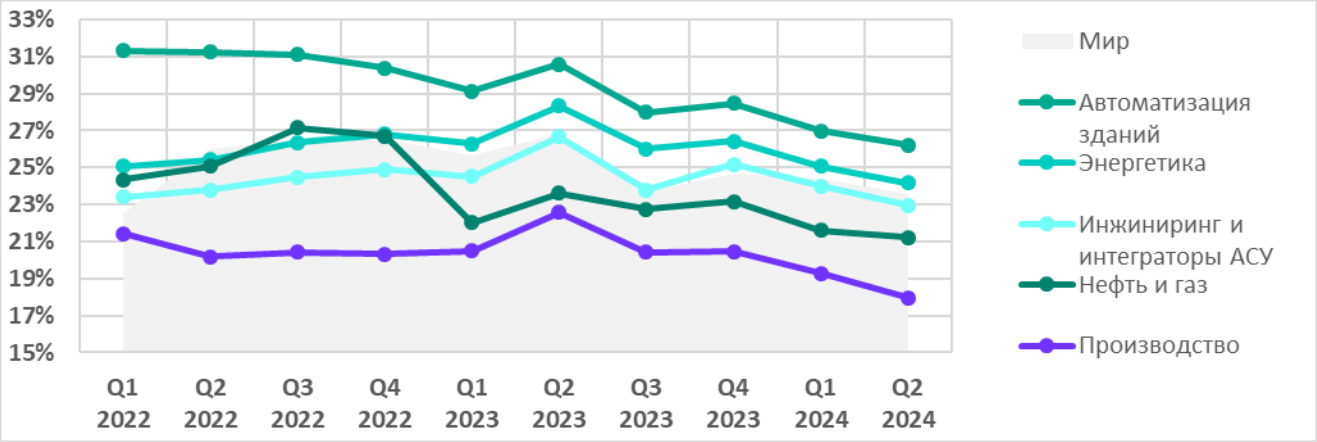
Некоторые отрасли

Автоматизация зданий традиционно 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



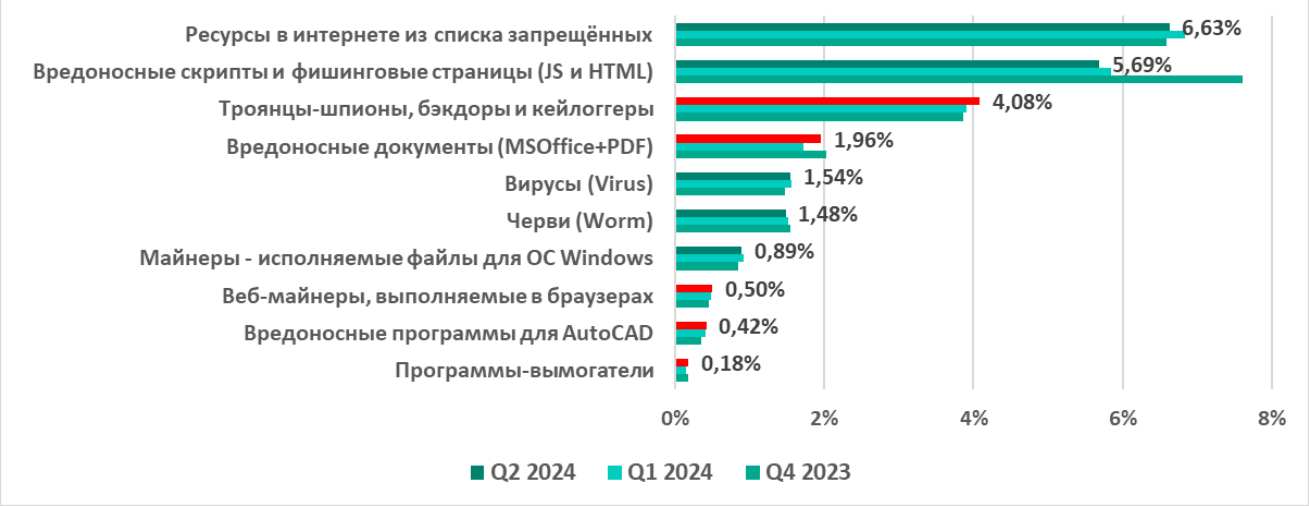
Во втором квартале 2024 года во всех отраслях процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился.



