

Продукты, решения и сервисы Positive Technologies

За 20 лет работы компания выработала визионерский подход к созданию своих решений. Метапродукты Positive Technologies меняют индустрию и радикально повышают защищенность компаний, а через них - отраслей и государств. Таким образом результативная кибербезопасность становится доступна любой организации в мире.

При разработке решений Positive Technologies опирается на многолетнюю практику и уникальные знания сотрудников исследовательского центра - одного из крупнейших в мире. В нем работают [белые хакеры \(white hats\), исследующие защищенность различных систем](#), и [эксперты по кибербезопасности](#), которые расследуют реальные инциденты и знают, как хакеры атакуют. Продукты компании соответствуют российским и международным стандартам безопасности, в том числе PCI DSS и ЦБ РС БР ИББС-2.6-2014, приказам ФСТЭК №17 и 21.

В портфеле Positive Technologies - более десятка высокотехнологичных продуктов. Они позволяют:

- останавливать хакера в автоматическом режиме силами одного человека;
- контролировать защищенность инфраструктуры и своевременно находить в ней уязвимости;
- выявлять инциденты ИБ в инфраструктуре любых масштабов, включая закрытые промышленные системы;
- детектировать атаки во внутреннем и внешнем трафике компаний;
- защищать веб-приложения от сложных атак;
- обнаруживать уязвимости и ошибки в приложениях, а также поддерживать процесс безопасной разработки;
- обнаруживать и отражать целевые и массовые атаки с применением современного вредоносного ПО;
- реагировать на киберугрозы как на конечных точках, так и в инфраструктуре в целом, объединяя для верификации атаки события и контекст из множества систем ИБ.

На базе продуктовой линейки Positive Technologies сформировано несколько решений, которые аккумулируют опыт по защите бизнеса в различных сферах и специфику российских и международных стандартов безопасности. В частности, компания предлагает решения:

- для построения распределенных систем кибербезопасности;
- построения SOC, в том числе в небольших инфраструктурах;
- раннего выявления сложных угроз;
- защиты веб-приложений;
- обеспечения безопасности объектов КИИ (включая взаимодействие с главным центром ГосСОПКА);
- построения центра ГосСОПКА.

Также компания предоставляет сервисное обслуживание и консультационные услуги в области кибербезопасности: непрерывный анализ защищенности бизнеса, обнаружение сложных инцидентов, реагирование на них и расследование, мониторинг защищенности корпоративных систем.

Продуктовый портфель

[MaxPatrol 02](#) – метапродукт, который позволяет обнаруживать и останавливать атаки злоумышленников в автоматическом режиме с измеримым эффектом силами одного человека. Решает проблему серьезного дефицита квалифицированных кадров в индустрии и помогает защитить организации по всему миру.

[MaxPatrol VM](#) – система, позволяющая выстроить процесс управления уязвимостями и контролировать защищенность IT-инфраструктуры компании в любой момент. Продукт собирает, обновляет и хранит полную информацию об активах. На основе этих данных система определяет новые уязвимости на узлах и предоставляет пользователю информацию о них, включая знания о трендовых и наиболее опасных уязвимостях (то есть тех, которые необходимо закрыть в первую очередь).

[MaxPatrol SIEM](#) – система мониторинга событий информационной безопасности. Постоянно пополняется знаниями экспертов о способах детектирования актуальных угроз и адаптируется к изменениям в защищаемой сети. В 2020 году количество продаж MaxPatrol SIEM выросло на 85%. За счет этого компания [вошла в тройку](#)

мировых вендоров с наибольшим годовым приростом продаж SIEM-решений. Согласно [исследованию IDC Global](#), Positive Technologies - единственный российский вендор в топ-20 мирового рынка SIEM-систем (2021).

[PT Network Attack Discovery](#) – система глубокого анализа сетевого трафика (Network Traffic Analysis, NTA) для выявления атак на периметре и внутри сети. Обеспечивает видимость происходящего в сети, обнаруживает активность злоумышленников, в том числе в зашифрованном трафике, и помогает в расследованиях.

[PT Sandbox](#) – песочница, позволяющая защитить инфраструктуру компании от целевых и массовых атак с применением вредоносного ПО и уязвимостей нулевого дня. Проверяет в изолированной виртуальной среде поступающие в компанию файлы и ссылки, выдает вердикт об их вредоносности или легитимности, блокирует угрозы.

[PT ISIM](#) – система анализа трафика сетей АСУ ТП. Позволяет находить следы нарушений информационной безопасности в технологических сетях, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства.

[PT Application Firewall](#) – межсетевой экран уровня веб-приложений.

Предназначен для защиты веб-ресурсов организаций от кибератак (атак L7 DDoS и атак нулевого дня), а также от угроз из списков OWASP Top 10 и WASC. Визионер магического квадранта Gartner.

[PT Application Inspector](#) – инструмент для выявления уязвимостей в приложениях.

Принцип работы продукта основан на сочетании статического (SAST), динамического (DAST), интерактивного (IAST) методов и анализа сторонних компонентов (SCA). Позволяет специалистам по ИБ выявлять и подтверждать уязвимости в исходном коде, а разработчикам - ускорить исправление кода на ранних стадиях разработки.

[PT MultiScanner](#) – система защиты от вирусных угроз. Выявляет вредоносные программы, блокирует их распространение в инфраструктуре и обнаруживает скрытое присутствие зловредов.

[MaxPatrol 8](#) – система, используемая для оценки защищенности IT-инфраструктуры. Позволяет определить эффективность процессов ИБ, а также обеспечивает выполнение требований стандартов.

[XSpider](#) – сканер уязвимостей, позволяющий оценить уровень защищенности сети компании. Проверяет рабочие станции, серверы, сетевые устройства и веб-приложения. Исследует узлы без применения заранее установленных агентов.

[«PT Ведомственный центр»](#) – система управления инцидентами. Автоматизирует процесс реагирования на инциденты и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и другие отраслевые CERT.

[PT Platform 187](#) – (комплексное решение, объединяющее ряд продуктов PT) - программно-аппаратный комплекс для реализации основных функций безопасности значимых объектов КИИ и взаимодействия с главным центром ГосСОПКА. Включает в себя набор технических средств, который помогает выполнить основные требования законодательства, автоматизирует процессы ИБ в организации и значительно повышает их эффективность.

Портфель решений

[PT XDR](#) – решение для выявления сложных киберугроз и реагирования на них. Собирает и анализирует разрозненные данные из множества систем, позволяет обнаруживать действия хакера в любой инфраструктуре и автоматически реагировать на атаки. Основано на экосистеме продуктов Positive Technologies и использует уникальные экспертные знания об угрозах для выявления атак.

[«Построение центра ГосСОПКА»](#) – комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ, созданное на основе продуктов компании. С его помощью служба ИБ сможет самостоятельно реализовать функции центра ГосСОПКА, а также получать услуги [экспертного центра безопасности Positive Technologies](#) (PT ESC).

[PT Anti-APT](#) – комплексное решение для выявления и предотвращения целевых атак. Позволяет максимально быстро обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования.

[Безопасность объектов КИИ](#) – система безопасности, помогающая реализовать меры защиты значимых объектов КИИ в соответствии с требованиями закона № 187-ФЗ. Объединяет в себе продукты, которые позволяют выполнять основные законодательные требования по защите значимых объектов КИИ, предотвращать и выявлять атаки и автоматизировать взаимодействие с ГосСОПКА.

[PT Industrial Cybersecurity Suite](#) – первая по-настоящему комплексная платформа для защиты промышленности от киберугроз. Она позволяет обнаруживать злоумышленника на всех этапах развития атаки в промышленных средах и своевременно реагировать на них. PT ICS обеспечивает комплексную безопасность в индустриальном сегменте компании, начиная от сетевых узлов и заканчивая технологическими устройствами.

Сервисный портфель

[PT Expert Security Center \(PT ESC\)](#) – экспертный центр безопасности Positive Technologies. Предоставляет услуги по обнаружению сложных инцидентов, реагированию на них и расследованию, а также по мониторингу защищенности корпоративных систем. Сервисы безопасности на базе продуктов, которые предлагает PT ESC, доказали свою эффективность во время экспертного сопровождения зимней Олимпиады-2014 в Сочи и чемпионата мира по футболу - 2018, в ходе которого специалисты помогли отразить 38 тыс. кибератак

на сервисы транспортной дирекции.

[Непрерывный анализ защищенности бизнеса](#) – услуги Positive Technologies по анализу защищенности бизнеса от киберугроз. Помогают непрерывно оценивать уязвимость компании для действий злоумышленников, своевременно предотвращать атаки и устранять их последствия. Спектр услуг включает три направления: Pentest 360, эмуляцию APT и red team vs. blue team.

[Исследование угроз и уязвимостей аппаратных решений](#) – услуги экспертной команды Positive Technologies, которые помогут устранить риски ИБ, связанные с уязвимостями аппаратных платформ.