Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации

Третий квартал 2024

25.12.2024

Версия 1.1

Цифры квартала 3
Статистика по всем угрозам 4
Исследуемые отрасли 6
Разнообразие обнаруженных вредоносных объектов 7
Вредоносные объекты, используемые для первичного заражения 9
Ресурсы в интернете из списка запрещенных 11
Вредоносные скрипты и фишинговые страницы (JS и HTML) 12
Вредоносные документы (MSOffice + PDF) 14
Вредоносное ПО следующего этапа 15
Программы-шпионы 15
Программы-вымогатели 16
Майнеры — исполняемые файлы для ОС Windows 16
Веб-майнеры 17
Самораспространяющееся вредоносное ПО. Черви и вирусы 18
Черви 18
Вирусы 19
Вредоносные программы для AutoCAD 19
Основные источники угроз 20
Интернет 20
Почтовые клиенты 21
Съемные носители 21
Сетевые папки 22
Методика подготовки статистики 23

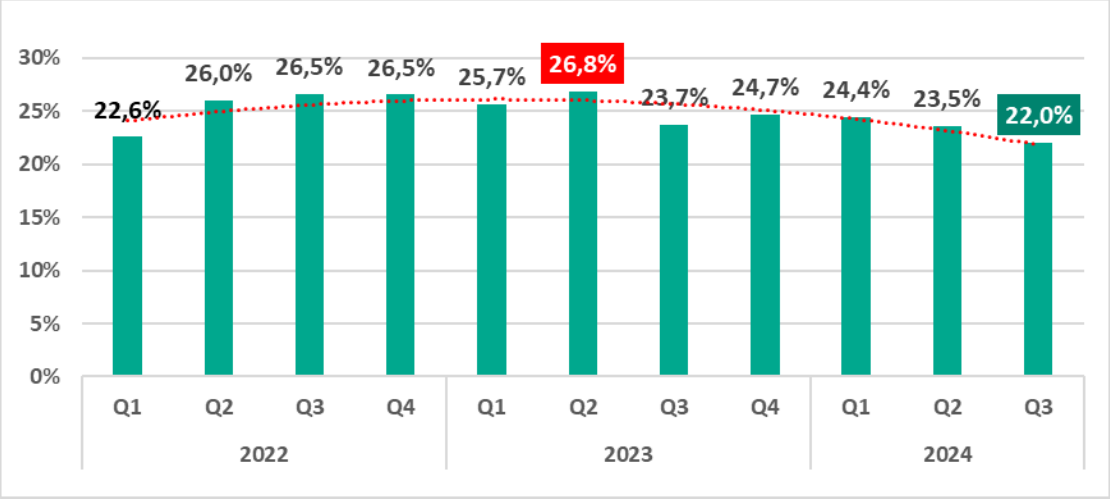
Цифры квартала

Показатель	II кв. 2024	III кв. 2024	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	23,5%	22,0%	-1,5 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Ресурсы в интернете из списка запрещенных	6,63%	6,84%	0,21 п. п.
Вредоносные скрипты и фишинговые страницы (JS и HTML)	5,69%	6,24%	0,55 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	4,08%	3,91%	-0,17 п. п.
Вредоносные документы (MSOffice + PDF)	1,96%	1,97%	0,01 п. п.
Вирусы (Virus)	1,54%	1,53%	-0,01 п. п.
Черви (Worm)	1,48%	1,30%	-0,18 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,89%	0,71%	-0,18 п. п.
Веб-майнеры, выполняемые в браузерах	0,50%	0,41%	-0,09 п. п.
Вредоносные программы для AutoCAD	0,42%	0,40%	-0,02 п. п.
Программы-вымогатели	0,18%	0,16%	-0,02 п. п.
Основные источники угроз			
Интернет	11,25%	10,84%	-0,41 п. п.
Почтовые клиенты	3,04%	2,95%	-0,09 п. п.
Съемные носители	0,92%	0,69%	-0,23 п. п.
Сетевые папки	0,13%	0,11%	-0,02 п. п.

Статистика по всем угрозам

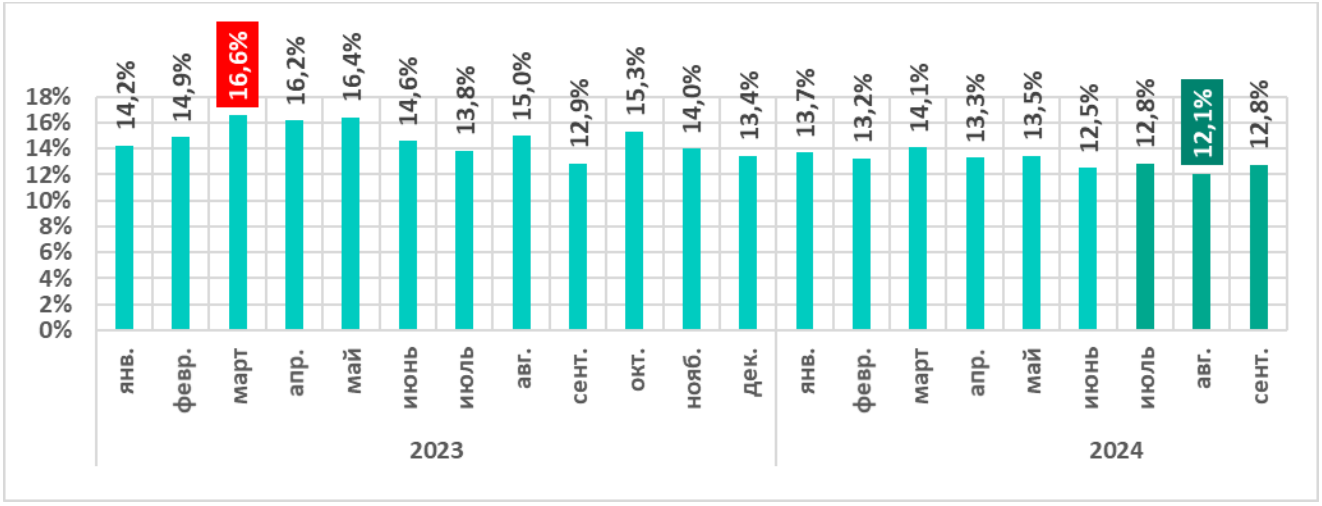
В третьем квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась по сравнению с предыдущим кварталом на 1,5 п. п. и составила 22,0%.

