Kaspersky ICS CERT

kaspersky

Динамика внешних и внутренних угроз АСУ

Второй квартал 2025 года

10.09.2025

Версия 1.0

Цифры

Показатель	I кв. 2025	II кв. 2025	Изменения за квартал
Доля атакованных компьютеров АСУ в мире	21,9%	20,5%	▼1,4 п. п.
Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий			
Вредоносные скрипты и фишинговые страницы	7,16%	6,49%	▼0,67 п. п.
Ресурсы в интернете из списка запрещенных	5,12%	5,91%	▲0,79 п. п.
Троянцы-шпионы, бэкдоры и кейлоггеры	4,20%	3,84%	▼0,36 п. п.
Вредоносные документы (MSOffice+PDF)	1,85%	1,97%	▲0,12 п. п.
Вирусы (Virus)	1,53%	1,29%	▼0,24 п. п.
Черви (Worm)	1,31%	1,22%	▼0,09 п. п.
Майнеры — исполняемые файлы для ОС Windows	0,78%	0,63%	▼0,15 п. п.
Веб-майнеры, выполняемые в браузерах	0,53%	0,30%	▼0,23 п. п.
Вредоносные программы для AutoCAD	0,34%	0,29%	▼0,05 п. п.
Программы-вымогатели	0,16%	0,14%	▼0,02 п. п.
Основные источники угроз			
Интернет	10,11%	9,76%	▼0,35 п. п.
Почтовые клиенты	2,81%	3,06%	▲0,25 п. п.
Съемные носители	0,52%	0,37%	▼0,15 п. п.
Сетевые папки	0,07%	0,05%	▼0,02 п. п.

Изменения за квартал

Во втором квартале 2025 года баланс сил в противостоянии киберугрозам продолжает смещаться в пользу промышленных предприятий — в основном за счет внедрения мер проактивной защиты и блокирования угроз на ранних этапах. Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, снизилась до минимального за последние несколько лет значения — 20,5%.

С практической точки зрения, опасность конкретной угрозы для компьютера АСУ и технологической сети в целом зависит от контекста, который определяется ответами на следующие вопросы:

- К какому этапу kill-chain относится заблокированная угроза? Это только загрузчик или уже шифровальщик?
- Была ли угроза заблокирована на периметре сети или уже в ее глубине?

Периметр сети, строго говоря, — это не только системы, доступные напрямую из интернета (таких, к слову сказать, осталось уже совсем немного), но и все те компьютеры внутри ОТ (включая ноутбуки), которые имеют доступ к интернету – веб-сайтам, мессенджерам и почте. Соответственно, если угроза заблокирована при попытке доступа к вредоносному веб-адресу, при загрузке вредоносного объекта из интернета или когда пользователь открывает фишинговое сообщение из электронной почты, то можно считать, что защищаемый компьютер находится на периметре сети.

Очевидно, что если угрозы заблокированы не на периметре, а уже внутри промышленной сети, то они несут более высокий риск. Обычно «внутри промышленной сети» означает, что угроза обнаружена и заблокирована в одной из следующих локаций:

- в оперативной памяти ОТ-компьютера;
- на его жестком диске;
- на сетевом диске;
- на подключенном к нему USB-устройстве.

> Рост активности вредоносного ПО в той части технологической сети, где информация из интернета доступна только оффлайн (распространяется на съемных носителях и через сетевые диски), – это признак проникновения угроз снаружи вглубь сети, например, в ходе фишинговой кампании или всплеска распространения вирусов. Очевидно, это сигнал задуматься, как эти угрозы смогли попасть внутрь, почему они не были заблокированы на более ранних этапах. Возможно, не все компьютеры внутри OT-сети надежно защищены и не все политики ИБ эффективно контролируются.

Множества угроз в технологической сети

Как было упомянуто выше, степень опасности, которую представляет собой угроза, сильно зависит от контекста.

Чтобы проследить за проникновением различных угроз от периметра вглубь сети, мы разделили компьютеры АСУ, на которых были заблокированы угрозы во втором квартале 2025 года (20,5% от всех), на три множества.