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

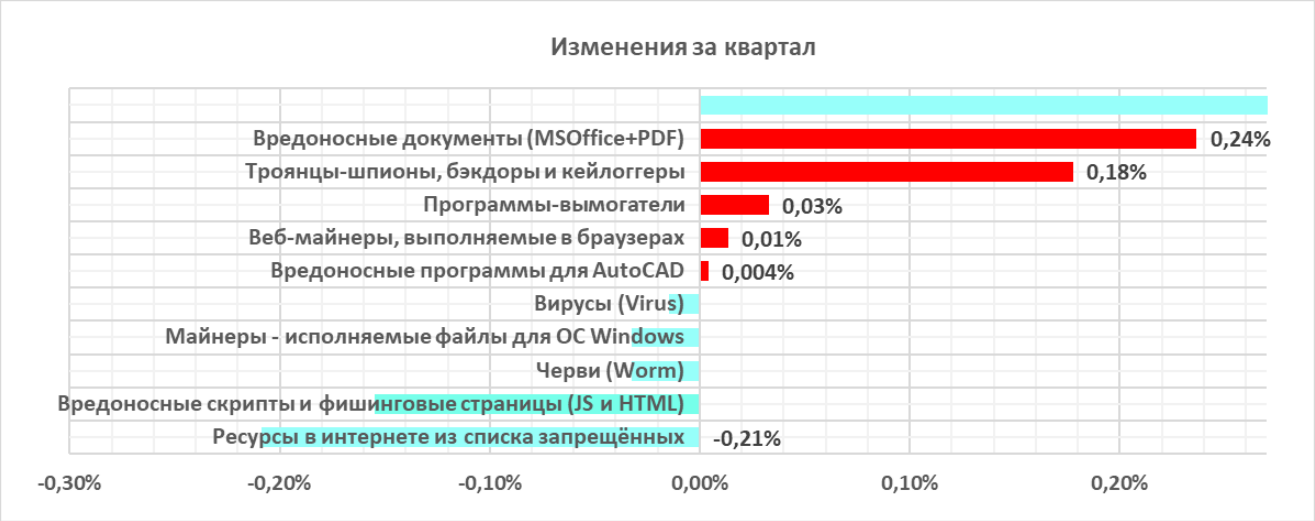
Разнообразие обнаруженного вредоносного ПО

Во втором квартале 2024 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано вредоносное ПО из 11 349 семейств, относящихся к различным категориям.



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

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



Изменение за второй квартал 2024 года процента компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий

Во втором квартале 2024 года по сравнению с предыдущим кварталом наиболее заметно вырос процент компьютеров АСУ, на которых были заблокированы вредоносные **программы-вымогатели** — в 1,2 раза.

Категории вредоносных объектов

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

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

Вредоносные объекты, используемые для первичного заражения

Вредоносные объекты, которые используются для первичного заражения компьютеров, — опасные веб-ресурсы, вредоносные скрипты и вредоносные документы.

Ресурсы в интернете 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).

Вредоносные скрипты и фишинговые страницы (JS и HTML)

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

Во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, продолжил снижаться и оказался минимальным с 2022 года.

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.

Процент компьютеров АСУ, на которых были обнаружены вредоносные документы, был максимальным во втором квартале 2022 года и с тех пор по большей части снижался — рост наблюдался только во втором квартале 2024 года.

Вредоносное ПО следующего этапа

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

Шпионское ПО применяется и для кражи информации, необходимой для доставки других вредоносных программ, таких как программы-