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



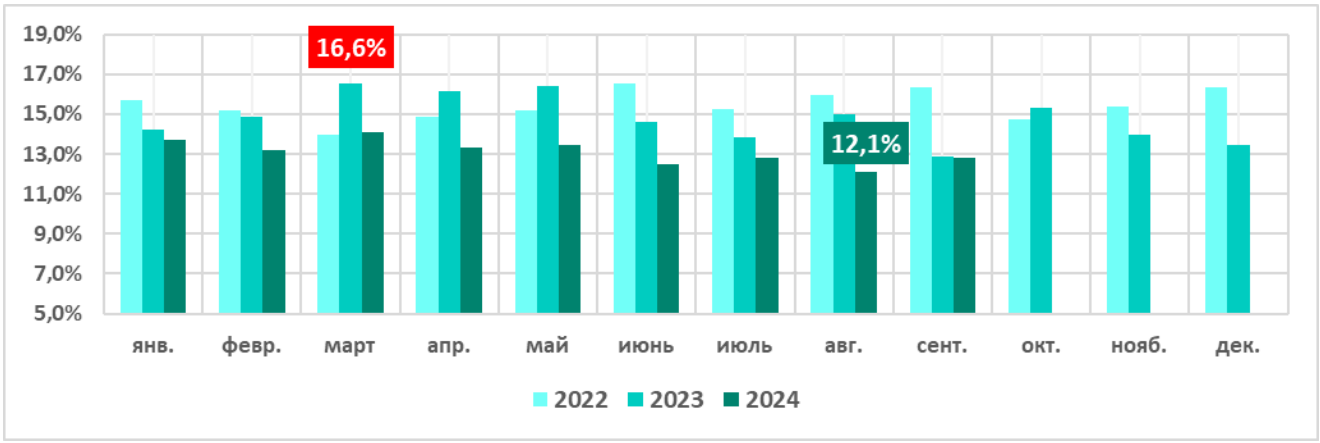
По сравнению с третьим кварталом 2023 года это значение уменьшилось на 1,7 п. п.

В течение третьего квартала 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, достигала наибольшего значения в июле и сентябре, а наименьшего — в августе. Более того, августовское значение — минимальное за весь период наблюдений.



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

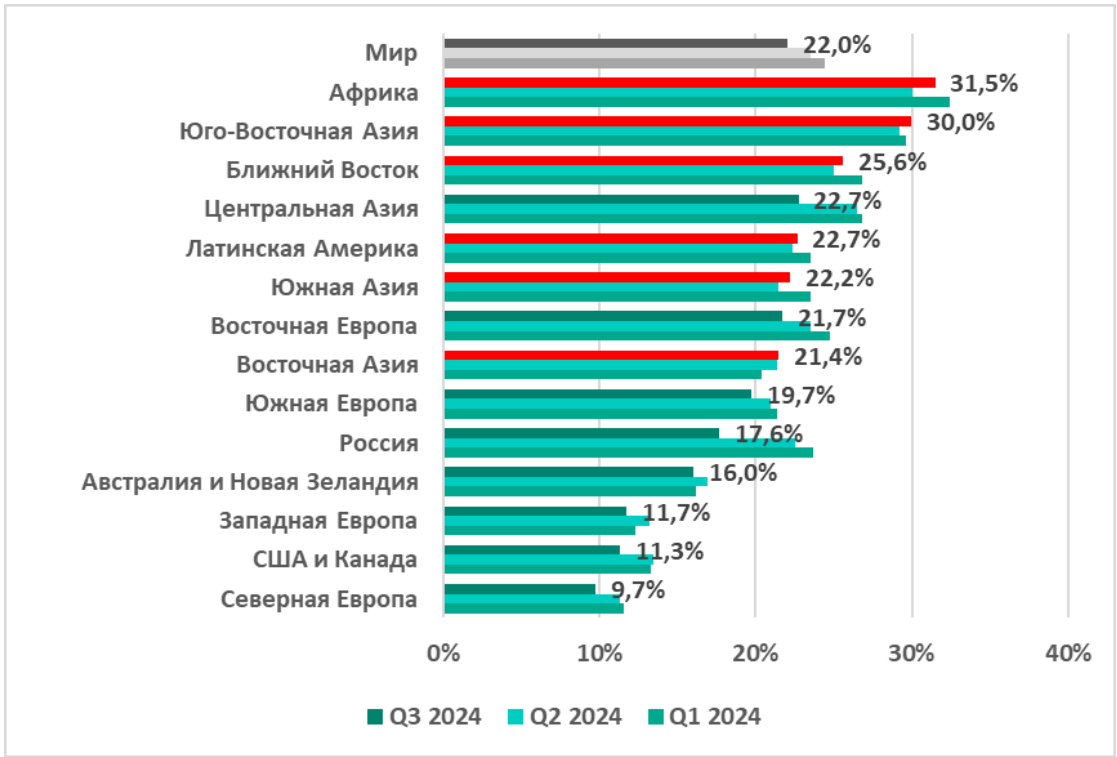
Месячные значения показателя в третьем квартала 2024 года меньше значений в те же месяцы предыдущего года.