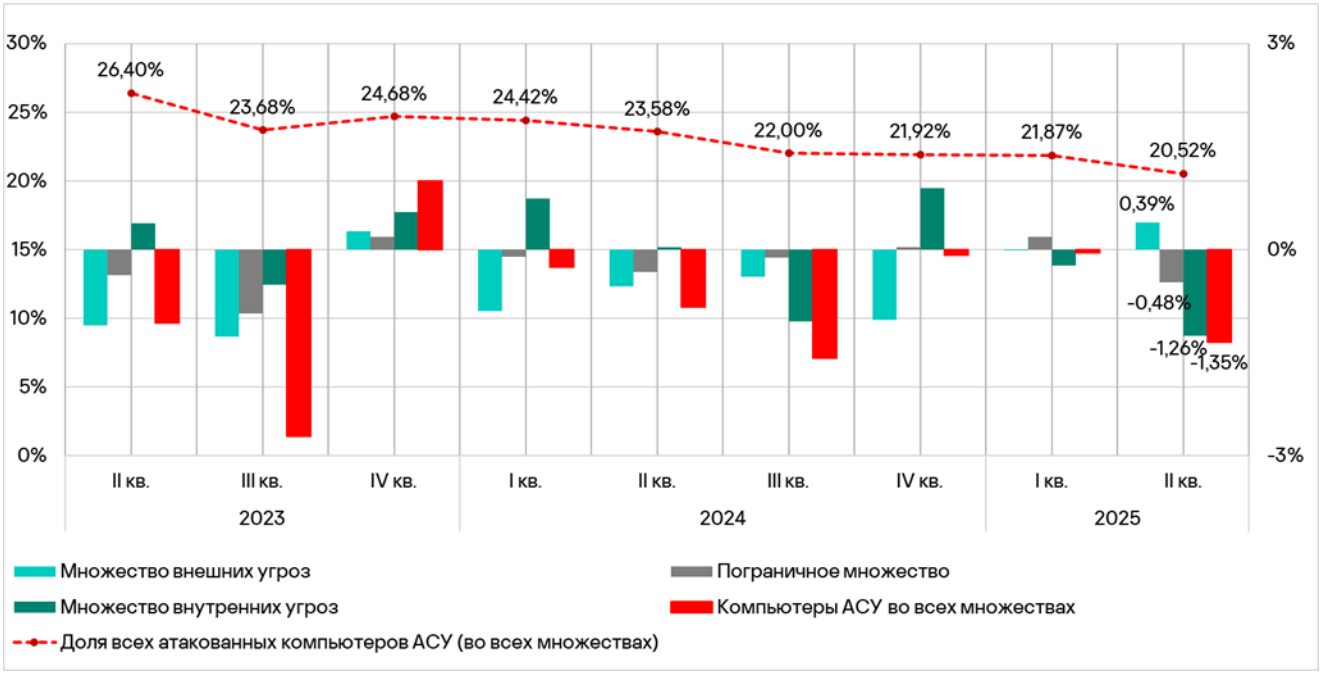
1. «Множество внешних угроз» — это компьютеры АСУ, на которых были заблокированы только внешние угрозы, доставляемые через интернет и корпоративную почту. Можно предположить, что, несмотря на доступность внешним угрозам, эти компьютеры оказались достаточно защищены. Атака не получила развитие. Очевидно, для уменьшения поверхности атаки и уменьшения вероятности развития атак необходимо приложить усилия для сокращения этого множества. Такие компьютеры составляют 8,94% от всех компьютеров АСУ.
2. «Пограничное множество» — это компьютеры АСУ, на каждом из которых были заблокированы как внешние, так и внутренние угрозы. Это тоже часть периметра сети. Однако на этих компьютерах средства защиты от попыток первоначального проникновения, возможно, не всегда срабатывали эффективно. Возможно, эти компьютеры столкнулись с более свежими или сложными векторами атак. Стоит обратить на такие компьютеры более пристальное внимание, чтобы разобраться в причинах такой ситуации и исключить возможность компрометации ОТ-сети. Возможно, уже имеются признаки инцидента ИБ. На такие компьютеры приходится 3,35% от всех компьютеров АСУ.
3. «Множество внутренних угроз» — это компьютеры АСУ, на которых были заблокированы только внутренние угрозы, в памяти компьютера АСУ, на локальных, съемных и сетевых дисках. Вне зависимости от того, как близко они находятся к периметру сети, эти компьютеры оказались доступны для развития атаки. Часть из них на самом деле может относиться ко второму (пограничному) множеству, ведь далеко не для всех угроз удается установить истинный вектор проникновения (например, скачав зашифрованный документ или защищенный паролем архив, обнаружить признаки угрозы в нем получится только после попытки его расшифровать / разархивировать). Все такие случаи также надо классифицировать и обработать команде ИБ организации в зависимости от того, что за угроза была обнаружена, и с учетом специфики информационных

систем. На такие компьютеры приходится 8,23% от всех компьютеров АСУ.

Статистика по каждому из этих сегментов по отдельности и в сравнении позволяет лучше понять ландшафт угроз АСУ и увидеть факторы, которые на него влияют.

