

kaspersky

Обзор 2026

Киберпульс. Государственный сектор. Россия.

Ключевая статистика киберугроз для госсектора в России

Количество кибератак на госсектор в России, I полугодие 2026 vs II полугодие 2025

Веб-угрозы

-14%

Угрозы на носителе

+25%

Распределение инцидентов высокой критичности по отраслевым секторам. Глобальная статистика.²



В ландшафте угроз отрасли наблюдается трансформация. Усиление веб-фильтрации в госорганизациях позволило сократить число инцидентов, связанных с массовыми киберугрозами, но они постепенно уступают место целевым атакам. В таких сценариях злоумышленники могут использовать локальные векторы распространения, включая съёмные носители, позволяющие обойти часть сетевых средств защиты.

Ландшафт киберугроз для госсектора в России, I полугодие 2026 vs II полугодие 2025

+82%

рост количества атак с ПО для кражи паролей¹

+11%

рост количества атак с применением шпионского ПО¹

-15%

снижение количества атак с применением бэкдоров, характерное для всех организаций в 2026 после всплесков предыдущих лет¹

+14%

рост количества атак с применением эксплойтов¹

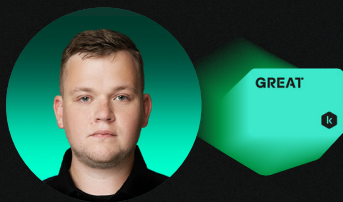
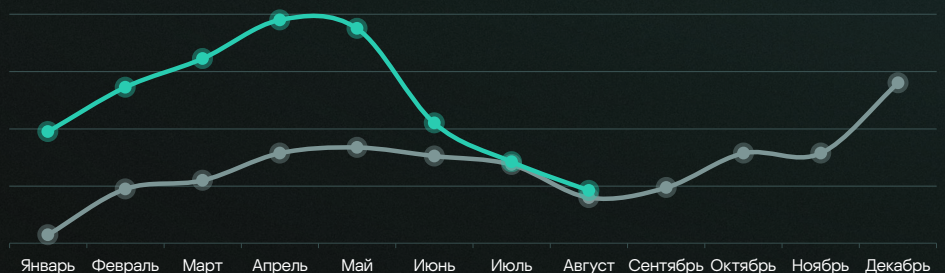
-4%

стабильно высокий уровень атак с применением программ-вымогателей (ransomware)¹

Сезонность атак с использованием программ-вымогателей на российский госсектор³

В атаках на госсектор наблюдается ярко выраженная сезонность, коррелирующая с деловой активностью. Как правило, пики приходятся на декабрь и май, а относительное снижение — на конец лета и январь.

2025 2026



Дмитрий Галов

Руководитель
Kaspersky GReAT в России

Российские госорганизации вынуждены защищать всё больше систем, сервисов и данных. Причем киберугрозы исходят сразу с нескольких направлений: хактивисты, кибершпионы, финансово мотивированные группы. Для масштабирования атак и одновременной работы с множеством целей злоумышленники используют ИИ. Всё это делает превентивные меры, такие как киберразведка, мониторинг, своевременное выявление аномалий и устранение уязвимостей, критически важными.

¹ По данным Kaspersky Global Research and Analysis Team (GReAT)

² По данным отчёта «Анатомия ландшафта киберугроз: глобальная аналитика и практические выводы»

³ По данным Kaspersky Cyber Threat Intelligence Team

Актуальные угрозы для госсектора в 2026 году

Librarian Likho: масштабируемые комплексные атаки

С конца 2025 года эксперты Kaspersky фиксируют постоянную активность АРТ-группы Librarian Likho, направленную на российские организации, в том числе из госсектора. Атаки **традиционно начинаются с фишинговых рассылок**. Вложения маскируются под предложения о сотрудничестве, договоры, платёжные и другие документы. После запуска **вредоносная программа устанавливает на устройство инструменты для удалённого доступа и закрепления в системе**, а также пытается отключить защитные механизмы.

