Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первый квартал 2024

27.05.2024

Version 1.1

Цифры квартала

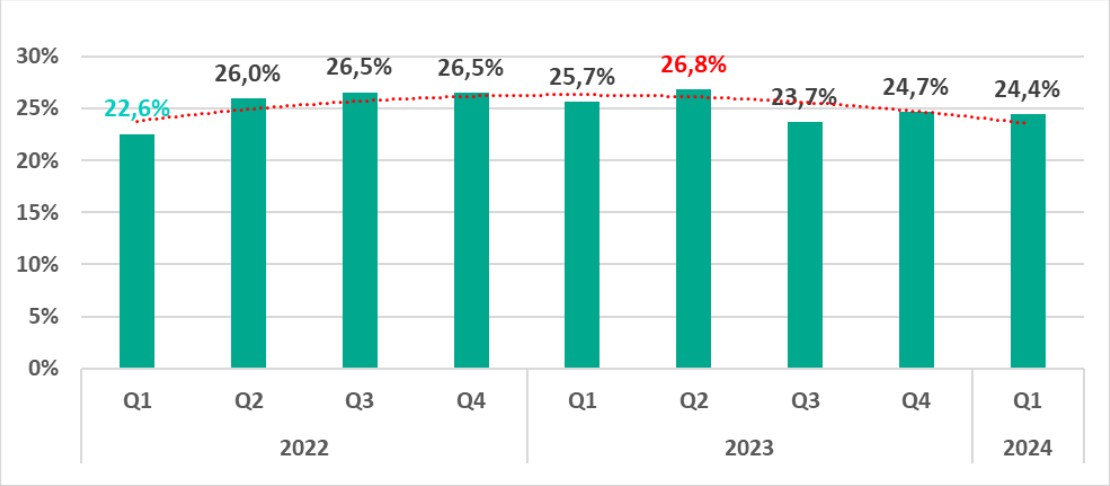
Показатель	Q4 2023	Q1 2024	Изменения за квартал
Процент атакованных компьютеров АСУ в мире	24,7%	24,4%	-0,3 п.п.
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Ресурсы в интернете из списка запрещённых	6,58%	6,84%	0,26 п.п.
Вредоносные скрипты и фишинговые страницы (JS и HTML)	7,61%	5,84%	-1,77 п.п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,86%	3,90%	0,04 п.п.
Вредоносные документы (MSOffice+PDF)	2,02%	1,72%	-0,30 п.п.
Вирусы (Virus)	1,48%	1,56%	0,08 п.п.
Черви (Worm)	1,55%	1,51%	-0,04 п.п.
Майнеры — исполняемые файлы для ОС Windows	0,84%	0,92%	0,08 п.п.
Веб-майнеры, выполняемые в браузерах	0,45%	0,49%	0,04 п.п.
Вредоносные программы для AutoCAD	0,36%	0,41%	0,05 п.п.
Программы-вымогатели	0,17%	0,15%	-0,02 п.п.
Основные источники угроз			
Интернет	13,25%	12,24%	-1,01 п.п.
Почтовые клиенты	3,15%	3,04%	-0,11 п.п.
Съемные носители	1,29%	1,13%	-0,16 п.п.
Сетевые папки	0,17%	0,15%	-0,02 п.п.

Статистика по всем угрозам

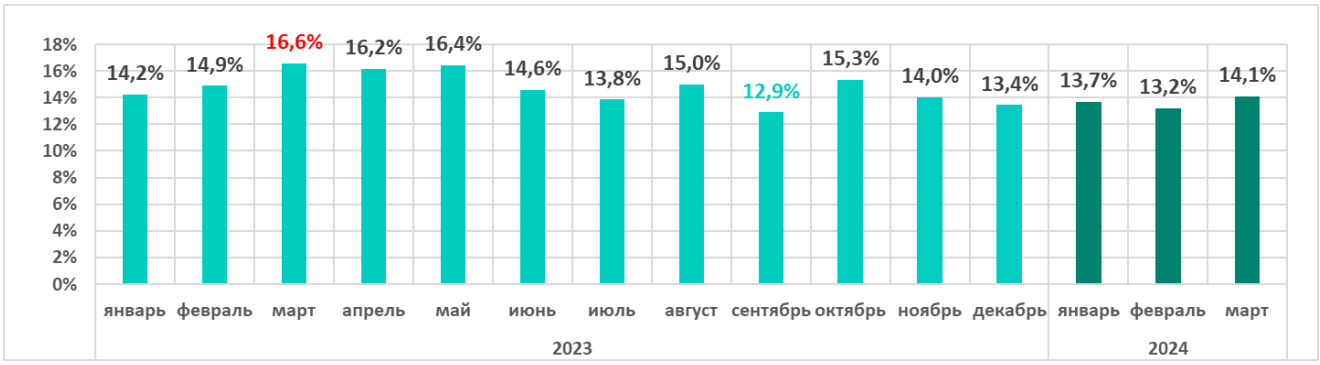
В первом квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился по сравнению с предыдущим кварталом на 0,3 п.п. и составил 24,4%.