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

В регионах[1] доля компьютеров АСУ, на которых в течение третьего квартала 2024 года были заблокированы вредоносные объекты, варьировалась от 9,7% в Северной Европе до 31,5% в Африке.

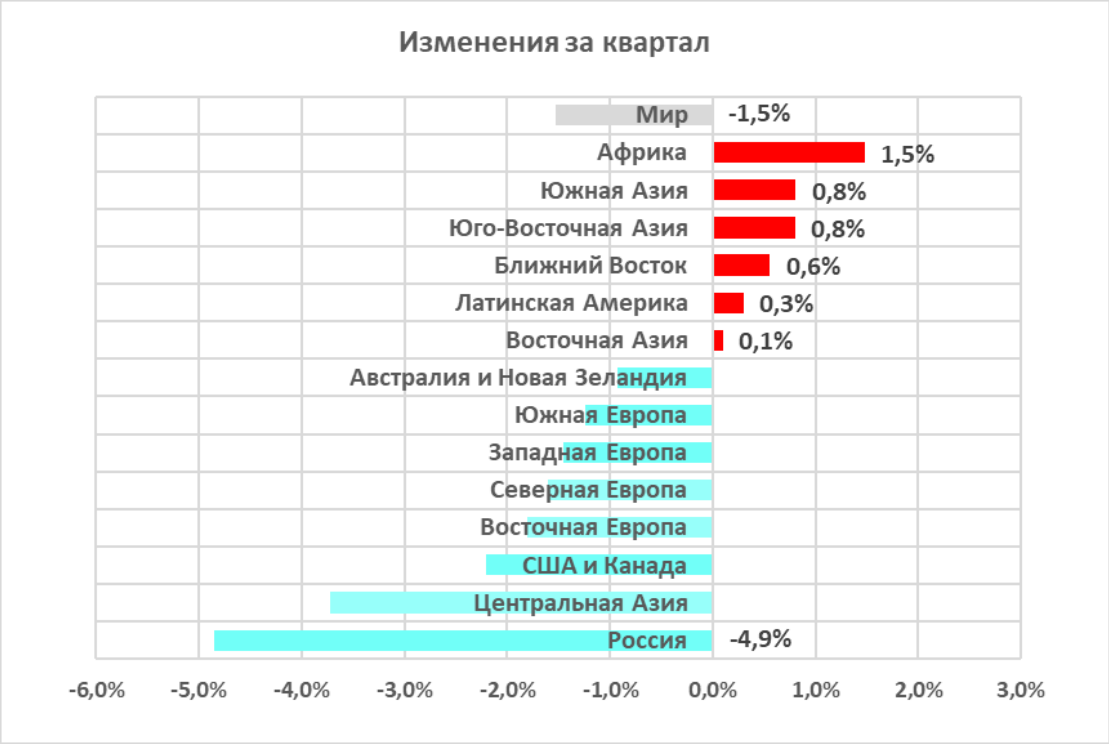
Рейтинг регионов по доле компьютеров АСУ, на которых были заблокированы вредоносные объекты в третьем квартале 2024 года



[1] В отчете учитывается статистика по США, полученная до 29 сентября 2024 года.

В шести регионах — Африке, Южной Азии, Юго-Восточной Азии, Латинской Америке, Восточной Азии, а также на Ближнем Востоке — показатели увеличились по сравнению с предыдущим кварталом.

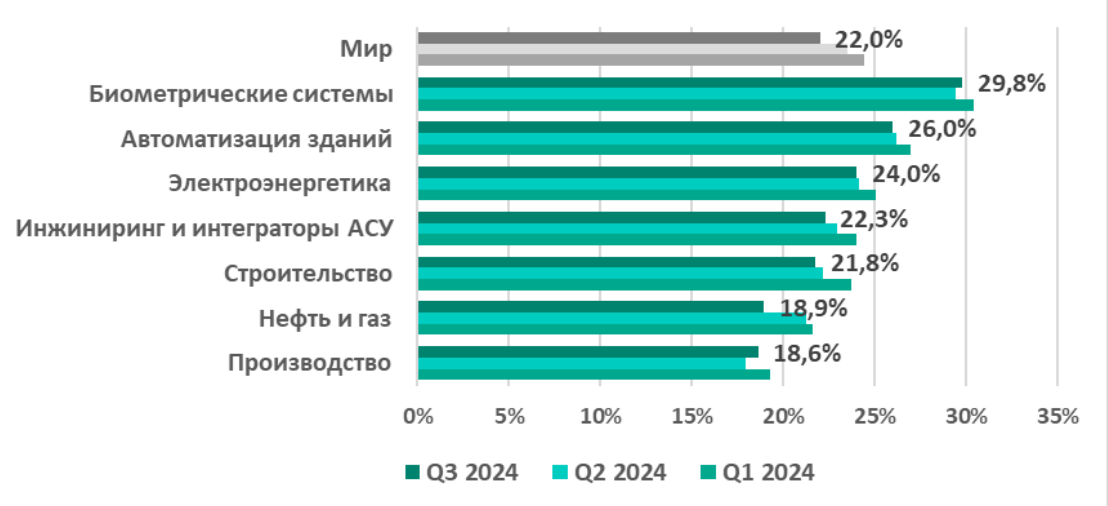
Регионы и мир. Изменение доли атакованных компьютеров за третий квартал 2024 года