На диаграмме ниже показано, как менялась доля компьютеров АСУ, на которых блокировались угрозы, для каждого из трех множеств. Чтобы оценить вклад каждого из множеств в общий процент атакованных компьютеров АСУ, мы использовали две оси на графике:

- левая ось и показатели на кривой отмечают долю компьютеров АСУ, на которых были заблокированы вредоносные объекты во всех множествах;
- правая ось и показатели столбиков гистограммы отражают изменение доли компьютеров АСУ (разницу от квартала к кварталу) для каждого из множеств по отдельности, а также суммы по всем множествам:
  - светло-зеленый цвет – множество внешних угроз;
  - серый цвет – пограничное множество;
  - темно-зеленый цвет – множество внутренних угроз;
  - красный цвет – все множества в совокупности.



Как видно на графике, снижение доли атакованных компьютеров АСУ во втором квартале 2025 года на фоне роста множества внешних угроз обусловлено уменьшением доли атакованных компьютеров АСУ, составляющих пограничное множество и множество внутренних угроз.

Рассмотрим угрозы в каждом из обозначенных множеств в разрезе категорий угроз, которые, отчасти, помогают определить, к какому шагу в kill-chain относится заблокированная угроза.

Категории угроз

Когда на компьютере блокируется доступ к вредоносному веб-адресу, веб-скрипту, фишинговой странице или почтовому вложению – это вероятное свидетельство начального этапа атаки. В то же время блокирование скриптов для популярных интерпретаторов (wscript, cmd, vbs, PowerShell, Python, AutoList и так далее), шпионского ПО, майнеров и программ-вымогателей может быть признаком следующего этапа атаки.

Прежде чем двинуться дальше, необходимо отметить три обстоятельства.

1. Не все угрозы удается классифицировать и определить для них точную категорию – компьютеры, на которых блокировались такие угрозы, в этом отчете представлены в виде отдельной группы «Угрозы, тип которых не определен»;
2. Больше чем на половине атакованных компьютеров АСУ за квартал блокировалась угроза только одной категории. Это позволяет использовать метод Монте-Карло для оценки того, к каким категориям угроз вероятнее всего относятся те угрозы, тип которых не определен.
3. Чуть меньше чем на половине атакованных компьютеров АСУ в течение квартала блокировались угрозы разных категорий. Эти компьютеры представляются наиболее проблемной областью с точки зрения ИБ, поскольку во многих случаях наличие множества разных угроз свидетельствует о скрытой активности вредоносного ПО. В этом отчете они представлены в виде отдельной группы «Комбинация двух и более категорий угроз»

На тепловой карте ниже различные категории вредоносного ПО показаны в разрезе описанных выше множеств компьютеров АСУ. Проценты в ячейках – это доли компьютеров АСУ, на которых были заблокированы соответствующие угрозы в соответствующих множествах. Сумма долей по всем категориям во всех сегментах равна 20,5% – то есть суммарной доле компьютеров АСУ, на которых было заблокировано вредоносное ПО во втором квартале 2025 года.

Категории угроз	Множество внешних угроз	Пограничное множество	Множество внутренних угроз
Вредоносные веб-адреса	2,77%	0,02%	0,28%
Вредоносные скрипты	2,30%	0,04%	0,22%
Угрозы, тип которых не определен	0,79%	0,26%	4,23%
Вредоносные документы (MSOffice + PDF)	0,21%	0,02%	0,06%
Шпионское ПО	0,09%	0,01%	0,37%
Веб-майнеры	0,01%	0,00%	0,00%
Вирусы	0,01%	0,01%	0,28%
Черви	0,00%	0,00%	0,21%
Исполняемые майнеры для ОС Windows	0,00%	0,00%	0,07%
Программы-вымогатели	0,00%	0,00%	0,01%
Вредоносное ПО для AutoCAD	0,00%	0,00%	0,01%
Комбинация двух и более категорий угроз	2,74%	2,49%	2,99%
Все угрозы	8,94%	3,35%	8,23%

Как видно на карте, угрозы разных типов неравномерно распределены по трем множествам.

Так, на компьютерах во множестве внешних угроз значительно больше угроз первого этапа, в то время как во множестве внутренних угроз – вредоносное ПО следующего этапа, часть которого скрывается среди угроз, тип которых не определен.

Такое распределение иллюстрирует процесс просачивания угроз следующего этапа вглубь сети, то есть переход от этапа первичного проникновения к следующему шагу, а в случае блокирования программам-вымогателей – к финальному.

Посмотрим, как от квартала к кварталу менялись показатели категорий вредоносного ПО на компьютерах АСУ в каждом отдельном множестве.

Внешние угрозы

Для начала рассмотрим статистику, полученную с компьютеров из множества внешних угроз, – то есть группы компьютеров АСУ, на которых были заблокированы только внешние угрозы (из почты или интернета).