По сравнению с первым кварталом 2023 года процент уменьшился на 1,3 п.п.

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

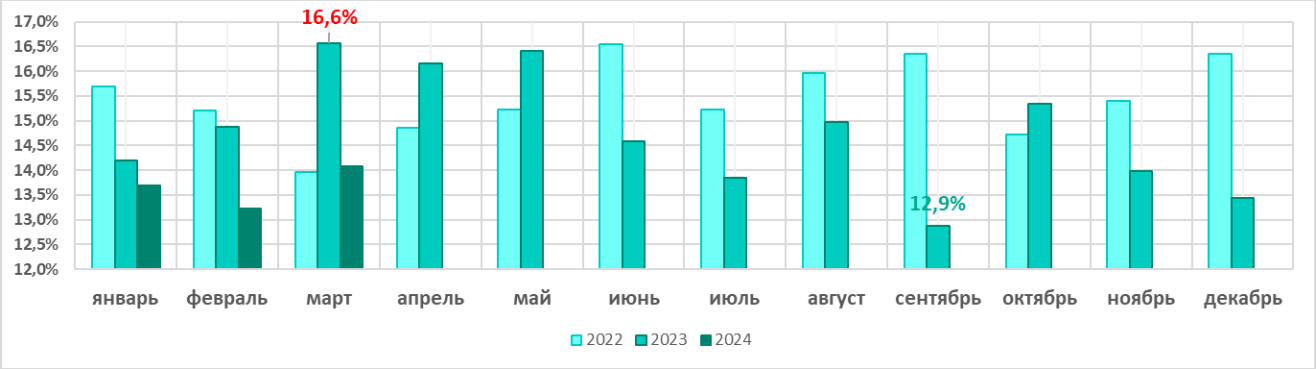


В течение первого квартала 2024 года самым высоким процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, был в марте, самым низким — в феврале.



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

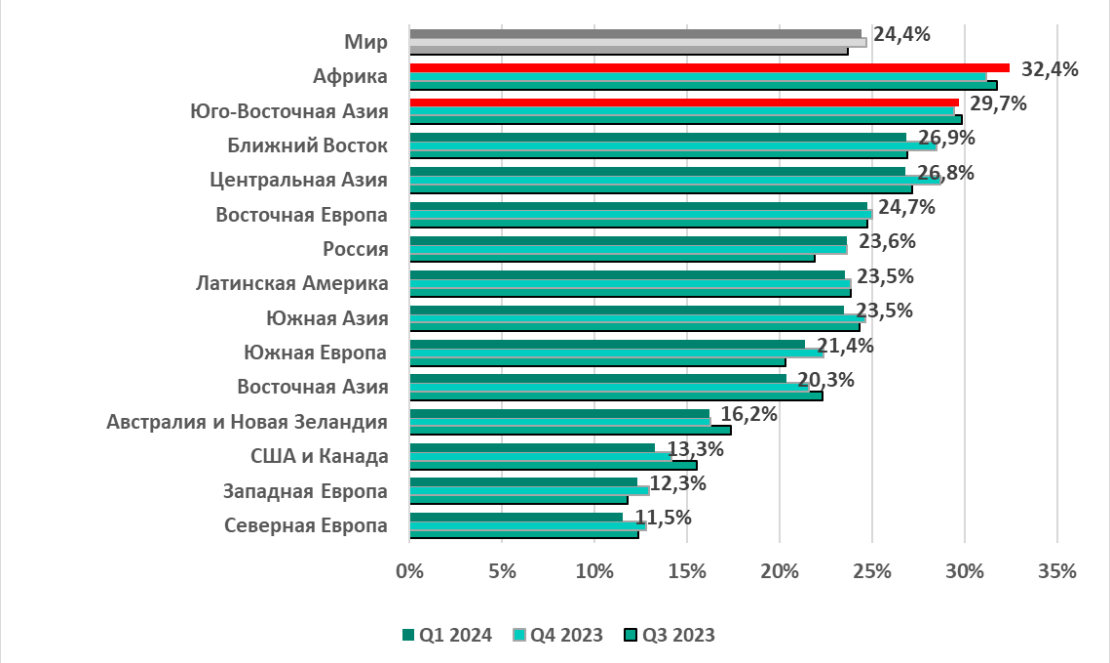
Проценты за первые три месяца 2024 года заметно меньше, чем в первые три месяца предыдущего (2023) года.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам 2021, 2022, 2023 и 2024 годов

