kaspersky

Киберпульс. Промышленность.

Россия.

Специально
для ИННОПРОМ-2026

Ключевая статистика киберугроз для промышленности в России

44%

компьютеров в промышленных организациях РФ столкнулись с киберугрозами в 2025 году (сегменты IT и OT)[1]

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

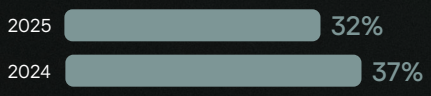
Доля компьютеров в промышленных организациях, столкнувшихся с угрозами, Q1 2026 vs Q1 2025

Шпионское ПО, бэкдоры и кейлоггеры	Шифровальщики	Вредоносное ПО для AutoCAD	Черви	Вирусы
+50%	+97%	+16%	+2,7%	+15%

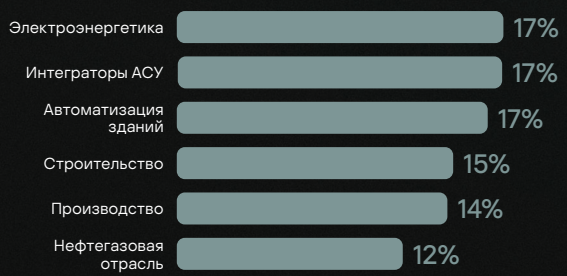
Угрозы для АСУ ТП

Главная отличительная черта промышленного сектора — наличие технологических процессов и ключевое значение АСУ ТП.

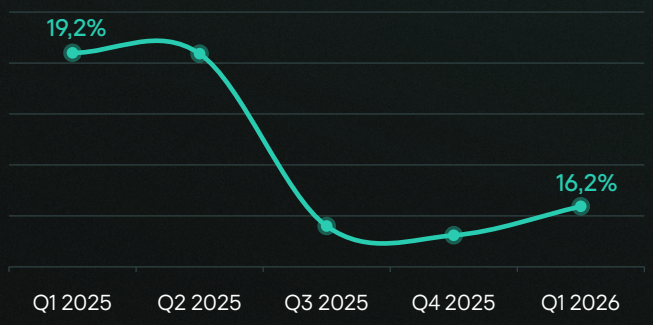
Доля компьютеров АСУ, подвергшихся атакам, 2025 vs 2024[1]



Доля компьютеров АСУ, подвергшихся атакам в разных отраслях промышленности, Q1 2026 г.



После снижения показателя в начале 2025 года в начале 2026 года наблюдается новый виток роста атак на АСУ ТП: доля компьютеров АСУ, на которых были заблокированы вредоносные объекты, превысила показатели предыдущего квартала.[1]



1 По данным Kaspersky ICS CERT

2 По данным глобального отчета Kaspersky Security Services «Анатомия ландшафта киберугроз»

Ключевые угрозы по доле компьютеров АСУ, подвергшихся атакам в 2025 году[3]

Ресурсы в интернете из списка запрещенных

11%

+13%
рост в Q1 2026[4]

Вредоносные скрипты и фишинговые страницы

9%

-5%
динамика в Q1 2026

Троянцы-шпионы, бэкдоры и кейлоггеры

6%

+9%
рост в Q1 2026

Анна Кулашова

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

«

Промышленность остаётся одной из наиболее атакуемых отраслей. Причин несколько: цифровизация расширяет поверхность атаки, объединение корпоративных и промышленных сетей повышает риски, а взаимодействие с подрядчиками с разным уровнем защищённости создаёт дополнительные возможности для злоумышленников. Поэтому предприятиям важно выстраивать комплексную систему защиты, учитывающую как особенности промышленной инфраструктуры, так и современные киберугрозы.

Программы-вымогатели (Ransomware) в атаках на промышленность[3]

Для технологических процессов в промышленности критичность последствий успешной атаки с использованием программ-вымогателей выше, чем в других секторах.

Поэтому сложившийся уровень защищенности промышленного сегмента (OT) позволяет держать долю атакованных организаций на низком уровне. Как правило, эта доля складывается из целевых атак повышенной сложности.

