Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

**Лекция №10 «Кибербезопасность АСУ ТП»**

**1. Текущее состояние кибербезопасности АСУ ТП.**

**2. Распространённые проблемы безопасности на промышленных предприятиях**

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

## 1. Текущее состояние кибербезопасности АСУ ТП.

По оценке экспертов Positive Technologies, во II квартале 2022 года доля атак на промышленные предприятия составила 13 % среди организаций — на 5 п. п. больше, чем в предыдущем, — а общее количество атак на промышленный сектор увеличилось на 53 % вследствие возросшей активности шифровальщиков. Доля атак с использованием вредоносных программ составила 76 %. Лидерами оказались программы-вымогатели (61 % от общего количества).

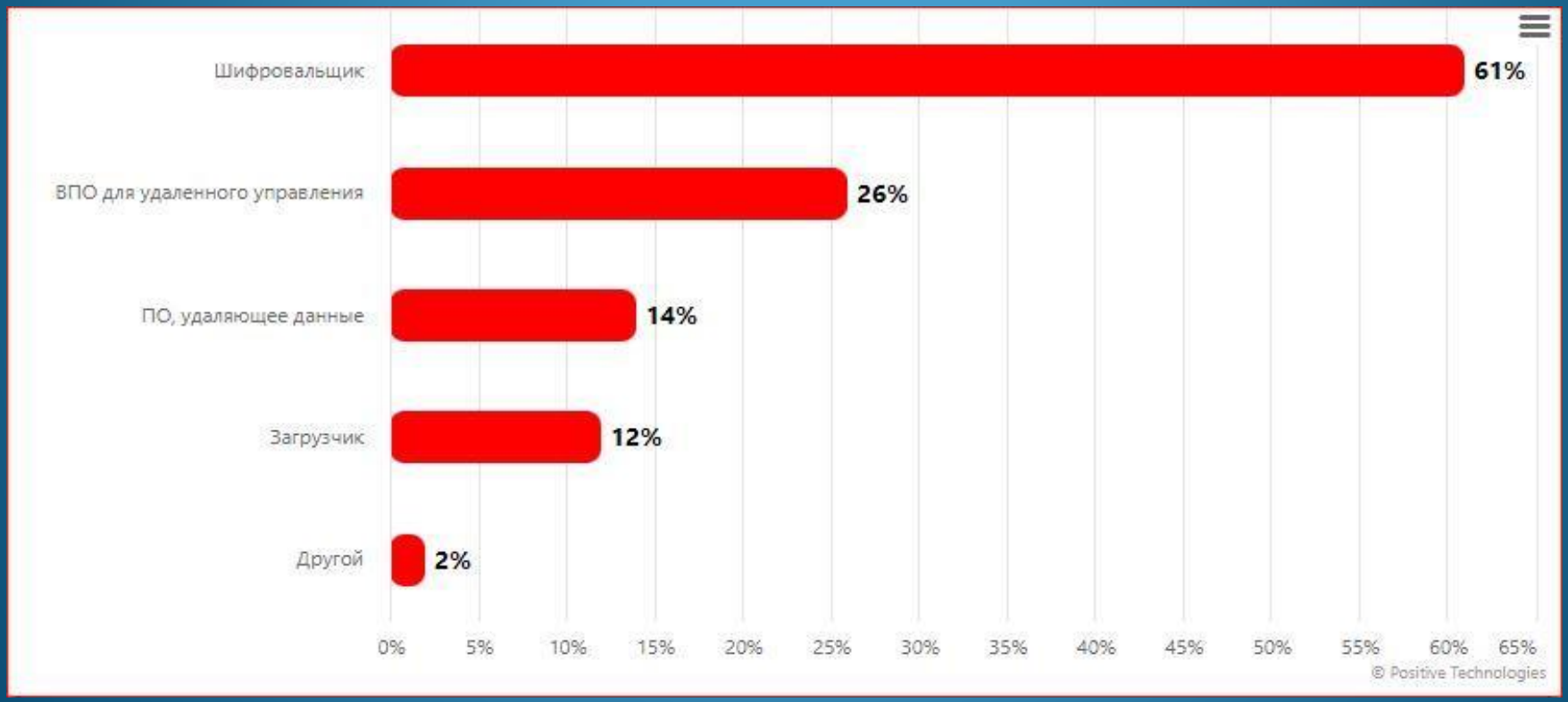
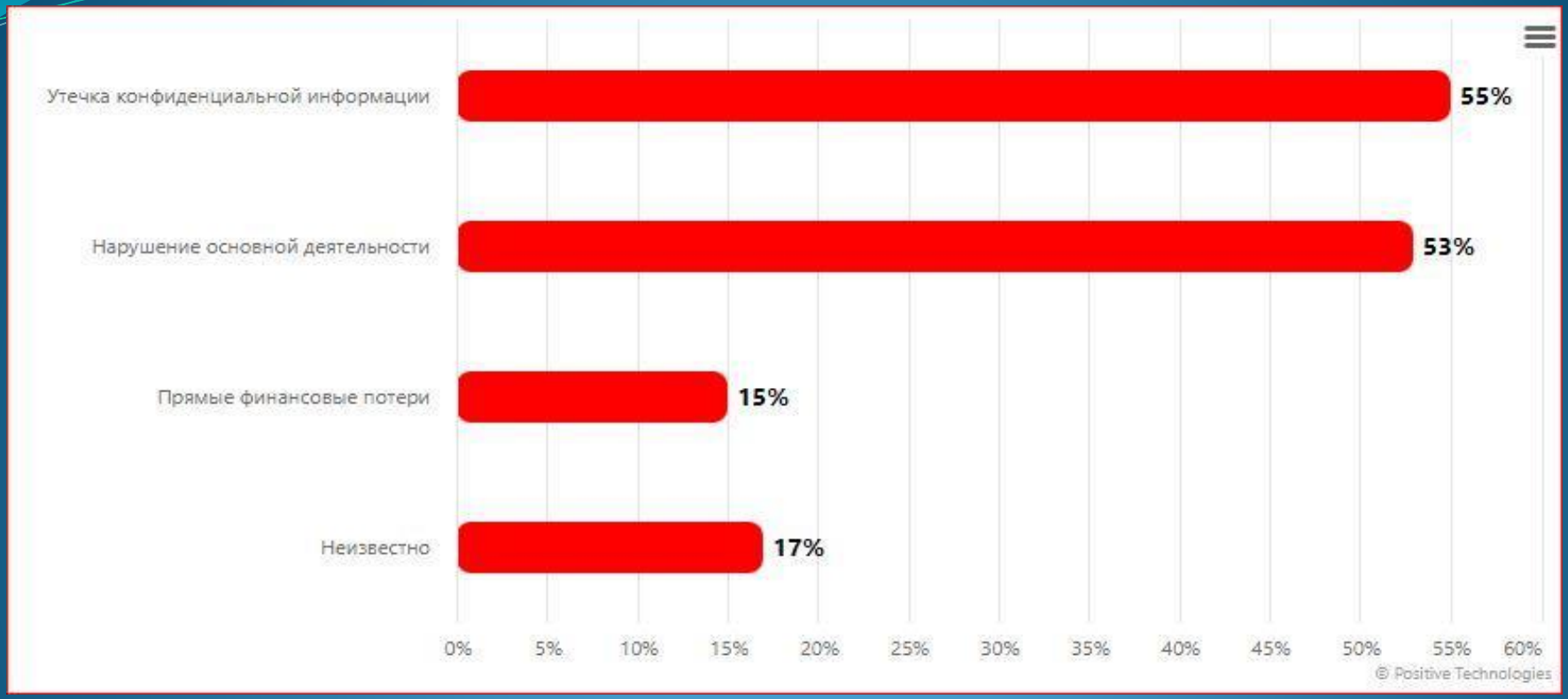



Рисунок 1. Основные типы вредоносных программ в атаках на промышленные организации

Более половины (53 %) случаев кибератак оказывали влияние на стабильное функционирование предприятий промышленного сектора.




Во II квартале 2022 года выделяется крупная атака злоумышленников Gonjeshke Darande на три иранских сталелитейных завода. В результате были нарушены технологические процессы производства, а на одном из заводов злоумышленникам удалось обрушить ковш с жидким чугуном, что вызвало пожар в цехе. По некоторым сведениям, в атаке использовалась вредоносная программа для удаления данных, что является одним из трендов предыдущего квартала.

Атаки на производственные объекты .

Открытыми уязвимостями и нарушениями в безопасности производственных систем пользуются злоумышленники. Как правило, атаки на крупные предприятия планируются заранее, поэтому им трудно противостоять. Выделяют следующие этапы кибератаки:

- поиск места проникновения; проникновение в сеть;
- сканирование сети — определение хостов, версий ПО (включая ОС) и оборудования, поиск сетевых устройств;
- первичный сбор информации; подготовка информационной базы — выбор вредоносных программ, эксплойтов, инструментов на основании собранных сведений;
- атака и эксплуатация.

Динамика кибератак на российские организации демонстрирует устойчивый рост угроз. По данным RED Security SOC (**центр мониторинга информационной безопасности**), в 2024 году зафиксировано почти 130 тысяч инцидентов информационной безопасности, что в 2,5 раза больше показателей 2023 года . Эксперты прогнозируют дальнейшее увеличение числа атак в 2025 году на 70-200%, что может привести к регистрации до 300 тысяч кибератак.

Особенно тревожным является рост заказных кибератак - их доля увеличилась с 10% в 2023 году до 44% в 2024 году. Это свидетельствует о профессионализации киберпреступности и переходе от хактивистских действий к коммерческим атакам с четкими финансовыми мотивами.
Объекты КИИ как приоритетная цель
Объекты критической информационной инфраструктуры составляют 64% от всех целей кибератак в России . При рассмотрении только высококритичных атак этот показатель возрастает до 68%, что на 10 процентных пунктов больше, чем в 2023 году.

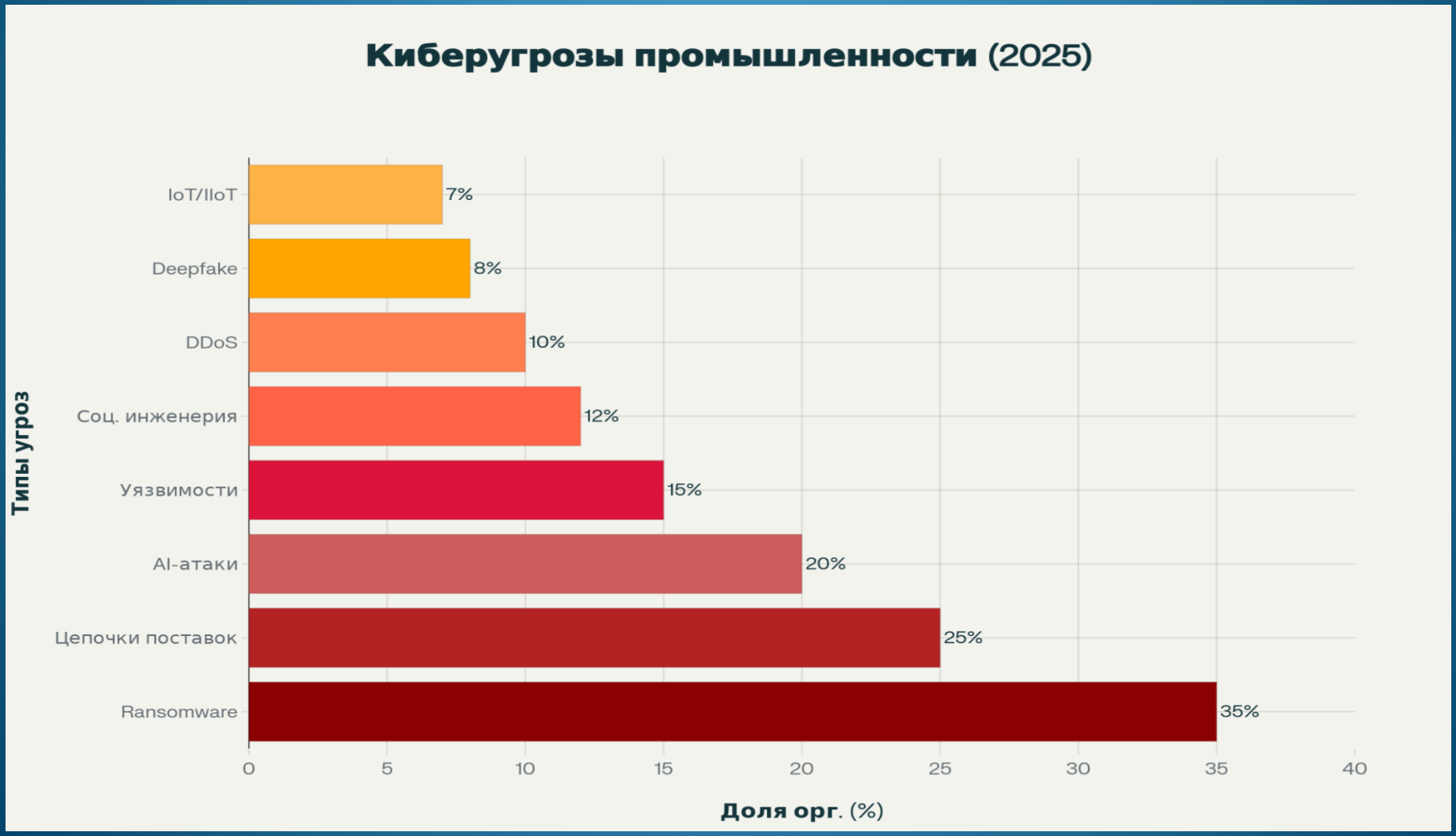
Объекты критической информационной инфраструктуры составляют главную цель для киберпреступников
Заместитель секретаря Совета Безопасности РФ Алексей Щевцов сообщил, что в 2024 году на российские объекты критической инфраструктуры было зафиксировано более 208 тысяч особо опасных кибератак [4]. Эти цифры подтверждают целенаправленный характер угроз и высокий приоритет КИИ для злоумышленников.

Эволюция атак с использованием ИИ

Искусственный интеллект кардинально меняет характер киберугроз. Эксперты Kaspersky ICS CERT отмечают, что злоумышленники активно используют ИИ на разных этапах подготовки и проведения атак - от разработки вредоносных инструментов до создания средств социальной инженерии. По данным исследований, упоминания о злонамеренных ИИ-инструментах на криминальных форумах выросли на 200%.
Особую опасность представляют deepfake-атаки. В 2024 году был зафиксирован случай мошенничества с использованием deepfake технологий на сумму $25 миллионов, когда преступники успешно имитировали голос и внешность руководителя компании Arup . Подобные атаки становятся все более доступными благодаря снижению технических барьеров и стоимости создания синтетических медиа.

# Основные типы угроз

Анализ экспертных прогнозов позволяет выделить ключевые типы киберугроз для промышленного сектора в 2025 году:



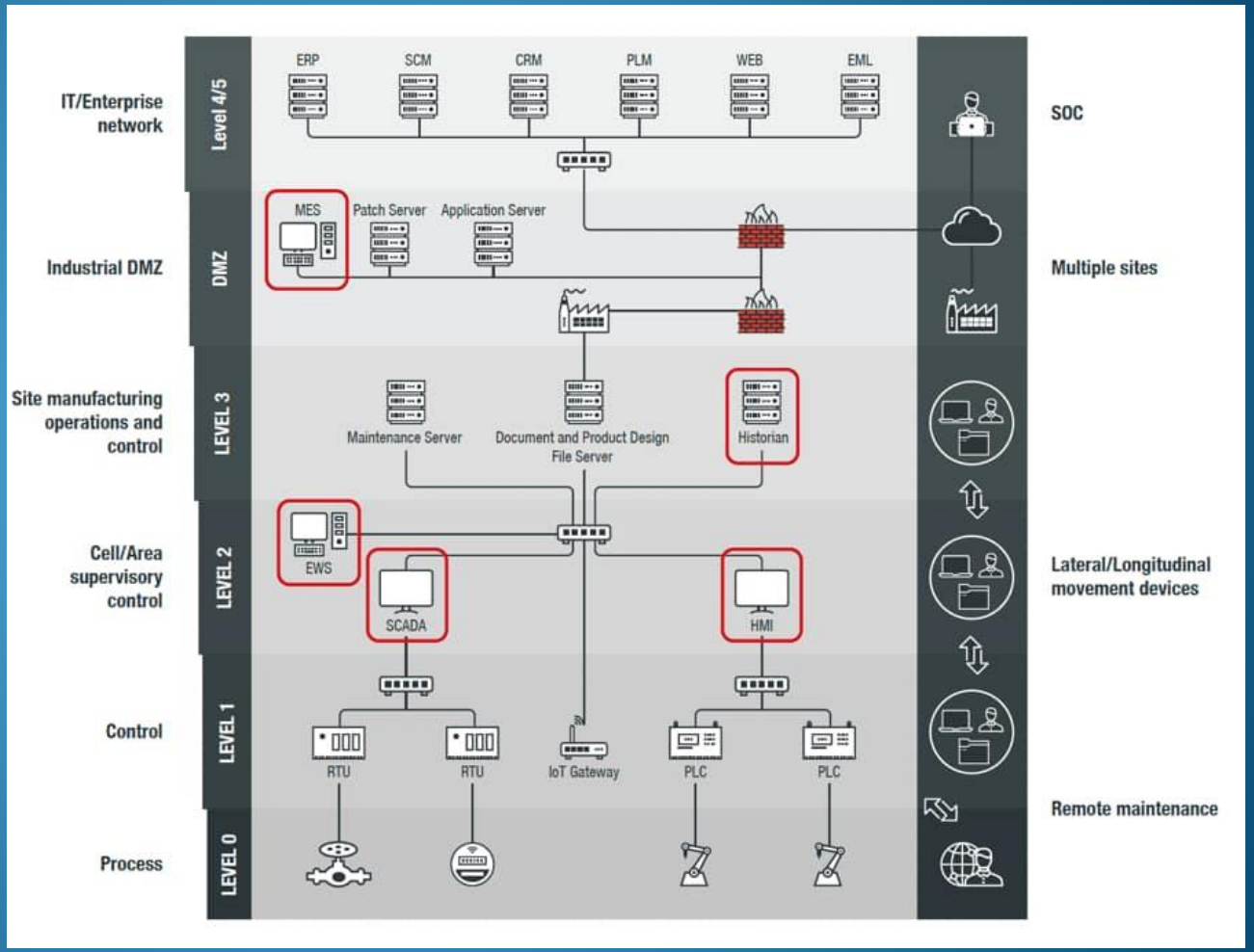
Прогноз киберугроз 2025: программы-вымогатели остаются главной угрозой для промышленности

Программы-вымогатели остаются доминирующей угрозой, составляя 35% от всех атак на промышленные предприятия. В мае 2025 года было зафиксировано 545 инцидентов с ransomware  (Шифровальщики)  по всему миру, что демонстрирует 15,95% рост по сравнению с апрелем.

Атаки на цепочки поставок занимают второе место (25%), отражая растущую сложность современных производственных экосистем. ИИ-powered атаки составляют 20% от общего количества угроз, что подчеркивает быструю адаптацию злоумышленников к новым технологиям.

# Уязвимости промышленных систем

Архитектурные проблемы Современные промышленные сети характеризуются высокой степенью интеграции операционных технологий (OT) с информационными системами (IT). Эта конвергенция создает новые векторы атак, поскольку традиционно изолированные промышленные системы становятся доступными через корпоративные сети.



Эксперты Kaspersky отмечают, что промышленные предприятия больше не могут полагаться на сокрытие информации о работе своих систем. Доступность разнообразного инструментария для работы с промышленным оборудованием делает разработку атак на производственные активы значительно более простой задачей.

Проблемы устаревших систем

Значительная часть промышленных систем построена на устаревших технологиях, которые изначально не проектировались с учетом современных угроз кибербезопасности. Принцип "работает - не трожь" в промышленной среде приводит к эксплуатации систем годами и даже десятилетиями без обновлений безопасности.
Особенно проблематична ситуация с Linux-системами в промышленной среде. Несмотря на распространенное мнение о их большей безопасности, защитить такие системы от целенаправленных атак может быть даже сложнее, чем Windows-инфраструктуру, из-за нехватки специализированных решений безопасности и квалифицированных специалистов.

## Состояние защищенности КИИ в России

### Результаты государственного контроля

Данные ФСТЭК России демонстрируют критическое состояние защищенности объектов КИИ. По результатам мониторинга 170 организаций, только 13% обеспечили минимальный базовый уровень защиты. У 40% организаций зафиксирован низкий уровень защищенности, а у 47% состояние защиты находится в критическом состоянии.

За 2024 год было проверено более 800 значимых объектов КИИ, при этом выявлено более 800 нарушений в обеспечении безопасности. В 40% случаев существовала реальная угроза стабильному функционированию объектов.

### Основные нарушения

Типичные нарушения в сфере КИИ включают:

- Несоответствие фактического состава значимых объектов данным в реестре
- Некорректная категоризация объектов КИИ
- Отсутствие контроля за подрядчиками
- Невыполнение мероприятий по выявлению уязвимостей
- Необновленные антивирусные базы
- Мониторинг событий с обычных корпоративных компьютеров вместо изолированных рабочих мест

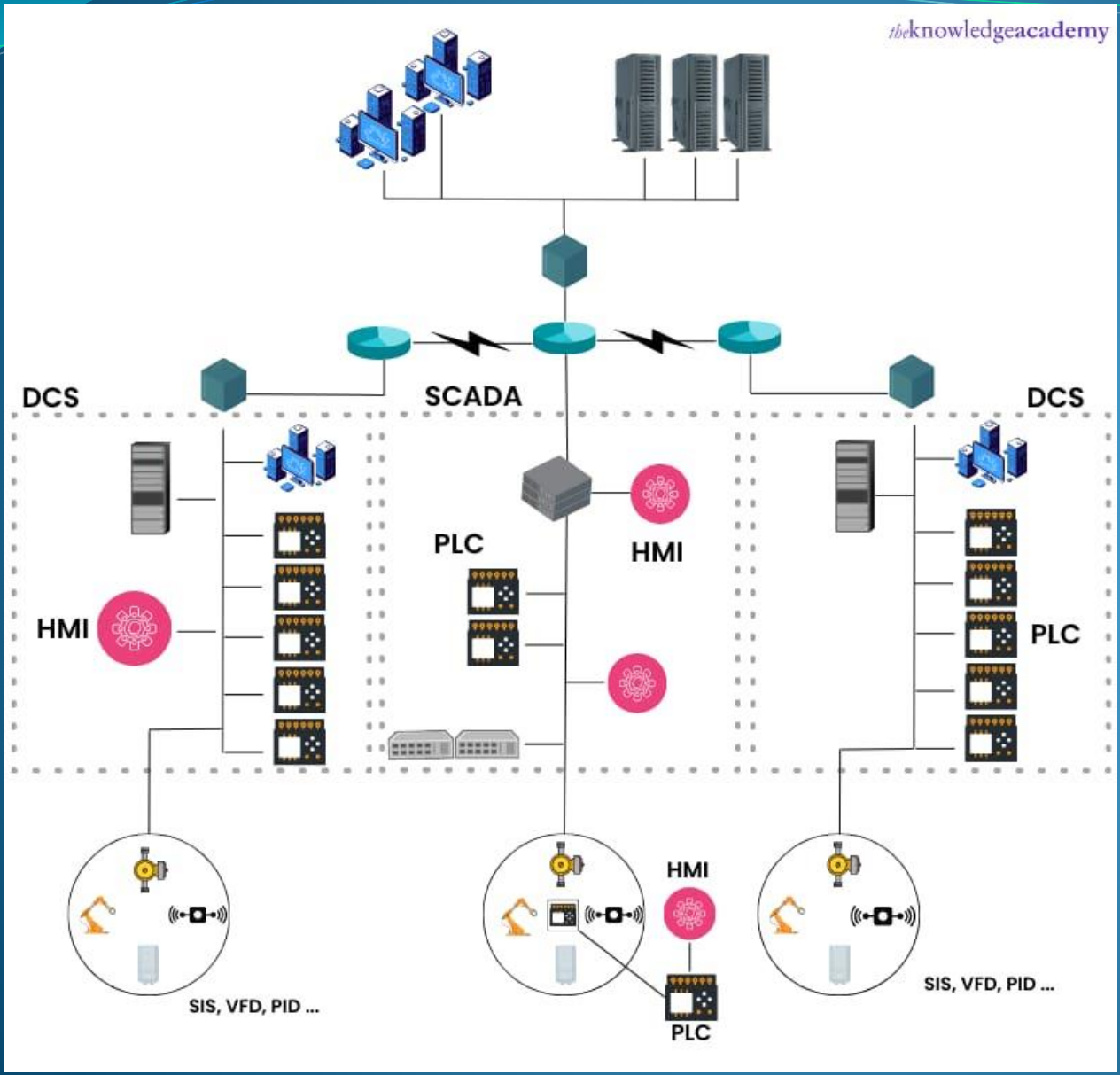
## Тенденции развития угроз

### Геополитический фактор

Текущая геополитическая обстановка существенно влияет на ландшафт киберугроз. В 2024 году количество прогосударственных APT-группировок, атакующих Россию и СНГ, увеличилось с 14 до 27. Было обнаружено 12 новых группировок, включая Unicorn, Dante, PhantomCore, ReaverBits и другие. Хактивистские группы также наращивают активность - в 2024 году не менее 17 таких группировок атаковали российские и белорусские организации, что на четыре больше, чем годом ранее. Размываются традиционные границы между хактивистами, APT-группами и киберпреступниками.

### Новые технологии как источник угроз

Внедрение новых технологий, таких как системы машинного обучения и квантовые вычисления, создает дополнительные риски для промышленных предприятий. Неосторожное использование технологий ИИ может привести к непреднамеренному раскрытию конфиденциальной информации и появлению новых, трудно прогнозируемых угроз безопасности.




Системы ИИ и уникальные данные, которые они используют, становятся новыми целями для кибератак. В отличие от традиционных ОТ-систем, они могут не представлять прямой угрозы функциональной безопасности, что делает их менее рискованной целью для злоумышленников.

Регуляторные изменения и требования

Ужесточение государственного контроля

ФСТЭК России планирует увеличить количество контрольных мероприятий более чем в 2 раза в 2025 году. Ведомство намерено создать рейтинг объектов КИИ по уровню кибербезопасности, который будет включать организации с недостаточной степенью защищенности.
Законодательные требования в области защиты КИИ продолжат совершенствоваться. Планируется усиление отраслевой составляющей для упрощения определения ресурсов, подлежащих обязательной защите.
Импортозамещение в кибербезопасности
В 2025 году продолжится реализация планов перехода на доверенные программно-аппаратные платформы. Все субъекты КИИ должны были разработать такие планы в 2024 году, а их реализация начнется в текущем году.
Актуальным остается выполнение требований Указа Президента России от 1 мая 2022 года № 250 о прекращении использования зарубежных средств защиты информации. Крупные субъекты КИИ не смогли полностью исключить применение таких средств на незначимых объектах к 1 января 2025 года.

Рекомендации по усилению защиты

Переход к практической безопасности

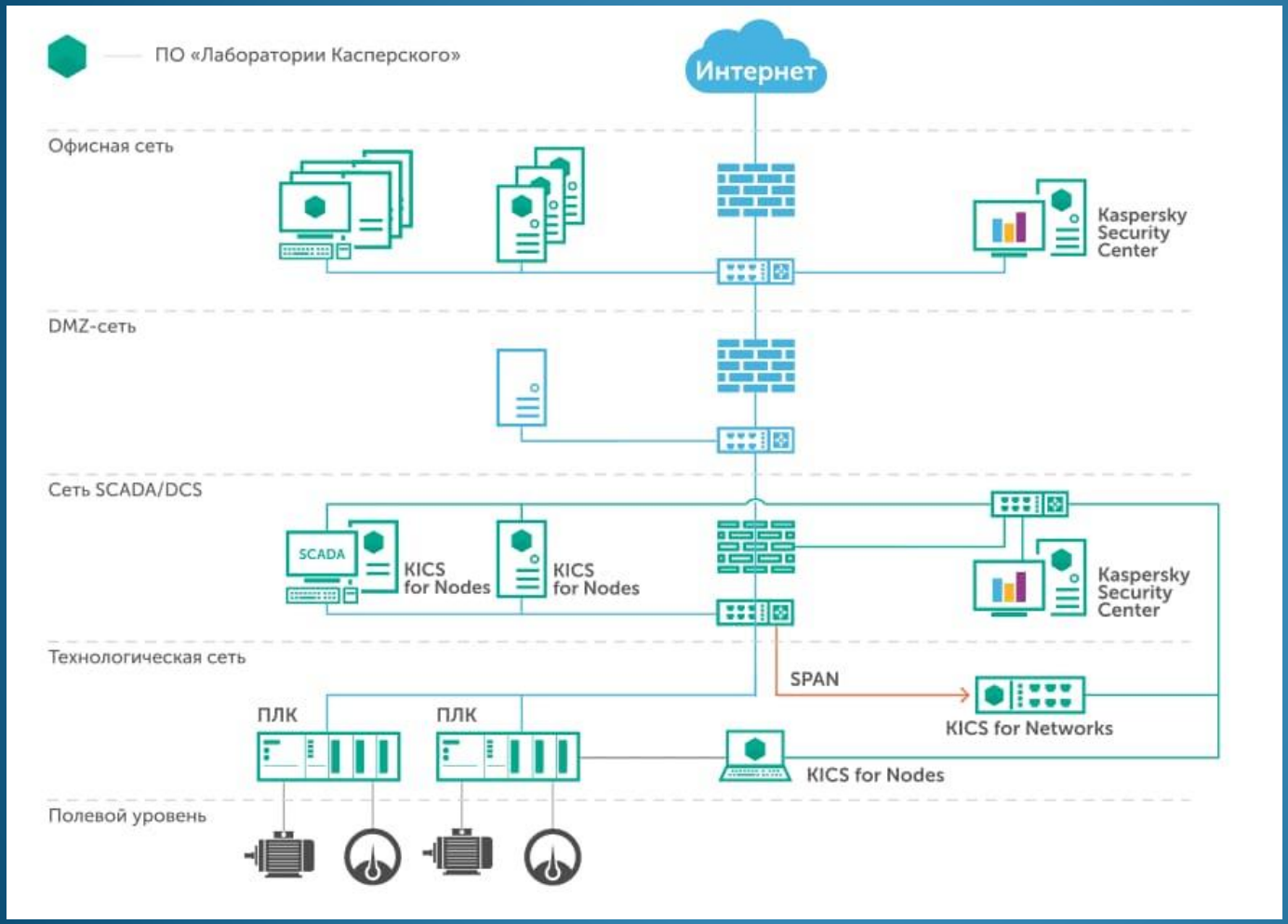
Ключевой тенденцией 2025 года станет переход субъектов КИИ от формального соблюдения требований к практической защите [16]. Этому способствуют:

- Рост числа атак и необходимость оперативного реагирования
- Появление информации об успешных атаках в медийном пространстве
- Повышение внимания руководства к информационной безопасности
- Ужесточение требований НПА с уклоном в практическую ИБ

Комплексный подход к защите
Эффективная защита промышленных сетей требует комплексного подхода, включающего:

Технические меры:
• Сегментация сетей и микросегментация критических активов
• Непрерывный мониторинг OT-среды с использованием специализированных решений
• Регулярные обновления и управление уязвимостями
• Внедрение решений класса Zero Trust для промышленных сетей

Организационные меры:
• Регулярные оценки рисков и аудиты безопасности
• Обучение персонала основам кибергигиены
• Разработка и тестирование планов реагирования на инциденты
• Управление рисками третьих сторон и цепочек поставок




Интеграция ИИ в защиту
Для противодействия ИИ-powered атакам необходимо внедрение собственных ИИ-решений для защиты. В 2025 году OT-защитники будут все больше полагаться на искусственный интеллект для автоматизации обнаружения угроз и реагирования на инциденты.

## Эволюция угроз

Эксперты прогнозируют несколько ключевых тенденций развития киберугроз в 2025 году:
Увеличение масштаба и сложности атак. Количество кибератак может вырасти на 70-200%, при этом атаки станут более комплексными, использующими множественные векторы одновременно.
Рост атак типа "вайпер". 2025 год может стать "годом вайпера" - программ-уничтожителей данных, которые не требуют выкупа, а просто уничтожают информацию.
Целевые атаки на цепочки поставок. Злоумышленники будут проводить детальный анализ цепочек поставок и наносить целевые удары по критическим узлам.

Секторальные риски
Наибольшему риску в 2025 году будут подвержены:
• Промышленные предприятия - 31% всех атак направлены на этот сектор
• Энергетические компании - критически важная инфраструктура остается приоритетной целью
• Финансовый сектор - высокие риски из-за цифровизации и ценности данных
• Телекоммуникации - важность для обеспечения связности всей экономики

## Эволюция угроз

Эксперты прогнозируют несколько ключевых тенденций развития киберугроз в 2025 году:
Увеличение масштаба и сложности атак. Количество кибератак может вырасти на 70-200%, при этом атаки станут более комплексными, использующими множественные векторы одновременно.
Рост атак типа "вайпер". 2025 год может стать "годом вайпера" - программ-уничтожителей данных, которые не требуют выкупа, а просто уничтожают информацию.
Целевые атаки на цепочки поставок. Злоумышленники будут проводить детальный анализ цепочек поставок и наносить целевые удары по критическим узлам.

Секторальные риски
Наибольшему риску в 2025 году будут подвержены:
• Промышленные предприятия - 31% всех атак направлены на этот сектор
• Энергетические компании - критически важная инфраструктура остается приоритетной целью
• Финансовый сектор - высокие риски из-за цифровизации и ценности данных
• Телекоммуникации - важность для обеспечения связности всей экономики

- За первые три квартала 2025 года каждая пятая успешная атака на организации (20%) была массовой. При этом каждая такая атака может иметь от десятков до нескольких тысяч жертв.

- Чаще всего жертвами массовых атак на организации становятся госучреждения (12%) и промышленность (9%); эти же отрасли являются самыми атакуемыми и в целевых атаках. Высокая ценность хранимых данных, геополитическая значимость, масштабная цифровизация, а также относительно незрелые процессы кибербезопасности — все это делает госучреждения и промышленность привлекательными, уязвимыми мишенями для киберпреступников.

- Самое частое последствие массовых атак — утечки конфиденциальных данных (40%). На втором месте — использование ресурсов жертвы для проведения атак (26%). Чаще всего это DDoS-атаки с использованием ресурсов компании, фишинговые атаки, в том числе от лица жертвы, а также использование ресурсов жертвы как канала распространения ВПО и для атаки на клиентов или партнеров.

- Помимо прямых последствий, массовые атаки порождают ряд системных проблем. Они вызывают многократное увеличение нагрузки на защитные механизмы и команды реагирования. Одновременное появление множества инцидентов приводит к перегрузке команд реагирования, что затрудняет своевременное выявление и отражение угроз.

- В 56% всех массовых атак злоумышленники использовали ВПО. Это выгодный подход: вложения в разработку или покупку готового ВПО быстро окупаются за счет масштабности кампаний. Другая важная причина массового использования ВПО — его высокая эффективность и простота применения, позволяющие злоумышленникам проникать в IT-инфраструктуру организаций, развивать атаку и доводить ее до полной компрометации критически важных систем.

- ВПО для удаленного управления (RAT) лидирует в массовых атаках с использованием ВПО (34%), поскольку обеспечивает злоумышленнику полный контроль над зараженными устройствами, позволяет автоматизировать сбор данных, перемещение по сети и установку дополнительного ПО, а также используется для создания ботнетов. Это делает его идеальным инструментом для автоматизированных кампаний.

- Шпионское ПО (22%) сохраняет высокую актуальность как в массовых, так и в целевых атаках благодаря своей универсальности: оно позволяет скрытно собирать конфиденциальные данные для последующей монетизации или использования в цепочках атак. В то же время применение майнеров (19%) хотя и остается характерным для массовых кампаний, становится менее выгодным из-за снижения доходности криптомайнинга.

- Шифровальщики (14%) сегодня остаются основным инструментом целевых атак, но благодаря широкой доступности платформ ransomware as a service (RaaS) и высокой степени автоматизации их использование в массовых атаках будет расти. В ближайшем будущем можно ожидать роста доли таких кампаний за счет низкого порога входа и высокой монетизации.

- Эволюция массовых атак проходит от простых, легко обнаруживаемых сценариев (с уже известными идентификаторами компрометации и раскрытыми уязвимостями) к сложным адаптивным кампаниям, где злоумышленники применяют обфускацию кода, автоматизированное создание вредоносных файлов, ботнеты с динамической логикой. Эти техники позволяют маскировать активность, избегать сигнатурного детектирования и масштабировать атаки без риска быстрого обнаружения. В результате граница между массовыми и целевыми атаками становится все менее четкой, а эффективная защита требует перехода на решения с поведенческим анализом, машинным обучением и комбинированием классов решений EPP и EDR.

- Для защиты от массовых атак критически важны профилактика социальной инженерии и своевременное устранение уязвимостей: регулярное обучение персонала, фильтрация электронной почты, контроль за вложениями и ссылками, а также эффективный процесс управления уязвимостями.

В текущем ландшафте киберугроз массовые кибератаки являются одной из ключевых угроз для организаций: за первые три квартала 2025 года массовой была каждая пятая успешная атака на организации (20%). Масштабный характер и высокая степень автоматизации подобных атак позволяют злоумышленникам проводить кампании, охватывающие тысячи жертв по всему миру.

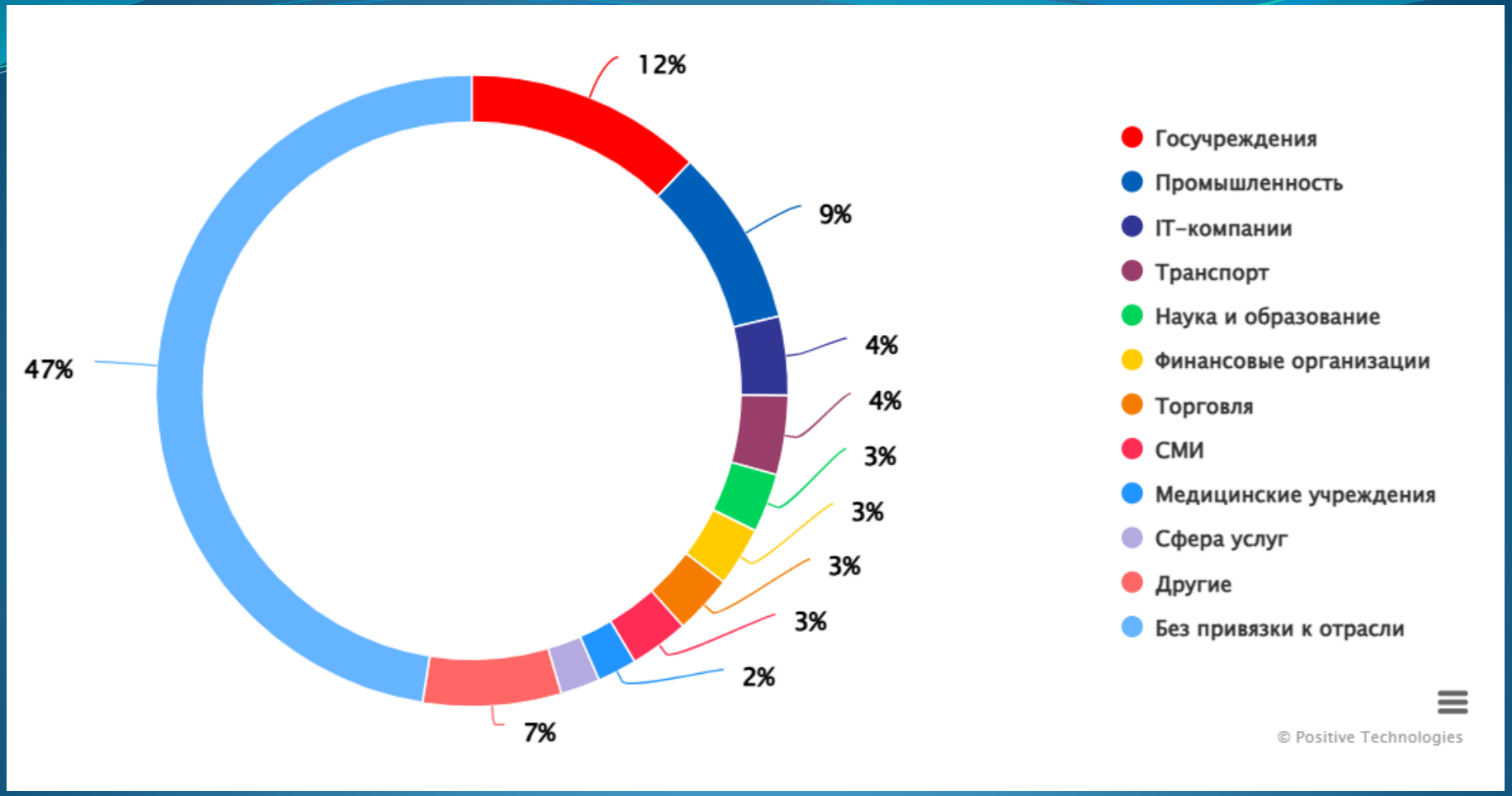
Так, в феврале 2025 года была обнаружена массовая кампания группировки вымогателей RansomHub, которая скомпрометировала более 600 организаций, в том числе в здравоохранении, финансовой сфере, а также предприятия критически важной инфраструктуры. Злоумышленники использовали уникальные методы шифрования, продвинутые техники обхода защиты и эксплуатацию известных уязвимостей. Это позволило им зашифровать критически важные файлы и требовать выкуп за их расшифровку.

Характерными признаками массовых кампаний являются:

- одинаковые признаки компрометации у множества разных жертв (например, одни и те же вредоносные файлы или домены);
- резкие всплески активности: сканирование сетей или попытки подключений исходят либо от одного и того же провайдера, либо с большого числа распределенных прокси-серверов;
- разнообразные цели атак, которые часто ограничиваются публично доступными сервисами — например, почтовыми серверами или системами удаленного доступа;
- быстрый захват как можно большего количества систем, а не детальная разведка.

Почти половина массовых атак (47%) происходит без привязки к конкретной отрасли: злоумышленники выбирают цели, стараясь охватить как можно больше жертв, эксплуатируя стандартные векторы атак и общие уязвимости, распространенные в инфраструктуре многих организаций.

Чаще всего жертвами массовых атак становятся госучреждения (12%) и промышленность (9%). Эти же отрасли наиболее часто страдают и в целевых атаках. Причина в их стратегической значимости, высокой ценности данных и в наличии системных уязвимостей как государственного сектора, так и промышленной отрасли.




**Категории жертв (доля массовых атак на организации, Q1–Q3 2025)**

Государственные структуры хранят конфиденциальную информацию о гражданах, процессах управления и национальной безопасности, что делает их главными объектами интереса злоумышленников. Их геополитическая значимость повышает привлекательность всех видов атак, особенно в условиях напряженной международной обстановки. Ярким примером служит массовая атака группировки Hazy Hawk, которая эксплуатировала неправильно настроенные DNS-записи, указывающие на заброшенные облачные сервисы.

Злоумышленники регистрировали новые ресурсы с теми же именами, перехватывая контроль над поддоменами известных организаций. В результате этой автоматизированной кампании были скомпрометированы десятки доверенных доменов, включая множество государственных сервисов, а также корпоративные домены крупных компаний. Через эти поддомены распространялись фишинг, поддельные приложения и вредоносная реклама, при этом злоумышленники использовали высокий рейтинг доверия родительских доменов для маскировки своих действий в поисковых системах.

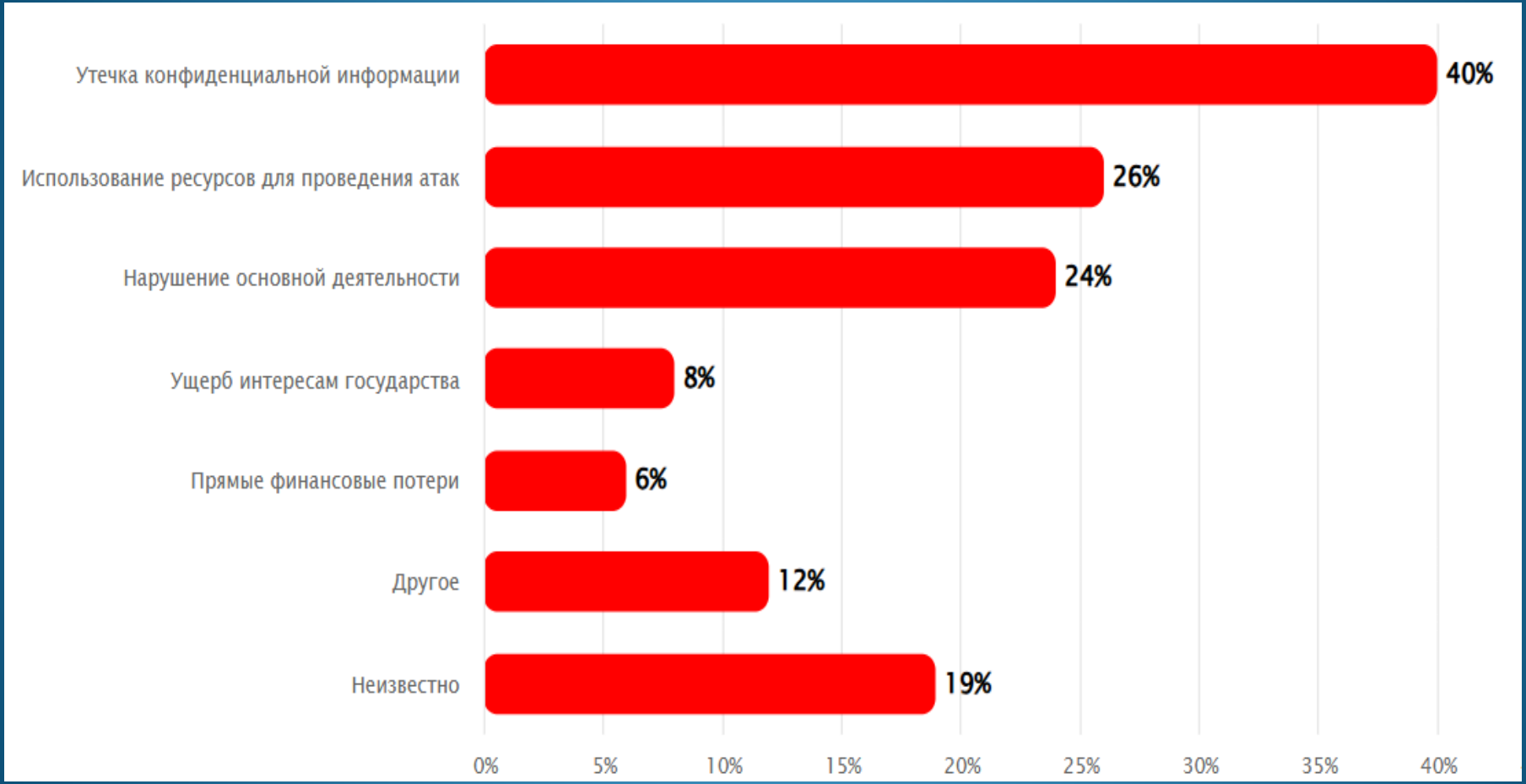
Промышленность также находится в зоне повышенного риска из-за активной цифровизации и интеграции информационных и операционных технологий, при этом уровень зрелости кибербезопасности в этой сфере остается низким. Производственные системы могут работать на устаревшем оборудовании без поддержки современных механизмов защиты, а нарушение технологического процесса может привести к остановке производства, финансовым потерям и даже к авариям. Так, в январе 2025 года группировка Rezet провела волну массовых атак на промышленные предприятия России.

Жертвами стали предприятия химической, пищевой и фармацевтической промышленности. Злоумышленники рассылали фишинговые письма с фальшивыми приглашениями на семинары по стандартизации оборонной продукции. Письма содержали архив с PDF-документом и вредоносной нагрузкой, запуск которой приводил к компрометации системы.

Массовые атаки способны приводить к серьезным последствиям для организаций, включая реализацию недопустимых событий: утечки конфиденциальных данных, остановку бизнес-процессов, потерю контроля над инфраструктурой и использование скомпрометированных систем для последующих атак.

Несмотря на отсутствие глубокой персонализации, присущей целевым атакам, масштаб и автоматизация позволяют наносить ущерб, сопоставимый с целевыми атаками.

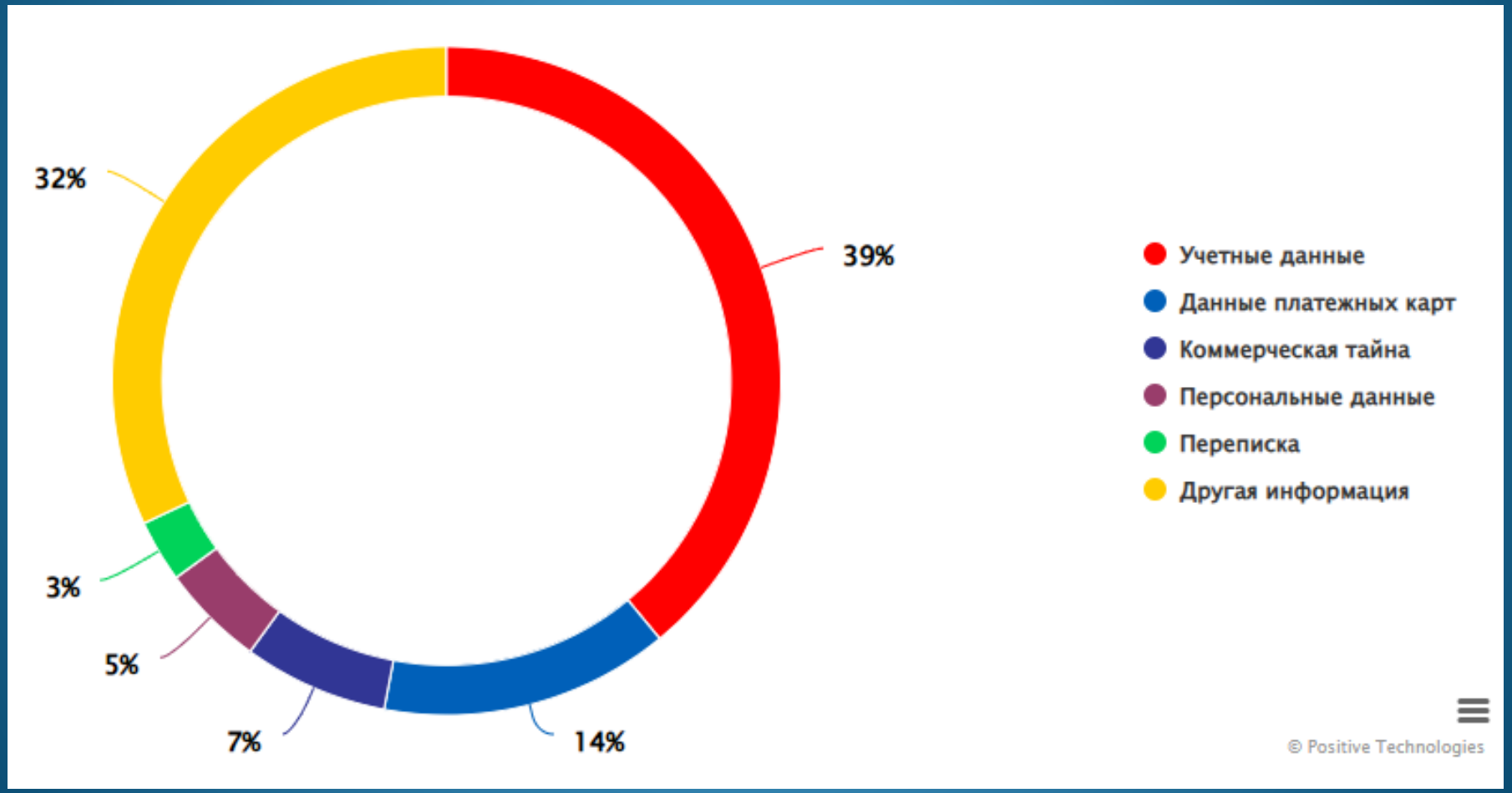
# Последствия массовых атак (доля успешных атак на организации, Q1–Q3 2025)



Самое частое последствие массовых атак — утечка конфиденциальных данных (40% успешных атак на организации). Чаще всего злоумышленники получают доступ к учетным данным (39% массовых атак, которые привели к утечкам), данным платежных карт (14%) и коммерческой тайне (7%).

В дальнейшем злоумышленники могут продать полученную информацию на теневых площадках — или использовать уже в целевых атаках (и это дополнительный риск для пострадавших организаций). Утечки могут стать причиной юридических санкций, репутационного ущерба, потери доверия со стороны партнеров и клиентов.

# Типы украденных данных (доля массовых атак на организации, Q1–Q3 2025)

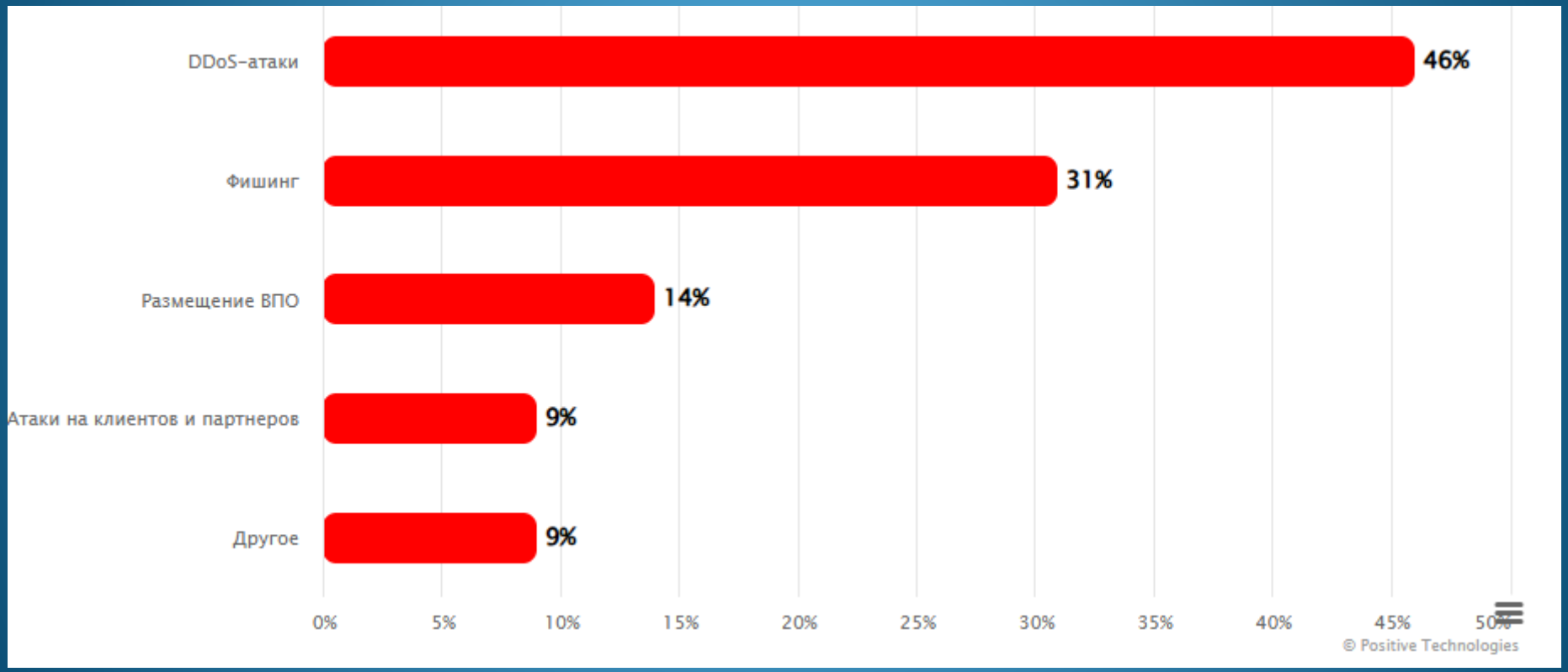


В 2025 году была выявлена кампания вредоносного ПО, распространяемого через поддельные проверки CAPTCHA. Через скомпрометированные сайты под видом проверки «Я не робот» в системе жертвы запускается инфостилер EDDIESTEALER. Он нацелен на кражу широкого спектра конфиденциальных данных, включая номера криптовалютных кошельков, учетные данные из браузеров, базы данных менеджера паролей, конфигурации FTP-клиентов и переписку из мессенджеров.

Более четверти массовых атак (26%) приводят к использованию скомпрометированных систем для проведения дальнейших атак, причем не только на организации, но и на частных лиц (это последствие специфическое именно для массовых кампаний). Чаще всего это DDoS-атаки с использованием ресурсов компании (46%), фишинговые атаки от лица третьих лиц или от лица жертвы (31%), а также использование ресурсов жертвы как канала распространения ВПО (14%) и атаки на клиентов или партнеров (9%). 7

Например, в январе 2025 года произошла компрометация интернет-магазина Casio UK и еще 17 сайтов, когда злоумышленники внедрили скрытый скрипт-скиммер в процесс оформления заказа. Этот скрипт перехватывал данные кредитных карт клиентов и передавал их на серверы атакующих. При этом сайты-жертвы использовались как доверенные площадки для сбора конфиденциальной информации, что повышало доверие со стороны пользователей и снижало вероятность обнаружения атаки. Так зараженная компания становится не только жертвой, но и инструментом в цепочке киберпреступлений — в данном случае каналом для кражи данных у клиентов.

# Способы использования скомпрометированных систем



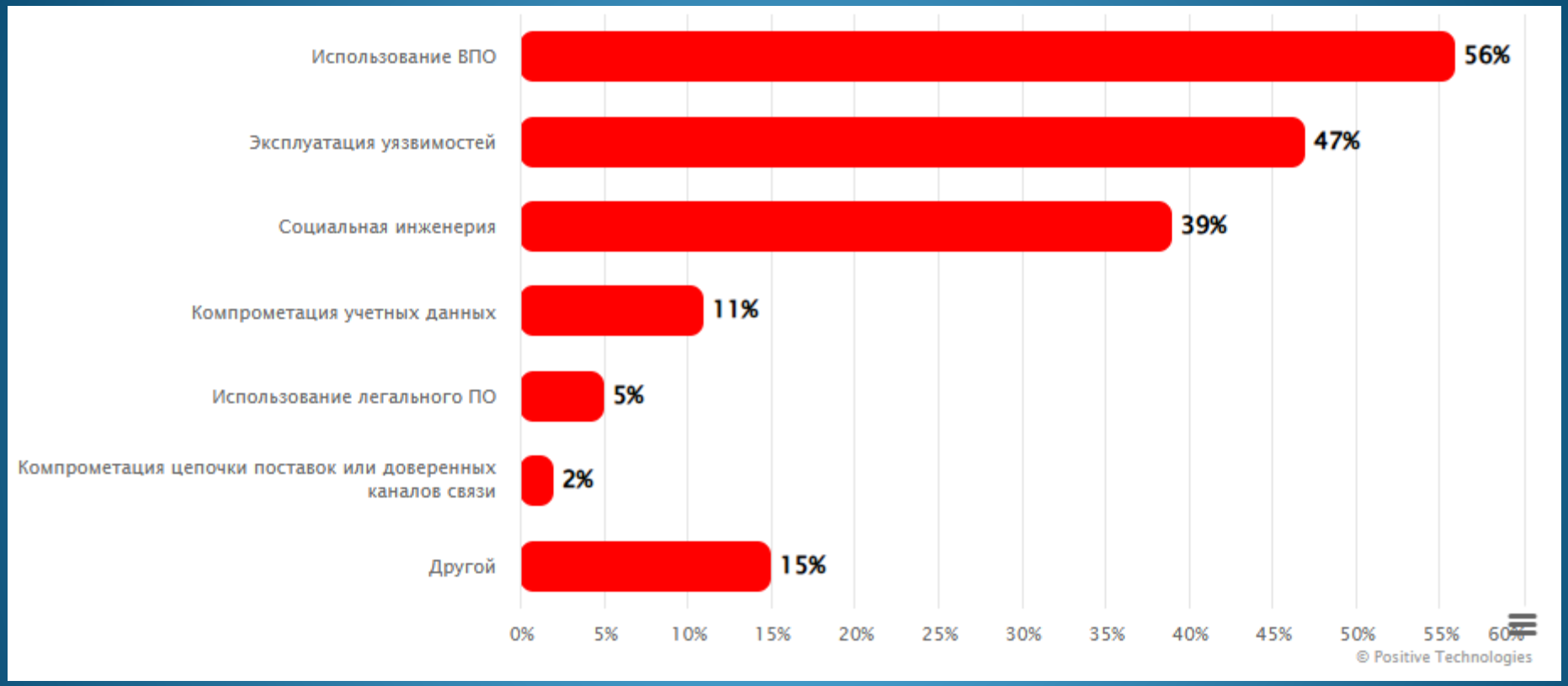
Практически каждая четвертая массовая атака за рассматриваемый период привела к нарушению основной деятельности организации (24%). Массовые атаки приводят к потере доступа к инфраструктуре или данным, сбоям в предоставлении сервисов клиентам и к нарушению внутренних бизнес-процессов. Например, уязвимость CVE-2025-6543 в Citrix NetScaler, связанная с переполнением памяти, массово использовалась злоумышленниками в атаках, направленных на отказ в обслуживании. Несколько организаций в Нидерландах были успешно атакованы с помощью этой уязвимости, а прокуратура королевства столкнулась со значительными сбоями в работе: у сотрудников не было доступа в интернет, с ними нельзя было связаться по электронной почте, а функциональность систем Citrix была ограничена.

Не стоит забывать, что, помимо прямых последствий, массовые атаки порождают ряд системных проблем. Они вызывают многократное увеличение нагрузки на защитные механизмы и команды реагирования. Одновременное появление множества инцидентов приводит к перегрузке команд SOC, CSIRT и поставщиков услуг MDR/EDR, что затрудняет своевременное выявление и отражение угроз. Постоянный поток событий генерирует большое количество ложных срабатываний, истощает аналитические ресурсы и способствует профессиональному выгоранию специалистов. В результате даже эффективные системы защиты оказываются под угрозой перегрузки, снижая общую готовность к реагированию и повышая риск критически опасных инцидентов.

## Как происходят массовые атаки

### ВПО — главный инструмент

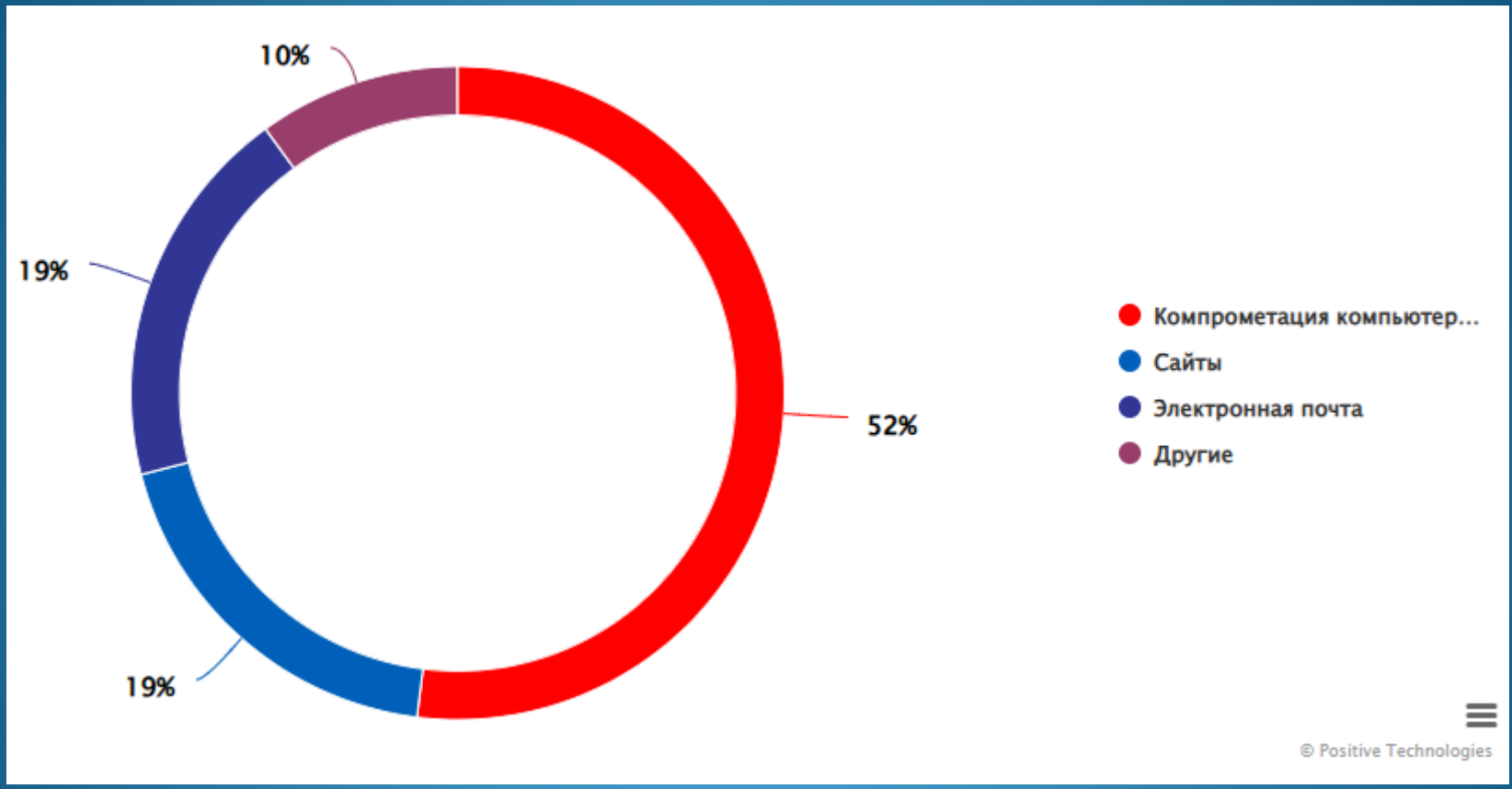
Главный принцип массовых атак — это охват большого числа жертв при минимальных затратах. Ключевую роль в них играет вредоносное программное обеспечение: его злоумышленники использовали в 56% успешных массовых атак. Одной из основных причин является его высокая эффективность при относительной простоте применения: оно позволяет злоумышленникам не только проникнуть в инфраструктуру и закрепиться в ней, но и развивать атаку вплоть до полной компрометации домена и критически важных систем, что может привести к реализации недопустимых событий. На начальных этапах массовых атак именно ВПО чаще всего используется для получения первичного доступа — будь то через вредоносные почтовые вложения, фишинговые сайты или эксплуатацию уязвимостей. Современный ландшафт ВПО — разнообразный и динамичный, а выбор инструментов определяется целями атакующих и их ресурсами, при этом вложения в разработку или покупку готового ВПО быстро окупаются за счет масштабности кампаний.



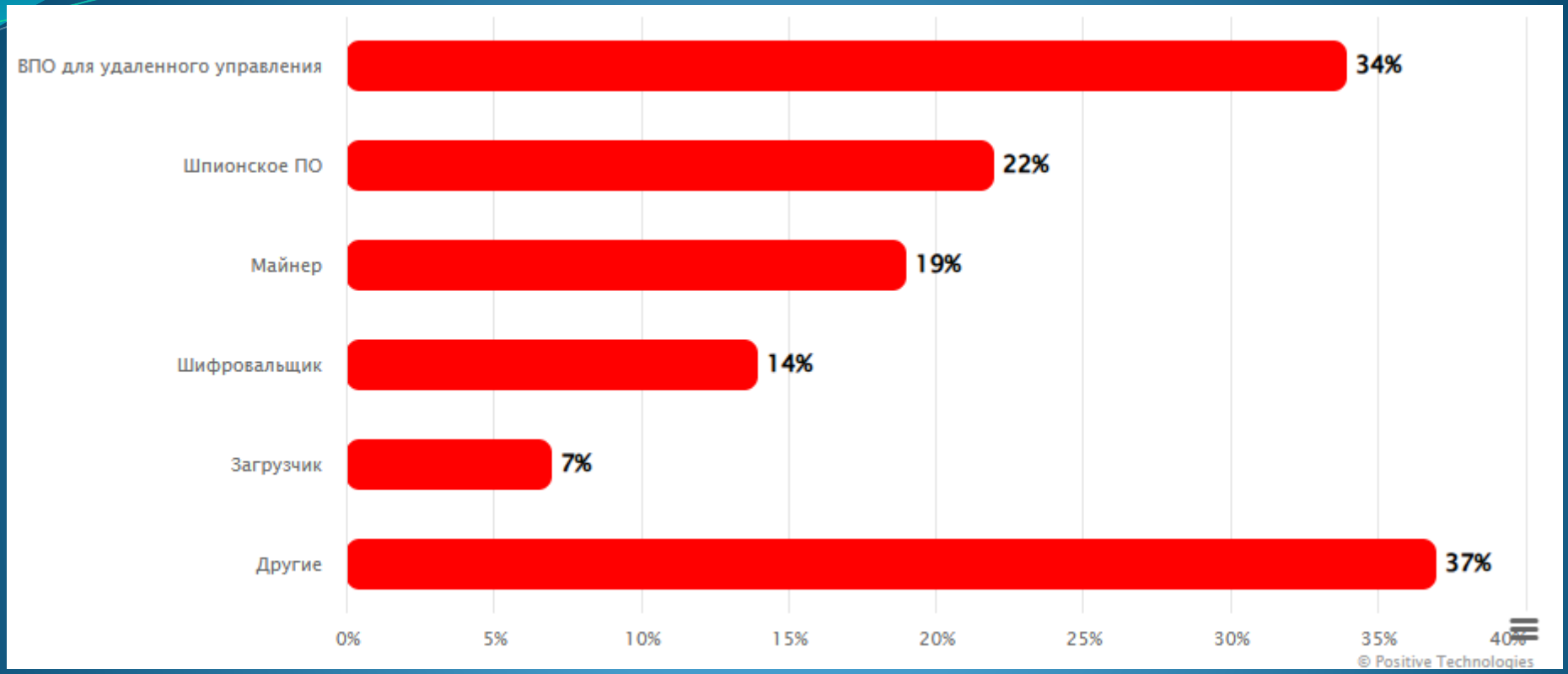

## Методы массовых атак

Второй причиной является доступность ВПО: современный теневой рынок предлагает широкий выбор готовых вредоносных решений для покупки или по подписке, включая инфостилеры, загрузчики, RAT и даже билдеры шифровальщиков в рамках моделей ransomware as a service (RaaS). Многие инструменты стоят от нескольких десятков до нескольких сотен долларов, а утечки мануалов известных группировок, таких как LockBit и Conti, позволяют даже начинающим злоумышленникам эффективно проводить сложные атаки. Затраты на создание или аренду ВПО (например, по модели MaaS/RaaS) несопоставимы с потенциальной прибылью — будь то выкуп, продажа украденных данных или доступа к инфраструктуре. Так, в исследовании рынка киберпреступности мы рассказывали, что чистая прибыль от успешной кибератаки может в пять раз превышать затраты на ее организацию.

Наиболее популярный канал распространения вредоносного ПО — компрометация компьютеров, серверов и сетевого оборудования (52%): злоумышленники взламывают устройства, подбирая учетные данные или эксплуатируя уязвимости. Вторым каналом являются сайты (19,5%): заражение происходит при посещении поддельных или скомпрометированных ресурсов, часто через автоматическую загрузку ВПО. На третьем месте электронная почта (18,9%), которая остается одним из самых эффективных методов доставки фишинговых писем с вредоносными вложениями или ссылками.




**Способы распространения ВПО**




**Какие типы ВПО используются в массовых атаках**

ВПО для удаленного управления (remote access trojan, RAT) занимает первое место среди типов вредоносного ПО в массовых кибератаках, его использовали в каждой третьей успешной атаке (34% случаев). Оно идеально соответствуют ключевым характеристикам массовых атак, которые отличаются высокой степенью автоматизации, параллелизма и масштабируемости.

RAT дает злоумышленнику полный контроль над зараженными устройствами: данный тип ВПО может выполнять команды, перемещаться по сети, запускать другие программы, собирать данные и устанавливать дополнительное ПО. Это делает такие инструменты идеальными для масштабирования атаки: после успешного заражения одного устройства, злоумышленник может использовать его как входную точку для дальнейшего распространения по внутренней сети или для сбора информации. Так, в марте 2025 года группировка Head Mare провела волну атак на промышленные предприятия России, затронув около 100 организаций. Злоумышленники рассылали фишинговые письма с ZIP-вложениями. В результате на зараженных системах устанавливался Python-бэкдор PhantomPyramid, предназначенный для удаленного управления, а также легитимный инструмент MeshAgent, используемый злоумышленниками для маскировки под административное ПО.

Кроме того, злоумышленники активно используют RAT для создания ботнетов — сетей зараженных устройств, которые могут использоваться для DDoS-атак, рассылки спама, фишинга или добычи криптовалюты. Благодаря автоматизированному управлению такие ботнеты легко масштабируются: новые жертвы добавляются в сеть, а команды распространяются на все узлы одновременно.

Шпионское ПО и майнеры применялись в каждой пятой атаке (22% и 19% соответственно). Однако стоит отметить, что шпионское ПО сохраняет высокую актуальность как в массовых, так и в целевых атаках благодаря своей универсальности, при этом майнеры становятся все менее выгодным инструментом из-за снижения доходности криптомайнинга. Их применение оправдано только при масштабном заражении очень большого числа устройств: они приносят небольшую прибыль с каждого устройства, но суммарный эффект достигается за счет широкого охвата, что делает их типичным элементом массовых кампаний, распространяемых через фишинг или эксплуатацию уязвимостей. Однако в целевых атаках майнеры практически не используются: их работа приводит к заметному падению производительности, что быстро привлекает внимание.

Шифровальщики (14%) сегодня остаются основным инструментом целевых атак, а благодаря широкой доступности платформ RaaS и высокой степени автоматизации их использование будет расти и в массовых атаках. Так, в феврале 2025 года российский малый и средний бизнес столкнулся с новой угрозой — вымогательской программой PE32. Этот шифровальщик — один из самых сложных и продвинутых, он использует стандарты постквантовой криптографии для шифрования данных в три раунда. Жертвами стали десятки предприятий, суммы выкупа варьировались от 500 до 150 000 долларов, выплачиваемых в биткоинах.

Технологии, ранее характерные для целевых вымогательских атак, все активнее адаптируются для массового применения: на теневых форумах появляется все больше объявлений о создании RaaS-сервисов, предлагающих готовые билдеры, мануалы и инфраструктуру для запуска кампаний. Благодаря росту конкуренции на криминальном рынке злоумышленники стремятся модернизировать свои платформы, добавляя уникальные функции и улучшая механизмы маскировки, чтобы привлечь как можно больше партнеров-исполнителей. Это позволяет даже малоопытным преступникам организовывать высокотехнологичные кампании с автоматизированной доставкой и обходом защиты.

В результате мы можем ожидать дальнейшего роста числа и доли массовых атак с использованием шифровальщиков, поскольку низкий порог входа, высокая степень автоматизации и значительная монетизация делают такие сервисы крайне привлекательными в условиях эскалации киберпреступности. Так, на русскоязычных киберпреступных форумах активизировалась новая платформа RaaS под названием Pay2Key, построенная на базе шифровальщика Mimic и ориентированная на массовые атаки с возможностью персонализации кампаний. Несмотря на негласные запреты на атаки по СНГ, злоумышленники провели как минимум три фишинговые кампании против российских компаний из сферы финансов, строительства и ритейла. Атаки начинались с рассылки фишинговых писем, содержащих либо вредоносные вложения в формате RAR, либо ссылки на файлы в Dropbox. После запуска самораспаковывающегося архива (SFX) на устройство загружался шифровальщик Pay2Key.

В 2025 году происходит явный переход от простых атак к более сложным адаптивным схемам. Теперь атаки гораздо труднее обнаружить традиционными сигнатурными методами; подтверждается общий тренд на переход к адаптивным угрозам.

**Искусственный интеллект в разработке ВПО**

Искусственный интеллект и методы машинного обучения все активнее используются злоумышленниками для подготовки и проведения атак. Согласно исследованию, в 5% техник из матрицы MITRE ATT&CK уже зафиксировано применение ИИ, включая подтехнику T1587.001 «Разработка собственных средств: вредоносное ПО».

Уже известны и случаи, когда ИИ использовался в подготовке именно массовых атак. Так, исследователи обнаружили массовую кампанию группировки Koske, которая демонстрирует признаки разработки ВПО с привлечением больших языковых моделей (LLM). Атака начинается с компрометации интерактивной среды разработки JupyterLab, после чего вредонос внедряется в систему жертвы через JPEG-изображения со встроенным исполняемым кодом. После загрузки файла запускается двухэтапная атака: в памяти исполняется библиотека на языке C, реализующая руткит. Параллельно запускается шелл-скрипт, который скачивает и активирует криптомайнер. Код Koske отличается высокой структурированностью, наличием подробных комментариев — все это указывает на использование ИИ. Кроме того, вредонос проявляет адаптивное поведение: проверяет доступ в интернет через curl, wget и raw TCP, автоматически восстанавливает соединение через прокси и переключается между майнинговыми пулами. Такие характеристики позволяют предположить, что ИИ не просто участвовал в генерации кода, но и способствовал созданию более автономной, скрытной и устойчивой угрозы.

**Маскировка вредоносного ПО**

Современные злоумышленники все чаще комбинируют проверенные временем инструменты с передовыми методами скрытия активности. Например, помимо генерации вредоносного ПО, злоумышленники применяют языковые модели для обфускации кода, что значительно усложняет его обнаружение и анализ средствами защиты информации.

Разработка вредоносного ПО развивается по двум параллельным направлениям:
переработка устаревшего кода для расширения функциональности;
совершенствование методов маскировки для обхода систем обнаружения.

Помимо методов обфускации, использование искусственного интеллекта может помочь злоумышленникам с обходом существующих систем защиты. Так, в августе 2025 года компания ESET обнаружила на VirusTotal программу-вымогателя на основе ИИ под названием PromptLock. Программа генерирует Lua-скрипты через модель GPT прямо на лету, из-за чего индикаторы компрометации меняются при каждом запуске. Помимо шифрования, программа может быть использована для кражи данных или для их уничтожения. Позже исследователи узнали, что это лишь проверка концепции (PoC), а не полностью рабочее ВПО, развернутое «в дикой природе». Мы можем видеть, что подобные системы уже достаточно сложны, чтобы обмануть экспертов по безопасности, заставив их думать, что перед ними настоящее вредоносное ПО.

**Боты нового поколения**

Эволюция массовых атак проявляется и в росте интеллектуальных бот-угроз, о чем свидетельствует исследование Imperva: если прежде боты были примитивными и их легко было обнаружить, то теперь, благодаря внедрению искусственного интеллекта, они превращаются в адаптивные, устойчивые к детектированию системы. Например, злоумышленники все чаще используют генеративный ИИ и платформы «бот как услуга» (BaaS), чтобы автоматизировать создание вредоносных сценариев даже без глубокой технической подготовки, что резко снижает порог входа для атак. При этом современные боты применяют машинное обучение для анализа защитных механизмов, маскировки под человека — через поддельные браузерные идентификаторы, residential-прокси и headless-браузеры — и многократного повторения атак до достижения цели. Традиционные меры, основанные на сигнатурах, часто не срабатывают, поэтому боты все лучше имитируют легитимное поведение пользователей и ускользают от обнаружения.

## Выводы

Массовые кибератаки в 2026 году останутся одной из распространенных и опасных угроз для организаций. Растет число автоматизированных, масштабируемых кампаний вредоносного ПО, и конечные устройства — компьютеры, серверы, виртуальные рабочие места — становятся главной мишенью злоумышленников. Раньше системы защиты успешно выявляли атаки по простым сигнатурам и известным уязвимостям, но в современных массовых атаках злоумышленники используют обфускацию кода, динамическую генерацию вредоносных файлов, ботнеты с адаптивной логикой и многоэтапные цепочки заражения. Эти техники позволяют избегать методов обнаружения, основанных на статических признаках и сигнатурах, маскировать активность под легитимную и быстро масштабировать атаки. В такой среде эффективная защита невозможна без комплексного подхода к безопасности конечных устройств (endpoint security). По данным AV-TEST, ежедневно в мире появляется более 450 тыс. новых вредоносов и нежелательных приложений. Объем известных образцов превысил 800 млн в базе AV-ATLAS. Общее число новых угроз показывает ежегодный устойчивый рост. Традиционные антивирусные решения, основанные исключительно на сигнатурном анализе, уже не способны обеспечить достаточный уровень защиты. Они отстают от темпов появления новых угроз. Даже эвристические методы анализа оказываются недостаточными перед лицом ИИ-обфускации и полиморфного кода.

На смену им приходят современные платформы защиты конечных точек (endpoint protection platform, EPP), которые формируют первый и самый важный рубеж обороны. EPP-решения объединяют несколько технологий в единую систему: антивирусный движок с анализом сигнатур и эвристикой, обнаружение и блокировку на основе эмуляции поведения ВПО, защиту от шифровальщиков, контроль устройств и приложений, защиту от сетевых угроз.

Современные платформы защиты конечных точек должны обеспечивать многоуровневый подход и максимальную оперативность. Для обеспечения эффективной защиты современное EPP-решение должно содержать все актуальные сигнатуры за последние три-четыре года, покрывающие все основные семейства вредоносного ПО.

Учитывая, что ежедневно появляется около полумиллиона новых угроз, критически важен не только размер базы, но и скорость ее обновления. Чем чаще актуальные сигнатуры и индикаторы доходят до агентов, тем быстрее система обнаружит недавно появившиеся угрозы. Оптимально обновлять базы несколько раз в день.

Хотя технические средства играют ключевую роль, безопасность конечных точек напрямую зависит и от человеческого фактора. Многие массовые атаки начинаются с фишинговых писем, содержащих вредоносные вложения или ссылки. Поэтому профилактика социальной инженерии становится важной частью защиты конечных устройств: регулярное обучение сотрудников, симуляции фишинговых атак, фильтрация почты. Кроме того, на безопасность конечных точек напрямую влияет управление уязвимостями. Средства защиты конечных устройств должны быть интегрированы в процесс устранения уязвимостей: это обеспечивает автоматизированное сканирование, актуальную картину уязвимостей и упрощает контроль исполнения мер по их устранению.

## 2. Распространённые проблемы безопасности на промышленных предприятиях

**1. Непроектные автоматизированные рабочие места (АРМ) со внешним выходом в интернет.**

**В технологической сети обнаруживаются непроектные АРМ для работы с базами данных (с подключёнными устойствами беспроводного доступа). Доступа к таким АРМ аудиторы обычно не получают, а следовательно, не могут проанализировать, есть ли на ней лицензированное ПО или пароль, обновлена ли операционная система и у кого ещё есть доступ к АРМ (а соответственно, и к технологической сети). С непроектного АРМ сотрудник мог подключаться к сети не только в рабочее время. Подобные АРМ представляют угрозу для всей технологической сети предприятия.**

**2. Открытый Wi-Fi.**

**Используется для удобного подключения к серверам группы администраторов.**

**С его помощью злоумышленник может получить доступ к технологической сети без проникновения в закрытые серверные помещения и физического доступа к серверам.**

## 3. Подключение по RDP.

Протокол удаленного рабочего стола работает путем установления соединения между компьютером пользователя (RDP-клиент) и удаленным сервером или компьютером, позволяя клиенту получить доступ к рабочему столу удаленного компьютера и управлять им.

При неограниченном доступе к компьютеру нарушитель может подключиться через рабочую станцию к остальным АРМ.
Злоумышленнику необязательно повышать свои права на узле, к которому он получил доступ, потому что в этих ярлыках уже прописаны логины и пароли администраторов для подключения.
Хакер может получить их по RDP-соединению без физического доступа к месту, а уже потом закрепиться в сети.

**4. Непроверенные сетевые устройства.**

**Такие устройства применяются в ходе пуско-наладочных работ, т.к. подрядчики часто используют различные сетевые устройства или встроенные модули беспроводной связи для удобства настройки, обновления, и т.п.**

**После проведения работ они могут остаться включенными, могут в активном состоянии собственными модули беспроводной связи технологических устройств.**

**Ряд сетевых устройств (принтеры, сканеры) могут иметь беспроводные интерфейсы. Обычно это слабозащищенные каналы.**

**Есть практика обслуживания АСУ ТП иностранными подрядчиками с организованным удалённым доступом через интернет. Любые сетевые устройства подвергают технологическую сеть рискам.**

**5. Отсутствие сегментации в сети.**

**В ходе аудитов часто обнаруживаются прямые подключения корпоративных сетей к серверам приложений в обход межсетевых экранов.**

**Технологическая и корпоративная сети должны быть разделены, физически и логически.**

**Если нет разделения на сегменты, сотрудник из корпоративной части сети может случайно или намерено проникнуть в технологическу.**

**Многие промышленные предприятия пострадали от шифрования Petya в 2017 году. Попав в выделенную корпоративную сеть, вредоносная программа смогла заразить сеть технологическую.**

**6. Использование паролей по умолчанию.**

**У всех вендоров есть свои стандартные кодовые слова для интеграторов.**

**На предприятиях используются одинаковые или взятые из инструкций по эксплуатации пароли.**

**Если на предприятии нет политики смены паролей, то они остаются неизменными и им может овладеть злоумышленник.**

**7. Отсутствие политики «чистого стола».**
**АРМ технологического процесса должны содержать только те программы и файлы, которые к нему непосредственно относятся**

**8. Открытый физический доступ к компонентам АСУ ТП. Ограничение физического доступа к компонентам АСУ ТП подразумевает электронные замки помещений, контроль допуска на объект, а также пломбирование шкафов с оборудованием.**
**В ходе проверок оказалось, что к части помещений с КТС АСУ ТП (комплекс технических средств АСУ ТП) есть бесконтрольный доступ, а некоторые не запираются.**

**9. Отсутствие обновлений и антивирусного ПО.**

**Несмотря на наличие антивирусных программ, на 90 % производств они не обновляются.**

**В ходе аудитов были обнаружены необновлённые операционные системы, РСУ (распределённая система управления), ПАЗ (противоаварийная защита) и др.**

**Каждая система РСУ / ПАЗ гарантированно работает на конкретной версии ОС, а следовательно, для обновления последней нужно обновить и первую.**

**Это, в свою очередь, влечёт за собой огромные вложения в модернизацию системы, так как поднятие ревизии — это платная услуга, которая порой требует и обновления контроллеров. Как следствие, РСУ / ПАЗ и операционная система остаются необновлёнными. Аналогичная ситуация — и с антивирусным ПО.**

**Наличие антивируса и своевременные обновления закрывают выявленные новые уязвимости.**

| | |
|---|---|
| Отсутствие обновлений и антивирусного ПО | 99% |
| Подключение по RDP | 85% |
| Открытый физический доступ к компонентам АСУ ТП | 75% |
| Непроверенные сетевые устройства | 70% |
| Отсутствие сегментации в сети | 65% |
| Открытый Wi-Fi | 60% |
| Использование паролей по умолчанию | 55% |
| Отсутствие политики «чистого стола» | 30% |
| Непроектные АРМ с внешним выходом в интернет | 15% |

Самые распространённые проблемы безопасности среди промышленных компаний

**Проблемы с безопасностью, выявленные во время аудита предприятий.**

**1.Предприятия обязаны принимать меры по аутентификации, идентификации и управлению доступом. К сожалению, требования выполняются лишь формально. Аудиты показали, что операторы работают под одной учётной записью и даже не меняют роли в среде визуализации и диспетчеризации АСУ ТП.**

**2. Зачастую на объектах не выполняются требования к подразделениям и специалистам по обеспечению ИБ: На 87 % предприятий либо нет соответствующих подразделений, либо обязанности возложены на сотрудников без должной квалификации и должных навыков.**

**3. В 8 из 10 организаций члены комиссии по категорированию объектов КИИ не имеют должных знаний для проведения работ и подписывали акты без ознакомления с ними.**

**4. Аналогичная ситуация — с обязательными регламентами, различными журналами регистрации, выдачи накопителей и паролей: несмотря на их наличие, в аудируемых объектах не было записей и подписей.**

**Согласно проекту постановления Правительства РФ «О порядке перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры», объекты КИИ обязаны перейти на отечественное ПО и сетевое оборудование. Однако на предприятиях продолжается использование иностранное оборудование и ПО.**

# Технические средства защиты промышленных систем.

Промышленные предприятия постоянно наращивают объем цифровизации. Одни и те же IT компоненты находят применение в автоматизации операционных и технологических процессов. Это значит, что для злоумышленника нет особой разницы, что атаковать: корпоративную или технологическую сеть. Способы и сценарии нападения одинаковы. При этом уровень кибербезопасности производственных систем часто ниже, чем в корпоративных.

В качестве примера комплексного решения для защиты промышленных предприятий приведём платформу промышленной кибербезопасности от компании Positive Technologies — PT Industrial Cybersecurity Suite (PT ICS).
Платформа построена по принципу единого портфеля сервисов и продуктов для корпоративных и технологических ИТ-инфраструктур, то есть одни и те же её компоненты могут одинаково эффективно применяться для решения задач по защите и построению процессов управления кибербезопасностью как в типовых корпоративных ИТ-инфраструктурах, так и в производственно-технологических, построенных в том числе на базе проприетарных технологий производителей средств промышленной автоматизации.

**В состав PT ICS входят:**

**Продукты.**
**MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox, PT XDR — комбинация ключевых продуктов Positive Technologies обеспечит комплексную кибербезопасность всего предприятия, включая сегмент АСУ ТП (SCADA).**

**Сервисы.**
**Полный спектр услуг по анализу защищенности промышленных систем и услуги PT ESC по обнаружению, реагированию и расследованию сложных инцидентов в АСУ ТП (SCADA).**

**Решение.**
**PT ICS помогает обнаружить злоумышленника на всех этапах развития атаки в промышленных средах и своевременно на них отреагировать. Платформа обеспечивает комплексную безопасность в индустриальном сегменте компании, начиная от сетевых узлов и заканчивая технологическими устройствами**

**PT ICS включает в себя такие классы продуктов, как SIEM, Vulnerability Management, NTA, EDR, Sandbox, Incident Management.**

**Платформа решает следующие прикладные задачи по кибербезопасности:**

**Обнаружение целевых и сложных угроз на конечных точках и реагирование на них.**

**Контроль изменений конфигураций, настроек безопасности, пользовательских политик доступа.**

**Обнаружение и анализ SCADA-специфичных вредоносных программ, инструментов APT.**

**Глубокий анализ трафика технологических сетей, выявление атак и аномалий, проактивный поиск угроз (Threat Hunting).**

**Управление уязвимостями индустриальных систем, построение процессов патч-менеджмента.**

**Обнаружение и управление инцидентами из области безопасности в промышленной инфраструктуре.**

**Автоматизация взаимодействия специалистов отдельных служб при управлении инцидентами, информировании, реагировании, расследовании, а также взаимодействия с НКЦКИ.**

**Ключевой особенностью и технологическим преимуществом PT ICS является применение кросс-продуктовых пакетов экспертизы, которые позволяют использовать все компоненты платформы даже на прикладном уровне АСУ ТП, где встречается весьма большое количество проприетарных технологий и компонентов. Кросс-продуктовые пакеты экспертизы ориентированы на поддержку продуктов и технологий отдельных производителей средств промышленной автоматизации (вендор-ориентированность) и включают в себя: скрипты сканирования SCADA и прошивок; роботы поиска уязвимостей компонентов АСУ ТП; транспорты к проприетарному ПО и прошивкам для сбора событий; нормализацию событий SCADA и прошивок; кейс-ориентированные корреляции; поддержку промышленных сетевых протоколов; технологии обнаружения цепочек инцидентов в технологическом трафике; эмуляторы технологических сред для выполнения поведенческого анализа файловых объектов; сигнатуры для обнаружения вредоносных программ, специфичных для SCADA или прошивок; подтверждение технической и функциональной совместимости с программным обеспечением SCADA и проприетарным системным ПО, прошивками.**

# Продукты PT ICS

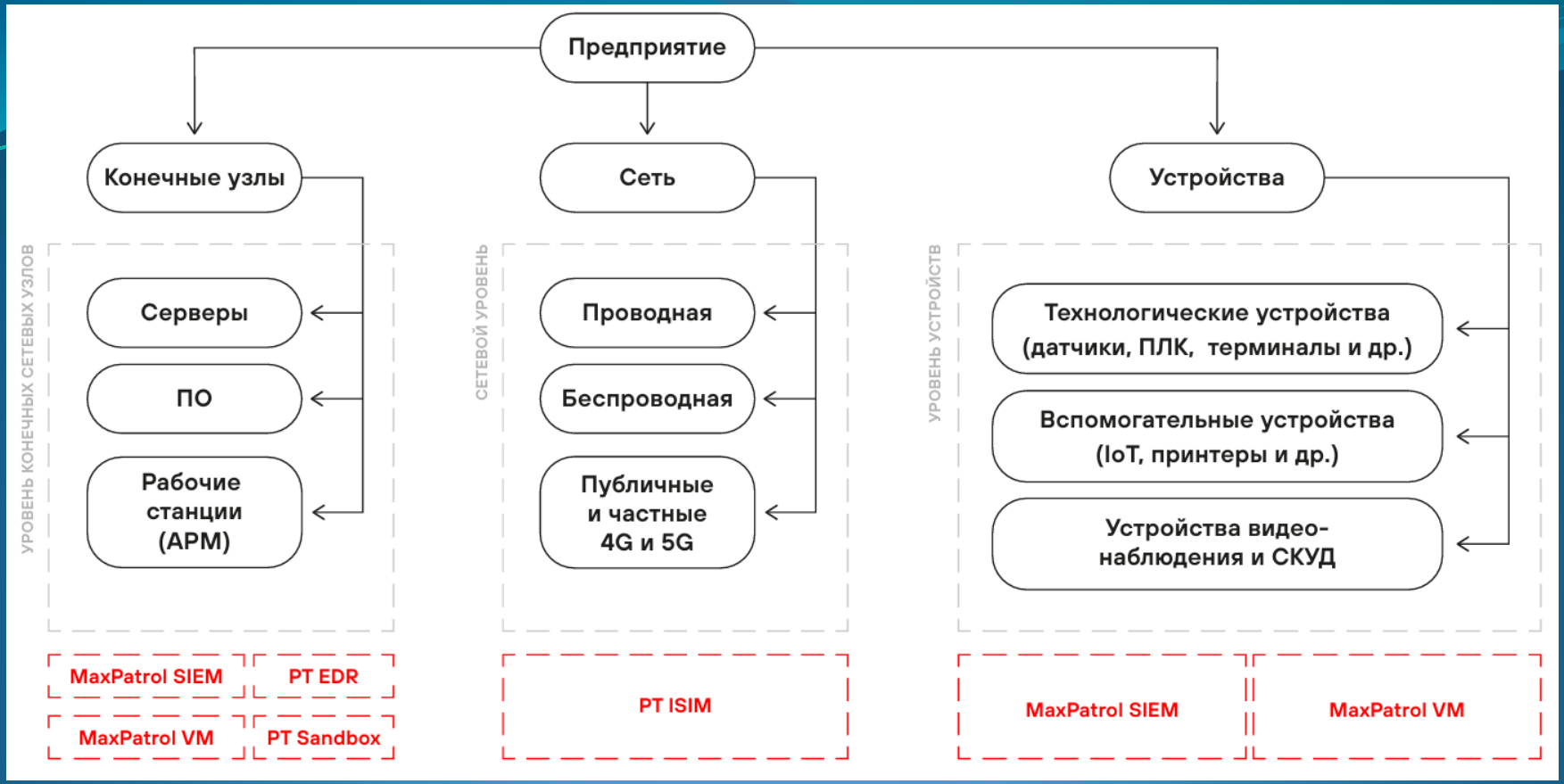
**MaxPatrol SIEM** для промышленности. Контролирует активность программного обеспечения и поведение пользователей на конечных узлах. Обнаруживает во всей IT инфраструктуре предприятия инциденты информационной безопасности и позволяет наладить процесс управления ими. Поддерживает иностранные и отечественные компоненты АСУ ТП (SCADA) «из коробки».

**MaxPatrol VM** для промышленности. Помогает построить эффективный процесс управления уязвимостями для всего предприятия. Собирает полные данные о компонентах технологической сети, выявляет уязвимости и контролирует их устранение.

**PT ISIM.** Осуществляет глубокий анализ трафика технологических систем. Предоставляет инструменты для проактивного поиска угроз (threat hunting), автоматически строит вектор атаки и делает ретроспективный анализ трафика. Поддерживает более 100 сетевых протоколов.

**PT Sandbox** для промышленности. Обнаруживает в файлах и ссылках неизвестное ВПО, нацеленное на компоненты АСУ ТП (SCADA) иностранных и отечественных производителей. Осуществляет статический и динамический анализ объектов как с узлов, так и из других источников. Дает возможность настроить среду эмуляции, «приманки» и состав ПО с учетом специфики компании.

**PT XDR** для промышленности. EDR-агенты PT XDR собирают и анализируют данные с конечных узлов, помогают осуществлять проактивный поиск угроз (threat hunting) и блокировать киберугрозы. Поддерживает популярные ОС «из коробки». Агенты адаптированы для работы на предприятиях




Все продукты платформы PT ICS разворачиваются в производственном сегменте компании. MaxPatrol SIEM собирает и анализирует журналы компонентов АСУ ТП. MaxPatrol VM получает всю информацию об активах и видит уязвимости в промышленном сегмента компании. PT ISIM анализирует сетевой трафик промышленного оборудования. PT Sandbox анализирует файлы и ссылки из почты, трафика, общих сетевых папок и конечных узлов АСУ ТП. PT XDR дает инструменты автоматического и выборочного реагирования на угрозы. Все это позволяет увидеть и предотвратить реализацию неприемлемых для бизнеса событий на каждом этапе развития атаки.

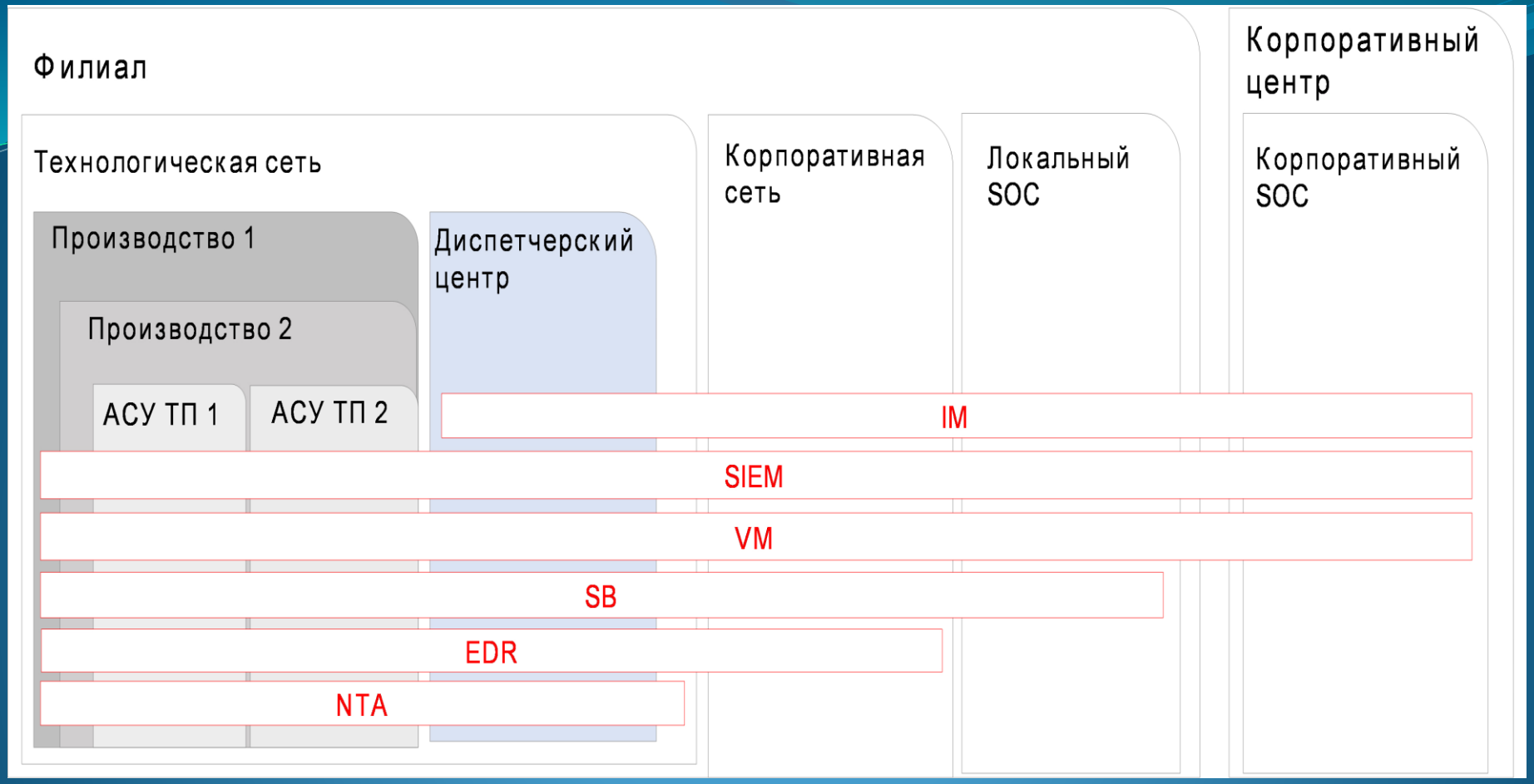



Рисунок 5. Базовая архитектура платформы PT ICS

**Анализ сетевого трафика (NTA) – это метод обнаружения вредоносных программ и аномалий различного типа, основанный на проверке данных, проходящих через узлы сети или по каналам передачи данных. Обычно NTA используется для:**

- **Сбора данных о том, что происходило и происходит в сети в режиме реального времени;**
- **Обнаружения вредоносных программ;**
- **Обнаружения уязвимых протоколов и шифров;**
- **Диагностики необычно медленной сети;**
- **Устранения «слепых зон» в защите и охвата комплексным мониторингом всей инфраструктуры.**

**Endpoint Detection & Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее.**
**В отличие от антивирусов, задача которых — бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При этом EDR-решения не могут полностью заменить антивирусы (EPP), поскольку эти две технологии решают разные задачи.**

**SB (Security Bypass) Обход механизмов безопасности.**
**VM (Virtual machine) виртуальная машина.**
**SIEM (Security information and event management) — это объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информацией о безопасности, и SEM (Security event management) — управление событиями безопасности.**
**Incident Management (IM) - управление инцидентами.**


Поддерживаемые российские АСУ ТП: Производитель AdAstrA (SCADA TRACE MODE 6), «Атомик Софт» («Альфа платформа»), «МПС софт» (MasterSCADA 3.12), «ПРОСОФТ» (AstraRegul), «РЕДКИТ ЛАБ» (Redkit SCADA 2.0).

Поддерживаемые иностранные АСУ ТП
AVEVA (Wonderware System Platform 2014, 2017),
Siemens (SIMATIC STEP 7 v5, SIMATIC TIA Portal Advanced/Pro 15.1*, SIMATIC TIA Portal Basic 15.1*, SIMATIC WinCC 7.4*, SIMATIC WinCC flexible 2007–2008),
Yokogawa (CENTUM VP R4–R6, ProSafe-RS R2–R4)

# Выводы

2025 год станет переломным для кибербезопасности промышленных сетей в России. Кратное увеличение числа и сложности атак, появление новых типов угроз на базе ИИ и усиление геополитического давления создают беспрецедентные вызовы для операторов КИИ.
Критически важным становится переход от формального соблюдения требований к построению реально работающих систем защиты. Организации должны инвестировать в современные технологии безопасности, обучение персонала и создание культуры кибербезопасности.

Государственные регуляторы продолжат ужесточение контроля и требований, что должно стимулировать повышение уровня защищенности КИИ. Однако успех в противодействии киберугрозам будет зависеть от готовности каждой организации взять на себя ответственность за безопасность критически важных активов.
Только комплексный подход, сочетающий технические, организационные и регуляторные меры, позволит обеспечить устойчивость промышленных сетей России в условиях нарастающих киберугроз.