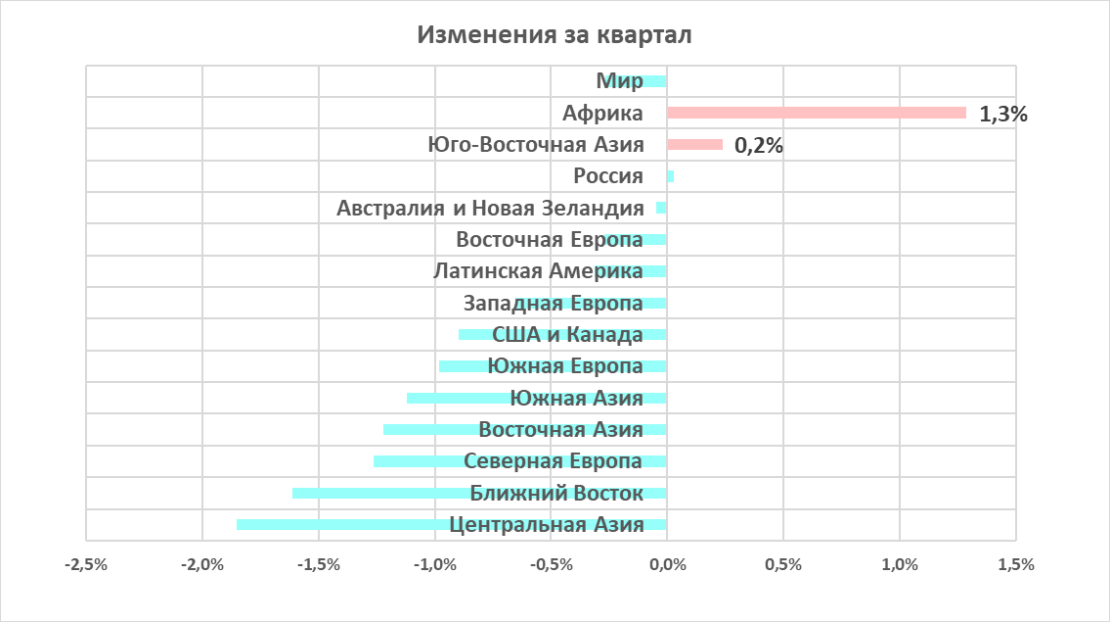
В регионах процент компьютеров АСУ, на которых в течение квартала были заблокированы вредоносные объекты, варьирует от 32,4% в Африке до 11,5% в Северной Европе.

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



Процент увеличился по сравнению с предыдущим кварталом в двух регионах, лидирующих в рейтинге по проценту атакованных компьютеров АСУ, — в Африке и Юго-Восточной Азии.

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

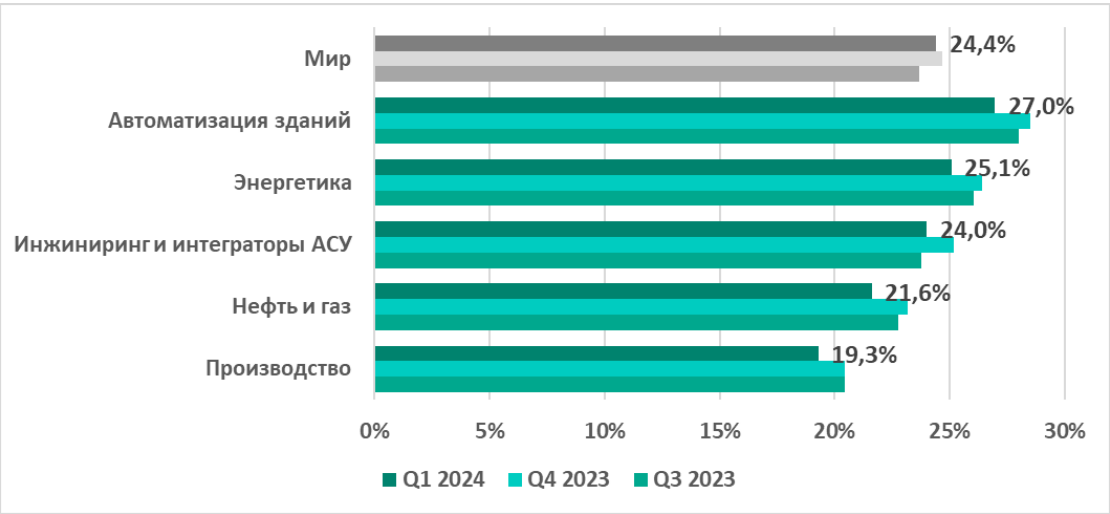


Подробнее о региональной статистике мы рассказываем в отчете по регионам.