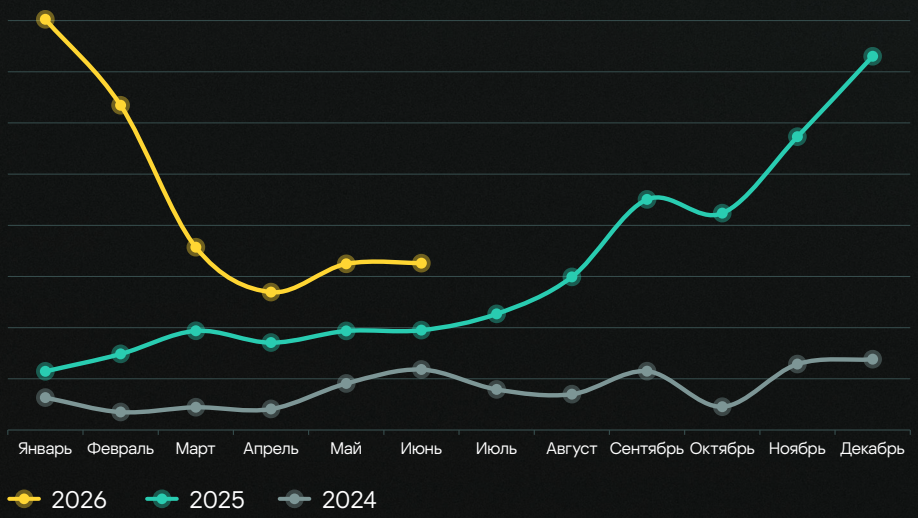
Тем не менее в начале 2026 года наблюдается тревожная тенденция.

x2,3

рост доли атакованных компьютеров АСУ в производственном сегменте.[3]

При этом шифровальщики по-прежнему остаются актуальной угрозой для корпоративных инфраструктур, в том числе промышленных предприятий. Несмотря на снижение показателя после пиковых значений в начале 2026 года, доля компьютеров, столкнувшихся с шифровальщиками, уже в первом полугодии заметно превышает уровни 2024 и 2025 годов. Это подтверждает сохраняющуюся активность атакующих и необходимость усиленной защиты промышленных организаций.

Изменение доли компьютеров в промышленности РФ, столкнувшихся с шифровальщиками, в течение года (сегменты IT и OT)[4]



3 Здесь и далее показатели Q1 2026 г. приводятся по сравнению с Q4 2025 г.

4 По данным Kaspersky ICS CERT

Ландшафт промышленных киберугроз: ключевые тренды

Цифровая атака — физическая кража

Цифровизация логистических цепочек создаёт новый вектор угроз — **киберпреступники взламывают IT-системы не только для шифрования данных или вымогательства, но и для организации физических краж грузов**. Компрометации различных участников логистических экосистем дают возможность атакующим перенаправлять доставку грузов в руки злоумышленников.

Группировки используют инсайдеров (водителей, логистов) в сочетании с фишингом и эксплуатацией уязвимостей IoT-устройств на складах и в транспорте.

Кибершпионаж

Широкое использование шпионского вредоносного ПО — общий тренд современного ландшафта угроз. **Промышленные предприятия России всё чаще становятся мишенью целевых атак с целью кражи конфиденциальной информации**, например, технологической документации, данных о производственных мощностях и результатов НИОКР.

В числе подверженных таким атакам отраслей — энергетика, металлургия, химическая промышленность, авиастроение. Злоумышленники применяют социальную инженерию против сотрудников предприятий, включая инженеров и конструкторов, используют нетривиальные подходы и комплексный инструментарий для сохранения долгосрочного присутствия в сетях.

+16%

рост числа атак с применением троянцев-шпионов на промышленные организации в России в Q1 2026[1]

Атаки на системы OT, имеющие доступ в интернет

Высокие показатели угроз для компьютеров АСУ, пришедших из интернета, отражают соответствующую глобальную проблему.

Причина — в том, что многие промышленные объекты, особенно удаленные производственные площадки, фактически получают доступ в интернет — постоянно или эпизодически — для выполнения различных производственных задач. **Человеческий фактор и недостатки систем защиты сетевого периметра при этом делают такие OT-системы точками первоначального проникновения** злоумышленников в технологический периметр промышленного объекта.

+6%

рост доли компьютеров АСУ ТП, на которых были обнаружены угрозы из интернета в Q1 2026[3]

Атаки с использованием ИИ

Искусственный интеллект все активнее используется в атаках на промышленные организации. Например, операторы платформы GLOBAL GROUP ransomware разработали автоматизированную систему для ведения переговоров о платеже выкупа, использующую чат-ботов на базе ИИ, чтобы не тратить время на обучение сотрудников английскому языку. Группа EvilAI маскировала вредоносные программы под инструменты повышения производительности на базе ИИ, а также частично разрабатывала вредоносный код с использованием LLM, чтобы усложнить обнаружение. Кроме того, **зафиксированы атаки на промышленные предприятия с использованием ИИ-агентов**, в которых операторы участвуют преимущественно на этапах планирования, таргетирования и контроля.

