Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Четвертый квартал 2024

17.03.2025

Версия 1.0

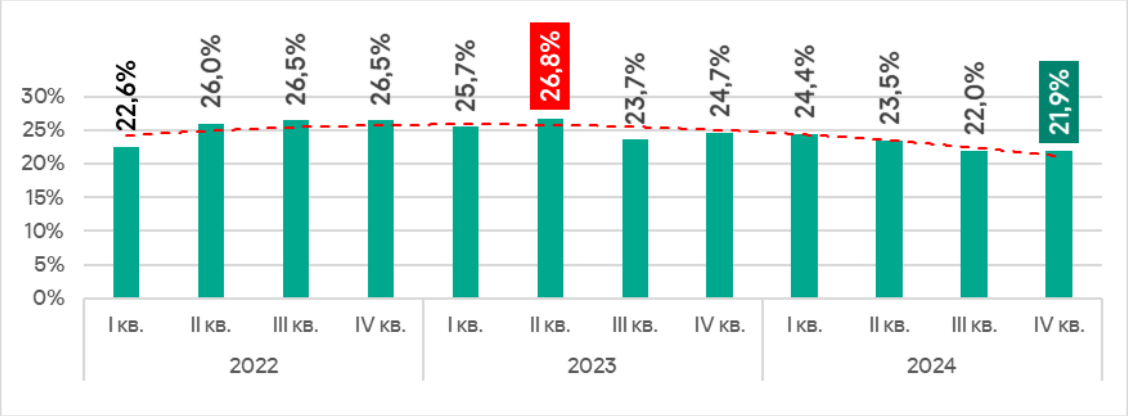
Цифры квартала

Показатель	III кв. 2024	IV кв. 2024	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	22,0%	21,9%	▼0,1 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	6,24%	7,11%	▲0,87 п. п.
Ресурсы в интернете из списка запрещенных	6,84%	5,52%	▼1,32 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	3,91%	4,30%	▲0,39 п. п.
Вредоносные документы (MSOffice+PDF)	1,97%	1,71%	▼0,26 п. п.
Вирусы (Virus)	1,53%	1,61%	▲0,08 п. п.
Черви (Worm)	1,30%	1,37%	▲0,07 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,71%	0,70%	▼0,01 п. п.
Веб-майнеры, выполняемые в браузерах	0,41%	0,39%	▼0,02 п. п.
Вредоносные программы для AutoCAD	0,40%	0.38%	▼0,02 п. п.
Программы-вымогатели	0,16%	0,21%	▲0,05 п. п.
Основные источники угроз			
Интернет	10,84%	9,98%	▼0,86 п. п.
Почтовые клиенты	2,95%	2,72%	▼0,23 п. п.
Съемные носители	0,69%	0,64%	▼0,05 п. п.
Сетевые папки	0,11%	0,08%	▼0,03 п. п.

Статистика по всем угрозам

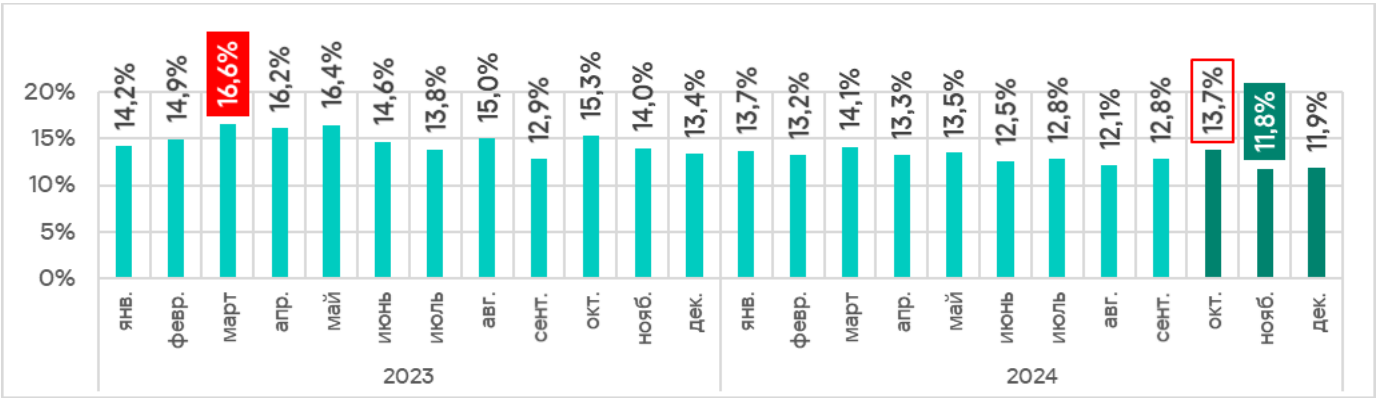
В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась по сравнению с предыдущим кварталом на 0,1 п. п. и составила 21,9%.

Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, 2022–2024 годы



По сравнению с четвертым кварталом 2023 года это значение уменьшилось на 2,8 п. п.

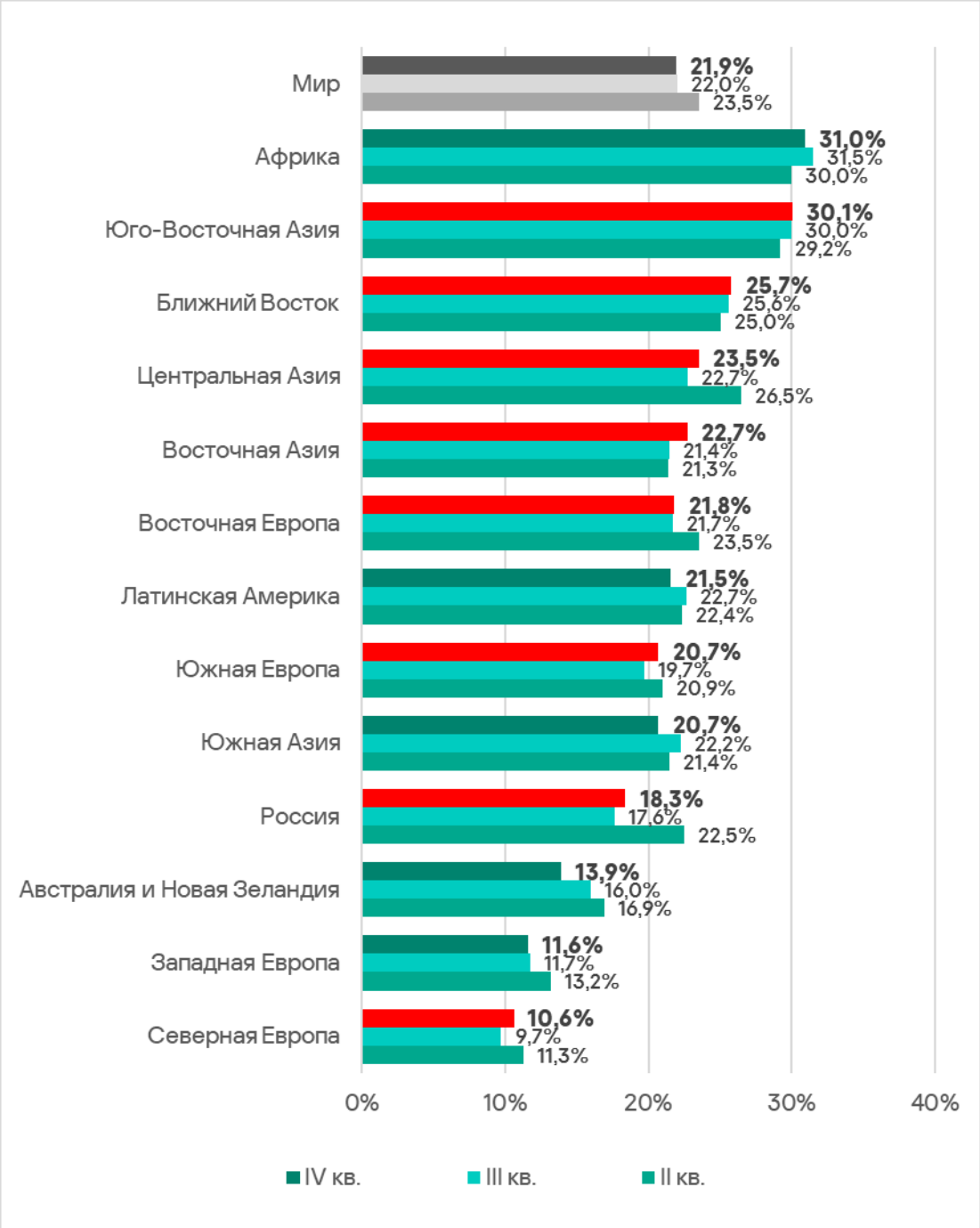
В течение четвертого квартала 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, достигла наибольшего значения в октябре, а наименьшего — в ноябре. Более того, ноябрьское значение — минимальное за два года.



Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, январь 2023 года — декабрь 2024 года

В регионах доля компьютеров АСУ, на которых в течение четвертого квартала 2024 года были заблокированы вредоносные объекты, варьировалась от 10,6% в Северной Европе до 31% в Африке.