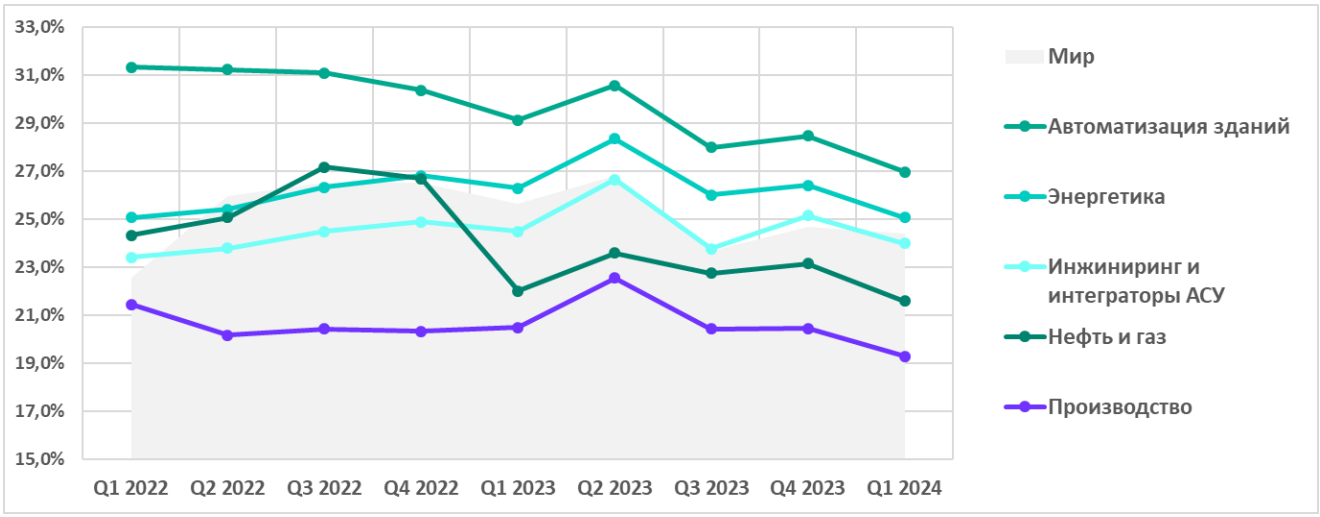
Некоторые отрасли

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



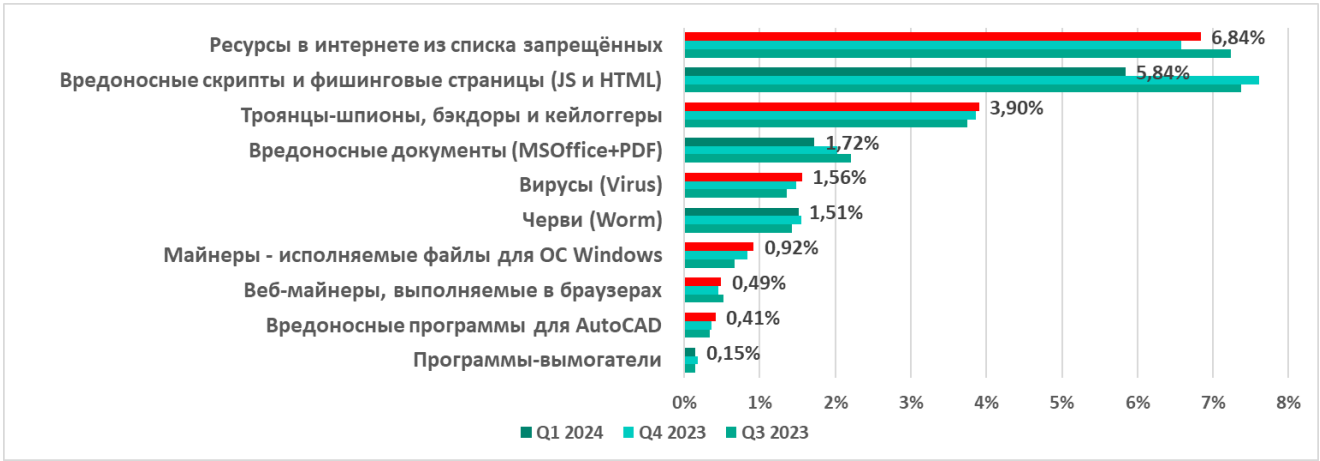
В первом квартале 2024 года во всех отраслях процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился.