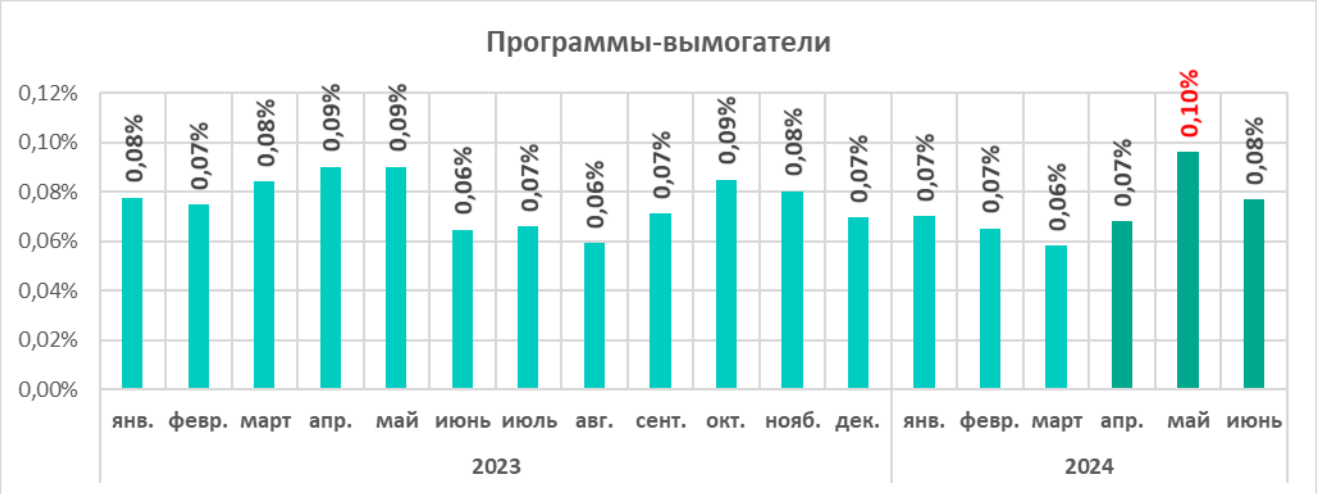
вымогатели и вредоносные программы для скрытого майнинга криптовалюты, а также для подготовки целенаправленных атак.

Процент компьютеров АСУ, на которых были заблокированы программы-шпионы, был минимальным в третьем квартале 2023 года и немного подрос за последние три квартала.

Программы-вымогатели

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, колеблется от квартала к кварталу в пределах 0,3 п.п.

Как видно на графике ниже, показатель программ-вымогателей значительно колебался в течение месяцев второго квартала и в мае 2024 года достиг своего наибольшего значения с начала 2023 года.



Майнеры — исполняемые файлы для ОС Windows

Процент компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, был минимальным в первом квартале 2023 года.

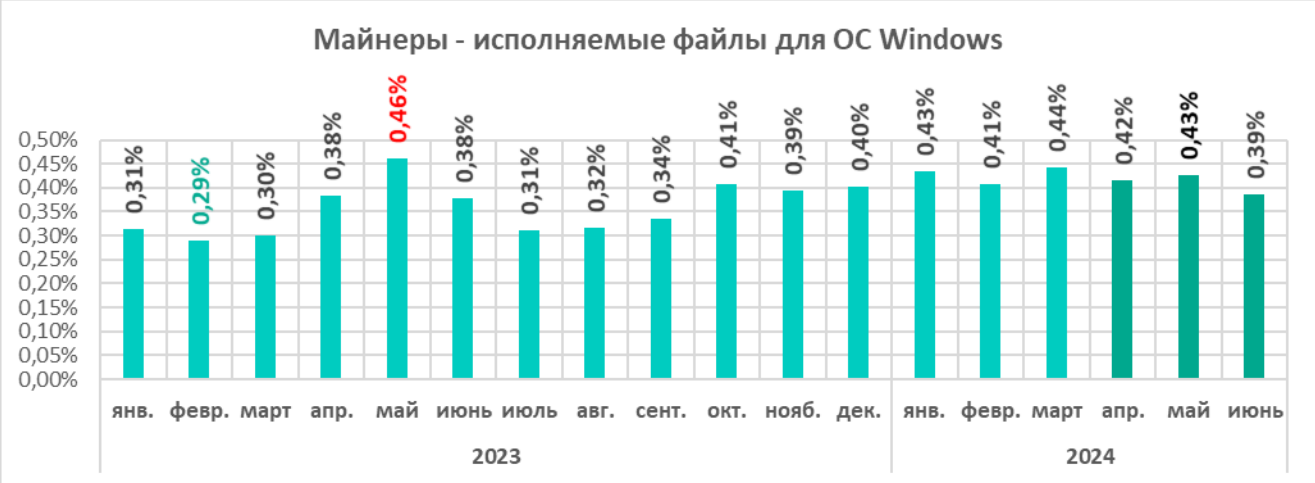
Наряду с «классическими» майнерами — приложениями, написанными на .Net, C++ или Python и предназначенными для скрытого майнинга криптовалют — появляются новые формы. Популярные методы бесфайлового выполнения вредоносного кода продолжают использоваться злоумышленниками, включая и тех, кто внедряет майнеры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