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



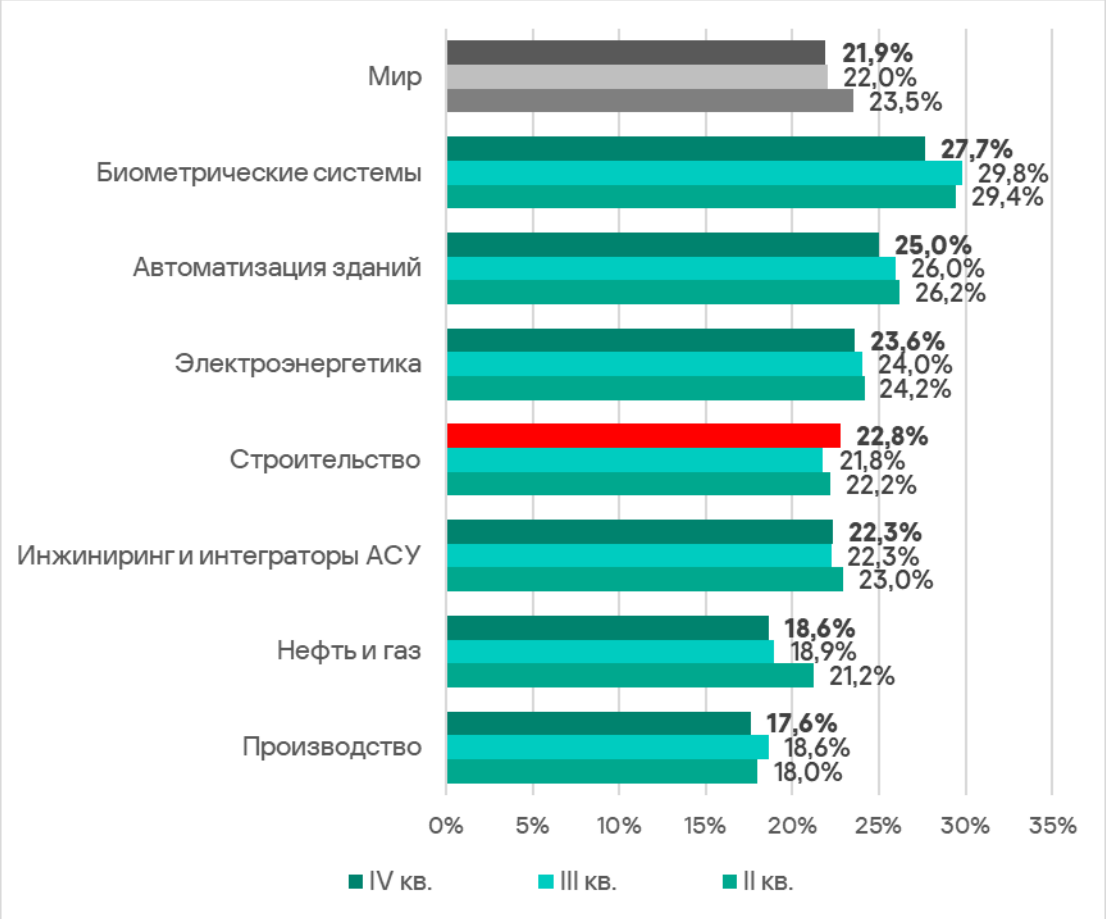
В восьми регионах из тринадцати, рассматриваемых в этом отчете, показатели увеличились по сравнению с предыдущим кварталом.

Регионы и мир. Изменение доли атакованных компьютеров за четвертый квартал 2024 года

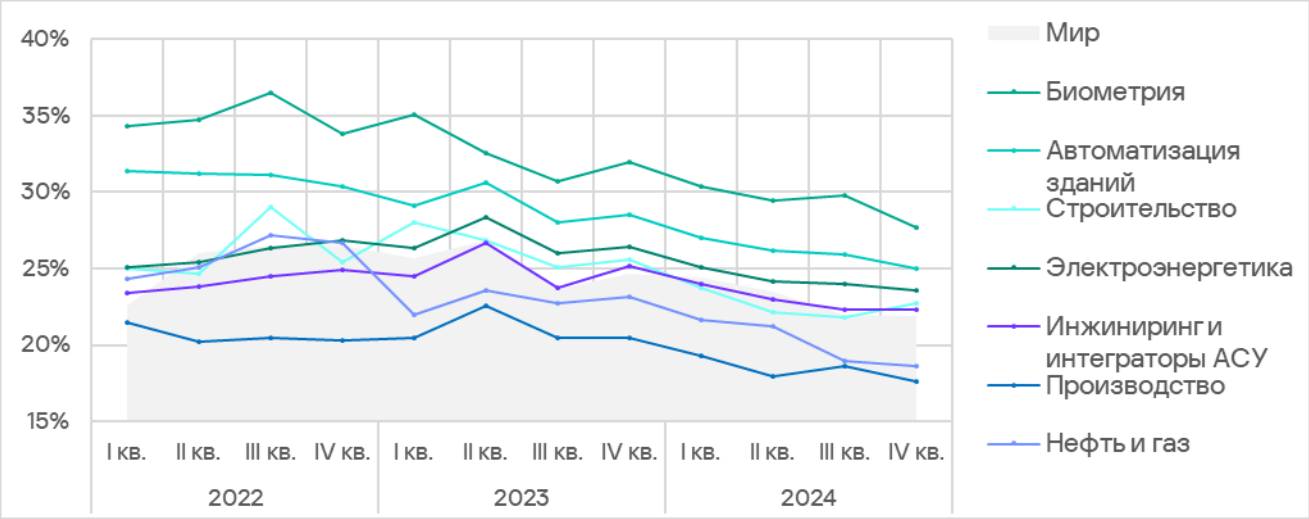
Исследуемые отрасли

Рейтинг исследуемых отраслей по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты, возглавляют биометрические системы.

Регионы и мир. Изменение доли атакованных компьютеров за четвертый квартал 2024 года



В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась в большинстве отраслей, за исключением строительства.



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

Разнообразие обнаруженных вредоносных объектов

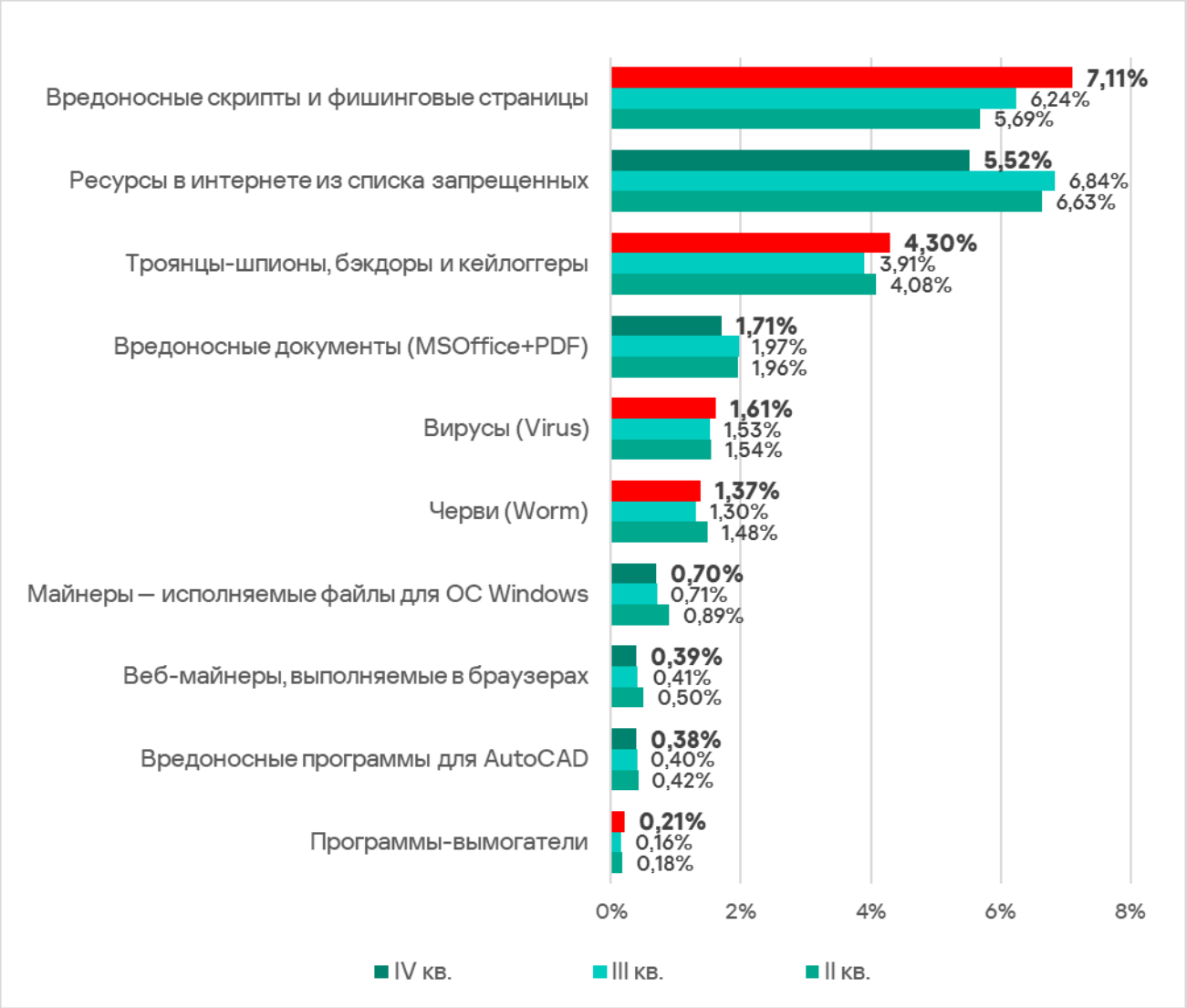
Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, по способу распространения и назначению можно условно разделить на три группы.