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

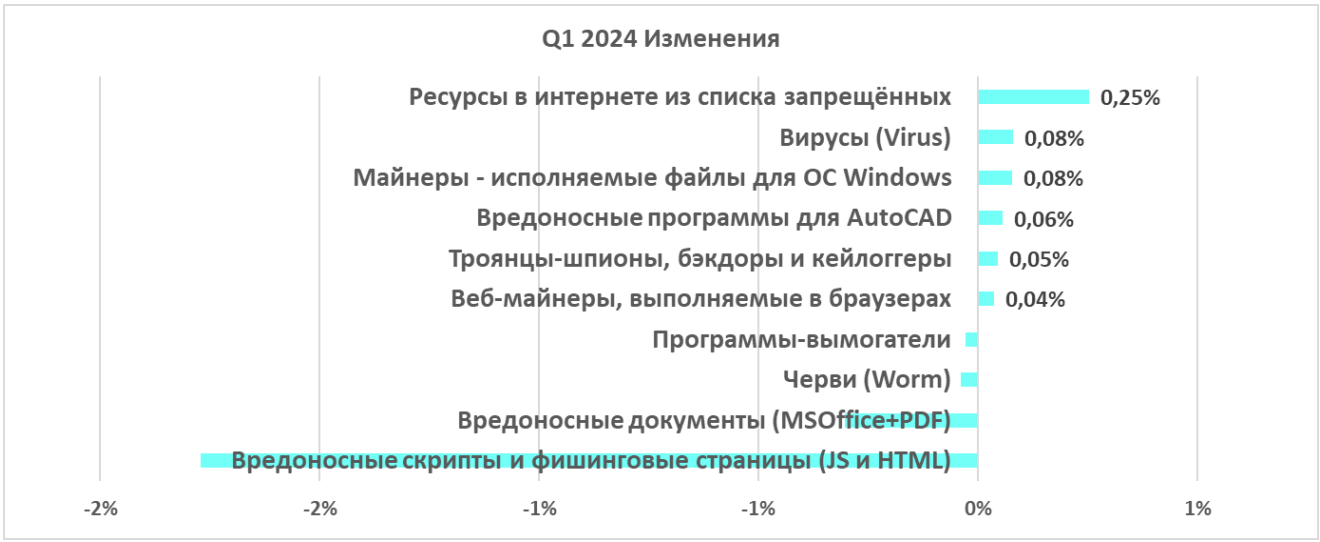
Разнообразие обнаруженного вредоносного ПО

В первом квартале 2024 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано вредоносное ПО из 10865 различных семейств, относящихся к различным категориям.



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.



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

В первом квартале 2024 года по сравнению с предыдущим кварталом наиболее заметно вырос процент компьютеров АСУ, на которых были заблокированы:

- вредоносные программы для AutoCAD — в 1,16 раза.

Категории вредоносных объектов

Вредоносные объекты различных категорий, 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.

Опасные веб-ресурсы (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 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.

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.

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).

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.

В первом квартале 2024 года процент компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, 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 вредоносные документы, был максимальным во втором квартале 2022 года и с тех пор снижается.

Вредоносное ПО следующего этапа

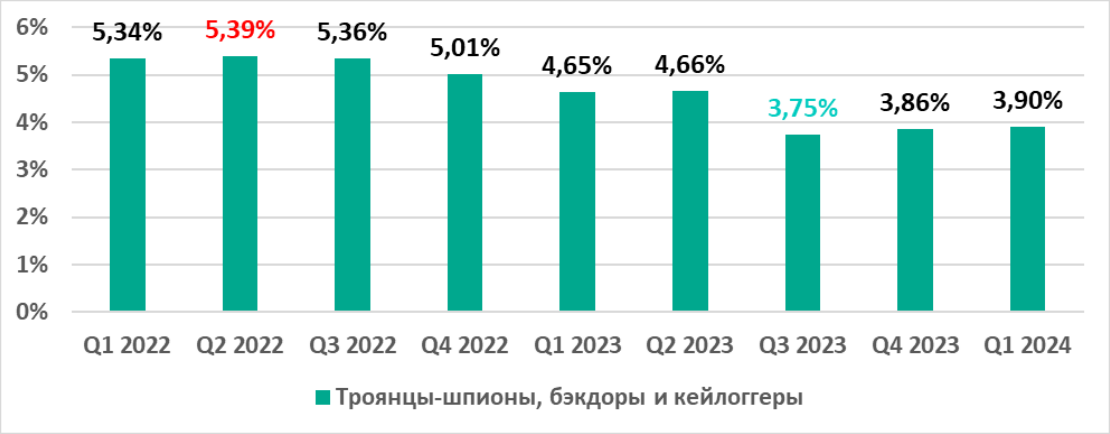
Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа — шпионское ПО, программы-вымогатели и майнеры. Как правило, чем выше процент компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, тем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