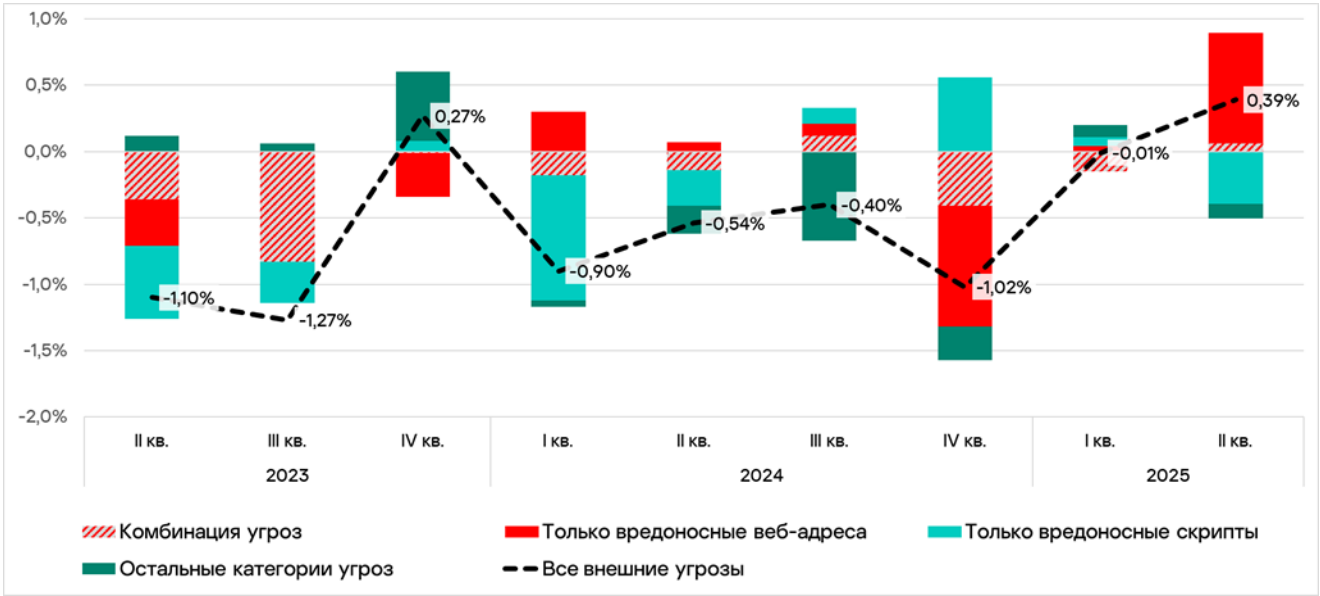
Во втором квартале 2025 года доля компьютеров АСУ, на которых блокировались только внешние угрозы, выросла на 0,39 п. п. по сравнению с первым кварталом.

На графике ниже показано изменение этого показателя от квартала к кварталу (черная пунктирная линия). Также показаны категории угроз, которые оказывают наибольшее влияние на показатель внешних угроз:

- вредоносные веб-адреса (показатели отмечены красным);
- вредоносные скрипты (показатели отмечены светло-зеленым).

Вклад компьютеров АСУ, на которых были заблокированы другие категории вредоносного ПО — только вредоносные документы, только шпионское ПО, только майнеры и т. д., — оказался небольшим, поэтому на графике ниже они объединены в группу «Остальные категории угроз» (отмечены темно-зеленым).

Показатели компьютеров АСУ, на каждом из которых за квартал были заблокированы угрозы двух и более категорий угроз, обозначены на графике как «Комбинация угроз» (красная штриховка).



Рост показателя веб-адресов связан с добавлением в списки «Лаборатории Касперского» вредоносных URL большого количества прямых ссылок на вредоносные коды, размещаемые на серверах публичных интернет-площадок, мессенджеров и файловых сервисов.

Создание множества уникальных ссылок на вредоносное ПО, хранящееся на легитимных публичных ресурсах и доступное по заданному веб-адресу, – для злоумышленников дело весьма простое. Для этого достаточно зарегистрировать почтовый аккаунт или купить виртуальный телефонный номер.

А вот обнаружение новых вредоносных ссылок, напротив, задача довольно непростая и ресурсоемкая. Например, чтобы найти новую вредоносную ссылку, нужно поймать доставляемый при обращении к ней экземпляр вредоносного ПО, либо обнаружить и исследовать экземпляр вредоносного ПО, ее использующий.