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

Вредоносные программы для AutoCAD могут распространяться разными способами, поэтому они не относится к конкретной группе.

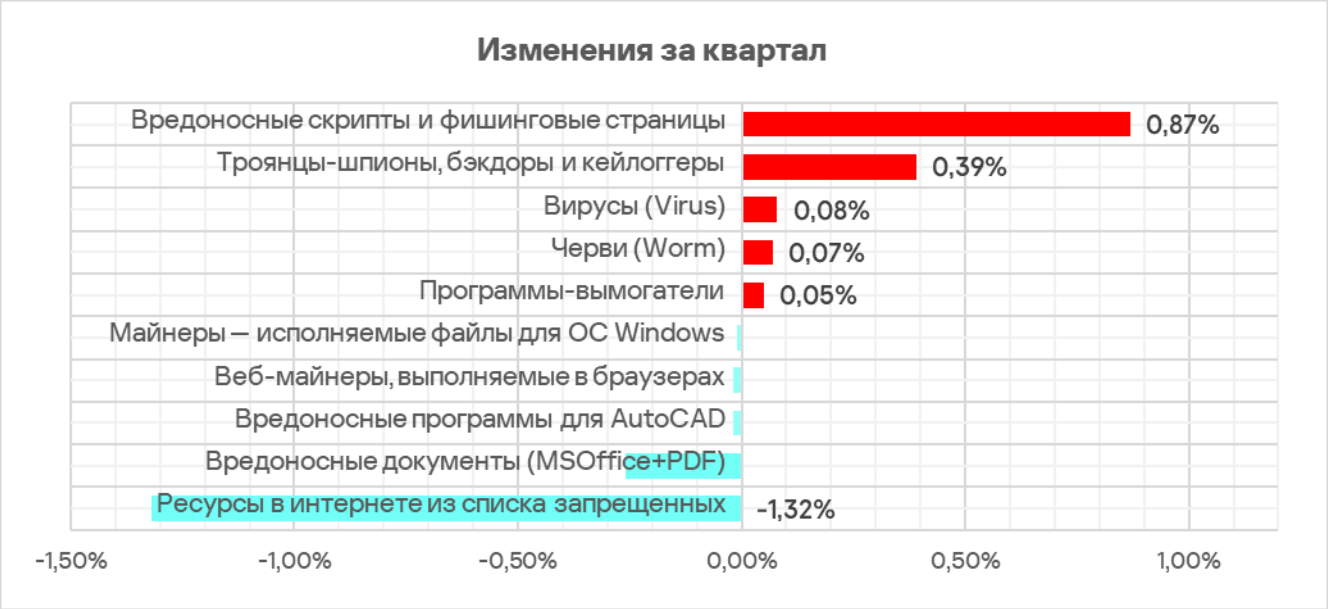
В четвертом квартале 2024 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 11 065 семейств, относящихся к различным категориям.

Вредоносные объекты, используемые для первичного заражения, обычно располагаются наверху рейтинга категорий угроз по доле компьютеров АСУ, на которых были заблокированы угрозы из вышеуказанных категорий.



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

[1] Полученные значения некорректно суммировать, потому что во многих случаях на одном компьютере за отчетный период могли быть заблокированы угрозы двух и более типов.



Изменение доли компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий, за третий квартал 2024 года (п. п.)

В относительном исчислении наиболее заметно (в 1,3 раза) выросла доля компьютеров АСУ, на которых были заблокированы **программы-вымогатели.**

Также стоит отметить пропорциональный рост долей компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы, шпионское ПО, черви** и **вирусы**. Значения соответствующих параметров увеличились в 1,1 раза.

Наиболее заметное пропорциональное снижение (в 1,2 раза) отмечено в долях компьютеров АСУ, на которых были заблокированы **запрещенные интернет-ресурсы** и **вредоносные документы.**

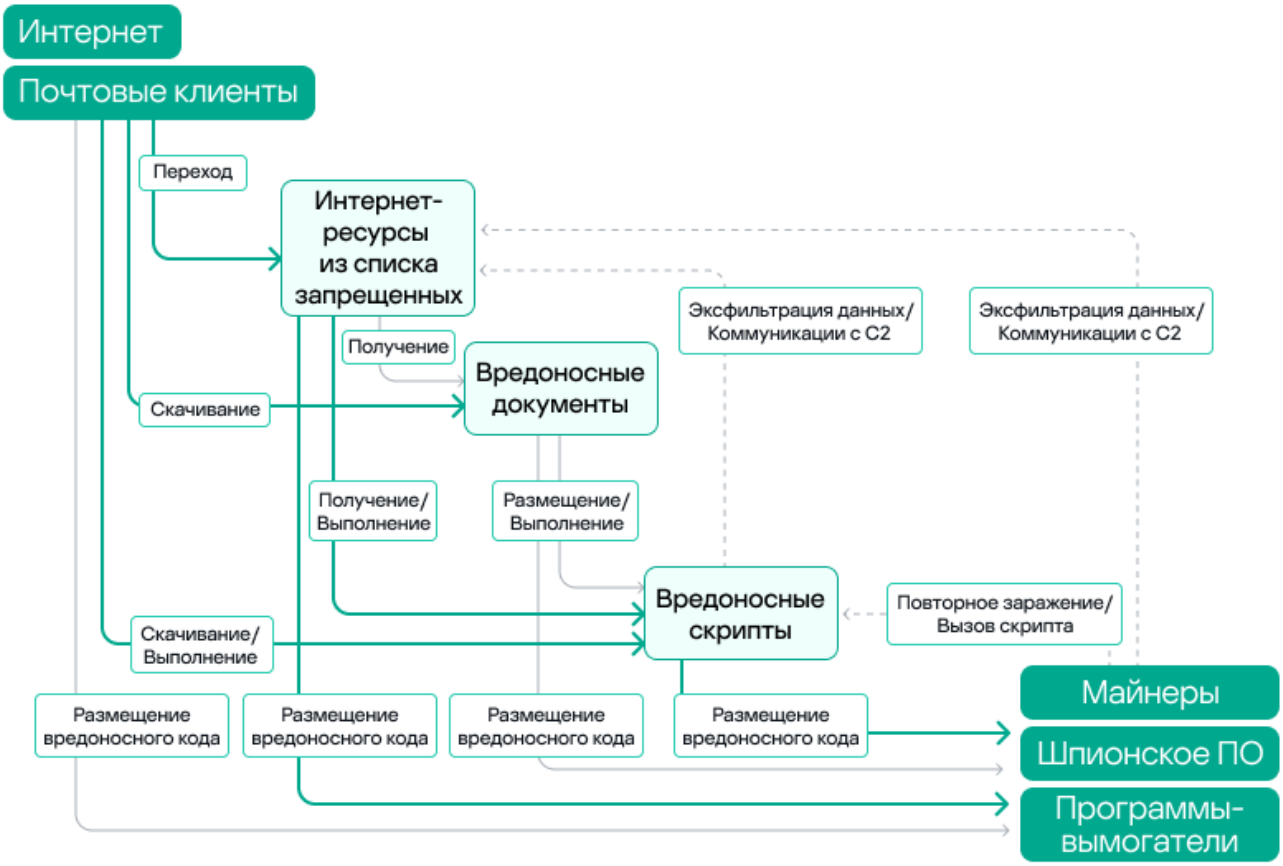
Вредоносные объекты, используемые для первичного заражения

Вредоносные объекты, которые используются для первичного заражения компьютеров АСУ: опасные веб-ресурсы, вредоносные скрипты и фишинговые страницы, а также вредоносные документы.

Такие вредоносные объекты активно распространяются, в результате они чаще остальных блокируются защитными решениями. Это отражается и в нашей статистике.

Типовые атаки, блокируемые в сети АСУ, представляют собой многоступенчатый процесс, где каждый последующий шаг злоумышленников направлен на повышение привилегий и получение доступа к другим системам путем эксплуатации присутствующих уязвимостей в системах и сетях АСУ.