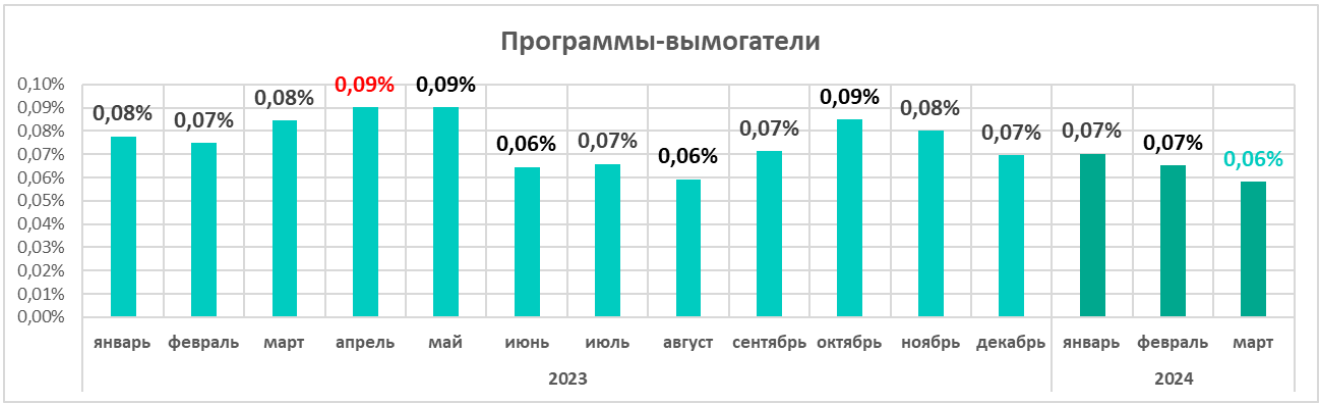
Процент компьютеров АСУ, на которых были заблокированы программы-шпионы, был минимальным в третьем квартале 2023 года и немного подрос за последние два квартала.



Программы-вымогатели

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

Как видно на графике ниже, показатель программ-вымогателей снижается с ноября 2023 года.

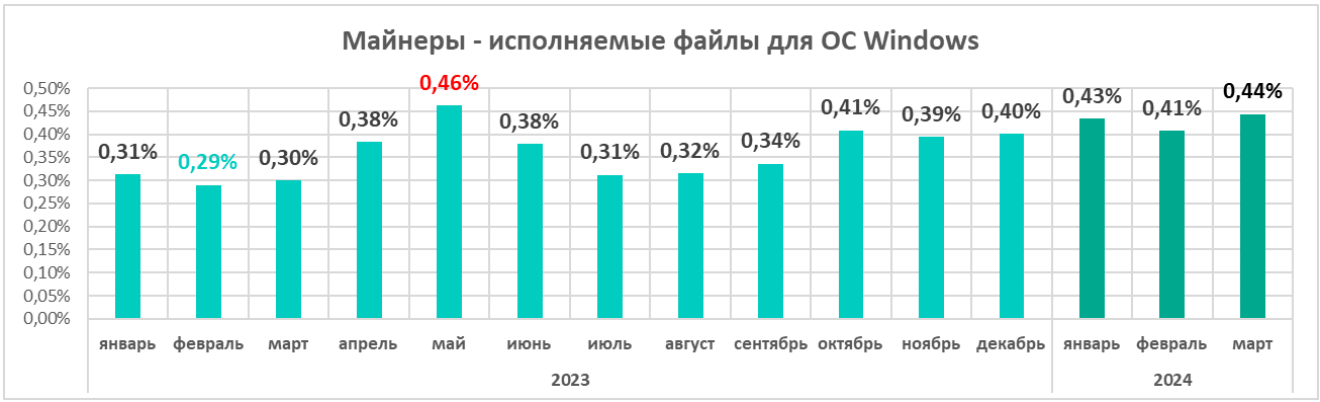


Майнеры — исполняемые файлы для ОС Windows

Процент компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Widows, был минимальным в первом квартале 2023. Со второго квартала 2023 года он увеличивается, и по сравнению с первым кварталом 2023 года вырос в 1,5 раза.

Среди майнеров, предназначенных для запуска на ОС Windows, одними из наиболее распространённых являются майнеры, распространяемые злоумышленниками с легитимным ПО в форме инсталляционных NSIS файлов.

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.



Веб-майнеры

Процент компьютеров АСУ, на которых были заблокированы веб-майнеры, был минимальным в последнем квартале 2023 года и немного подрос в первом квартале 2024.