На графике ниже представлена динамика доли компьютеров АСУ, на которых были заблокированы:

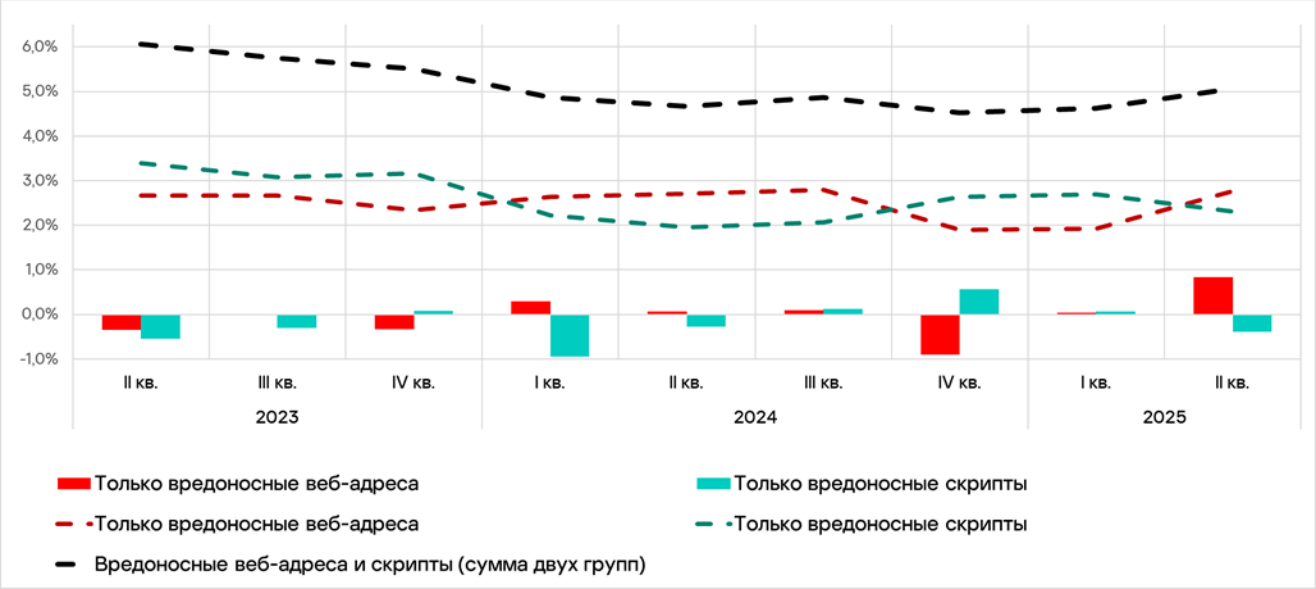
- только вредоносные веб-адреса (красная пунктирная линия);
- только вредоносные скрипты (зеленая пунктирная линия);
- суммарные показатели компьютеров АСУ из обеих групп (черная пунктирная линия).

Изменения показателей компьютеров АСУ в соответствующих группах отражены на гистограмме (красные и зеленые столбики).

На графике можно видеть, начиная с третьего квартала 2023 года, подъемы и спады показателей на протяжении одного-двух кварталов, отражающие время жизни двух типов атак (зеленая линия выше красной), в ходе которых были использованы разные техники первичного заражения. На эту динамику очевидным образом влияют не только возможности злоумышленников, но и изменения в методах детектирования угроз.

Так, в четвертом квартале 2023 года активно использовались для заражения сайтов уязвимости в WordPress, вредоносная кампания известна под названием Balada Injector. Соответственно, выросла доля компьютеров АСУ, на которых блокировались вредоносные веб-адреса.

В четвертом квартале 2024 года и первом квартале 2025 года активно распространялись фишинговые скрипты, направленные на заражение пользователей шпионским ПО. Вредоносная кампания известна под названиями FakeCaptcha и ClickFix. Соответственно, выросла доля компьютеров АСУ, на которых блокировались вредоносные скрипты.



Как видно на графике, показатели этих двух групп связаны. Снижение в группе только вредоносных скриптов во многом обусловлено блокированием веб-адресов, на которых размещаются скрипты для создания фишинговых страниц и всплывающих сообщений. Такого рода фишинг — под видом капчи, заявления от техподдержки, сообщения от полиции и тому подобное — активно используется злоумышленниками для того, чтобы убедить пользователя выполнить инструкцию по самозаражению компьютера (в том числе с использованием популярных легитимных приложений для удаленного администрирования — Remote Access Tool).

Внутренние угрозы

Далее посмотрим статистику в сегменте внутренних угроз. Во втором квартале 2025 года доля атакованных компьютеров АСУ в этом сегменте уменьшилась на 1,26 п. п. Значительный вклад в изменение показателя, как показано на графике ниже, внесли компьютеры, на которых блокировались:

- две и более категорий угроз (комбинация угроз, красная штриховка);
- угрозы, категория которых не определена (серый цвет).