Основная цель кампании — получить устойчивый удалённый доступ к заражённым компьютерам и учётным данным пользователей. В частности, **злоумышленники собирали сохранённые в браузерах и почтовых клиентах пароли и передавали их операторам атаки**. Данная кампания отличается от предыдущих масштабом и высокой степенью автоматизации. Кроме того, добавилась техническая вариативность на разных этапах атак: в новых командах в скриптах URL командного сервера не прописан в коде, а динамически меняется при помощи набора переменных.



[Подробнее](#)

Внутренние демоны DAEMON Tools

В апреле 2026 года было обнаружено **заражение популярного установщика ПО DAEMON Tools вредоносным кодом**. Скомпрометированные версии программы распространялись с **8 апреля** и были подписаны легитимным сертификатом разработчика, поэтому могли казаться пользователям доверенными. По данным Kaspersky GReAT, зафиксированы тысячи попыток заражения в более чем 100 странах, в отдельных случаях наблюдалось дальнейшее развитие атаки — в том числе в организациях государственного управления, науки, производства и розничной торговли.

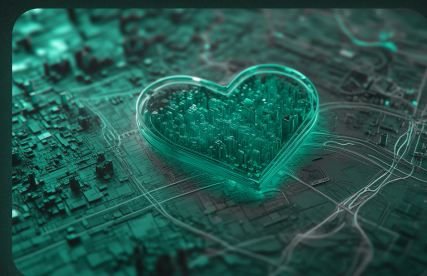


[Подробнее](#)

Показательно, что **после установки вредоносная программа сначала собирала информацию о компьютере, а затем злоумышленники отбирали интересующие их устройства для дальнейшего развития атаки** и установки бэкдоров. В частности, сложный инструмент QUIC RAT был обнаружен на компьютере российского учебного заведения. Таким образом, кампания демонстрирует опасность атак на цепочки поставок: компрометация одного популярного программного продукта позволяет получить первоначальный доступ к большому числу организаций, после чего атакующие могут выборочно развивать атаку против наиболее интересных для них целей.

HeartlessSoul: кибершпионаж под видом авиационного ПО

В апреле 2026 года Kaspersky раскрыла кампанию группы HeartlessSoul, которая с осени 2025 года атакует преимущественно российские организации, в том числе государственные органы, с целью кибершпионажа. **Атака начиналась с фишингового письма с архивом** или с вредоносной рекламы, где **под видом специализированного авиационного ПО** предлагалось скачать установщик. После запуска на компьютере выполнялась цепочка скриптов PowerShell, которая загружала JavaScript-загрузчик, а затем — основной RAT-троянец. Он давал злоумышленникам **удалённый доступ к системе** и позволял **собирать файлы, делать скриншоты, получать данные из браузеров и мессенджеров**, а также **собирать геоинформационные материалы** — например, карты и данные GPS. Для закрепления в системе вредоносная программа использовала стандартные механизмы Windows, а связь с инфраструктурой атакующих осуществлялась через управляющие серверы. Исследователи также обнаружили пересечения инфраструктуры HeartlessSoul с инфраструктурой группы GOFEE, которая ранее атаковала российский госсектор.



[Подробнее](#)

Stan Ghouls: в стремлении к удалённому доступу

В феврале 2026 года Kaspersky описала кампанию группы Stan Ghouls (Bloody Wolf), которая атакует организации госсектора в России и странах Центральной Азии. Атаки начинаются с **целевого фишингового письма с PDF, замаскированным под официальные судебные или другие деловые документы**. В самом PDF жертве предлагают скачать Java — под видом необходимого компонента для просмотра материалов, однако вместо этого загружается вредоносное ПО. Файл показывает пользователю ложное **сообщение об ошибке, после чего скачивает и запускает легитимный инструмент удалённого управления NetSupport RAT**. В результате злоумышленники получают **удалённый контроль над компьютером** и могут использовать его для дальнейших действий. Исследователи также обнаружили на связанной с кампанией инфраструктуре файлы Mirai, что может указывать на интерес группы к атакам на IoT-устройства.