Во втором квартале 2024 года значительная часть майнеров для Windows, обнаруженных на компьютерах АСУ, представляла собой архивы, чьи названия имитировали легальное программное обеспечение. Эти архивы не содержат реального программного обеспечения, но включают в себя файл формата Windows LNK, более известный как ярлык. Однако целевой объект (или путь), на который указывает LNK-файл, не является обычным приложением, а представляет собой команду, которая может выполнить вредоносный код, например, скрипт PowerShell. Злоумышленники все чаще выбирают PowerShell, с помощью которого код вредоносного ПО (в том числе майнеров), помещенный в аргументы командной строки, выполняется исключительно в памяти, то есть бесфайловым способом.

Другой популярный метод внедрения майнеров, обнаруживаемых на компьютерах АСУ, заключается в использовании таких майнеров

криптовалют как XMRig, NBMiner, OneZeroMiner и т. д. Подобные майнеры, не являясь вредоносным ПО, детектируются защитными решениями как RiskTools. Злоумышленники используют их в сочетании со специфическими конфигурационными файлами, позволяющими визуально скрывать выполнение майнера от пользователя.

Процент компьютеров АСУ, на которых были заблокированы майнеры — исполняемые файлы для ОС Windows, с октября 2023 года выше показателей всех предыдущих месяцев 2023 года, за исключением мая 2023 года.



Веб-майнеры

Процент компьютеров АСУ, на которых были заблокированы веб-майнеры, продолжил немного расти во втором квартале 2024 года.

Самораспространяющееся вредоносное ПО. Черви и вирусы

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

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

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

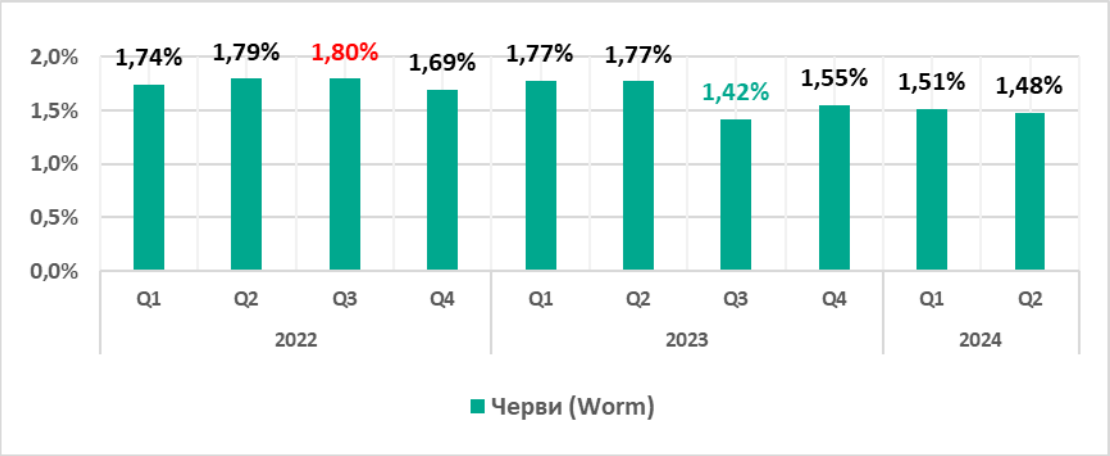
В мире процент компьютеров АСУ, на которых были заблокированы вирусы и черви, потихоньку растет после минимума в третьем квартале 2023 года.