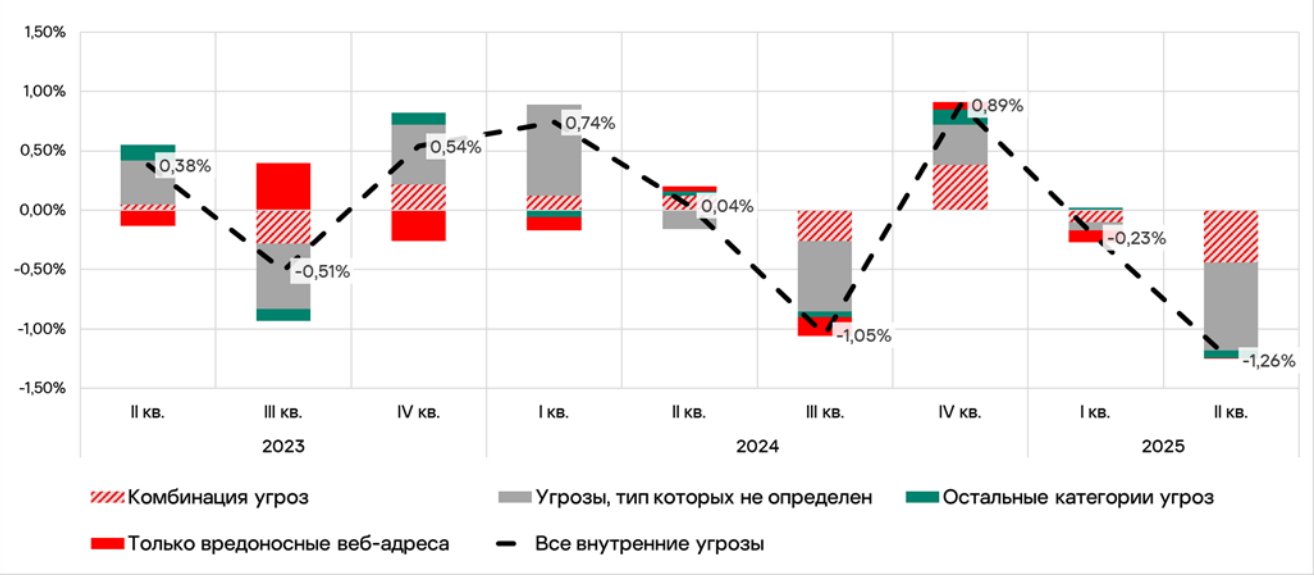
На графике также отдельно показан вклад категории «Только вредоносные веб-адреса» (красный цвет).

Тут важно пояснить, что категория вредоносных веб-адресов во внутреннем сегменте ОТ, где нет интернета и почты, — это вредоносные адреса, которые обнаруживаются при сканировании реестра, а не блокируются при попытке доступа в интернет.

Можно констатировать, что компьютеры АСУ из множества внутренних угроз могут стать доступными для внешних угроз. Так, в периоды обслуживания, компьютер не имеющий доступ в интернет, может его получить. То же касается и ноутбуков инженеров, которые могут оказываться в сети различных объектов, в корпоративной и публичных сетях.

Нередко бывает, что такие компьютеры более уязвимы для угроз из интернета и почты, чем компьютеры из множества внешних угроз – просто потому, что на «внутренних» компьютерах АСУ используется устаревшее ПО, обновление которого невозможно, невыгодно или не является приоритетом.

Доли остальных категорий угроз значительно не изменились, и их суммарное значение в общем изменении составило всего -0.07 п. п.



Также на графике можно отметить следующие особенности:

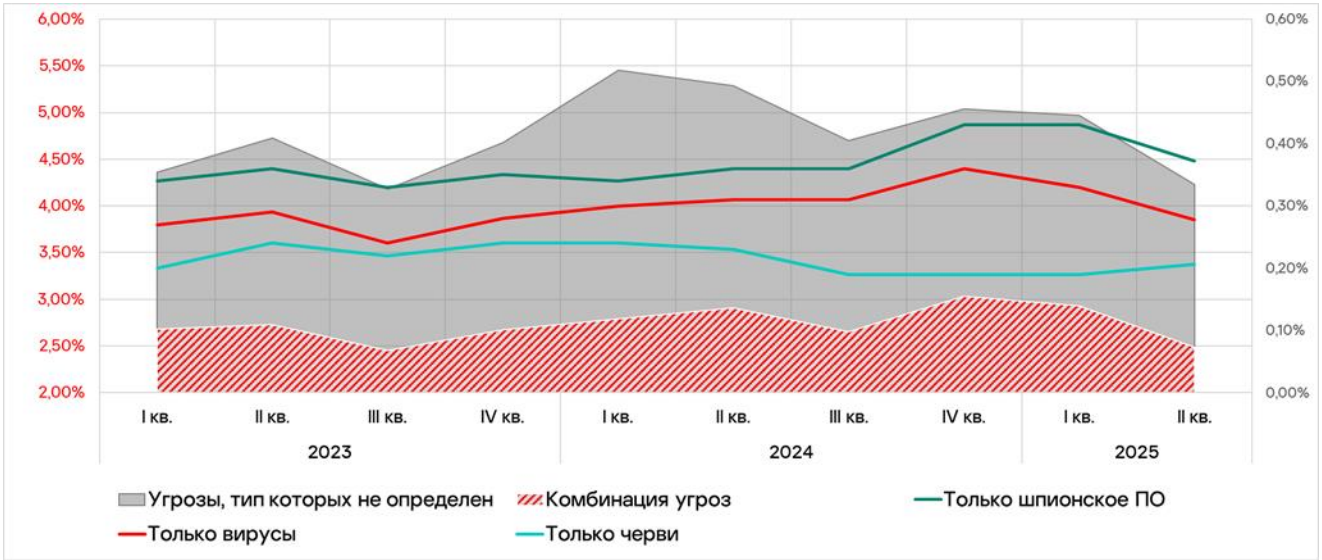
- цикличность подъемов и спадов среди всех угроз, что характерно для циклов активности самораспространяющегося ПО (локальных заражений);
- влияние вредоносных веб-адресов на изменение доли всех атакованных компьютеров во множестве внутренних угроз хаотично и затухает, эта категория в меньшей степени похожа на группу угроз, тип которых не определен;
- заметное влияние угроз, тип которых не определен, а также комбинации нескольких угроз на итоговое значение доли атакованных компьютеров во множестве внутренних угроз;

- положительная корреляция (с параметрами R=0,8, p<0,005) между группой компьютеров, на которых блокировались только угрозы, тип которых не определен, и группой компьютеров с комбинацией угроз – другими словами, вероятно, это очень похожие компьютеры АСУ.

Если сравнить изменения показателей категорий «Вирусы», «Шпионское ПО» и «Черви» с изменением доли компьютеров АСУ, на которых блокировались только неизвестные угрозы, то обнаружится, что сходство весьма велико (в случае вирусов коэффициент корреляции равен R=0,67, при p<0,005). Такое же сильное сходство наблюдается и при сравнении с компьютерами, на каждом из которых были заблокированы угрозы разных категорий (комбинация угроз).

На графике ниже:

- левая ось и две области отражают динамику изменения доли компьютеров АСУ, на которых были заблокированы:
  - угрозы, тип которых не определен (серый цвет);
  - комбинации различных угроз (красная штриховка);
- правая ось и линии отмечают динамику доли компьютеров АСУ, на которых были заблокированы категории угроз:
  - шпионское ПО;
  - вирусы;
  - черви.



Таким образом, в случаях, когда на компьютере АСУ во множестве внутренних угроз блокируется более одной угрозы, или категория угрозы не определена, с большой вероятностью блокируются вирусы, черви и шпионское ПО.

В итоге мы можем прийти к выводу, что снижение доли атакованных компьютеров АСУ во втором квартале 2025 года во множестве внутренних угроз связано со снижением доли компьютеров АСУ, зараженных шпионским ПО и вирусами.

Также весьма вероятно, что проактивное блокирование вредоносных веб-адресов во множестве внешних угроз, а также различных угроз следующего этапа в пограничном множестве (см. далее в отчете) позволило снизить поток вредоносного ПО, которое просачивается вглубь технологической сети.

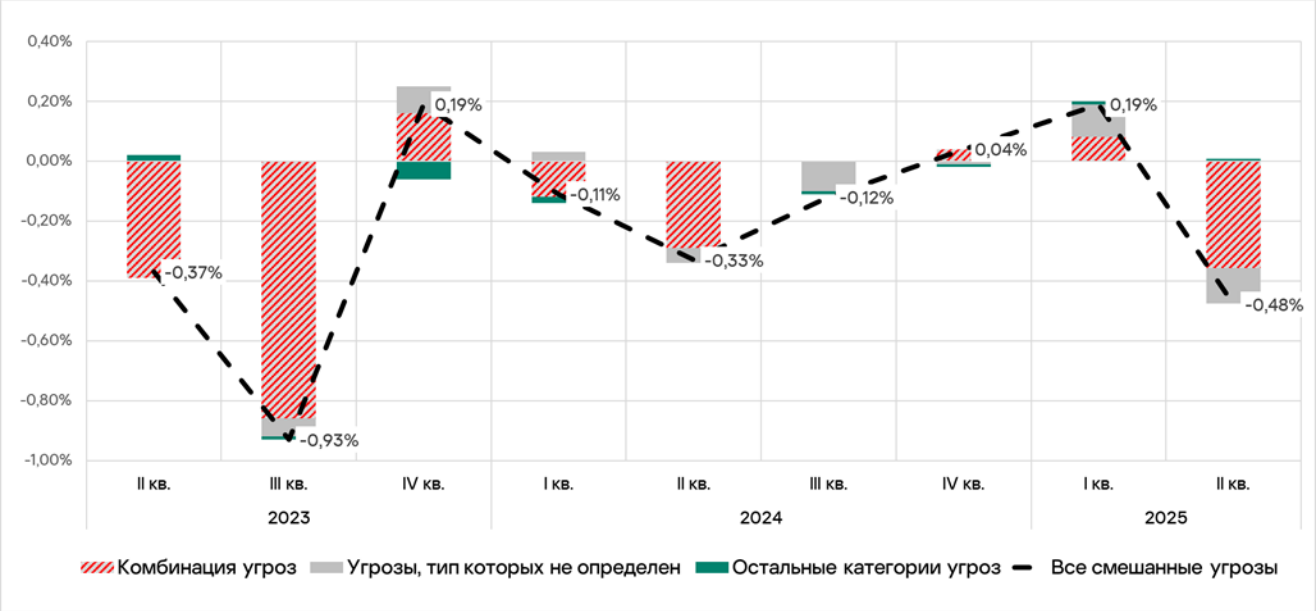
Вклад в снижение доли вирусов преимущественно внесли компьютеры АСУ, используемые в сферах строительства, биометрии и автоматизации зданий в России, Азии и на Ближнем Востоке. Это, в первую очередь, связано с возвратом к устойчивой тенденции на снижение доли вирусов в мире, после пика заражений в перечисленных индустриях и регионах в четвертом квартале 2024 года. Подробнее читайте в региональной версии отчета, который будет опубликован в ближайшее время.

Пограничное множество

Судя по статистике по компьютерам АСУ, оказавшимся в пограничном множестве, в этой зоне наибольшую группу представляют компьютеры, на которых блокировались несколько угроз сразу и в меньшей степени — компьютеры, на которых блокировались только угрозы неопределенного типа.

Блокирование угроз, категория которых не определена, в пограничном множестве явно указывает на то, как эти угрозы проникают внутрь сети — через интернет и почту в пограничном множестве.

На графике ниже показано, как менялись доли атакованных компьютеров АСУ в этих группах от квартала к кварталу.



Как видно на графике, основной вклад в изменение показателей компьютеров из пограничного множества вносят компьютеры АСУ, на каждом из которых блокировалось более одной уникальной угрозы.

На тепловой карте ниже показано, какие категории угроз блокировались на компьютерах, где встречалась комбинация угроз.

Видно, что компьютеры с угрозами, категории которых не были определены, составляют значительную часть в пограничном множестве, так же как и компьютеры, на которых блокировались вредоносные адреса и вредоносные скрипты. В данном случае это буквально могут быть одни и те же компьютеры, поскольку здесь мы рассматриваем случаи, когда на компьютере за квартал блокировались угрозы нескольких категорий.

Также стоит отметить, что в пограничном множестве, так же как и во множестве внутренних угроз, высока доля вирусов и червей. В практическом смысле это значит, что такие компьютеры могут участвовать в распространении шпионского ПО, вирусов и червей. Такое распространение может проходить как случайно, так и умышленно – для реализации атаки через поставщика (supply-chain) или доверенного партнера (trusted partner).

Категории угроз	Сегмент внешних угроз	Пограничный сегмент	Сегмент внутренних угроз
Угрозы, тип которых не определен	2,06%	2,68%	2,27%
Вредоносные скрипты	1,77%	1,60%	0,55%
Шпионское ПО	1,15%	1,11%	1,10%
Вредоносные веб-адреса	1,05%	1,67%	0,13%
Вредоносные документы (MSOffice + PDF)	0,85%	0,55%	0,30%
Веб-майнеры	0,14%	0,12%	0,06%
Исполняемые майнеры для ОС Windows	0,14%	0,22%	0,24%
Черви	0,06%	0,37%	0,58%
Вирусы	0,04%	0,39%	0,57%
Программы-вымогатели	0,01%	0,06%	0,06%
Вредоносное ПО для AutoCAD	0,00%	0,08%	0,20%

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[1].

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

- серверы управления и сбора данных (SCADA);
- серверы 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.

Компьютеры, передающие нам статистику, принадлежат организациям из разных отраслей. Наиболее широко представлены химическая промышленность, металлургия, инжиниринг и интеграторы АСУ,

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

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», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com