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

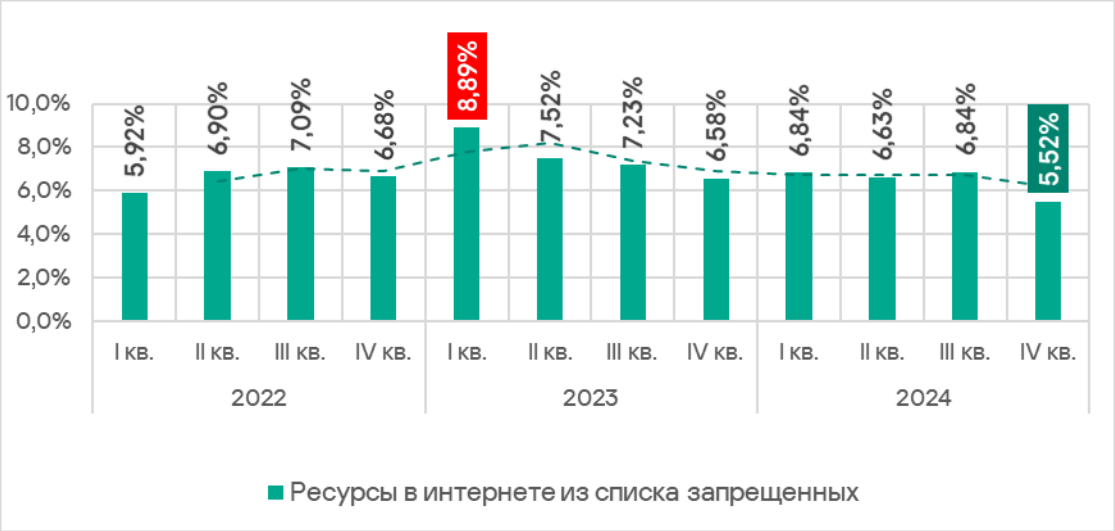


Цепочка атаки: от первичного заражения до вредоносного ПО следующего этапа

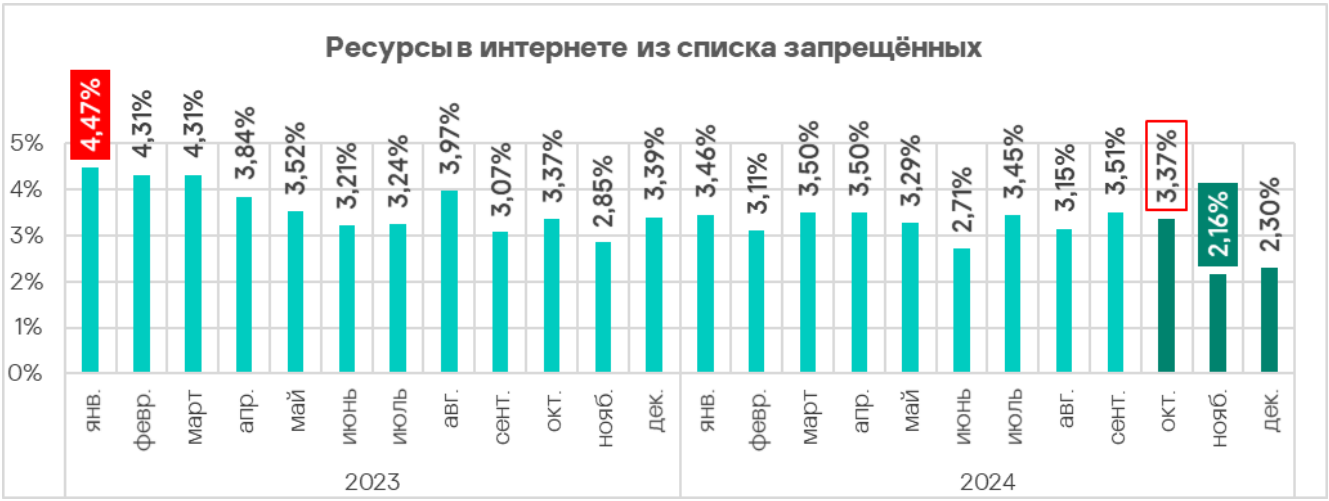
Ресурсы в интернете из списка запрещенных

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

В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, снизилась до наименьшего значения за рассматриваемый период.



На диаграмме ниже показано ежемесячное изменение доли компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, в течение двух последних лет. В ноябре 2024 года показатель достиг минимального значения за два года.



Как отмечалось в нашем отчете за третий квартал 2024 года, увеличение доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы

из списка запрещенных, главным образом обусловлен ростом количества вновь созданных доменных имен и IP-адресов, используемых киберпреступниками в качестве инфраструктуры управления и контроля (C2) для распространения вредоносного ПО и фишинговых атак.

На снижение доли вредоносных и потенциально опасных веб-ресурсов в ноябре-декабре 2024 года, вероятно, повлияли не только решительные меры по противодействию угрозам, реализуемые на различных уровнях — начиная от владельцев ресурсов, хостинг- и интернет-провайдеров и заканчивая правоохранительными органами. Другой возможный фактор — стремление злоумышленников менять доменные имена и IP-адреса в попытке избежать обнаружения на первом этапе — по списку уже известных интернет ресурсов.

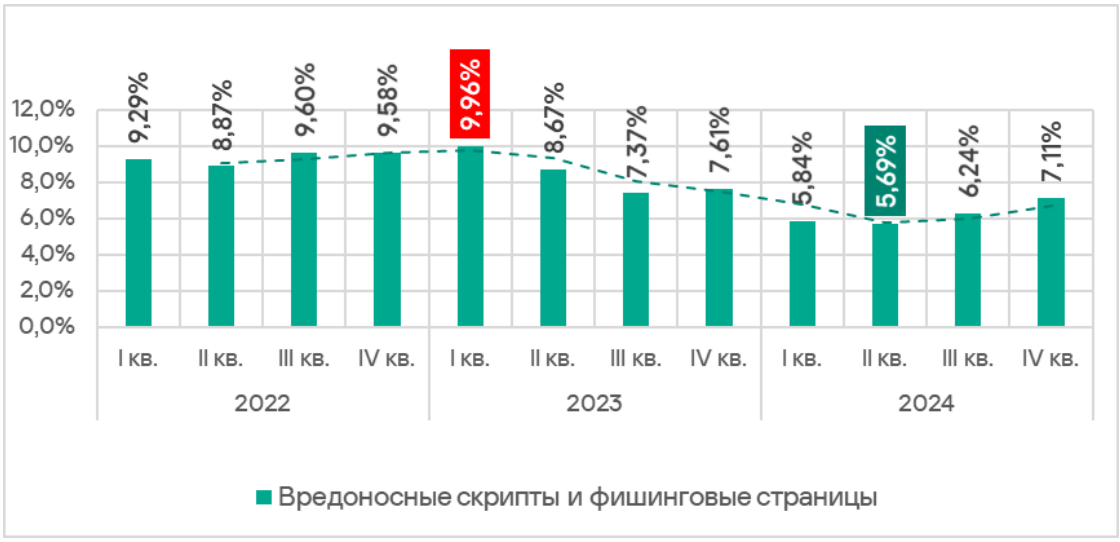
На практике это означает, что до тех пор, пока вредоносный интернет-ресурс не будет обнаружен и добавлен в список запрещенных, он не отражается в статистике, что, очевидно, ведет к снижению показателя по опасным веб-ресурсам.

Но вместе с тем в четвертом квартале наблюдался рост доли для следующего компонента в цепочке атаки — вредоносных скриптов и фишинговых страниц, шпионского ПО и программ-вымогателей.

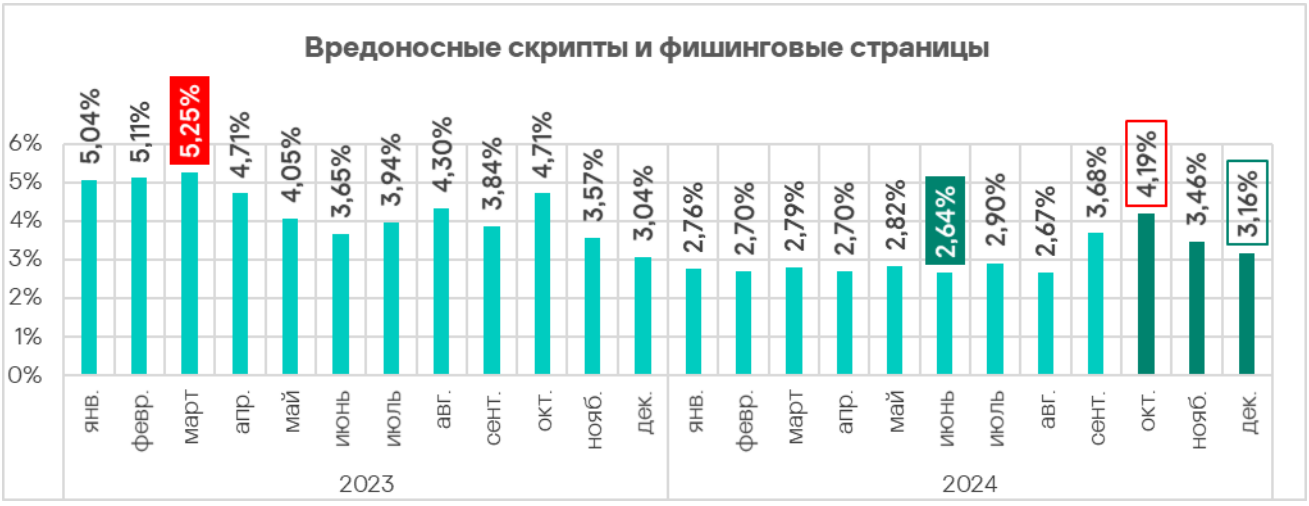
Вредоносные скрипты и фишинговые страницы (JS и HTML)

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 по электронной почте.