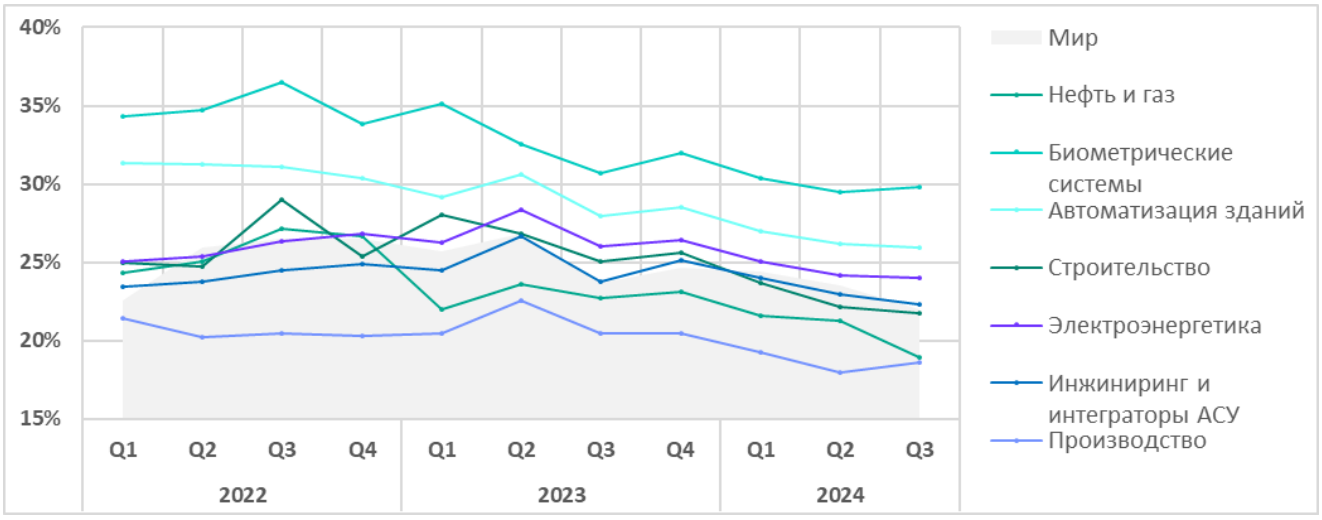
Исследуемые отрасли

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

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



В третьем квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшилась в большинстве отраслей, за исключением биометрических систем и производства.



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.

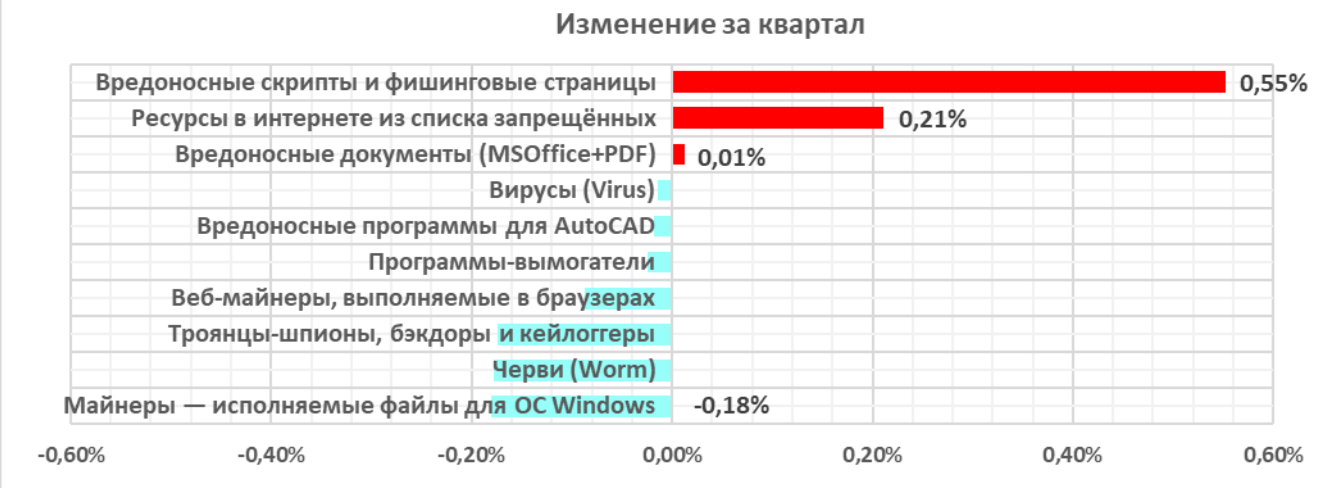
1. Вредоносные объекты, используемые для первичного заражения.
   Эта категория включает в себя ресурсы в интернете из списка запрещенных; вредоносные скрипты и фишинговые страницы; вредоносные документы.
2. Вредоносное ПО следующего этапа.
   Эта категория включает в себя программы-шпионы, программы-вымогатели, 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 третьем квартале 2024 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации заблокировано вредоносное ПО из 11 882 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[2], на которых была предотвращена активность вредоносных объектов различных категорий



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

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

На диаграмме выше видно, что доля вредоносных объектов, используемых для первичного заражения, увеличилась по сравнению со вторым кварталом 2024 года. Наиболее заметно (в 1,1 раза) выросла доля компьютеров АСУ, на которых были заблокированы **вредоносные скрипты и фишинговые страницы.**