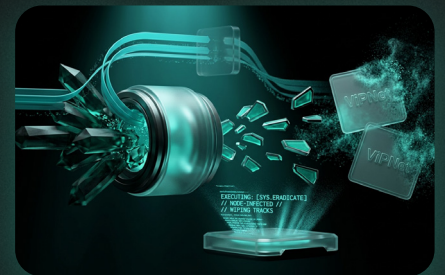


[Подробнее](#)

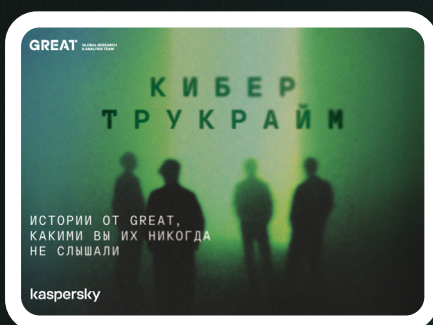
HelloNet: целевая атака полного цикла

Летом 2026 года была зафиксирована сложная целевая кибератака HelloNet против российских предприятий из государственного, промышленного, энергетического, транспортно-логистического и образовательного секторов.

Для заражения злоумышленники используют систему обновлений **ViPNet** — ПО для создания защищённых сетей. Атака реализуется через технику **DLL sideloading*** — ей подвержен один из компонентов ViPNet, который запускается при старте операционной системы. В кампании применяется ранее неизвестный сложный инструментарий, с помощью которого **атакующие загружают дополнительные вредоносные компоненты, проксируют трафик и запускают новые вредоносные нагрузки**, а также выполняют команды в заражённой системе, а затем очищают файлы журналов ПО ViPNet, скрывая свою активность. В одной из заражённых систем был **выявлен новый бэкдор HelloBackdoor**, используемый для манипуляций с файловой системой.



[Подробнее](#)



Захватывающие истории мирового кибербеза — в новом подкасте от Kaspersky GReAT

[Слушать](#)

* DLL sideloading — атака, при которой злоумышленники распространяют вредоносную библиотеку DLL (Dynamic Link Library) вместе с легитимным приложением, которое её выполняет.

Рекомендации ИБ на 2026 год



Игорь Кузнецов

Директор Kaspersky GReAT

О Kaspersky GReAT

Kaspersky GReAT основан в 2008 году. В его задачи входит поиск и исследование наиболее сложных атак, кампаний кибершпионажа, новых методов заражения, эксплойтов, использующих уязвимости нулевого дня. Сегодня в команде центра более 30 экспертов, работающих по всему миру: в Европе, России, Южной Америке, Азии, на Ближнем Востоке. Они известны своими достижениями в расследовании наиболее сложных атак, включая кампании кибершпионажа и киберсаботажа.

В свете актуальных угроз эксперты «Лаборатории Касперского» напоминают о советах, особенно актуальных для организаций государственного сектора:



Наладить комплексный мониторинг инфраструктуры

Важно видеть полную цепочку атаки — от первоначального проникновения до попыток закрепления и перемещения по сети. SIEM-система, граф связей и другие продвинутые инструменты для расследования инцидентов — необходимость для современных организаций.



Максимально укрепить защиту конечных устройств

Эффективная антивирусная защита, блокирующая массовые угрозы — фундамент ИБ. Но и без дополнительных инструментов класса EDR или даже XDR, выявляющих аномалии в процессах и поведении пользователей, уже не обойтись.



Уделить особое внимание рискам цепочек поставок

Необходимо контролировать используемое ПО и оперативно оценивать масштаб потенциальных компрометаций.



Использовать актуальные данные Threat Intelligence

Информация о тактиках и инструментах АPT-групп ускоряет обнаружение и расследование инцидентов.



Контролировать удалённое администрирование

Следует особо тщательно отслеживать использование PowerShell, SSH и других инструментов, которые злоумышленники часто применяют для маскировки активности. Регулярный общий аудит прав доступа и контроль действий администраторов также являются необходимыми процессами.



Использовать комплексный подход к защите

Интеграция средств защиты конечных устройств, сетевой безопасности, SIEM-системы и других компонентов в единую XDR-платформу помогает эффективнее противодействовать сложным атакам.