В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, продолжила расти.



Как показано на диаграмме ниже, ежемесячное значение показателя в четвертом квартале достигло максимума в октябре, после чего постепенно снизилось к декабрю.

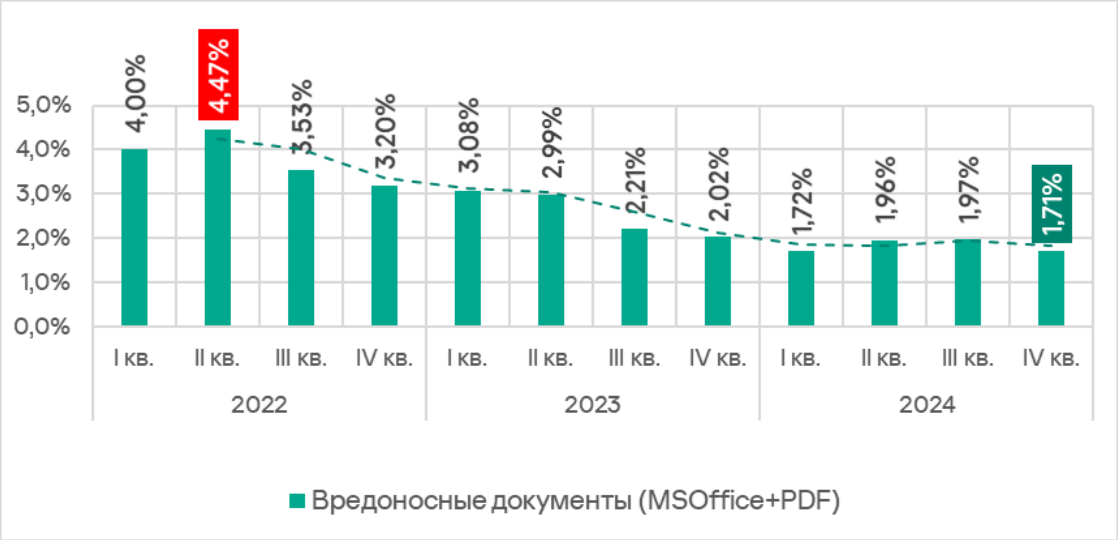


Значительное увеличение доли вредоносных скриптов и фишинговых страниц в октябре – следствие серии широкомасштабных фишинговых атак в конце лета и начале осени 2024 года, о чем упоминалось в нашем отчете за третий квартал 2024 года. Тогда злоумышленники использовали вредоносные скрипты, которые выполнялись в браузере, имитируя различные окна с интерфейсами, похожими на CAPTCHA, сообщения об ошибках браузера и аналогичные всплывающие окна, чтобы инициировать загрузку вредоносного ПО следующего этапа — стилер Lumma или троянец Amadey.

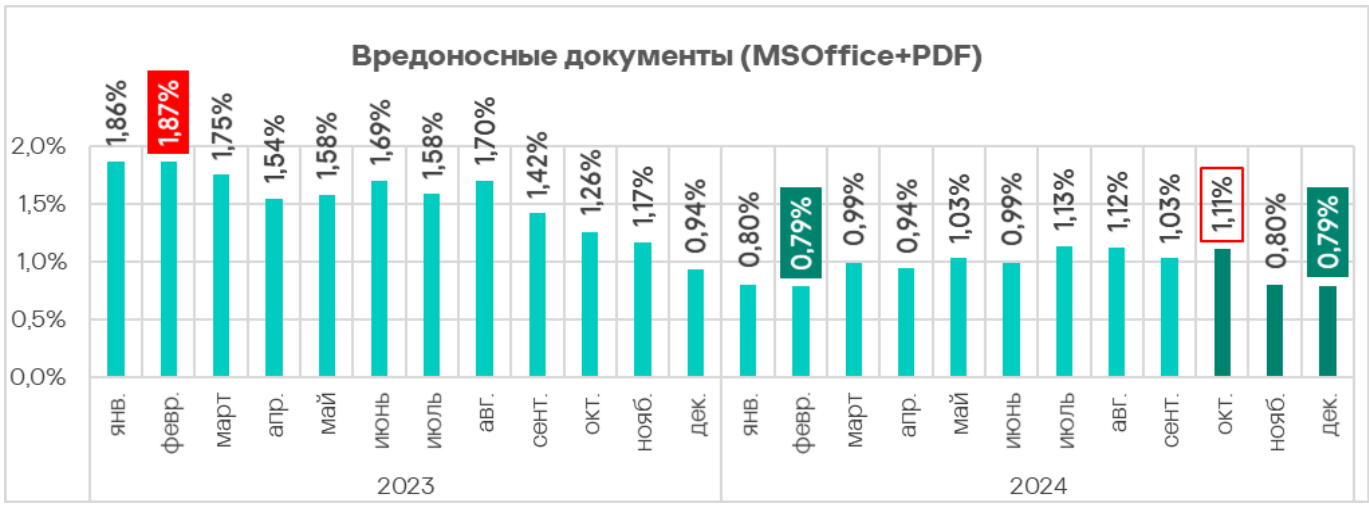
Вредоносные документы (MSOffice + PDF)

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 четвертом квартале 2024 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, достигла минимального значения за рассматриваемый период.



Как показано на диаграмме ниже, в декабре 2024 года доля компьютеров АСУ, на которых были обнаружены вредоносные документы, достигла наименьшего ежемесячного значения за два года.



Вредоносное ПО следующего этапа

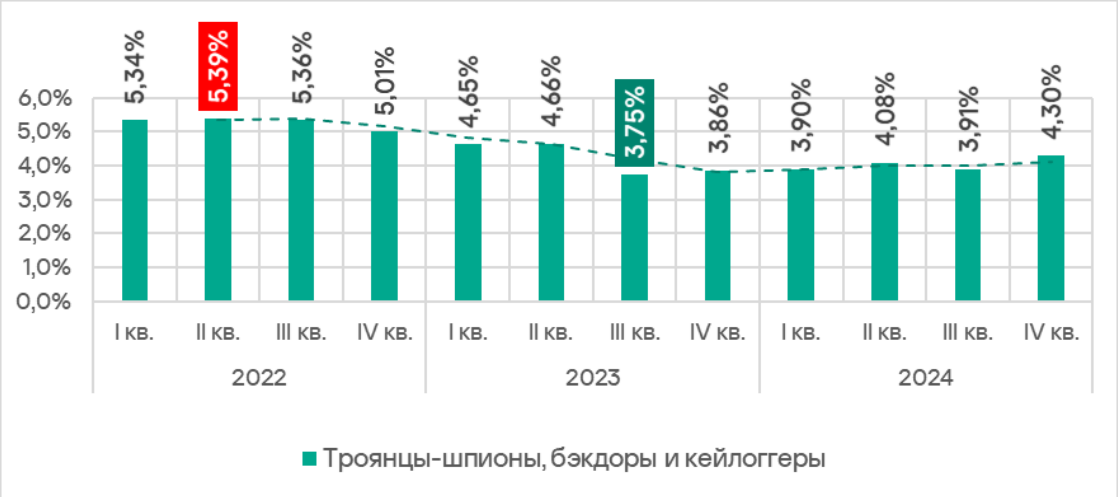
Вредоносные объекты, которые используются для первичного заражения компьютеров, доставляют на компьютеры жертв вредоносное ПО следующего этапа — шпионское ПО, программы-вымогатели и майнеры. Как правило, чем выше доля компьютеров АСУ, на которых блокируется вредоносное ПО первичного заражения, тем выше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