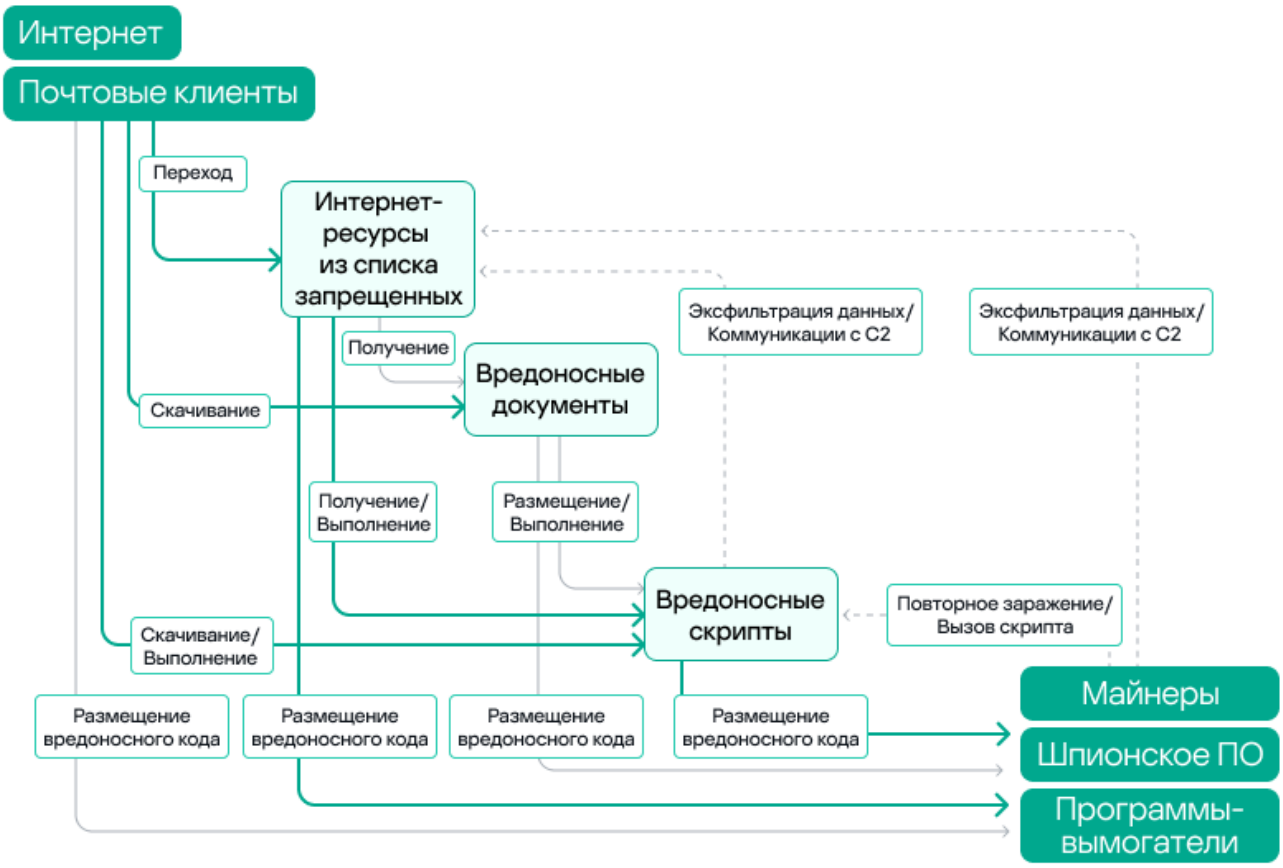
Вредоносные объекты, используемые для первичного заражения

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

Логика атак злоумышленников предполагает, что 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.



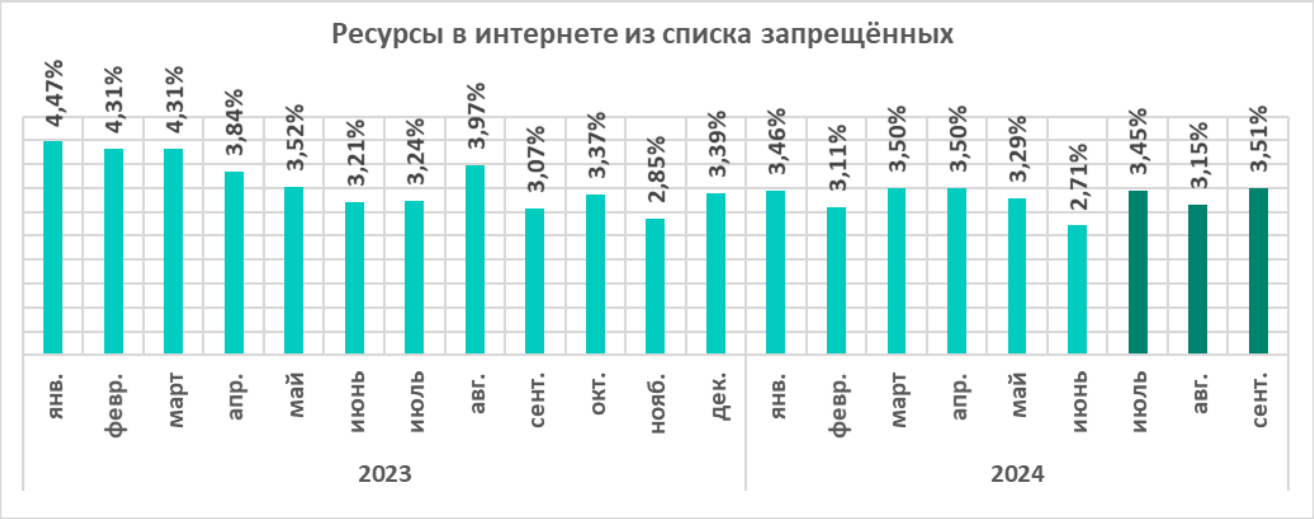
Цепочка атаки: от первичного заражения до вредоносного ПО следующего этапа

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 третьем квартале доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных, немного увеличилась, но в целом в 2024 году этот показатель стабилен.