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.

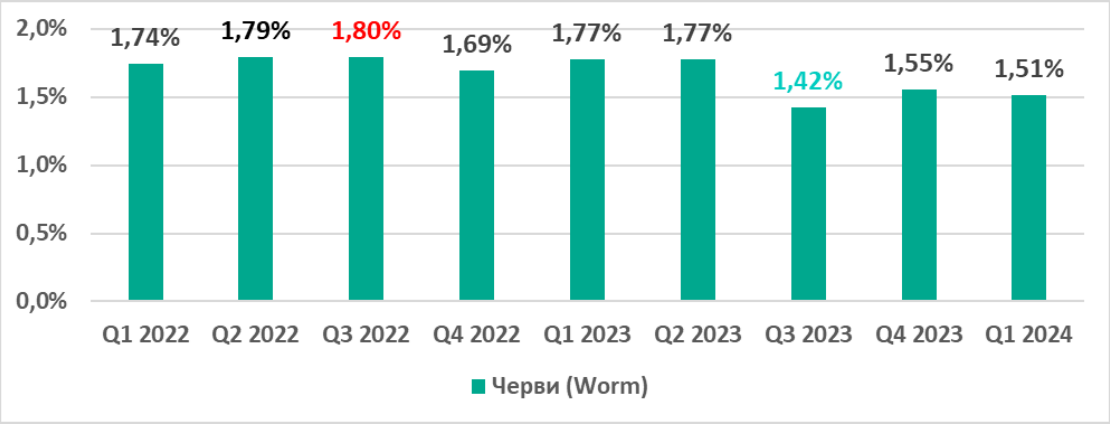
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

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 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.

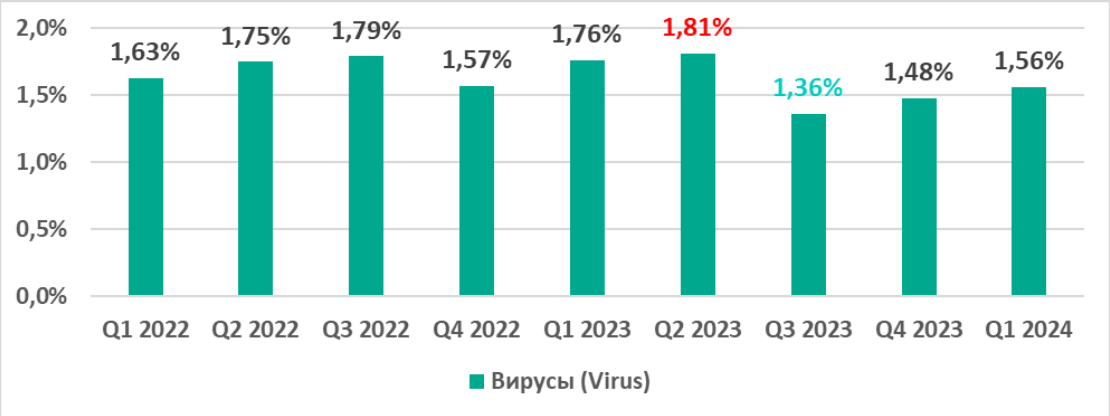
В мире процент компьютеров АСУ, на которых были заблокированы вирусы и черви, потихоньку растет после минимума в третьем квартале 2023 года.

Черви



Вирусы

Процент компьютеров АСУ, на которых были заблокированы вирусы, растет после минимума третьего квартала 2023 года, однако пока не превысил показатели кварталов 2022 года и первых двух кварталов 2023.