Программы-шпионы

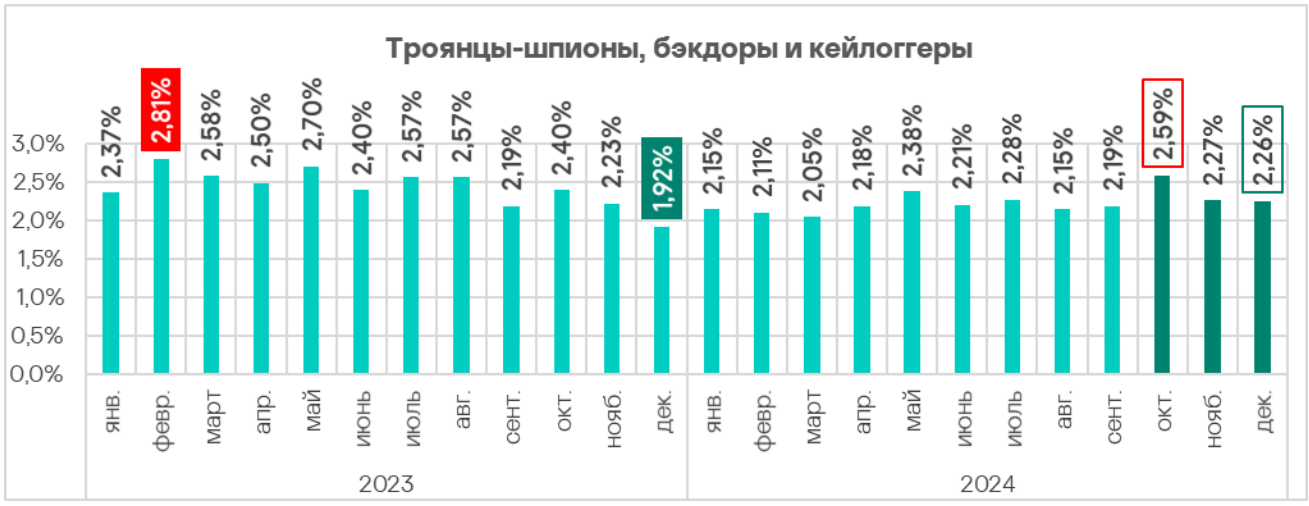
Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры) встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Шпионское ПО используется для несанкционированного удаленного доступа и кражи конфиденциальной информации. В большинстве случаев конечная цель атак с применением 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.

В четвертом квартале 2024 года доля компьютеров АСУ, на которых было заблокировано шпионское ПО, выросла по сравнению с предыдущим кварталом.

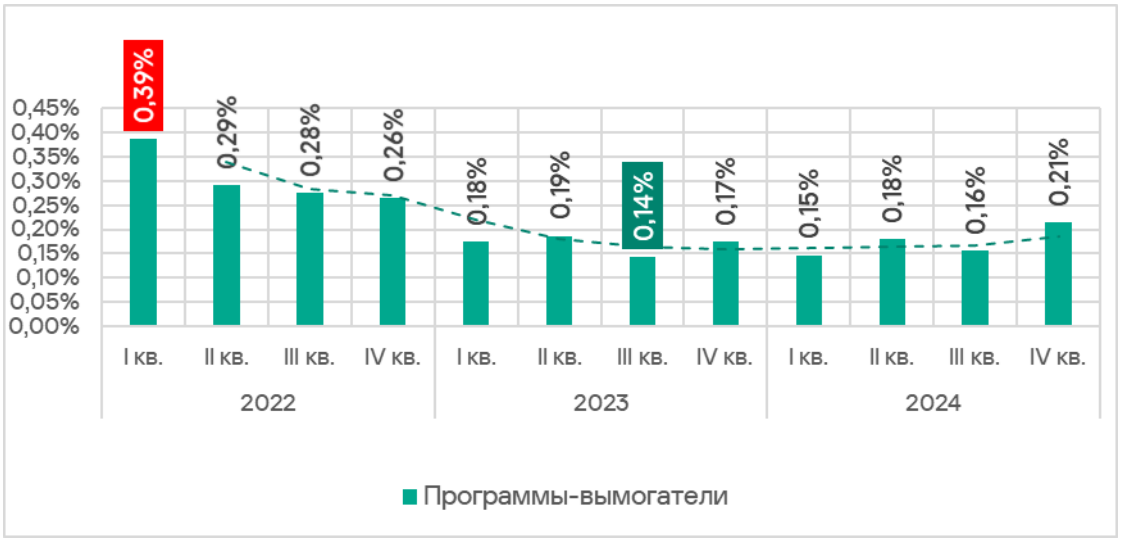


В октябре доля компьютеров АСУ, на которых было обнаружено шпионское ПО, достигла наибольшего ежемесячного значения за 2024 год.

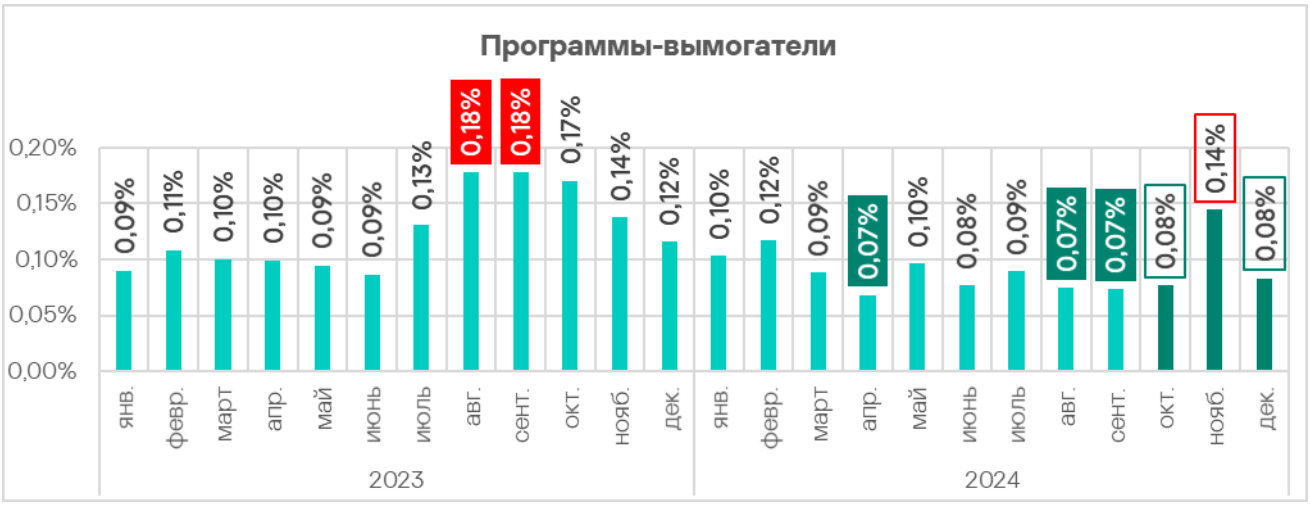


Программы-вымогатели

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, возросла в 1,3 раза, достигнув максимального значения с начала 2023 года.



Рост показателя главным образом обусловлен его резким увеличением в ноябре. Показатель в ноябре оказался наивысшим ежемесячным значением за 2024 год.



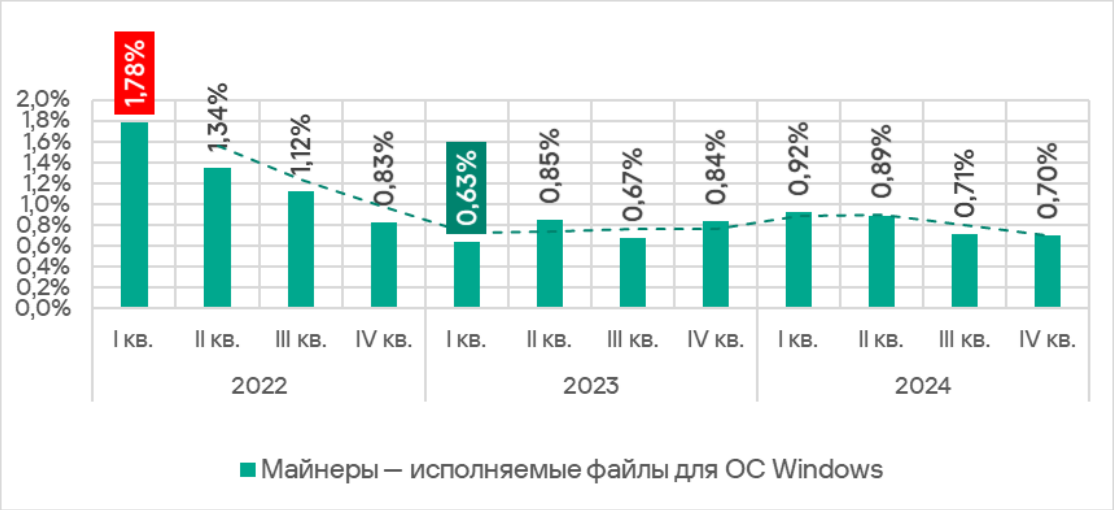
Майнеры — исполняемые файлы для ОС Windows