На графике ниже видно, как ежемесячно в течение квартала менялась доля компьютеров АСУ, на которых были заблокированы ресурсы в интернете из списка запрещенных. Максимального (и наивысшего с сентября 2023 года) значения показатель достиг в сентябре 2024 года.



Значительное увеличение в июле доли компьютеров АСУ, на которых были заблокированы интернет-ресурсы из списка запрещенных, обусловлено

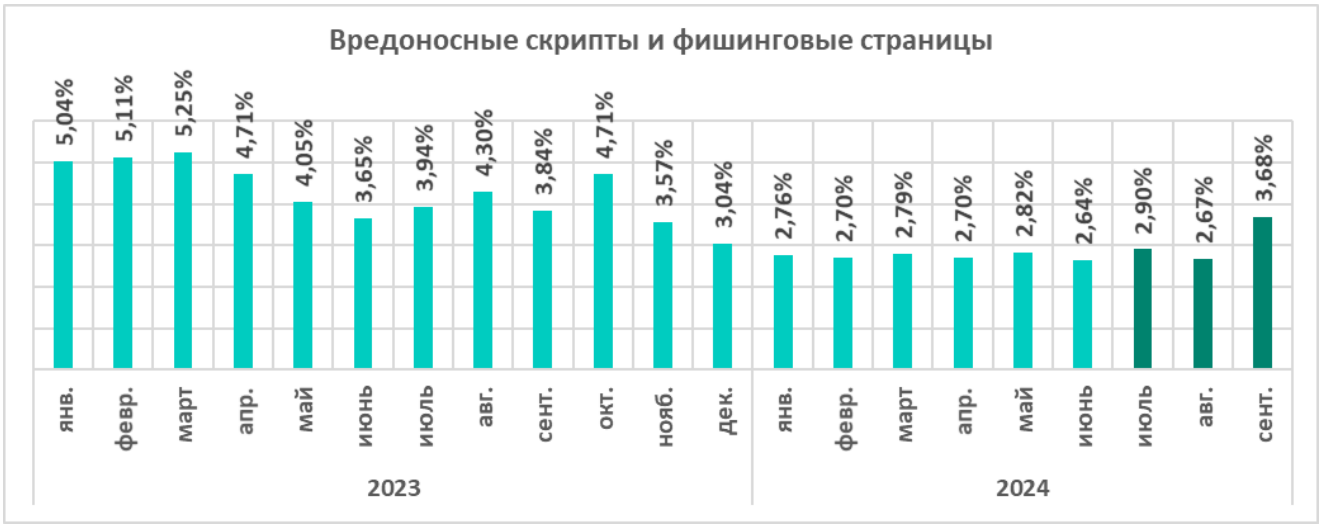
прежде всего ростом количества заново созданных вредоносных доменных имен и IP-адресов, которые киберпреступники использовали в качестве инфраструктуры управления (C2) для распространения вредоносных программ и фишинговых атак.

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 третьем квартале 2024 года доля компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, увеличилась после того, как в предыдущем квартале достигла минимального значения за весь рассматриваемый период.

Ежемесячное значение показателя колебалось в течение всего третьего квартала, достигнув в сентябре 2024 года наиболее высокого значения с ноября 2023 года.



Значительное увеличение доли компьютеров АСУ, на которых были заблокированы вредоносные скрипты и фишинговые страницы, вызвано серией широкомасштабных фишинговых атак в августе и сентябре 2024 года. В ходе этих атак злоумышленники использовали вредоносные скрипты, которые выполнялись в браузере, имитируя различные окна с CAPTCHA-подобными интерфейсами, сообщениями об ошибках браузера и аналогичными всплывающими окнами. Эти скрипты предназначены для того, чтобы обманом заставить пользователей следовать простым инструкциям, которые в конечном итоге запускают загрузку вредоносного ПО следующего уровня — стилер Lumma или троянец Amadey.

Фишинговые приманки распространялись по различным каналам, включая фишинговые электронные письма (например, поддельные уведомления об уязвимостях, якобы от GitHub) и вредоносные ссылки и вредоносную рекламу на файлообменных сервисах. Инструкции, предоставляемые фишинговыми скриптами, обманом заставляли пользователей выполнять вредоносные команды PowerShell для загрузки программ-шпионов.

Важно отметить, что и Lumma, и Amadey предназначены для кражи учетных данных из браузеров и менеджеров паролей. Кроме того, было замечено, что Amadey использует модули для кражи учетных данных из различных систем удаленного доступа к рабочему столу компьютера (VNC)[3].

Раскрытие этих учетных данных значительно повышает риск последующих атак, например с применением программ-вымогателей, поскольку злоумышленники могут использовать украденные данные для доступа к критическим системам и дальнейшей эскалации своих атак.