Черви

В сетях АСУ встречаются 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,

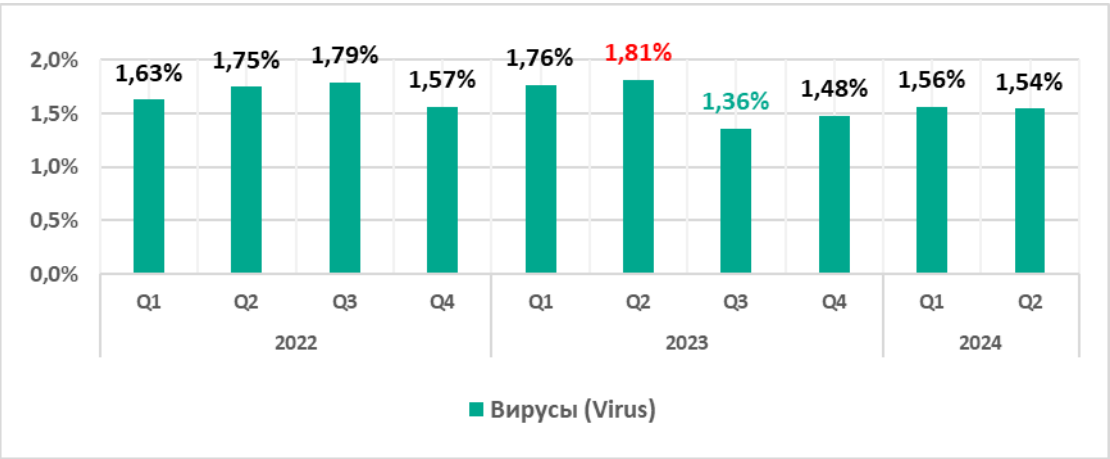
но еще актуальных в технологических сетях уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

Во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы черви, продолжал снижаться.



Вирусы

Во втором квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вирусы, немного снизился.

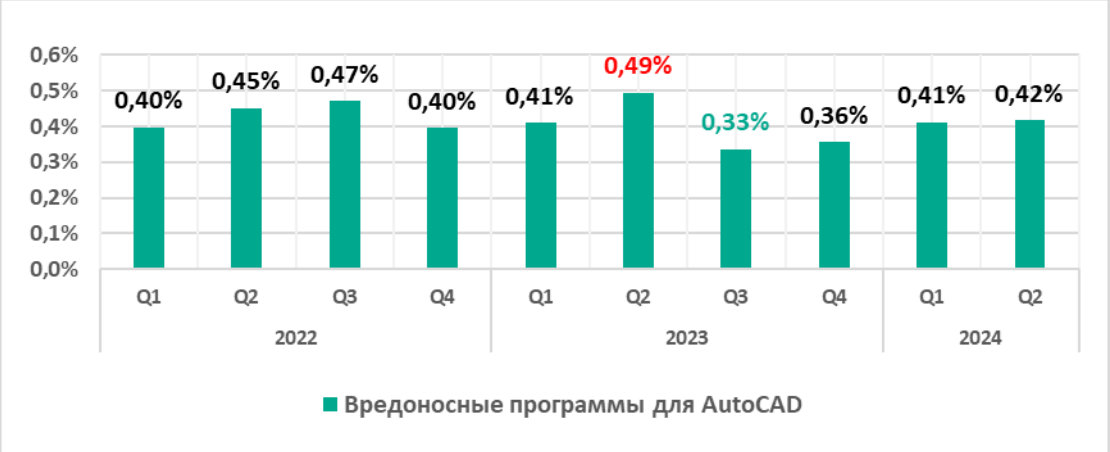


Вредоносные программы для AutoCAD

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

Как правило, это минорная угроза, которая в рейтинге категорий вредоносных объектов по проценту компьютеров АСУ, на которых она была заблокирована, занимает последние места.

Во втором квартале 2024 года процент компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, незначительно вырос.