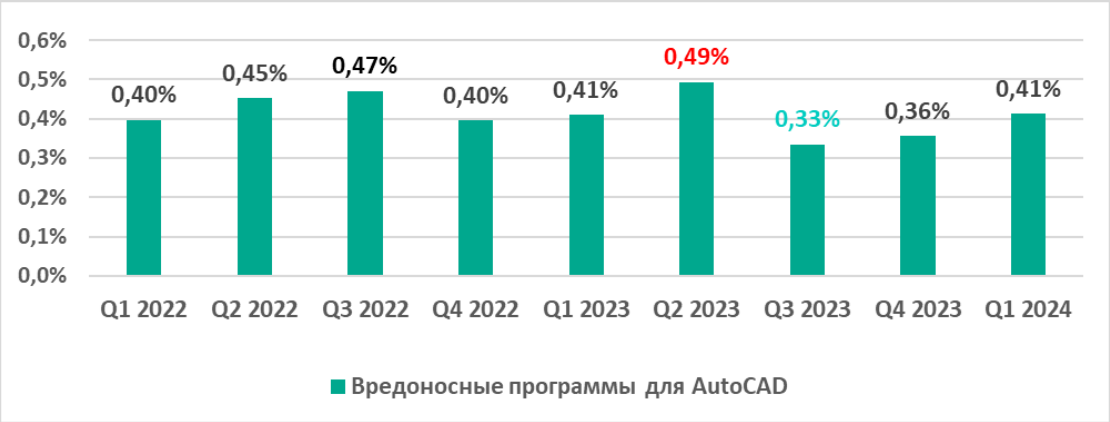


Вредоносные программы для AutoCAD

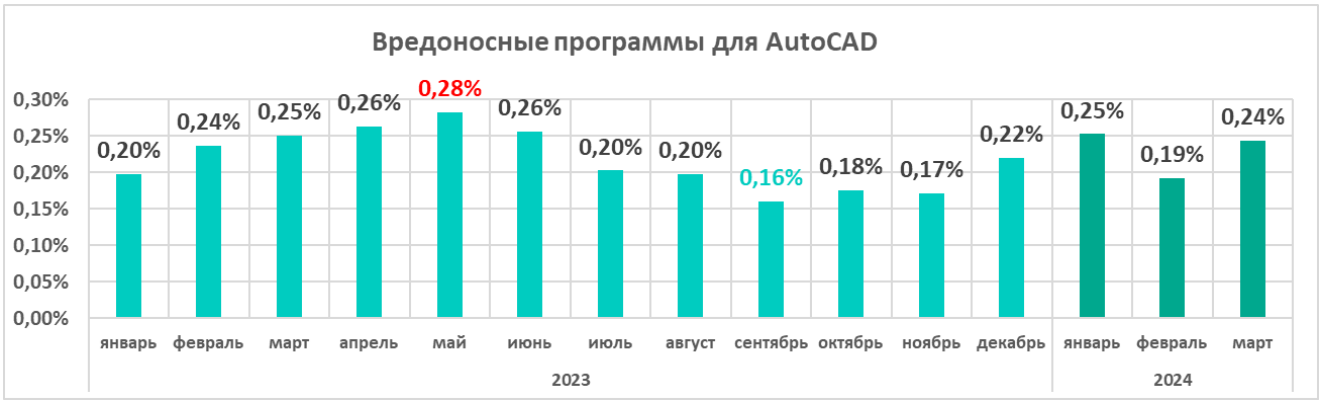
Эта категория вредоносного ПО может распространяться по-разному, поэтому не относится к конкретной группе.

Как правило, это минорная угроза, которая в рейтинге категорий вредоносных объектов по проценту компьютеров АСУ, на которых оно было заблокировано, занимает последние места.

В первом квартале 2024 года процент компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, вырос в 1,16 раз.



В первые три месяца 2024 года показатель майнеров был близок к уровню середины 2023 года, когда был отмечен максимум.



Основные источники угроз

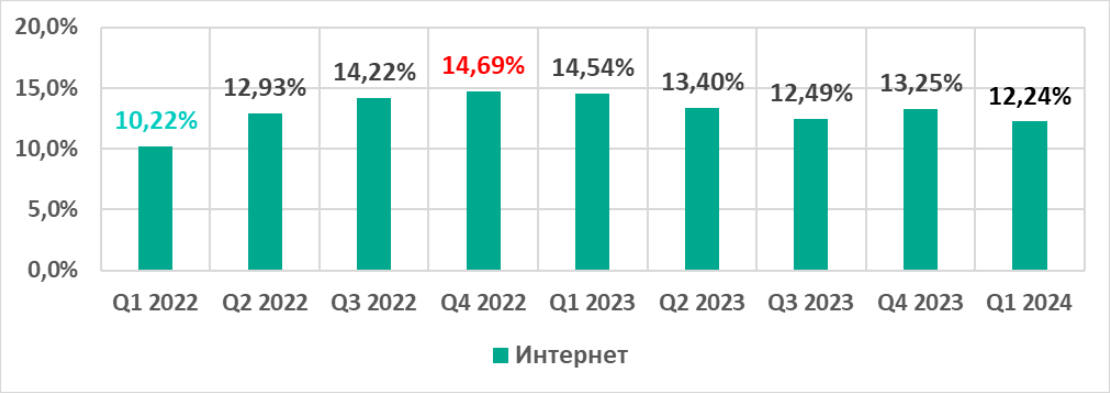
Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, почтовые клиенты и съемные носители. (Отметим, что источники заблокированных угроз надёжно установить удается не во всех случаях.)

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников угроз снизился для всех основных источников угроз.

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

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

Интернет



Почтовые клиенты

Съёмные носители

Сетевые папки

Минорный источник угроз — сетевые папки. 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 во 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 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.

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