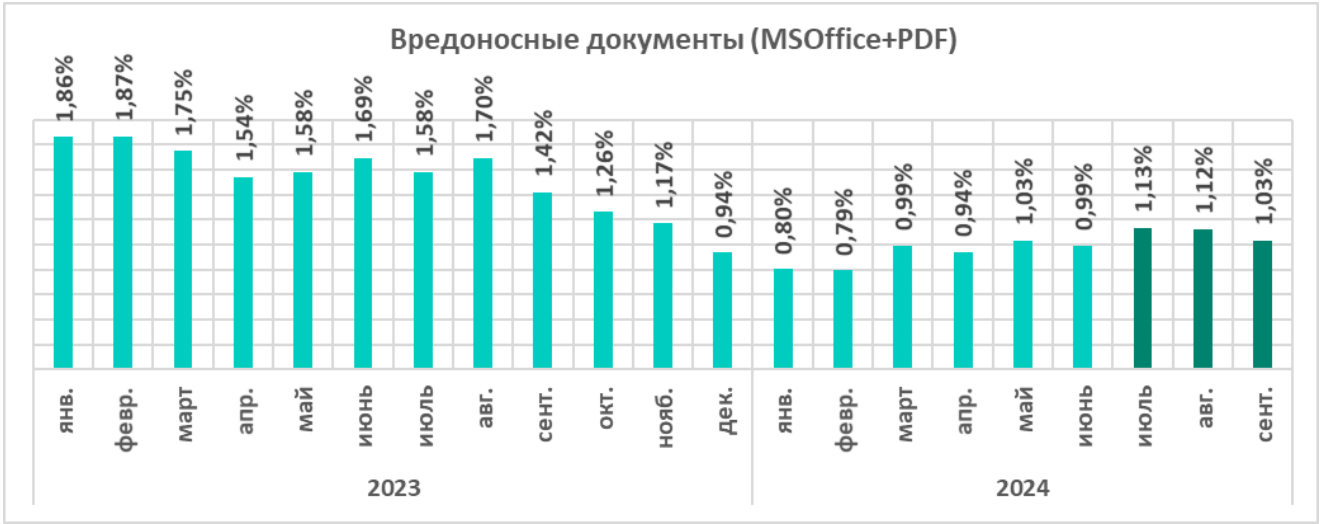
[3] Подробности — в статье «Lumma/Amadey: запусти шелл-код, чтобы доказать, что ты не робот» на сайте Securelist

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.

Доля компьютеров АСУ, на которых были обнаружены вредоносные документы, достигла максимального значения во втором квартале 2022 года и с тех пор преимущественно уменьшалась вплоть до второго квартала 2024 года, когда произошел рост показателя. Он незначительно увеличился и в третьем квартале.

Как показано на диаграмме ниже, в третьем квартале 2024 года наивысшего уровня доля компьютеров АСУ, на которых были обнаружены вредоносные документы, достигла в июле, после чего пошла на спад. Июльское значение — самое высокое, начиная с декабря 2023 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.

Программы-вымогатели

Доля компьютеров АСУ, на которых были заблокированы программы-вымогатели, продолжает колебаться от квартала к кварталу в пределах 0,03 п. п.

Майнеры — исполняемые файлы для ОС Windows

Доля компьютеров АСУ, на которых блокируются майнеры — исполняемые файлы для ОС Windows, была минимальной 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.

В третьем 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.

Веб-майнеры

Доля компьютеров АСУ, на которых были заблокированы веб-майнеры, в третьем 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.

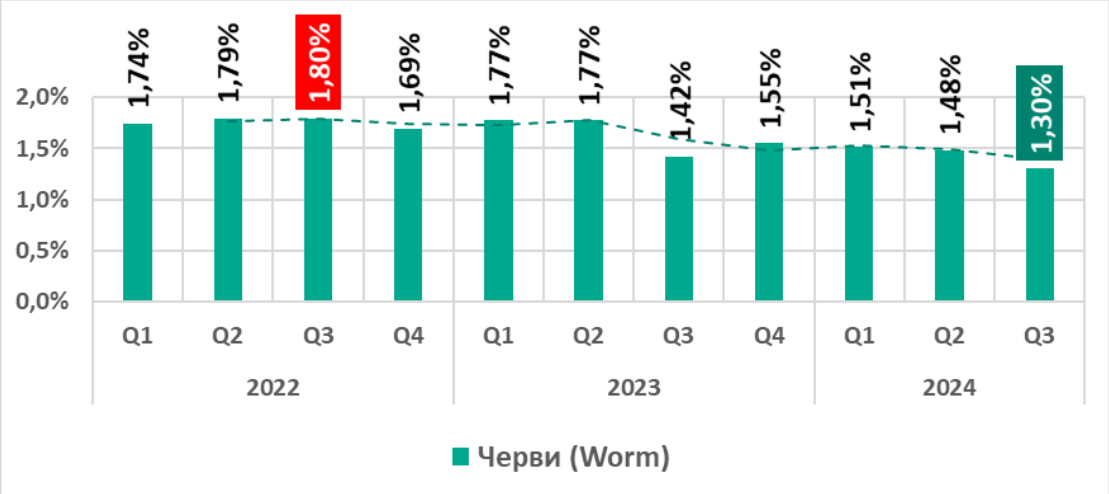
Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

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

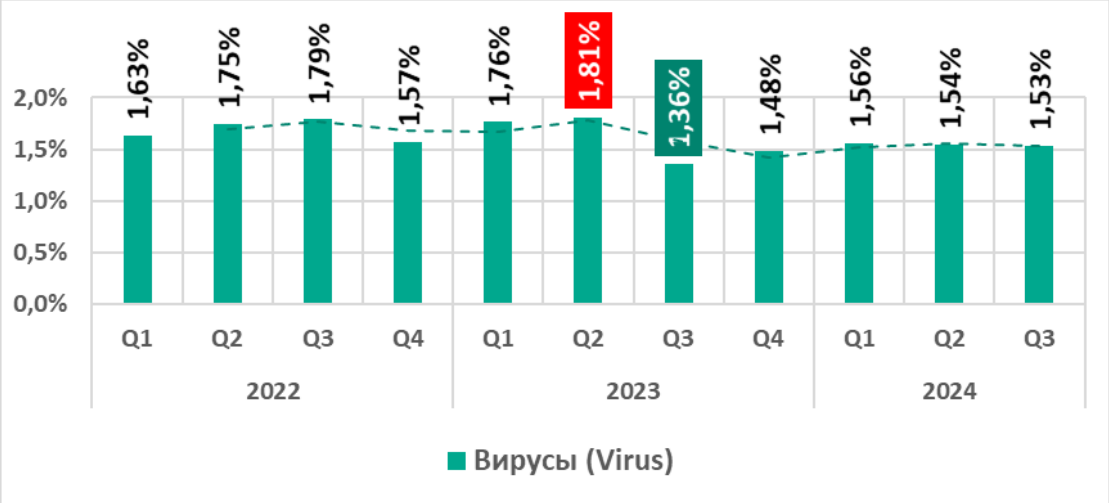
В сетях АСУ встречаются новые версии червей, используемые злоумышленниками для распространения шпионского ПО, программ-вымогателей и майнеров. Чаще всего эти черви используют эксплойты известных уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