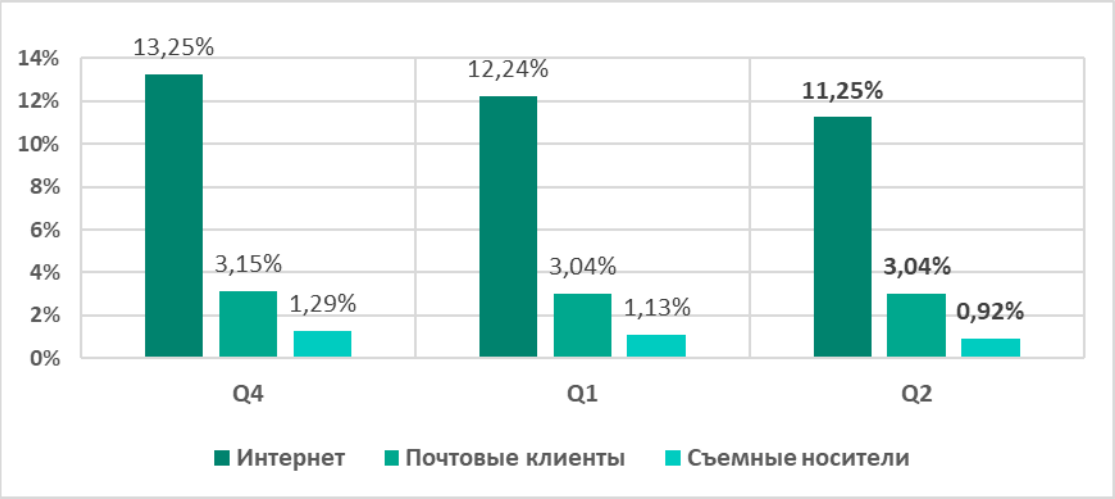
Основные источники угроз

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

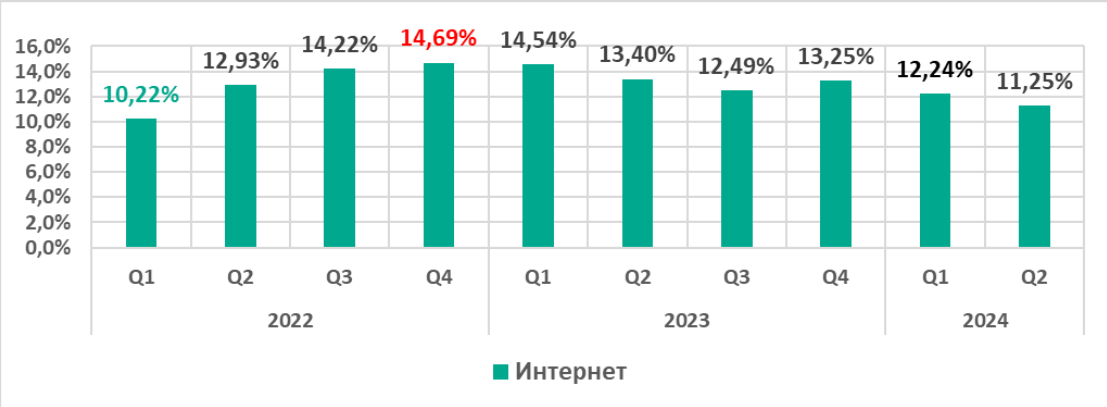
Во втором квартале 2024 года снизился процент компьютеров АСУ, на которых были заблокированы угрозы из интернета и угрозы, распространяемые на съемных носителях.

Для угроз из почты и угроз, распространяемых на съемных носителях, показатель за второй квартал 2024 года, как и за первый, был минимальным с 2022 года. Для интернета процент был меньше только два года назад — в первом квартале 2022 года.

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



Интернет



Почтовые клиенты

Съемные носители

Сетевые папки

Сетевые папки — минорный источник угроз. Процент компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, также был наименьшим с 2022 года.

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].

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

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 систем автоматизации зданий
- серверы хранения данных (Historian)
- шлюзы данных (OPC)
- стационарные рабочие станции инженеров и операторов
- мобильные рабочие станции инженеров и операторов
- человеко-машинный интерфейс (HMI)
- компьютеры, используемые для администрирования технологических сетей и сетей систем автоматизации зданий
- компьютеры, используемые для программирования АСУ/ПЛК

Компьютеры, участвующие в статистике, принадлежат организациям из различных отраслей. Наиболее распространены химическая промышленность, металлургия, проектирование и интеграция АСУ, нефть и газ, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность, фармацевтика. Сюда также входят системы от инжиниринговых и интеграционных фирм, которые работают с предприятиями в различных отраслях, а также системы управления зданиями, физической безопасности и обработки биометрических данных.

Атакованными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, квартал, 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