Рекомендации командам ИБ на 2026 год

Евгений Гончаров
Руководитель Kaspersky ICS CERT

Устаревшие OT-системы, разработанные без учета требований конструктивной безопасности и несовместимые с современными средствами защиты, равно как и прочие, хорошо известные проблемы, не позволяют гарантированно защитить промышленную среду от киберугроз, что делает ее слабым звеном информационной безопасности организаций. Длинные цепочки поставок и разветвленные сети доверенных партнеров многократно усложняют задачу, расширяя поверхность атаки далеко за пределы периметра не только технологической, но и офисной сети. Злоумышленники хорошо осведомлены об уязвимости операционных технологий и используют эти знания в атаках, что может привести к остановке производства и, следовательно, большим потерям. Поэтому обеспечение комплексной защиты с учётом специфики каждого конкретного предприятия и непрерывный мониторинг киберугроз должны быть приоритетом промышленных организаций.

Ключевые рекомендации «Лаборатории Касперского» ИБ-командам промышленных организаций:

1 Защита конечных узлов

- Специализированные решения — промышленные продукты для технологических сетей (например, Kaspersky Industrial Cybersecurity), корпоративные — для ИТ-сегментов, с поведенческим анализом и контролем запуска приложений и, по возможности, с подключением к Kaspersky Security Network
- Минимизация поверхности атаки — отключение неиспользуемых портов, белые списки приложений, контроль съёмных носителей
- Устранение уязвимостей — регулярные обновления ОС и ПО, компенсирующие меры для устаревших систем

2 Сегментация и контроль сети

- Изоляция сегментов — VLAN, NGFW, строгие ACL с минимально необходимым набором разрешений
- Контроль удалённого доступа — блокировка несанкционированных VPN, доступ через DMZ и терминальные серверы
- Непрерывный мониторинг — обнаружение аномалий и нарушений политик

3 Управление учётными данными

- Многофакторная аутентификация — для административных консолей, критических систем и внешних сервисов
- Строгие парольные политики — 12+ символов, разные классы, смена каждые 90 дней
- Принцип минимальных привилегий — ограничение админ-прав, хранение секретов только в менеджерах паролей

4 Мониторинг и реагирование

- SIEM с правилами корреляции — отслеживание подозрительных входов, изменений в системе, аномального трафика
- EDR/XDR или MDR-сервисы — для обнаружения сложных угроз и поведенческого анализа
- Надёжные резервные копии — минимум 3 копии, автономное хранение, регулярное тестовое восстановление

5 Защита от фишинга и обучение

- Многоуровневая фильтрация почты — проверка вложений в песочнице, периодическое пересканирование
- Обучение персонала — симуляции атак, тренинги по безопасной работе
- Процедуры реагирования — готовые инструкции, мониторинг угроз через Threat Intelligence

Kaspersky ICS CERT

Подробнее

Международный центр исследования безопасности промышленных систем и реагирования на инциденты. Команда ICS CERT выявляет и анализирует киберугрозы и уязвимости АСУ ТП, консультирует организации, разрабатывает методики защиты и предоставляет аналитические данные о текущих угрозах для OT-систем.

Единая концепция промышленной безопасности

Kaspersky OT CyberSecurity

Технологии

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Знания

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Экспертиза

Набор экспертных сервисов для комплексной промышленной кибербезопасности

Технологии

Основные

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Unified Monitoring and Analysis Platform

Фокусные

- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Решения на базе KasperskyOS

- Kaspersky IoT Secure Gateway
- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Знания

Аналитика угроз	Кибергигиена	Тренинги
Kaspersky ICS Threat Intelligence	Kaspersky Security Awareness	Kaspersky ICS CERT Training

Экспертиза

Анализ защищенности	Управляемая защита	Реагирование на инциденты
Kaspersky ICS Security Assessment	Kaspersky Managed Detection and Response	Kaspersky Incident Response

Кибербезопасность — стратегический актив промышленных организаций

Цифровая трансформация промышленности ставит перед предприятиями новые задачи, связанные с ИБ — технические, юридические и кадровые. Технологии «Лаборатории Касперского» позволяют выстроить надежную структуру кибербезопасности даже в условиях нехватки специалистов и необходимости соблюдения строгих нормативных требований.