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

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

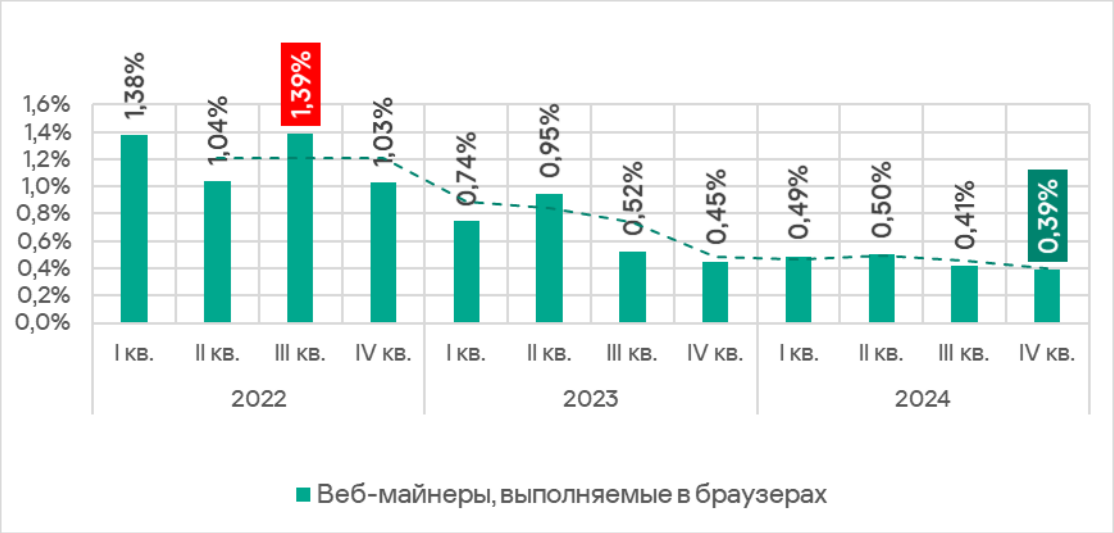
Другой популярный метод внедрения майнеров, обнаруживаемых на компьютерах АСУ, заключается в использовании таких майнеров криптовалют как XMRig, NBMiner, OneZeroMiner и т. д. Подобные майнеры, не являясь вредоносным ПО, детектируются защитными решениями как RiskTools. Злоумышленники используют их в сочетании со специфическими конфигурационными файлами, позволяющими визуально скрывать выполнение майнера от пользователя.

В четвертом квартале 2024 года доля компьютеров АСУ, на которых были выявлены майнеры в формате исполняемых файлов для Windows, снизилась и оказалась наименьшей за весь 2024 год.



Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, в четвертом квартале 2024 года снизилась и достигла минимального значения за рассматриваемый период.



Самораспространяющееся вредоносное ПО. Черви и вирусы

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

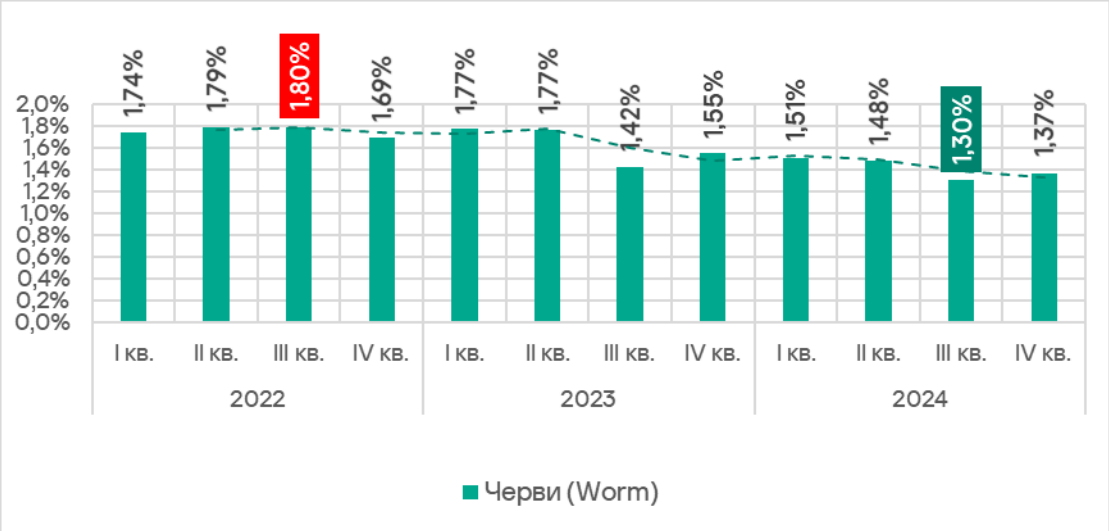
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

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

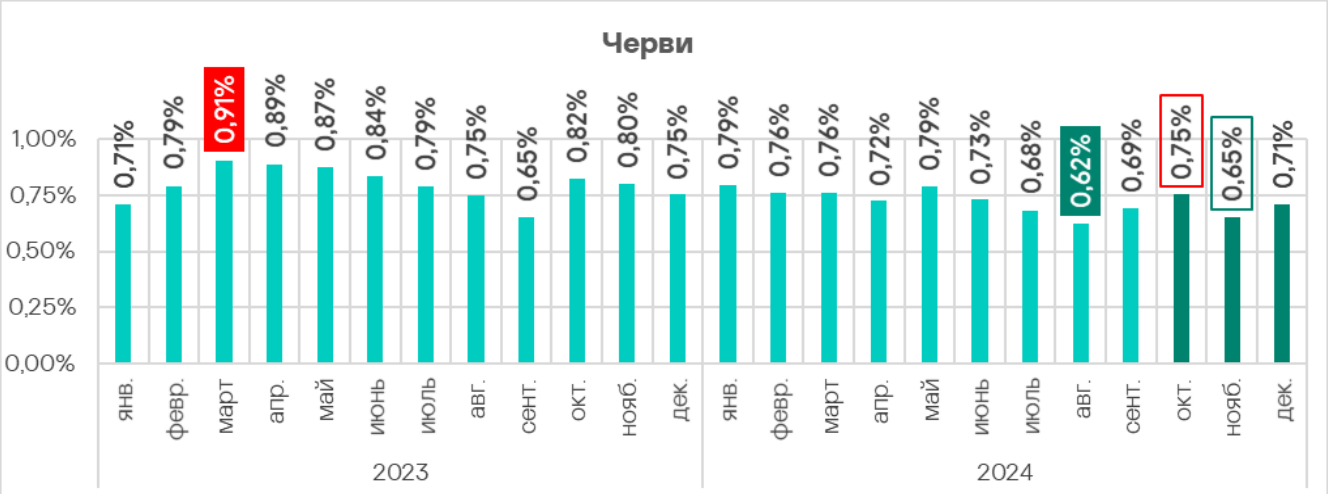
Черви

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

Достигнув в третьем квартале 2024 года минимального значения за весь рассматриваемый период, доля компьютеров АСУ, на которых были заблокированы черви, увеличилась в четвертом квартале 2024 года.

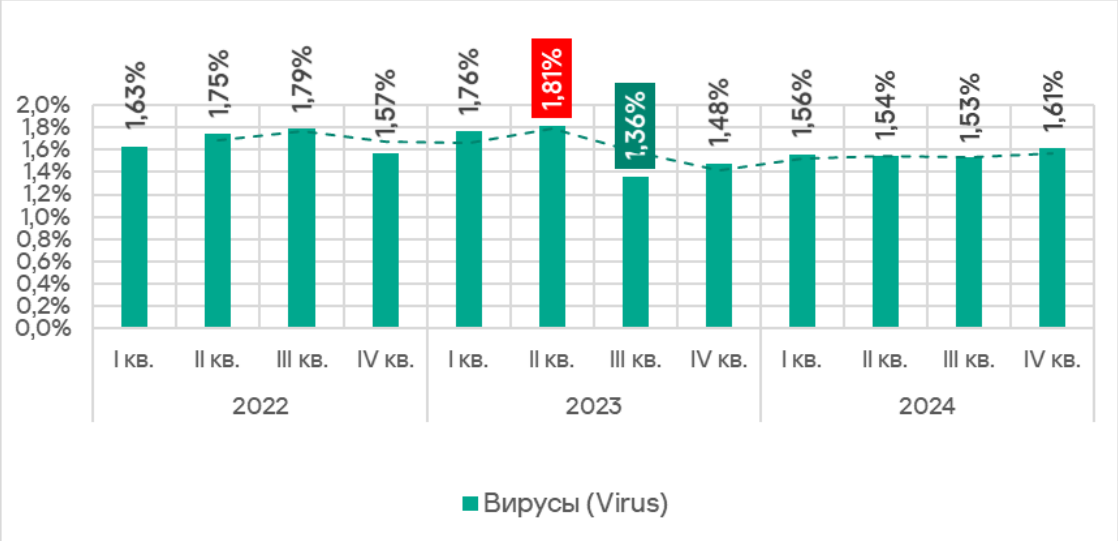


Рост показателя обусловлен скачком значения в октябре.