Взгляд вперед: на что обратить внимание уже сейчас

1

Государственный «периметр» окончательно размоется

Всё больше критичных процессов будет зависеть от подрядчиков, разработчиков ПО и интеграторов. Компрометация подрядчика станет более выгодным способом обхода периметра госорганизации.

2

Доверенное ПО превратится в одно из главных полей атаки

В ближайшие годы злоумышленники будут активнее искать возможности скомпрометировать обновления, библиотеки, репозитории и инструменты, которым сотрудники доверяют по умолчанию. Особенно опасен сценарий, когда вредоносная активность начинается уже после легитимной установки или обновления.

3

Кибершпионаж становится всё более актуальным

Ввиду высокой политической, экономической и социальной ценности информации, находящейся в распоряжении госорганов, количество кибератак с целью шпионажа будет только расти. Значение для злоумышленников имеют уже не только файлы, но и контекст, который используется для проникновения в инфраструктуру во всё более таргетированных кампаниях.

4

Кибератаки будут всё чаще направлены на нарушение процессов, а не только на кражу данных

Для государства критичным последствием может стать не утечка информации сама по себе, а невозможность оказать услугу, провести платёж, обработать обращение или обеспечить работу информационной системы. Поэтому в ближайшие годы мы, вероятно, увидим больше атак, где конечная цель — снизить операционную устойчивость государственного учреждения.

5

Автоматизация защиты станет ответом на автоматизацию атак

Если атакующие смогут с помощью ИИ одновременно вести сотни кампаний, ИБ-команды не смогут отвечать на них исключительно вручную. Будет расти значение автоматизированного поиска угроз, корреляции событий и XDR-подхода, когда информация с рабочих станций, серверов, почты и сети сводится воедино для восстановления полной картины атаки.



Анна Кулашова

Вице-президент «Лаборатории Касперского» по развитию бизнеса в России и странах СНГ



Государственный сектор находится под постоянным кибердавлением — это традиционно одна из самых атакуемых отраслей. Но в этом и причина высокого уровня ИБ-зрелости в госорганизациях: процессы и регламенты выстроены, EDR и сегментация стали стандартом, регулярно проводятся киберучения и обучение сотрудников. Сегодня фокус смещается на новые зоны риска — проактивное противостояние сложным целевым атакам с применением ИИ, противодействие социальной инженерии в рамках первоначальных векторов кибератак, своевременное управление уязвимостями, защита цепочек поставок. Ежегодно у нас появляются новые классы решений, способные обеспечить устойчивость организаций в стратегической перспективе, и все они готовы к масштабным внедрениям в госорганизациях.

Возможности портфолио «Лаборатории Касперского» для госорганизаций

С 2025 года действует [Приказ ФСТЭК России № 117](#) «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Документ определяет стандарты кибербезопасности в госорганизациях, обязательные технические и организационные меры по защите информации, а также ответственность за исполнение требований.

Предложение «Лаборатории Касперского» для реализации ключевых мер по защите информации согласно Приказу ФСТЭК России № 117:

Антивирусная защита и защита конечных устройств



Kaspersky Security для бизнеса



Kaspersky Endpoint Detection and Response Expert

Мониторинг, корреляция, анализ событий ИБ, обеспечение непрерывного взаимодействия с ГОССОПКА



Kaspersky Unified Monitoring and Analysis Platform

Сегментация и межсетевое экранирование



Kaspersky NGFW

Обнаружение и предотвращение вторжений на сетевом уровне



Kaspersky Anti Targeted Attack

Защита сервисов электронной почты



Kaspersky Security для почтовых серверов

Управление уязвимостями и обновлениями



Kaspersky Vulnerability Management

Контроль уровня защищенности информации в информационных системах



Kaspersky Security Assessment

Защита от DDoS-атак



Kaspersky DDoS Protection

Повышение уровня знаний пользователей по вопросам защиты информации



Kaspersky Automated Security Awareness Platform

Единая платформа безопасности класса XDR (расширенное обнаружение и реагирование) для всесторонней защиты ИТ-инфраструктуры



Kaspersky Symphony XDR

Регуляторный хаб знаний в области информационной безопасности

Портал с актуальной информацией о регуляторных требованиях в сфере кибербезопасности для организаций государственного сектора и технологиях для их реализации.