Мы готовы предложить фокусные решения, которые отвечают бизнес-приоритетам вашего предприятия.

Для нефтегазового сектора

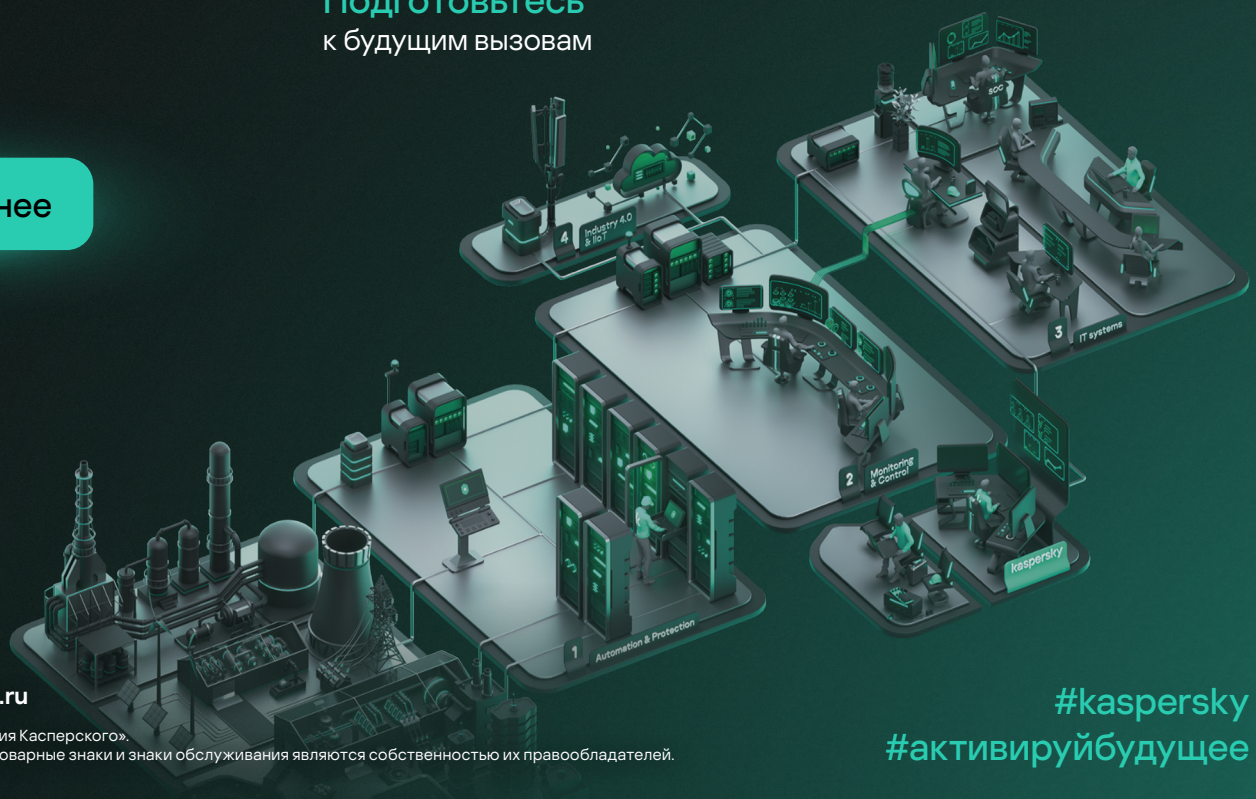
Для энергетического сектора

Промышленная киберустойчивость

Пошаговый, структурированный подход обеспечит устойчивость промышленных компаний к киберугрозам. Посмотрите, как защитить предприятие, обеспечив стабильность и безопасность процессов в соответствии с нормативными требованиями.

1. **Проведите** инвентаризацию активов
2. **Оцените** риски
3. **Обеспечьте** базовую защиту
4. **Выявите** угрозы и аномалии
5. **Проведите** аудит безопасности
6. **Оптимизируйте** сегментацию и зонирование сети
7. **Усильте** SOC
8. **Подготовьтесь** к будущим вызовам

Подробнее



www.kaspersky.ru

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

#kaspersky
#активируйбудущее