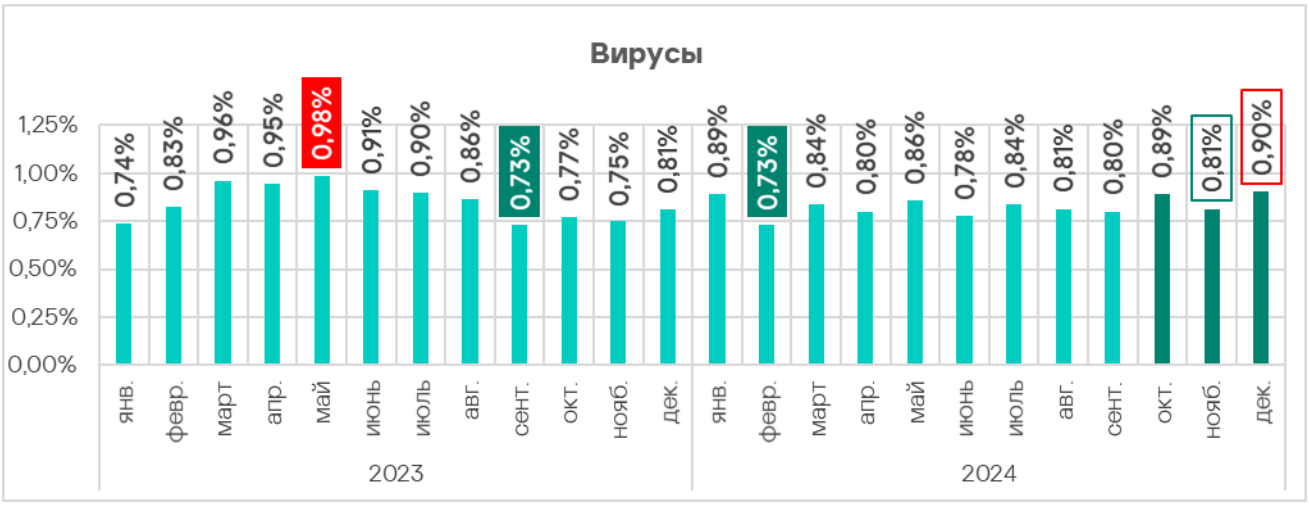


Вирусы

Доля компьютеров АСУ, на которых были заблокированы вирусы, выросла в четвертом квартале 2024 года.



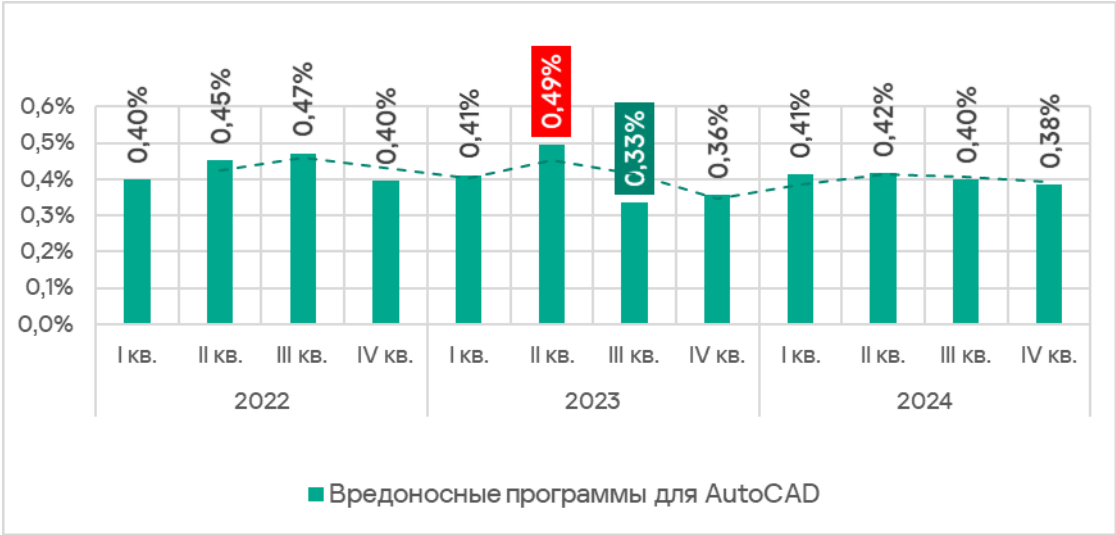
Ежемесячное значение показателя варьировалось в течение четвертого квартала, достигнув пика в декабре 2024 года. Это наивысшее месячное значение за 2024 год.



Вредоносные программы для AutoCAD

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

В четвертом квартале 2024 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, продолжила снижение.

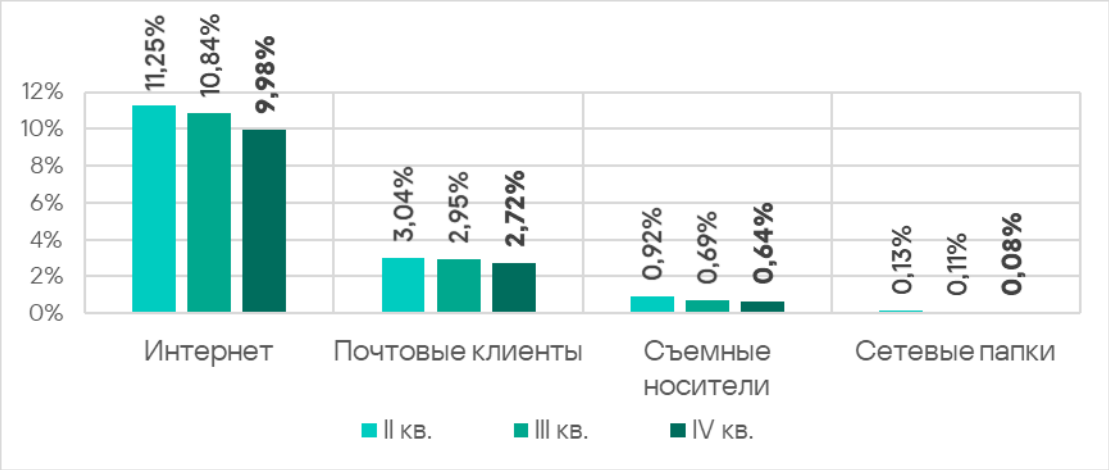


Основные источники угроз

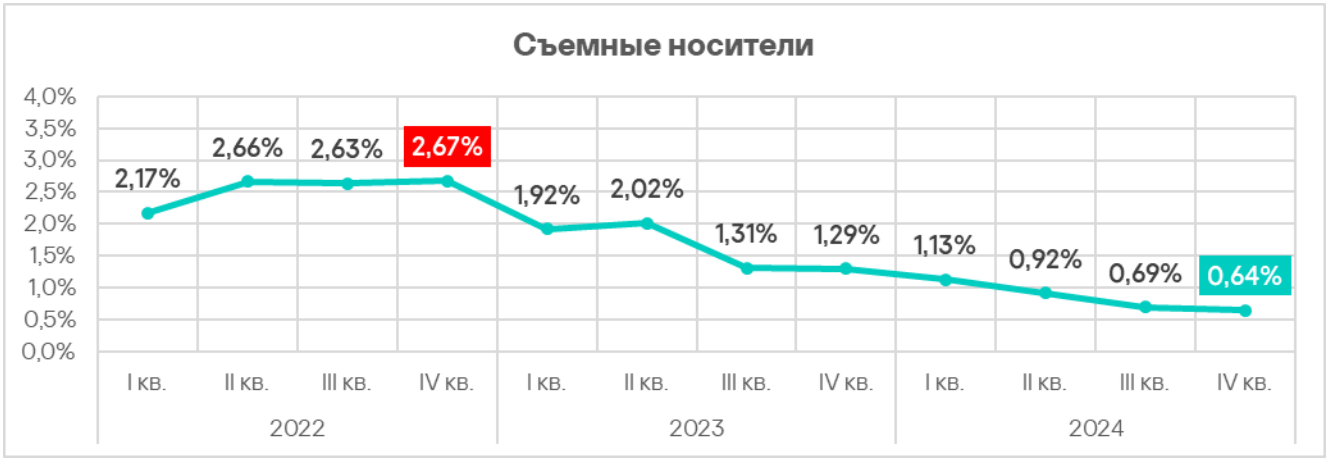
Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, почтовые клиенты и съемные носители. Отметим, что достоверно установить источники заблокированных угроз удается не во всех случаях.

В четвертом квартале 2024 года доля компьютеров АСУ, на которых были заблокированы угрозы из источников, рассмотренных в этом отчете, снизилась.

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



Показатели по всем рассматриваемым источникам достигли своих минимальных значений с начала 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 дает нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счет обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за ее объема и потребляемых ресурсов.

Переданная пользователем информация содержит только те типы и категории данных, которые описаны в соответствующем Соглашении KSN. Эти данные не только в значительной мере помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[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 автоматизации зданий;
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human machine interface (HMI);
- компьютеры, используемые для администрирования технологических сетей и сетей автоматизации зданий;
- компьютеры программистов АСУ/ПЛК.

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

Компьютеры, передающие нам статистику, принадлежат организациям из разных отраслей. Наиболее широко представлены химическая промышленность, металлургия, инжиниринг и интеграторы АСУ, нефтегазовая отрасль, энергетика, транспорт и логистика, пищевая промышленность, легкая промышленность и фармацевтическая отрасль. Сюда же входят системы инжиниринговых компаний и интеграторов АСУ, работающих с предприятиями в самых разных отраслях, а также системы управления зданиями, физической безопасности и обработки биометрических данных.

Атакованными мы считаем те компьютеры, на которых в течение исследуемого периода (на графиках выше это месяц, полугодие, год — в зависимости от контекста) защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете доли машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение исследуемого периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение исследуемого периода мы получали обезличенную информацию.

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