В третьем квартале 2024 года доля компьютеров АСУ, на которых были заблокированы черви, уменьшилась и достигла минимума за весь рассматриваемый период.



Вирусы

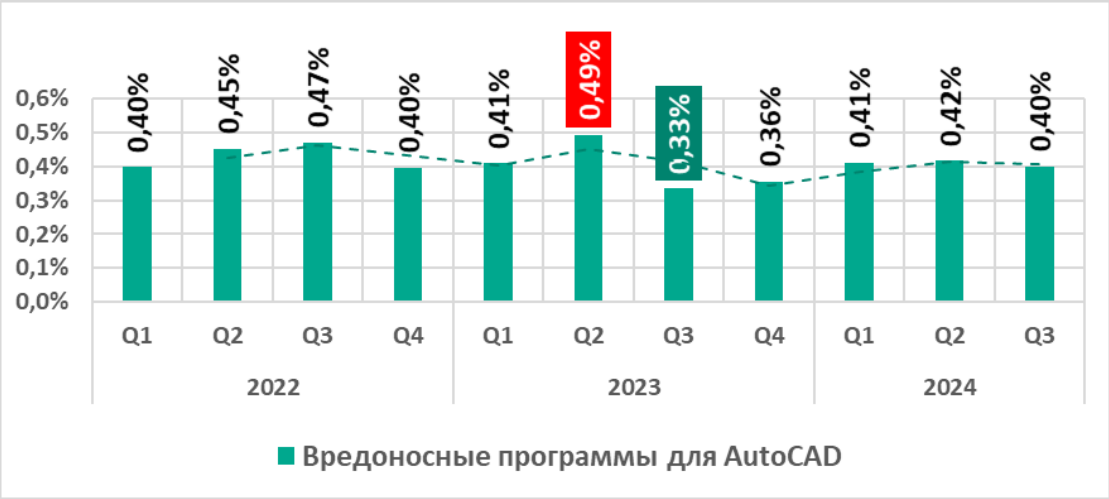
Доля компьютеров АСУ, на которых были заблокированы вирусы, в третьем квартале 2024 года немного сократилась.



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 третьем квартале 2024 года доля компьютеров АСУ, на которых было заблокировано вредоносное ПО для AutoCAD, немного уменьшилась.

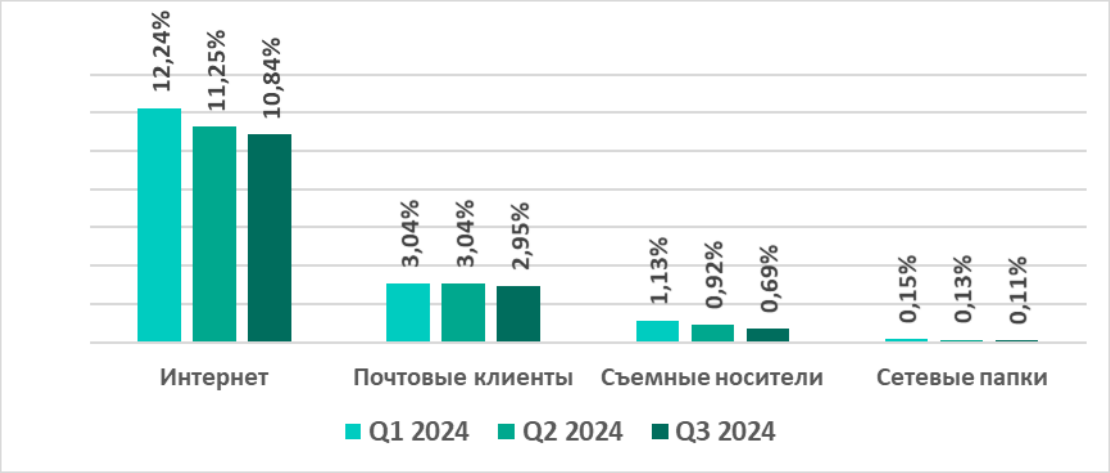


Основные источники угроз

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 третьем квартале 2024 года доли компьютеров АСУ, на которых были заблокированы угрозы из источников, рассмотренных в этом отчете, снизились.

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



Интернет

Почтовые клиенты

Доля компьютеров АСУ, на которых были заблокированы угрозы из почтовых клиентов, в третьем квартале 2024 года достигла минимального значения за рассматриваемый период.

Съемные носители

Доля компьютеров АСУ, на которых были заблокированы угрозы со съемных носителей, в третьем квартале также оказалась минимальной за весь рассматриваемый период.

Сетевые папки

Сетевые папки — незначительный источник угроз. Доля компьютеров АСУ, на которых были заблокированы угрозы в сетевых папках, также достигла минимума, начиная 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 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[4].

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.

[4] 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