[Подробнее](#)



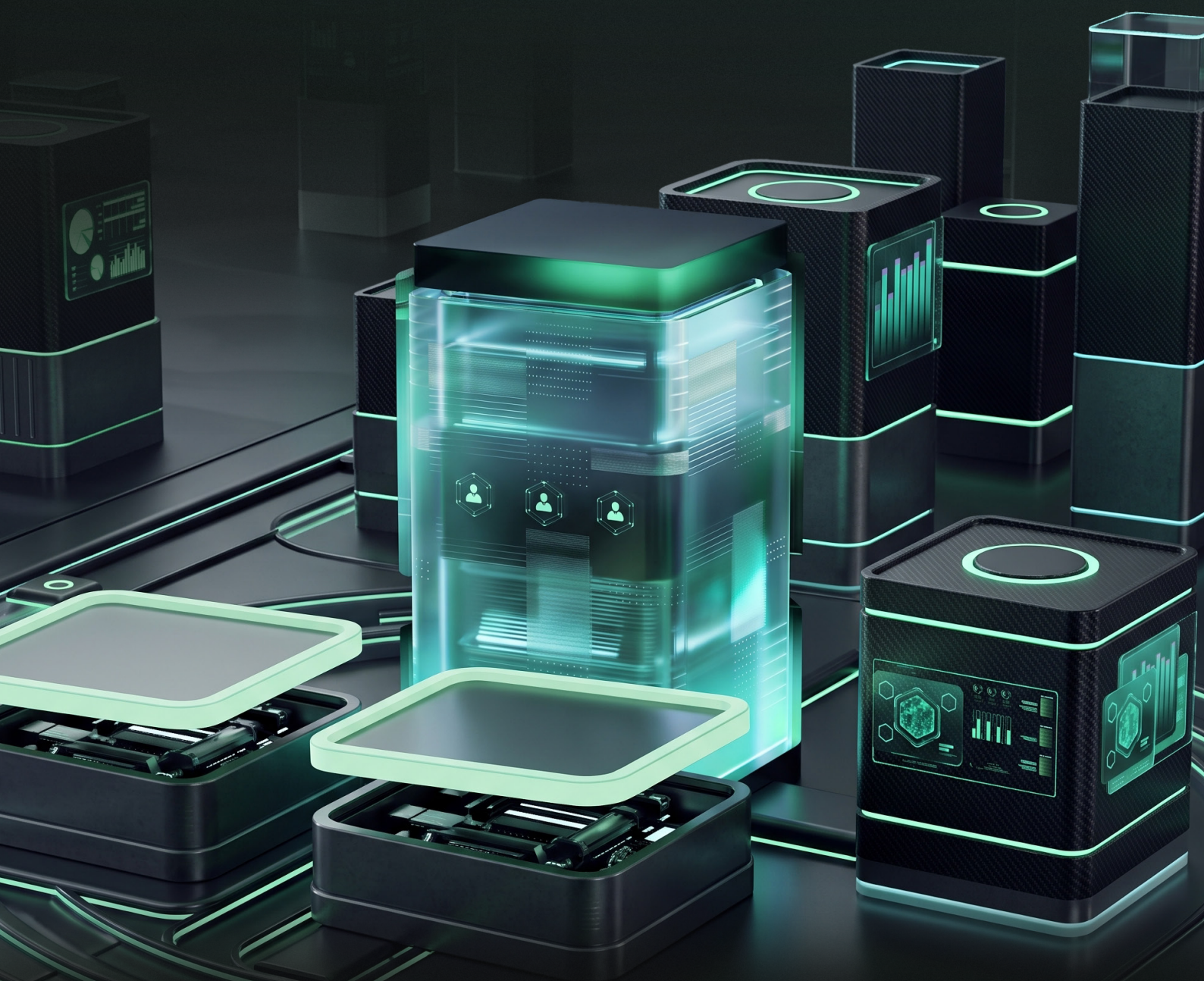
Больше отраслевых
обзоров угроз

[Подробнее](#)



Подробные технические
разборы атак

[Подробнее](#)



www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее