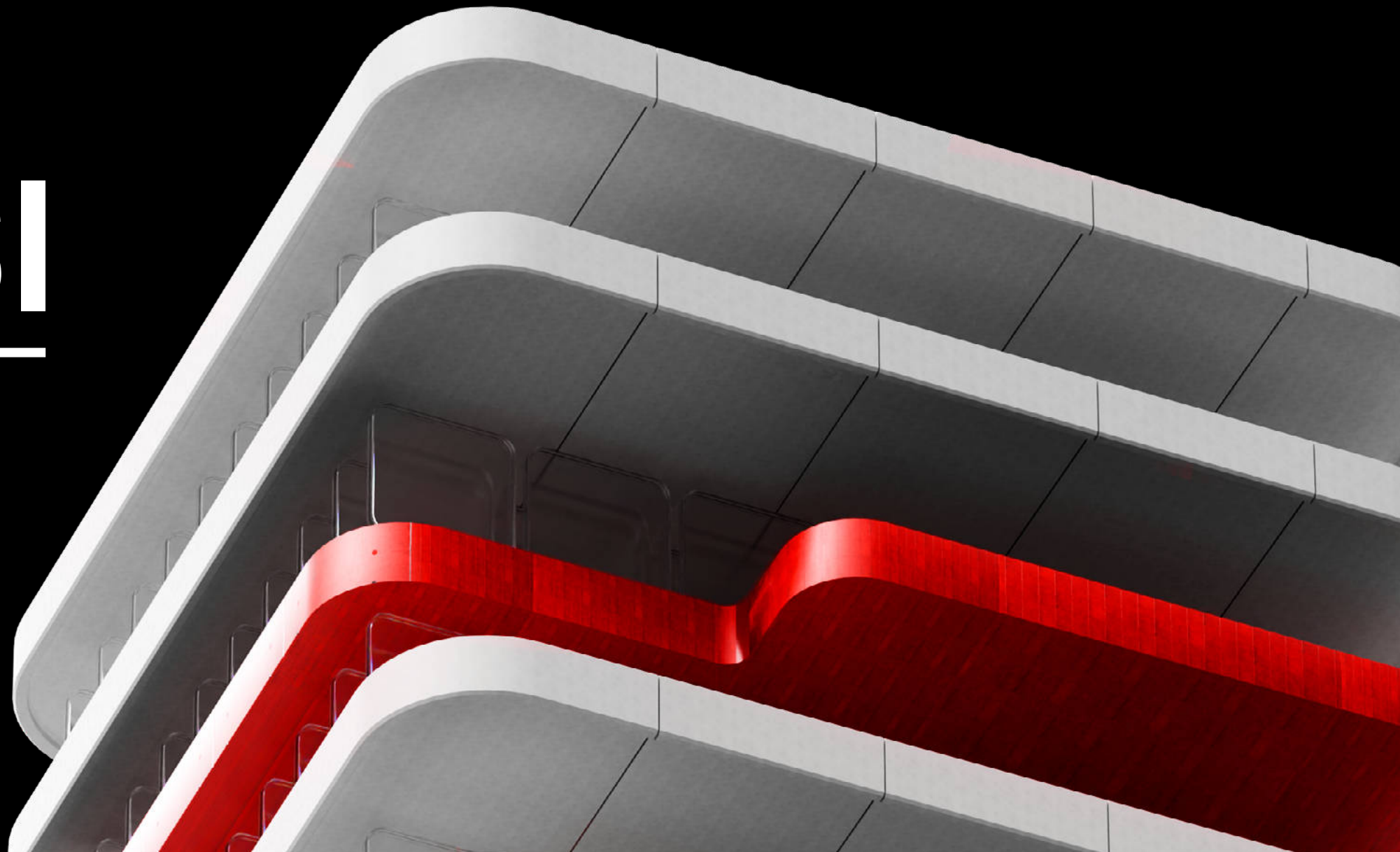
pt

25

Годовой отчет

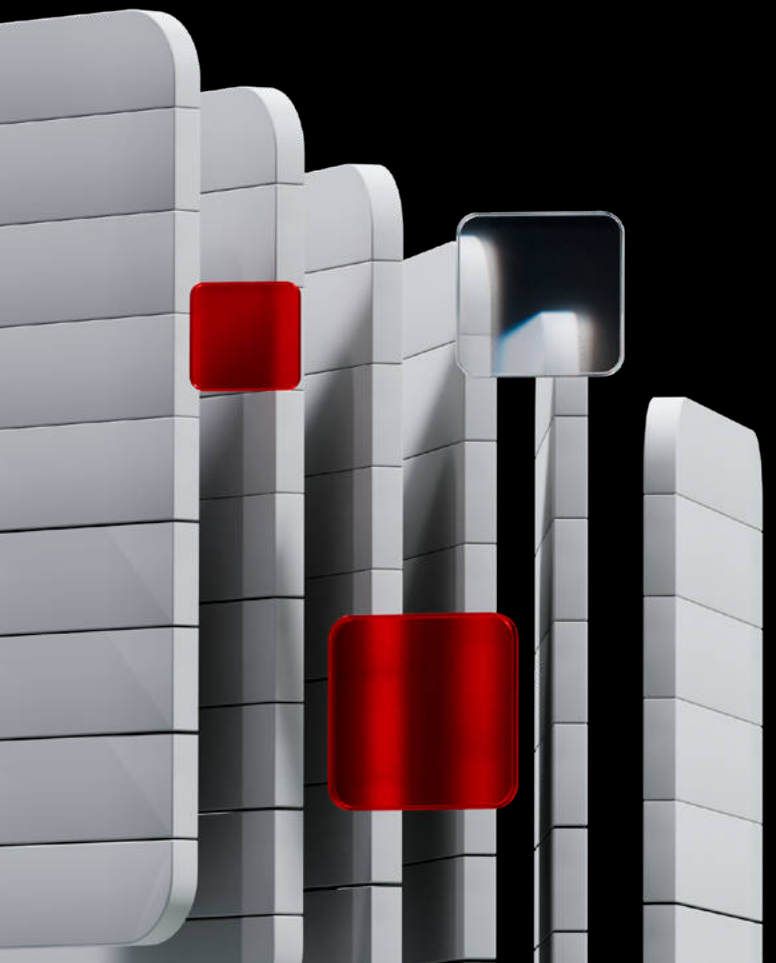
POSI

АРХИТЕКТУРА РЕЗУЛЬТАТА



СОДЕРЖАНИЕ

1 О компании
2 Стратегический обзор
3 Продукты, решения, сервисы
4 Финансовые результаты
5 Взаимодействие с инвесторами
6 Устойчивое развитие
7 Корпоративное управление
8 Приложения



2025 год подтвердил работоспособность архитектуры нашего бизнеса. Продукты, процессы и управленческие решения объединены в единую систему, которая дает измеримый результат.

Мы обновили архитектуру процессов и повысили предсказуемость и управляемость результата.

Гайденс по отгрузкам выполнен. Объем отгрузок в 2025 году составил 33,6 млрд руб. (+40% год к году). Это не результат удачи или внешних факторов, а следствие инженерного подхода к планированию и дисциплины исполнения. Возвращение показателя NIC в положительную зону подтверждает устойчивость системы и позволяет рассмотреть возможность возврата к выплате дивидендов.

Благодаря широкой линейке продуктов, решений и сервисов мы можем предложить клиентам целостную «архитектуру результата», которая гарантирует невозможность наступления недопустимых для бизнеса событий.
Наш подход в области результативной кибербезопасности поддерживает фокус на измеримом результате для заказчиков. Наша компания сохраняет способность выпускать по несколько прорывных продуктов и решений каждый год, успешно адаптируясь к изменениям рынка и технологического ландшафта.

PT X

PT NGFW

Endpoint Security

MaxPatrol EPP
MaxPatrol EDR

Архитектуру результата формируют профессионалы, которые умеют выстраивать систему и доводить ее до измеримых показателей.

Инженерный подход к решениям. Измеримый результат в ключевых метриках. Эта архитектура стала надежным фундаментом для устойчивого роста бизнеса в 2026 году.

Выполнение целей на 2025 год

Компания вернулась к целевым темпам роста, гайденс по отгрузкам выполнен

+40% рост год к году

33,6 млрд руб.

отгрузки

10–15%

рост российского рынка кибербезопасности в 2025 году[1]

Возвращение NIC в положительную зону

2,7 млрд руб.

на 5,4 **млрд** руб больше, чем в 2024 году

Возвращение к возможности выплачивать дивиденды

- Положительный NIC дает возможность рассмотреть вопрос о выплате дивидендов

Сохранение численности штата на уровне середины 2024 года

2605

сотрудников работают в Компании по состоянию на конец 2025 года

Снижение операционных расходов

- **–25%** расходы, не связанные с оплатой труда,

  в том числе:
- **–20%** отраслевые мероприятия и развитие бизнеса
- **–41%** business support
- **–65%** расходы на маркетинг

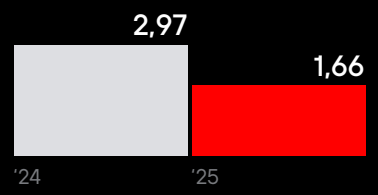
Компания сохранила инвестиции в R&D на уровне прошлого года

9,1 млрд руб.

составили инвестиции в R&D в 2025 году

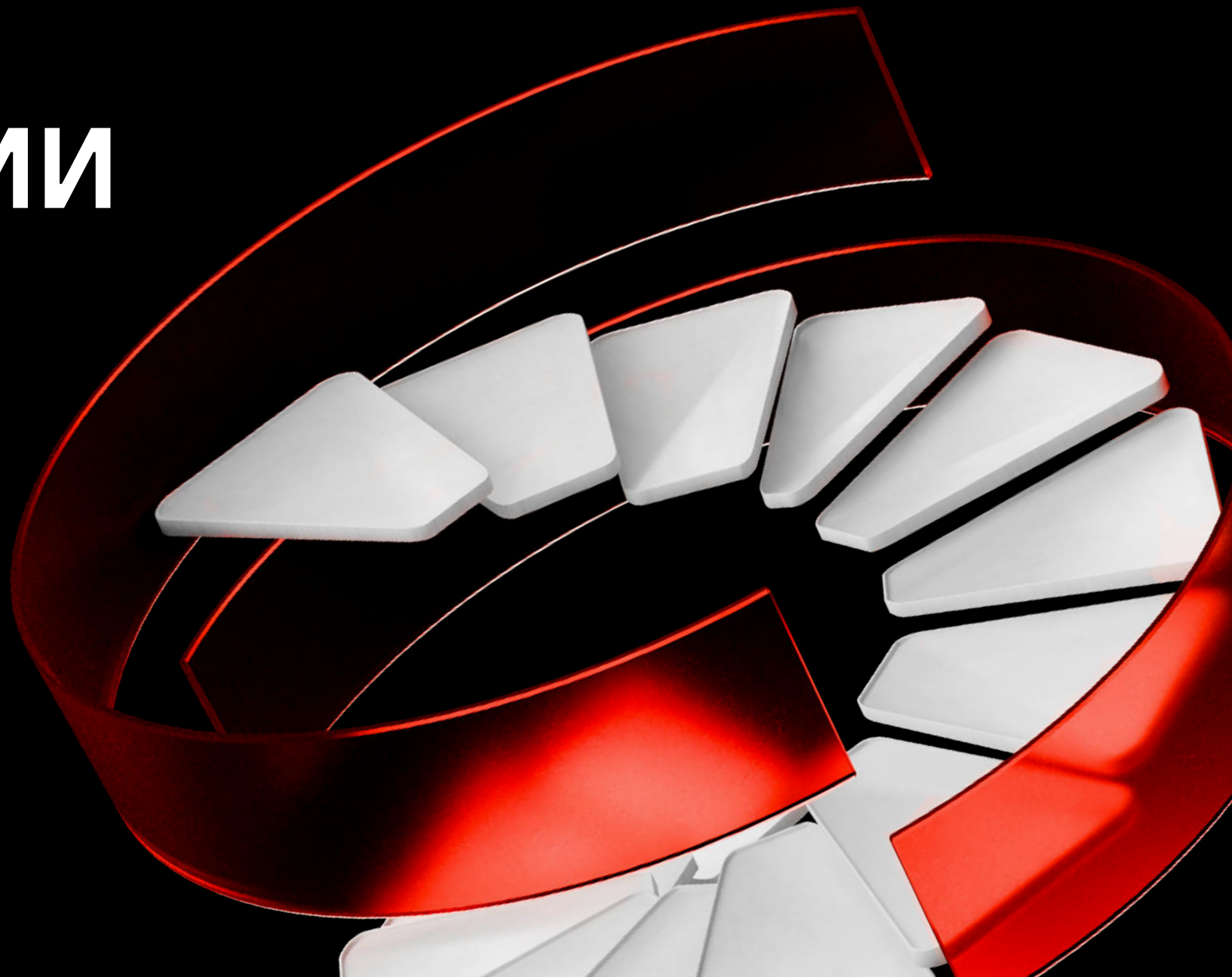
Снижение уровня долговой нагрузки

Net Debt / EBITDA



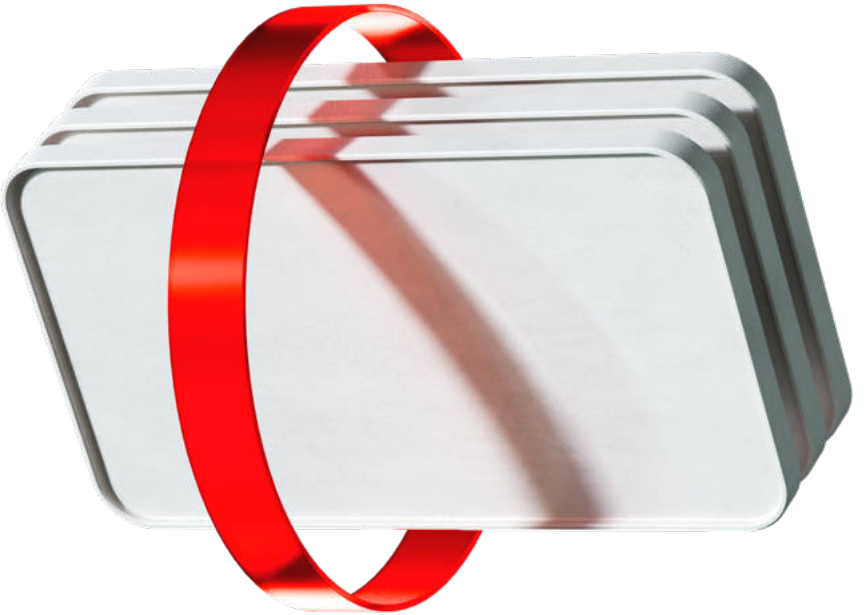
1 По экспертным оценкам
2 Чистая прибыль без учета капитализируемых расходов

О КОМПАНИИ



- Защищаем от недопустимого
- Нацелены на результат
- 2025 год: цифры и достижения
- События года
- Привлекательность для инвесторов
- Наша география
- Наша бизнес-модель
- Наши клиенты

ЗАЩИЩАЕМ ОТ НЕДОПУСТИМОГО



Positive Technologies — ведущий разработчик продуктов, решений и сервисов для результативной кибербезопасности и первая публичная компания отрасли на Московской бирже.

Уже более 20 лет мы создаем технологии, которые помогают бизнесу и государству эффективно противостоять цифровым угрозам. Наши продукты и сервисы позволяют выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики, делая недопустимые события невозможными.

Positive Technologies является одним из лидеров российского рынка кибербезопасности[1]. Наш технологический портфель охватывает большинство категорий средств защиты информации и продолжает расширяться. Мы стремимся стать первым российским технологическим гигантом в области кибербезопасности, который сможет уверенно конкурировать с мировыми лидерами.

Positive Technologies — первая российская компания, разместившая акции на Московской бирже в формате прямого листинга. Этот шаг позволил нам создать дополнительный инструмент мотивации для сотрудников и профессионалов рынка. Мы придерживаемся принципов прозрачности и открытости перед акционерами, демонстрируя стабильное развитие и устойчивость бизнеса. В основе стратегии нашего бизнеса лежит приверженность долгосрочному росту и созданию ценности для инвесторов.

1 Согласно исследованиям ЦСР и Б1.

Краткая история Компании[1]

сотрудников	продуктов		
6	1	2002	Основание Компании. Открытие первого офиса и разработка первого продукта — XSpider
45	2	2008	Выход второго продукта Компании — MaxPatrol 8
199	2	2011	Проведение первого международного форума по кибербезопасности Positive Hack Days
382	4	2013	Защищаем Всемирную летнюю универсиаду в Казани
400	4	2014	Защищаем Олимпиаду в Сочи
450	5	2015	Выход MaxPatrol SIEM — флагманского продукта Компании, на долю которого в последние годы приходится наибольший процент отгрузок
800+	9	2018	Защищаем выборы Президента России Защищаем чемпионат мира по футболу
900	9	2019	Защищаем Всемирную зимнюю универсиаду в Красноярске
1000+	9	2020	Защищаем голосование по поправкам к Конституции

1 С полной историей Компании можно ознакомиться здесь.

Краткая история Компании

	сотрудников	продуктов и решений	
2021	1200+	14	■ Positive Technologies вышла на биржу путем прямого листинга и стала первой в России публичной компанией из отрасли кибербезопасности ■ Денис Баранов стал Генеральным директором Positive Technologies, сменив основателя Компании Юрия Максимова. Юрий Максимов возглавил Совет директоров ■ Защищаем выборы в Государственную думу
2022	1500+	17	■ Число акционеров Компании превысило 100 тыс. ■ Акции Positive Technologies были переведены в котировальный список первого уровня, а также включены в базу расчета четырех индексов Мосбиржи: широкого рынка, малой и средней капитализации, информационных технологий, инноваций ■ Positive Technologies провела вторичное размещение акций на Мосбирже
2023	2200+	20	■ Количество акционеров Positive Technologies удвоилось — теперь их более 205 тыс. ■ Впервые с момента выхода на биржу капитализация Компании превысила 100 млрд руб. ■ Акции Positive Technologies были включены в основной индекс Мосбиржи ■ Форум Positive Hack Days вышел за пределы закрытых площадок и превратился в большой городской киберфестиваль
2024	3100+	25+	■ Защищаем международный мультиспортивный фиджитал-турнир «Игры будущего» ■ Вывод на рынок PT NGFW — межсетевого экрана нового поколения ■ Первая M&A-сделка Компании: приобретение доли в белорусской компании «ВИРУСБЛОКАДА»
2025	2600+	25+	■ Возвращение к темпам роста, вдвое превышающим динамику рынка кибербезопасности в России ■ Фокус на повышение эффективности бизнеса ■ Создание антивирусной лаборатории ■ Стартовали коммерческие продажи собственного антивируса на базе MaxPatrol EPP, представили концепцию Endpoint Security ■ Запустили PT X как облачное решение для сегмента малого и среднего бизнеса

НАЦЕЛЕНЫ НА РЕЗУЛЬТАТ

Результат кибербезопасности — киберустойчивость

Киберустойчивость — способность организации (отрасли, государства) стабильно функционировать в условиях проведения кибератак, направленных на реализацию недопустимых событий.

1. Определяем недопустимые для организации события
2. Усложняем путь хакера и ускоряем реагирование
3. Измеряем кибер-устойчивость на кибериспытаниях с участием реальных хакеров

Допустимое событие

Приостановка оборудования, которая вызвала задержку выполнения одного из контрактов

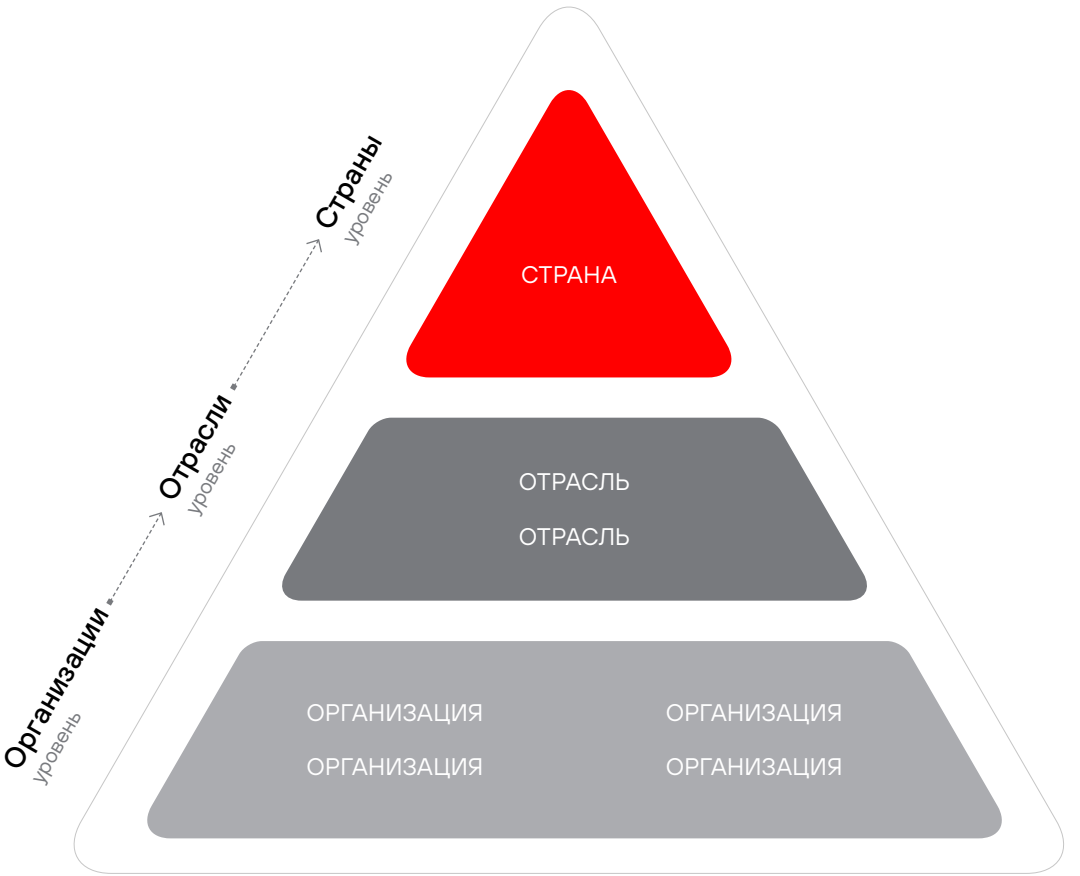
Недопустимое событие

Техногенные аварии с экологическим ущербом и угрозой жизни из-за взлома технологического процесса

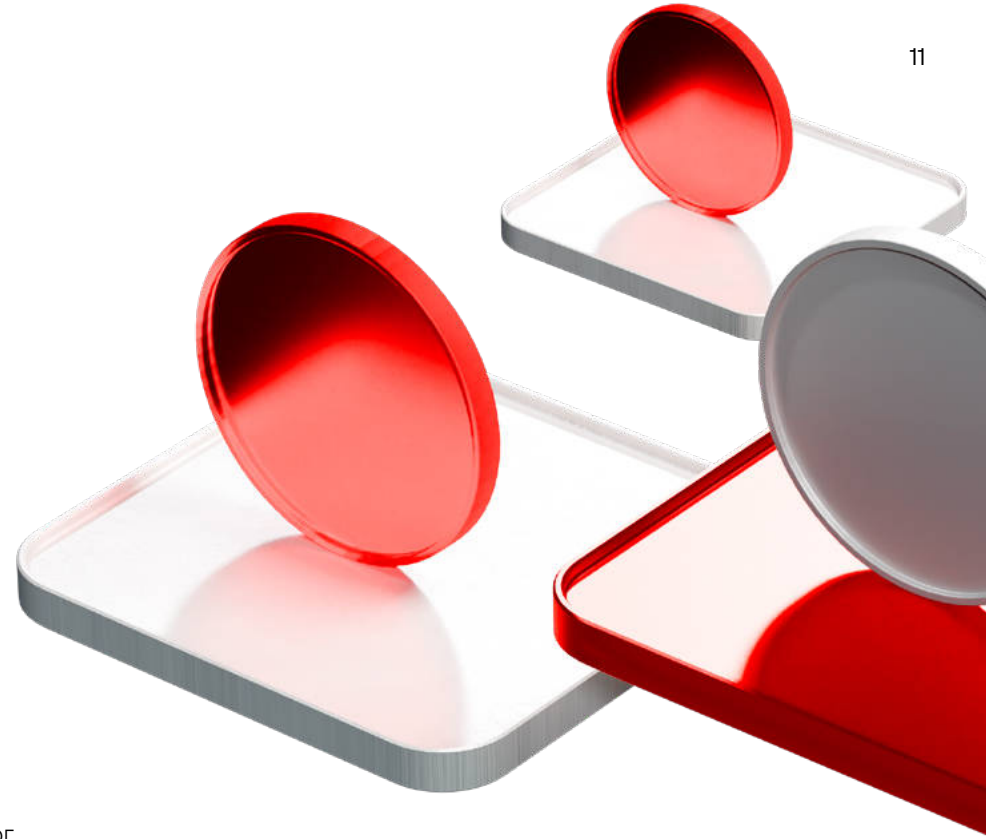
Двигаясь на уровне компаний, индустрий и стран

Мы создаем безопасное цифровое будущее

Критическая национальная инфраструктура	Построение локальной индустрии кибербезопасности, государственный SOC, взращивание комьюнити, глобальные мероприятия
Отрасли	Финансы, телекоммуникации, промышленность
Организации	3000+ клиентов из всех отраслей экономики — в enterprise- и SME-сегментах



Наши продукты, сервисы и услуги дают подтверждаемый результат



время

Атаки ›

Защищаем ИТ-инфраструктуру, чтобы хакерам было было сложно и дорого взломать ее

время

Реагирования =

Видим и останавливаем хакеров, которые проникли в инфраструктуру, до наступления недопустимого события

итог

Киберустойчивость

Проверяем надежность своих продуктов на кибериспытаниях

bugbounty.standoff365.com/programs/pt_product

Результативная кибербезопасность в 2025 году

В 2025 году измеримая кибербезопасность с гарантированным результатом стала актуальна для компаний любого масштаба и уровня зрелости процессов информационной безопасности (ИБ). Руководители хотят не просто тратить средства на защиту, а быть уверенными в ее эффективности. Этот фокус отражается и в повестке регуляторов. Резонансные инциденты 2025 года показали: большой бюджет и серьезные усилия еще не гарантируют киберустойчивость. Рынку нужны новые подходы к оценке результатов, способные обеспечить уверенность, причем ежедневную, в результативности средств и мер безопасности.

Positive Technologies помогает выстраивать результативную кибербезопасность компаниям и госучреждениям, которые при постановке целей, планировании затрат на ИБ и выборе средств защиты фокусируются на предотвращении событий, способных нанести их деятельности необратимый ущерб. Убедиться в защищенности от неприемлемых событий — объективно, на практике и с понятным результатом, — как и получить уверенность в киберустойчивости в целом, можно, лишь выйдя на киберисытания.

В 2025 году Компания запустила инициативы по приведению заказчиков к измеримой киберустойчивости в кратчайшие сроки. Ими стали облачное решение PT X, в рамках которого Positive Technologies гарантирует защиту с покрытием финансовых рисков: помогает выйти на киберисытания и при выполнении компаниями «киберминимума» выплачивает вознаграждение исследователям в случае взлома. PT X помогает компаниям усилить защиту или команду одним решением, без необходимости покупать отдельные продукты. Для усиления или в период развития собственных центров мониторинга информационной безопасности (SOC) Positive Technologies также представила набор сервисов PT Boost. Он помогает компаниям прийти к измеримому результату максимально быстро и с полной экспертной поддержкой Positive Technologies.

Компании уже оценили результаты этих решений и сервисов. Так, например, Rambler&Co вместе с нами сделала кибербезопасность измеримой за три месяца, а Министерство цифрового развития и связи (Минцифры) Оренбургской области внедрило новые подходы к киберустойчивости и оценило их на киберисытаниях.

В 2025 году стартовал уникальный в индустрии проект, в рамках которого лидеры рынка в течение трех лет будут совместно выстраивать киберустойчивость «Почты России». Positive Technologies стала партнером по внедрению результативной ИБ в корпоративном сегменте. Наша задача — сделать так, чтобы злоумышленники не могли реализовать три из пяти стратегических рисков компании.

Отличительная черта проекта — результат каждого из трех этапов подтверждается на киберучениях, в ходе которых независимые команды белых хакеров оценят реальную способность выстроенной комплексной системы кибербезопасности отражать сложные атаки. Мы рассчитываем, что полученный в ходе проекта опыт сможем масштабировать на другие системно значимые компании. Результативная ИБ содействует кооперации отечественных игроков кибербезопасности. Сотрудничая друг с другом, мы вместе начинаем мыслить в терминах измеримой защиты, конкретных и честных итогов выполненной работы и будем в силах не только качественно повысить защищенность отдельных компаний и отраслей, но и усилить национальную киберустойчивость.

Rambler&Co сделали кибербезопасность измеримой за три месяца

Процессы уже были хорошо выстроены, налажено взаимодействие ИБ.

Что мы сделали

Тонко настроили СЗИ и инфраструктуру для фокусной защиты от недопустимого, а также помогли выйти на кибериспытания, чтобы непрерывно оценивать результат работы ИБ.

Какой результат

Компания вышла на новый уровень кибербезопасности с понятными инструментами измерения.

Подробнее о кейсе

Недопустимое событие

вывод денежных средств из «1С»

На кибериспытаниях

с октября 2024 года

Используемые продукты

- MaxPatrol SIEM
- PT NAD
- PT NGFW
- MaxPatrol EDR
- PT Application Firewall

40

рекомендаций
по ИТ-харденингу

Почта России строит результативную кибербезопасность

Независимая оценка результата

По результатам red teaming часть денег достается либо вендору и интегратору, либо команде хакеров.

2024–2027

сроки проекта

Уникальная коллаборация

19 российских вендоров

работают над защитой Почты России

Три этапа построения киберустойчивости, по результатам каждого из которых проводится независимый red teaming.

За защиту от недопустимых событий **в корпоративном сегменте** отвечает Positive Technologies.

УНИКАЛЬНЫЙ МАСШТАБ ИНФРАСТРУКТУРЫ

в корпоративный сегмент Почты России входят

3 центра

обработки данных — ЦОД (два в Москве и один в Адлере)

83

Управления федеральной почтовой службой (УФПС)

38 тыс.

почтовых отделений по всей стране (ОПС)

Центральный аппарат

Казначейство

Security Information & Event Management

MaxPatrol SIEM

Web Application Firewall

PT Application Firewall

Next-Generation Firewall

PT NGFW

Static Application Security Testing

PT Application Inspector

Dynamic Application Security Testing

PT BlackBox

Vulnerability Management

MaxPatrol 8 + MaxPatrol VM + XSpider

Network Sandboxing

PT Sandbox

Network Traffic Analysis / NDR

PT Network Attack Discovery

Industrial Security

PT Industrial Security Incident Manager, PT Industrial Cybersecurity Suite

Endpoint Detection & Response

MaxPatrol EDR

Продуктовая линейка Positive Technologies насчитывает более 25 продуктов и решений.

Мы являемся лидерами рынка корпоративной кибербезопасности в ключевых технологических нишах. Мы работаем над расширением клиентской базы и продуктовой линейки, фокусируясь на результативности работы наших решений и комплексной защищенности клиентов. В сравнении с прошлым годом клиентская база увеличилась за счет как привлечения новых заказчиков, так и увеличения продаж действующим клиентам. При этом нам удалось сохранить практически всех прежних пользователей, которые не только продлевают лицензии, но и увеличивают инсталляционную базу.

Рынок кибербезопасности растет

Российский рынок кибербезопасности продолжает демонстрировать двузначные темпы роста, существенно опережая динамику ИТ-сектора в целом. Согласно прогнозам аналитиков, российский рынок кибербезопасности ожидает существенный рост в ближайшие годы.

968[1] **млрд руб.**

прогнозный объем рынка к 2030 году

21%[1]

среднегодовой темп роста (CAGR) до 2030 года

19%[1]

прогнозный рост российского рынка кибербезопасности в 2025 году

Positive Technologies по итогам 2025 года вернулась к целевым темпам роста бизнеса, вдвое превышающим динамику рынка кибербезопасности в России.

Цифровизация затрагивает все сферы жизни, делая кибербезопасность неотъемлемым элементом устойчивого развития общества. Усложнение ландшафта киберугроз и рост их влияния на бизнес-процессы диктуют необходимость проактивного подхода к защите. Это формирует долгосрочный тренд на внедрение высокотехнологичных решений кибербезопасности, которые становятся гарантией непрерывности бизнеса и доверия со стороны клиентов.

В 2025 году российский рынок кибербезопасности окончательно перешел от фазы экстренного импортозамещения к этапу глубокой структурной пересборки. Для инвесторов и участников рынка этот период стал проверкой на способность не просто расти вместе с рынком, а создавать устойчивые технологические платформы, отвечающие новым требованиям регуляторов и усложняющемуся ландшафту угроз.

374[1] **млрд руб.**

объем рынка кибербезопасности в России в 2025 году

Подробнее о динамике рынка кибербезопасности читайте в разделе «Обзор рынка»

1 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2025–2030 годы».

Сохраняем инвестиции в R&D

В Positive Technologies мы выстроили подход к разработке, который сочетает классические принципы и современные организационные модели.

Сегодня мы стараемся быть максимально гибкими. Гибкими как с точки зрения организационной структуры, так и с точки зрения того, как мы смотрим на технологии, которым доверяем и в которые верим. Прогресс развивается настолько стремительно, что технологии, которые еще вчера служили нашей опорой, сегодня могут стать ограничением. Поэтому мы стараемся построить модель разработки, где опыт и наследие Компании не препятствуют созданию инноваций.

Мы стремимся сохранить баланс между накопленным опытом и свежим взглядом молодых специалистов. Новое поколение разработчиков, свободное от влияния устоявшихся практик, привносит в Компанию инновационные идеи и смелость в принятии решений. Мы создаем среду, где их подходы могут органично сочетаться с опытом наших экспертов, формируя идеальную почву для развития.

Наш исследовательский центр — один из крупнейших в Европе. В нем работают белые хакеры (white hats), исследующие защищенность различных систем, и эксперты по кибербезопасности, которые изучают инциденты и понимают, как реальные преступники наносят компаниям непоправимый ущерб. На их знаниях и опыте строятся наши продукты.

В течение года Компания продолжила усиливать команду сильными специалистами и экспертами в области кибербезопасности, сохранив количество сотрудников на уровне середины 2024 года.

9,1 млрд руб.

составил объем инвестиций в R&D в 2025 году

Объем инвестиций в R&D в 2025 году составил 9,1 млрд руб., что позволяет в полной мере реализовать стоящие перед Компанией бизнес-задачи и поддерживать высокие темпы разработки новых продуктов и решений. Компания сохраняет возможность выходить на мировые рынки и запускать продукты, способные конкурировать с ведущими мировыми аналогами.

Мы понимаем важность инвестиций в R&D и убеждены, что это позволит нам обеспечить **непрерывность роста масштаба бизнеса** Positive Technologies в последующие годы.

Подробнее в разделе «Инвестируем в экспертность»

Наши новые продукты и развитие метапродуктов

Эволюция управления киберугрозами

NEW

XSpider PRO

Сканер уязвимостей нового поколения

Запустили в декабре 2025 года

MaxPatrol VM

Система управления уязвимостями

MaxPatrol Carbon

Интеллектуальная система управления источниками угроз и анализа киберустойчивости

Метапродукт

Технологии для сильного SOC

MaxPatrol O2

Автоматизирует все сложные и рутинные процессы: от обнаружения и расследования кибератак до оперативного реагирования на них

Метапродукт

MaxPatrol SIEM

Система, превращающая поток событий в список приоритизированных инцидентов с нужным для расследования контекстом

NEW

MaxPatrol 360

Единый центр управления расследованиями и операционной работой SOC

Запуск в апреле 2026 года

Новинки 2025 года

NEW

Endpoint Security

Концепция полной защиты конечных устройств. Представлена в виде двух продуктов — MaxPatrol EPP и MaxPatrol EDR.

Стартовали коммерческие продажи собственного антивирусного решения MaxPatrol EPP в декабре 2025 года

Представили в октябре 2025 года

NEW

PT X

Облачное решение для мониторинга и реагирования с гарантией результата

Запустили в октябре 2025 года

NEW

PT Dephaze

Автопентест для оценки уровня защищенности внутренней инфраструктуры

Запустили в феврале 2025 года

NEW

PT Data Security

Платформа нового поколения для обеспечения безопасности данных

Запустили в октябре 2025 года

NEW

PT Email Security

Система многоуровневой защиты корпоративной почты

Анонсировали в октябре 2025 года, коммерческий запуск в апреле 2026 года

Подробнее читайте в разделе «Продукты, решения, сервисы»

Фокусные продукты в своих сегментах

PT NGFW

Высокопроизводительный и надежный межсетевой экран нового поколения

PT ISIM

Единая система обеспечения киберустойчивости промышленных инфраструктур, на базе которой можно выстраивать защиту всего промышленного контура

PT Application Firewall

Высокопроизводительный межсетевой экран для непрерывной защиты веб-приложений и их API

PT Application Inspector

Инструмент для выявления уязвимостей и тестирования безопасности приложений, безопасная разработка

2025 ГОД: ЦИФРЫ И ДОСТИЖЕНИЯ

Финансовые показатели 2025 года соответствуют ранее представленным прогнозам менеджмента.

33,6 млрд руб.

составили отгрузки за 2025 год

2,7 млрд руб.

управленческая чистая прибыль (NIC)

Отгрузки за 2025 год

Объем отгрузок за 2025 год составил 33,6 млрд руб. По итогам года Positive Technologies вновь демонстрирует темпы роста бизнеса, вдвое превышающие динамику роста рынка кибербезопасности в России. Для сравнения: объем отгрузок Компании по итогам 2024 года составил 24,1 млрд руб.

NIC

Наряду с существенным ростом объема отгрузок Компания сфокусировалась на операционной эффективности и строгом контроле за расходами, сохранив их в рамках изначального бюджета. Это позволяет говорить о выполнении одной из ключевых финансовых целей года — возвращении управленческой чистой прибыли (NIC) в положительную зону.

В 2026 году Positive Technologies продолжит фокусироваться на поддержании высокой финансовой эффективности и планирует сохранить общий объем расходов на уровне 2025 года. Вместе с ростом объема отгрузок это станет важным шагом в достижении целевого уровня маржинальности по NIC в среднесрочной перспективе.

Продукты-лидеры

Объем бизнеса

- MaxPatrol SIEM
- MaxPatrol VM
- PT Network Attack Discovery
- PT NGFW
- PT Application Firewall

Темпы роста

>x2,5

- MaxPatrol EDR

>x2

- PT NGFW
- MaxPatrol O2
- PT Network Attack Discovery
- MaxPatrol SIEM
- MaxPatrol VM
- PT ISIM

Скорость продажи

MaxPatrol EPP
Менее месяца
от идеи до бюджета

PT NGFW
Три дня от заказа до отгрузки

PT X
Восемь дней от потребности
до продажи

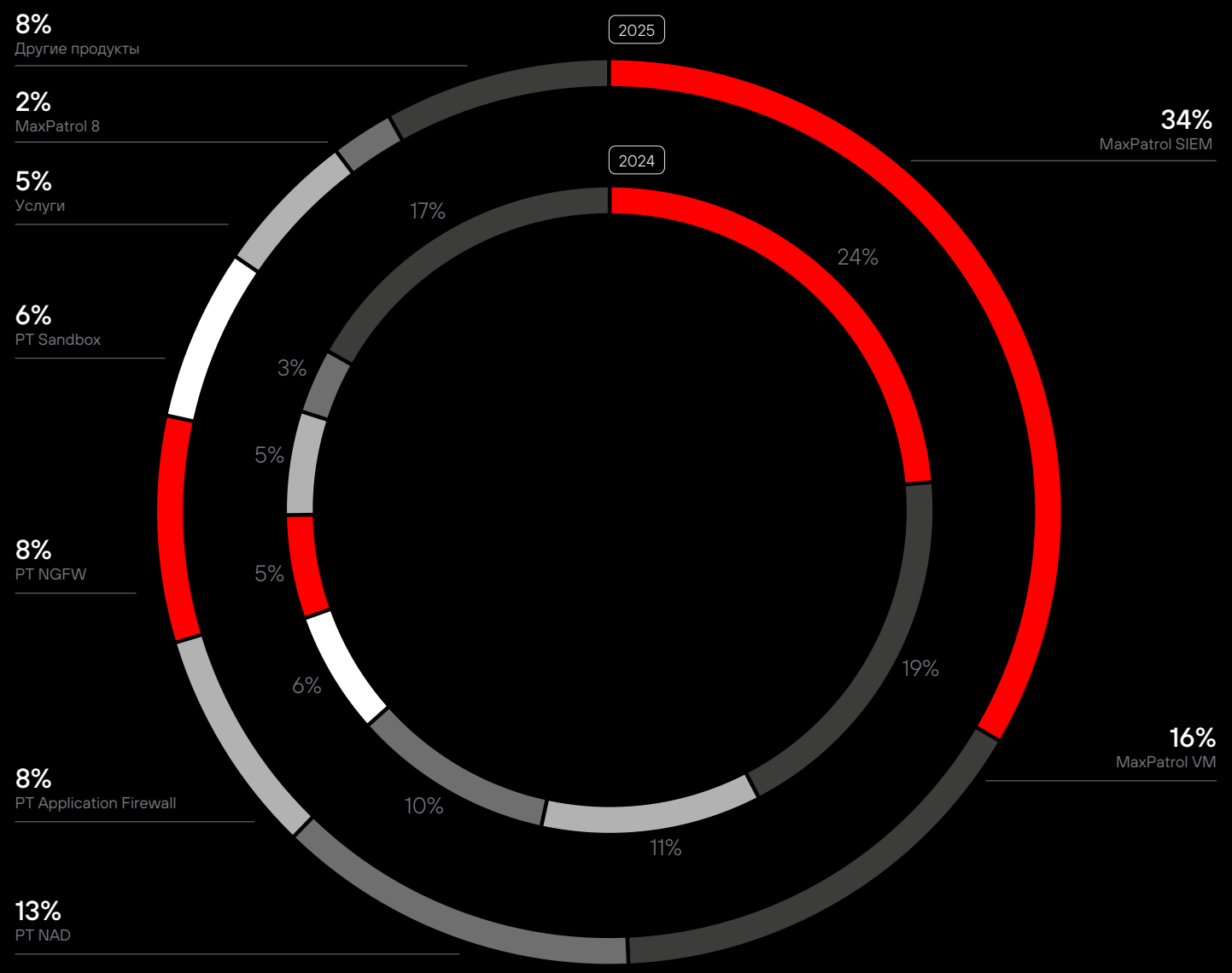
PT Network Attack Discovery
Один день от начала пилота
до первого реагирования

Обучение
Один день от первого
обсуждения до оплаты

Привлечение новых клиентов

- PT Dephaze
- PT X
- PT NGFW
- MaxPatrol EPP

Отгрузки с НДС в разбивке по продуктам



Positive Education — центр практического обучения, созданный на базе экспертизы Positive Technologies

Центр формирует устойчивые навыки противодействия киберугрозам у специалистов, управленцев и руководителей, помогая организациям выстраивать системную защиту и повышать уровень киберустойчивости.

Развитие кибербезопасности невозможно без сильных специалистов

Positive Education — центр обучения, где соединяются практика, технологии и опыт Positive Technologies, чтобы готовить лидеров кибербезопасности: тех, кто укрепляет киберсуверенитет через распространение знаний, повышение осведомленности о киберугрозах и создание устойчивой экосистемы защиты компаний и государства.

Результаты 2025 года

14,5 тыс.

специалистов усилили компетенции благодаря практикумам и образовательным программам центра

›100

генеральных директоров, а также

›400

управленцев и представителей органов власти, ресурсоснабжающих организаций и бизнес-объединений прошли обучение, направленное на интеграцию кибербезопасности в стратегию развития компаний

90

молодых специалистов более чем из

25

стран Азии, Африки, Ближнего Востока и Латинской Америки объединил Positive Hack Camp

500

специалистов ИТ и ИБ обучены в Индонезии, ОАЭ, Египте, что усилило международное присутствие и локальную экспертизу

8 тыс.

специалистов подтвердили свои компетенции по работе с продуктами Positive Technologies

500

учебных заведений Армении, Беларуси, Казахстана, Киргизии, России и Узбекистана отправили своих преподавателей на обучение, что позволило масштабировать подготовку специалистов через образовательные системы этих стран

Подробнее о Positive Education читайте в разделе «Устойчивое развитие»

СОБЫТИЯ ГОДА

1. Провели Positive Hack Days Fest в «Лужниках»
2. Участие Компании в ПМЭФ
3. Провели три кибербитвы Standoff
4. Создание антивирусной лаборатории
5. Провели три митапа Positive Hack Talks (Египет, Индонезия, Бразилия)
6. Positive Hack Camp
7. Выход коммерческой версии PT Data Security
8. Positive Security Day
9. Представлена концепция Endpoint Security
10. Стартовали коммерческие продажи собственного антивируса на базе MaxPatrol EPP
11. Запустили PT X
12. Запустили PT Dephaze

ПРИВЛЕКАТЕЛЬНОСТЬ ДЛЯ ИНВЕСТОРОВ

Мы реализуем планы по вхождению в высшую лигу эмитентов на российском фондовом рынке.

Входим в основные индексы Мосбиржи: **IMOEX** и **РТС**

Входим в индексы Мосбиржи (широкого рынка, IT, малой и средней капитализации, инноваций)

Акции торгуются **в первом котировальном списке**

Высокий рейтинг кредитоспособности — **ruAA («Эксперт РА»), AA-(RU) (АКРА)**

Регулярно раскрываем финансовую и управленческую отчетность

Лидер в IR-рейтинге от SMART-LAB, включающем более 200 эмитентов

Наша следующая цель — стать **новой голубой фишкой**

Подробнее читайте в разделе «Взаимодействие с инвесторами»

НАША ГЕОГРАФИЯ

Россия остается приоритетным рынком Positive Technologies. Компания одновременно развивает международное присутствие и нацелена на укрепление позиций на глобальном рынке кибербезопасности. Офисы Positive Technologies работают в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске и Томске.

В 2025 году Positive Technologies усилила работу в фокусных регионах, расширяла присутствие и адаптировала стратегии для выхода на новые рынки.

СНГ

Россия,
Беларусь,
Казахстан,
Узбекистан

Ближний Восток и Северная Африка (MENA)

Алжир,
Бахрейн,
Египет,
Иордания,
Саудовская Аравия,
Ирак,
Иран,
Катар,
Палестина,
ОАЭ,
Оман,
Тунис

Латинская Америка[1] (LATAM)

Бразилия,
Мексика,
Перу,
Уругвай,
Куба

Африка

ЮАР,
Эфиопия,
Танзания,
Уганда,
Сенегал,
Экваториальная Гвинея

Азиатско-Тихоокеанский регион (APAC)

Вьетнам,
Индия,
Индонезия,
Малайзия,
Пакистан,
Республика Корея,
Таиланд

1 Включая Карибы.

Экспансия на международные рынки

Топ-3 торгового предложения

- PT NAD
- PT Application Inspector
- Профессиональные сервисы в области оценки кибербезопасности

Международные мероприятия

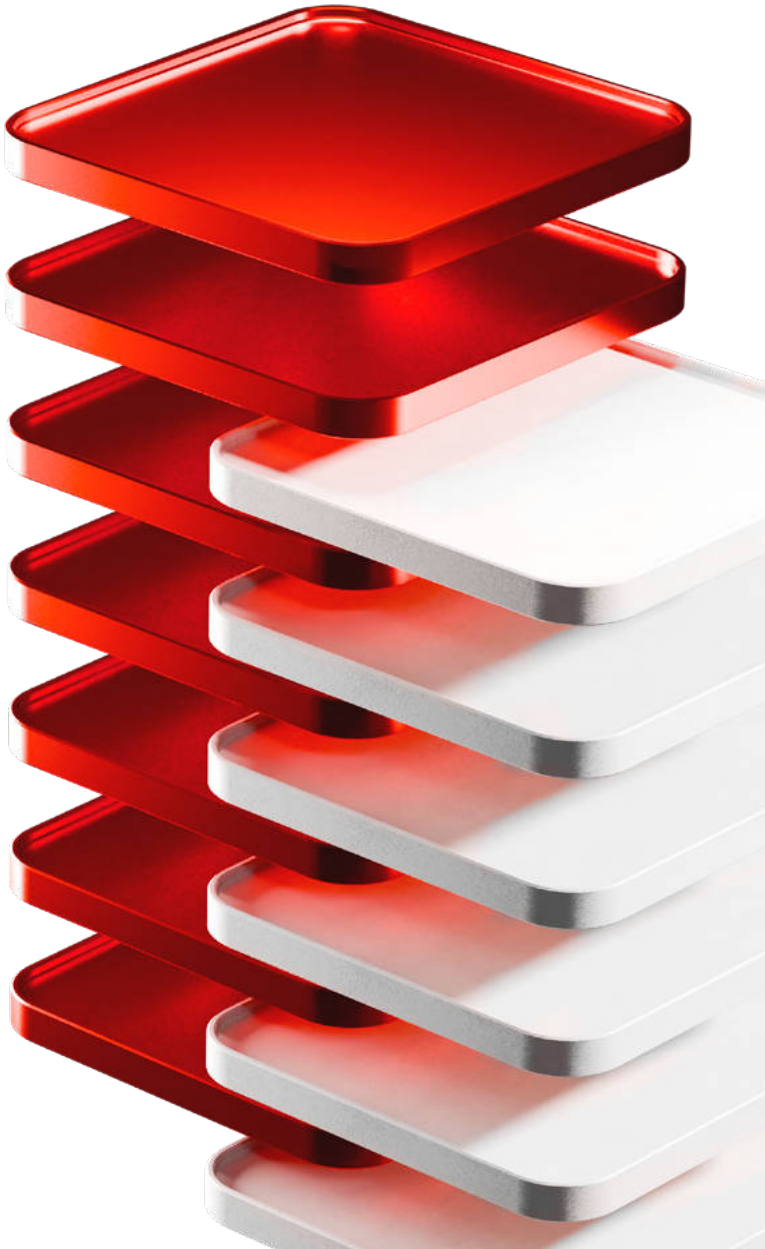
- Positive Hack Days в Москве — **более 300** делегатов из **42** стран
- GISEC (ОАЭ), GITEX (ОАЭ), FDC (Египет), ELECOMP (Иран), NCC (Индонезия)
- Партнерский день Positive Technologies, Сан-Паулу (Бразилия)
- Киберучения CyberDrill (Египет, Оман, Марокко, Куба)
- Standoff Hacks (Индия)
- Активное взаимодействие с OIC-CERT

Формируем кадровую основу кибербезопасности

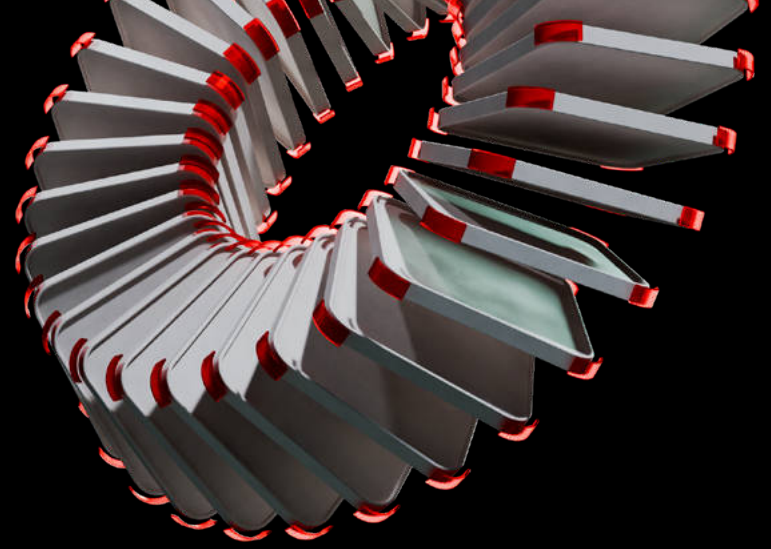
Совместно с ведущими вузами Индонезии готовим новое поколение специалистов для цифрового суверенитета:

- UGM,
- ITB,
- Muhammadiyah University и другие

Подробнее читайте в разделе «Развитие бизнеса за рубежом»



НАША БИЗНЕС-МОДЕЛЬ



Бизнес-модель Positive Technologies сочетает технологическое лидерство, глубокую экспертизу и инновационный подход к кибербезопасности. Мы закладываем в основу наших продуктов собственные технологии. Именно они обеспечивают результативность и выстраивают непреодолимый барьер для злоумышленников.

Мы не просто развиваем Компанию, а создаем ценности для клиентов, общества, сотрудников и акционеров. Наши продукты и сервисы помогают в достижении результативной кибербезопасности, а стратегический подход обеспечивает устойчивое развитие и укрепляет позиции на рынке, определяя будущее отрасли.

Наши ресурсы

Визионер рынка кибербезопасности

- 24 года опыта в исследованиях и разработке
- Организуем ключевые события в профессиональной среде ИБ:
  - Positive Hack Days — форум по практической кибербезопасности
  - The Standoff — крупнейшая в мире открытая кибербитва
  - Positive Education — центр обучения Positive Technologies, где практики обучают результативной кибербезопасности

Наш портфель

›25 продуктов и решений

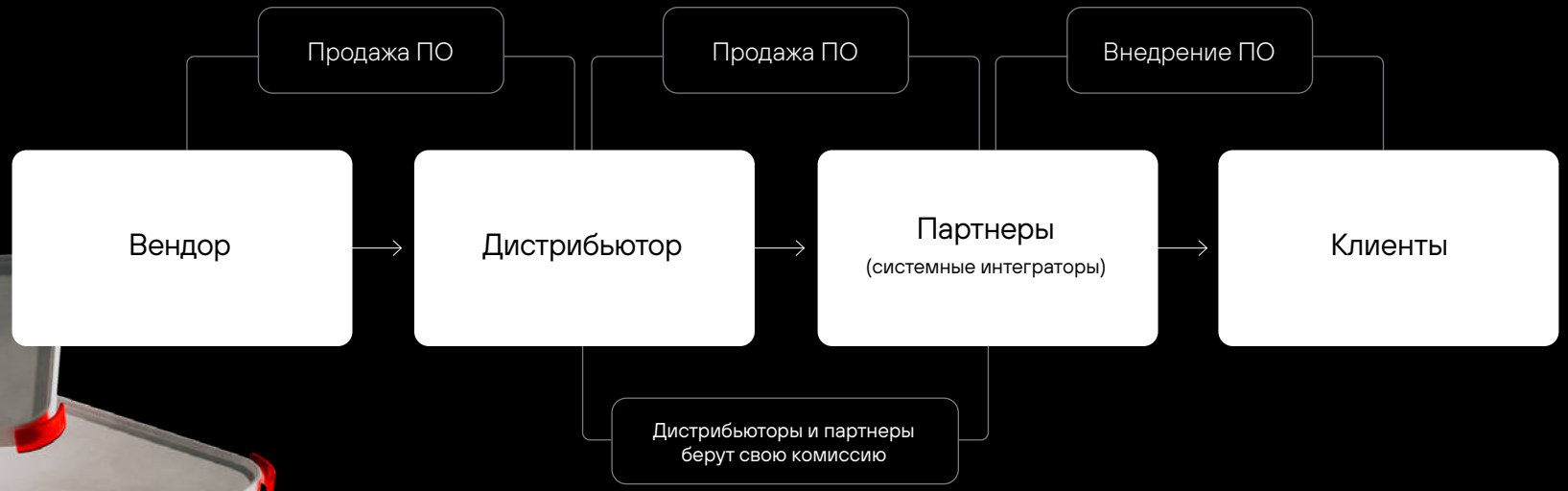
›600 партнеров — ведущих интеграторов

Сильная команда

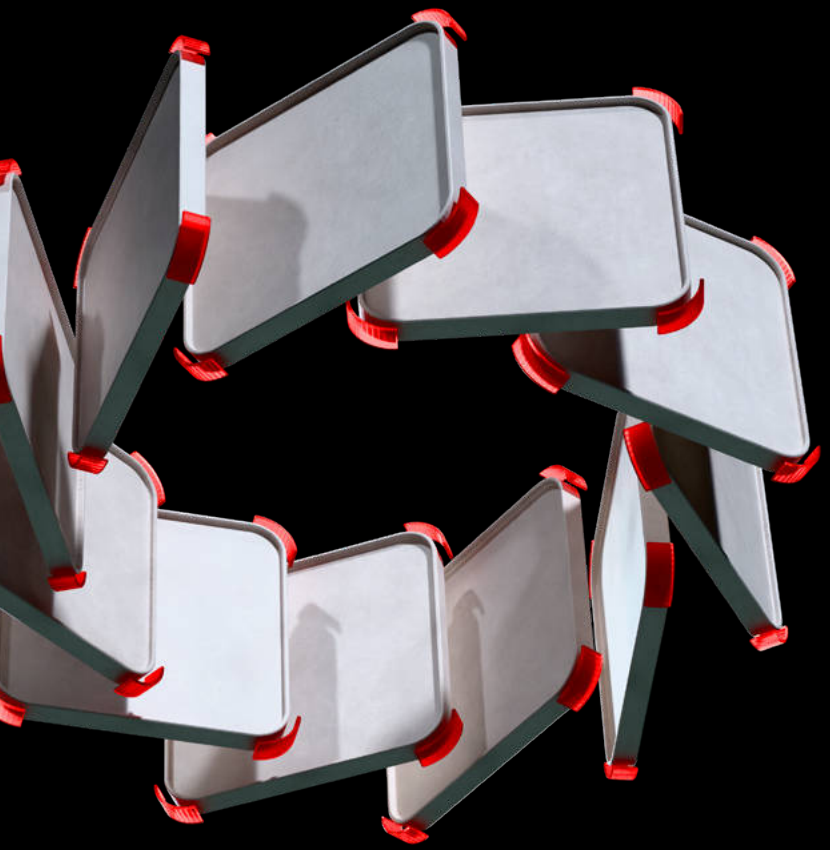
›2,5 тыс. сотрудников

Ведущие эксперты отрасли и ключевые спикеры в сфере ИБ

Как устроен процесс продажи



Создаем ценности для всех заинтересованных сторон



Для клиентов

- Обеспечиваем стабильную работу бизнеса и государственных структур
- Выстраиваем результативную кибербезопасность: делаем недопустимые события невозможными
- Создаем автопилот кибербезопасности: программный комплекс сам отражает хакерские атаки, а обеспечивать работоспособность системы может один специалист
- Помогаем клиентам оперативно заместить программное обеспечение ушедших с рынка зарубежных вендоров

Для общества

- Обеспечиваем цифровую безопасность страны и цифровой суверенитет
- Защищаем государственные структуры и частные компании, в том числе объекты критической информационной инфраструктуры (КИИ), не позволяя злоумышленникам нарушить производственные процессы, вызвать перебои в поставках продовольствия, спровоцировать экологическую катастрофу и привести к другим недопустимым событиям
- Обеспечиваем защиту мероприятий федерального значения
- Формируем профессиональную среду специалистов по кибербезопасности

Для сотрудников

- Обеспечиваем интересные задачи, возможность расти и развиваться в среде профессионалов
- Наши сотрудники — совладельцы Компании

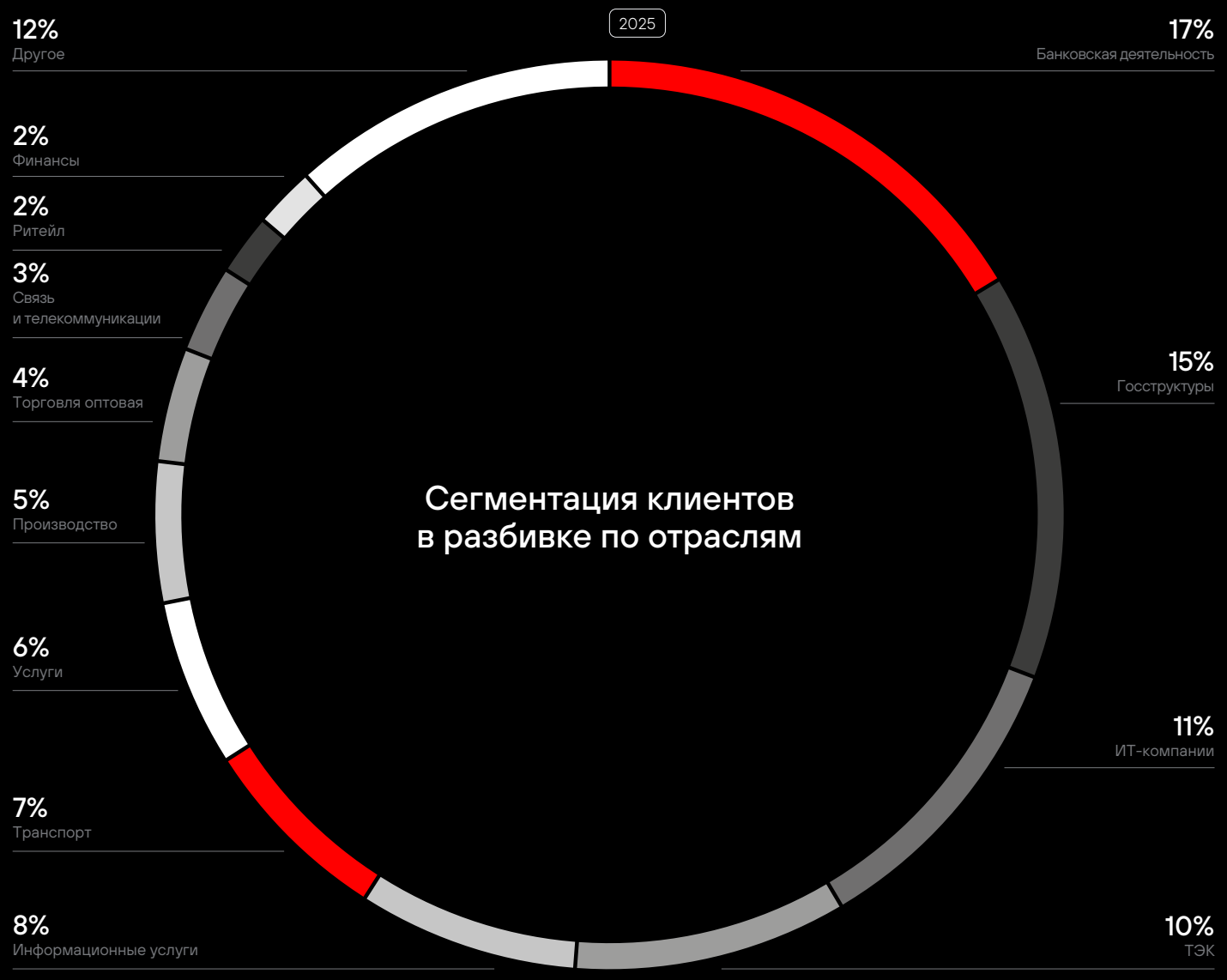
Для акционеров

- Восходящая голубая фишка
- Обеспечиваем рост капитализации Компании
- Делаем наш бизнес и отчетность прозрачными и доступными, формируя новые стандарты работы с инвесторами

НАШИ КЛИЕНТЫ

Мы помогаем крупным компаниям из всех ведущих отраслей российской экономики. Среди наших клиентов банки (17%), государственные структуры (15%), ИТ-компании (11%) и предприятия топливно-энергетического комплекса (10%).

Широкая диверсификация клиентской базы способствует стабильному развитию бизнеса и укреплению позиций Компании.



Диверсификация клиентской базы

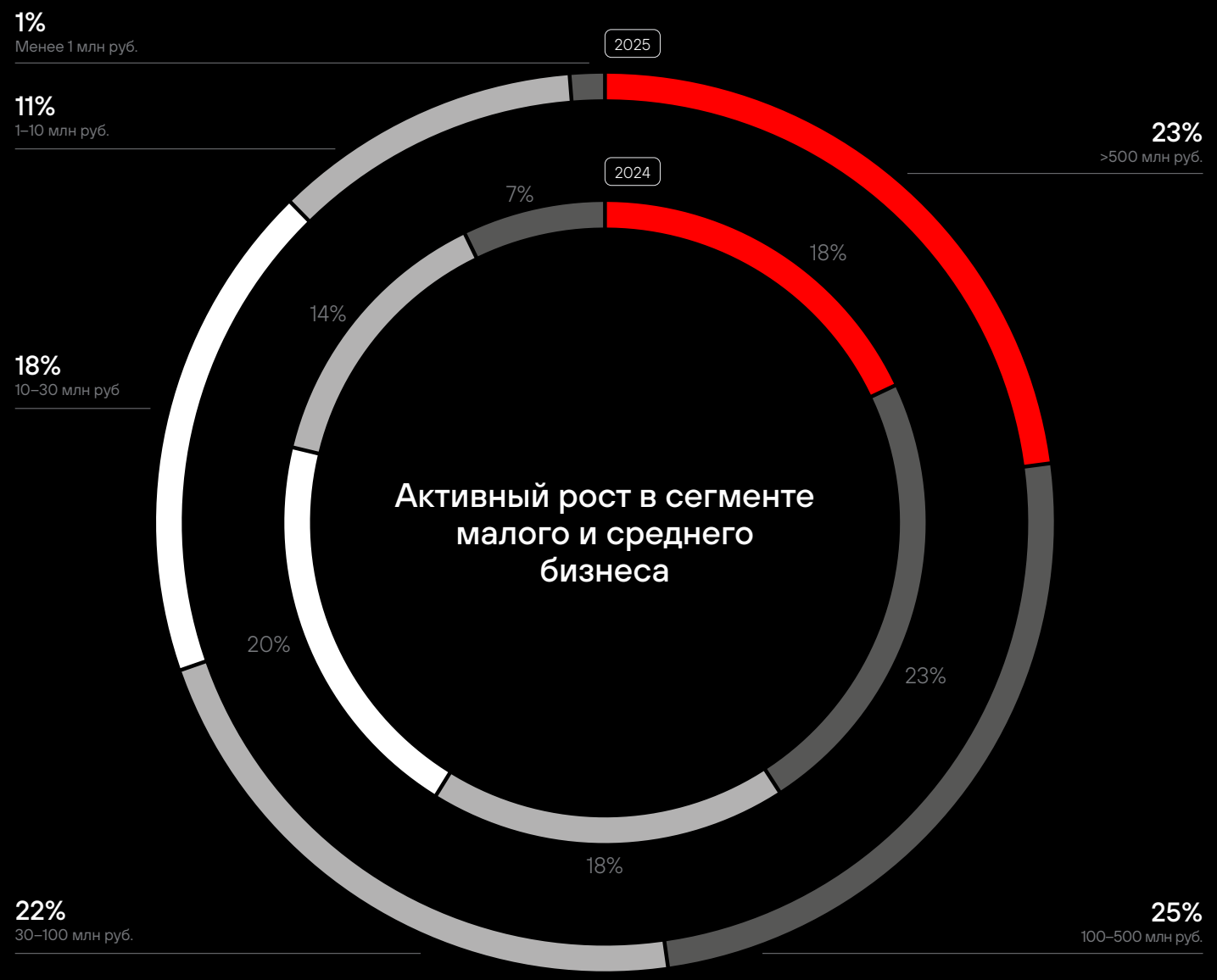
›1,9 тыс.

новых клиентов — цель на 2026 год

70%

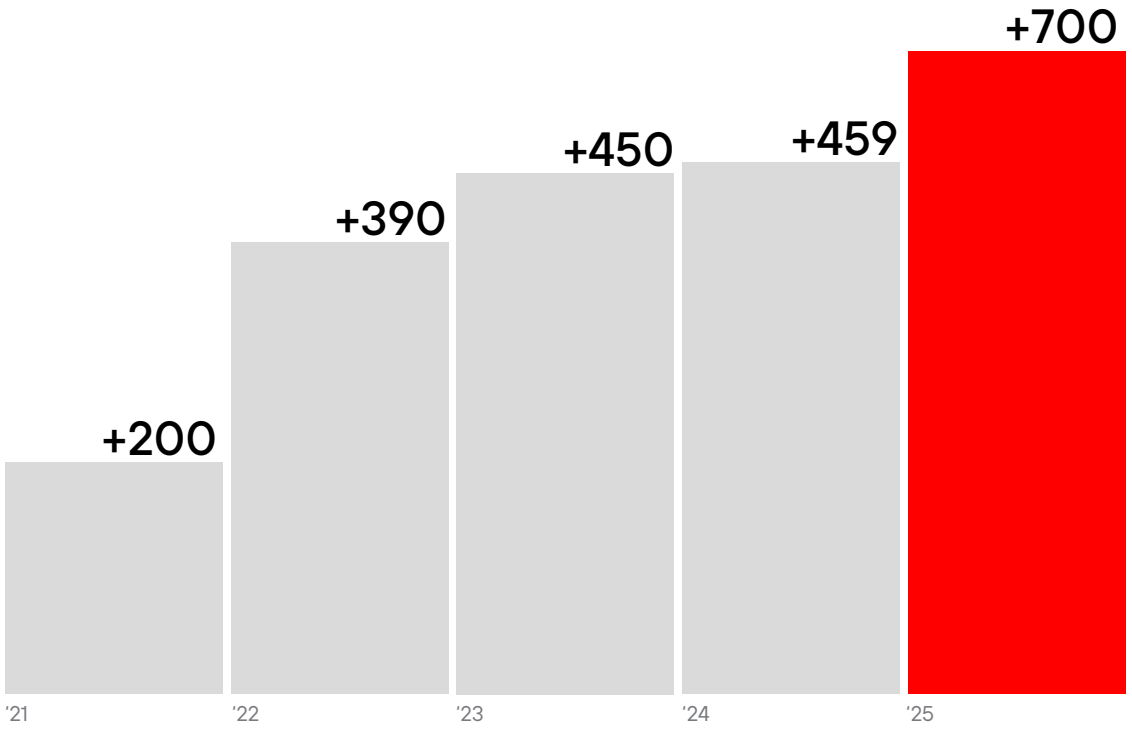
доля отгрузок целевому сегменту крупных корпоративных клиентов в 2025 году

Каждый год мы активно увеличиваем количество наших заказчиков. Это новый мощный вектор развития бизнеса. По итогам 2025 года к нам присоединилось 700 новых клиентов, а в 2026 году мы ставим перед собой цель привлечь более 1,9 тыс. компаний. Для нашего бизнеса критически важно привлекать новых клиентов и предлагать действующим заказчикам новые продукты. Это особенно значимо, поскольку продление лицензий на продукты обычно составляет около 40% от стоимости первоначальной лицензии.



Мы реализуем крупные проекты по построению результативной кибербезопасности.

Прирост новых клиентов год к году, компаний



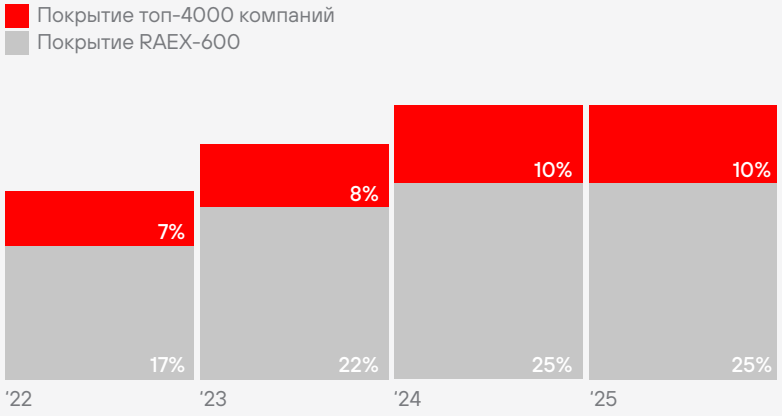
ПОТЕНЦИАЛ РОСТА КЛИЕНТСКОЙ БАЗЫ

У нас высокий потенциал роста как по увеличению числа клиентов, так и по росту числа продуктов на одного клиента. На данный момент на одного клиента в среднем приходится два-три продукта Positive Technologies, тогда как наша продуктовая линейка насчитывает более 25 продуктов и решений.

10%

из списка 4 тыс. крупнейших компаний России являются клиентами Positive Technologies

Потенциал роста клиентской базы



СТРАТЕГИЧЕСКИЙ ОБЗОР

- Обращение Генерального директора
- Обзор рынка
- Наша стратегия
- Развитие бизнеса за рубежом

ОБРАЩЕНИЕ ГЕНЕРАЛЬНОГО ДИРЕКТОРА

Уважаемые совладельцы, клиенты, партнеры!

2025 год стал для Positive Technologies годом глубокой трансформации — в первую очередь, внутренней. Подступаясь к реализации этой задачи, мы определили две основные цели: вернуть бизнесу способность расти и развиваться быстрее рынка, а также разобраться с внутренними причинами, которые и привели к неприемлемой для нас ситуации. С финансовой точки зрения это означало выйти на плановые темпы роста бизнеса и вернуть возможность выплачивать дивиденды акционерам, как мы публично заявили годом ранее.

На данный момент компания успешно отработала по всем направлениям и полностью завершила эту трансформацию. Существенные изменения произошли в коммерческом блоке компании. Мы вывели практику работы с прогнозом продаж на новый уровень: пересобрали процессы, упразднили роли с непрозрачными целями и задачами и очистили прогноз от бизнес-гипотез, что позволило на порядок точнее видеть поступление денег в течение всего финансового года. Сегодня отдел продаж работает как единый слаженный механизм, где понятен вклад каждого сотрудника в усиление конкретного доходного трека, а наши продавцы на всех уровнях ощущают личную и командную ответственность за достижение финансового результата.

В рамках внутренней трансформации мы проанализировали все направления деятельности компании с точки зрения необходимости, рациональности и вклада в стратегию. Важно было понять, насколько актуальны наши продуктовые начинания на текущий момент. Для этого мы отделили успешные направления от неуспешных, стратегически важные — от оттягивающих ресурсы, выявили причины успеха или неэффективности по каждому из них, оценили соответствие полученных результатов амбициям компании.

Дополнительно мы посмотрели на людей с точки зрения их управленческого и кадрового потенциала, уровня ресурсного состояния, выгорания и многих других факторов. В результате этого анализа мы предприняли ряд действий: зафиксировали численность сотрудников, снизили операционные затраты и при этом сохранили те стратегические начинания, которые должны помочь компании интенсивно развиваться и достигать успехов при изменении ИТ-ландшафта.

Positive Technologies продолжила движение к максимально полному технологическому портфелю. Разработанный нами межсетевой экран нового поколения PT NGFW — первый продукт за историю компании, который преодолел планку несколько миллиардов рублей отгрузок за первый год и продемонстрировал быструю окупаемость.

Денис Баранов

Генеральный директор
Positive Technologies

В 2025 году компания выпустила полноценное решение MaxPatrol Endpoint Security для защиты конечных устройств, суммарное количество защищаемых им устройств уже превысило 155 тысяч. А значит, мы способны активно штурмовать рынок антивирусных решений, на котором традиционно доминировали другие вендоры. Произошел также внутренний технологический прорыв в области метапродуктов на основе технологий Data Lake и искусственного интеллекта, которыми мы серьезно занимались и в которые инвестировали на протяжении последних лет. Прогрессу в реализации многих наших задумок в направлении метапродуктов способствовал и глобальный технологический прорыв в развитии больших языковых моделей за последние годы.

Сегодня наша компания обладает полным набором технологий, опытом, насмотренностью и отработанной методикой на том уровне, который позволяет нам брать на себя обязательства за обеспечение результата. Мы понимаем, как гарантировать результат и как контролировать его достижение через киберисспытания. Благодаря этой нашей способности, технологическим прорывам в области искусственного интеллекта, развитии метапродуктов, а также технологии Data Lake в 2025 году мы запустили сервис PT X — первое на рынке облачное решение для мониторинга и реагирования с финансовым обязательством гарантировать результат. В том случае если на публичных киберисспытаниях внешние белые хакеры смогут успешно атаковать защищаемую нами компанию, то вознаграждение исследователям платим мы, а не клиент. Такое обязательство — правильная и честная демонстрация ценности нашего продукта. Спрос на PT X оказался высок, особенно в сегменте среднего бизнеса: всего за три месяца с начала запуска появилось 12 клиентов. Это связано с тем, что динамика кибератак меняется, ущерб для бизнеса становится осязаем и очевиден для генеральных директоров и акционеров компаний. Мы отвечаем на их потребности и фактически создаем новый рынок — не рынок продажи средств защиты, а рынок обязательств гарантировать результат. Это стало возможно благодаря отработке нашей методики ИБ 2.0 и появлению технологии, которая позволяет масштабировать уникальный сервис.

Кроме того, в 2025 году мы анонсировали портал, в котором аккумулируются данные об уязвимостях в программном обеспечении и оборудовании производителей со всего мира. Регулярно обновляемая база этого сервиса содержит максимально полные сведения о более чем 300 тыс. уязвимостей и их исследователях, а также рекомендации вендоров.

В мае 2025-го при поддержке Минцифры России и стратегическом партнерстве Правительства Москвы мы провели самый массовый за всю историю киберфестиваль Positive Hack Days. Это мероприятие — стратегически значимая площадка, на которой российскии производители представляют технологии кибербеза, в том числе для международного бизнес-сообщества. Фестиваль посетили более 150 тыс. человек, включая гостей из более чем 40 стран — в основном из Азии, Африки, Ближнего Востока и Латинской Америки. Positive Hack Days — мощнейший инструмент развития международного бизнеса и продвижения на уровне B2G. А летом 2025-го наша ежегодная международная программа по практической кибербезопасности Positive Hack Camp собрала на летнюю школу около сотни талантливых специалистов из 27 стран мира.

Все эти изменения привели к тому, что сейчас компания находится в очень хорошей форме. Во-первых, мы обогнали рынок по темпам роста, как и планировали. Во-вторых, наша команда одна из лучших по составу на всех уровнях — и в индустрии, и в стране в целом. По моему личному мнению, сегодня Positive Technologies напоминает спортсмена, который очень хорошо «просушился», сохранив при этом свои амбиции. Это позволяет нам снова брать на себя задачи по приведению капитализации к справедливой оценке: в этом году мы будем стремиться к тому, чтобы рыночная капитализация и акционерная стоимость соответствовали темпам роста бизнеса и отражали внутренний потенциал компании.

В 2026 году мы планируем продолжить расти опережающими темпами, жестко контролировать расходы и удерживать их на уровне 2025 года, за счет чего выйти на более амбициозные показатели и увеличить дивидендную базу.

Спасибо, что вы с нами!

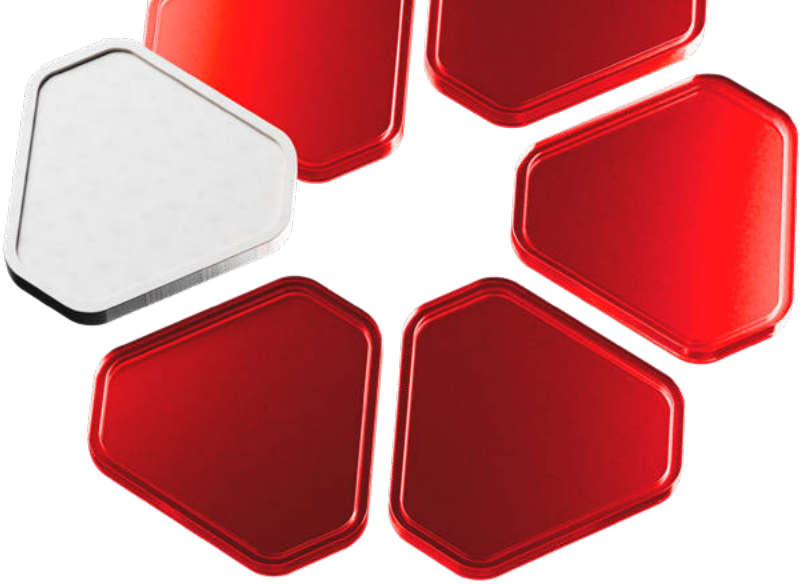
МЫ СНЯЛИ ПЕРВЫЙ В МИРЕ НАУЧНО-ПОПУЛЯРНЫЙ ФИЛЬМ О РЕВЕРС-ИНЖИНИРИНГЕ

Это документальный фильм о том, как люди разбирают сложные технологические системы по частям, чтобы понять их устройство, творчески переосмыслить и создать что-то новое — более совершенное и безопасное. Фильм о реверс-инженерах – тех, кто знает, как получить доступ ко всему.

Через факты и личные истории экспертов индустрии мы рассказываем о развитии реверса за последние 100 лет – от промышленности после Первой мировой и больших ЭВМ до ИИ и «киберпанка, который мы заслужили» в ближайшем будущем.

В проекте приняли участие практики отрасли и исследователи в том числе из Positive Technologies, «Лаборатории Касперского», Т-Банка.

Смотрите фильм «Как получить доступ ко всему: реверс-инжиниринг» бесплатно в онлайн-кинотеатрах PREMIER, «Иви» и «КИОН», на платформах Rutube и «VK Видео».



ОБЗОР РЫНКА

Российский рынок

Методология и контекст

Обзор подготовлен на основе данных ведущих аналитических агентств (Центр стратегических разработок (ЦСР) и Б1). При анализе данных за 2025 год мы опираемся на прогнозные показатели, так как итоговая рыночная статистика публикуется с временным лагом. Мы учитываем различия в методологиях исследований: оценки могут варьироваться в зависимости от базы расчета (выручка поставщиков или затраты конечных клиентов) и периметра учитываемых ИБ-сервисов.

Ключевые показатели и долгосрочный прогноз

В 2025 году российский рынок кибербезопасности (ИБ) окончательно перешел от фазы экстренного импортозамещения к этапу глубокой структурной пересборки. Для инвесторов и участников рынка этот период стал проверкой на способность не просто расти вместе с рынком, а создавать устойчивые технологические платформы, отвечающие новым требованиям регуляторов и усложняющемуся ландшафту угроз.

17–19%[1][2]

рост российского рынка кибербезопасности в 2025 году

350–374[3][4] **млрд руб.**

объем рынка кибербезопасности в России в 2025 году

Российский рынок ИБ продолжает демонстрировать двузначные темпы роста, существенно опережая динамику ИТ-сектора в целом.

1 Исследование Б1 «На защите цифровой экономики. Рынок информационной безопасности».
2 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2025–2030 годы».
3 Исследование Б1 «Рынок информационной безопасности (ИБ-продукты и ИБ-услуги), рассчитанный в деньгах поставщиков» (то есть без учета наценки за перепродажу продуктов в каналах продаж).
4 По оценкам ЦСР.

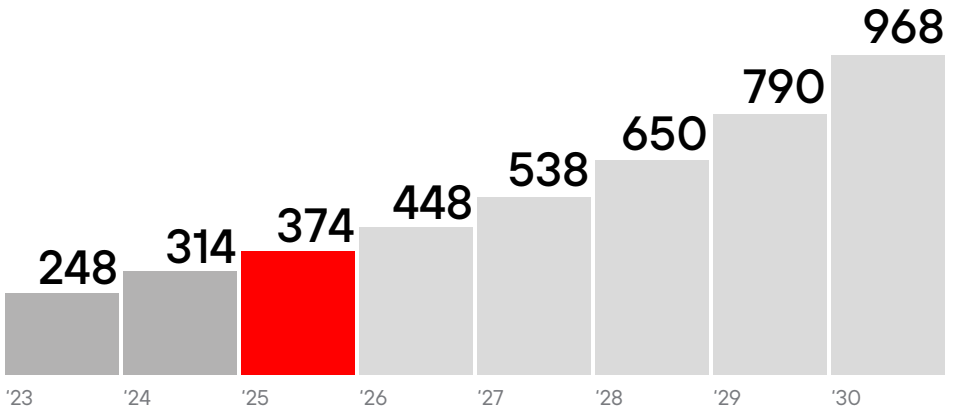
681[1]–968[2] млрд руб.

прогнозный объем рынка к 2030 году

Прогноз ЦСР

- В 2025 году объем рынка достигнет **374 млрд руб.**, что на 19% выше показателя 2024 года (314 млрд руб.).
- На горизонте до 2030 года рынок обладает потенциалом роста до **968 млрд руб.** со среднегодовым темпом (CAGR) на уровне 21%.

Прогноз развития рынка кибербезопасности, млрд руб.[5]



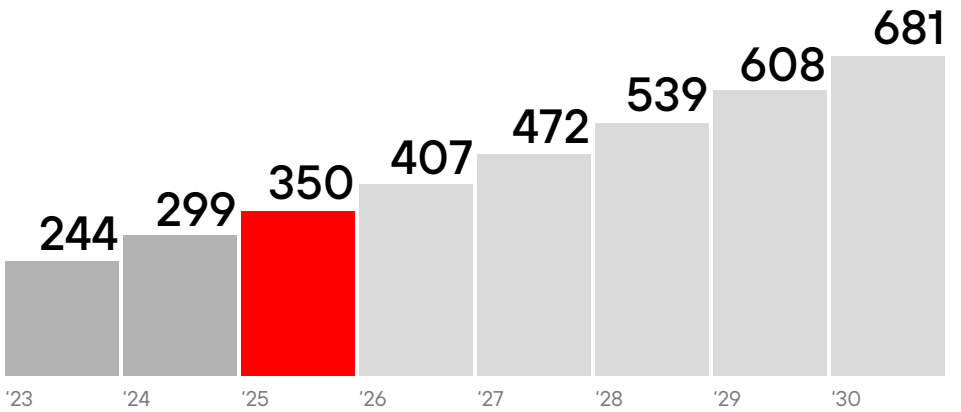
15[3]–21[4]%

среднегодовой темп роста (CAGR) до 2030 года

Прогноз Б1

- В 2025 году российский рынок ИБ вырастет на 17%, достигнув объема **350 млрд руб.** (в ценах поставщиков).
- В долгосрочной перспективе (до 2030 года) прогнозируется устойчивый рост на уровне 15%, что на 3 п. п. выше темпов развития ИТ-сектора.
- К 2030 году рынок может достичь объема **681 млрд руб.**

Прогноз развития рынка кибербезопасности, млрд руб.[6]



1 По оценке Б1.
2 По оценке ЦСР.
3 По оценке Б1.
4 По оценке ЦСР.
5 Рынок в деньгах клиентов. Данная оценка учитывает, помимо прочего, прогнозные темпы роста ВВП Российской Федерации (согласно текущему прогнозу Министерства экономического развития Российской Федерации до 2028 года) с последующим восстановлением темпов роста сектора ИБ к 2030 году до 23%.
6 Рынок в деньгах поставщиков, прогноз сформирован исходя из актуальных прогнозов макроэкономического развития России.

Драйверы роста российского рынка ИБ на горизонте 2025–2030 годов[1]

На долгосрочном горизонте динамика рынка поддерживается комплексом системных факторов, которые трансформируют кибербезопасность из вспомогательной ИТ-функции в фундамент устойчивости бизнеса.

1 Главным драйвером продолжит выступать **активная государственная политика**, направленная на укрепление национальной безопасности и обеспечение технологического суверенитета.

Кибербезопасность закреплена в стратегических документах России как ключевой элемент национальной устойчивости. Принятие «Концепции технологического развития до 2030 года» и включение ИБ в стратегию национальной безопасности способствовали формированию комплексной системы поддержки отечественных разработчиков, усилению программ импортозамещения и развитию суверенных ИТ-инфраструктур. Государство фактически определило кибербезопасность как приоритетную отрасль, обеспечивая ей институциональную и регуляторную поддержку.

2 Существенной поддержкой отрасли является сохранение налоговых льгот для российских ИТ- и ИБ-компаний. Продление нулевой ставки НДС на реализацию отечественного программного обеспечения (ПО), включенного в реестр Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России), позволяет разработчикам сохранять конкурентоспособность на внутреннем рынке, направлять высвобожденные средства на развитие и удерживать квалифицированные кадры. Отказ от введения НДС с 2026 года подтвердил стратегическую значимость отрасли для государства и укрепил доверие бизнеса к долгосрочной политике в сфере технологического суверенитета.

3 Рост деструктивности кибератак в 2024–2025 годах стал еще одним мощным стимулом для развития рынка. Кибератаки на российские компании наглядно показали, что злоумышленники все чаще нацелены не на кражу данных, а на физическое разрушение ИТ-инфраструктуры и парализацию бизнес-процессов. Компании начали воспринимать кибербезопасность не как техническую функцию, а как стратегическую задачу, напрямую влияющую на устойчивость бизнеса. В результате растет спрос на решения по мониторингу и реагированию на инциденты, а также на услуги по киберстрахованию.

1 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2025–2030 годы».

Драйверы роста российского рынка ИБ на горизонте 2025–2030 годов

4 Важным фактором, стимулирующим рост рынка, является усиление требований регуляторов и повышение ответственности компаний за утечки данных. Введение в 2025 году оборотных штрафов в размере до 3% годового оборота за повторные инциденты заставляет бизнес пересматривать подходы к защите информации. Это активизировало спрос на современные системы защиты персональных данных, аудит безопасности и консалтинговые услуги. Таким образом, регуляторные меры становятся фактором повышения зрелости рынка, стимулируя внедрение более совершенных технологий и процессов.

5 Рост применения технологий искусственного интеллекта (ИИ) также стимулирует рынок кибербезопасности. С одной стороны, ИИ создает новые угрозы — от подмены обучающих данных до автоматизированных фишинговых атак, с другой — становится инструментом защиты, лежащим в основе новых интеллектуальных систем детектирования и реагирования.

6 Драйвером на рынке услуг продолжит выступать кадровый дефицит в сфере ИБ. Нехватка квалифицированных специалистов вынуждает компании все чаще обращаться к аутсорсинговым и сервисным моделям (MSSP и MDR). Рынок управляемых сервисов кибербезопасности растет особенно быстро: бизнес стремится делегировать функции мониторинга, реагирования и анализа угроз профессиональным поставщикам. Параллельно развивается практика краудсорсинговых услуг, таких как программы багбаунти, которые получают поддержку со стороны государства и привлекают десятки тысяч независимых исследователей. Это расширяет охват тестирования и способствует повышению общей устойчивости цифровых сервисов.

Внешние факторы, сдерживающие рост рынка

Несмотря на позитивные прогнозы, эксперты ЦСР и участники рынка выделяют ряд факторов-ограничителей, способных замедлить динамику отрасли в среднесрочной перспективе.

1 Экономические факторы

Высокая ключевая ставка (в среднем 19,2% в 2025 году) ограничивает доступ к дешевому заемному капиталу, что ведет к снижению инвестиционной активности в ИБ-отрасли. Особое давление на маржинальность бизнеса окажет повышение страховых взносов для ИТ-компаний с 7,6 до 15% с 2026 года (для выплат в пределах базы). Данная мера потребует от вендоров жесткого фокуса на операционной эффективности и может привести к росту стоимости конечных ИБ-решений для заказчиков.

2 Усиление регулирования

Порог входа для новых разработчиков средств защиты информации (СЗИ) и сервисов повышается. Новые правила регистрации в реестре отечественного ПО (Постановление № 1236[1]) теперь включают обязательную совместимость продукта как минимум с двумя доверенными операционными системами (ОС) и требования к отсутствию иностранного контроля (более 50% владения у граждан России). Кроме того, обсуждаемый законопроект о создании реестра ФСБ для «белых хакеров» лишает исследователей анонимности и вводит жесткую регламентацию деятельности, что может замедлить развитие сегмента краудсорсингового анализа защищенности.

3 Внешние ограничения

Санкционное давление вынуждает российские компании ориентироваться преимущественно на внутренний рынок.

1 Постановление Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

НЕРАВНОМЕРНЫЙ РОСТ И УСКОРЕНИЕ КОНСОЛИДАЦИИ

Совокупность экономических и регуляторных факторов создает на российском рынке ИБ эффект «фильтрации». Высокая стоимость заемного капитала, растущая налоговая нагрузка и ужесточение требований к совместимости ПО формируют высокий порог входа для новых участников и малых технологических компаний. Мелкие компании и молодые проекты сталкиваются с серьезными финансовыми и правовыми трудностями, им все труднее конкурировать.

Однако для крупных игроков эти барьеры не становятся преградой, а в ряде случаев выступают катализатором роста. Лидеры рынка обладают достаточным запасом маржинальности и административным ресурсом, что позволяет им не только оперативно адаптироваться к новым правилам регуляторов, но и эффективно удовлетворять спрос, ранее распределявшийся между нишевыми компаниями или ушедшими западными вендорами.

Несмотря на внешнее давление, ключевые игроки сохраняют потенциал роста темпами, опережающими среднерыночные показатели. Таким образом, сдерживающие факторы ускоряют консолидацию отрасли, в которой устойчивость к регуляторным и финансовым рискам становится важным конкурентным преимуществом.

Ключевой вызов и стратегический приоритет[1]

Центральной задачей периода стал переход от фрагментарной закупки ИБ-инструментов к построению целостной архитектуры защиты.

Заказчики все чаще предпочитают интегрированные экосистемные решения, упрощающие управление безопасностью и повышающие эффективность защиты. Это приводит к росту спроса на платформенные или экосистемные продукты, охватывающие большой спектр задач и обеспечивающие легкую интеграцию, интегрированный клиентский опыт и консоли управления.

Вендоры с широким портфелем решений будут иметь преимущество перед конкурентами в ближайшие два-три года.

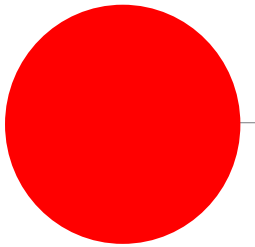
При этом на рынке останется место для инновационных технологических команд, ориентированных на отдельные точечные решения.

1 Исследование Б1 «На защите цифровой экономики. Рынок информационной безопасности».

Структура рынка: продукты и сервисы

Российский рынок ИБ сохраняет классическое деление на сегменты ИБ-продуктов и ИБ-услуг. Каждое из этих направлений критически важно для формирования комплексной защиты бизнеса и государственных структур.

29,4%
103 млрд руб.
ИБ-услуги



70,6%
247 млрд руб.
ИБ-продукты (СЗИ)

2025

Прогноз на 2025 год

Согласно оценкам Б1, в 2025 году ожидается следующее распределение объемов рынка (в ценах поставщиков).

Долгосрочная перспектива и структурная трансформация (до 2030 года)[1]

К 2030 году структура рынка претерпит качественные изменения. Прогнозируется, что доля продуктов составит 72%, в то время как на долю услуг придется 28%. Незначительное снижение доли сервисного сегмента (на 2 п. п. относительно текущих значений) будет вызвано сокращением объемов разовых проектных работ. При этом качественный рост внутри сегмента обеспечат новые модели потребления.

- **Структура потребления.** Российский рынок ИБ сохраняет выраженную ориентацию на корпоративный и государственный секторы. Ключевым потребителем выступает сегмент B2B[2], формирующий около 83% выручки. Доля B2G[3] (федеральные и региональные органы власти) составляет примерно 15%, в то время как на массовый потребительский сегмент (B2C[4]) приходится лишь 2% от общего объема рынка.

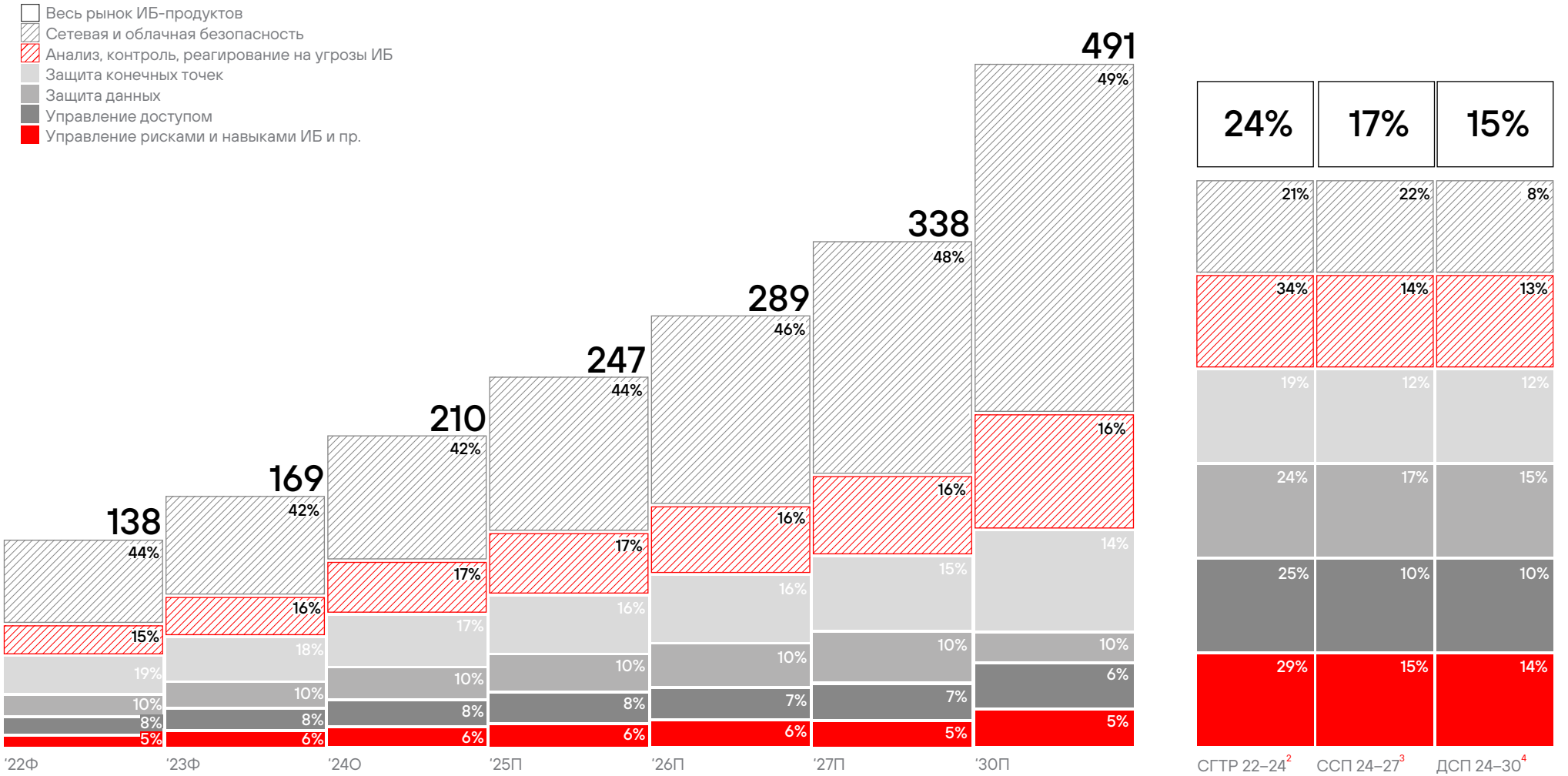
- **Локомотив роста услуг** — аутсорсинг и MSS. Данный сегмент будет расти опережающими темпами (на 3 п. п. быстрее рынка в целом). Основными драйверами станут критическая нехватка квалифицированных кадров, необходимость мгновенного реагирования на инциденты и массовый переход компаний на сервисные модели подписки.

- **Лидер продуктового сегмента** — сетевая и облачная безопасность. Это направление станет самым динамичным со среднегодовым темпом роста (CAGR) на уровне 18%. Развитие сектора продиктовано реализацией отложенного спроса на импортозамещение сетевого оборудования и стремительной миграцией бизнеса в облачные инфраструктуры, требующие специализированных средств защиты приложений.

1 Исследование Б1 «На защите цифровой экономики. Рынок информационной безопасности».
2 Рынок, на котором компании продают товары и услуги другим компаниям.
3 Рынок, на котором компании продают товары и услуги государственным учреждениям.
4 Рынок, на котором компании продают товары и услуги конечным потребителям (частным лицам).

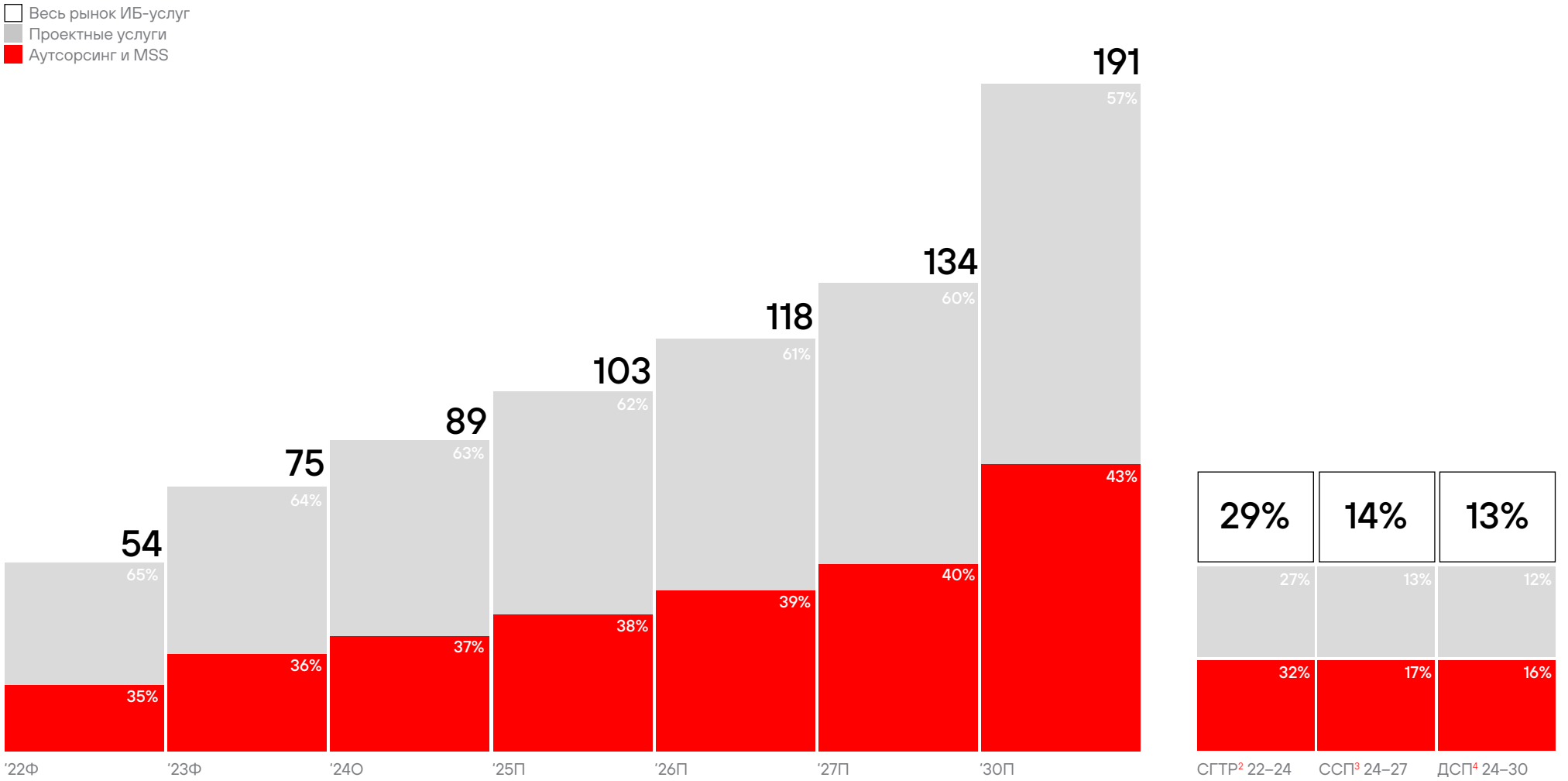
2030

Динамика рынка ИБ-продуктов в России[1], млрд руб.



1 Исследование Б1. Рынок в деньгах поставщиков, прогноз сформирован исходя из актуальных прогнозов макроэкономического развития Российской Федерации. Прогноз на 2030 год в разрезе технологий сделан на основе текущих технологических трендов и ландшафта угроз и может измениться в связи с развитием новых технологий атаки и защиты.
2 Среднегодовой темп роста.
3 Среднесрочный прогноз.
4 Долгосрочный прогноз.

Динамика рынка ИБ-услуг в России[1], млрд руб.



1 Исследование Б1. Рынок в деньгах поставщиков, прогноз сформирован исходя из актуальных прогнозов макроэкономического развития Российской Федерации. Прогноз на 2030 год в разрезе технологий сделан на основе текущих технологических трендов и ландшафта угроз и может измениться в связи с развитием новых технологий атаки и защиты.
2 Среднегодовой темп роста.
3 Среднесрочный прогноз.
4 Долгосрочный прогноз.

Конкурентный ландшафт и позиция Positive Technologies

Российский рынок кибербезопасности прошел этап глубокой трансформации и на сегодняшний день представлен преимущественно отечественными игроками. По данным исследователей (Б1 и ЦСР), в отрасли активно работают около 300 компаний, из которых 190 специализируются на разработке собственных ИБ-продуктов.

Лидеры рынка

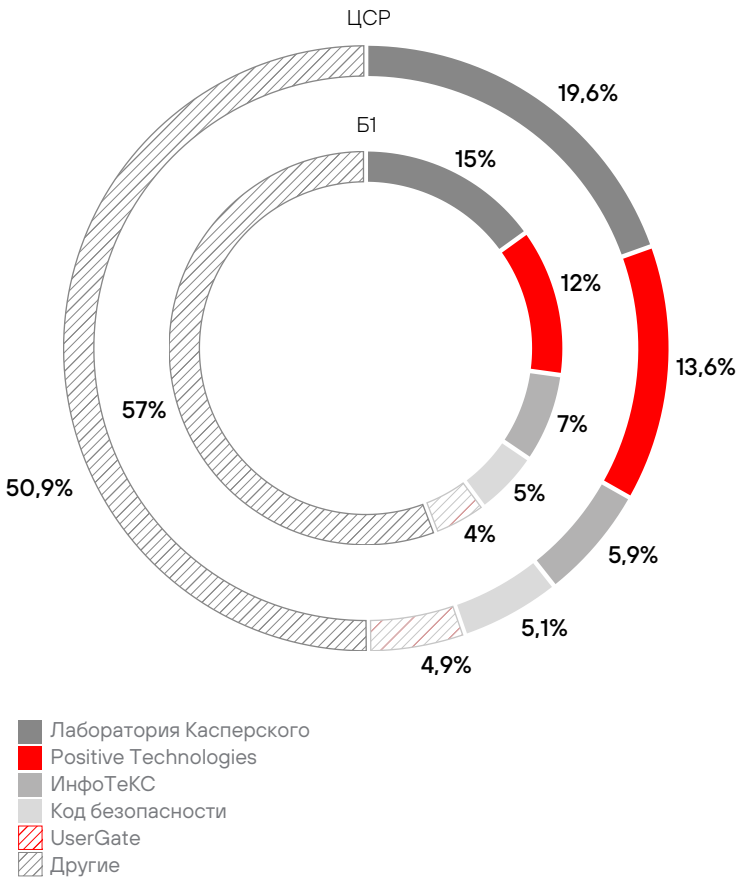
Рынок СЗИ характеризуется высокой степенью консолидации: на топ-5 вендоров приходится значительная доля выручки всего сегмента.

Сравнение долей рынка по данным ведущих аналитиков

Разные методологии оценки дают небольшие расхождения в цифрах, но подтверждают единый состав группы лидеров.

1 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы».
2 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2024-2028 годы».
3 Исследование ЦСР «Прогноз развития рынка кибербезопасности в Российской Федерации на 2025-2030 годы».

Доли вендоров средств защиты информации на рынке по результатам 2024 года



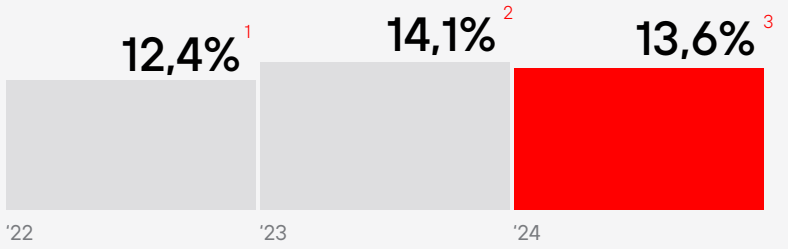
Динамика рыночной доли в 2024 году

Positive Technologies стабильно удерживает статус одного из лидеров рынка СЗИ, прочно занимая **второе место** среди российских разработчиков.

В 2024 году Компания столкнулась с серьезными вызовами. Итоговые показатели оказались ниже первоначальных ожиданий менеджмента: Компания не выполнила ранее заявленный прогноз (гайденс) по ряду показателей. Эти результаты нашли свое отражение в оценке рыночной доли Positive Technologies в рамках методологии ЦСР: по итогам 2024 года она составила **13,6%** (относительно базы 14,1% в 2023 году). Данное изменение оценки в первую очередь фиксирует специфику отчетного периода и финансовые результаты участников именно за 2024 год.

Positive Technologies подтверждает свой статус ведущего игрока во всех критически важных сегментах: от реализации комплексных сервисных проектов до вывода на рынок инновационных решений в новых технологических нишах. Наша стратегия остается неизменной — обеспечение результативной кибербезопасности для бизнеса и государства, что является залогом долгосрочной инвестиционной привлекательности Компании.

Доля Positive Technologies в 2022–2024 годах



Международный рынок

Состояние и перспективы мирового рынка кибербезопасности

В настоящее время глобальный рынок кибербезопасности находится в фазе устойчивого роста, обусловленного цифровизацией экономики и усложнением киберугроз. Однако оценки ведущих аналитических агентств относительно темпов этого роста и итоговых объемов рынка заметно различаются.

На середину 2020-х годов оценки объема рынка варьируются в широком диапазоне — от **97 млрд до 302 млрд долл. США к 2025 году**. Несмотря на разницу в цифрах, все аналитики сходятся в прогнозе устойчивого роста до конца десятилетия.

Анализ данных позволяет выделить три основные линии прогнозирования.

1 Умеренно оптимистичные сценарии
(Mordor Intelligence, Precedence Research)

Эта группа агентств ожидает высокую динамику со среднегодовым темпом роста (CAGR) в диапазоне 12,28–12,6%.

- Mordor Intelligence прогнозирует рост с **235,5 млрд долл. США** в 2025 году до **471,9 млрд** к 2031 году.
- Precedence Research дает наиболее амбициозный прогноз, оценивая рынок в **301,9 млрд долл. США** в 2025 году с достижением **878,5 млрд к 2034 году**.

2 Сценарий структурного удвоения
(анализ Б1)

Аналитики компании Б1 занимают в своих прогнозах наиболее взвешенную позицию. Их подход базируется на консолидации данных Gartner и Statista, что позволяет рассматривать динамику рынка через призму его «структурного удвоения» в среднесрочной перспективе.

Согласно отчету Б1, глобальный сектор кибербезопасности находится в цикле кратного роста, который охватывает период с 2022 по 2028 год. В рамках этой модели выделяются следующие ключевые этапы.

- **Базис (2022 год):** фактический показатель объема глобального рынка в 2022 году составил **144 млрд долл. США**.
- **Целевой ориентир** (2028 год): к концу периода рынок достигнет отметки **294 млрд долл. США**.
- **Темпы роста:** прогнозируемый среднегодовой прирост составит порядка **12%**. Это позволяет рынку ИБ стабильно опережать темпы развития совокупного ИТ-сектора на 3–4 п. п.

3 Консервативный сценарий
(Statista)

Оценка Statista заметно сдержаннее как по объемам, так и по темпам развития.

- **Ожидаемый объем** рынка к 2025 году — **196,51 млрд долл. США**.
- **Прогнозируемый темп роста** (CAGR) на период 2025–2030 годов составляет 6,18%, а объем рынка в 2030 году достигнет **265,17 млрд долл. США**.

Сводная таблица прогнозов

	Mordor Intelligence	Precedence Research	Б1	Statista
Объем глобального рынка кибербезопасности в 2025 году[1], млрд долл. США	235,5	301,9	184[2]	196,51
Целевой показатель, млрд долл. США / год	471,9 к 2031 году	878,5 к 2034 году	294 к 2028 году	265,17 к 2030 году
Прогнозный CAGR, %	12,3	12,6	12	6,18

1 Оценка аналитических агентств.
2 Справочно приведена оценка объема рынка в 2024 году, так как оценка объема рынка в 2025 году отсутствует.

Ключевые драйверы роста мирового рынка ИБ

Согласно исследование компании **Б1**, стремительное развитие рынка ИБ обусловлено комплексом факторов: от изменения ландшафта угроз до фундаментальной перестройки бизнес-стратегий и госрегулирования.

1 Трансформация ИБ в стратегический бизнес-приоритет

Кибербезопасность перестала быть узкотехнической задачей и перешла в плоскость управления рисками на уровне высшего руководства.

- **Интеграция в бизнес: 84%** компаний в мире классифицируют риски ИБ как критически важные для бизнеса.
- **Внимание топ-менеджмента:** для **64%** организаций вопросы киберзащиты стали постоянным пунктом повестки советов директоров.

2 Эволюция и эскалация угроз

Рост рынка напрямую коррелирует с увеличением частоты и разрушительности кибератак.

- **Интенсивность:** более **50%** компаний столкнулись с реализацией киберрисков в течение последних двух лет.
- **Геополитический фактор:** с 2021 года количество политически мотивированных атак увеличилось почти в **пять раз**.
- **Рост преступности:** увеличение численности киберпреступных группировок и совершенствование их инструментария заставляют бизнес наращивать защитные бюджеты.

3 Технологические вызовы. Облака и ИИ

Цифровая трансформация создает новые векторы атак, требующие современных решений.

- **Облачная безопасность:** переход на облачные решения привел к резкому скачку инцидентов в 2023 году — число вторжений в облачную среду выросло на **75%**, а общее количество связанных с ней инцидентов — на **110%**.
- **Фактор ИИ:** генеративный ИИ становится инструментом в руках хакеров. По прогнозам, в ближайшем будущем **22%** всех атак и утечек будут напрямую связаны с внедрением ИИ-технологий.

4 Регуляторное давление

Государственное регулирование выступает мощным катализатором инвестиций.

- **Законодательная активность:** только за период 2023–2024 годов в мире было принято более **170 новых законов** в сфере защиты данных и борьбы с утечками.
- **Влияние на бюджеты: 83%** организаций подтверждают, что именно ужесточение законодательства стало ключевым стимулом для увеличения их инвестиций в ИБ.

5 Дефицит компетенций

Внутренние кадровые проблемы заставляют компании обращаться к рынку внешних ИБ-услуг и автоматизированных решений.

- **Кадровый голод:** менее **50%** руководителей считают, что их компании обладают штатом и компетенциями, достаточными для отражения современных угроз.

Точки роста глобального рынка кибербезопасности

1

Самый быстрорастущий сегмент на глобальном рынке ИБ-продуктов — сетевая и облачная безопасность, чей прогнозируемый среднегодовой рост составит 15%, то есть на 3 п. п. больше, чем в среднем по рынку, в первую очередь за счет увеличения количества онлайн-приложений и сетевых угроз, развития облачных технологий и необходимости защиты облачных сред.

2

На рынке ИБ-продуктов быстрее других будут расти следующие технологии: защита облачных решений, платформы защиты конечных точек на предприятиях, решения Zero Trust[1], межсетевые экраны, ПО в области аналитики и выявления угроз, решения в области выявления и управления уязвимостями.

3

На рынке ИБ-услуг самым динамичным сегментом будет аутсорсинг и MSS[2] с прогнозируемым среднегодовым ростом 15%. В основном это связано с нехваткой квалифицированных специалистов по ИБ, высокими затратами на формирование внутренних компетенций, необходимостью ускоренного реагирования на инциденты и общим ростом популярности сервисных моделей защиты информации.

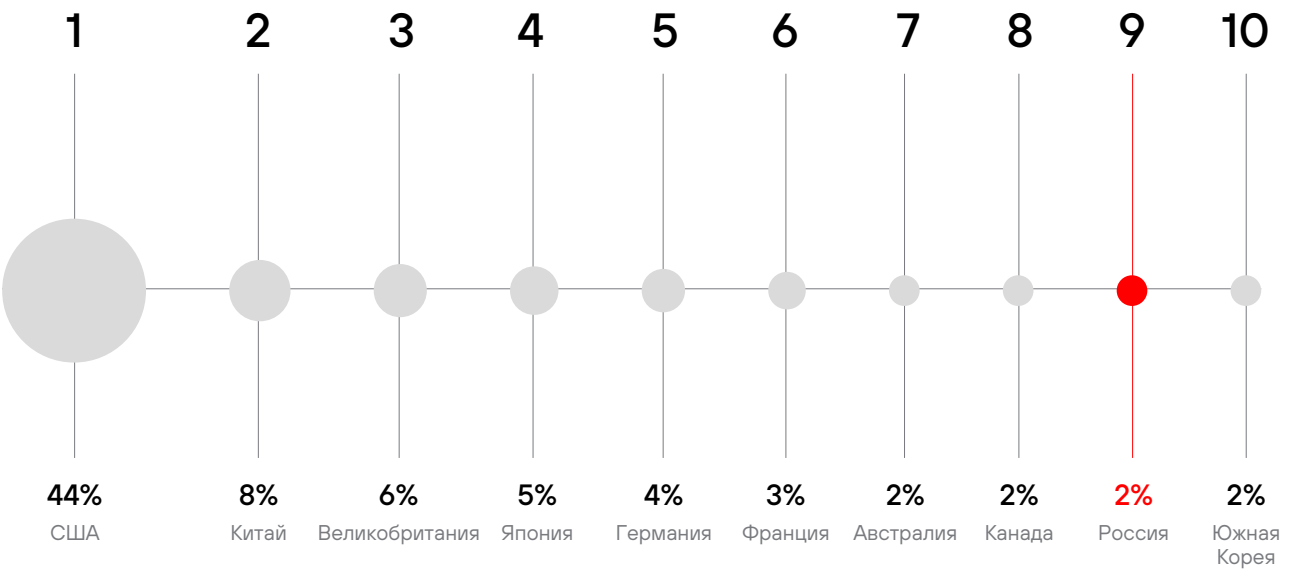
4

На рынке ИБ-услуг ключевой точкой роста станут сервисы MDR[3], которые в 2024–2028 годах будут в среднем прибавлять по 18% в год.

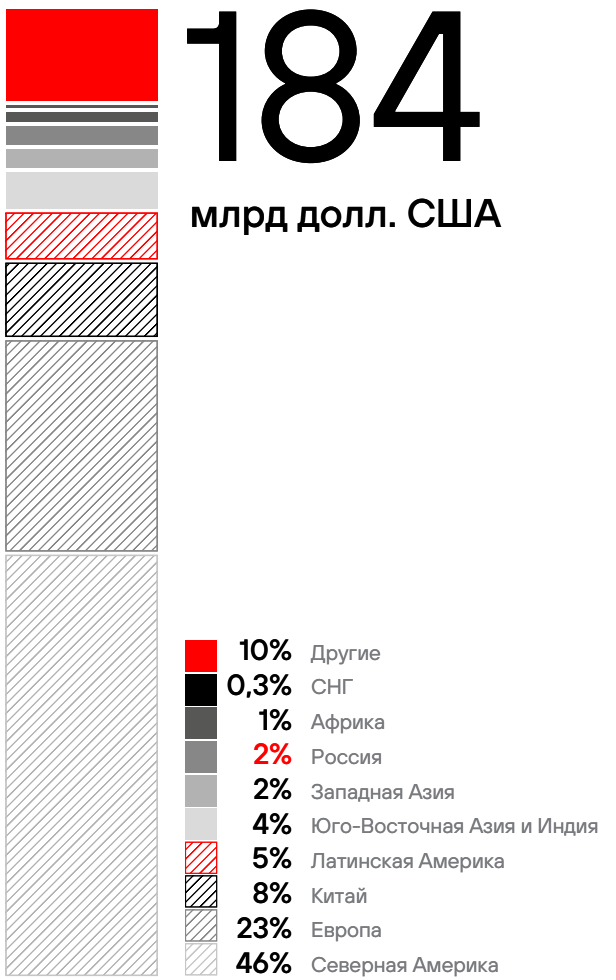
1 Концепция «нулевого доверия», в рамках которой рабочие процессы пересматриваются на основе отсутствия доверия к любому пользователю перед началом каждой операции.
2 Управляемые сервисы безопасности.
3 Услуги по защите от киберугроз за счет расширенных возможностей мониторинга, обнаружения и быстрого реагирования на инциденты.

Региональная динамика: место России в глобальной экосистеме

Доля топ-10 стран



Доли стран в общих тратах на ИБ в 2024 году



Мировой рынок ИБ характеризуется чрезвычайно высокой географической концентрацией: на топ-10 стран приходится подавляющая часть всех мировых расходов на кибербезопасность.

Россия входит в число лидеров по расходам на ИБ и занимает по этому показателю **девятое место в мире.**

9

Технологические тренды

Тренды от Positive Technologies

Эксперты Positive Technologies выделили основные технологические тренды в сфере кибербезопасности.

Современный ландшафт киберугроз трансформируется из точечных атак в «цифровые штормы» — комплексные, высокоавтоматизированные и разрушительные воздействия. В ответ на это индустрия переходит от формальной защиты к стратегии кибербезопасности, нацеленной на результат.

Тренд № 1

Применение AI[1], ML[2] в российских решениях для кибербезопасности

Использование технологий AI и ML в средствах защиты является ключевым трендом 2025 года. Цель — повысить качество ключевых функций продуктов (детектирование угроз, выявление наиболее слабых мест инфраструктуры), снизить количество рутинных операций, сократить время реакции на инциденты. Помимо этого, большие языковые модели (LLM), например, могут собирать дополнительный контекст, позволяющий сократить время анализа инцидентов ИБ.

Безусловно, полезность технологий должна быть проверена на практике, измерена и подтверждена большим числом клиентов. AI-модели лишь начинают использоваться в качестве компонентов средств защиты и пока не стали гейм-чейнджерами для клиентов, но следующий год, судя по тому, какие задачи уже смог взять на себя AI, может стать переломным.

1 Искусственный интеллект (ИИ).
2 Машинное обучение — совокупность методов ИИ, с помощью которых можно создавать самообучающиеся компьютерные системы.

Тренды от Positive Technologies

1 Данные об угрозах — собранная, проанализированная и обогащенная информация о текущих и потенциальных киберугрозах.
2 SOC (Security Operations Center, центр мониторинга информационной безопасности) — структурное подразделение организации, отвечающее за оперативный мониторинг ИТ-среды и предотвращение киберинцидентов. Специалисты SOC непрерывно осуществляют контроль за сообщениями, поступающими от технических средств, чтобы как можно оперативнее выявить и устранить угрозу ИБ.
3 Защита конечных точек.
4 Система мониторинга событий кибербезопасности и управления инцидентами.
5 NTA/NDR — системы кибербезопасности для глубокого анализа сетевого трафика с целью обнаружения и реагирования на сложные киберугрозы.
6 Тестирование на проникновение.
7 Программа, в рамках которой компании платят независимым исследователям (этичным хакерам) за поиск и сообщение об уязвимостях в их ПО, продуктах или ИТ-инфраструктуре, позволяя исправить ошибки до того, как их используют злоумышленники.

Тренд № 2

Возвращение в облака

После 2022 года многие компании стали ярыми противниками облаков. На фоне санкционной политики зарубежные вендоры в моменте отозвали лицензии, из-за чего «окирпичились» продукты, имеющие связь с западными облаками. Кроме того, они прекратили обновлять экспертизу в продуктах (сигнатуры и патчи безопасности), что привело к потенциальной уязвимости этих СЗИ.

В 2024 год тренд на использование облаков начал разворачиваться, а в 2025-м — усиливаться. Одновременно с этим растет доверие к российским облачным сервисам, а на фоне дефицита серверов и оборудования они иногда являются единственным решением для бизнеса.

Вендоры в сфере кибербезопасности также используют облачные платформы для оказания дополнительных услуг клиентам, будь то расширенные данные threat intelligence[1], позволяющие обогатить срабатывания средств защиты, или применение AI- и ML-технологий, требующих высокопроизводительных серверов, которые не всегда есть на стороне клиента. MDR-, MSS-провайдеры тоже являются частью тренда: компании строят кибербезопасность под ключ из облака, передавая провайдерам данные с сенсоров SOC[2] (из решений классов EDR[3], SIEM[4], NTA/NDR[5]).

По мнению экспертов Positive Technologies, тренд сохранится в ближайшие годы, и направление, связанное с облачными технологиями, будет развиваться быстрее других в сфере ИТ и ИБ.

Тренд № 3

Результативность и измеримая кибербезопасность

На фоне громких кибератак последних лет и 2025 года в частности у многих компаний возник запрос на то, чтобы регулярно получать объективное понимание своей защищенности и измерять результат применения той или иной технологии или функции в целом. Этот запрос может включать:

- требование гарантий от сервис-провайдеров (например, выполняющих функции SOC);
- проведение пентеста[6] или проектов red team для оценки защищенности и проверки эффективности собственного SOC;
- выход на площадку багбаунти[7], где у компании есть возможность протестировать защищенность ИТ-инфраструктуры или ее отдельных элементов в разных форматах: экспресс-багбаунти, классическая программа поиска уязвимостей или киберисытания;
- привлечение вендорского надзора за тем, как интегратор внедряет технологии;
- проведение хэлсчека и других проверок атомарных функций продуктов.

Все вышеперечисленное свидетельствует о повышении уровня зрелости компаний и о продолжающемся переходе от бумажной безопасности к практико-ориентированной. Тенденция будет усиливаться в ближайшие годы, потому что это единственный путь к пониманию собственной защищенности на фоне возрастающего количества и сложности кибератак.

Тренды от Positive Technologies

Тренд № 4

Развитие экосистемных решений и упрощение технологий ИБ

Развитие экосистемных и платформенных решений становится ответом на стремление заказчиков упростить ИТ-ландшафт, повысить уровень интеграции и обеспечить сквозное управление кибербезопасностью. Популярность платформ, способных бесшовно объединять различные инструменты защиты, неизбежно растет. Этот процесс подстегивается качественным изменением рынка: за последние несколько лет число компаний с собственными подразделениями ИБ увеличилось многократно, в том числе за счет малого и среднего бизнеса. Однако на фоне расширения рынка дефицит кадров продолжает усиливаться. Это ведет к снижению порога входа в профессию и ставит перед вендорами новую задачу — адаптировать свои продукты под запросы менее подготовленных специалистов.

В гонке ИБ-производителей победят те, кто предложит не просто разрозненные функции, а интегрированные платформы, ориентированные на удобство пользователя:

- внедрение интеллектуальных ассистентов и автоматизацию рутинных операций;
- переход к наглядной визуализации аномалий и результатов работы средств защиты;
- радикальное упрощение работы с логами и событиями безопасности.

Такой подход востребован не только внутри страны, но и на рынках государств-партнеров, сталкивающихся с аналогичными вызовами. Вендор, сумевший объединить технологическую мощь платформы с простотой ее эксплуатации, не только укрепит позиции в России, но и получит стратегическое преимущество на международной арене.

Тренды от Gartner

Аналитики Gartner также определили 10 стратегических технологических трендов на 2026 год, которые объединены в три ключевые темы: «Архитектор» (The Architect), «Синтезатор» (The Synthesist) и «Авангард» (The Vanguard). Эти инновации направлены на создание устойчивого фундамента, оркестрацию интеллектуальных систем и защиту ценностей бизнеса в мире, где доминирует ИИ.

Главные стратегические технологические тренды Gartner на 2026 год

Сейчас (1–3 года)
Скоро (3–5 лет)

1 AI-Native Development Platforms
2 AI Supercomputing Platforms
3 Confidential Computing
4 Multiagent Systems
5 Domain-Specific Language Models
6 Physical AI
7 Preemptive Cybersecurity
8 Digital Provenance
9 AI Security Platforms
10 Geopatriation

1 Архитектор — построение фундамента для ИИ-трансформации

Тренды этой группы сосредоточены на создании масштабируемых и безопасных основ для внедрения цифровых инноваций.

- **AI-Native Development Platforms:** платформы разработки, созданные на базе генеративного ИИ, упрощают создание ПО и позволяют небольшим командам быстро выпускать гибкие продукты корпоративного уровня. Согласно прогнозам, к 2030 году 80% организаций перейдут от больших команд разработчиков к малым группам, усиленным ИИ.
- **AI Supercomputing Platforms:** эти платформы объединяют CPU, GPU и специализированные чипы (ASIC) для обработки сверхсложных нагрузок, таких как обучение моделей и симуляции. Ожидается, что к 2028 году более 40% ведущих компаний внедрят гибридные вычислительные архитектуры в свои основные бизнес-процессы.
- **Confidential Computing:** технология обеспечивает защиту данных непосредственно в процессе их обработки в памяти процессора (TEE), что позволяет безопасно использовать ИИ даже в недоверенных облачных средах. К 2029 году более 75% операций в сторонних инфраструктурах будут защищены этим методом.

2 Синтезатор — создание новой ценности через оркестрацию

В центре внимания этой группы — интеграция специализированных моделей и интеллектуальных агентов для автоматизации и повышения точности бизнес-процессов.

- **Multiagent Systems (MAS):** системы, в которых группы специализированных ИИ-агентов взаимодействуют для решения сложных общих задач, обеспечивая динамическую оркестрацию операций вместо линейной автоматизации.
- **Domain-Specific Language Models (DSLMs):** специализированные языковые модели, обученные на данных конкретных отраслей (финансы, медицина), обеспечивают на 40% более высокую точность и лучший комплаенс по сравнению с универсальными LLM.
- **Physical AI:** внедрение ИИ в роботов, дроны и автономное оборудование позволяет машинам воспринимать физический мир, принимать решения и действовать самостоятельно, повышая производительность в логистике и промышленности.

3 Авангард — безопасность, доверие и управление

Тренды этого блока призваны защитить репутацию компаний и обеспечить соответствие регуляторным нормам в эпоху цифровой фрагментации.

- **Preemptive Cybersecurity:** смещение парадигмы защиты от реагирования к проактивному предотвращению атак через прогнозирование действий злоумышленников и автоматизированное моделирование угроз. К 2028 году ИБ-продукты, лишенные превентивных функций, потеряют рыночную актуальность.
- **Digital Provenance:** системы верификации происхождения данных и ПО, которые становятся критически важными для защиты от дипфейков и атак на цепочки поставок.
- **AI Security Platforms:** единые инструменты для контроля безопасности как собственных, так и сторонних ИИ-приложений, централизующие мониторинг и соблюдение политик использования. К 2028 году такие платформы будут использовать более 50% предприятий.
- **Geopatriation (геопатриация):** перенос данных и рабочих нагрузок из глобальных публичных облаков в суверенные или региональные инфраструктуры для минимизации геополитических рисков и соблюдения требований суверенитета данных. Прогнозируется, что к 2030 году этот подход примут более 75% организаций в Европе и на Ближнем Востоке.

В 2026 году роль ИБ-специалиста сместится от ручного анализа событий к роли «архитектора правил» и тренера нейросетевых моделей. Победу на рынке одержат компании, предлагающие не просто ПО, а «архитектуру результата», гарантирующую невозможность наступления недопустимых для бизнеса событий.

2025 год стал временем серьезных испытаний и перемен в кибербезопасности. Бизнес осознал цену кибератак и начал требовать гарантий и ответственности, государство усилило контроль за цифровым пространством, а технологии (в частности, ИИ) изменили правила игры в самой сути атак и защиты. В 2026 году эти тенденции, скорее всего, получат дальнейшее развитие. Мир движется к тому, что кибербезопасность перестает быть узкой технической темой — она влияет на финансовые показатели, на устойчивость экономики и на общество в целом. Соответственно, внимание к ней со стороны руководителей, регуляторов и общественности будет только расти. Новые вызовы, будь то автономные ИИ-угрозы или геополитическое противостояние в киберпространстве, потребуют от всех участников скоординированных и инновационных подходов. Главный урок 2025 года очевиден: кибербезопасность — не роскошь и не формальность, а неотъемлемое условие развития и стабильности в цифровую эпоху. В 2026 году нас ждет развитие этой новой реальности, где устойчивость к киберрискам станет одним из определяющих факторов успеха на всех уровнях.

НАША СТРАТЕГИЯ

Positive Technologies стремится к глобальному технологическому лидерству, выступая в роли визионера и трендсеттера мировой индустрии кибербезопасности. Мы выходим за рамки традиционных подходов, создавая связи между ИТ и ИБ и формируя принципиально новые стандарты защиты.

Для поддержания высоких темпов развития бизнеса, опережающих динамику рынка в среднесрочной перспективе, мы сохраняем гибкость, оперативно адаптируемся к изменениям и используем новые возможности. Наша стратегия определяет ключевые направления роста, оставляя команде свободу в выборе инструментов и решений для их достижения.

Наши главные цели

1. Укрепление лидерства на российском рынке за счет вывода на рынок инновационных продуктов и решений
2. Поддержание высоких темпов роста бизнеса
3. Расширение присутствия на международных рынках
4. Рост капитализации Компании в соответствии с динамикой роста бизнеса

Наши стратегические приоритеты и цели на 2026 год

- Результативная кибербезопасность: мы делаем недопустимые события невозможными
- Выпуск продуктов, имеющих конкурентное преимущество в мировом масштабе
- Создание автопилота в сфере кибербезопасности
- Международная экспансия

Positive Technologies строит стратегию развития на четких и формализованных задачах, ориентированных на годовой горизонт планирования. Это позволяет нам динамично адаптироваться к изменениям, сохраняя устойчивый вектор развития.

На 2026 год Компания ставит перед собой конкретную финансовую цель — сохранить темпы роста бизнеса, вдвое превышающие динамику роста рынка кибербезопасности. Этот ориентир отражает наши амбиции по дальнейшему развитию бизнеса, укреплению позиций на рынке и расширению ключевых направлений.

При формировании финансовых ориентиров мы фокусируемся на реалистичности целей, обеспечивая их достижимость и четкую связь с результатами работы команды продаж. Такой подход помогает нам не только эффективно планировать рост бизнеса, но и поддерживать прозрачность и предсказуемость для всех участников процесса.

В 2026 году Positive Technologies продолжит фокусироваться на поддержании высокой финансовой эффективности и будет стремиться ограничить общий объем расходов на уровне 2025 года. Наряду с ростом объема отгрузок это станет важным шагом в достижении целевого уровня маржинальности по NIC в среднесрочной перспективе.

Цели на 2026 год

Вернуть рост капитализации, соответствующий темпам роста бизнеса

1. Приблизить маржинальность по NIC к целевым значениям
2. Продолжить выплачивать дивиденды
3. Удержать затраты flat в 2026 году
4. Сохранить темпы роста бизнеса, вдвое превышающие динамику роста рынка кибербезопасности

Выполнение целей на 2025 год

1 Компания вернулась к целевым темпам роста, гайденс по отгрузкам выполнен

+40% рост год к году

33,6 млрд руб.

составили отгрузки в 2025 году

10–15%

Рост российского рынка кибербезопасности в 2025 году[1]

2 Возвращение NIC[2] в положительную зону

2,7 млрд руб.

на **5,4 млрд** руб. больше, чем в 2024 году

3 Возвращение к возможности выплачивать дивиденды

- Положительный NIC дает возможность рассмотреть вопрос о выплате дивидендов

4 Сохранение численности штата на уровне середины 2024 года

2605

сотрудников работают в Компании по состоянию на конец 2025 года

5 Снижение операционных расходов

–25% расходы, не связанные с оплатой труда,

в том числе:

–20% отраслевые мероприятия и развитие бизнеса

–41% business support

–65% расходы на маркетинг

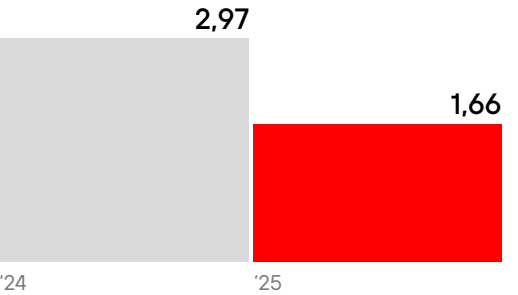
6 Компания сохранила инвестиции в R&D на уровне прошлого года

9,1 млрд руб.

составили инвестиции в R&D в 2025 году

7 Снижение уровня долговой нагрузки

Net Debt / EBITDA



1 По экспертным оценкам.
2 Чистая прибыль без учета капитализируемых расходов.

Наши стратегические проекты

Результативная кибербезопасность: мы делаем недопустимые события невозможными

Наши продукты, сервисы и услуги дают подтверждаемый результат

В 2025 году измеримая кибербезопасность с гарантированным результатом стала актуальна для компаний любого масштаба и уровня зрелости процессов ИБ.

Руководители хотят не просто тратить средства на защиту, а быть уверенными в ее эффективности. Этот фокус отражается и в повестке регуляторов. Резонансные инциденты 2025 года показали: большой бюджет и серьезные усилия еще не гарантируют киберустойчивость. Рынку нужны новые подходы к оценке результатов, способные обеспечить уверенность, причем ежедневную, в результативности средств и мер безопасности.

Positive Technologies помогает выстраивать результативную кибербезопасность компаниям и госучреждениям, которые при постановке целей, планировании затрат на ИБ и выборе средств защиты фокусируются на предотвращении событий, способных нанести их деятельности необратимый ущерб. Убедиться в защищенности от неприемлемых событий — объективно, на практике и с понятным результатом, — как и получить уверенность в киберустойчивости в целом, можно, лишь выйдя на кибериспытания.

Результативная кибербезопасность: мы делаем недопустимые события невозможными

2024–2027

Почта России строит результативную кибербезопасность

В 2025 году Компания запустила инициативы по приведению заказчиков к измеримой киберустойчивости в кратчайшие сроки. Ими стали облачное решение PT X, в рамках которого Positive Technologies гарантирует защиту с покрытием финансовых рисков: помогает выйти на кибериспытания и при выполнении компаниями «киберминимума» выплачивает вознаграждение исследователям в случае взлома. PT X помогает компаниям усилить защиту или команду одним решением, без необходимости покупать отдельные продукты. Для усиления или в период развития собственных SOC Positive Technologies также представила набор сервисов PT Boost. Он помогает компаниям прийти к измеримому результату максимально быстро и с полной экспертной поддержкой Positive Technologies.

Компании уже оценили результаты этих решений и сервисов. Так, например, Rambler&Co вместе с нами сделала кибербезопасность измеримой за три месяца, а Минцифры Оренбургской области внедрило новые подходы к киберустойчивости и оценило их на кибериспытаниях.

В 2025 году стартовал уникальный в индустрии проект, в рамках которого лидеры рынка в течение трех лет будут совместно выстраивать киберустойчивость Почты России. Positive Technologies стала партнером по внедрению результативной ИБ в корпоративном сегменте. Наша задача — сделать так, чтобы злоумышленники не могли реализовать три из пяти стратегических рисков компании.

Отличительная черта проекта — результат каждого из трех этапов подтверждается на киберучениях, в ходе которых независимые команды белых хакеров оценят реальную способность выстроенной комплексной системы кибербезопасности отражать сложные атаки. Мы рассчитываем, что полученный в ходе проекта опыт сможем масштабировать на другие системно значимые компании. Результативная ИБ содействует кооперации отечественных игроков кибербезопасности. Сотрудничая друг с другом, мы вместе начинаем мыслить в терминах измеримой защиты, конкретных и честных итогов выполненной работы и будем в силах не только качественно повысить защищенность отдельных компаний и отраслей, но и усилить национальную киберустойчивость.

Подробнее о проектах по построению результативной кибербезопасности читайте в разделе «О Компании»

PT NGFW

Межсетевой экран нового поколения. Продукт относится сразу к двум нишам: это и средство защиты, так как обеспечивает безопасность периметра компании от внешних угроз, и ИТ-решение, от которого зависит доступность интернета для корпоративных пользователей и скорость доступа к внешним ресурсам. Ключевые особенности PT NGFW — высокая производительность, стабильность и надежность.

В 2025 году наш флагманский продукт PT NGFW прошел стадию признания: он получил отличные отзывы от партнеров и уже эксплуатируется крупнейшими заказчиками. Учитывая специфику и инертность крупного бизнеса, мы рассматриваем отчетный период как фундамент для экспансии. 2026 год станет для Компании временем реализации накопленного потенциала, когда технологическое превосходство трансформируется в кратный рост финансовых результатов.

146,3 млрд руб.

по оценке Центра стратегических разработок к 2030 году рынок NGFW составит.

Positive Technologies планирует занять **не менее половины** этого рынка

Главные достижения 2025 года

Подробнее о PT NGFW читайте в разделе «Продукты, решения, сервисы»

>x2

рост продаж

250

внедрений за год

1 тыс.

устройств продано

Endpoint Security

Концепция полной защиты конечных устройств. Представлена в виде двух продуктов — MaxPatrol EPP и MaxPatrol EDR.

Клиенты могут планомерно использовать базовую защиту и усиливать ее по мере необходимости, защищаясь и от массовых атак, и от продвинутых хакеров. Такая комбинация делает Positive Technologies более конкурентной, в том числе и на международном рынке.

Точки роста

В 2026 году Компания предоставляет клиентам комплексное предложение для всесторонней защиты устройства, а не отдельные продукты. Клиенты смогут начать с базовой защиты и усилить ее для противодействия сложным атакам.

На текущий момент мы становимся вторым вендором, который способен предоставить мощную связку решений EPP + EDR.

Это рыночная тенденция, которая де-факто является стандартом в западных решениях, которые ранее привыкли использовать в том числе и наши клиенты.

5%

минимальный целевой ориентир Компании по доле на российском рынке

Мы также продолжаем наращивать свое присутствие на международном рынке, **конкурируя с крупнейшими игроками** индустрии кибербезопасности, включая традиционных поставщиков антивирусного ПО.

MaxPatrol EPP

Endpoint Security

Система комплексной защиты устройств от массового вредоносного программного обеспечения (ВПО), вирусов и программ-шифровальщиков. Решение формирует фундаментальный уровень киберустойчивости организации, обеспечивая безопасную среду для цифровой трансформации бизнеса. В современных реалиях наличие EPP является необходимым стандартом технологической гигиены и обязательным условием непрерывности бизнес-процессов.

Бизнес-обоснование

- Рынок продуктов для защиты конечных устройств в России составляет, по разным оценкам, около 30 млрд руб. Сегмент включает антивирусы и более функциональные корпоративные решения (EDR). Если ранее Positive Technologies работала в основном в сегменте продвинутых решений против APT, то теперь Компания может предлагать комплексное решение.
- Компания планирует занять долю не менее 5% этого рынка.
- У ряда клиентов антивирусный контур закрывают конкурентные продукты. Единое предложение Positive Technologies позволит таким заказчикам использовать единый агент и снизить капитальные и операционные затраты как ИБ-, так и ИТ-команд. Совместное предложение EDR + EPP повышает потенциал увеличения среднего чека Positive Technologies. В проектах, где клиенты выбирают MaxPatrol EDR, Компания сможет дополнить контур комплексным решением MaxPatrol EPP.
- Продукт хорошо включается в подход Positive Technologies к РКБ. В комплексных проектах удастся закрывать больше векторов атак и не зависеть от сторонних решений в инфраструктуре заказчика.

Точки роста

- Соответствие требованиям регуляторов в России и Беларуси — сертификация САВЗ — снимает барьер для продаж в Enterprise. Особенно важно для финансового сектора, где есть требование двух независимых сертифицированных антивирусов.
- Усиливаем возможности превентивной защиты. Это и паритет по сравнению с конкурентами, и значимый шаг к результативной кибербезопасности — снижаем поверхность атаки у клиентов, популярные методы проникновения не сработают.
- Международный рынок — конкуренция с мировыми лидерами и OEM.
- Увеличение клиентской базы — продажи в «юбки» холдингов, где тяжелые экспертные решения недоступны.
- У нас многие клиенты именно для антивирусной защиты применяют продукты конкурентов. Предложение от Positive Technologies позволит таким клиентам использовать наш единый агент — это заметное снижение капитальных и операционных затрат как ИБ-, так и ИТ-команд. Совместное предложение = увеличение среднего чека.

Подробнее о MaxPatrol EPP читайте в разделе «Продукты, решения, сервисы»

MaxPatrol EDR

Endpoint Security

Защищает компьютеры, серверы и виртуализированные рабочие места от сложных кибератак. Это инструмент для компаний с высокой зрелостью ИБ, которые учитывают риск атак не только массовых вирусов и ВПО, но и со стороны продвинутых злоумышленников и организованных группировок.

Точки роста

- Рынок EDR-решений России — около 4 млрд руб. (экспертная оценка). В 2025 году мы заняли на нем 22% и показываем рост в 2,5 раза год к году.
- Соответствие требованиям нового класса защитных решений от ФСТЭК — СОР. Мы одними из первых вендоров выполнили сертификационные требования. Это важно клиентам для соблюдения требований приказа ФСТЭК № 117 (требования к защите информации для ГИС и ИС госсектора).
- Важно снижать операционные затраты на установку и настройку продукта — такую функциональность развиваем в 2026 году еще больше. В конечном итоге клиент получит установку и ввод продукта в эксплуатацию за один день.
- Ультимативная защита — хакеры, привыкшие обходить антивирусы и другие средства защиты, не смогут это сделать в случае MaxPatrol EDR, защита работает всегда. Продукт уже на Bug Bounty, и проверить его защищенность могут исследователи со всего мира.

Подробнее о MaxPatrol EDR читайте в разделе «Продукты, решения, сервисы»

PT X

Облачное решение для мониторинга
и реагирования на киберугрозы в режиме 24/7.

Бизнес-обоснование

Новая реальность кибербезопасности показывает, что жертвами атак становятся не только крупные корпорации, но и компании среднего и малого бизнеса. Во многих таких организациях либо нет выделенных специалистов по ИБ, либо функции ИБ выполняют универсальные сотрудники, которые не могут обеспечить круглосуточный мониторинг и реагирование.

В этой ситуации наличие PT X зачастую является единственным шансом получить экспертный уровень защиты.

К Positive Technologies нередко обращаются компании, которые столкнулись со взломом. Даже после работы нашей команды Incident Response риск повторного инцидента сохраняется.

Теперь Positive Technologies предлагает срочную помощь при инциденте, дает доступную и постоянную защиту из облака, а также гарантирует ее результативность через вывод клиента на киберисытания.

Точки роста

- Развитие ML/AI-технологий и расширение их применения и автоматизации для еще более точного и быстрого разбора инцидентов у клиентов.
- Первые референсы по клиентам, которые выполнили наши рекомендации и вышли на киберисытания.

Подробнее о PT X читайте в разделе
«Продукты, решения, сервисы»

PT ISIM

Защита промышленных инфраструктур

Система обеспечения киберустойчивости промышленных инфраструктур.

Почему мы решили пойти в промышленный сегмент

Цифровизация промышленности неизбежно ведет к расширению поверхности атаки, то есть к увеличению числа точек входа для злоумышленника. Наши технологии развиваются в соответствии с новой реальностью и управляют рисками не точечно, а по всей инфраструктуре.

Базовые меры безопасности в промышленности в перспективе десяти лет больше не будут сводиться к простой изоляции контура. Так как промышленность активно цифровизируется, ИТ-сегмент потребует большего взаимодействия с технологическим сегментом (ОТ). К тому же структура ролей будет усложняться — появляются новые роли (например, CDTO), отвечающие за нативное взаимодействие ИТ- и ОТ-сегментов.

- **Чтобы следовать миссии и сделать цифровую трансформацию промышленности безопасной**

Чтобы промышленные предприятия могли развиваться и не бояться вызовов цифровизации, мы строим продукт для киберустойчивости, покрывающий всю промышленную инфраструктуру — от сетевого уровня и технологических сегментов до конечных узлов и сервисов.

- **Чтобы удовлетворить спрос по обеспечению киберустойчивости в промышленной безопасности**

Рынок OT Security в России находится на ранней стадии развития: при большом объеме промышленной инфраструктуры покрытие средствами защиты остается низким. Мы прогнозируем сценарий, при котором в ближайшие пять лет рынок OT Security будет расти быстрее рынка IT Security почти в два раза.

Драйверы спроса

- **Вызовы цифровизации для промышленности:** расширение поверхности для кибератак, усложнение контроля технологического контура и рост рисков инцидентов и простоя.
- **Усиление регуляторного давления (ФСТЭК/КИИ):** среди значимых объектов КИИ минимально необходимый уровень защиты обеспечен только у 36% организаций. А внедрять и подтверждать выполнение установленных мер защиты нужно всем промышленным предприятиям.
- **Зарождающийся спрос на унифицированные инструменты** для сбора и агрегации данных со всей производственной инфраструктуры в единое хранилище (например, Data Lake) для анализа и принятия управленческих решений. С этим потенциально могут помочь ИБ-продукты для ОТ.

Ответ Positive Technologies на запрос рынка в 2025 году

Эволюция PT ISIM — от ОТ-сетевого сенсора в систему обеспечения киберустойчивости промышленных инфраструктур.

Цель: сделать ОТ инфраструктуру предприятия защищенной, управляемой и устойчивой, а управление — прозрачным.

Наши главные ресурсы — технологичность и промышленная экспертиза.

Подробнее о PT ISIM читайте в разделе «Продукты, решения, сервисы»

PT Dephaze

Автопентест для оценки уровня защищенности внутренней инфраструктуры. PT Dephaze поможет перейти от разовых проверок к непрерывной оценке защищенности. Система действует как реальный хакер: проводит разведку, выявляет уязвимости, эксплуатирует их в конкретном окружении и оценивает эффективность средств защиты. Вы получаете объективную картину состояния инфраструктуры в условиях, максимально приближенных к боевым.

Бизнес-обоснование

Пентест остается единственным корректным способом оценить реальную защищенность организации. При этом сам рынок в классическом понимании выглядит ограниченным, поэтому фокус был сделан не на его объеме, а на роли пентеста как ключевой точки входа. PT Dephaze задумывался как открывающий продукт в логике «пентест → продукты» и инструмент, который масштабирует завоевание заказчиков.

Подробнее о PT Dephaze читайте в разделе «Продукты, решения, сервисы»

Подробнее о PT NAD читайте в разделе «Продукты, решения, сервисы»

PT NAD

Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий хакеров в трафике.

Стратегия и точки роста 2026 года

PT NAD остается самым технологичным средством анализа трафика на рынке. Уникальная технология DPI обеспечивает гарантированную стабильность работы продукта.

Развитие функционала будет сфокусировано на трех направлениях:

1. Новый движок поиска угроз: увеличение скорости и глубины обнаружения аномалий для расследований инцидентов любого масштаба.
2. Функция реагирования: расширение продукта в плоскость активной защиты — переход от детекта к автоматизированному реагированию на угрозы на сетевом уровне.
3. Развитие ML-технологий: повышение точности детектирования и снижение ложных срабатываний за счет ML-модулей.

MaxPatrol O2

Автопилот для результативной кибербезопасности. Обнаружение и остановка хакера с минимальным участием человека. Продукт автоматизирует процессы обнаружения, расследования и реагирования на кибератаки для защиты в условиях ограниченных ресурсов.

Точки роста

- Дефицит квалифицированных специалистов.
- Рост количества инцидентов.
- Требование сокращения времени расследования.
- Повышение эффективности SOC без увеличения штата.

Ожидание 2026 года — масштабирование внедрений за счет зрелой архитектуры и связки с управленческим слоем.

До 30%

зафиксировано снижение нагрузки на команду в пилотах

Стратегический эффект 2026 года

Объединение продуктов в единую архитектуру позволяет:

- переходить от точечных продаж к архитектурным проектам,
- расширять сегмент за счет облачной модели,
- формировать понятную траекторию роста клиента внутри портфеля.

Ключевой трек 2026 года — развитие платформенной модели SOC с тремя уровнями: обнаружение, управление, автоматизация.

Подробнее о MaxPatrol O2 читайте в разделе «Продукты, решения, сервисы»

MaxPatrol SIEM

Ожидание на 2026 год

Сохранение темпов роста за счет расширения адресуемого сегмента через облачную модель и обновление технологической базы.

Система управления событиями ИБ, предназначенная для выявления сложных и целенаправленных кибератак в инфраструктурах любого масштаба.

Система собирает и анализирует события безопасности из различных источников ИТ-инфраструктуры и помогает SOC-командам обнаруживать угрозы и инциденты в режиме реального времени.

Текущая позиция

В 2025 году продукт показал почти двукратный рост выручки год к году. Доля рынка увеличилась и составила 63%. Рост обеспечен спросом со стороны клиентов к стабильному и зрелому продукту, который отвечает запросам рынка и регуляторов как в технологическом уровне, так и ценовом.

Стратегия 2026 года

Развитие идет в двух моделях поставки:

- On-premise — для крупных инфраструктур и регулируемых отраслей.
- Cloud — для компаний, которым требуется быстрый запуск SOC без длительного инфраструктурного цикла.

В 2026 году усиливается пользовательский контур:

- новый интерфейс,
- AI-ассистент,
- повышение производительности,
- масштабируемость.

Точки роста

- Компании, переходящие от MSSP к собственному SOC.
- Средний сегмент, где важна скорость запуска.
- Заказчики с растущими объемами данных.

Облачная версия рассматривается как **новый тип** поставки MaxPatrol SIEM, а не отдельный продукт и является точкой роста в 2026 году.

Подробнее о MaxPatrol SIEM читайте в разделе «Продукты, решения, сервисы»

PT Application Firewall

Высокопроизводительный межсетевой экран для непрерывной защиты любых приложений — от небольших сайтов до больших enterprise-приложений — от внешних киберугроз. Он предоставляет возможность гибкой настройки и может масштабироваться в соответствии с требованиями бизнеса. PT Application Firewall PRO содержит сильнейшую на российском рынке экспертизу по обнаружению и блокировке целенаправленных атак, основанную на собственном опыте проведения пентестов и на данных от исследовательской группы Positive Research и специалистов PT ESC. PT Application Firewall защищает приложения более 700 крупных отечественных организаций.

Подробнее о PT Application Firewall читайте в разделе «Продукты, решения, сервисы»

По итогам 2025 года PT Application Firewall:

- стал значительно производительнее;
- лучше масштабируется в распределенных инфраструктурах;
- проще и безопаснее конфигурируется;
- глубже интегрируется с другими продуктами Компании;
- стал удобнее для повседневной эксплуатации.

Эти изменения создают прочную основу для дальнейшего развития продукта в 2026 году.

Объем рынка WAF в 2026 году

7 млрд руб.
SAM[1]

4 млрд руб.
SOM[2]

1 SAM (Serviceable Addressable Market) — доступный объем рынка.
2 SOM (Serviceable Obtainable Market) — реально достижимый объем рынка.

PT Data Security

Для нас **безопасность данных** — это новое и стратегически важное направление развития. Мы расширяем продуктовый портфель, фокусируясь на решении одной из самых критичных задач для бизнеса, напрямую влияющей на его репутацию, капитализацию и операционную эффективность. В целом мы рассматриваем 2025 год как точку выхода продукта на рынок и формирования устойчивой базы для масштабирования в 2026 году и далее.

Платформа нового поколения для обеспечения безопасности данных. Объединяет в себе инвентаризацию, автоматизированную классификацию и мониторинг обращений к данным независимо от их места размещения и представления. Таким образом, обеспечивает полную видимость всей инфраструктуры хранения и обработки данных компании.

Бизнес-обоснование

Мы запустили разработку **PT Data Security** как ответ на системный запрос рынка: данные стали ключевым активом бизнеса и одновременно — одной из главных целей атак со стороны злоумышленников. При этом управление безопасностью данных для большинства компаний по-прежнему остается серьезной проблемой: оно фрагментировано, трудозатратно и неэффективно из-за использования морально устаревших средств защиты, созданных 10–15 лет назад и не рассчитанных на современные ИТ-ландшафты.

Сегодня такие понятия, как утечки данных, вышли далеко за пределы узкого ИБ-сообщества и воспринимаются как понятные и измеримые риски для бизнеса, влияющие на операционную устойчивость, финансовые показатели и репутацию компаний.

Компании сталкиваются сразу с несколькими ключевыми вызовами при построении единой системы безопасности данных:

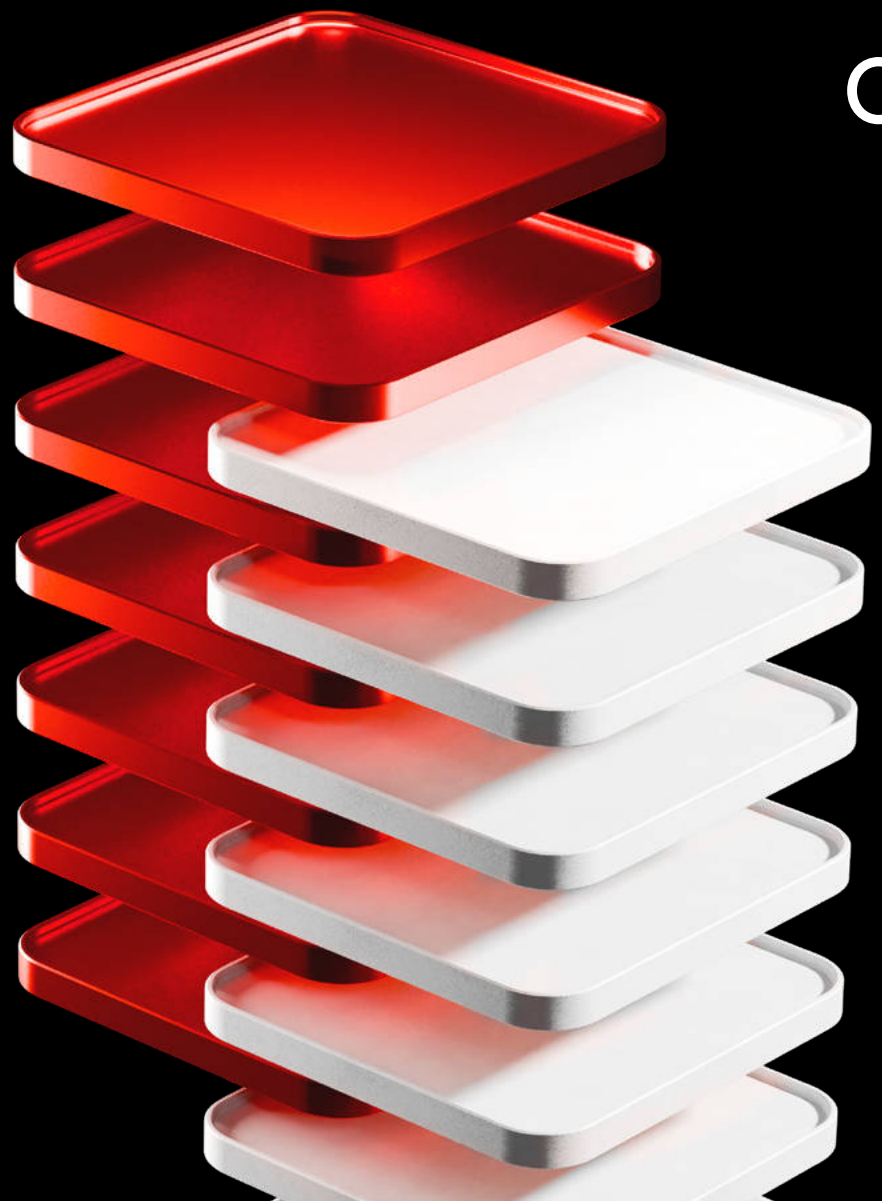
- стремительный рост объемов данных, а также числа и типов хранилищ;
- высокая распределенность инфраструктуры хранения и обработки данных — от десятков до сотен и тысяч сегментов;
- невозможность сформировать целостную картину и обеспечить полную видимость данных из-за разрозненности классических инструментов защиты.

С точки зрения бизнеса это приводит к избыточным трудовым и финансовым затратам на приобретение и поддержку нескольких решений одновременно, отсутствию полной прозрачности инфраструктуры и появлению большого количества слепых зон, не покрытых ни одним средством защиты. Именно такие зоны чаще всего становятся точками входа для злоумышленников.

Подробнее о PT Data Security читайте в разделе «Продукты, решения, сервисы»

Партнерства

Соглашение о стратегическом партнерстве в области бизнеса, технологий и экспертизы между Positive Technologies и CyberOK



Объекты продаж

VULNUM

Собственная база знаний об уязвимостях, эксплойтах и патчах безопасности, обогащенная своей экспертизой

СКИПА

Система контроля и информирования поверхности атак (External Attack Surface Management, EASM)

PentOps

Сервис непрерывного тестирования на проникновение внешнего периметра

Наши ключевые ресурсы — люди и технологии

Сильная и эффективная команда

В течение 2025 года Компания продолжила усиливать команду сильными специалистами и экспертами в области кибербезопасности, сохранив количество сотрудников на уровне середины 2024 года. Знания и опыт профессионалов с глубокой отраслевой экспертизой, а также сильная команда продаж позволяют Компании уверенно двигаться вперед, решая самые сложные задачи.

За последние несколько лет мы прошли через значительную трансформацию, изменив подход к организации команд и процессов разработки. Мы отошли от традиционных департаментов и «цехов», перейдя к кросс-функциональным микрокомандам, которые работают как внутренние стартапы. Такие команды не только разрабатывают решения, но и несут ответственность за их развитие, что повышает гибкость, ускоряет внедрение инноваций и улучшает качество продуктов. Такой подход позволяет нам быстрее адаптироваться к изменяющимся требованиям рынка, улучшать качество продуктов и внедрять инновации на каждом этапе разработки.

Создание сильной и эффективной команды — часть нашей стратегии, направленной на развитие передовых технологий и устойчивое развитие бизнеса.

ИНВЕСТИЦИИ В R&D: ФУНДАМЕНТ УСТОЙЧИВОГО РОСТА

Развитие технологий и создание инновационных решений — ключевые драйверы роста Positive Technologies. Мы сохраняем инвестиции в исследования и разработки (R&D), поскольку убеждены, что именно это обеспечит долгосрочное масштабирование бизнеса и укрепление позиций Компании на рынке кибербезопасности.

В 2025 году объем вложений в разработку новых продуктов, совершенствование существующих решений, а также в технологические и инфраструктурные проекты составил 9,1 млрд руб., что сопоставимо с уровнем прошлого года. Инвестиции в R&D — стратегическая необходимость, поскольку инвестиции в технологии формируют будущие конкурентные преимущества Компании.

Мы осознанно выбираем путь инвестиций в передовые разработки, понимая, что это фундамент долгосрочного успеха и устойчивого лидерства на рынке.

РАЗВИТИЕ БИЗНЕСА ЗА РУБЕЖОМ

Топ-3 торгового предложения

- PT NAD
- PT Application Inspector
- Профессиональные сервисы в области оценки кибербезопасности

2025 год стал для Компании годом активного развития зарубежного бизнеса. Мы продолжили масштабировать внутренние ресурсы, чтобы эффективно развивать и поддерживать наши проекты для иностранных партнеров и заказчиков, работающих за пределами России, а также развивать собственные инициативы в области образования для специалистов за рубежом.

В отчетном году Компания значительно расширила международное присутствие. Увеличение штата pre-sales-инженеров и менеджеров по продажам в ключевых регионах позволило обеспечить локальную поддержку клиентов на их родном языке с учетом часовых поясов и возможностью очного взаимодействия.

Наибольшим спросом из нашего торгового предложения в 2025 году пользовались PT NAD, PT Application Inspector и наши профессиональные сервисы в области оценки кибербезопасности.

НАШИ ФОКУСНЫЕ РЕГИОНЫ

Ближний Восток и Северная Африка (MENA)

Алжир, Бахрейн, Египет, Иордания, Ирак, Иран, Катар, ОАЭ, Оман, Палестина, Саудовская Аравия, Тунис

СНГ

Беларусь, Казахстан, Узбекистан

Азиатско-Тихоокеанский регион (APAC)

Вьетнам, Индия, Индонезия, Малайзия, Пакистан, Республика Корея, Таиланд

Латинская Америка[1] (LATAM)

Бразилия, Мексика, Перу, Уругвай, Куба

Африка

ЮАР, Эфиопия, Танзания, Уганда, Сенегал и Экваториальная Гвинея

1 Включая Карибы.

Ближний Восток и Северная Африка (MENA)

›20

проектов в 7 странах

›x5

рост выручки в 2025 году

›20

партнерских соглашений

2025 год стал годом активного роста нашего бизнеса в регионе Ближнего Востока и Северной Африки. За этот период мы реализовали более 20 проектов в семи странах региона — Саудовской Аравии, ОАЭ, Омане, Катаре, Египте, Иордании и Тунисе. Наши решения были внедрены в ключевых отраслях экономики, в том числе в государственном секторе, финансовых организациях и промышленности. Основной фокус проектов был направлен на защиту приложений и проведение сервисов по оценке защищенности, что позволило заказчикам повысить устойчивость своих цифровых инфраструктур к современным киберугрозам. Благодаря этому развитию выручка по сравнению с 2024 годом увеличилась более чем в пять раз.

Не менее важным направлением нашей работы стало развитие профессионального сообщества и обмен экспертизой. В течение года мы провели три практических киберучения CyberDrill — в Египте, Омане и Марокко, — где участники могли отработать сценарии реагирования на реальные кибератаки. Параллельно наша команда активно участвовала в крупнейших отраслевых мероприятиях региона, включая GISEC, GITEX, E-CRIME, FDC и BlackHat, где мы делились экспертизой и обсуждали ключевые тренды развития кибербезопасности.

Еще одним важным результатом года стало развитие партнерской экосистемы. Мы подписали более 20 партнерских соглашений с ведущими системными интеграторами и поставщиками управляемых сервисов в регионе. Кроме того, мы выстроили активное взаимодействие с международной организацией OIC-CERT, а также с национальными центрами и агентствами по кибербезопасности стран региона MENA. Это сотрудничество направлено на обмен информацией об актуальных киберугрозах и укрепление коллективной устойчивости цифровой инфраструктуры региона.

Мероприятия:

- GISEC
- GITEX
- E-CRIME
- FDC
- BlackHat
- Киберучения CyberDrill в Египте, Омане и Марокко
- Взаимодействие с OIC-CERT

Защищаем:

- государственный сектор,
- финансовые организации,
- промышленность

ИРАН

Первые продажи:

- банковский сектор,
- государственные учреждения,
- телеком-операторы.

›10 активных партнеров

Сертификация
всей продуктовой линейки

По итогам активной работы в регионе мы завершили сертификацию всей продуктовой линейки Positive Technologies. Уже состоялись первые продажи в ключевых отраслях — банковском секторе, государственных учреждениях и у телеком-операторов. Параллельно активно развивается партнерская сеть: на сегодняшний день у нас более десяти активных партнеров, которые помогают масштабировать присутствие и реализовывать проекты на рынке.

Латинская Америка (LATAM)[1]

В 2025 году Positive Technologies продолжила развитие бизнеса в Латинской Америке, расширяя присутствие на новых рынках региона. Среди ключевых результатов года — закрытие первого проекта Компании в Уругвае в секторе здравоохранения, что стало важным шагом в расширении географии Positive Technologies.

В Мексике было успешно реализовано первое продление проекта для государственного заказчика, подтвердившее востребованность решений Компании и открывающее возможности для дальнейшего развития сотрудничества с государственным сектором.

Одним из значимых событий года стали первые в истории Кубы практические киберучения Cyberdrill, проведенные при участии представителей государственных структур и профильных министерств. Мероприятие позволило продемонстрировать экспертизу Positive Technologies в области практической кибербезопасности.

Компания также продолжила развитие партнерской экосистемы, включая проведение первого партнерского дня в Бразилии и расширение сотрудничества с локальными интеграторами и дистрибьюторами.

Мероприятия:

- Киберучения CyberDrill (Куба)
- Партнерский день Positive Technologies в Сан-Паулу (Бразилия)

Защищаем:

- государственный сектор (Мексика),
- сектор здравоохранения (Уругвай)

1 Включая Карибы.

АФРИКА

>20 пилотных проектов

Победы в крупных конкурсах

PT NAD, MaxPatrol VM,
PT Application Inspector, MaxPatrol SIEM

В 2025 году удалось добиться эффективного локального присутствия Positive Technologies в ЮАР, Эфиопии, Танзании, Уганде, Сенегале и Экваториальной Гвинее. Компания заключила соглашения с ведущими игроками-партнерами в ИТ- и ИБ-индустриях, а также получила поддержку по направлению GR и со стороны руководителей развития бизнеса (BDM) у крупных LE-заказчиков. Для работы в регионе были наняты местные sales- и pre-sales-сотрудники.
В выбранных локациях успешно реализовано более 20 пилотных проектов; обеспечены победы в крупных конкурсах в отношении продуктов Positive Technologies: PT NAD, MaxPatrol VM, PT Application Inspector, MaxPatrol SIEM. В 2026 году Positive Technologies планирует реализовать полноценное присутствие в выбранных локациях для масштабирования коммерческого успеха и поиска новых объектов продаж.

Юго-Восточная Азия

PT NAD

защищает нефтегазовый сектор Индонезии Pertamina

Расширение сотрудничества с вузами

Готовим новое поколение сильных специалистов совместно с ведущими университетами Индонезии:

UGM, ITB, Muhammadiyah University и другими

2025 год стал прорывным для бизнеса Компании в Индонезии. Мы реализовали две ключевые вехи. Первая — это экспансия в нефтегазовый сектор. Теперь наш флагманский продукт PT NAD защищает инфраструктуру подразделения Pertamina, который является лидером нефтегазовой промышленности в Индонезии. На данный момент ведутся переговоры для масштабирования этого успеха и защиты не только ИТ-, но и ОТ-сегмента и внедрения нашего решения во все группы компаний Pertamina.

Вторая веха — развитие киберобразования. По заказу Министерства образования мы создаем систему подготовки специалистов по кибербезопасности для страны. Вместе с ведущими университетами Индонезии — UGM, ITB, Muhammadiyah University и другими — внедряем образовательные программы и практическую подготовку на базе симуляции реальных атак.

В ближайшие годы это позволит сформировать более 5 тыс. специалистов, которые будут обеспечивать устойчивость и защищенность цифровой среды Индонезии.

ИНДИЯ

По итогам первого полноценного года работы в Индии Компания сформировала устойчивую партнерскую экосистему и пул проектов в крупнейших индустриальных центрах: Дели, Калькутте, Мумбаи, Ахмедабаде и Бенгалуру. В активной фазе находятся несколько проектов на объектах критической энергетической инфраструктуры Индии. Отдельный интерес вызывает портфель продуктов и сервисов в области обучения кибербезопасности. Компания развивает это направление совместно с рядом университетов. Сотрудничество с Confederation of Indian Industry перешло на новый уровень. Конфедерация собирает официальную делегацию индийских компаний на Positive Hack Days.

СНГ

Первые продажи PT NGFW в Беларуси

Наиболее высокую динамику в регионе демонстрируют рынки кибербезопасности Беларуси и Узбекистана. Темпы их развития сегодня превышают общемировые, при этом показатели роста Positive Technologies опережают рыночные значения. Знаковым событием года стал успешный старт продаж нашего флагманского межсетевого экрана нового поколения — PT NGFW — на территории Беларуси. Это подтверждает высокую востребованность инновационных технологий Компании в странах Содружества.

Партнерский канал

16 партнеров Premium и Advanced

14 онлайн-курсов

73 30% от базы
партнера обучаются онлайн

7 очных мероприятий в MENA, LATAM, Азии, Иране

›50 партнеров прошли очное обучение

›80% лидов сгенерировано партнерами

В 2025 году Positive Technologies активно развивала партнерский канал как ключевой инструмент масштабирования международного бизнеса. Компания внедрила партнерскую программу и вывела 16 партнеров на уровни Premium и Advanced. Параллельно совершенствовалась система дистанционного обучения: количество специализированных курсов по продуктам увеличилось с пяти до 14. На текущий момент на онлайн-платформе проходят подготовку 73 партнера (около 30% всей базы), тогда как ранее их число не превышало 18. Для повышения прикладных компетенций в регионах MENA, Азии, Иране и Латинской Америке было проведено семь офлайн-мероприятий по глубокому обучению установке и траблшутингу продуктов, в которых приняли участие более 50 партнеров.

Важным этапом стал запуск международного партнерского портала. По итогам года более 80% лидов было сгенерировано партнерами.

ПРОДУКТЫ, РЕШЕНИЯ, СЕРВИСЫ

- Принципы и подходы к разработке
- Инвестируем в экспертность
- Наши продукты
- Наши услуги и экспертиза

ПРИНЦИПЫ И ПОДХОДЫ К РАЗРАБОТКЕ

Positive Technologies разрабатывает продукты, ориентируясь на современные технологические тренды и используя передовые технологии.

Каждый новый продукт становится органичной частью нашей продуктовой линейки, включающей более 25 продуктов и решений, предназначенных для обеспечения максимальной киберустойчивости бизнеса. Разработка и тестирование технологий в среднем занимают около двух лет, чтобы гарантировать надежность, эффективность и соответствие актуальным вызовам отрасли.

Развитие технологий

Основные инвестиции в создание Security Data Lake были сделаны два-три года назад: закуплена необходимая инфраструктура и сформирована команда, которая занимается обучением собственных больших языковых моделей для обнаружения хакерских атак на основе данных от всех наших продуктовых агентов. Наша глобальная цель остается неизменной — создать своего рода автопилот кибербезопасности, при котором даже сложная атака может быть остановлена одним специалистом.

Важно подчеркнуть, что такой «автопилот» был бы невозможен без технологий искусственного интеллекта. Мы разрабатываем и обучаем собственные модели, которые работают внутри инфраструктуры Компании и постоянно совершенствуются на основе нашей экспертизы. В этом процессе участвует большая команда специалистов: хакеры-исследователи, эксперты по кибербезопасности и ML-специалисты, создающие алгоритмы машинного обучения.

Модели обучаются на совокупности данных — нашей внутренней экспертизе и информации, поступающей от клиентов. При этом все клиентские данные обрабатываются и хранятся в закрытой защищенной среде: они используются для обучения моделей и повышения эффективности обнаружения атак.

В результате сочетания инфраструктуры Security Data Lake, собственной экспертизы и технологий искусственного интеллекта мы формируем уникальную технологическую базу. Именно на основе этих данных и алгоритмов появляются новые продукты и решения, которые позволяют быстрее выявлять угрозы, автоматизировать реагирование на атаки и постепенно приближаться к созданию полноценного автопилота кибербезопасности.

ML в продуктах Positive Technologies

В течение 2025 года мы сохраняли фокус на развитии технологий машинного обучения в наших продуктах. ML берет на себя часть задач по мониторингу вредоносной активности и реагированию на инциденты, снижая нагрузку на сотрудников SOC.

Например, ML-модуль поведенческого анализа Behavioral Anomaly Detection (MaxPatrol BAD) в этом году получил новые ML-модели, обученные на основе экспертизы Positive Technologies в расследовании инцидентов. Интеграция с модулем расширяет возможности системы мониторинга событий ИБ MaxPatrol SIEM за счет поведенческого анализа и сокращает длительность расследований с часов до минут. Обновленный MaxPatrol BAD уже доказал свою эффективность на международной кибербитве Standoff 16. Кроме того, благодаря использованию больших языковых моделей (LLM) нам удалось значительно ускорить наполнение MaxPatrol SIEM экспертизой.

Среди других новшеств — первый proof of concept детекта, позволяющего системе поведенческого анализа сетевого трафика PT Network Attack Discovery (PT NAD) с помощью технологий машинного обучения обнаруживать атаки с использованием VPN на потоке.

Машинное обучение активно используется и в сетевой песочнице PT Sandbox. С помощью новой ML-модели продукт непрерывно выявляет неизвестное и скрытое ВПО по трафику поведенческого анализа, позволяя распознавать вредоносные программы в среднем на две недели раньше, чем они появляются в общедоступных базах. Мы также активно разрабатываем нашу новую технологию статического анализа ВПО на основе нейросетей.

AI-модуль, определяющий сенситивность информации[1], — уникальная особенность единого решения для защиты данных PT Data Security, коммерческий релиз которого состоялся осенью 2025 года. За счет обучения на боевых, а не на синтетических данных была достигнута высокая точность ML-алгоритма. Она позволяет PT Data Security находить любые типы данных, в том числе с высокой энтропией (например, Ф. И. О., название компании, номер телефона), а также фиксировать их расположение в документе. AI-модель показывает 92-процентную точность, что является лучшим результатом среди ведущих решений для бизнеса.

PT Application Firewall использует технологии машинного обучения для проактивной защиты веб-приложений: проверяет загружаемые файлы, обнаруживает web-shell, недоступные для традиционного сигнатурного анализа, и в реальном времени выявляет аномальное поведение запросов с автоматической блокировкой подозрительных IP-адресов.

Модуль поиска уязвимостей класса Malicious Code на базе ML позволяет автоматически выявлять скрытые угрозы, от backdoor и обфускации до утечек данных и атак на цепочку поставок, еще на этапе анализа кода. Используя ML-классификатор и поиск поведенческих паттернов, система сокращает ручное ревью до 40% и помогает предотвратить компрометацию продукта, выявляя вредоносную логику до выхода в прод.

Облачный DAST в PT BlackBox больше не ограничивается сухими отчетами: с функцией How to Fix на базе Positive LLM он сразу объясняет разработчикам, как устранять уязвимости. По нажатию одной кнопки сканер генерирует понятные рекомендации — с объяснением причины, пошаговым планом исправления и примерами кода. Это позволяет командам быстрее переходить от обнаружения проблемы к ее реальному устранению без привлечения специалистов по безопасности.

Мы переосмыслили архитектуру автопилота для результативной кибербезопасности MaxPatrol O2, перенеся его ядро в облако и внедрив AI-агенты на базе развернутой на наших мощностях LLM.

1 Сенситивная (чувствительная) информация — конфиденциальные и потенциально уязвимые данные, требующие особой защиты.

Технологии AI в продуктах Positive Technologies

MaxPatrol O2 (AI\ML)

Агенты проводят авторасследования, закрывая 20–40% инцидентов автоматически

MaxPatrol SIEM

ML-модели детектируют то, что не видят правила. AI-ассистент разбирает сложные процессы, может писать сложные правила за человека

PT Sandbox, Email Security (AI\ML)

Модель анализирует трафик и ловит то, что не видят классические движки

PT NAD

ML-модель детектирует «Телеграм». Пользовательские правила профилирования находят аномалии в трафике

PT Data Security (ML)

Модель находит сенситивные данные с точностью 92%

PT X (AI/ML)

Объединяет все возможности технологий AI/ML, которые есть в продуктах — компонентах PT X

PT Application Inspector

Модуль поиска уязвимостей класса Malicious Code на базе ML позволяет автоматически выявлять скрытые угрозы, от backdoor и обфускации до утечек данных и атак на цепочку поставок еще на этапе анализа кода

PT BlackBox

Облачный DAST в PT BlackBox с функцией How to Fix на базе Positive LLM помогает быстро обнаружить и реально устранить проблемы в коде без привлечения специалистов по безопасности

PT Application Firewall

ML-механизмы защиты проверяют загружаемые файлы и выявляют web-shell, не обнаруживаемые сигнатурным анализом, а модуль ML Anomaly Detection анализирует поведение запросов к ресурсам и автоматически блокирует IP-адреса с аномальной активностью

Трансформация подходов к разработке

В Positive Technologies мы выстроили подход к разработке, который сочетает классические принципы и современные организационные модели. У нас есть так называемый manufacturing — классическая разработка, где команды привязаны к конкретным направлениям и отвечают за создание и развитие технологий, которые находятся в их зоне ответственности.

Внутренние стартапы

Однако за последние годы мы прошли через серьезную трансформацию. Мы решили отказаться от традиционного деления на узконаправленные команды, такие как backend- и frontend-разработка или команды по базам данных. Вместо этого мы перешли к формированию кросс-функциональных команд, собранных вокруг конкретных задач. Такие команды работают по принципу «под ключ» — создают и развивают компоненты, которые включают в себя все аспекты: от уровня backend и хранения данных до уровня взаимодействия с пользователем.

Кросс-функциональные команды действуют как внутренние стартапы. Они не только разрабатывают решения, но и берут на себя ответственность за их дальнейшее развитие. Такой подход позволяет нам быстрее адаптироваться к изменяющимся требованиям рынка, улучшать качество продуктов и внедрять инновации на каждом этапе разработки.

Гибкость как основа прогресса

Сегодня главная цель, которую мы преследуем, — это быть максимально гибкими. Гибкими как с точки зрения организационной структуры, так и с точки зрения того, как мы смотрим на технологии, которым доверяем и в которые верим. Прогресс развивается настолько стремительно, что технологии, которые еще вчера служили нашей опорой, сегодня могут стать ограничением. Поэтому мы стараемся построить модель разработки, где опыт и наследие Компании не препятствуют созданию инноваций.

Баланс между опытом и новаторством

Мы стремимся сохранить баланс между накопленным опытом и свежим взглядом молодых специалистов. Новое поколение разработчиков, свободное от влияния устоявшихся практик, привносит в Компанию инновационные идеи и смелость в принятии решений. Мы создаем среду, где их подходы могут органично сочетаться с опытом наших экспертов, формируя идеальную почву для развития.

Максимальная степень свободы

Помимо классического процесса разработки, в Positive Technologies мы активно инвестируем в посевные проекты, которые, по нашему мнению, обладают большим потенциалом. Эти инициативы дают командам полную свободу действий: они начинают с нуля, выбирают любые технологии и подходы, опираются на те наработки и экспертизу, которым доверяют.

Мы намеренно создаем такую среду, где опыт Компании, накопленный за годы работы, не становится ограничивающим фактором. Наш подход позволяет командам искать новые решения, экспериментировать и находить «ту самую вишенку» — инновации, которые могут определить будущее отрасли.

ИНВЕСТИРУЕМ В ЭКСПЕРТНОСТЬ

Наш исследовательский центр — один из крупнейших в Европе. В нем работают белые хакеры (white hats), исследующие защищенность различных систем, и эксперты по кибербезопасности, которые изучают инциденты и понимают, как реальные преступники наносят компаниям непоправимый ущерб. На их знаниях и опыте строятся наши продукты.

Наши эксперты

- входят в международные экспертные организации OIC-CERT и AVAR, укрепляя глобальные механизмы противодействия киберугрозам;
- расследуют крупнейшие инциденты и киберпреступления в России, обеспечивая оперативное реагирование на критические угрозы;
- обеспечивают безопасность знаковых событий — чемпионатов мира по футболу, президентских и региональных выборов, «Игр Будущего», минимизируя риски кибератак в реальном времени;
- отслеживают киберугрозы по всему миру, выявляя новые хакерские группировки и предотвращая атаки до их массового проявления, чтобы минимизировать риски для бизнеса;
- обнаруживают критические уязвимости в популярных продуктах, таких как Microsoft, предотвращая масштабные эксплуатации и делая цифровую среду безопаснее для миллионов пользователей;
- развивают индустрию кибербезопасности через открытые проекты: наши IDS-правила интегрированы в VirusTotal, any.run и другие платформы, а исследования публикуются в ведущих СМИ и технических изданиях, укрепляя доверие к экосистеме.

Антивирусная лаборатория Positive Technologies[1]

Летом 2025 года Positive Technologies объявила о создании антивирусной лаборатории на базе экспертного центра безопасности (PT Expert Security Center, PT ESC).

Она объединила опыт, технологии и знания трех продуктовых экспертных команд по противодействию ВПО — отделов сетевой экспертизы, песочницы и защиты конечных устройств. За прошедшие шесть месяцев в антивирусной лаборатории сформирован также отдел антивирусной экспертизы, который расширил имеющиеся компетенции по обнаружению ВПО. Помимо поведенческой, сетевой и YARA-экспертизы[2], освоен новый подход по обнаружению зловредного поведения программ на основе уникальной технологии эмуляции.

Среди основных технологических достижений лаборатории за полгода можно выделить следующие:

- увеличение в четыре раза объема и скорости обработки семплов для генерации антивирусных записей;
- увеличение количества записей в антивирусной базе на 25%;
- организацию собственного процесса обновления антивирусной базы и повышение в два раза частоты ее публикации;
- проведение аудита безопасности модуля самозащиты агента MaxPatrol EDR, которое позволило в последнем релизе продукта устранить 27 сценариев компрометации системы защиты;
- расширение сетевой экспертизы коллекцией сигнатур для обнаружения майнеров;
- внедрение (совместно с ML-командой) в PT Sandbox новой модели машинного обучения, предназначенной для выявления трафика ВПО и уже подтвердившей способность выявлять ранее не встречавшиеся угрозы, для которых еще не написаны классические сетевые правила;
- внедрение системы автоматизации анализа сработок сетевых сигнатур для пользователей, использующих преимущества облачного подхода (это позволило свести к минимуму время реагирования на ложные срабатывания в обновлениях экспертизы);
- внедрение бета-версии подсистемы поведенческого анализа Android-приложений в PT Sandbox.

В следующем году нашей приоритетной задачей станет развитие методов обнаружения и блокировки ВПО в продукте класса EPP (платформе для защиты конечных устройств от массовых атак), продажи которого уже начались. Мы также намерены планомерно развивать и масштабировать экспертизу в уже существующих продуктах Positive Technologies.

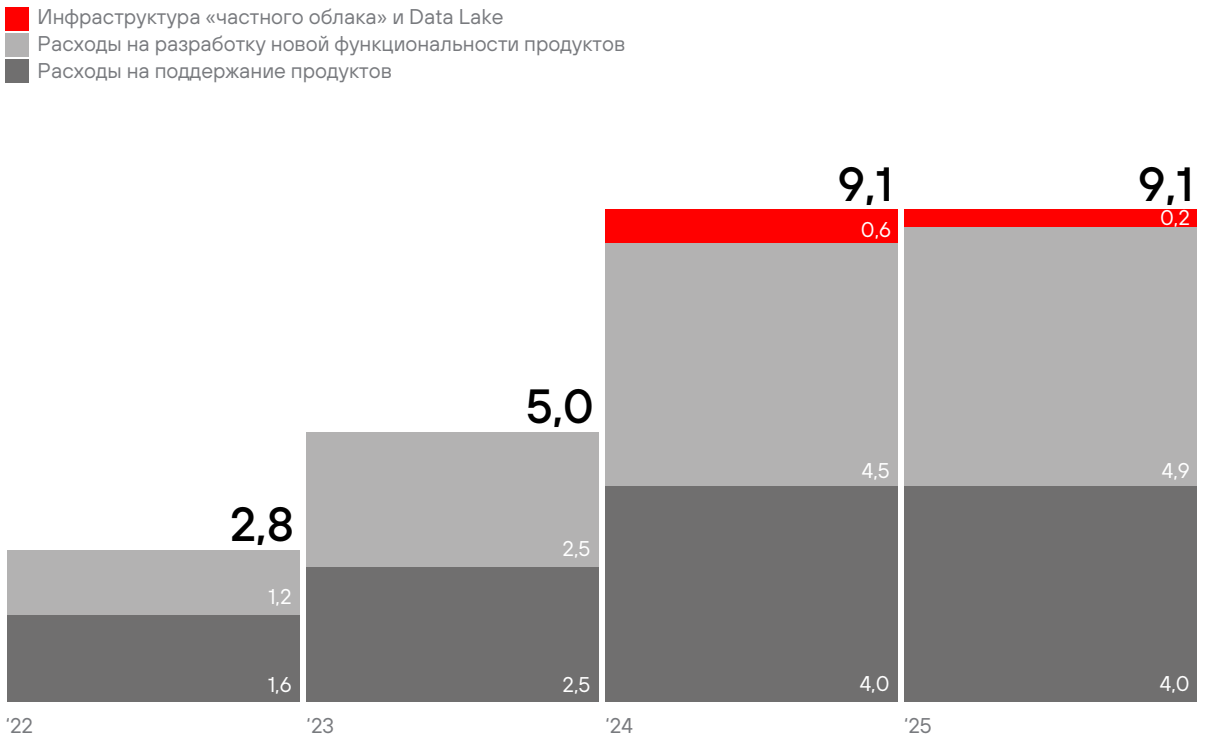
1 Подробнее о результатах работы антивирусной лаборатории Positive Technologies за 2025 год читайте в статье.
2 Описания сигнатур целевых атак и вторжений в ИТ-инфраструктуру организации; YARA-правила используются для распознавания и классификации вредоносных файлов.

Сохраняем инвестиции в R&D

Мы продолжаем инвестировать в исследования разработку (R&D), так как убеждены, что это обеспечит устойчивый рост масштабов бизнеса Positive Technologies в последующие годы. Объем инвестиций в R&D в 2025 году составил 9,1 млрд руб.
Такие инвестиции позволяют нам в полной мере реализовывать стратегические задачи и поддерживать высокие темпы разработки новых продуктов и решений.

Инвестиции в разработку новых продуктов и доработку существующих решений — один из драйверов роста бизнеса Positive Technologies.

Общие расходы на R&D, млрд руб.



НАШИ ПРОДУКТЫ

Чтобы поддерживать темпы роста бизнеса, мы активно инвестируем в разработку новых продуктов. Наши наработки воплощают в себе новейшие технологии, определяя дальнейшее развитие отрасли кибербезопасности. Многие наши продукты уже стали золотым стандартом в своих технологических сегментах и пользуются заслуженным признанием на рынке.

Карта рынка наших продуктов — лидеров в своих сегментах

Security Information & Event Management
MaxPatrol SIEM

Web Application Firewall
PT Application Firewall

Next-Generation Firewall
PT NGFW

Vulnerability Management
MaxPatrol 8 + MaxPatrol VM + XSpider

Network Sandboxing
PT Sandbox

Static Application Security Testing
PT Application Inspector

Network Traffic Analysis/NDR
PT Network Attack Discovery

Endpoint Detection & Response
MaxPatrol EDR

Industrial Security
PT Industrial Security Incident Manager, PT Industrial Cybersecurity Suite

Dynamic Application Security Testing
PT BlackBox

Наши продукты гибкие и могут применяться на популярных операционных системах, таких как Windows, Linux и MacOS, и российских ОС из единого реестра отечественного ПО. Кроме того, они подходят даже для тех операционных систем, которые уже сняты с поддержки, что позволяет использовать их в государственных компаниях, малом и среднем бизнесе.

ПРОДУКТЫ POSITIVE TECHNOLOGIES ЛИДИРУЮТ В КЛЮЧЕВЫХ ИБ-СЕГМЕНТАХ

SIEM
MaxPatrol SIEM

Vulnerability Management
MaxPatrol VM + MaxPatrol 8 + XSpider

Web Application Firewall
PT Application Firewall

Network Traffic Analysis/NDR
PT Network Attack Discovery

Static Application Security Testing
PT Application Inspector

Network Sandboxing
PT Sandbox

Next-Generation Firewall
PT NGFW

Увеличиваем время атаки и сокращаем время реагирования

Увеличиваем время АТАКИ

Продукты помогут проверить инфраструктуру клиента, увидеть лазейки для проникновения и защитить ее, чтобы хакерам было сложно и дорого взламывать.

Сокращаем время РЕАГИРОВАНИЯ

Продукты помогут увидеть аномалии в поведении пользователей, обнаружить хакеров и остановить их, чтобы предотвратить недопустимое событие.

Точка проникновения хакера

Недопустимое событие

Узнать

- Анализ и устранение источников угроз внутри инфраструктуры
- Проверка защищенности с помощью автопентеста

Защитить

- Защита инфраструктуры (сети, конечные устройства, электронная почта)
- Защита приложений

Обнаружить и остановить

- Мониторинг и реагирование на инциденты
- Использование сенсоров и агентов

Знаем, как заранее защититься

Цель — увеличить время реализации кибератаки

Обнаружить и защитить

PT X

Облачное решение для мониторинга и реагирования с гарантией результата

Оценить и усилить защищенность

Анализ и усиление защищенности

MaxPatrol Carbon

Интеллектуальная система управления источниками угроз и анализа киберустойчивости

MaxPatrol VM

Система для управления уязвимостями

MaxPatrol HCC

Модуль комплаенс-контроля

XSpider PRO

Сканер уязвимостей нового поколения

Оценка защищенности

PT Dephaze

Автопентест для оценки уровня защищенности внутренней инфраструктуры

PT Knockin

Онлайн-сервис для оценки защищенности электронной почты

Защитить

Защита инфраструктуры и данных

PT NGFW

Высокопроизводительный и надежный межсетевой экран нового поколения

MaxPatrol EPP

Антивирусная защита конечных устройств

PT Sandbox

Песочница для защиты от целевых атак с использованием ВПО

PT Data Security

Платформа для инвентаризации, автоматизированной классификации и мониторинга данных

PT Email Security

Многоуровневая защита корпоративной почты

Защита приложений

PT Application Inspector

Продукт для эффективного выявления уязвимостей в программном коде приложений и заимствованных компонентах

PT Container Security

Решение для комплексной защиты контейнерных инфраструктур

PT Application Firewall

Высокопроизводительный межсетевой экран для непрерывной защиты веб-приложений и их API

PT BlackBox

Анализатор защищенности веб-приложений, способный выявлять уязвимости без доступа к исходному коду

PT Cloud Application Firewall

Облачная версия продукта для непрерывной защиты веб-приложений

Знаем, как обнаружить и остановить

Цель — снизить время обнаружения и реагирования на инцидент

Обнаружить и защитить

PT X

Облачное решение для мониторинга и реагирования с гарантией результата

Мониторинг и реагирование на инциденты

Технологии для сильного SOC

MaxPatrol O2

Автоматизирует все сложные и рутинные процессы от обнаружения и расследования кибератак до оперативного реагирования на них

MaxPatrol SIEM

Превращает поток событий в список приоритизированных инцидентов с нужным для расследования контекстом

MaxPatrol 360

Единый центр управления расследованиями и операционной работой SOC

Сенсоры и агенты

PT NAD

Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий хакеров в трафике

MaxPatrol EDR

Автономный агент для защиты конечных устройств от сложных и целевых атак

PT Sandbox

Песочница для защиты от целевых атак с использованием ВПО

Мониторинг технологической инфраструктуры

PT ISIM

Система обеспечения киберустойчивости промышленных инфраструктур

Продукты для анализа и усиления защищенности инфраструктуры

Каждая компания проходит последовательный путь к зрелой кибербезопасности. Этот путь неизменно начинается с базового, но стратегически важного вопроса: где находятся ключевые уязвимости инфраструктуры?

Эволюция управления киберугрозами: от поиска уязвимостей до моделирования кибератак и анализа киберустойчивости

XSpider PRO → MaxPatrol VM → MaxPatrol Carbon

Этап 1

Базовый уровень — сканирование уязвимостей

На начальном этапе рынок традиционно опирается на инструменты класса vulnerability scanner. Решения уровня XSpider (эволюционировавшего в 2025 году в XSpider PRO) закрывают потребности компаний с инфраструктурой до 500 хостов, обеспечивая базовую видимость уязвимостей.

Сканер имеет два режима анализа (black box и white box), актуальную базу экспертизы и низкие аппаратные требования. Основной сценарий использования продукта — запуск сканирования и выпуск отчета с выявленными уязвимостями.

Данная модель эффективна на ранних этапах цифрового развития, однако ее ограничения становятся очевидны по мере роста инфраструктуры и усложнения ИТ-ландшафта. В этот момент простого сканирования недостаточно, ведь важно не просто обнаружить уязвимости, а выстроить процесс по их устранению.

Этап 2

Переход к зрелости — Risk-Based Vulnerability Management

С увеличением масштаба бизнеса возникает необходимость учитывать контекст риска. Компании переходят от количественного подхода к качественной оценке угроз.

Решения класса Risk-Based VM, такие как MaxPatrol VM с модулем MaxPatrol HCC, помогают выстраивать полноценный процесс управления в компаниях enterprise-сегмента, даже на инфраструктуре свыше 100 тыс. активов. К ключевым возможностям продуктов этого класса относится управление жизненным циклом уязвимостей, контроль соответствия требованиям безопасности, харденинг и внедрение процессов устранения уязвимостей с понятными SLA.

Приоритизация смещается в сторону рискориентированного подхода: учитываются критичность активов, актуальные угрозы и регуляторные методики (в том числе ФСТЭК).

Несмотря на кажущуюся завершенность модели, именно на этом этапе большинство организаций сталкиваются с ее фундаментальными ограничениями. Учет даже самых критичных уязвимостей и активов не всегда гарантирует, что хакер не сможет получить доступ к целевым системам. Учитывать полный спектр угроз, которые могут стать лазейкой на пути хакера помогает следующий класс решений — Exposure Management.

Этап 3

Смена парадигмы — Exposure Management

Следующий этап развития связан не с эволюцией инструментов, а с переосмыслением самой модели защиты.

Современные атаки строятся не вокруг отдельных уязвимостей, а вокруг цепочек: комбинаций уязвимостей, ошибок конфигурации, компрометированных учетных записей и особенностей сетевой архитектуры. В этих условиях классические подходы теряют эффективность.

Exposure Management отвечает на этот вызов, смещая фокус с вопроса «что уязвимо?» на «какие пути атаки реально достижимы для злоумышленника?».

MaxPatrol Carbon представляет собой мета-уровень управления киберугрозами:

- управление полной поверхностью атаки,
- моделирование и анализ потенциальных путей атак,
- приоритизация мер защиты на основе реального бизнес-риска,
- проактивная оценка киберустойчивости до реализации инцидента.

Результатом становится качественное изменение уровня киберустойчивости: организация не становится «абсолютно защищенной» — это недостижимая цель, — но становится экономически и технически невыгодной целью для атакующих.

Переход к Exposure Management является неизбежным этапом развития рынка. Ключевой вопрос для организаций — не «произойдет ли этот переход», а «успеют ли они реализовать его до наступления недопустимых событий».

Positive Technologies занимает уникальную позицию на российском рынке как единственный вендор, предлагающий полнофункциональное решение класса Exposure Management — MaxPatrol Carbon, основанное на собственной технологии моделирования путей атак.

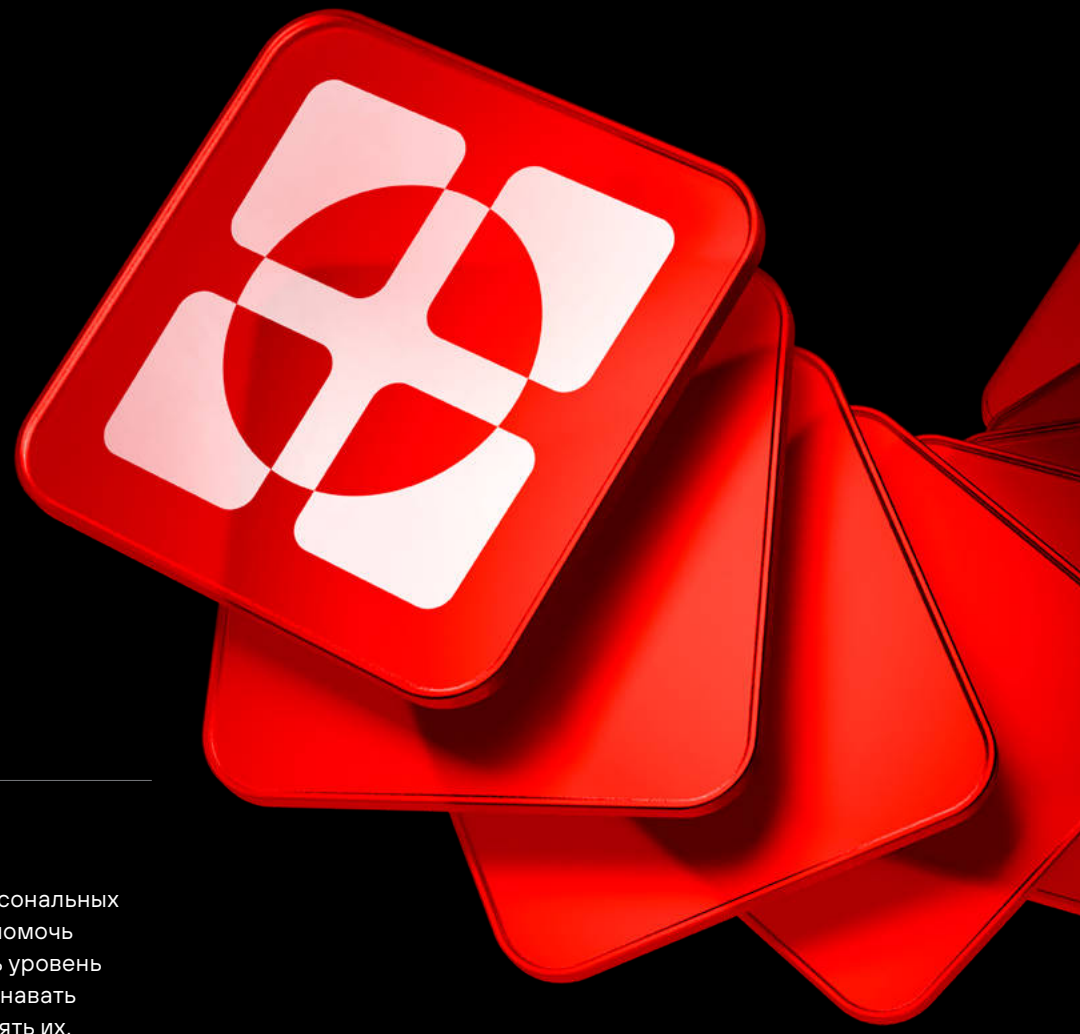
Концепция «делать меньше — защищать больше» отражает трансформацию проактивного подхода к кибербезопасности и формирует новую норму эффективности для отрасли.

2,8 млрд долл. США

оценка глобального рынка Exposure Management при среднегодовом темпе роста 8,1%, что отражает структурный сдвиг в превентивных подходах к кибербезопасности

Выявление уязвимостей, слабых мест в инфраструктуре

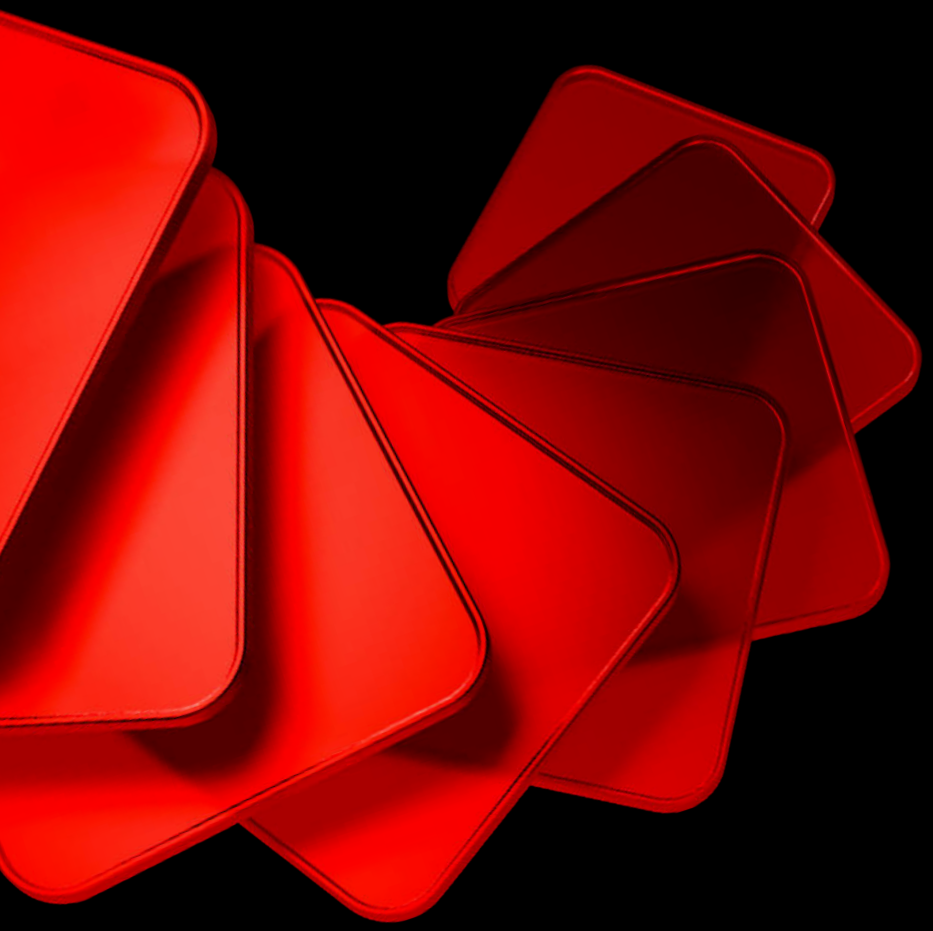
XSpider PRO



Сканер уязвимостей нового поколения с двумя режимами сканирования: черный и белый ящик. Продукт для компаний с небольшой инфраструктурой, ориентирован на рынок SMB.

АКТУАЛЬНОСТЬ И ПРЕДПОСЫЛКИ РАЗРАБОТКИ

Эксплуатация уязвимостей остается одним из основных методов атак злоумышленников. В 53% атак использование недостатков безопасности приводит к утечкам конфиденциальной информации — персональных данных (29%), учетных данных (26%), коммерческой тайны (20%). При этом в силу вступил Федеральный закон от 30 ноября 2024 года № 420-ФЗ, который определил оборотные штрафы за утечку персональных данных — до 500 млн руб. Чтобы помочь российским компаниям повысить уровень своей защищенности, вовремя узнавать об опасных уязвимостях и устранять их, Positive Technologies создала сканер нового поколения, который показывает полную картину уязвимостей в инфраструктуре.



ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

XSpider PRO находит бреши в сетях и системах и дает рекомендации по их устранению. Продукт имеет низкие аппаратные требования, что позволяет эффективно внедрять его в любую инфраструктуру без затрат на дополнительные серверные мощности.

Команда XSpider PRO сделала упор на экспертизу. Сканер нового поколения включает обширную базу уязвимостей, основанную на сведениях из БДУ ФСТЭК, CVE, OWASP Top 10, а также собственной базы Positive Technologies. Благодаря актуальной экспертизе XSpider PRO с высокой точностью выявляет уязвимости в инфраструктуре.

Продукт также полностью адаптирован для работы на Astra Linux, что отвечает запросу отечественных компаний и позволяет внедрять его в любую импортозамещенную инфраструктуру.

ТОЧКИ РОСТА

- Рост в сегменте SMB клиентов в России путем замены продукта MaxPatrol 8 и XSpider, а также ростом новых клиентов с начальным уровнем кибербезопасности.
- Новые клиенты в сегменте LE, для которых XSpider PRO станет дополнительным инструментом обеспечения безопасности отдельных сценариев.

Выявление уязвимостей, слабых мест в инфраструктуре

MaxPatrol VM

Система управления уязвимостями с доставкой информации о трендовых уязвимостях за 12 часов.

Делает инфраструктуру труднодоступной для хакера, строит процесс управления уязвимостями, помогает соответствовать требованиям ИБ.

Positive Technologies вошла в топ-7 вендоров в отчете IDC по мировому рынку средств управления уязвимостями и киберугрозами по итогам 2024 года (Worldwide Device Vulnerability and Exposure Management Market Shares, 2024).

76% +5,11% год к году

доля MaxPatrol VM в сегменте Vulnerability management / управление уязвимостями[1]

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса VM в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- Экспертиза продукта. Высокое качество детектов уязвимостей, доставка информации о трендовых уязвимостях в продукт за 12 часов.
- Стабильная работа продукта даже на больших инсталляциях.
- Запатентованная технология инвентаризации активов.

ИТОГИ 2025 ГОДА

В 2025 году мы сосредоточились на увеличении производительности и стабильности работы продукта.

- **Продукт стал быстрее:** расчет уязвимостей ускорился в два раза, отображение информации в интерфейсе — в семь раз. Поиск по PDQL стал как минимум в пять раз быстрее. В модуле MaxPatrol HCC проверка активов на соответствие стандартам безопасности стала более чем в 10 раз быстрее. Оптимизированные настройки позволяют системе производить сбор данных с активов на 30–40% быстрее. Благодаря этому специалисты по ИБ могут быстрее реагировать на угрозы и, как следствие, быстрее передать эту информацию ИТ-специалистам для закрытия недостатков безопасности.
- За счет оптимизации архитектуры система стабильно работает у клиентов с крупными инфраструктурами.
- Команда MaxPatrol VM также повысила качество детектов. MaxPatrol VM 2.10 в три раза точнее обнаруживает недостатки безопасности за счет пересмотра уже существующих детектов и использования современных методологий.
- Обновлена и улучшена функциональность проверки безопасности паролей.
- Улучшен модуль комплаенс-контроля и харденинга инфраструктуры MaxPatrol HCC. Этот модуль проверяет ИТ-инфраструктуру на соответствие стандартам кибербезопасности, что позволяет пользователям соблюдать требования приказа ФСТЭК России № 117. В MaxPatrol HCC был добавлен графический конструктор для создания собственных стандартов и требований. Пользователи могут использовать встроенный шаблон и редактировать в нем параметры или самостоятельно создавать стандарты и требования с нуля под собственную инфраструктуру и регламенты.

ТОЧКИ РОСТА

- Фокус на улучшение пользовательского опыта и ускоренного достижения ценности (time to value) через технологические инновации:
  - ML/AI как для расширения сценариев использования, так и для развития экспертного блока (скорость и качество экспертизы по уязвимостям в продукте);
  - развитие и улучшение существующих технологий для расширения пользовательских сценариев.

Выявление уязвимостей, слабых мест в инфраструктуре

MaxPatrol Carbon

Интеллектуальная система управления источниками угроз и анализа киберустойчивости

MaxPatrol Carbon — это метапродукт, который анализирует инфраструктуру с точки зрения злоумышленника, моделируя пути компрометации критически важных активов, и помогает своевременно устранять наиболее опасные источники угроз для проактивного повышения киберустойчивости компании.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- Представляет собой уникальное для российского рынка решение класса Threat Exposure Management — следующего этапа развития Vulnerability Management, направленного на повышение защищенности компании за счет превентивного анализа полной поверхности атаки, в соответствии с подходами Gartner и IDC.

- Управляет потенциальной площадью атаки, в том числе анализирует уязвимости, ошибки конфигурации, избыточные права, сетевой доступ и другие недостатки инфраструктуры с учетом их опасности для бизнеса.
- Включает в себя уникальную технологию моделирования угроз PT Threat Modeling Engine, которая позволяет прогнозировать потенциальные пути атак и выявлять наиболее опасные источники угроз.
- Непрерывно анализирует уровень защищенности компании от реализации атак разного уровня сложности.
- Повышает эффективность ИТ и ИБ: показывает, как выполнение мер усиления защиты сокращает количество и повышает сложность потенциальных путей атакующих, что позволяет экономить ресурсы ИБ и ИТ, концентрируясь на наиболее значимых задачах.
- Преобразует стратегию киберустойчивости в конкретные шаги по ее достижению, для того чтобы сделать компанию слишком сложной и дорогой целью для хакеров.

ИТОГИ 2025 ГОДА

С момента коммерческого запуска MaxPatrol Carbon продемонстрировал устойчивое технологическое развитие и подтвердил эффективность проактивного подхода к выявлению путей возможных атак в инфраструктуре и управлению на их основе всеми источниками угроз, а не только уязвимостями, на 10 проектах внедрений.

Первые внедрения на инфраструктурах разного масштаба подтвердили, что продукт позволяет снижать трудозатраты команд ИБ и ИТ на более чем 80% за счет точной приоритизации задач и фокусирования на устранении 1–3% наиболее критичных недостатков, напрямую влияющих на киберустойчивость компании.

ТЕХНОЛОГИИ И ЭКСПЕРТИЗА

- Существенно расширены сценарии атак: в два раза увеличено количество учитываемых атакующих действий для расширения вариативности сценариев атак.
- Добавлены новые рекомендации: по исправлению ошибок конфигураций, настройке политик сетевого доступа, общим инфраструктурным настройкам, журналированию событий безопасности и контролю привилегий пользователей.

Полностью переработан алгоритм оценки опасности потенциальных маршрутов атак, что помогает фокусироваться на наиболее опасных сценариях.

МАСШТАБИРУЕМОСТЬ И РАБОТА С КРУПНЫМИ ИНФРАСТРУКТУРАМИ

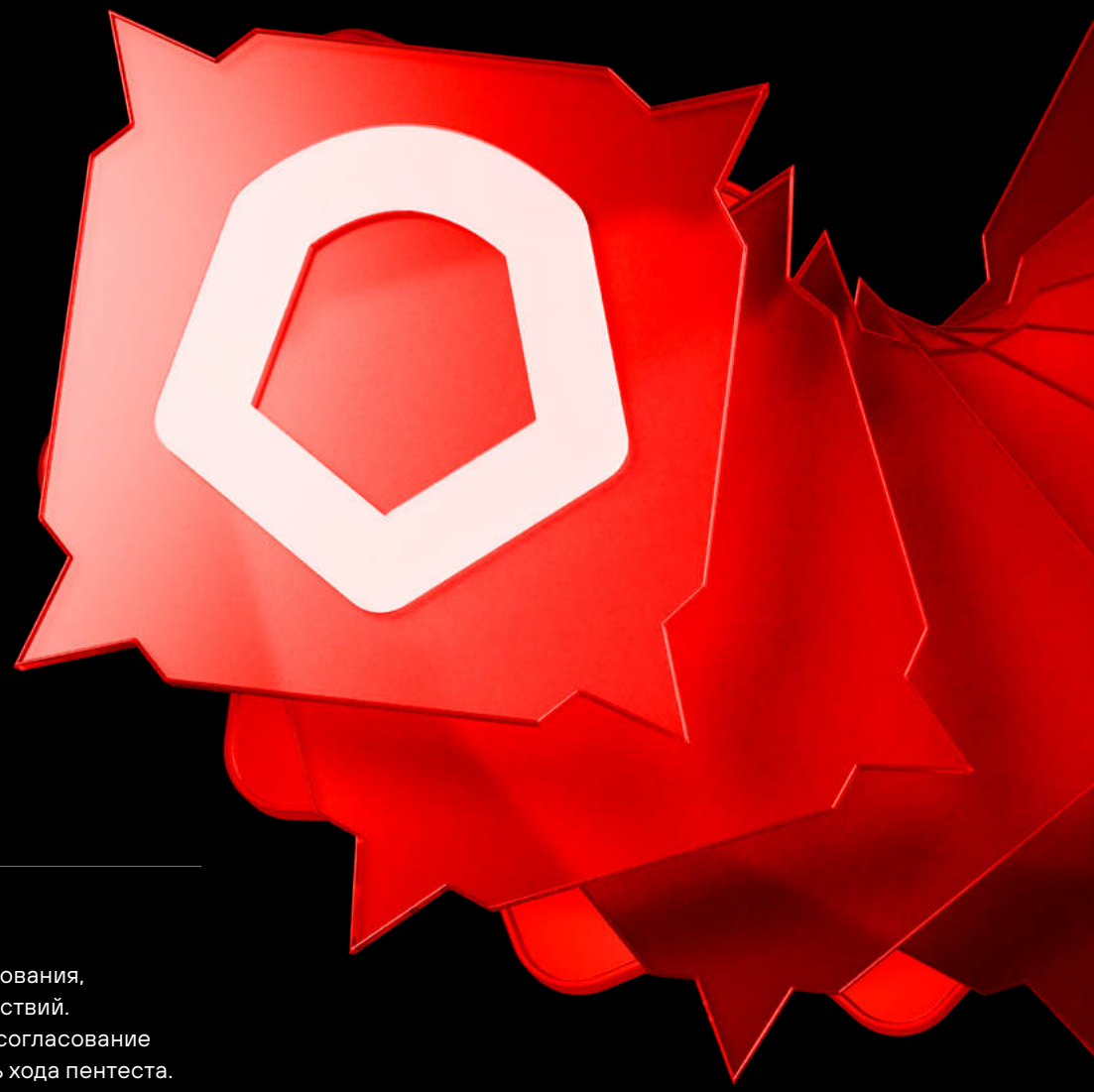
- Поддерживается работа с крупными инфраструктурами >20 тыс. активов.
- Расширена поддержка сетевых устройств, популярных на рынке Российской Федерации, и разработан новый движок топологии, обеспечивающий более быстрое и точное построение карты сети и расчет достижимости.

АНАЛИТИКА, СЦЕНАРИИ И ОТЧЕТНОСТЬ

- Реализовано автоматическое формирование наиболее популярных сценариев реализации недопустимых событий, что упрощает работу специалистов по ИБ.
- Улучшена визуализация: добавлена подробная визуализация каждого маршрута, позволяющая наглядно показать путь злоумышленника до критического актива.
- Отчеты: в разделе статистики появилась возможность сформировать отчет по объему выполненных рекомендаций и их влиянию на количество маршрутов атак.
- Дашборды и виджеты: добавлены страницы с виджетами по готовности инфраструктуры к эффективному использованию системы и основным метрикам киберустойчивости.

Выявление уязвимостей, слабых мест в инфраструктуре

PT Dephaze

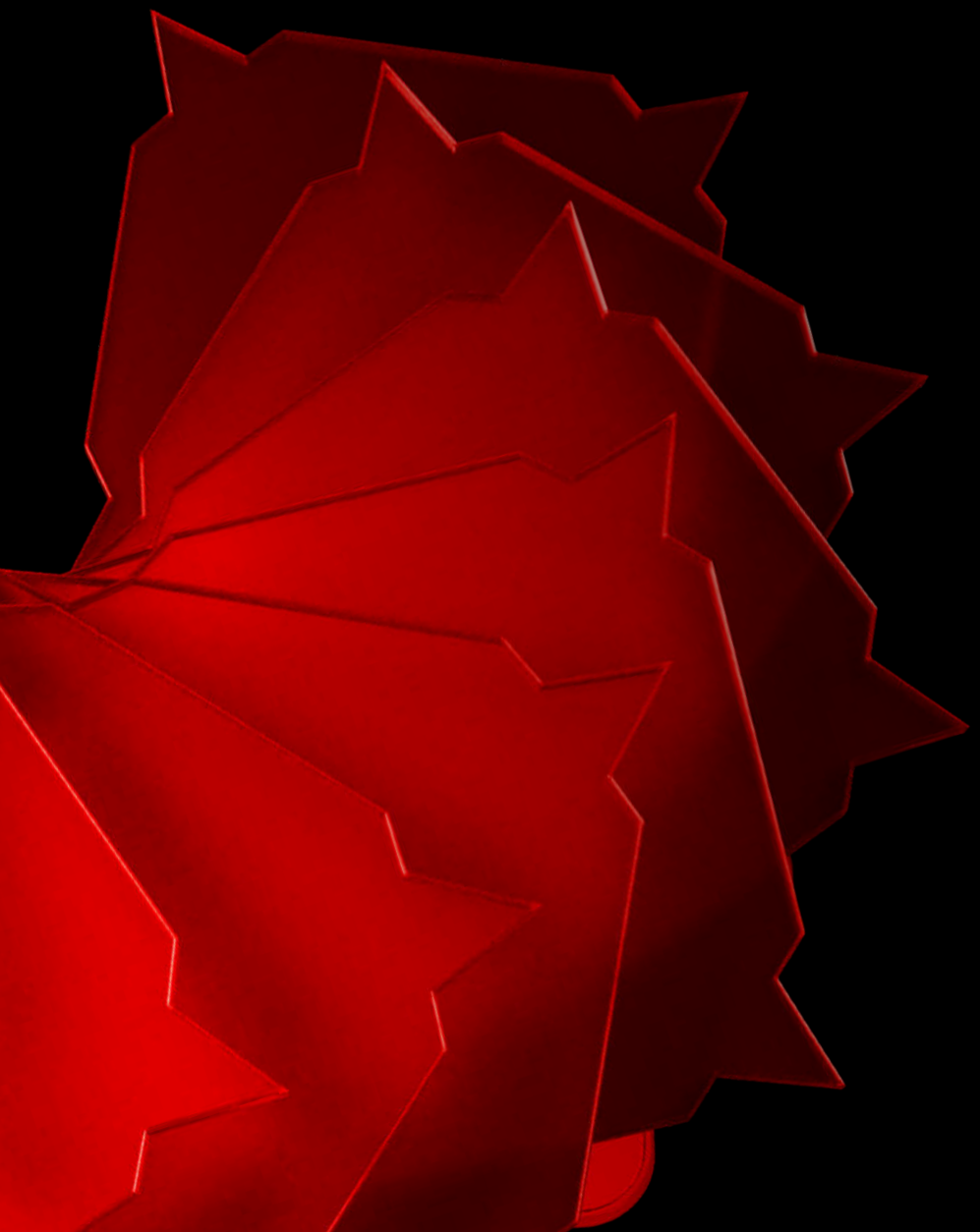


Автопентест для оценки уровня защищенности внутренней инфраструктуры.

PT Dephaze поможет перейти от разовых проверок к непрерывной оценке защищенности. Система действует как реальный хакер: проводит разведку, выявляет уязвимости, эксплуатирует их в конкретном окружении и оценивает эффективность средств защиты. Вы получаете объективную картину состояния инфраструктуры в условиях, максимально приближенных к боевым.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Автоматизация:** не требует постоянного участия экспертов.
- **Реалистичность цепочек атак:** максимальная за счет экспертизы ESC и Red Team PT.
- **Масштабируемость:** охват всей инфраструктуры, включая территориально распределенные сегменты.
- **Гибкость:** настройка тестирования, исключений, атакующих действий.
- **Контроль и безопасность:** согласование действий, полная видимость хода пентеста.
- **Информативность:** отчеты показывают реальные пути компрометации и слабые места в защите.



БИЗНЕС-ОБОСНОВАНИЕ

Пентест остается единственным корректным способом оценить реальную защищенность организации. При этом сам рынок в классическом понимании выглядит ограниченным, поэтому фокус был сделан не на его объеме, а на роли пентеста как ключевой точки входа.
PT Dephaze задумывался как открывающий продукт в логике «пентест → продукты» и инструмент, который масштабирует завоевание заказчиков.

ИТОГИ 2025 ГОДА

- 27 февраля 2025 года вышел коммерческий релиз.
- 60+ пилотных проектов за год и и 150+ заявок на проведение к текущему моменту.
- В октябре 2025 года вышел релиз версии 2025.3.0.
- Полностью безопасная эксплуатация продукта — от настроек для атак до полного согласования любых действий.
- Прозрачность при пентесте — детализация всех атакующих действий, их данных, времени выполнения.
- Добавлено более 70 атак для типового ландшафта инфраструктуры российских организаций.
- Полноценное моделирование атак на Active Directory — от первоначального доступа до полного компрометирования домена, включая эксплуатацию уязвимостей в PKI.
- Поддержка различных сред — проверка защищенности не только Windows-, но и Linux-инфраструктур.
- Тестирование критически важных приложений — GitLab, Veeam, FTP и СУБД (PostgreSQL, MS SQL) на наличие слабых конфигураций и возможностей удаленного выполнения кода.

Продукты для защиты инфраструктуры и данных

PT NGFW

Межсетевой экран нового поколения. Продукт относится сразу к двум нишам: это и средство защиты, так как обеспечивает безопасность периметра компании от внешних угроз, и ИТ-решение, от которого зависит доступность интернета для корпоративных пользователей и скорость доступа к внешним ресурсам. Ключевые особенности PT NGFW — высокая производительность, стабильность и надежность.

По оценке Центра стратегических разработок, рынок NGFW составит

146,3 млрд руб.

к 2030 году. Positive Technologies планирует занять **не менее половины** этого рынка

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Линейка ПАК PT NGFW включает 10 моделей: решения как для небольших филиалов, так и для центров обработки данных.
- Самый производительный российский межсетевой экран благодаря модернизированному стеку TCP/IP и собственным алгоритмам модулей безопасности (IPS, DPI, антивирус и более чем 10 тыс. сигнатур от PT Expert Security Center)
- Понятный и отзывчивый веб-интерфейс и открытый API.
- Собственный протокол отказоустойчивости, позволяющий реализовать переключения в случае аварии менее чем за 300мс. Это гарантирует стабильную работу сервисов в высоконагруженных сетях.
- Поддержка до 100 тыс. правил безопасности на одно устройство.

ГЛАВНЫЕ ДОСТИЖЕНИЯ 2025 ГОДА

- Первый российский межсетевой экран нового поколения, сертифицированный согласно новым требованиям ФСТЭК России к многофункциональным межсетевым экранам уровня сети по 4 классу защиты (сертификат ФСТЭК № 4877 от 19 ноября 2024 года, переоформлен 22 декабря 2025 года).
- Получили сертификат ФСТЭК России на межсетевой экран типа «Д» и запустили разработку промышленной NGFWплатформы. Это позволит выйти на новый для PT NGFW рынок — защиты АСУ ТП.
- PT NGFW выбрали для защиты своей инфраструктуры не только субъекты КИИ (крупные финансовые организации, банки, муниципальные органы госуправления и другие), но и коммерческие компании, чей выбор традиционно шире, так как не ограничен только российскими решениями.
- PT NGFW получил первые публичные истории успеха с Rambler&Co, одним из крупнейших медиахолдингов России, финтех-сервисом JoyMoney, крупным дальневосточным банком.
- ПАК PT NGFW внесен в единый реестр российских программ для электронных вычислительных машин и баз данных Минцифры России и единый реестр российской радиоэлектронной промышленности Минпромторга России.
- Рекордный функциональный прирост. За год реализовано более 100 новых функций, востребованных рынком, в том числе: S2S VPN, BFD, BGP Community, ICAP, CLI, DHCP relay и другие. Новая функциональная версия ПО выходит каждые два месяца.
- PT NGFW прошел сертификацию в Оперативно-аналитическом центре при Президенте Республики Беларусь, а также получил сертификат соответствия требованиям технического регламента Республики Беларусь «Средства электросвязи. Безопасность».
- Вышли на рынок СНГ: Беларусь, Армения, Азербайджан. Провели первые отгрузки заказчикам из Беларуси.
- PT NGFW — крупнейшая отгрузка Positive Technologies на международном рынке. Наша платформа стала одним из ключевых элементов защиты критической информационной инфраструктуры в сетях стран Юго-Восточной Азии. Кроме того, работаем над выходом нарынки стран Латинской Америки.
- Количество партнеров и дистрибьюторов с собственным демофондом PT NGFW достигло 48 компаний, которые инвестировали более 80 млн руб.
- Стабильно выдерживаем кратчайшие сроки отгрузки ПАК — менее чем за две недели с момента размещения заказа.
- Расширили партнерскую сеть. У PT NGFW появилось восемь авторизованных сервисных центров, которые прошли подготовку, могут оказывать полную техническую поддержку и предоставлять персонализированные услуги гарантированно высокого качества по всей России.

ТАКЖЕ В 2025 ГОДУ:

- создали комьюнити вокруг продукта PT NGFW;
- провели серию технических онлайн-марафонов «PT NGFW: исповедь инженеров», количество участников которой превысило 1 тыс. человек;
- продолжили рассказывать о внутренней кухне разработки в реалити-проекте «PT NGFW за стеклом»;
- провели открытое тестирования PT NGFW модели 2010 в лаборатории «Инфосистемы Джет» и показали лучшие результаты производительности;
- активно сотрудничаем с ведущими сетевыми сообществами Linkmeup, GetNet;
- выпустили обучающие курсы на базе собственной платформы и в учебных центрах;
- продолжили проводить регулярные семинары для заказчиков и партнеров;
- поддерживаем программу try & buy, позволяющую выкупить оборудование только после успешной опытной эксплуатации.

›x2
рост продаж

250
внедрений за год

1 тыс.
устройств продано

Endpoint Security

Концепция полной защиты конечных устройств. Представлена в виде двух продуктов — MaxPatrol EPP и MaxPatrol EDR.

Клиенты могут планомерно использовать базовую защиту и усиливать ее по мере необходимости, защищаясь и от массовых атак, и от продвинутых хакеров. Такая комбинация делает Positive Technologies более конкурентной, в том числе и на международном рынке.

ТОЧКИ РОСТА

- В 2026 году Компания предлагает клиентам комплексное предложение для всесторонней защиты устройства, а не отдельные продукты. Клиенты смогут начать с базовой защиты и усилить ее для противодействия сложным атакам.
- На текущий момент мы становимся вторым вендором, который способен предоставить мощную связку решений EPP + EDR.
- Это рыночная тенденция, являющаяся де-факто стандартом в западных решениях, которые ранее привыкли использовать в том числе и наши клиенты.
- 5% — минимальный целевой ориентир Компании по доле на российском рынке. Мы также продолжаем наращивать свое присутствие на международном рынке, конкурируя с крупнейшими игроками индустрии кибербезопасности, включая традиционных поставщиков антивирусного ПО.

MaxPatrol EPP

Система комплексной защиты устройств от массового ВПО, вирусов и программ-шифровальщиков. Решение формирует фундаментальный уровень киберустойчивости организации, обеспечивая безопасную среду для цифровой трансформации бизнеса. В современных реалиях наличие EPP является необходимым стандартом технологической гигиены и обязательным условием непрерывности бизнес-процессов.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- Антивирус способен обнаруживать замаскированные угрозы, целые семейства ВПО по их поведению, а не отдельные экземпляры.
- Продукт не ограничивается антивирусом: помимо простого удаления зловредных файлов, предусмотрены дополнительные действия, реализующие сценарии защиты от вирусов-шифровальщиков и вайперов (ПО для уничтожения данных).
- MaxPatrol EPP тесно взаимодействует с ранее выпущенным на рынок продуктом класса EDR (MaxPatrol EDR). Концепция единого предложения избавляет клиентов от необходимости устанавливать несколько программных компонент (агентов) на свои устройства. Такой подход снижает нагрузку на устройства, минимизирует возможные конфликты и упрощает эксплуатацию.

БИЗНЕС-ОБОСНОВАНИЕ

- Рынок продуктов для защиты конечных устройств в России составляет, по разным оценкам, около 30 млрд руб. Сегмент включает антивирусы и более функциональные корпоративные решения (EDR). Если ранее Positive Technologies работала в основном в сегменте продвинутых решений против APT, то теперь Компания может предлагать комплексное решение.
- Компания планирует занять долю не менее 5% этого рынка.
- У ряда клиентов антивирусный контур закрывают конкурентные продукты. Единое предложение Positive Technologies позволит таким заказчикам использовать единый агент и снизить капитальные и операционные затраты как ИБ-, так и ИТ-команд.
- Совместное предложение EDR + EPP повышает потенциал увеличения среднего чека Positive Technologies. В проектах, где клиенты выбирают MaxPatrol EDR, Компания сможет дополнить контур комплексным решением MaxPatrol EPP.
- Продукт хорошо включается в подход Positive Technologies к РКБ. В комплексных проектах удастся закрывать больше векторов атак и не зависеть от сторонних решений в инфраструктуре заказчика.

ИТОГИ 2025 ГОДА

- Приобрели технологию белорусской компании «ВИРУСБЛОКАДА». Вместо трех-четырех лет разработки с нуля интегрировали наработки и усилили их многолетним опытом Positive Technologies в защите крупных российских компаний.
- Международное присутствие позволило также обогатить продукт экспертизой по отражению зарубежных группировок.
- На 25% увеличили базу антивирусных сигнатур после приобретения технологии.
- Получили первые продажи, продукт показал себя на играх Standoff 16. Используем продукт во внутреннем контуре. При развернутом MaxPatrol EDR антивирусную функциональность получили на тех же агентах. Аналогичный сценарий доступен и нашим клиентам.
- Приобретение доли «ВИРУСБЛОКАДЫ» стало первой M&A-сделкой Positive Technologies. Интеграцию провели оперативно, в составе единой команды и без сбоев, не прерывая выпуск обновлений.

ТОЧКИ РОСТА

- Соответствие требованиям регуляторов в России и Беларуси — сертификация САВЗ — снимает барьер для продаж в Enterprise. Особенно важно для финансового сектора, где есть требование двух независимых сертифицированных антивирусов.
- Усиливаем возможности превентивной защиты. Это и паритет по сравнению с конкурентами, и значимый шаг к РКБ — снижаем поверхность атаки у клиентов, популярные методы проникновения не сработают.
- Международный рынок — конкуренция с мировыми лидерами и OEM.
- Увеличение клиентской базы — продажи в «юбки» холдингов, где тяжелые экспертные решения недоступны.
- Многие наши клиенты именно для антивирусной защиты применяют продукты конкурентов. Предложение от Positive Technologies позволит таким клиентам использовать наш единый агент — это заметное снижение капитальных и операционных затрат как ИБ-, так и ИТ-команд. Совместное предложение = увеличение среднего чека.

MaxPatrol EDR

Защищает компьютеры, серверы и виртуализированные рабочие места от сложных кибератак. Это инструмент для компаний с высокой зрелостью ИБ, которые учитывают риск атак не только массовых вирусов и ВПО, но и со стороны продвинутых злоумышленников и организованных группировок.

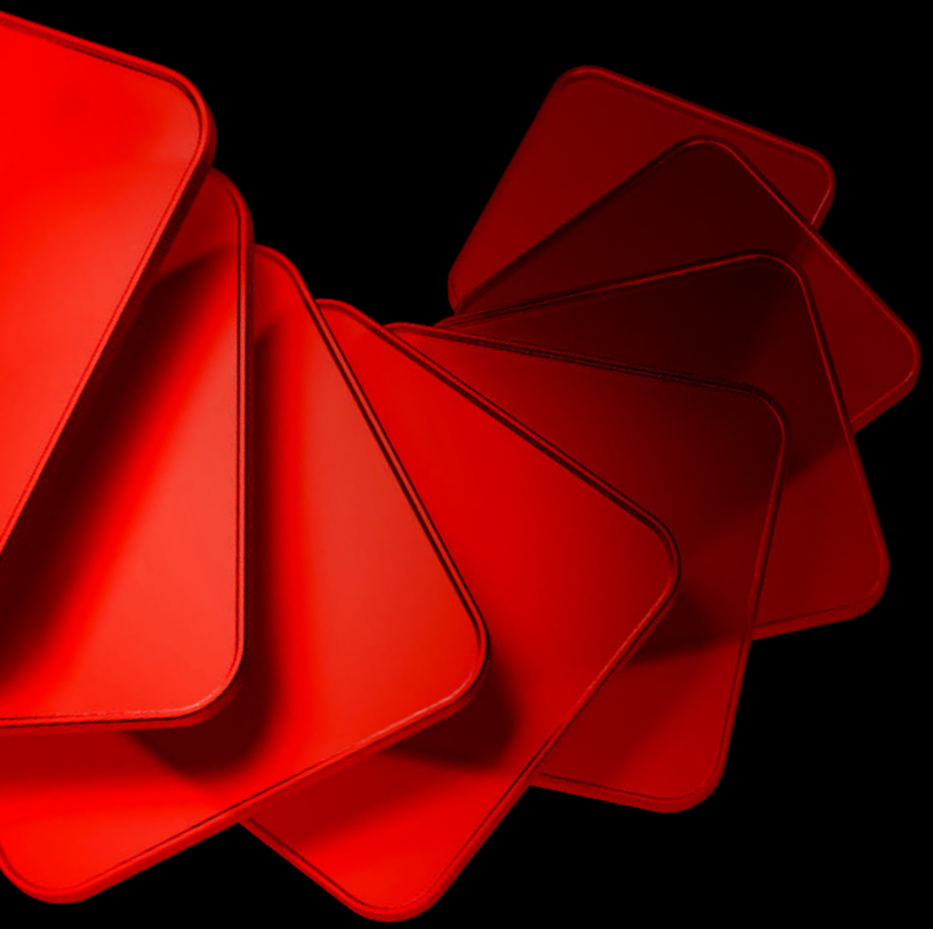
22%

доля MaxPatrol EDR в сегменте Endpoint Detection & Response / обнаружение и реагирование на конечных устройствах[1]

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- Поддержка более 30 ОС, что особенно важно в условиях импортозамещения и использования различных отечественных ОС у крупных корпоративных клиентов и государственных организаций.
- Самый широкий выбор действий реагирования на киберугрозы по сравнению с конкурентами. Это важно для специалистов SOC: решение закрывает задачи разной сложности и помогает снижать операционные затраты.
- Автономная работа. Защита сохраняется, когда устройства не в сети, сотрудники находятся в командировках или работают удаленно без постоянного подключения к корпоративной сети.

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса EDR в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).



ИТОГИ 2025 ГОДА

- Очень крупные внедрения продукта, в том числе проекты масштаба 80+ серверов управления и 40 тыс. защищаемых устройств.
- Суммарное количество защищаемых устройств превысило 155 тыс.
- MaxPatrol EDR стал одним из ключевых элементов облачного решения PT X, которое обеспечивает быстрый старт и легкое развертывание защиты у клиентов.
- Единый агент — это ключевой поставщик данных для Security Data Lake, обеспечивающий движение к облачным и гибридным технологиям защиты будущего.

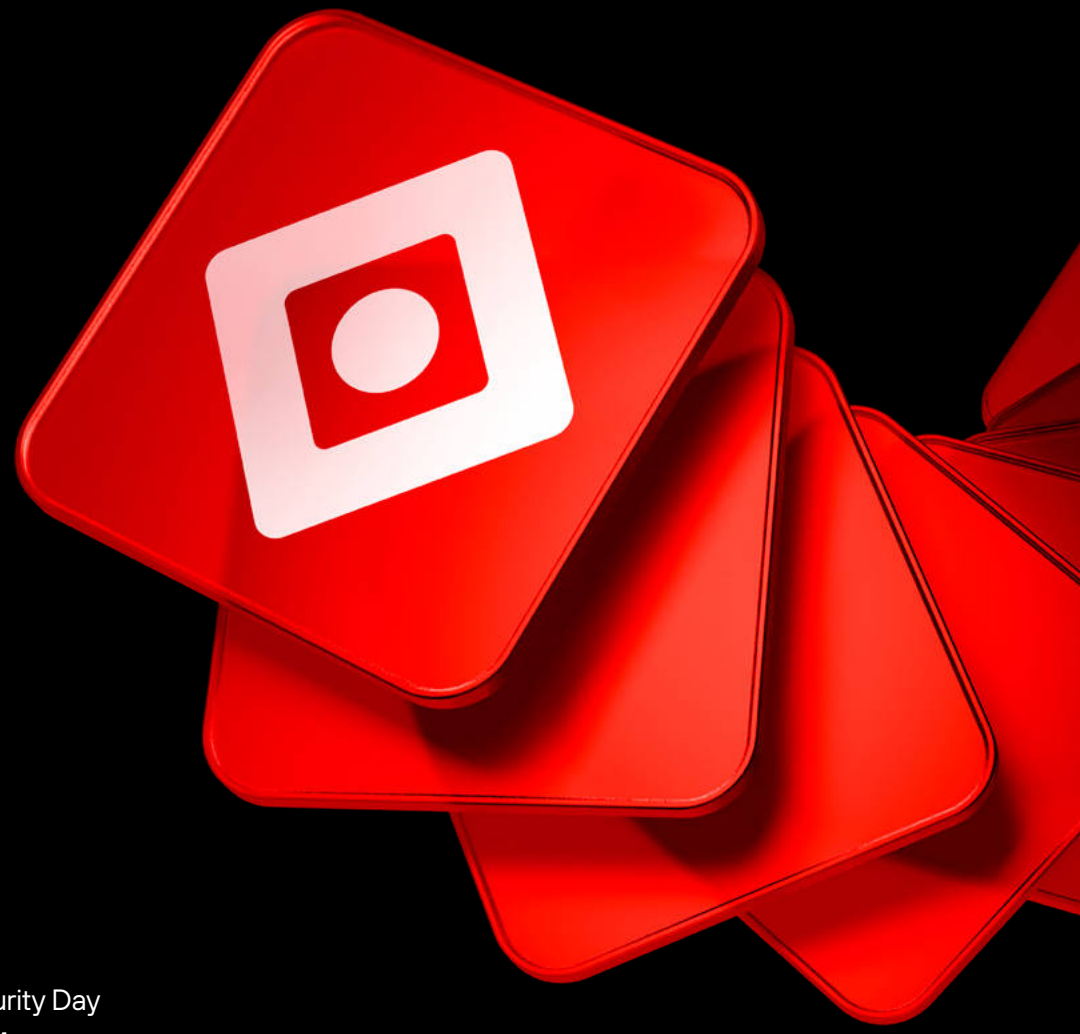
›155 тыс.

суммарное количество защищаемых устройств

ТОЧКИ РОСТА

- Рынок EDR-решений России — около 4 млрд руб. (экспертная оценка). В 2025 году мы заняли на нем 22% и показываем рост в 2,5 раза год к году.
- Соответствие требованиям нового класса защитных решений от ФСТЭК — СОР. Мы одними из первых выполнили сертификационные требования. Это важно клиентам для соблюдения требований приказа ФСТЭК № 117 (требования к защите информации для ГИС и ИС госсектора).
- Важно снижать операционные затраты на установку и настройку продукта — такую функциональность развиваем в 2026 году еще больше. В конечном итоге клиент получит установку и ввод продукта в эксплуатацию за один день.
- Ультимативная защита — хакеры, привыкшие обходить антивирусы и другие средства защиты, не смогут это сделать в случае MaxPatrol EDR, защита работает всегда. Продукт уже на Bug Bounty, и проверить его защищенность могут исследователи со всего мира.

PT Email Security



Продукт для многоуровневой защиты корпоративной почты. В его основе песочница PT Sandbox, а также функциональность почтового шлюза для защиты от спама, фишинга и других массовых угроз. Коммерческий релиз запланирован на апрель 2026 года.

За 2025 год прошли путь от концепций и прототипов к предварительной версии продукта. Данная версия установлена в SOC Positive Technologies и проходит промышленную эксплуатацию в опытном режиме. Продукт анонсирован на конференции Positive Security Day в октябре 2025 года, где были продемонстрированы возможности его использования в будущем в качестве комплексного решения по защите почты.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- Единое решение защиты почты (подход «всё в одном решении») — антиспам- и антифишинг-движок собственной разработки, средства статического анализа, включая антивирус PT AV, базу PT IoC и набор правил PT ESC. PT Crawler для выявления угроз в ссылках, а также поведенческий анализ в виртуальных машинах с ловушками, которые позволяют раскрыться ВПО, еще не замеченному антивирусными сигнатурами.
- Технологическая основа от PT Sandbox — удобство установки и работы, гибкость продукта, быстрая доставка обновлений.
- Базы знаний, антивирусная лаборатория, источники данных об угрозах из экспертного центра PT ESC.
- Интеграция с продуктами Positive Technologies — MaxPatrol SIEM, PT NAD, MaxPatrol EDR, PT NGFW, PT AF, PT ISIM.

БИЗНЕС-ОБОСНОВАНИЕ

За последние пять лет атаки на электронную почту эволюционировали от массового спама к высокоцелевым фишинговым кампаниям, оставаясь главным вектором киберугроз. Простые ссылки заменились QR-кодами, ведущими на фишинговые ресурсы и переводящими пользователей за пределы защищаемого контура организации. Архивы с паролем из вложений заменились архивами-полиглотами, размещенными на общедоступных легальных файлообменных сервисах, снижающих опасения пользователей. Фишинговые атаки стали более точечными за счет применения ИИ, а сервисы для фишинга (Phishing-as-a-Service) вовсе снизили порог входа — они доступны даже неквалифицированным злоумышленникам.

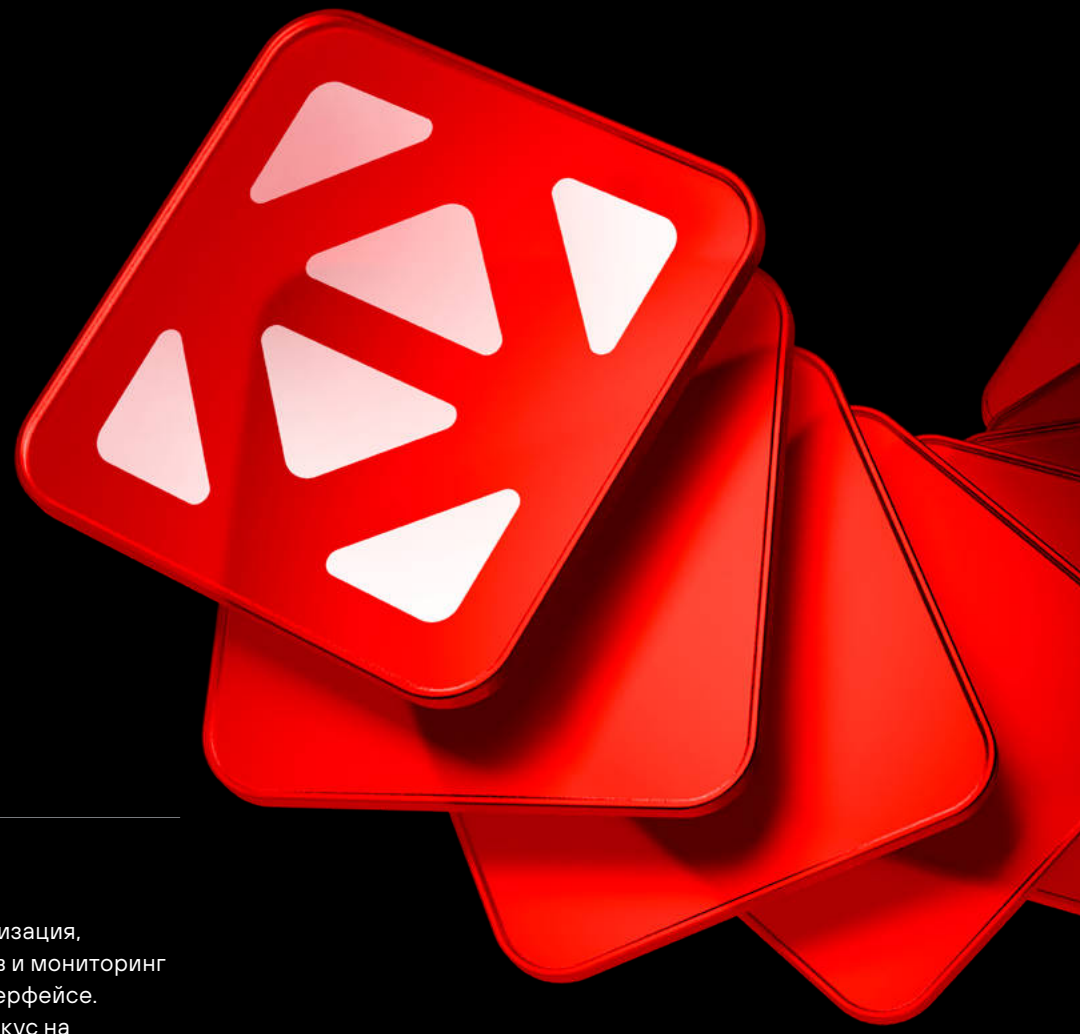
Эти тезисы подтверждаются статистикой за прошедший год — 86% успешных атак социальной инженерии осуществляется через электронную почту.

PT Email Security стал финальным аккордом в продуктовой линейке — средством многоуровневой защиты электронной почты, построенным на основе зарекомендовавшей себя песочницы PT Sandbox. Продукт защищает не только от сложного ВПО, которое проявляет себя лишь в ходе динамического анализа, но и от массового спама и адресного фишинга.

ТОЧКИ РОСТА

1. Новый смысл для известного класса продуктов:
   - от почтового шлюза (SEG) → к многоуровневой платформе предотвращения email-атак.
2. Фокус на ransomware-сценариях (шифровальщики как угроза № 1, от которой защищает PT ES):
   - продажа через тезис: остановка атаки до стадии шифрования;
   - детект loader / stealer / C2, а не только финального ВПО.
3. Sandbox-first архитектура как ключевой дифференциатор:
   - поведенческий анализ вместо сигнатур;
   - обнаружение неизвестных и целевых атак.
4. Монетизация базы PT Sandbox:
   - апгрейд существующих клиентов;
   - превращение Sandbox в экспертное ядро всей email-защиты.
5. Ответ на новые типы атак 2026 года:
   - QR phishing, AI-фишинг, polyglot-архивы, PhaaS
   - акцент на анализе ссылок и многоэтапных атак.
6. Системная ценность (SOC-ready):
   - интеграция с MaxPatrol SIEM, MaxPatrol EDR, PT NAD, PT AF, PT NGFW;
   - единый контекст атаки и ускорение расследований.
7. Снижение сложности и совокупной стоимости владения (TCO):
   - замена «зоопарка СЗИ» одним решением;
   - упрощение архитектуры и эксплуатации.

PT Data Security



PT Data Security — это платформа нового поколения для обеспечения безопасности данных. Объединяет в себе инвентаризацию, автоматизированную классификацию и мониторинг обращений к данным независимо от их места размещения и представления. Таким образом, обеспечивает полную видимость всей инфраструктуры хранения и обработки данных компании.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Унификация всех типов данных:** работает со структурированными, неструктурированными и полуструктурированными данными в рамках одной платформы.
- **Продвинутая AI-классификация:** минимум ложных срабатываний, автоматизация, адаптация под бизнес-глоссарий и модели доступа конкретной компании.
- **Полная видимость данных и инфраструктуры:** инвентаризация, классификация, анализ рисков и мониторинг обращений — всё в одном интерфейсе.
- **Автоматизация тяжелого:** фокус на классификации, которая составляет фундамент защиты данных, снижает количество ручных операций и освобождает время специалистов по ИБ для анализа.

БИЗНЕС-ОБОСНОВАНИЕ

Мы запустили разработку **PT Data Security** как ответ на системный запрос рынка: данные стали ключевым активом бизнеса и одновременно — одной из главных целей атак со стороны злоумышленников. При этом управление безопасностью данных для большинства компаний по-прежнему остается серьезной проблемой: оно фрагментировано, трудозатратно и неэффективно из-за использования морально устаревших средств защиты, созданных 10–15 лет назад и не рассчитанных на современные ИТ-ландшафты.

Сегодня такие понятия, как «утечки данных», вышли далеко за пределы узкого ИБ-сообщества и воспринимаются как понятные и измеримые риски для бизнеса, влияющие на операционную устойчивость, финансовые показатели и репутацию компаний.

Компании сталкиваются сразу с несколькими ключевыми вызовами при построении единой системы безопасности данных:

- стремительный рост объемов данных, а также числа и типов хранилищ;
- высокая распределенность инфраструктуры хранения и обработки данных — от десятков до сотен и тысяч сегментов;
- невозможность сформировать целостную картину и обеспечить полную видимость данных из-за разрозненности классических инструментов защиты.

С точки зрения бизнеса это приводит к избыточным трудовым и финансовым затратам на приобретение и поддержку нескольких решений одновременно, отсутствию полной прозрачности инфраструктуры и появлению большого количества слепых зон, не покрытых ни одним средством защиты. Именно такие зоны чаще всего становятся точками входа для злоумышленников.

PT Data Security создавался как единая платформа, которая позволяет:

- централизованно работать с данными независимо от места их размещения и формата;
- связывать безопасность данных с реальными бизнес-рисками за счет единой системы построения и управления политиками безопасности, адаптируемой под конкретную компанию;
- снижать совокупную стоимость владения за счет автоматизации, использования AI-подходов и консолидации всех функций безопасности данных в одном решении.

Для нас **безопасность данных** — это новое и стратегически важное направление развития. Мы расширяем продуктовый портфель, фокусируясь на решении одной из самых критичных задач для бизнеса, напрямую влияющей на его репутацию, капитализацию и операционную эффективность.

ИТОГИ 2025 ГОДА

В 2025 году мы выпустили первую версию **PT Data Security**, которая зафиксировала ключевую продуктовую идею и задала основу дальнейшего развития направления:

- все данные, независимо от формата и способа представления, — в одном месте;
- все задачи по работе с данными и их безопасности — в одном месте;
- продвинутая классификация данных с применением AI, ориентированная на практическую пользу для бизнеса, с минимальным количеством ложных срабатываний.

Основной целью первого релиза была демонстрация наших продуктовых идей и подхода широкому кругу клиентов и партнеров, а также сбор рыночного отклика и практической обратной связи. Параллельно мы вели проработку собственного бэклога уникальных функций, формируя долгосрочное видение развития продукта.

В результате релиза и последующих обсуждений мы привлекли более 30 клиентов и партнеров, которые высоко оценили выбранный подход и концепцию платформы.

По итогам первых пилотных проектов и взаимодействия с рынком мы сформировали топ клиентских запросов, которые легли в основу публичной части роадмапа продукта.

Таким образом, на сегодняшний день планы развития PT Data Security на 2026 год разделены на две части:

- **публичная часть** — составляет около половины всех планов и доступна для клиентов и партнеров Компании по запросу;
- **непубличная часть** — включает уникальные сценарии и «киллер-фичи», формирующие долгосрочное конкурентное преимущество продукта.

Результаты реализации непубличной части роадмапа мы планируем представить рынку по факту готовности, в том числе на **Positive Security Day в октябре**, где будет показана версия **PT Data Security 2.0**, адаптированная под специфику крупного enterprise-сегмента.

В целом мы рассматриваем 2025 год как точку выхода продукта на рынок и формирования устойчивой базы для масштабирования в 2026 году и далее.

PT Application Firewall

Высокопроизводительный межсетевой экран для непрерывной защиты любых приложений — от небольших сайтов до больших enterprise-приложений — от внешних киберугроз. Он предоставляет возможность гибкой настройки и может масштабироваться в соответствии с требованиями бизнеса. PT Application Firewall PRO содержит сильнейшую на российском рынке экспертизу по обнаружению и блокировке целенаправленных атак, основанную на собственном опыте проведения пентестов и на данных от исследовательской группы Positive Research и специалистов PT ESC. PT Application Firewall защищает приложения более 700 крупных отечественных организаций.

48%

доля PT Application Firewall в сегменте Web Application Firewall / межсетевой экран для веб-приложений[1]

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса WAF в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Точечное машинное обучение.** Помогает обнаруживать угрозы определенного класса (например, обфусцированный веб-шелл) и аномалии в трафике без риска появления ложных срабатываний и ухудшения производительности.
- **Расширенные механизмы полноценной защиты API-трафика.** Обнаруживают атаки внутри API-запросов за счет анализа вложенных данных, поддерживают современные технологии (SOAP, RestAPI, GraphQL API и JWT) и позволяют блокировать атаки из рейтинга OWASP API Security Top 10.
- **Собственный модуль распознавания внедрений.** Продвинутый механизм точно выявляет атаки с использованием внедрения кода (SQL injection, JavaScript, OSCommand injection, XPath, LDAP и другие), повышает эффективность защиты и уменьшает число ложных срабатываний.
- **Шаблоны политик безопасности для популярных приложений.** Готовые редактируемые шаблоны минимизируют время активации защиты, учитывают особенности и специфические уязвимости для каждого языка, совместимы с CMS-решениями Bitrix, OWA, ASP.NET и другими.
- **Виртуальный патчинг.** Дополнительный уровень защиты, который помогает выявлять и блокировать попытки эксплуатации до того, как уязвимости будут исправлены.
- Мы анализируем отчеты о реальных векторах атак и уязвимостях приложений, полученные от белых хакеров на платформе Standoff Bug Bounty, анализируем способность PT Application Firewall защищать от таких атак и постоянно совершенствуем продукт.
- Экспертная база международного уровня за счет многообразия источников ее пополнения.
- Собственная библиотека языковых контекстов совместно с лексическим и синтаксическим анализом запросов позволяет значительно повысить точность обнаружения атак, снижая количество ложных срабатываний, по сравнению с сигнатурным анализом.
- Заботимся не только о приложении, но и о ваших клиентах: модуль WAF.js предотвращает атаки на пользователей, сохраняя их лояльность и защищая вашу репутацию.

ИТОГИ 2025 ГОДА

2025 год стал для PT Application Firewall PRO годом системного развития продукта: мы последовательно улучшали архитектуру, производительность и эксплуатационные свойства решения, ориентируясь на реальные сценарии использования в инфраструктурах заказчиков.

Основные усилия команды были сосредоточены:
- на повышении производительности ядра обработки трафика;
- масштабируемости и работе в распределенных инфраструктурах;
- повышении стабильности и предсказуемости обновлений;
- развитии интеграций и автоматизации;
- улучшении UX для повседневной работы инженеров ИБ и эксплуатации.

КЛЮЧЕВЫЕ ТЕХНОЛОГИЧЕСКИЕ РЕЗУЛЬТАТЫ

Существенный рост производительности ядра

В течение всего 2025 года велась непрерывная работа по оптимизации ядра обработки трафика PTAF, отвечающего за применение политик безопасности.

Результат:
- при сравнении версии **4.1.6 (декабрь-2024)** и версии **4.3.0 RC** (декабрь-2025)
  - **производительность для большинства сценариев эксплуатации выросла в два раза,**
  - в отдельных сценариях рост оказался выше двукратного.

Практический эффект для заказчиков:
- инсталляции, рассчитанные на ~50 тыс. RPS, на новых версиях способны обрабатывать до ~100 тыс. RPS;
- рост пропускной способности достигается без **обновления аппаратных платформ;**
- снижается TCO и упрощается масштабирование при росте нагрузки.

МАСШТАБИРОВАНИЕ И РАБОТА В РАСПРЕДЕЛЕННЫХ ИНФРАСТРУКТУРАХ

Синхронизация параметров защиты между экземплярами PT AF

В 2025 году была реализована возможность синхронизации параметров защиты приложений между экземплярами PT AF, установленными в разных ЦОД.

К концу года функциональность была доведена:
- автоматическая синхронизация по расписанию (4.2.2).

Ценность:
- устранение конфигурационного дрейфа;
- единая модель защиты для распределенных инсталляций;
- упрощение эксплуатации в multi-DC и geo-distributed сценариях.

СТАБИЛЬНОСТЬ И УПРАВЛЯЕМОСТЬ ИЗМЕНЕНИЙ

Бесшовное применение конфигурации

В течение года был значительно переработан механизм применения конфигурации:
- изменения динамической и статической конфигурации применяются «на лету»;
- по умолчанию включен механизм поэтапного применения конфигурации (rolling update);
- снижены риски влияния изменений на обработку трафика.

Результат:
- более предсказуемое поведение;
- снижение операционных рисков;
- повышение доверия пользователя в разрезе процедуры изменения конфигурации.

ИНТЕГРАЦИИ И ЭКОСИСТЕМА

Аутентификация через внешние сервисы

Добавлена поддержка аутентификации через внешние сервисы по протоколу OAuth 2.0.

Ценность:
- интеграция с корпоративными IAM;
- упрощение управления доступом;
- повышение соответствия требованиям заказчиков к централизованной аутентификации.

ICAP и интеграции с внешними системами анализа

В 2025 году реализована поддержка протокола **ICAP**:
- возможность отправки файлов на внешние ICAP-серверы для дополнительной проверки;
- интеграция с системами антивирусного и репутационного анализа;
- сокращение технологического разрыва с PT Application Firewall 3 и потенциальный рост миграций на PRO.

Улучшение наблюдаемости и аналитики

- Расширены возможности фильтрации событий безопасности.
- Улучшена работа с временными диапазонами на дашбордах.
- Добавлена отправка расширенных данных (включая ошибки) во внешние SIEM-системы.
- Улучшена прозрачность действий, выполняемых при срабатывании правил.

Результат:
- быстрее расследование инцидентов, меньше слепых зон, лучшее понимание поведения защиты.

РАЗВИТИЕ МЕХАНИЗМОВ ЗАЩИТЫ

В течение года:
- добавлены новые правила для защиты популярных платформ и технологий;
- расширена поддержка современных протоколов (HTTP/2, WebSocket);
- реализована поддержка HTTP/2;
- оптимизированы существующие механизмы (например, защита от CSRF);
- улучшена работа с исключениями и шаблонами правил.

ИТОГ

По итогам 2025 года PT Application Firewall:
- стал **значительно производительнее**;
- лучше масштабируется в распределенных инфраструктурах;
- проще и безопаснее конфигурируется;
- глубже интегрируется с другими продуктами Компании;
- стал удобнее для повседневной эксплуатации.

Эти изменения создают прочную основу для дальнейшего развития продукта в 2026 году.

ОБЪЕМ РЫНКА WAF[1] В 2026 ГОДУ

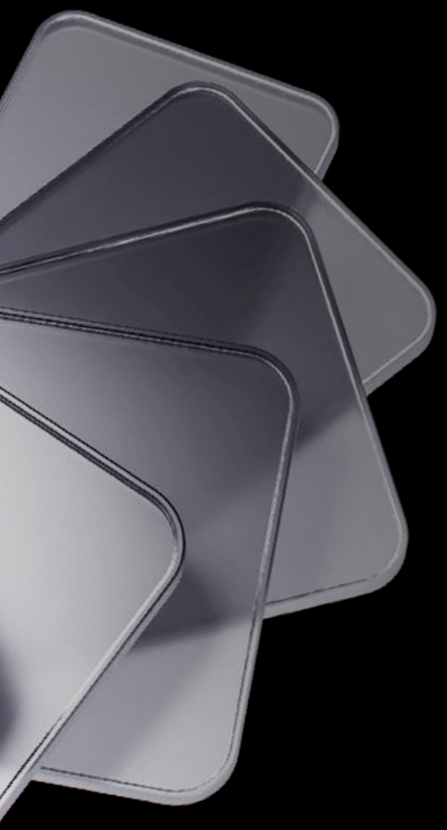
7 млрд руб.
SAM[2]

4 млрд руб.
SOM[3]

1 По совокупности сегментов Cloud и On-premise в вендорских деньгах.
2 SAM (Serviceable Addressable Market) — доступный объем рынка.
3 SOM (Serviceable Obtainable Market) — реально достижимый объем рынка.

PT Cloud Application Firewall

PT Cloud Application Firewall — облачный межсетевой экран для веб-приложений и API, который защитит от кибератак, утечки данных, не позволит злоумышленникам получить доступ к учетным записям пользователей и нарушить работу вашего бизнеса.



ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Собственный модуль распознавания внедрений.** Продвинутый механизм точно выявляет атаки с использованием внедрения кода (SQL injection, JavaScript, OSCommand injection, XPath, LDAP и другие), повышает эффективность защиты и уменьшает число ложных срабатываний.
- **Шаблоны политик безопасности для популярных приложений.** Готовые редактируемые шаблоны минимизируют время активации защиты, учитывают особенности и специфические уязвимости для каждого языка, совместимы с CMS-решениями Bitrix, OWA, «1С» и другими.
- **Виртуальный патчинг.** Дополнительный уровень защиты, который помогает выявлять и блокировать попытки эксплуатации до того, как уязвимости будут исправлены.
- **Полноценный WAF в облаке.** Пользователям доступна полная функциональность PT Application Firewall PRO, включая возможность тонкой настройки профилей защиты.
- **Единственный в России WAF,** постоянно тестируемый на Standoff Bug Bounty. Белые хакеры непрерывно ищут уязвимости в продукте, а значит, вы получаете решение, защищенность которого подтверждена и тестируется круглосуточно.
- **Гибкая тарифная сетка.** Любой бизнес может подобрать оптимальную цену защиты в зависимости от объема трафика и не переплачивать.

ИТОГИ 2025 ГОДА

146
количество заказчиков

200%
+15% рынка
рост

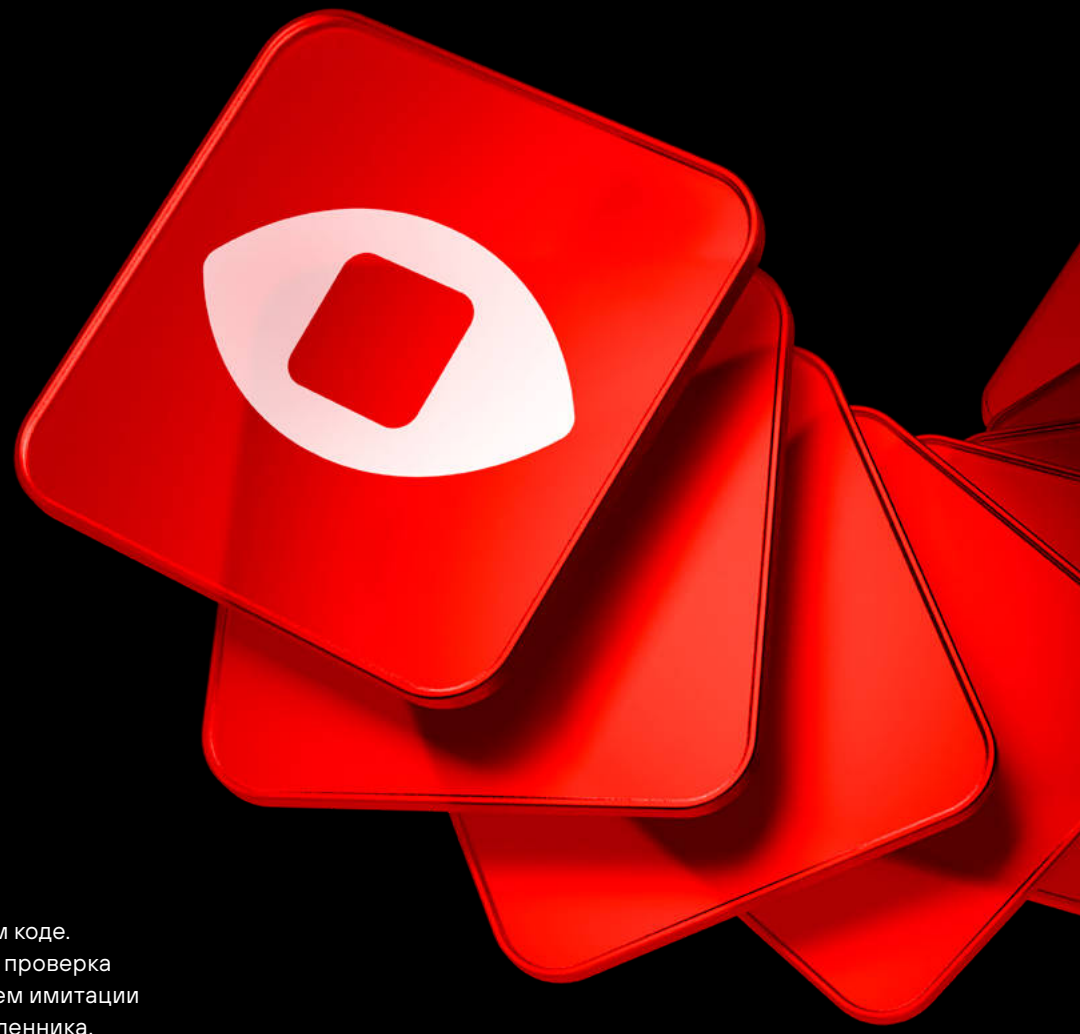
ПЛАНЫ НА 2026 ГОД

220
количество заказчиков

200%
+25% рынка
рост

Безопасная разработка

PT Application Inspector



PT Application Inspector — инструмент для эффективного выявления уязвимостей в программном коде приложений и заимствованных компонентах.

Ключевая особенность PT Application Inspector — точность результатов сканирования. Продукт сочетает следующие технологии: статический (SAST) с уникальной технологией символьного выполнения, анализ сторонних компонентов (SCA), а также динамический анализ (DAST).

- SAST, статический анализ — поиск уязвимостей в исходном коде.
- DAST, динамический анализ — проверка готового веб-приложения путем имитации действий реального злоумышленника.
- SCA, анализ сторонних компонентов — выявление уязвимостей в заимствованном коде.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Минимум ложных срабатываний.** Символьное выполнение снижает количество ложных срабатываний: анализ показывает, какие уязвимости действительно могут быть использованы, снижая затраты на проверку.
- **Удобная совместная работа.** PT Application Inspector обеспечивает возможность командной работы без ограничений по количеству приложений, сканирований и пользователей даже для минимальных конфигураций.
- **Выявление уязвимых сторонних библиотек.** PT Application Inspector обнаруживает такие библиотеки и определяет, действительно ли приложение использует их уязвимые части. Дополнив обработку результатов SCA анализом кода (SAST), мы в десятки раз сократили число ложных срабатываний и повысили информативность результатов.
- **Практическая экспертиза.** Специалисты отдела анализа защищенности регулярно пополняют базу знаний продукта информацией об уникальных уязвимостях, обнаруженных в реальных приложениях.
- **Синергический эффект гибридных технологий.** Наши методы анализа эффективны не только сами по себе. Объединив SAST и DAST, мы получили возможность автоматического подтверждения уязвимостей, что позволяет сократить трудозатраты на обработку результатов анализа.
- **Детектор скрытых функций.** PT Application Inspector обнаруживает признаки недекларированных возможностей, что помогает выявлять механизмы обхода защиты, целенаправленно заложенные в код.

ИТОГИ 2025 ГОДА

Гибкость и управляемость анализа безопасности

Управление правилами безопасности через DSL

- Реализован DSL для описания правил анализа безопасности без доработки ядра и сложных скриптов.
- DSL позволяет задавать входные точки данных, потенциально опасные операции и фильтры в декларативном виде.
- Единый подход работает для нескольких языков (Go, Java, JavaScript/TypeScript, PHP, Python).
- Низкий порог входа и возможность адаптации анализа под стандарты конкретной компании или проекта.

Смысл: анализ безопасности стал настраиваемым, управляемым и масштабируемым без увеличения операционных затрат.

Группы правил анализа

- Реализована возможность объединять правила анализа в группы и подключать их выборочно к проектам.
- Проекты больше не обязаны использовать полный набор проверок.
- Упрощена настройка анализа под разные команды, типы приложений и уровни критичности.

Смысл: выше точность анализа, быстрее внедрение и эксплуатация.

Масштабируемость и удобство в CI/CD и больших инсталляциях

Метки и очередь сканирования в CI/CD

- Решена проблема параллельных запусков сканирования в одной ветке.
- Добавлена возможность ожидания завершения предыдущего сканирования вместо аварийного завершения.
- Реализованы уникальные метки сканирований для прозрачного отслеживания запусков в CI/CD и веб-интерфейсе.

Смысл: стабильные и предсказуемые пайплайны даже при высокой параллельности разработки.

Упрощение CI/CD-интеграции: aiCTL

- Выпущена beta-версия единого CLI-инструмента aiCTL.
- Принцип «одна команда — одно действие» упрощает сценарии автоматизации.
- Поддержка всех ключевых операций: проекты, ветки, сканирование, ожидание, отчеты.
- Публичная разработка с ориентацией на комьюнити (выходим в open-sourse).

Смысл: быстрое и предсказуемое внедрение в любые CI/CD-процессы.

Работа с ветками и параллельной разработкой

- Один проект теперь поддерживает несколько git-веток.
- Сканирования по разным веткам не блокируют друг друга.
- Результаты анализа и триажа синхронизируются между ветками с сохранением контекста.

Смысл: безопасность встроена в реальный процесс разработки без дополнительных сущностей и ручных операций.

Пагинация списка проектов

- Внедрена постраничная загрузка проектов.
- Существенно улучшена отзывчивость интерфейса при большом количестве проектов.

Смысл: продукт комфортно используется в крупных организациях и масштабных установках.

Поддержка современных языков и фреймворков

- Java (Java 21, Vert.x 5.0.4),
- Scala (Play Framework 2.8.19),
- .NET / C# (C# 11, C# 12, .NET 8, .NET 9),
- JavaScript / TypeScript (React, Angular 18),
- Go (Go 1.25),
- Python (Starlette 0.27.0),
- PHP (Yii 2.0.42).

Новый модуль анализа сторонних компонентов (SCA)

Контекстный SCA: совместная работа SCA + SAST

- Реализован контекстный анализ зависимостей:
  - система не только находит уязвимые компоненты,
  - но и определяет фактическое использование уязвимого кода в приложении.
- Анализ фокусируется на вызовах методов и сценариях использования, которые с наибольшей вероятностью приводят к эксплуатации уязвимости.
- Каждое реальное использование уязвимого компонента в коде фиксируется как отдельная уязвимость.

Смысл: внимание концентрируется не на всем потенциально опасном, а на том, что действительно влияет на безопасность приложения.

Приоритизация и прозрачность результатов

- В результатах анализа:
  - реальные уязвимости, которые используются в коде, подсвечиваются отдельно,
  - остальные считаются потенциальными и доступны через фильтры.

- Для каждой уязвимости доступна расширенная информация:
  - уровень и вектор CVSS,
  - источники,
  - версия компонента и лицензия (при наличии),
  - ссылка на конкретный файл и строку кода, где происходит использование.

Смысл: проще принимать решения, быстрее разбирать результаты, меньше ручной работы.

Граф зависимостей

- Контекстный анализ дополняется графом зависимостей, который:
  - показывает все найденные уязвимые компоненты,
  - визуализирует связи между прямыми и транзитивными зависимостями.

- Это позволяет видеть, как именно уязвимость «приходит» в проект: напрямую или через цепочку библиотек.

Смысл: прозрачность состава ПО и понимание реальных путей риска внутри приложения.

Надежность, качество и зрелость продукта

- Снижение количества обращений в RND со стороны поддержки (–35%).
- Снижение числа багов в продакшене (–15%).
- Существенное расширение автоматизированного тестирования (145 новых тестов).
- Средняя задержка релизов — около трех дней.
- Существенно улучшена документация (127 новых и 235 обновленных разделов).

Смысл: продукт стабилен в эксплуатации и предсказуем в развитии.

Развитие плагинов для IDE

- Глубокая интеграция IDE-плагинов с сервером анализа (push/pull, автосинхронизация, удаленные сканирования).
- Встроенный ассистент для ускоренного триажа уязвимостей.
- Массовое управление статусами уязвимостей.
- Экспериментальный Copilot для генерации исправлений уязвимостей с помощью LLM.

Смысл: сокращение времени от обнаружения проблемы до ее исправления в коде.

РЫНОК PT AI 2026[1]

4,5 млрд руб.

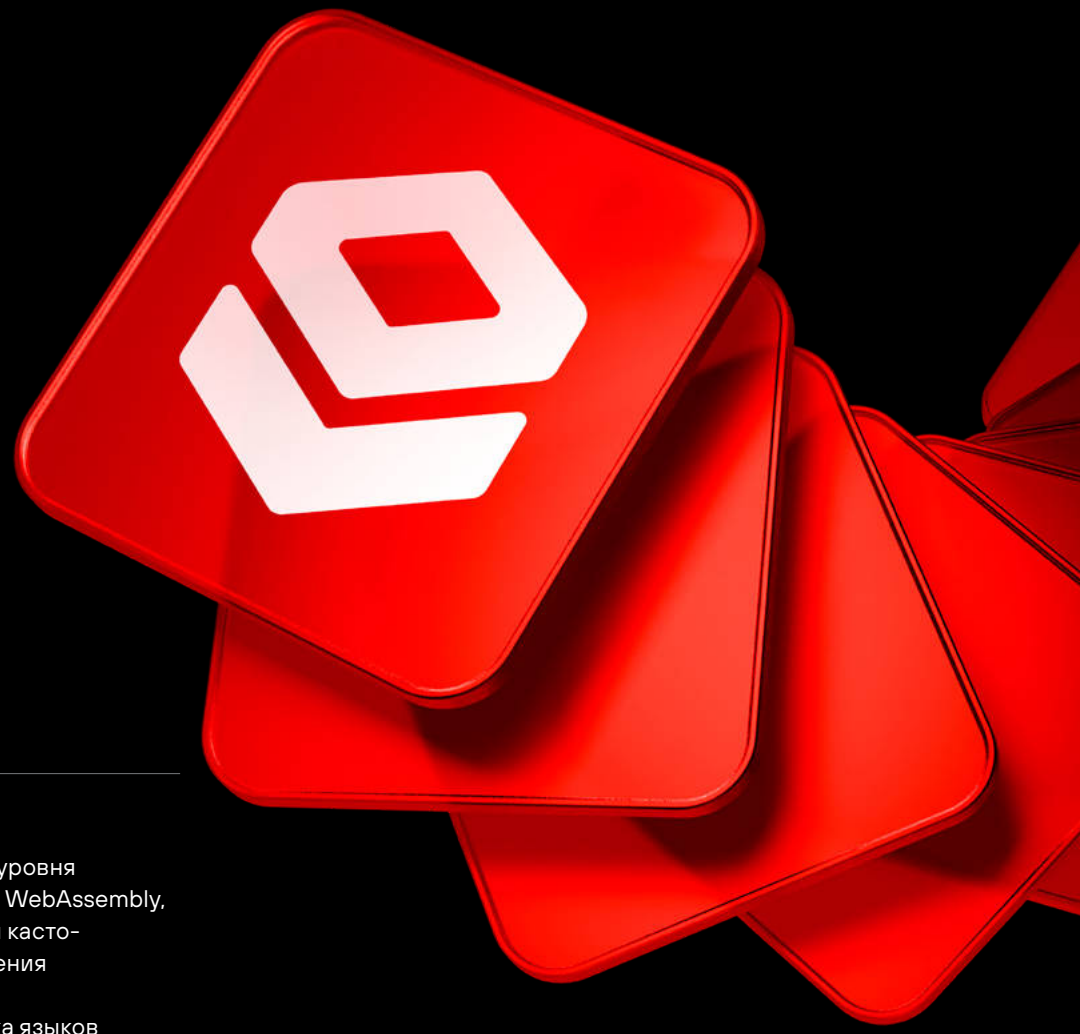
SAM[2]

1,8 млрд руб.

SOM[3]

1 В деньгах вендоров
2 SAM (Serviceable Addressable Market) — доступный объем рынка
3 SOM (Serviceable Obtainable Market) — реально достижимый объем рынка

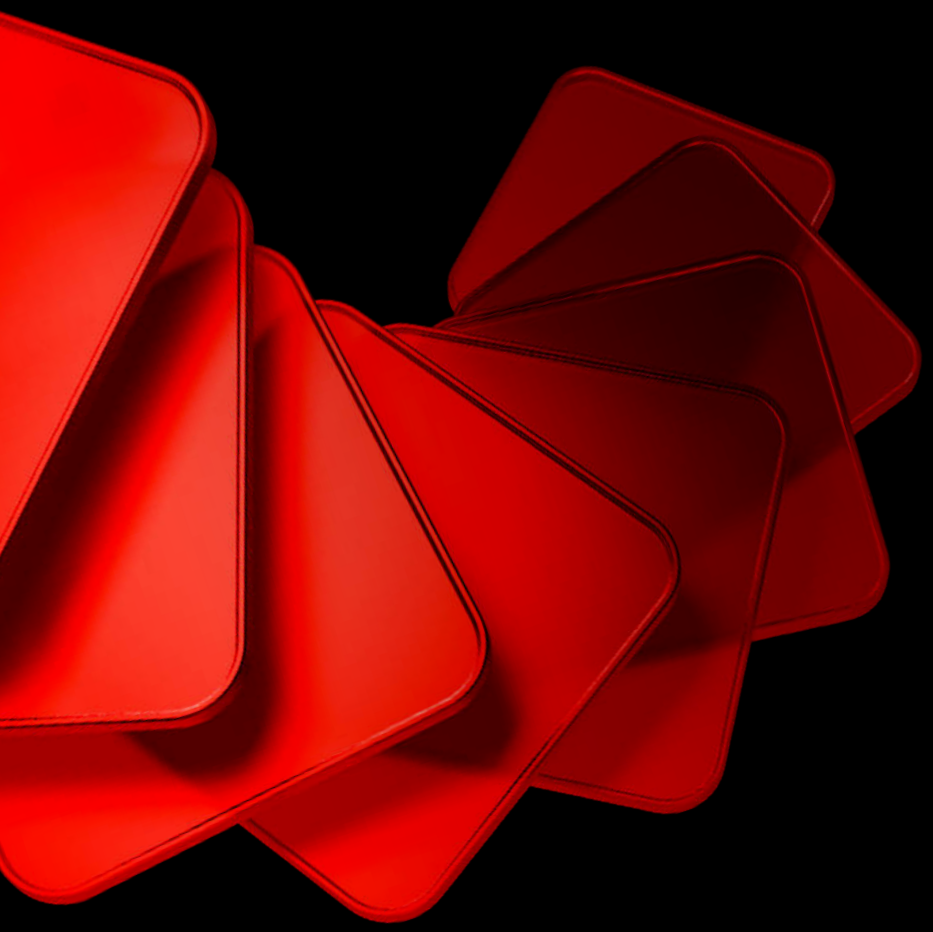
PT Container Security



Решение для комплексной защиты контейнерных инфраструктур. Обеспечивает безопасность разработки программных систем, использующих механизмы контейнерной виртуализации.

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Мультикластерность.** Централизованное управление несколькими кластерами Kubernetes вне зависимости от их расположения экономит время специалистов по ИБ. Решение легко устанавливается и позволяет настроить потребление ресурсов в зависимости от обрабатываемого потока событий.
- **Security as code.** Практическая реализация подхода, который позволяет описывать политики безопасности на языках программирования высокого уровня с использованием технологии WebAssembly, дает возможность создавать и кастомизировать правила обнаружения под нужды клиента.
- **Создание политик.** Поддержка языков программирования для разработки политик предоставляет неограниченные возможности для реализации логики реагирования на инциденты ИБ, возникающие при работе приложений.



- **Движок выявления аномалий.** Собственный производительный движок для контроля соблюдения политик и поиска аномалий в рантайме контейнеров позволяет гибко настраивать мониторинг событий, а встроенный набор правил обнаружения — выявлять угрозы «из коробки».
- **Покрытие всего цикла использования приложений.** Безопасность обеспечивается на всех этапах — от анализа образов в процессе сборки до контроля обращений к API кластера и событий, возникающих в ходе работы.
- **Быстрый старт.** Встроенные правила для защиты API и проверки на безопасность манифестов Kubernetes позволяют защитить кластер сразу после установки продукта.

ИТОГИ 2025 ГОДА

1. Успешные приобретения опытными клиентами с повышенной экспертизой: Департамент информационных технологий г. Москвы (ДИТ Москвы), «Юнирест».
2. Релизы с ключевым функционалом:
   - 0.6 — уникальный инструментарий для расследований произошедших инцидентов рантайма запущенных контейнеров, периодическое сканирование реестров образов, поддержка Active Directory (LDAP), поддержка хранилища Yandex Cloud.

     Новая экспертиза: запуск криптомайнера; внедрение кода с помощью LD_PRELOAD; запуск процесса напрямую из памяти; эскалация привилегий: capabilities; инструменты для активной разведки сети; создание reverse shell; подозрительное изменение файлов настройки запланированных заданий; подозрительное изменение чувствительных системных файлов.
   - 0.7 — поддержка контроля и управления несколькими кластерами с безотказной работой при отсутствии сетевой связности, онлайн-установка продукта без использования дистрибутива вообще через update.ptsecurity.com.

     Новая экспертиза:
     - BASE64: декодирование данных, изменение прав, уязвимость Ingress Nightmare (запуск вредоносного кода);
     - OPENSSL: загрузка пользовательской библиотеки;
     - OPENSSL: чтение и запись файлов;
     - OPENSSL: запуск SSL/TLS-сервера, подозрительное изменение SSH-ключей.
   - 0.8 — поддержка работы с продуктом через публичное API.

     Новая экспертиза:
     - создание экземпляра интерфейса io_uring,
     - изменение параметров генерации дамп-файла процесса,
     - запуск бесфайлового процесса.

- 0.9 — поддержка метрик работы компонентов и ИБ-нагрузки продукта с поставкой дашбордов для мониторинга, единственная среди конкурентов возможность управления видами источников мониторинга рантайма (вплоть для контроля обращения за конкретным файлом или отслеживания определенного сискола).

Новая экспертиза:
- обнаружение изменений файла core_pattern в файловой системе procfs;
- обнаружение создания жестких ссылок на файлы;
- обнаружение изменения файла с помощью замены новым;
- обнаружение руткитов в пространстве ядра;
- обнаружение настройки и запуска процессов через usermode helper API.

3 Выпуск open-source-версии.
- Являемся евангелистами контейнерной безопасности в России.

Выступления:
- созвон сообщества про Runtime Radar Ever Secure в Zoom **09.12**,
- вебинар с анонсом Runtime Radar **11.11,**
- подскаст про OpenSource с Ozon Tech,
- доклад «Как не сломать деплой вашего Cloud Native приложения» на митапе Selectel **27.11**,
- доклад «Tetragon: лучшие практики и нюансы разработки Tracing Policy» на Infra.conf'**25 06.25**,
- доклад «Что такое kprobes и где они обитают?» на ZeroNights **2025 11.25**.

Статьи:
- статья «Как не потерять свои контейнеры у себя в инфраструктуре?», **08.25**,
- статья ««Tetragon: лучшие практики и нюансы разработки Tracing Policy», **11.25**,
- статья «Kprobes и где они обитают», **12.25**.

Внутренние митапы в Компании:
- «Мониторинг функций ядра Linux с помощью eBPF. Как искать функции для детектирования угроз? Инструменты и рекомендации», **07.25**,
- «Анатомия кошмара: препарируем Ingress Nightmare», 09.25.

РЫНОК PT CONTAINER SECURITY / RUNTIME RADAR 2026[1]

1,35 млрд руб.

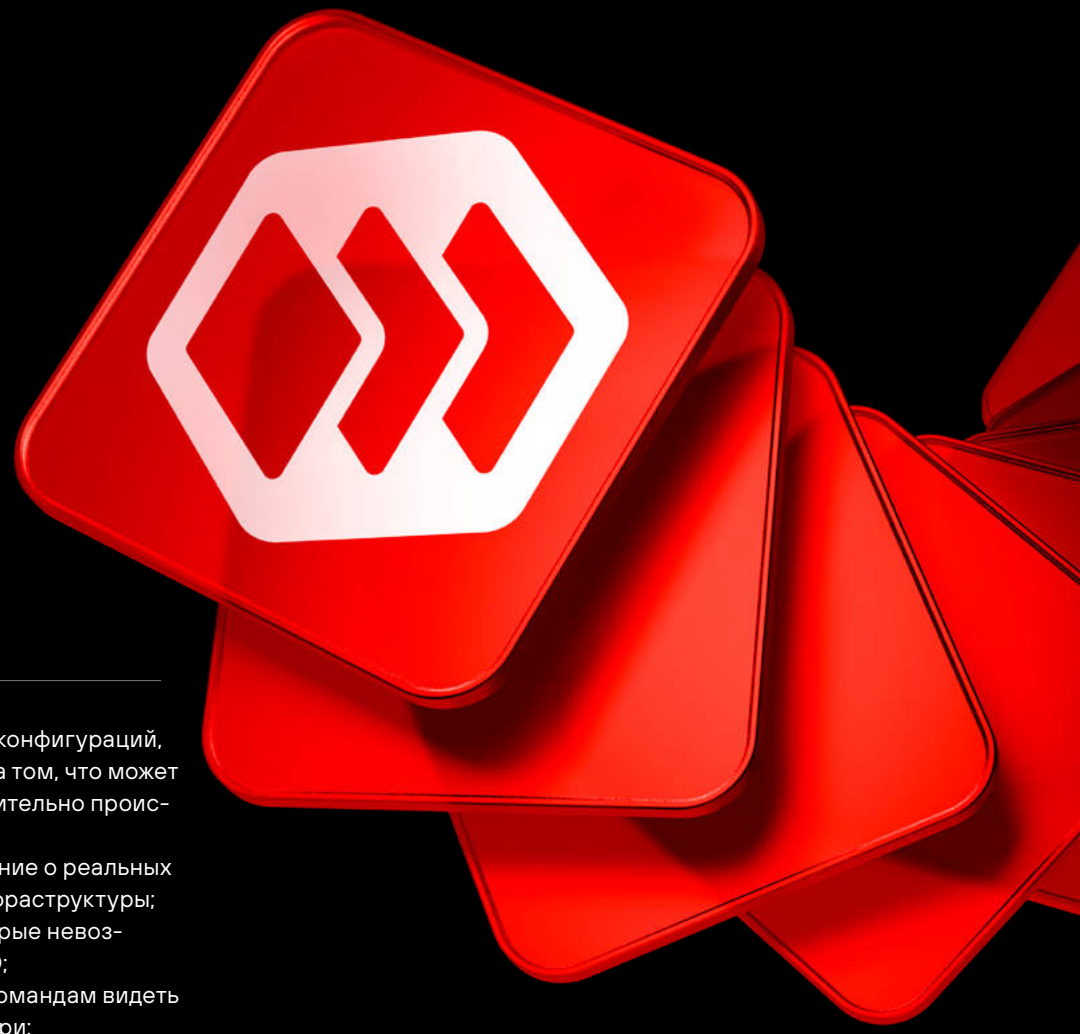
SAM[2]

0,3 млрд руб.

SOM

1 В деньгах вендоров.
2 Доступный объем рынка.

Runtime Radar



Открытое решение для мониторинга безопасности и реагирования на инциденты в контейнеризированных средах.

Контейнеризация радикально изменила подход к разработке и эксплуатации приложений, но одновременно усложнила задачу их защиты. Короткое время жизни контейнеров, высокая динамика Kubernetes-сред и глубокая абстракция инфраструктуры делают классические средства ИБ малоэффективными.

Runtime Radar — это исследовательский и практический проект Positive Technologies, который показывает, что на самом деле происходит внутри контейнеров в момент атаки. Решение собирает и анализирует рантайм-события, фиксируя реальные техники атак, аномалии и опасные паттерны поведения в продуктивных средах.

В отличие от сканеров образов и конфигураций, Runtime Radar фокусируется не на том, что может пойти не так, а на том, что действительно происходит в рантайме:

- дает объективное представление о реальных угрозах для контейнерной инфраструктуры;
- показывает техники атак, которые невозможно выявить на этапе CI/CD;
- помогает SOC и DevSecOps-командам видеть поведение контейнеров изнутри;
- служит основой для построения эффективных политик рантайм-защиты;
- встраивается в архитектуру ИБ вашей компании за счет кастомизируемых интеграций с syslog, почтой, вебхуками.

ЧТО ФИКСИРУЕТ RUNTIME RADAR

- Эксплуатацию уязвимостей в рантайме контейнеров.
- Попытки повышения привилегий и нарушения изоляции контейнера (container escape).
- Аномальные системные вызовы и процессы.
- Любые действия внутри наблюдаемых контейнеров (например, злоупотребление правами, API Kubernetes и сервисными учетными записями).

БИЗНЕС-ОБОСНОВАНИЕ

Потенциал рынка: согласно Gartner, к 2026 году 90% крупнейших международных компаний будут использовать контейнеры при построении ИТ-инфраструктуры. Однако есть ключевые вызовы рынка в Российской Федерации:

- ограниченный рынок — менее 2 млрд руб., низкая зрелость заказчиков (не понимают предметную область, и отсутствуют бюджеты на защиту контейнерных сред);
- высокая конкуренция (Luntry, Kaspersky, CrossTech, MTS RED, T1 — это только компании в России);
- высокое влияние решения на доступность инфраструктуры заказчиков.
- Проблема — текущими ресурсами нет возможности в краткие сроки нагнать конкурентов по функционалу, не работает подход top-down-продаж. Решение — выпуск open-source-версии продукта с прицелом на получение market-share. Основная целевая метрика — число активных пользователей.
- Преимущество — ключевой визионерский функционал по защите runtime для Kubernetes, включая экспертизу. Продвижение нашего месседжа на большую аудиторию.
- Цель — занять нишу на рынке и место у ключевых клиентов, не вступая в прямую конкуренцию с «Лабораторией Касперского» и Luntry.
- Фокус — развитие RR, достижение PMF, затем планируем постепенно повышать конверсию клиентов в платных вводом дополнительной функциональности и появлением сертифицированной версии продукта PT CS.

ИТОГИ 2025 ГОДА

- Анонс и запуск Runtime Radar.
- Мы самое популярное open-source-решение от Positive Technologies (125 звезд на Github, 200 инсталляций, семь PR).
- Мы единственный продукт среди отечественных конкурентов (Luntry, Kaspersky, CrossTech, MTS RED, T1) с open-source-версией (у иностранных решений — Stackrox, Aqua Security, Prisma Cloud — OSS-части присутствуют у всех).

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- **Фокус на реальных атаках**

  Показывает не абстрактные риски и CVE, а реальные сценарии атак, которые реализуются в контейнерных средах после внедрения приложений, и уязвимости, которые эксплуатируются злоумышленниками.

- **Создан с опорой на данные продуктивных сред**

  Все выводы и сценарии в Runtime Radar строятся на наблюдениях экспертов за реальными инфраструктурами, поэтому особенно релевантны для SOC, DevSecOps и архитекторов.

- **Гибридный подход к обнаружению угроз**

  Детекторы пишутся на Тьюринг-полном языке программирования, объединяя в себе лучшее от поведенческого и сигнатурного анализа. Runtime Radar также позволяет создавать свои детекторы.

- **Работает там, где сканеры бессильны**

  Большинство инструментов применяются на этапах CI/CD и создания конфигурации. Runtime Radar работает в момент атаки, когда контейнер уже запущен и взаимодействует с ИТ-системой. Решение закрывает слепые зоны, недоступные для image scanning и статического анализа.

- **Глубокий контекст Kubernetes**

  Анализируются с учетом pod, namespace, container, capabilities, сервисных аккаунтов и Kubernetes API. Это превращает набор необработанных технических событий в понятные инциденты, которые можно расследовать.

- **Минимальная нагрузка, незаметность**

  Технология eBPF позволяет собирать телеметрию без внедрения агентов в контейнеры и без влияния на приложения. Такой подход эффективен для продуктивных сред и высоконагруженных систем.

Продукты для обнаружения и реагирования на кибератаки

Технологии для сильного SOC

- MaxPatrol SIEM
- MaxPatrol 360
- MaxPatrol O2

Стратегический трек 2026 года

Единая концепция продуктов для сильного SOC

Концепция включает три функциональных слоя SOC.

Слой обнаружения — MaxPatrol SIEM обеспечивает сбор, корреляцию и выявление инцидентов.

Слой управления расследованиями — MaxPatrol 360 объединяет инциденты и события из различных источников и формирует единый операционный контур работы SOC.

Слой интеллектуального анализа — MaxPatrol O2 анализирует взаимосвязи между событиями, строит последовательность атак и автоматизирует часть аналитической работы SOC.

Продукты могут использоваться как совместно, так и независимо, в зависимости от инфраструктуры клиента. MaxPatrol 360 и MaxPatrol O2 способны работать с различными источниками событий и системами мониторинга, включая сторонние решения.

Продукты для обнаружения и реагирования на кибератаки

MaxPatrol SIEM

Система управления событиями ИБ, предназначенная для выявления сложных и целенаправленных кибератак в инфраструктурах любого масштаба.

Система собирает и анализирует события безопасности из различных источников ИТ-инфраструктуры и помогает SOC-командам обнаруживать угрозы и инциденты в режиме реального времени.

63% +5,63% год к году

доля MaxPatrol SIEM в сегменте SIEM[1]

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса SIEM в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

1 AI и машинное обучение

MaxPatrol BAD —
ML-модуль поведенческого анализа:

- выявляет сложные целенаправленные атаки без настройки правил (0-day, insider threat, etc);
- приоритизирует сработки и снижает шум — позволяет сосредоточиться на действительно опасных событиях;
- предоставляет расширенный контекст по событию, снижая время на расследование.

Экспертиза безопасности

- 1687 правил корреляции (на 31 декабря 2025 года);
- покрытие 368 техник MITRE ATT&CK (v17.1);
- доставка контента для трендовых уязвимостей — до 72 часов;
- детектирование четырех zero-day уязвимостей за год.

2 Архитектура и масштабирование

- Собственный декларативный язык запросов PDQL.
- Поддержка сложной аналитики, фильтраций и группировок.
- Масштабируемая архитектура.
- Обработка более 50 тыс. EPS на одном конвейере (более 500 тыс. EPS при горизонтальном масштабировании).
- Поддержка high-availability-кластеров для ElacticSearch. В LogSpace запланировано на 2026 год (релиз R.28, LogSpace 1.7).

3 Конкурентные преимущества

Фокус на импортозамещение
Поддержка отечественных ОС: Astra Linux 1.8.x, «Альт Линукс», «Альт Домен». Экспертиза и контент для российских инфраструктур:

- FreeIPA,
- ALD Pro,
- «Альт Домен»,
- интеграция с российскими аналогами Active Directory.

В 2025 году развитие MaxPatrol SIEM было сосредоточено на повышении стабильности, производительности и удобства работы аналитиков.

Ключевые изменения:

- реализован механизм flow control: устойчивость к резким скачкам нагрузки;
- адаптивное управление ресурсами;
- в интерфейсе реализован ряд функций, который повышает эффективность работы аналитика SOC;
- увеличено покрытие техник MITRE ATT&CK;
- добавлены данные о новых инструментах APT-группировок и хактивистов (на основе расследований Incident Response и Red Team).

Экспертный контент:

- регулярные обновления — раз в две недели (для сравнения — в 2024 году было один раз в месяц);
- критические уязвимости — до трех суток в 2025 году;
- публикации о повышении стабильности MaxPatrol SIEM.

ТЕКУЩАЯ ПОЗИЦИЯ

В 2025 году продукт показал почти двукратный рост выручки год к году. Доля рынка увеличилась и составила 63%. Рост обеспечен спросом со стороны клиентов к стабильному и зрелому продукту, который отвечает запросам рынка и регуляторов как на технологическом уровне, так и на ценовом.

СТРАТЕГИЯ 2026 ГОДА

Развитие идет в двух моделях поставки:

- On-premise — для крупных инфраструктур и регулируемых отраслей;
- Cloud — для компаний, которым требуется быстрый запуск SOC без длительного инфраструктурного цикла.

Облачная версия рассматривается как новый тип поставки MaxPatrol SIEM, а не отдельный продукт и является гипотезой роста в 2026 году.

В 2026 году усиливается пользовательский контур:

- новый интерфейс,
- AI-ассистент,
- повышение производительности,
- масштабируемость.

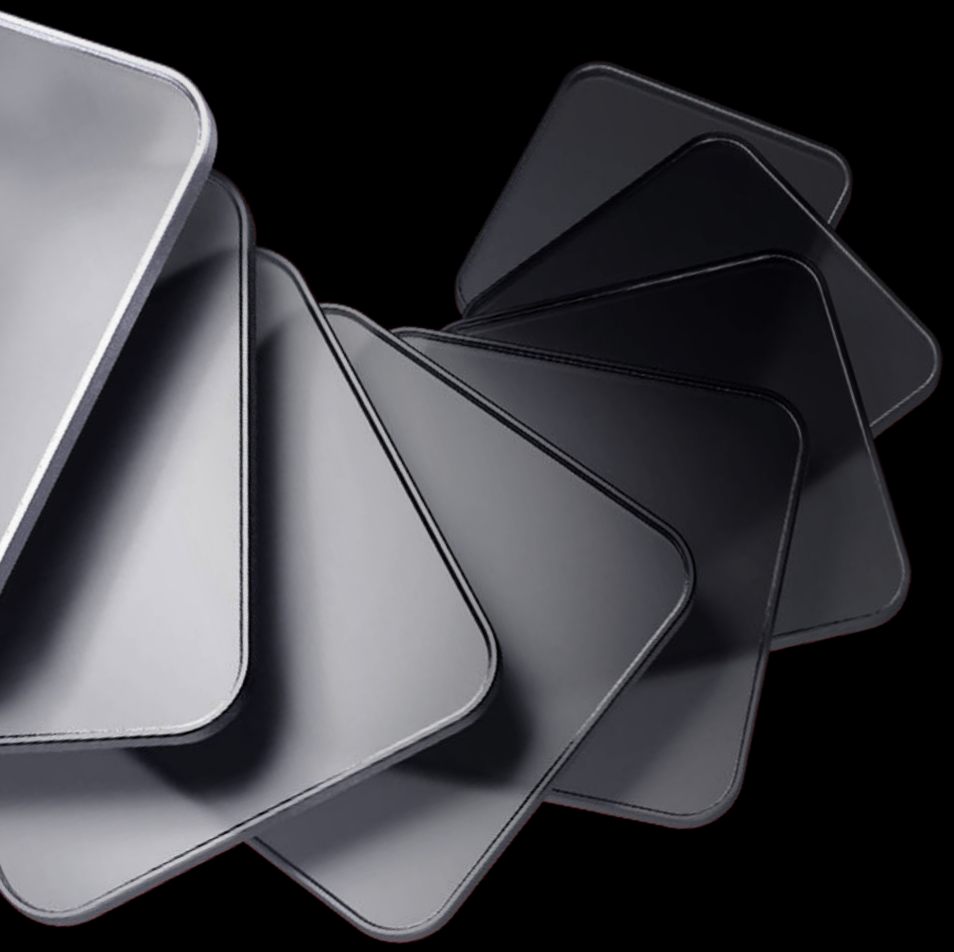
ТОЧКИ РОСТА

- Компании, переходящие от MSSP к собственному SOC.
- Средний сегмент, где важна скорость запуска.
- Заказчики с растущими объемами данных.

Ожидание на 2026 год — сохранение темпов роста за счет расширения адресуемого сегмента через облачную модель и обновление технологической базы.

MaxPatrol O2

Автопилот для результативной кибербезопасности. Обнаружение и остановка хакера с минимальным участием человека. Продукт автоматизирует процессы обнаружения, расследования и реагирования на кибератаки для защиты в условиях ограниченных ресурсов.



КЛЮЧЕВЫЕ ИЗМЕНЕНИЯ

1 **Переход в облако**

- Поддержка горизонтального масштабирования — работа с большими инфраструктурами.
- Всегда свежая версия — больше не нужно планировать работы по обновлениям на стороне клиента.
- Собственные LLM для AI в контуре Positive Technologies — данные клиентов не уходят третьим лицам.

2 **Обновление архитектуры**

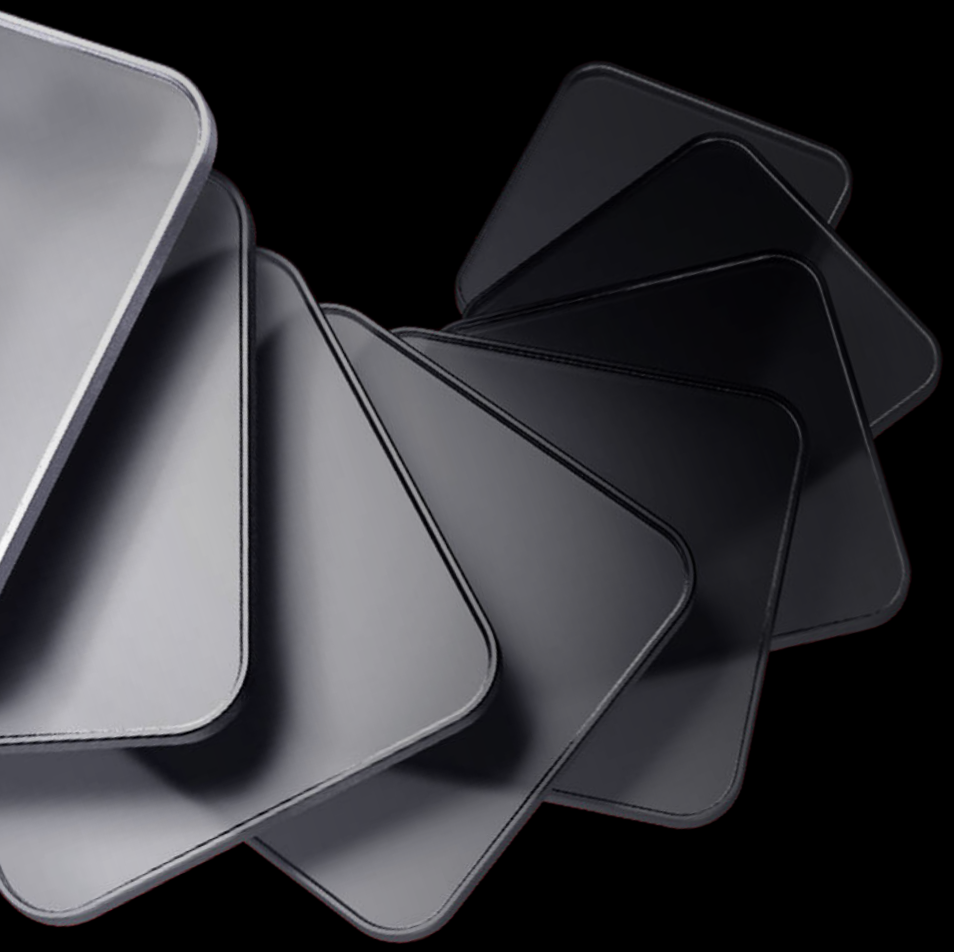
- Появление механизма локального хранилища — больше нет экстранагрузки от O2 на on-prem SIEM клиента.
- SIEM-агностичность — возможность поддержки сторонних SIEM без значительных доработок.
- Нативная поддержка сторонней экспертизы — больше не нужно писать правила разбора корреляций и инцидентов.

3 **Поддержка работы с инцидентами**

- Расследование инцидентов из источников — расследование того, что есть, вместо увеличения объема работы аналитика дополнительными сигналами.
- Обновленный UI — работа с инцидентами с привычным для данной работы функционалом (реализован процесс управления инцидентами со статусами и ответственными).

4 **AI-агент для расследований**

- Расширение сценариев расследования — уход от детерминированной логики, AI-агент принимает решения о том, как вести расследование.
- Резюме о расследовании — ознакомьтесь с ключевыми артефактами атаки и таймлайном, чтобы принять решение, не тратя время на анализ множества событий.
- Вынесение вердиктов по инцидентам — сэкономьте время, закрывая автоматически легитимную активность.



Ожидание 2026 года — масштабирование внедрений за счет зрелой архитектуры и связки с управленческим слоем.

В 2025 году продукт был перестроен архитектурно:

- снижена инфраструктурная нагрузка,
- пересмотрена модель обработки данных,
- внедрены ML-механизмы,
- повышена масштабируемость,
- обеспечена поддержка облачной модели.

Роль в архитектуре клиента

- Автоматическое построение последовательности атаки.
- Автоматический анализ взаимосвязей между инцидентами.
- Формирование вердиктов.
- Снижение нагрузки на аналитиков SOC.

ТОЧКИ РОСТА

- Дефицит квалифицированных специалистов.
- Рост количества инцидентов.
- Требование сокращения времени расследования.
- Повышение эффективности SOC без увеличения штата.

В пилотах зафиксировано снижение нагрузки на команду до 30%.

СТРАТЕГИЧЕСКИЙ ЭФФЕКТ 2026 ГОДА

Объединение продуктов в единую архитектуру позволяет:

- переходить от точечных продаж к архитектурным проектам,
- расширять сегмент за счет облачной модели,
- формировать понятную траекторию роста клиента внутри портфеля.

Ключевой трек 2026 года — развитие платформенной модели SOC с тремя уровнями: обнаружение, управление, автоматизация.

MaxPatrol 360

Единый центр управления расследованиями и операционной работой SOC. Решение объединяет функции мониторинга, централизованного управления инцидентами и детектирующей экспертизы, мониторинга инфраструктуры, а также автоматизации процессов расследования, реагирования и аналитики, обеспечивая повышение киберустойчивости и прозрачности операционной деятельности заказчиков.

РОЛЬ ПРОДУКТА В ПРОДУКТОВОМ ПОРТФЕЛЕ

Разработка и вывод на рынок MaxPatrol 360 обусловлены эволюцией требований заказчиков и развитием продуктового портфеля Positive Technologies. Клиенты Компании отмечали необходимость наличия единой платформы, позволяющей интегрированно использовать как решения Positive Technologies, так и решения сторонних вендоров в рамках повседневной операционной деятельности SOC.

MaxPatrol 360 устраняет данный функциональный разрыв, формируя надстройку над существующими продуктами Компании и другими средствами защиты информации, обеспечивая их объединение в единую операционную среду.

ПРИЧИНА СОЗДАНИЯ ПРОДУКТА

В 2025 году была зафиксирована структурная проблема: в инфраструктуре заказчиков используется 30–50 разрозненных систем мониторинга. Инциденты фиксируются, но не связаны в единую картину. Потери происходят на уровне операционной работы, а не на уровне обнаружения угрозы.

На рынке представлены SIEM и SOAR, однако отсутствует слой централизованного управления реагированием и расследованиями. MaxPatrol 360 создан в 2025 году как ответ на этот дефицит.

РОЛЬ ПРОДУКТА

- Единое окно работы SOC.
- Связывание инцидентов из разных источников.
- Формирование последовательности событий кибербезопасности для оперативного расследования.
- Централизация операционной деятельности.

Влияние на бизнес и финансовые показатели

Запуск MaxPatrol 360 усиливает конкурентные позиции ключевых продуктов Positive Technologies, включая **MaxPatrol SIEM, MaxPatrol VM, MaxPatrol NAD, MaxPatrol EDR** и другие решения, за счет расширения сценариев их совместного использования и повышения ценности комплексных внедрений для заказчиков.

Платформа также формирует дополнительный источник выручки, в том числе за счет:

- лицензирования уровня Security Operations;
- увеличения среднего чека существующих клиентов;
- увеличения совокупного дохода от одного клиента на протяжении всего срока сотрудничества;
- расширения возможностей кросс-продаж внутри продуктового портфеля.

Отличительные характеристики и зрелость решения

MaxPatrol 360 разрабатывался с ориентацией на требования крупных корпоративных SOC, распределенных инфраструктур и провайдеров сервисов безопасности (MSSP).

Продукт создавался выделенной командой разработки, что позволило обеспечить высокую скорость вывода решения на рынок. Период от формализации концепции до внедрения полнофункционального решения в промышленную эксплуатацию у крупных заказчиков составил менее шести месяцев. В настоящее время платформа продолжает активно развиваться и масштабироваться.

Текущий статус и планы развития

По состоянию на отчетную дату MaxPatrol 360 эксплуатируется в пилотном режиме ограниченным числом заказчиков в промышленной среде. Выход решения на широкий рынок запланирован на II квартал 2026 года.

MaxPatrol 360 является значимым элементом долгосрочной продуктовой стратегии Positive Technologies, направленной на развитие экосистемного подхода, повышение устойчивости бизнеса и формирование основы для дальнейшего роста выручки Компании.

ТОЧКИ РОСТА

- Компании с распределенной инфраструктурой.
- Партнеры и MSSP.
- Зрелые SOC с высокой операционной нагрузкой.
- Заказчики, масштабировавшие SIEM, но не процессы.

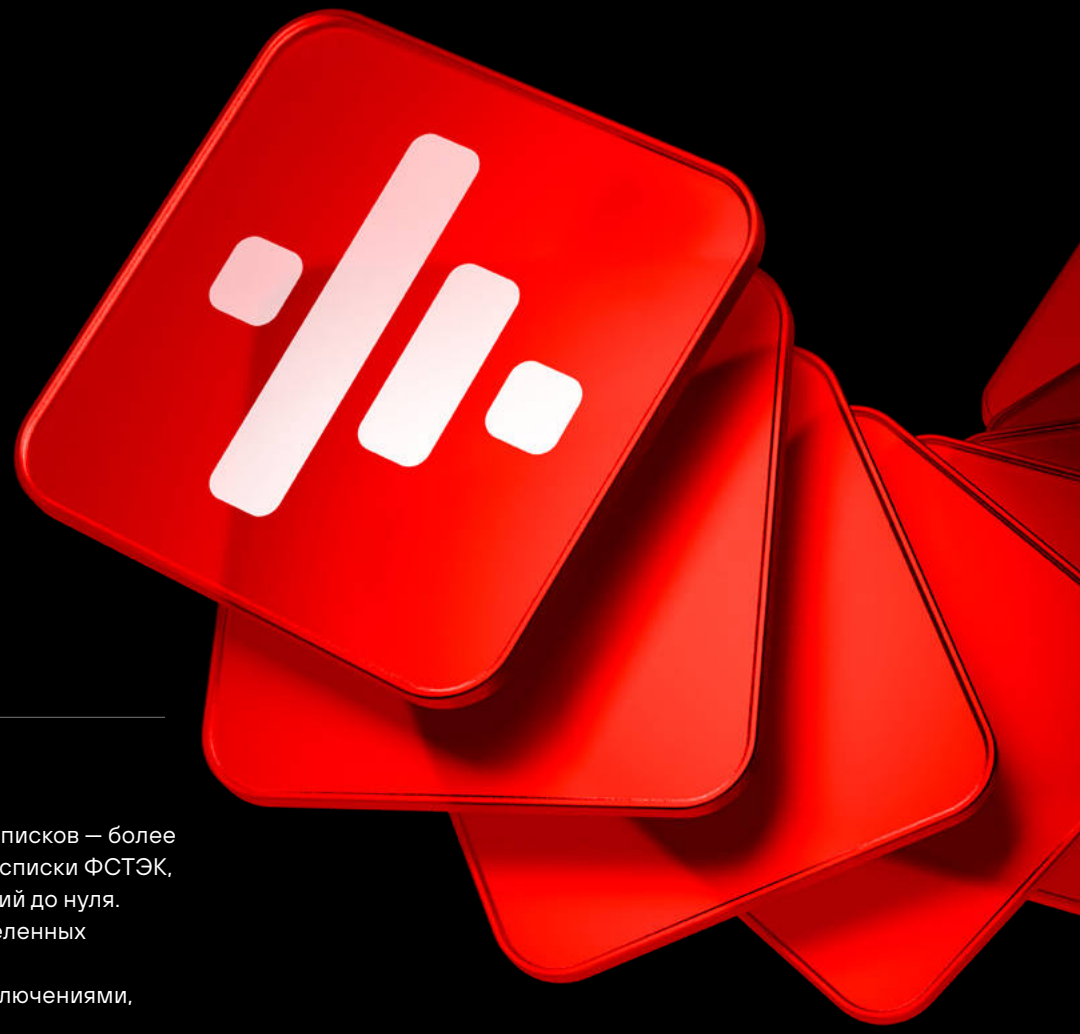
2026 год — этап закрепления категории и объяснения рынку необходимости данного слоя.

PT NAD

Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий хакеров в трафике.

59%

доля PT NAD в сегменте NTA&NDR / системы анализа трафика[1]



ИТОГИ 2025 ГОДА

- Увеличение скорости сигнатурного анализа в три раза благодаря оптимизации ядра DPI.
- Запуск Центральной консоли — единого интерфейса для управления распределенными системами с безопасным шифрованием данных.
- Внедрение хранения метаданных в облаке (Elasticsearch / OpenSearch as a Service) — снижение требований к железу, гибкое масштабирование и управление TCO.
- Добавление плейбуков — автоматизация реакции на инциденты, единая интерпретация событий безопасности.
- Расширение репутационных списков — более 40 тыс. индикаторов, включая списки ФСТЭК, снижение ложных срабатываний до нуля.
- Улучшение работы в распределенных инсталляциях:
  - управление профилями и исключениями,
  - поддержка MPLS-трафика,
  - визуализация сетевых связей при атаках (NTLM Relay).
- Снижение TCO и повышение удобства за счет облачных решений, централизации управления и автоматизации.

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса NTA&NDR (не включает решения класса Sandbox) в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

ТЕКУЩАЯ ПОЗИЦИЯ

По итогам 2025 года продукт показал уверенный рост выручки относительно 2024 года. Доля рынка увеличилась и составила 59%.

Рост обеспечен высоким спросом со стороны крупного бизнеса и госкорпораций на зрелый и технологически стабильный продукт, способный решать проблему импортозамещения без потери качества. Ключевым драйвером стал выход ряда значимых обновлений, которые напрямую повлияли на операционную эффективность клиентов: централизированное управление георасспределенными информационными системами и снижение совокупной стоимости владения (TCO).

КЛЮЧЕВЫЕ ДРАЙВЕРЫ 2025 ГОДА

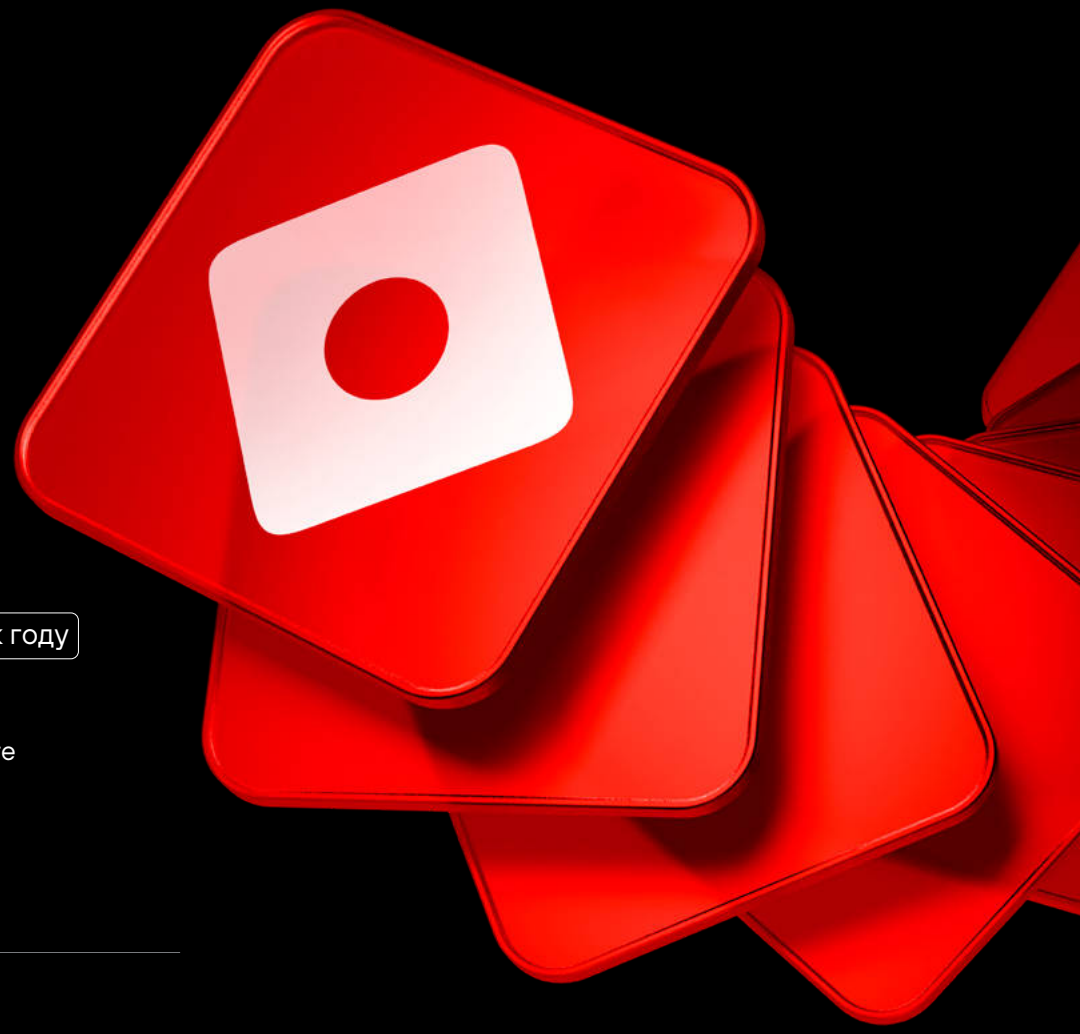
- **Центральная консоль.** Бизнес получил возможность масштабировать сетевую безопасность на дочерние организации (ДЗО) без расширения штата. В условиях кадрового голода это позволило обеспечить одинаково высокое качество анализа трафика и детекта угроз по всей сети группы компаний, а не только в головном офисе.
- **Экономическая эффективность (TCO).** Бизнес платит меньше за владение продуктом, при этом качество работы PT NAD не снижается, а значит, уровень защищенности активов остается максимальным.
- **Технологическое превосходство.** Уникальная технология глубокого анализа трафика (PT DPI) позволяет заказчику видеть всю картину сети целиком. Для бизнеса это означает главное: уверенность, что злоумышленник не останется незамеченным даже при использовании сложных зашифрованных протоколов.

СТРАТЕГИЯ И ТОЧКИ РОСТА 2026 ГОДА

- PT NAD остается самым технологичным средством анализа трафика на рынке. Уникальная технология DPI обеспечивает гарантированную стабильность работы продукта.
- Развитие функционала будет сфокусировано на трех направлениях:

1. Новый движок поиска угроз — увеличение скорости и глубины обнаружения аномалий для расследований инцидентов любого масштаба.
2. Функция реагирования — расширение продукта в плоскость активной защиты, переход от детекта к автоматизированному реагированию на угрозы на сетевом уровне.
3. Развитие ML-технологий — повышение точности детектирования и снижение ложных срабатываний за счет ML-модулей.

PT Sandbox



PT Sandbox — песочница, которая позволяет обнаруживать новые вирусы, эксплойты нулевого дня, программы-вымогатели и другое сложное ВПО. Она не только детектирует угрозы, но и не допускает их проникновение в контур компании, обеспечивая комплексную защиту от целенаправленных атак и массовых угроз.

65% +4% год к году

доля PT Sandbox в сегменте Sandbox/песочницы[1]

ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Выявляет сложные угрозы**

  Обнаруживает неизвестные вирусы, продвинутое вредоносное ПО, а также ПО, нацеленное на SCADA-системы.

- **Предотвращает целенаправленные атаки**

  Позволяет настраивать среду эмуляции и приманки с учетом отраслевой специфики организации, защищая от тщательно подготовленных атак.

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса Sandbox (в том числе компонентов Sandbox в составе комплексных продуктов) в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

- **Защищает отечественные ОС**

  Поддерживает виртуальные среды с Astra Linux, «Альт» и «РЕД ОС», готов к установке на Astra Linux.

- **Высокое качество обнаружения**

  Каждый объект анализируется в PT Sandbox динамическими и статическими методами, основанными на правилах PT Expert Security Center, с помощью технологий машинного обучения, а также проверяется несколькими антивирусами, доступными «из коробки».

- **Легкое встраивание в инфраструктуру**

  PT Sandbox поддерживает множество вариантов интеграции, а гибкий API позволяет использовать песочницу в любой конфигурации информационных систем.

- **Гибкая кастомизация виртуальных сред**

  В них можно добавить специфическое ПО (и его версии), которое действительно используется в компании и может стать точкой входа для злоумышленников.

- **Экспертные технологии от PT ESC**

  Уникальные правила для обнаружения ВПО, в том числе с помощью ML-технологий, ловушки и приманки для раскрытия вредоносного поведения, защита от техник обхода песочниц.

- **PT Sandbox — первая песочница с искусственным интеллектом в реестре российского ПО**

  Сведения о наличии искусственного интеллекта в PT Sandbox включены в реестровую запись о продукте.
  С помощью настраиваемого машинного обучения песочница анализирует более 8,5 тыс. признаков поведения объекта: действия процессов, цепочки вызовов API, сетевое взаимодействие, создание вспомогательных объектов, тем самым обеспечивая высокую точность выявления неизвестных целенаправленных угроз.

ИТОГИ 2025 ГОДА

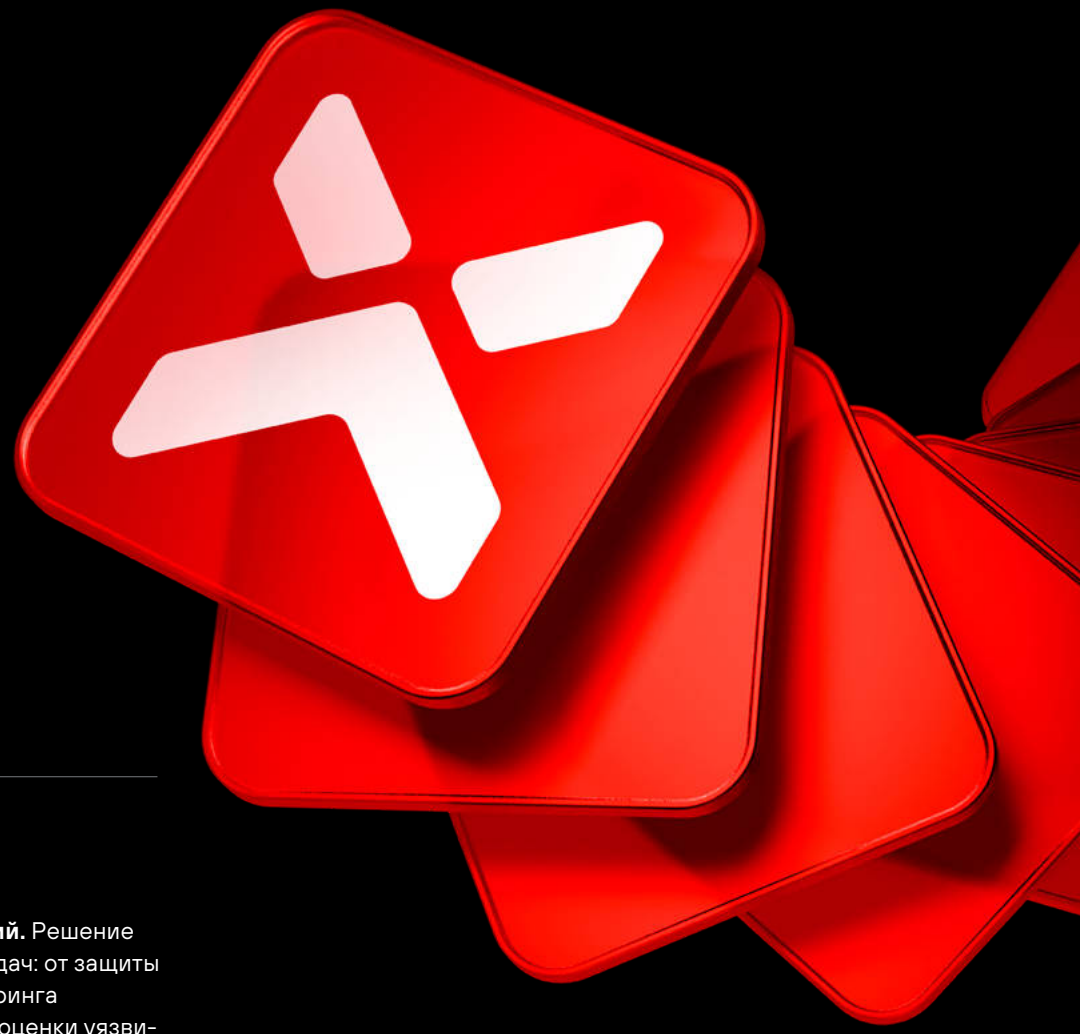
За 2025 год выпущено 10 релизов продукта.
Из них можно выделить:

- ML на сетевом трафике ПА — поведенческий анализ сетевого трафика с помощью технологии машинного обучения;
- пользовательские YARA-правила — добавление правил, разработанных специалистами по ИБ заказчиков;
- новый карантин — расширены возможности работы с карантином;
- мониторинг системы — мониторинг модулей системы и аппаратных ресурсов в Grafana;
- РПА — поведенческий анализ в интерактивном режиме и настройка приоритетов поведенческого анализа;
- расширенный API — получение списка заданий через публичный API;
- новые источники — подключение S3-хранилищ в качестве источников;
- новые форматы файлов и проверка QR — проверка ссылок из QR-кодов;
- управление образами ПА — расписание обновления, управление очередью, выбор базовых образов;
- средство проверки PT AV — продукт сертифицирован ФСТЭК по дополнительному профилю защиты ИТ.САВЗ.Б4.ПЗ;
- новые возможности интеграции — добавлены или улучшены возможности интеграции с PT NGFW, PT ISIM, PT EDR, PT AF PRO.

Для быстрого старта в защите от вендора

PT X

Облачное решение для мониторинга и реагирования на киберугрозы в режиме 24/7.



ОТЛИЧИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ

- **Ответственность за результат, а не формальные SLA.** Используя PT X с учетом рекомендаций Positive Technologies, клиент может выйти на кибериспытания, чтобы измерить защищенность компании. Если белые хакеры реализуют недопустимое для клиента событие, Positive Technologies готова выплатить им вознаграждение.
- **Уникальный набор технологий.** Решение закрывает широкий спектр задач: от защиты конечных устройств и мониторинга до анализа сетевого трафика, оценки уязвимостей на компьютерах и серверах, а также детальной проверки ВПО.

- **Финансовая гарантия защиты.** При выполнении условий киберминимума (требований для обеспечения защищенности ИТ-инфраструктуры) клиент PT X может застраховать компанию от киберрисков у одного из партнеров страхования. При соблюдении заказчиком требований Positive Technologies берет на себя оплату страховой премии, и в случае кибератаки клиент получит компенсацию.
- **Топовая экспертиза.** Непрерывная защита обеспечивается за счет поддержки от специалистов экспертного центра безопасности PT ESC, имеющих опыт в области выявления, предотвращения и расследования тысяч сложных кибератак.
- **Быстрый результат.** Достаточно установить агенты на конечные устройства, и уже через несколько часов появляются первые результаты: защита от шифровальщиков, ВПО и эксплуатации распространенных уязвимостей в инфраструктуре.

БИЗНЕС-ОБОСНОВАНИЕ

Новая реальность кибербезопасности показывает, что жертвами атак становятся не только крупные корпорации, но и компании среднего и малого бизнеса. Во многих таких организациях либо нет выделенных специалистов по ИБ, либо функции ИБ выполняют универсальные сотрудники, которые не могут обеспечить круглосуточный мониторинг и реагирование.

В этой ситуации наличие PT X зачастую является единственным шансом получить экспертный уровень защиты.

К Positive Technologies нередко обращаются компании, которые столкнулись со взломом. Даже после работы нашей команды Incident Response риск повторного инцидента сохраняется.

Теперь Positive Technologies предлагает срочную помощь при инциденте, дает доступную и постоянную защиту из облака, а также гарантирует ее результативность через вывод клиента на киберисытания.

РЕЗУЛЬТАТЫ 2025 ГОДА

- К концу года у PT X было 12 коммерческих клиентов. Основную долю составил ретейл, также среди клиентов представлены финансовый сектор, спортиндустрия и разработка ПО.
- Под защитой PT X находится более 30 тыс. активов в различных компаниях. Средний размер защищаемой инфраструктуры — 2,1 тыс. конечных устройств.
- Клиенты в два раза чаще выбирают pro-версию решения по сравнению с base, несмотря на более высокую стоимость. Это подтверждает соответствие продукта рынку и ориентацию заказчиков на практический результат, а не на формальное выполнение требований.
- В процессе подключения новых клиентов более чем в половине случаев PT X обнаруживает в инфраструктуре заказчика индикаторы компрометации (ВПО, шифровальщики, майнеры, следы удаленного управления и другие). Такой результат показывает, что PT X помогает предотвращать серьезные киберинциденты, становясь для бизнеса стратегическим партнером с самого первого дня.

ТОЧКИ РОСТА

- Развитие ML/AI-технологий и расширение их применения и автоматизации для еще более точного и быстрого разбора инцидентов у клиентов.
- Первые референсы по клиентам, которые выполнили наши рекомендации и вышли на киберисытания.

Для защиты промышленных инфраструктур

Ответ Positive Technologies на запрос рынка в 2025 году

Эволюция PT ISIM — от OT-сетевого сенсора в систему обеспечения киберустойчивости промышленных инфраструктур.

Цель: сделать OT инфраструктуру предприятия защищенной, управляемой и устойчивой, а управление — прозрачным.

Наши главные ресурсы — технологичность и промышленная экспертиза.

Почему мы решили пойти в промышленный сегмент

Цифровизация промышленности неизбежно ведет к расширению поверхности атаки, то есть увеличению числа точек входа для злоумышленника. Наши технологии развиваются в соответствии с новой реальностью и управляют рисками не точечно, а по всей инфраструктуре.

Базовые меры безопасности в промышленности в перспективе десяти лет больше не будут сводиться к простой изоляции контура. Так как промышленность активно цифровизируется, ИТ-сегмент потребует большего взаимодействия с технологическим сегментом (OT). К тому же структура ролей будет усложняться — появляются новые роли (например, CDTO), отвечающие за нативное взаимодействие ИТ- и OT-сегментов.

1 Чтобы следовать миссии и сделать цифровую трансформацию промышленности безопасной

Чтобы промышленные предприятия могли развиваться и не бояться вызовов цифровизации, мы строим продукт для киберустойчивости, покрывающий всю промышленную инфраструктуру — от сетевого уровня и технологических сегментов до конечных узлов и сервисов.

2 Чтобы удовлетворить спрос по обеспечению киберустойчивости в промышленной безопасности

Рынок OT Security в России находится на ранней стадии развития: при большом объеме промышленной инфраструктуры покрытие средствами защиты остается низким. Мы прогнозируем сценарий, при котором в ближайшие пять лет рынок OT Security будет расти почти в два раза быстрее рынка IT Security.

Драйверы спроса

- **Вызовы цифровизации для промышленности:** расширение поверхности для кибератак, усложнение контроля технологического контура и рост рисков инцидентов и простоя.
- **Усиление регуляторного давления (ФСТЭК/КИИ):** среди значимых объектов КИИ минимально необходимый уровень защиты обеспечен только у 36% организаций. А внедрять и подтверждать выполнение установленных мер защиты нужно всем промышленным предприятиям.
- **Зарождающийся спрос на унифицированные инструменты** для сбора и агрегации данных со всей производственной инфраструктуры в единое хранилище (например, Data Lake) для анализа и принятия управленческих решений. С этим потенциально могут помочь ИБ-продукты для OT.

Для защиты промышленных инфраструктур

PT ISIM

Система обеспечения киберустойчивости промышленных инфраструктур.

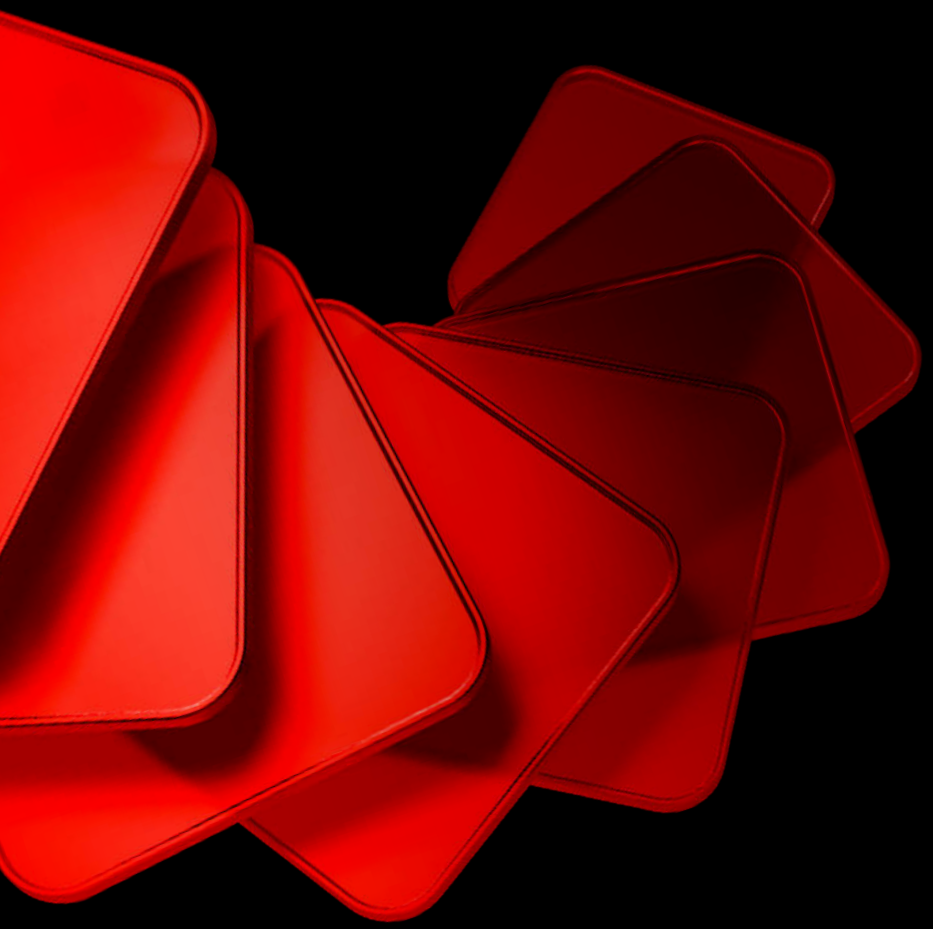
16%

доля PT ISIM в сегменте Industrial Security / промышленная кибербезопасность, защита АСУ ТП[1]

ДЛЯ КИБЕРУСТОЙЧИВОСТИ ПРОМЫШЛЕННОГО КОНТУРА PT ISIM СЕГОДНЯ ОБЕСПЕЧИВАЕТ:

- **полную видимость технологической среды:** трафик промышленных протоколов, журналы событий операционных систем промышленного ПО, конфигурации промышленных контроллеров, технологическая телеметрия — все собирается и анализируется в едином контексте;
- **управление поверхностью атаки:** уязвимости, отклонения, риски конфигураций;
- **обнаружение угроз и аномалий, в том числе** в изолированных сегментах — выявление критичных команд/событий;
- **сдерживание и предотвращение инцидентов на конечных узлах;**
- **соответствие большей части ключевых групп мер ФСТЭК для КИИ** и планомерное расширение этого покрытия.

1 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса Industrial Security в 2025 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).



ЧТОБЫ УСКОРЯТЬ TIME-TO-VALUE И МАСШТАБИРОВАНИЕ, КОМАНДА PT ISIM:

- интегрировала в платформу антивирус, а также средства управления активами, обнаружения уязвимостей и продвинутой защиты конечных точек. Для упрощенных процессов закупки, развертывания и эксплуатации все это поставляется в едином ПАК;
- создала центр промышленной R&D-экспертизы, который регулярно поставляет обновления в PT ISIM: разбирает промышленные протоколы, исследует промышленный софт и оборудование, находит уязвимости. Это расширяет возможности продукта, повышает точность мониторинга, анализа и детекта. Такая глубина экспертизы позволяет нам разбираться в особенностях каких-либо промышленных технологий лучше их разработчиков;
- готовит обучающую программу по кибербезопасности АСУ ТП для снижения дефицита компетенций у заказчика (плановая дата запуска курса — апрель 2026 года).

ОСНОВНЫЕ ДОСТИЖЕНИЯ PT ISIM ЗА 2025 ГОД

- Встроенный антивирус для АСУ ТП.
- Расширенный Asset Management (AM) — инвентаризация активов через пассивный анализ трафика, сетевой сканер и агент ISIM Endpoint.
- Запуск Vulnerability Management (VM) — обнаружение уязвимостей на ОС Windows, Linux, ПЛК и сетевых устройствах с рекомендациями по устранению.
- Улучшенное представление карты сети и контроль конфигурации — визуализация статусов и состояния безопасности, автоматическое структурирование данных и визуального представления сети, журнал изменений.
- Развитие PT ISIM Endpoint (EDR) — глубокий аудит ПО, железа, учетных записей и сетевых соединений на SCADA-серверах и АРМ.
- Расширение поддержки промышленных протоколов — Profinet, CIP, SLMP, COS и других.
- Развитие новой архитектуры продукта с применением коллекторов для централизованного мониторинга и контроля безопасности распределенных инфраструктур с удаленными или изолированными сегментами.

НАШИ УСЛУГИ И ЭКСПЕРТИЗА

Набор инструментов и экспертизы, который позволяет заранее выявить уязвимости, выстроить надежную защиту и оперативно среагировать, если атака все же случилась.

Offensive[1]

- Тестирование на проникновение
- Red Team
- Анализ защищенности отдельных систем и сервисов
- Positive Labs
- АСУ ТП

Defensive[2]

- Расследование и реагирование на инциденты
- Ретроспективный анализ

Аналитические сервисы

- PT Surveying
- Хардкор ИТ

Облачные сервисы

- PT Fusion (SaaS)
- PT Maze (SaaS)

- Positive Education

- Standoff 365

1 Услуги, направленные на поиск и эксплуатацию уязвимостей в инфраструктуре компании путем имитации хакерских атак.
2 Услуги по обнаружению, расследованию и реагированию на инциденты ИБ.

Тестирование на проникновение

Пентест — это услуга по выявлению возможных векторов атак на ресурсы компании с использованием различных моделей нарушителя. Мы помогаем заказчикам обнаружить способы, которыми злоумышленники могут проникнуть в корпоративную сеть извне, повысить привилегии внутри системы вплоть до захвата полного контроля над инфраструктурой.

Ключевые направления

- Внешнее тестирование на проникновение
- Внутреннее тестирование на проникновение /развитие атаки на внутренние сети
- Социотехнические атаки
- Атаки на беспроводные сети

Конкурентные преимущества и экспертиза

Реализация услуг обеспечивается силами PT SWARM — специализированного подразделения Positive Technologies.

Штат команды насчитывает более 100 высококвалифицированных экспертов по анализу защищенности, специализирующихся на различных направлениях: тестирование на проникновение инфраструктуры, имитация атак APT-группировок, поиск уязвимостей в веб-приложениях, системах дистанционного банковского обслуживания, смарт-контрактах и т. д.

Наличие большого числа высококвалифицированных специалистов позволяет гибко формировать проектные группы, привлекая узкоспециализированных экспертов для достижения максимальных результатов.

Наши эксперты находят уязвимости нулевого дня (0-day) в различном ПО на проектах. Результативность команды подтверждена многочисленными регистрациями в базе CVE и выступлениями на международных конференциях.

Профессиональный уровень команды подтвержден сертификатами ведущих международных организаций: OSCP, OSCE, OSWE, OSEP, CRTE, OSWA и других.

Многолетняя практика и использование собственных исследовательских наработок обеспечивают высокую статистику успешной реализации векторов атак на проектах.

Итоги 2025 года

- Получено 110 запросов на услугу, проведено 38 проектов.
- Наблюдается стабильный спрос на услугу. Высокий процент успешного выявления уязвимостей подтверждает ценность предложения для клиентов

Red Team

Комплексная оценка эффективности защиты от целенаправленных атак на корпоративную информационную систему заказчика в формате 24/7. Услуга представляет собой реалистичную имитацию действий APT-группировок с использованием всех доступных способов атак для достижения целей заказчика или наступления недопустимых событий. Задача нашей команды — подтвердить возможность реализации целей и остаться незамеченными, задача команды ИБ заказчика — мониторить и реагировать на наши атаки.

Ключевой функционал и возможности

- Имитация атак APT-группировок в режиме 24/7.
- Использование различных способов проникновения в локальные вычислительные сети (ЛВС), доступных реальным злоумышленникам: сетевой периметр, социальная инженерия, беспроводные сети, физический доступ (розетки в общедоступных зонах) и многие другие экзотические векторы.
- Проверка возможности реализации недопустимых событий в технологическом сегменте с привлечением экспертов по АСУ ТП (опция).
- Применение техник сокрытия хакерской активности, отвлечения внимания и т. д. — изучение бизнес-процессов заказчика для проверки возможности реализации недопустимых событий.

Методология:

- заказчик устанавливает цели или определяет недопустимые события;
- полноценное сопротивление со стороны команды безопасности заказчика;
- реалистичное моделирование действий потенциальных злоумышленников.

Результаты:

- комплексная оценка: уровень защищенности инфраструктуры + эффективность работы служб ИБ/SOC = показатель готовности заказчика к реальным атакам.

Итоги 2025 года

Рост числа проектов в 2025 году в 2,5 раза отражает переход заказчиков к более зрелым практикам кибербезопасности и потребность в глубокой проверке устойчивости инфраструктуры к реальным угрозам.

Анализ защищенности отдельных систем и сервисов

Услуга по выявлению уязвимостей и недостатков в обеспечении безопасности конкретных систем с последующим предоставлением рекомендаций по их устранению.

Функционал

Анализ защищенности охватывает широкий спектр систем и сервисов:

- веб-приложения,
- мобильные приложения,
- системы дистанционного банковского обслуживания (ДБО),
- приложения с инновационными технологиями (блокчейн и смарт-контракты, биометрия),
- POS-терминалы,
- банкоматы.

Результаты:

- выявлены уязвимости разных видов, допущенные при разработке или эксплуатации системы,
- практические рекомендации по устранению выявленных недостатков,
- приоритизация рисков по критичности.

Примеры проектов:

- проект по анализу защищенности и проверке корректности работы генератора чисел у «Национальной лотереи»;
- проект по анализу защищенности блокчейн-платформы.

Итоги 2025 года

По итогам года зафиксировано 192 обращения заказчиков, из которых реализовано 126 проектов, что подтверждает устойчивый интерес рынка к специализированному анализу защищенности критичных систем.

Positive Labs

R&D-центр Positive Labs занимается комплексным анализом защищенности микроэлектроники и встраиваемых систем. Команда экспертов проводит глубокое исследование электронных устройств — от простых сенсоров до сложных встраиваемых систем — для усиления защиты разрабатываемых продуктов и верификации безопасности сторонних решений.

Функционал

Анализ защищенности микроэлектроники:
- анализ архитектуры на аппаратном уровне,
- поиск уязвимостей в железе,
- исследование firmware,
- проверка устойчивости к Side-Channel-атакам,
- тестирование на атаки класса Fault-Injection.

Исследование электронных устройств:
- полный спектр: от простых сенсоров до сложных встраиваемых систем,
- анализ критичных компонентов инфраструктуры.

Комплексное исследование экосистем:
- оценка безопасности не только отдельных компонентов,
- анализ всей экосистемы взаимодействующих устройств.

Конкурентные преимущества

- Уникальная экспертиза: практический опыт специалистов в аппаратных атаках и защите.
- Проведение фаззинг-тестирования продуктов Positive Technologies как элемент обеспечения процессов безопасной разработки ПО.
- Собственные технологии: самостоятельно спроектированные исследовательские стенды.
- Высокоточное оборудование и специализированные средства анализа: не требуется привлечение сторонних подрядчиков, что также позволяет обеспечить высокий уровень конфиденциальности проектов.
- Полный цикл: от низкоуровневого анализа железа до исследования прошивок и протоколов.

Итоги 2025 года

В 2025 году существенно выросло число исследований, приведших к устранению критичных уязвимостей в широко используемых продуктах.

Выявлены и ответственно раскрыты уязвимости в продуктах ведущих производителей:
- Broadcom — прошивки высокоскоростных сетевых адаптеров (США),
- Renesas Electronics — однокристальные микроконтроллеры,
- Espressif Systems — микроконтроллеры.

АСУ ТП

Услуга по комплексному анализу защищенности автоматизированных систем управления технологическими процессами (АСУ ТП) с глубоким погружением в специфику производства. Экспертиза охватывает как информационную, так и функциональную безопасность промышленных систем, выявляя уязвимости, которые могут привести к технологическим авариям и остановке производства.

Ключевые возможности

- Анализ защищенности промышленных систем управления
- Оценка рисков для технологического процесса
- Поиск уязвимостей в специализированном промышленном оборудовании и ПО
- Рекомендации по повышению уровня защищенности АСУ ТП

Уникальная методология:

- глубокое погружение в технологический процесс: детальное изучение специфики производства заказчика;
- учет уникальности: понимание, что каждое производство уникально по отраслевым и проектным особенностям;
- двойной фокус: анализ влияния уязвимостей не только на ИБ, но и на функциональную безопасность АСУ ТП;
- оценка последствий: определение возможных технологических проблем и аварийных ситуаций при эксплуатации уязвимостей.

Конкурентные преимущества

- Мультидисциплинарная экспертиза: объединение компетенций экспертов по пентестам, Red Team и промышленной автоматизации.
- Комплексный подход: анализ не только технологического сегмента, но и корпоративной инфраструктуры в единой методологии.
- Исследовательские компетенции: собственные исследования промышленного оборудования и ПО, выявление 0-day уязвимостей.
- Понимание производства: экспертиза в технологических процессах, а не только в ИТ-безопасности

Развитие сервиса:

- отработка комплексной методологии — объединение экспертизы в АСУ ТП с пентестами и Red Team проектами,
- формирование экспертизы по взаимосвязи корпоративного и технологического сегментов,
- накопление знаний об уникальных технологических процессах различных отраслей.

Результаты 2025 года

Исследовательская деятельность:

- выявлено **122 0-day уязвимости** в отечественном и зарубежном промышленном ПО и оборудовании;
- **средняя оценка критичности** всех обнаруженных уязвимостей: **8,3/10** (высокий) по шкале CVSS 4.0;
- вклад в повышение безопасности промышленных систем на рынке.

Охват исследований

Вендоры:

- проанализированы решения семи производителей (преимущественно в области автоматизации энергетики).

Оборудование:

- исследовано пять устройств: ПЛК, промышленное коммуникационное оборудование, устройства сбора и передачи данных (УСПД).

Специализированное ПО:

- проанализировано семь систем: SCADA-системы, энергетические системы управления (EMS), среды разработки и рантаймы.

Расследование и реагирование на инциденты

Услуга по восстановлению хронологии и обстоятельств инцидента информационной безопасности.

Ключевой функционал и возможности

- Восстановление полной картины инцидента
- Установление хронологии событий
- Оперативные рекомендации для локализации атаки
- Анализ методов и инструментов злоумышленников
- Рекомендации по предотвращению повторных инцидентов

Конкурентные преимущества

- Одна из наиболее востребованных услуг в портфеле
- Опыт участия в расследовании резонансных инцидентов
- Опытная команда экспертов по реагированию и расследованию

Итоги 2025 года

В 2025 году команда приняла участие в расследовании ряда резонансных инцидентов[1].
С 2026 года запущено новое направление — расследования в рамках киберстрахования, что расширяет экспертизу и охват услуги.

По итогам 2025 года зафиксировано **76 обращений заказчиков**, из которых реализовано **62 проекта**, что подтверждает критическую важность сервиса для бизнеса заказчиков и доверие к нашей команде PT ESC.

1 Детальная информация о ходе и результатах данных работ не раскрывается в соответствии с условиями соглашений о конфиденциальности (NDA) и политикой защиты интересов заказчиков.

Ретроспективный анализ

Услуга по поиску следов прошлых и текущих атак в ИТ-инфраструктуре заказчика. Проактивная проверка на факт компрометации систем.

Функционал

- Выявление индикаторов компрометации в инфраструктуре
- Обнаружение следов как завершенных, так и активных атак
- Анализ исторических данных безопасности

Форматы услуги:

- полный ретроспективный анализ — глубокая проверка всей инфраструктуры с верификацией найденных следов компрометации с заказчиком;
- экспресс-анализ — ускоренная оценка критичных сегментов на признаки компрометации.

Конкурентные преимущества

- Гибкость подхода под различные потребности и бюджеты заказчиков
- Технологии поиска сложных и скрытых угроз

Итоги 2025 года

В течение года было 100 обращений заказчиков, из них реализовано 24 проекта. Осенью 2025 года зафиксирован всплеск спроса на услугу на фоне резонансных взломов крупных компаний. Заказчики массово переходят к проактивной модели безопасности, инициируя проверки инфраструктуры на предмет скрытой компрометации.

PT Surveying

PT Surveying — сервис быстрой и объективной оценки уровня киберзащищенности компаний любой отрасли. Комплексное решение для анализа готовности организации противостоять кибератакам, оценки надежности контрагентов и принятия бизнес-решений на основе киберрисков.

Ключевые возможности

- Экспресс-оценка внешнего периметра
  - Сканирование на наличие уязвимостей
  - Классификация уязвимостей по уровню критичности
- Оценка внешних цифровых угроз
  - Мониторинг теневого интернета (Dark Web)
  - Анализ закрытых хакерских каналов
  - Поиск утечек данных организации
  - Выявление объявлений о продаже доступов в инфраструктуру
  - Обнаружение призывов к кибератакам на компанию
- Ретроспективный анализ событий ИБ на ключевых хостах
  - Поиск индикаторов компрометации внутри инфраструктуры организации
  - Раннее выявление злоумышленников
- Оценка внутренних практик ИБ
  - Анализ процессов и политик безопасности
  - Оценка превентивных и реактивных методов защиты
  - Проверка подходов к восстановлению после атак
  - Оценка на основе структурированных анкет

Целевая аудитория и сценарии применения

- Самооценка: определение собственного уровня киберзащищенности.
- Корпоративный контроль: мониторинг ИБ дочерних и связанных компаний.
- Due Diligence: выбор безопасных поставщиков, подрядчиков, провайдеров услуг.
- Мониторинг контрагентов: отслеживание цифровой репутации партнеров.
- Страхование: определение условий киберстрахования и оценка рисков.
- Инвестиции: принятие решений при M&A и инвестиционных сделках.
- Кредитование: оценка киберрисков при выдаче займов и кредитов.
- Экспертиза: использование инструментов и знаний реальных атакующих.

Проблема рынка

Бизнесу критически важно понимать киберриски контрагентов, но нет быстрого и доступного способа получить объективную оценку. Традиционные методы (аудиты, проверки) занимают недели и стоят дорого. При этом киберинциденты у партнеров напрямую влияют на бизнес: от нарушения цепочек поставок до репутационных потерь.

PT Surveying

Новые требования рынка

- Регуляторы усиливают требования к контролю рисков в цепочках поставок.
- Инвесторы включают киберриски в критерии оценки при сделках.
- Страховые компании требуют объективные данные для киберстрахования.
- Банки начинают учитывать киберзащищенность при кредитовании.

Бизнес-обоснование

1. Новая ниша: создание продукта на стыке ИБ-услуг и бизнес-аналитики.
2. Массовый рынок: каждая компания оценивает десятки контрагентов — потенциал огромен.
3. Подписочная модель: регулярный мониторинг контрагентов = рекуррентная выручка.
4. Кросс-сейл: клиенты сервиса становятся потенциальными заказчиками других услуг при выявлении проблем.
5. Монетизация экспертизы: преобразование методологии анализа угроз в масштабируемый сервис.
6. Первопроходцы: раннее занятие ниши до прихода конкурентов.

Результаты 2025 года

Запуск сервиса:
- коммерческий запуск осенью 2025 года;
- немедленный отклик рынка: поступление запросов на оценку.

Первые проекты:
- реализация пилотных и коммерческих проектов;
- валидация ценности сервиса в реальных бизнес-сценариях;
- отработка процессов и методологии оценки.

Рыночная валидация:
- подтверждение спроса из различных сегментов (корпорации, инвесторы, страховщики);
- формирование первых кейсов применения;
- сбор обратной связи для приоритизации развития.

ХардкорИТ

ХардкорИТ — услуга по неинвазивному анализу ИТ-инфраструктуры с выдачей рекомендаций по ее трансформации и повышению защищенности. Заказчик предоставляет конфигурации систем, эксперты проводят глубокий анализ без активного вмешательства в работающую инфраструктуру. В основе услуги лежит методология, которая позволяет максимально усложнить достижение недопустимых событий для хакера, попавшего в инфраструктуру, чтобы заказчик успел его обнаружить и отреагировать.

Ключевые возможности

- Анализ конфигураций ИТ-инфраструктуры
- Выявление недостатков архитектуры и настроек безопасности
- Разработка стратегии трансформации инфраструктуры
- Моделирование потенциальных векторов атак реализации недопустимых событий
- Практические рекомендации по устранению уязвимостей и повышению защищенности
- Рекомендации по развитию ИБ, дорожная карта

Методология:

- неинвазивный подход: анализ проводится на основе предоставленных конфигураций без активного тестирования;
- выполнение расчета времени атаки и времени обнаружения;
- возможность анализа критичных систем без остановки бизнес-процессов.

Конкурентные преимущества

- Безопасность: нулевой риск сбоев и нарушения работы систем (в отличие от пентеста).
- Комплексность: оценка не только уязвимостей, но и архитектурных решений.
- Стратегический взгляд: рекомендации по трансформации, а не только по устранению проблем.
- Доступность: можно проводить для высоконагруженных и критичных систем.

Альтернатива традиционным подходам

Услуга позиционируется как современная альтернатива классическим сервисам, включая пентесты, для организаций, которым важна глубокая экспертная оценка без рисков для инфраструктуры.

Проблема рынка

Традиционные методы оценки безопасности (пентесты, сканирование) имеют ограничения:

- риски для production-систем при активном тестировании,
- невозможность полноценно тестировать критичную инфраструктуру,
- фокус на точечных уязвимостях, а не на системных проблемах архитектуры,
- высокие требования к подготовке инфраструктуры для тестирования.

ХардкорИТ

Запрос заказчиков

Компании нуждаются в глубоком экспертном анализе без рисков остановки бизнеса, особенно для высоконагруженных систем, критичной производственной инфраструктуры, сложных распределенных архитектур, систем, требующих непрерывной работы 24/7.

Бизнес-обоснование

1. Новая ниша: занятие позиции между аудитом и пентестом.
2. Расширение аудитории: доступ к заказчикам, для которых традиционный пентест неприемлем.
3. Меньше барьеров: простота запуска проекта (не нужна сложная подготовка инфраструктуры).
4. Высокая маржинальность: экспертный анализ с меньшими операционными затратами.
5. Долгосрочные отношения: рекомендации по трансформации ведут к повторным проектам.
6. Дифференциация: уникальное предложение на фоне стандартных услуг ИБ.

Итоги 2025 года

Фиксируется устойчивый рост спроса на услуги на базе методологии ХардкорИТ. Заказчики все чаще выбирают неинвазивный анализ как основной или дополнительный метод оценки защищенности.

Развитие методологии:

- расширение охвата анализируемых технологий и платформ,
- формализация процесса анализа конфигураций,
- разработка чек-листов и стандартов оценки,
- создание базы знаний типовых недостатков конфигураций.

Позиционирование:

- утверждение как альтернативы традиционным сервисам (пентесты, сканирование),
- формирование понимания ценности неинвазивного подхода у заказчиков,
- расширение применения на критичные и высоконагруженные системы.

PT Fusion

Облачный портал для работы с данными киберразведки. Комплексное решение для аналитиков SOC, специалистов по Threat Intelligence (TI) и команд реагирования на инциденты, объединяющее все необходимые инструменты для оперативного анализа угроз в единой платформе.

Ключевые возможности

- Проверка образцов ВПО
- Поиск по индикаторам компрометации (IoC)
- Исследование данных PDNS (Passive DNS)
- Библиотека угроз: хакерские группировки, семейства ВПО, уязвимости

Конкурентные преимущества

- Комплексность: все инструменты TI в одном месте — не требуется переключение между источниками.
- Экспертиза: разработан ИТ-аналитиками экспертного центра PT ESC на основе реального опыта расследований.
- Облачная архитектура: мгновенный доступ без необходимости развертывания on-premise.
- Автоматизация: устранение ручной обработки разрозненных данных, ускорение процессов анализа.

Проблема рынка

Увеличение числа кибератак, рост их скорости и сложности, использование ИИ злоумышленниками создают острую потребность в оперативном анализе угроз. Однако данные разбросаны по множеству источников, а их ручная обработка отнимает критическое время у команд безопасности.

Бизнес-обоснование

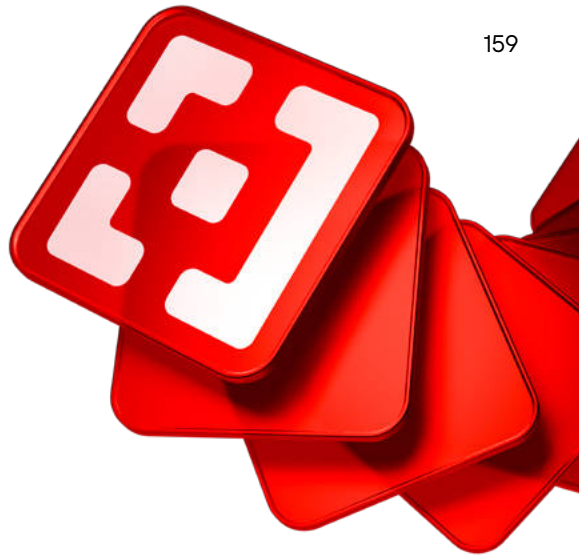
1. Монетизация экспертизы: преобразование накопленных знаний экспертного центра PT ESC в масштабируемый продукт.
2. Новая бизнес-модель: переход от разовых услуг к подписочной модели с предсказуемой регулярной выручкой.
3. Расширение аудитории: доступ к сегменту компаний, которые не готовы покупать дорогие услуги, но нуждаются в TI-инструментах.
4. Удержание клиентов: создание постоянной точки контакта с заказчиками между проектами услуг.

Результаты 2025 года

Запуск MVP:
- публичный анонс и вывод продукта на рынок;
- немедленный интерес целевой аудитории — поток заявок на пилотирование.

Пилотирование и валидация:
- запуск программы пилотных проектов с заказчиками;
- совместное тестирование функционала в реальных SOC-процессах;
- сбор обратной связи для приоритизации развития.

Развитие сервиса:
- обогащение функционала на основе обратной связи первых пользователей.



PT Maze

Облачное решение для защиты iOS- и Android-приложений от реверс-инжиниринга, создания клонов и взлома. Протектор кода на базе экспертизы этичных хакеров Positive Technologies в области исследования безопасности мобильного ПО.

Ключевые возможности

- Защита от реверс-инжиниринга мобильных приложений
- Предотвращение создания клонов приложений
- Защита интеллектуальной собственности разработчиков
- Противодействие поиску уязвимостей злоумышленниками
- Защита пользовательских данных и финансовых транзакций

Технологии

- Протектор кода, объединяющий лучшие мировые практики
- Поддержка двух ведущих мобильных платформ: Android и iOS
- Облачная модель доставки для удобства интеграции

Конкурентные преимущества

- Экспертиза: разработан на основе более чем десятилетнего опыта команды этичных хакеров по реверс-инжинирингу.
- Знание противника: создатели защиты знают все методы атак изнутри.
- Полная сервисная поддержка: не просто продукт, а комплексное решение с экспертным сопровождением от Positive Technologies.
- Проверенная эффективность: технологии защиты основаны на реальных кейсах взломов и их предотвращения.

Целевая аудитория

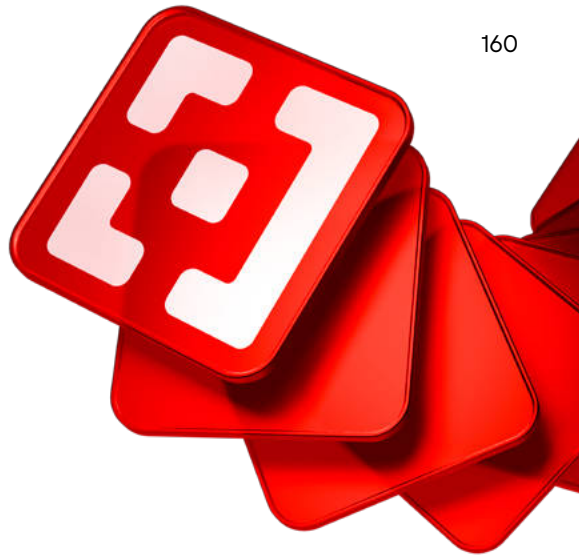
Универсальное решение для любой компании с мобильным приложением независимо от отрасли. Особенно актуально для секторов с повышенными требованиями к безопасности: финансы, ретейл, страхование, игровая индустрия, корпоративный сегмент и государственный сектор.

Проблема рынка

Недостаточная защищенность кода остается одной из самых критичных проблем мобильных приложений. Тренд усиливается: в рейтинге OWASP Mobile Top 10 эта угроза поднялась с десятого места (2014) на седьмое (2024).

Масштаб угрозы

- Реверс-инжиниринг позволяет злоумышленникам искать уязвимости.
- Создание клонов приложений, неотличимых от оригинала.
- Кража интеллектуальной собственности разработчиков.
- Атаки на пользователей для хищения денег и персональных данных.



PT Maze

Бизнес-обоснование

1. Монетизация уникальной экспертизы: преобразование более чем десятилетнего опыта анализа защищенности мобильных приложений в коммерческий продукт.
2. Растущий рынок: рост угрозы (OWASP Top 10) означает рост спроса на защиту.
3. Подписочная модель: переход к предсказуемой рекуррентной выручке от облачного сервиса.
4. Масштабируемость: продукт позволяет охватить массовый сегмент, недоступный для услуг (малый и средний бизнес).
5. Синергия с услугами: усиление экосистемы — клиенты анализа защищенности мобильных приложений становятся потенциальными покупателями защиты.

Развитие рынка и перспективы

Рыночная конъюнктура:

- рынок защиты мобильных приложений растет вслед за цифровизацией бизнеса и усилением угроз. Проблема реверс-инжиниринга поднялась в OWASP Top 10 с десятого на седьмое место, что отражает ее критичность для индустрии.

Окно возможностей:

- финансовый сектор активно ищет решения для защиты банковских приложений;
- ретейл и маркетплейсы наращивают инвестиции в мобильные каналы;
- регуляторы усиливают требования к безопасности мобильного ПО;
- широкий рынок — защита актуальна для любой компании с мобильным приложением.

Стратегия развития

1. Углубление в приоритетных вертикалях (финансы, ретейл, госсектор).
2. Географическая экспансия на рынки региона.
3. Развитие функционала под новые угрозы и платформы.
4. Построение партнерской сети для масштабирования.
5. Создание экосистемы интеграций с dev-инструментами.

ссылка

Positive Education

Positive Education — центр практического обучения, который готовит специалистов и управленцев к работе в условиях реальных киберугроз.

Объединяет экспертизу Positive Technologies, практику и технологии для формирования устойчивой кибербезопасности в компаниях и на уровне государств.

Ключевые направления:

- подготовка ИБ-специалистов через практикумы
- развитие управленческих компетенций (CISO, CIO, CEO)
- обучение работе с продуктами и технологиями защиты
- образовательные программы с университетами

Центр практического обучения, созданный на базе экспертизы Positive Technologies.

Центр формирует устойчивые навыки противодействия киберугрозам у специалистов, управленцев и руководителей, помогая организациям выстраивать системную защиту и повышать уровень киберустойчивости.

Дефицит ИБ-специалистов в России остается критическим и составляет около 45%, что эквивалентно нехватке около 50 тыс. человек. Нехватка специалистов особенно критична в условиях роста киберугроз. По данным Positive Technologies, в первом полугодии 2025 года использование ВПО в атаках достигло 76%, а основными последствиями стали утечки конфиденциальных данных (52%) и нарушение деятельности компаний (45%). Эксперты прогнозируют дальнейший рост числа кибератак на 30–35% в 2026 году.

Развитие кибербезопасности невозможно без сильных специалистов.

Positive Education — центр обучения, где соединяются практика, технологии и опыт Positive Technologies, чтобы готовить лидеров кибербезопасности: тех, кто укрепляет киберсуверенитет через распространение знаний, повышение осведомленности о киберугрозах и создание устойчивой экосистемы защиты компаний и государства.

Результаты 2025 года

- Усилили компетенции в области кибербезопасности у 14 500 специалистов благодаря практикумам и образовательным программам.
- 400+ управленцев и представителей органов власти сформировали понимание построения кибербезопасности и необходимости прохождения кибериспытаний.
- 8 тыс. специалистов подтвердили свои компетенции по работе с продуктами Positive Technologies, обеспечивая более эффективное использование технологий защиты в ежедневной практике.
- Провели обучение среди 500 специалистов ИТ и ИБ в Индонезии, ОАЭ, Египте, что усиливает международное присутствие Positive Technologies и способствует развитию локальной экспертизы в каждой из стран.
- Провели глобальную образовательную инициативу Positive Hack Camp, где объединили 90 молодых специалистов более чем из 25 стран Азии, Африки, Ближнего Востока и Латинской Америки.
- Завершили обучение преподавателей из 500 учебных заведений Армении, Беларуси, Казахстана, Киргизии, России и Узбекистана, что позволило масштабировать подготовку специалистов через образовательные системы этих стран.

Платформа Standoff 365

Кибербитва Standoff

Standoff Hackbase

Standoff Defend

Standoff Bug Bounty

Платформа Standoff 365 — это более 32 тыс. зарегистрированных пользователей и целая экосистема ИБ-продуктов. Мы не занимаемся написанием ИБ-политик, комплаенс, документами и аттестациями, а фокусируемся на практических аспектах построения защищенных систем, на атаках, взломах, обнаружении хакеров и реагировании. При этом на платформе есть место не только для профессионалов, но и для начинающих специалистов, которые только ищут свой путь в отрасли и могут прокачать свои скилы.

Алексей Новиков,
управляющий директор Positive Technologies

Кибербитва Standoff

Платформа Standoff 365

Кибербитва Standoff — международные соревнования по кибербезопасности, которые помогают организациям повысить зрелость служб ИБ в условиях интенсивных кибератак, а белым хакерам — совершенствовать свои профессиональные навыки.

>2 тыс. специалистов по кибербезопасности

приняли участие в публичных кибербитвах и киберучениях Standoff за 2025 год

Кибербитва Standoff

В 2025 году:

- провели три международные кибербитвы: Standoff 15 во время PHDays Fest, Standoff в специальном новом формате во время Петербургского международного экономического форума, а также кибербитву Standoff 16, финал которой прошел в рамках Positive Security Day в октябре. Всего в кибербитвах официально приняла участие 141 команда из 40 стран;
- провели международные игры по кибербезопасности, которые были направлены на привлечение студенческого комьюнити. Из почти 200 команд, участвовавших в отборочном туре, в основной этап прошли 16 синих и 30 красных команд. По итогам игр три лучшие команды получили право участия в майской битве Standoff;
- активно развивали формат проверки навыков защитников. Киберучения прошли в Омане, Египте, Марокко, на Кубе и в Беларуси.

Standoff Bug Bounty

Платформа Standoff 365

Standoff Bug Bounty — платформа для поиска уязвимостей в ИТ-системах и инфраструктуре компаний, которые проверяют надежность своих ресурсов, предоставив доступ к ним исследователям безопасности.

В 2025 году мы активно развивали Standoff Bug Bounty:

- запустили 233 программы — это в 2,2 раза больше, чем в 2024 году, когда количество программ уже показывало кратный рост относительно 2023 года;
- позволили багхантерам заработать 160 млн руб. (против 95 млн руб. годом ранее) и сдать почти 8 тыс. отчетов (в сравнении с ~5 тыс. в 2024 году);
- увеличили количество иностранных багхантеров на платформе в три раза, развивая тренд на интернационализацию, начатый в 2024 году;
- провели в Индии второй международный ивент Standoff Hacks после первого запуска во Вьетнаме в 2024 году.

Standoff Bug Bounty

Standoff Defend

Платформа Standoff 365 | Полигоны для синих и для красных

Standoff Defend — онлайн-полигон с виртуальной ИТ-инфраструктурой для синих команд, доступный в режиме 24/7 и позволяющий повысить готовность бизнеса к отражению APT-атак.

- В апреле 2025 года провели запуск в формате онлайн-марафона: в течение месяца любой желающий мог протестировать продукт и оценить его ключевые возможности.
- Подготовили более 300 часов теории, 180 часов практики расследования реальных инцидентов и атак, а также 12 сценариев сложных атак от APT-группировок.
- Провели более 20 пилотов продукта для крупных компаний и собрали свыше 150 лидов, а более пяти компаний уже включили Standoff Defend в свои планы развития команд SOC.

Standoff Defend

Standoff Hackbase

Платформа Standoff 365 | Полигоны для синих и для красных

Standoff Hackbase — онлайн-полигон для красных команд с реалистичными копиями ИТ-систем, на котором можно получать навыки в пентесте в режиме 24/7.

- В июле 2025 года презентовали полностью пересобранный полигон для красных Standoff Hackbase — запустили сезоны и сезонный рейтинг.
- Полностью обновили структуру контента и разделили его на несколько сегментов:
  - Bootcamp — для новичков,
  - Standalone — для исследования отдельных виртуальных машин,
  - Industry — сегмент с разветвленной инфраструктурой, как в реальных компаниях.
- За 2025 год более 2,3 тыс. пользователей на полигоне сдали хотя бы один отчет. Во всех сегментах было реализовано более 13 тыс. критических событий.

С начала 2025 года количество пользователей платформы увеличилось с 18 тыс. до 32 тыс.

Standoff Hackbase

Полигоны для синих и для красных

В апреле 2025 года мы перезапустили онлайн-полигон Standoff 365. Платформа была разделена на два специализированных продукта: Standoff Defend (для команд защиты — синих) и Standoff Hackbase (для специалистов по анализу защищенности — красных).

ФИНАНСОВЫЕ РЕЗУЛЬТАТЫ

- Отгрузки и валовая прибыль отгрузок
- Выручка
- Операционные расходы
- Расходы на разработку и создание активов
- EBITDA и чистая прибыль
- EBITDAC и NIC
- Долговая нагрузка и управление долгом
- Основные финансовые результаты 2025 года

Мы придерживаемся принципов прозрачности и открыто делимся результатами своей работы со всеми заинтересованными сторонами. В дополнение к обязательной отчетности по МСФО мы традиционно раскрываем ряд управленческих метрик.

ОТГРУЗКИ И ВАЛОВАЯ ПРИБЫЛЬ ОТГРУЗОК

Мы используем показатель «отгрузки» — валовый объем законтрактованных поставок лицензий, оборудования, товаров и услуг в адрес дистрибьютора или конечного покупателя за отчетный период, включая НДС. Этот показатель более своевременно отражает рост Positive Technologies по сравнению с показателем выручки, который признает часть объема отгрузок как выручку будущих периодов.

Отгрузки с НДС отличаются от выручки по МСФО:

- на сумму НДС;
- отгрузки 2025 года со сроками оплаты позднее 31 марта 2026 года исключаются из показателя «отгрузки с НДС»;
- отгрузка сертификатов на абонентское обслуживание (услуги технической поддержки, подписка на услуги анализа инцидентов и другое) отражается в полной сумме в момент заключения контракта;
- отгрузки лицензий на ПО отражаются в полной сумме в момент заключения контракта;
- рибейты[1] покупателям не уменьшают сумму отгрузок, входят в состав себестоимости.

1 Рибейт — премия за достижение объемов продаж и субсидирование покупателей.

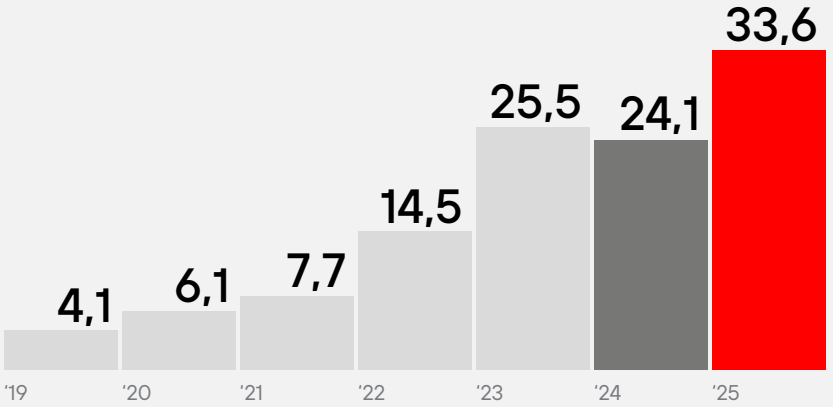
Итоговый объем оплаченных отгрузок клиентам Компании в 2025 году составил 33,6 млрд руб., что на 40% выше показателя прошлого года.

По итогам года Positive Technologies вновь демонстрирует темпы роста бизнеса, вдвое превышающие динамику роста рынка кибербезопасности в России. Мы достигли стратегически важных целей: обеспечили стабильность Компании, вернув уверенность в росте бизнеса в будущем.

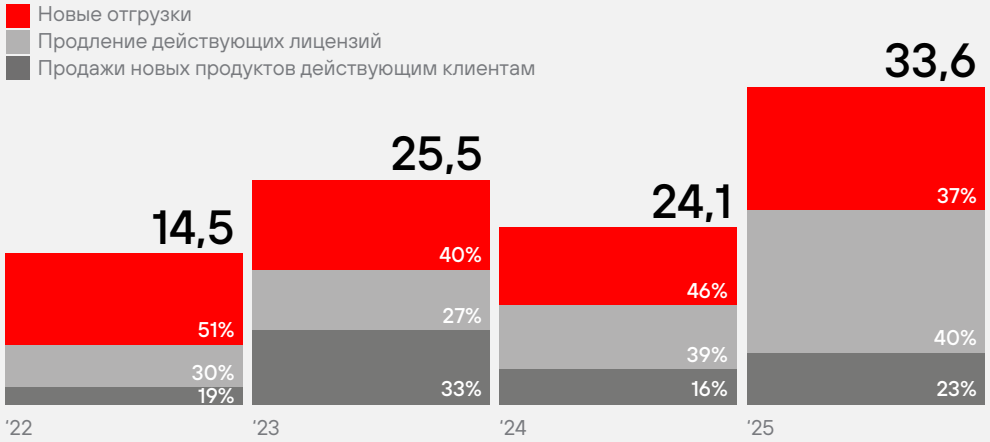
+40%

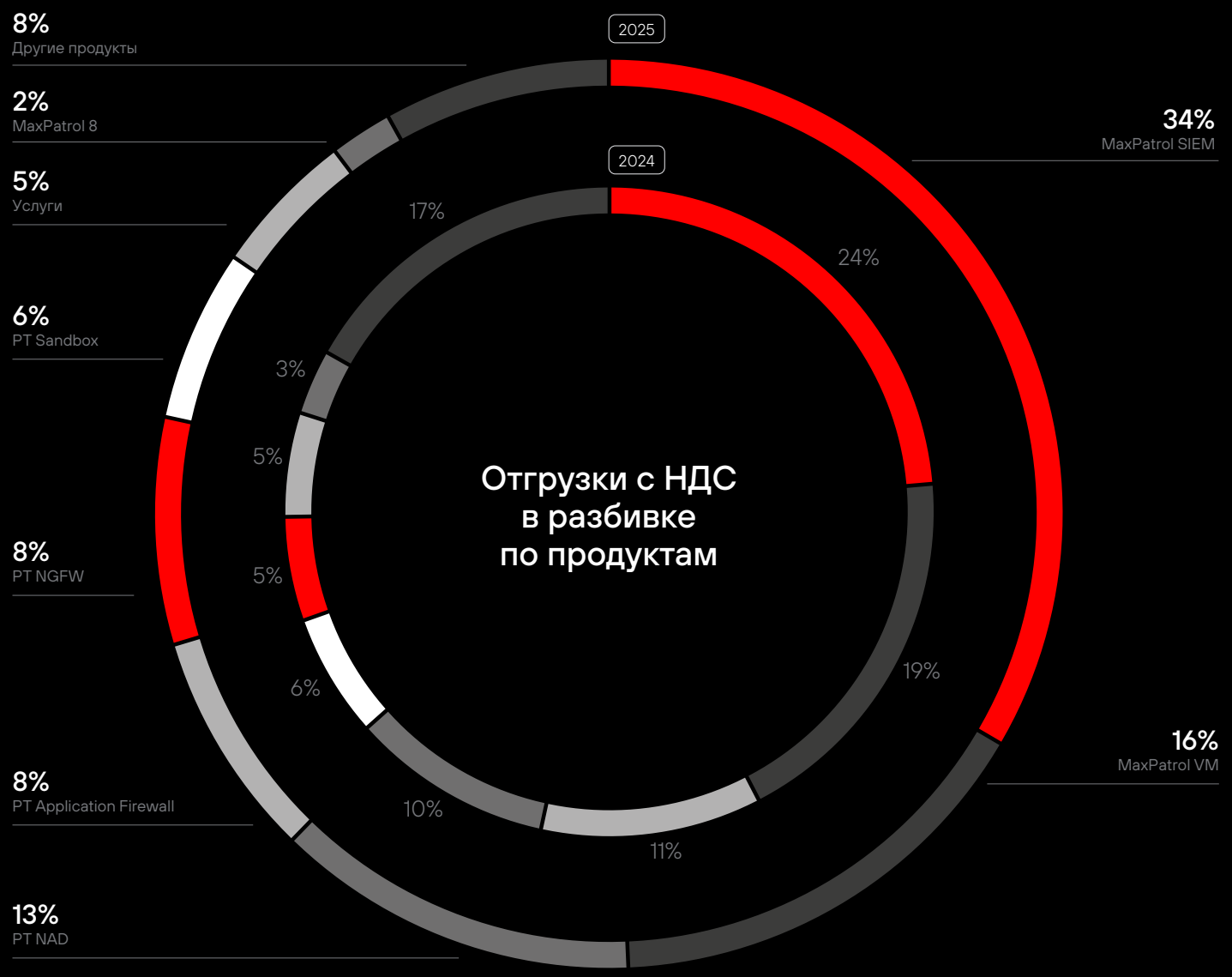
рост отгрузок год к году

Отгрузки, млрд руб.



Продления и новые отгрузки в 2025 году, млрд руб.





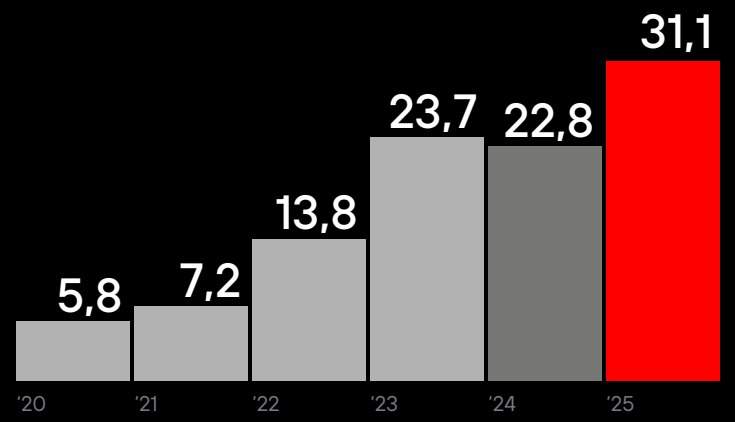
В структуре продаж продуктами-лидерами, показавшими наибольший вклад в общий результат, стали MaxPatrol SIEM (34%), MaxPatrol VM (16%) PT Network Attack Discovery (13%).

Валовая прибыль отгрузок, представляющая собой отгрузки, уменьшенные на сумму НДС, бонусов партнерам и прочих прямых расходов, по итогам 2025 года составила **31,1 млрд руб.**, что на 37% больше показателя прошлого года (22,8 млрд руб.).

+37%

рост валовой прибыли отгрузок год к году

Валовая прибыль отгрузок, млрд руб.



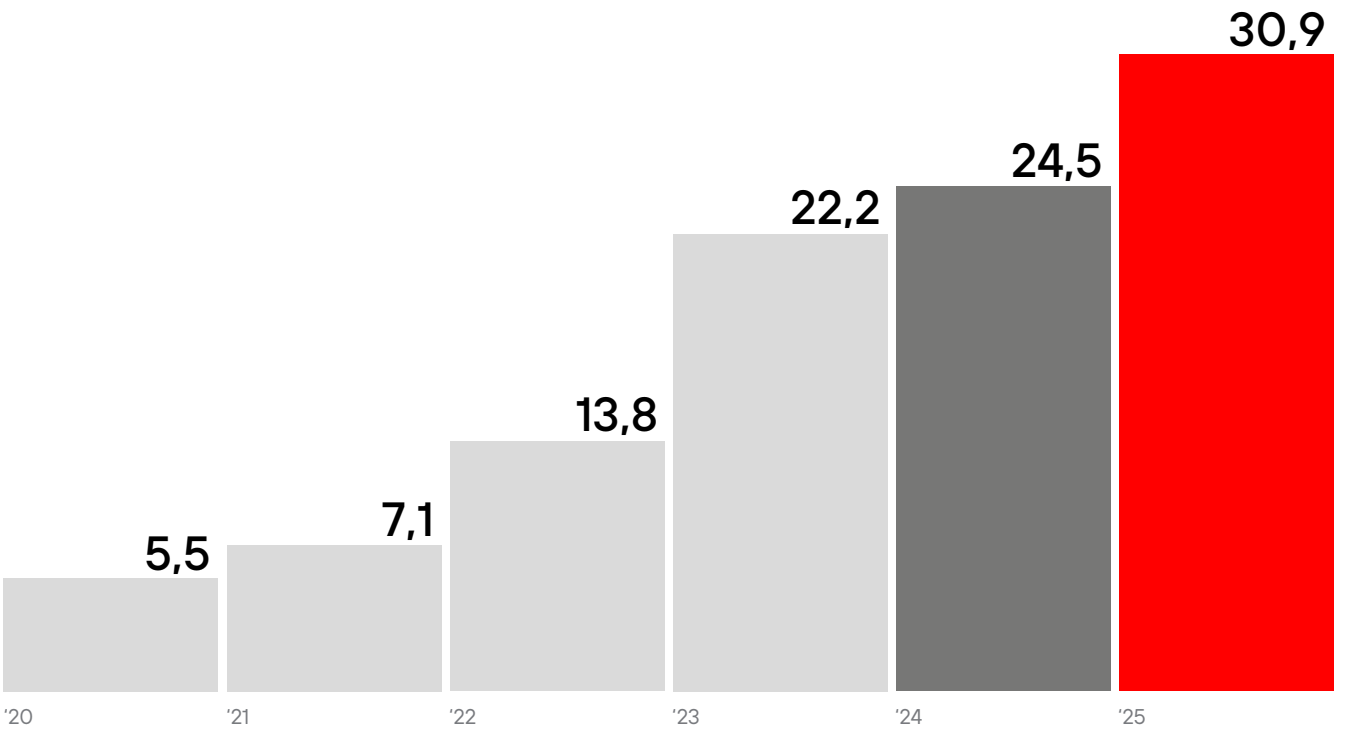
ВЫРУЧКА

Выручка по МСФО увеличилась **на 26%, до 30,9 млрд руб.** Разница между показателями «Отгрузки» и «Выручка по МСФО» включает в себя разницу в НДС, сроках признания технической поддержки, пролонгации лицензий и корректировку на оплаты, произведенные до 31 марта 2026 года.

+26%

рост выручки год к году

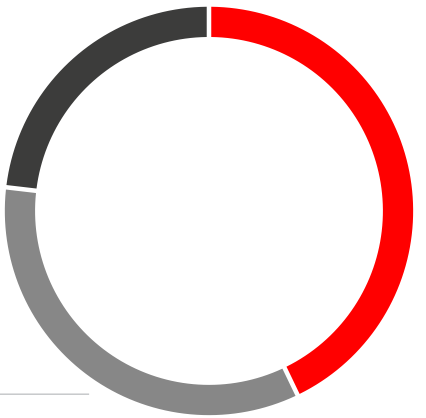
Выручка, млрд руб.



ОПЕРАЦИОННЫЕ РАСХОДЫ

Операционные расходы, не связанные с оплатой труда, снизились на 25%. В структуре операционных расходов основную долю (43%) составили расходы на R&D и технологические инфраструктурные проекты, 34% — продажи и развитие, а доля расходов на поддержку бизнеса и инфраструктуры составила 23%.

Структура операционных расходов



РАСХОДЫ НА РАЗРАБОТКУ И СОЗДАНИЕ НЕМАТЕРИАЛЬНЫХ АКТИВОВ

Масштабные инвестиции в разработку и развитие продуктов, а также технологические и инфраструктурные проекты — это фундамент для устойчивого роста нашего бизнеса. Общий объем инвестиций в R&D[1] составил 9,1 млрд руб., что сопоставимо с уровнем прошлого года. На фоне оптимизации операционных расходов Компания сохранила инвестиции в R&D для обеспечения возможности создавать новые прорывные продукты, новые рынки и выходить в сегменты рынка, где ранее доминировали другие вендоры.

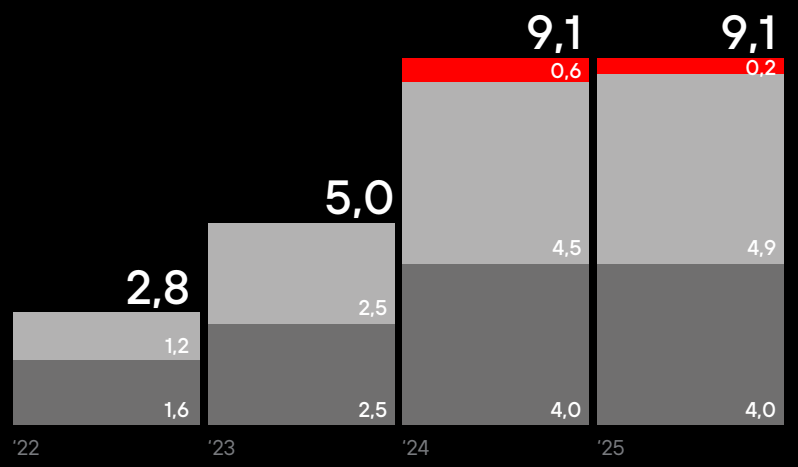
Продукты на разных стадиях жизненного цикла требуют разного объема капитальных затрат. В 2025 году наибольший их объем пришелся на MaxPatrol SIEM, PT NGFW и MaxPatrol VM.

1 Включает расходы на поддержание продуктов, разработку новой функциональности продуктов, технологические и инфраструктурные проекты.

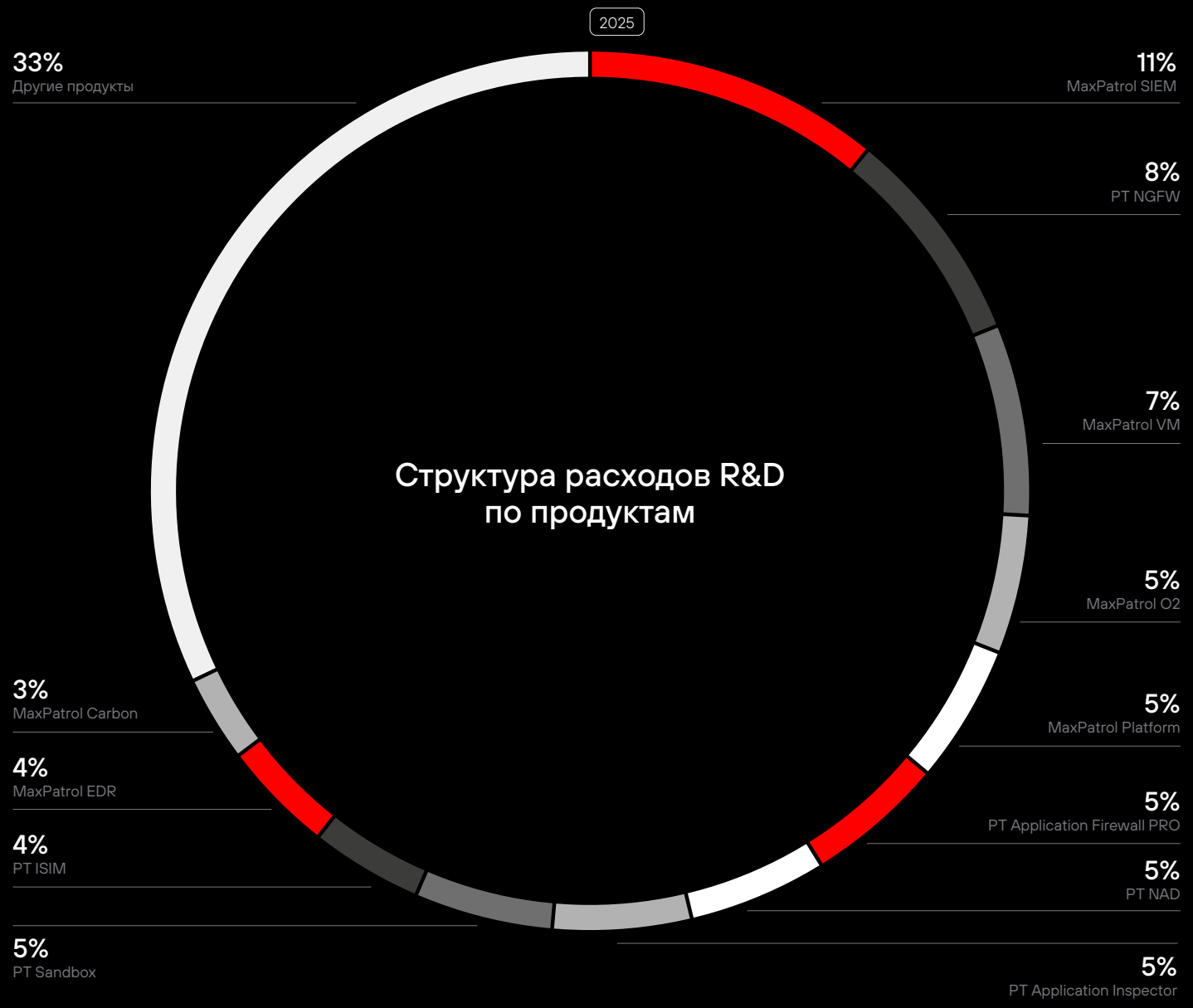
Инвестиции в разработку продуктов

Общие R&D-расходы[1], млрд руб.

- Инфраструктура «частного облака» и Data Lake
- Расходы на разработку новой функциональности продуктов
- Расходы на поддержание продуктов



1 Включая Standoff.



EBITDA И ЧИСТАЯ ПРИБЫЛЬ

По результатам 2025 года показатель EBITDA Positive Technologies составил **12,3 млрд руб. (+91% к результатам 2024 года).** Рентабельность EBITDA составила **40%**.

Чистая прибыль за 2025 год составила 7,3 млрд руб. (3,7 млрд годом ранее).

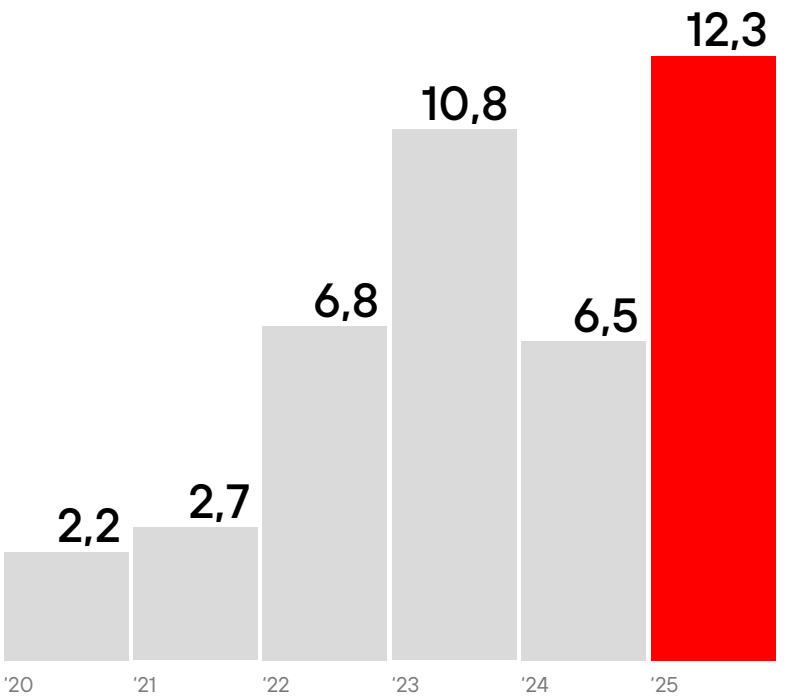
+91%

рост EBITDA год к году

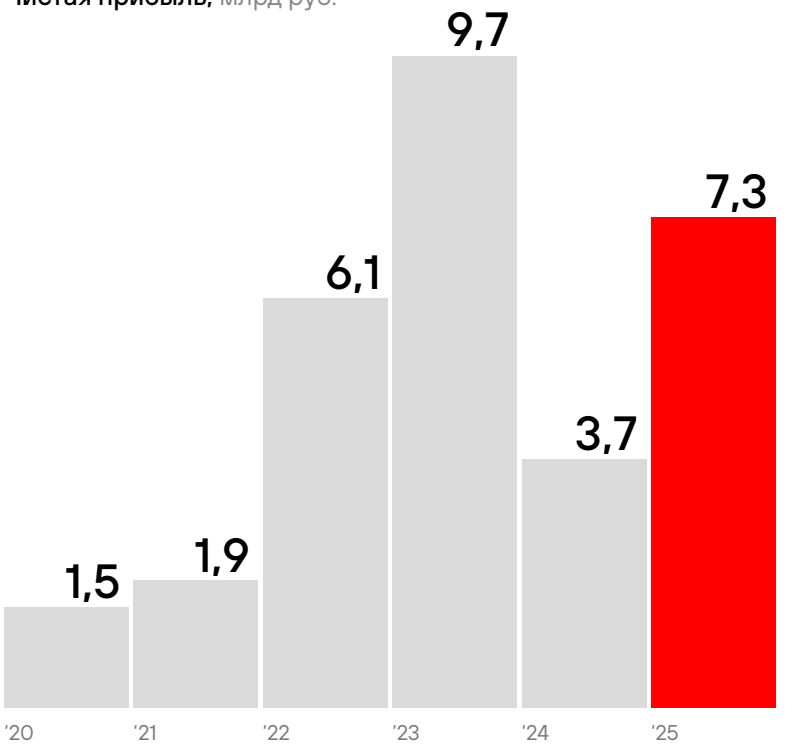
+99%

рост чистой прибыли в 2025 году

EBITDA, млрд руб.



Чистая прибыль, млрд руб.



EBITDAC И NIC

EBITDAC, управленческий показатель, который отличается от EBITDA на сумму разницы между отгрузками и выручкой, а также сумму капитализируемых расходов, составил 7,1 млрд руб., что на 8,4 млрд руб. выше показателя прошлого года.

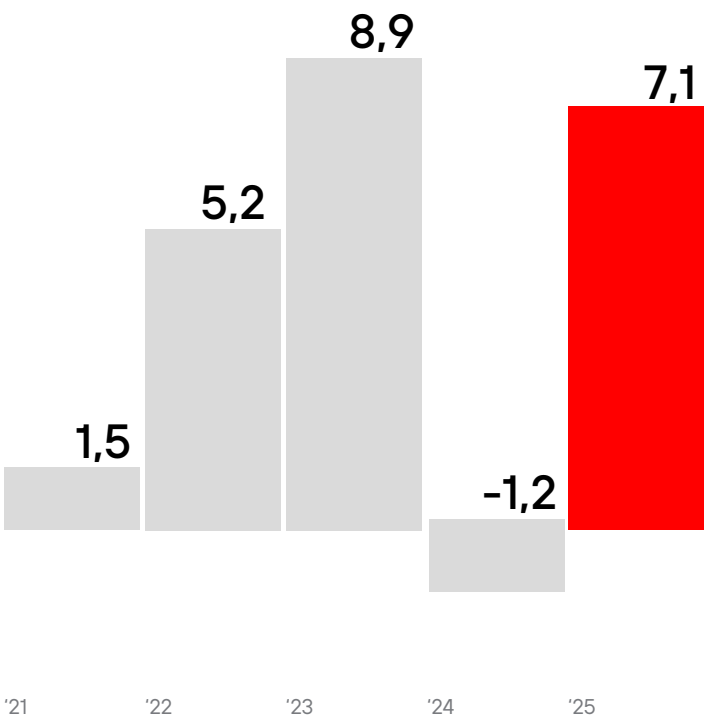
Второй важный управленческий показатель — NIC[1]. Именно показатель NIC лежит в основе дивидендной политики Positive Technologies. Рост управленческой прибыли позволяет Компании наращивать дивидендный потенциал и продолжать увеличение дивидендных выплат в результате расширения бизнеса и сохранения высокой финансовой эффективности.

Одной из финансовых задач 2025 года было возвращение NIC в положительную зону. Она выполнена с хорошим запасом, что позволяет вновь рассмотреть возможность выплаты дивидендов, подтвердив нацеленность на повышение инвестиционной привлекательности акций, в том числе в рамках дивидендной политики Компании.

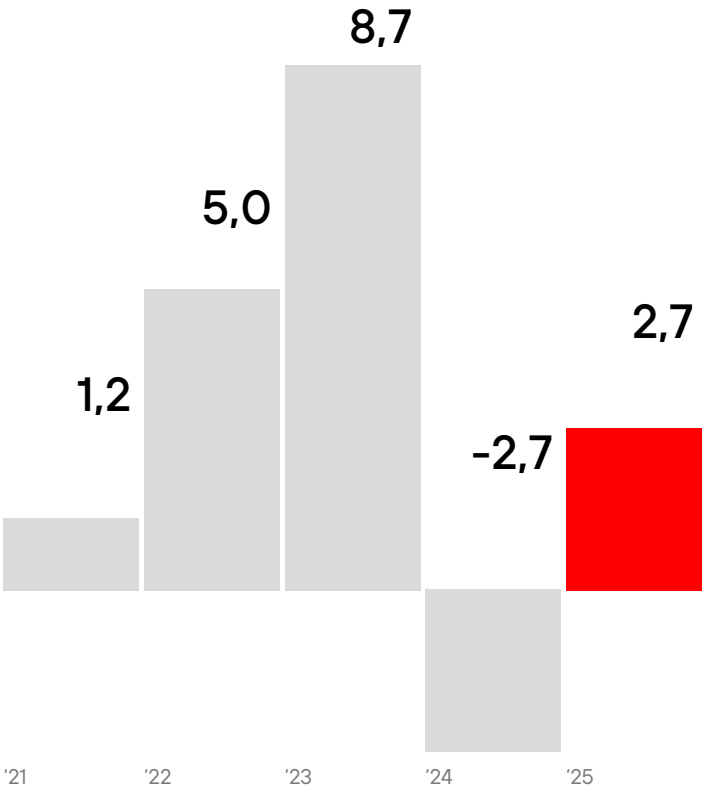
В 2025 году NIC составил 2,7 млрд руб., что на 5,4 млрд руб. больше показателя прошлого года.

Подробнее о Дивидендной политике Positive Technologies

EBITDAC, млрд руб.



NIC, млрд руб.



1 NIC — чистая прибыль без учета капитализации расходов (Net Income Before Capitalization of Expenses).

ДОЛГОВАЯ НАГРУЗКА И УПРАВЛЕНИЕ ДОЛГОМ

Отношение чистого долга к EBITDA по состоянию на конец 2025 года составляет 1,66.

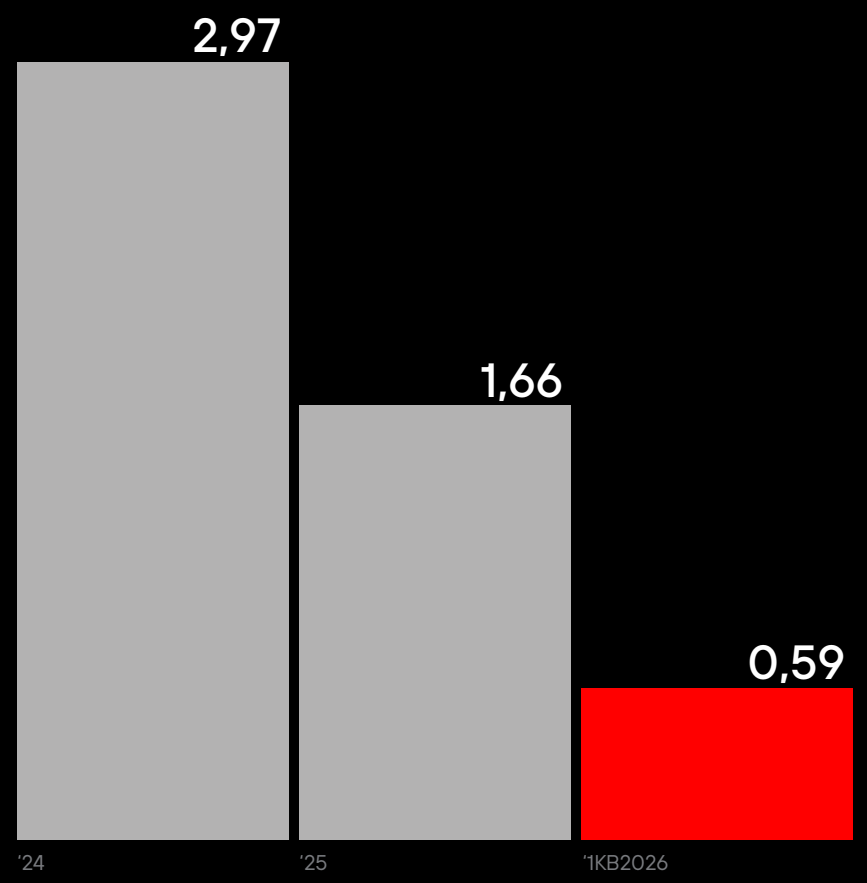
В 2025 году Positive Technologies продолжила реализацию стратегии по улучшению структуры и показателей долгового портфеля. В результате Компании удалось снизить долговую нагрузку до комфортного уровня — 1,66.

Positive Technologies существенно улучшила структуру долгового портфеля, снизив зависимость от краткосрочных банковских кредитов. С этой целью в 2025 году был размещен выпуск облигаций, что позволило Компании привлекать долгосрочное финансирование на более комфортных и предсказуемых условиях.

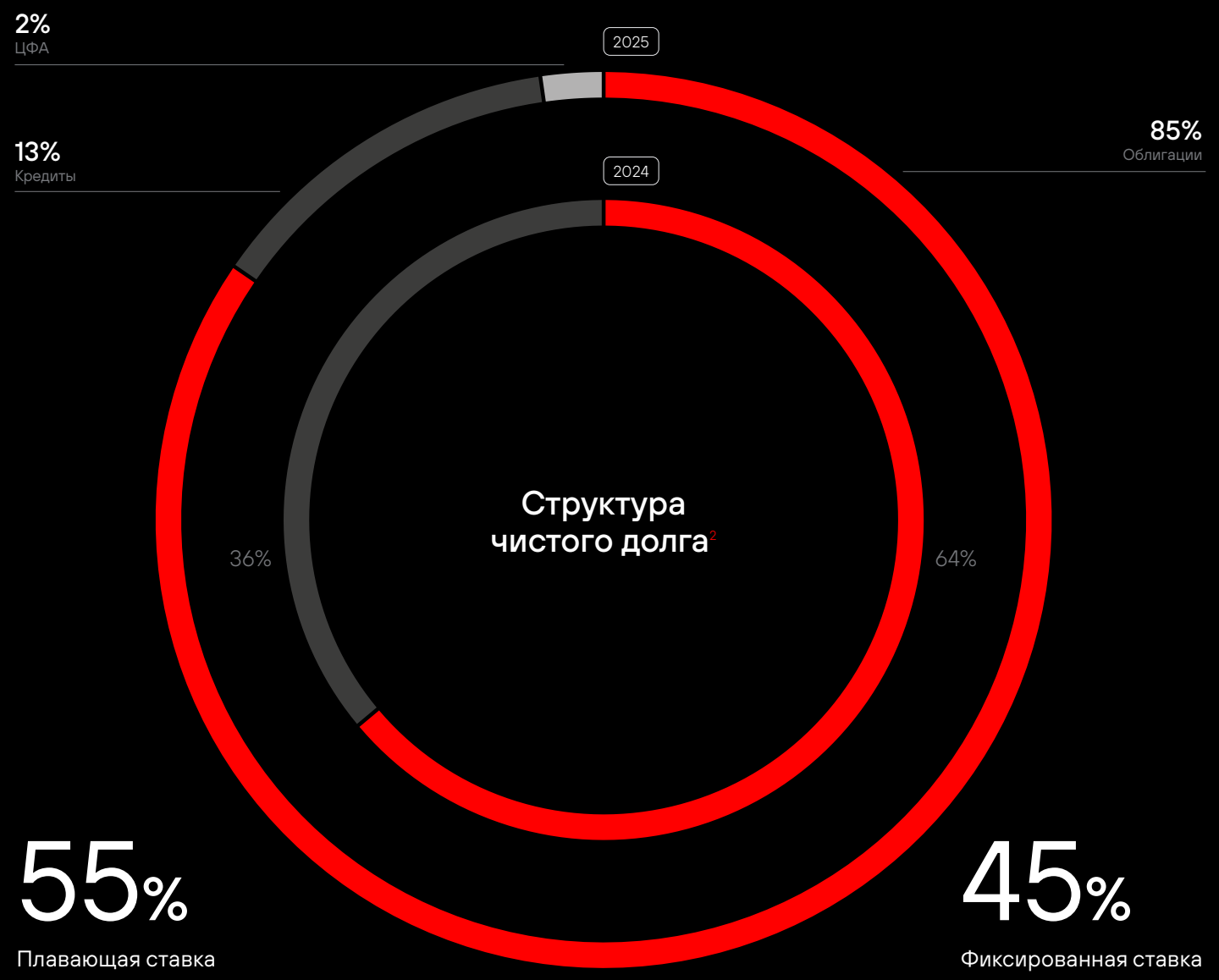
Также в отчетном периоде Компания осуществила дебютный выпуск ЦФА. Данный шаг стал логичным развитием финансовой стратегии Компании, направленной на диверсификацию источников заимствований путем расширения используемых видов долгового финансирования и оптимизации стоимости краткосрочной ликвидности за счет использования высокотехнологичных финтехрешений.

Доля облигаций в общем портфеле заимствований по состоянию на конец отчетного периода составила 85%.

Чистый долг / EBITDA LTM[1]



1 Без арендной задолженности, не применяется МСФО 16.



2 Расчет структуры чистого долга произведен исходя из логики, что в первую очередь Группа погашает кредиты и займы как наиболее подверженный риску элемент финансирования.

Основные финансовые результаты 2025 года

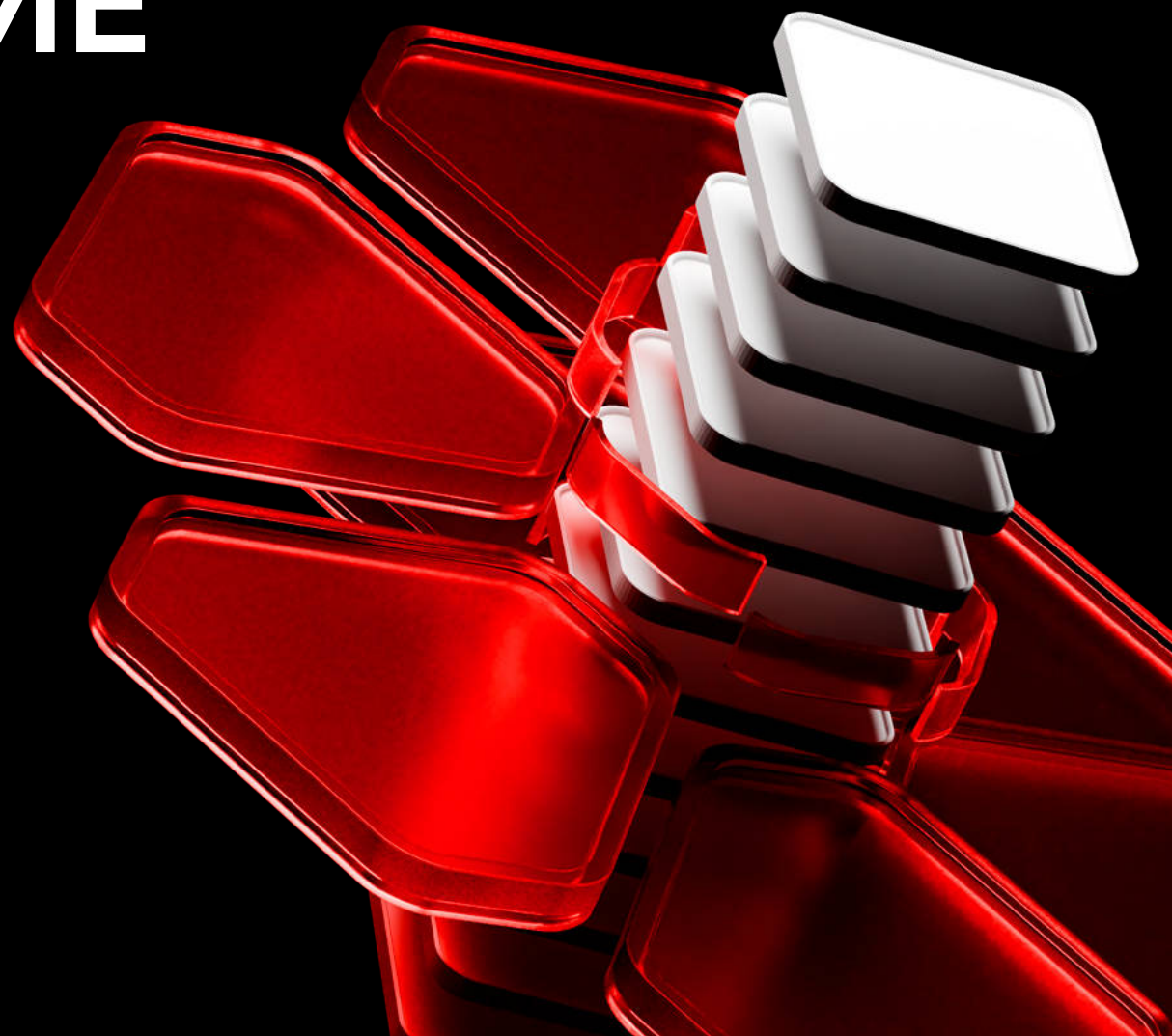
Показатель	2021, факт	2022, факт	2023, факт	2024, факт	2025, факт	Изменение год к году, %
Отгрузки с НДС, млрд руб.	7,7	14,5	25,5	24,1	**33,6**	**40**
Валовая прибыль отгрузок, млрд руб.	7,2	13,8	23,7	22,8	**31,1**	**37**
Доля валовой прибыли от отгрузок без НДС, %	96	98	95	97	**95**	**–**
EBITDAC, млрд руб.	1,6	5,2	8,9	(1,2)	**7,1**	**674**
NIC (чистая прибыль без капитализации расходов), млрд руб.	1,2	5,0	8,7	(2,7)	**2,7**	**203**
Рентабельность по NIC, %	16	35	35	–	**8**	
NIC за вычетом налога на сверхприбыль, млрд руб.		4,8				–
Рентабельность по NIC, %		34				
Разница между управленческой отчетностью и МСФО[1]:						
Корректировка по выручке, млрд руб.	(0,4)	(0,3)	(1,6)[5]	0,9	**(1,7)**	**–283**
Капитализируемые расходы, млрд руб.	1,5	1,9	3,5	6,4	**6,4**	**0**
Амортизация расходов и прочее, млрд руб.	(0,4)	(0,5)	(0,9)	(1,4)	**(0,7)**	**52**
МСФО-метрики						
Выручка[2], млрд руб.	7,1	13,8	22,2	24,5	**30,9**	**26**
EBITDA[3], млрд руб.	2,7	6,8	10,8	6,5	**12,3**	**91**
Рентабельность по EBITDA, %	38	50	49	26	**40**	**+14 п. п.**
Чистая прибыль, млрд руб.[4]	1,9	6,1	9,7	3,7	**7,2**	**99**

1 Подробнее см. раздел 3 в МСФО отчетности за 12 месяцев 2024 года.
2 Выручка = Отгрузки без НДС + Корректировка по выручке - бонусы покупателям.
3 EBITDA = EBITDAC + Корректировка по выручке + Капитализируемые расходы.
4 Чистая прибыль = NIC + Корректировка по выручке + Капитализируемые расходы + Амортизация расходов.
5 Корректировка включает разницу в признании техподдержки на (1,2) млрд руб., пролонгирующихся лицензий на (0,5) млрд руб., а также корректировку на оплаты до 31 марта 2026 года на сумму 0,4 млрд руб.

Разница между управленческой отчетностью и МСФО

	2025 год	2024 год
Отгрузки с НДС	**33,6**	**24,1**
НДС	(1)	(0,6)
Отгрузки без НДС	**32,6**	**23,5**
Разницы между отгрузками и выручкой	(1,7)	0,9
Выручка МСФО	**30,9**	**24,5**
EBITDA	**12,3**	**6,5**
Разницы между отгрузками и выручкой, за исключением рибейтов покупателям	1,2	(1,3)
Капитализированные расходы и прочее	(6,4)	(6,4)
EBITDAC	**7,1**	**(1,2)**
Прибыль за период	**7,3**	**3,7**
Разницы между отгрузками и выручкой, за исключением рибейтов покупателям	1,2	(1,3)
Капитализированные расходы и прочее	(6,4)	(6,4)
Амортизация капитализированных расходов, капитализация процентов и прочее	0,7	1,4
NIC	**2,7**	**(2,7)**

ВЗАИМОДЕЙСТВИЕ С ИНВЕСТОРАМИ



- Обращение IR-директора
- Открытость и прозрачность как основа успеха
- POSI на бирже
- Дивидендная политика и дивидендная история
- Долговые инструменты
- Акционерный капитал и принципы работы с капиталом
- Календарь инвестора

ОБРАЩЕНИЕ IR-ДИРЕКТОРА

Уважаемые инвесторы!

Для Positive Technologies прозрачность и открытость — это не просто декларация принципов, а фундамент нашей устойчивости. Мы руководствуемся этими принципами с самого первого дня нашей публичности и твердо убеждены, что доверие строится не на красивых графиках, а на готовности Компании вести честный диалог даже в самые сложные периоды.

Именно поэтому в основе наших отношений с акционерами и участниками рынка лежит архитектура создания ценности, где прозрачность процессов превращает управление Компанией в понятную и предсказуемую для инвесторов систему. В частности, значимую роль в этом играют дополнительно раскрываемые нами управленческие показатели, которые сегодня формируют отраслевой стандарт отчетности.

Прошлый год стал для нас временем проверки на прочность и восстановления привычных для нас темпов роста бизнеса. Открыто признав отклонения от прогнозов финансового результата 2024 года, мы не просто сохранили связь с рынком, а получили важный кредит доверия для глубокой трансформации. В 2025 году наша стратегия, направленная на повышение эффективности бизнеса, дала результаты. Компания смогла вернуться к целевым темпам роста, опережающим динамику рынка вдвое, сохранила инвестиции в разработку продуктов и показала высокий уровень финансовой дисциплины.

Системная оптимизация процессов помогла нам укрепить финансовый фундамент, а реализация стратегии по улучшению структуры и показателей долгового портфеля позволила снизить долговую нагрузку до комфортного уровня – 1,66.

Одной из финансовых задач 2025 года было возвращение NIC в положительную зону. Она выполнена с хорошим запасом, что позволяет вновь рассмотреть возможность выплаты дивидендов, подтвердив нашу нацеленность на повышение инвестиционной привлекательности акций, в том числе в рамках дивидендной политики Компании.

Сегодня мы продолжаем строить Компанию, где каждое решение обосновано, а результат закономерен. Мы не только реализуем передовые практики взаимодействия с инвесторами и повышения их вовлеченности, но и создаем их. Ваша неизменная поддержка в периоды перемен подтверждает, что рынок ценит честность так же высоко, как и технологические достижения. Спасибо, что вы с нами!

Юрий Мариничев

Директор по связям с инвесторами Positive Technologies

ОТКРЫТОСТЬ И ПРОЗРАЧНОСТЬ КАК ОСНОВА УСПЕХА

В 2025 году Positive Technologies сохранила верность своим принципам и продолжила развивать честный диалог с инвестиционным сообществом.

Мы провели серию знаковых мероприятий, включая масштабный День инвестора в «Лужниках», где в формате живого общения обсуждали с акционерами и аналитиками текущие результаты и стратегические планы Компании. Активное участие в профильных IR-конференциях позволило нам укрепить связи с ключевыми участниками рынка и расширить круг профессиональных контактов.

Мы продолжили совершенствовать наши коммуникации, делая ставку на развитие социальных сетей и внедрение новых инструментов взаимодействия. Наша задача — сделать сложный бизнес в сфере кибербезопасности прозрачным и понятным для каждого инвестора независимо от его профессионального опыта. Мы стремимся к тому, чтобы информация о Компании была максимально доступной, а взаимодействие с нами — комфортным.

Наша главная цель — формирование сообщества лояльных инвесторов, которые не только видят финансовые перспективы, но и разделяют наши ценности и миссию. Мы ценим оказанное доверие и верим, что искренний интерес акционеров к жизни Компании создает надежный фундамент для нашего общего долгосрочного успеха.

Наш сайт

Датабук

Годовой отчет

Прямой контакт

Акционерный капитал Positive Technologies объединяет как розничных, так и институциональных инвесторов. Мы понимаем, что за каждым вложением стоит не просто финансовый расчет, а высокая степень доверия к нашей стратегии и команде. Именно поэтому живое общение остается для нас приоритетным форматом взаимодействия.

Личные встречи позволяют выйти за рамки стандартных отчетов и графиков. Офлайн-мероприятия дают нам возможность услышать каждого акционера, ответить на самые острые вопросы и обсудить будущее Компании в режиме реального времени. Мы убеждены, что взаимодействие лицом к лицу сокращает дистанцию, помогая лучше понимать ожидания рынка и превращая отношения с акционерами в долгосрочное и взаимовыгодное партнерство.

15 онлайн-эфиров и трансляций для инвесторов

31 встреча с аналитиками

3 Дня инвестора POSI

Участие в

11 конференциях для розничных инвесторов

7 образовательных мероприятиях

36 профильных мероприятиях и круглых столах

6 региональных встреч с инвесторами в партнерстве с банками и брокерами

18 встреч с инфлюенсерами

16 встреч с институциональными инвесторами

День инвестора в «Лужниках»: кибербезопасность для каждого

С 22 по 24 мая 2025 года спорткомплекс «Лужники» вновь стал центром притяжения, объединив профессионалов и любителей технологий на международном киберфестивале Positive Hack Days Fest. За три дня открытую часть мероприятия посетило более 150 тыс. человек, которые смогли узнать, как устроен цифровой мир, и повысить уровень своей киберграмотности.

День инвестора в «Лужниках»

~450

участников очной сессии

~2,6

тыс. пользователей смотрели онлайн-трансляцию мероприятия

Программа фестиваля была продумана для всей семьи. Взрослые, студенты и школьники знакомились с карьерными возможностями в ИТ и ИБ, а самые маленькие посетители участвовали в тематических активностях. Гости своими глазами увидели кибербезопасность в действии, наблюдая за масштабной битвой Standoff в цифровом мегаполисе.

Для Компании Positive Hack Days является не просто местом встречи экспертов, а мощным инструментом для развития бизнеса. Традиционно центральное место в структуре фестиваля занимает насыщенная деловая программа.

Одним из главных событий мероприятия стал День инвестора, прошедший на Большой спортивной арене. Этот формат позволил акционерам и аналитикам совместить обсуждение планов развития бизнеса Компании с погружением в атмосферу кибербезопасности. В рамках первой части сессии представители Московской биржи, эксперты венчурного рынка и ведущие ИТ-аналитики обсудили потенциал российского технологического сектора и ключевые драйверы его роста. Вторая часть была посвящена планам развития Positive Technologies: топ-менеджеры Компании рассказали о совершенствовании технологий, уникальной экспертизе и новых рыночных горизонтах.

Официальная программа завершилась сессией Q&A, где каждый участник мог задать прямой вопрос руководству. Неформальное общение продолжилось и после сессии, позволяя инвесторам обмениваться опытом и заводить полезные знакомства. Такие встречи в рамках киберфестиваля помогают нам поддерживать высокий уровень прозрачности и объединять инвестиционное сообщество вокруг идей технологического развития и важности кибербезопасности.

Помимо масштабного мероприятия для инвесторов в «Лужниках», в отчетном году мы провели еще два Дня инвестора POSI. Встречи, прошедшие в апреле и ноябре 2025 года, были посвящены результатам деятельности Компании за 2024 год и девять месяцев 2025 года. Мероприятия транслировались в прямом эфире, что позволило и гостям в зале, и онлайн-зрителям получить ответы на свои вопросы из первых рук — от топ-менеджмента Компании.

Новые грани диалога

Мы стремимся к тому, чтобы коммуникация с инвестиционным сообществом была максимально живой и разносторонней. Для этого в 2025 году Positive Technologies задействовала самые разные форматы — от классических встреч топ-менеджмента с аналитиками до уникальных погружений в специфику продуктов и экскурсий по офису.

Важной частью нашей работы стали регулярные встречи с аналитиками, финансовыми журналистами и инфлюенсерами. Регулярное общение с лидерами мнений и ключевыми экспертами рынка помогает нам оставаться прозрачными на каждом этапе развития, превращая сухие цифры отчетности в живую историю технологического лидерства.

Мы также открыли двери нашего офиса, организовав серию экскурсий. Это дало возможность инвесторам и экспертам познакомиться с внутренней кухней Компании, увидеть рабочие процессы и пообщаться с командой в неформальной обстановке. В октябре наши акционеры, аналитики и инфлюенсеры смогли глубже погрузиться в технологическую повестку на мероприятии Positive Security Day.

Особое внимание мы уделяем образовательной составляющей, помогая инвесторам лучше разбираться в специфике кибербезопасности. Так, в августе состоялась встреча аналитиков ведущих брокеров с Алексеем Лукацким. Бизнес-консультант и евангелист кибербезопасности рассказал о сложных продуктах киберзащиты, используя простые аналогии с физическими системами безопасности, что сделало наши технологии понятными даже для неспециалистов.

Расширяем аналитическое покрытие

Positive Technologies активно расширяет взаимодействие с банковским сообществом и независимыми аналитиками. Мы ценим глубокую экспертизу профессиональных участников рынка: внешние обзоры и оценки подтверждают надежность наших данных и помогают инвесторам формировать объективный взгляд на бизнес. Для нас это важный этап «верификации» нашей открытости, который укрепляет доверие к Компании как к зрелому публичному эмитенту.

31
встреча
с аналитиками

18
встреч
с инфлюенсерами

16
встреч
с институциональными
инвесторами

Оценка акций Positive Technologies инвестбанками и независимыми аналитиками

Команда аналитиков	Целевая цена акции, руб.
Freedom Finance Global 12.02.2025	1700
Т-Инвестиции 14.02.2025	1640 держать
СберИнвестиции 14.02.2025	1400
ИФК Солид 08.04.2025	1900
Финам 19.04.2025	2904 покупать
Альфа-Инвестиции 22.04.2025	2350 выше рынка
Freedom Finance Global 24.04.2025	1480
Т-Инвестиции 20.06.2025	1450 держать
Газпромбанк 09.07.2025	1700 покупать

Команда аналитиков	Целевая цена акции, руб.
Финам 14.07.2025	2904 покупать
Альфа-Инвестиции 01.08.2025	2350 покупать
Цифра брокер 01.08.2025	2226 покупать
Эйлер 04.08.2025	2100 покупать
СберИнвестиции 04.08.2025	1400 держать
Промсвязьбанк 04.08.2025	1645 покупать
ИБ Синара 04.08.2025	1300 держать
Т-Инвестиции 11.08.2025	1500 держать
Эйлер 11.11.2025	2100 покупать

Команда аналитиков	Целевая цена акции, руб.
СберИнвестиции 11.11.2025	1600 покупать
Промсвязьбанк 11.11.2025	1580 покупать
Freedom Finance Global 11.11.2025	1250–1350 покупать
БКС 11.11.2025	1000 продавать
Т-Инвестиции 12.11.2025	1350 держать
Альфа-Инвестиции 24.11.2025	1950 покупать
ВТБ Моя аналитика 03.12.2025	2124 покупать
БКС 18.12.2025	1000 продавать
Промсвязьбанк 25.12.2025	1550 покупать

Идем в регионы

В 2025 году мы продолжили расширять географию нашего присутствия, подтверждая, что для прямого и честного диалога с инвесторами не существует границ. Мы стремимся быть на связи с акционерами не только в столице, но и в самых разных регионах России.

В партнерстве с крупнейшими федеральными банками и брокерами команда Positive Technologies провела серию региональных встреч. Мы посетили Архангельск, Екатеринбург, Санкт-Петербург и Уфу. Эти мероприятия объединили сотни частных инвесторов, представителей регионального финансового сообщества и лидеров мнений.

10 декабря в Якутске состоялась финальная встреча регионального цикла 2025 года. IR-директор встретился с местным сообществом акционеров и частных инвесторов, чтобы рассказать о Компании и перспективах развития бизнеса.

Такие встречи позволяют нам лучше понимать запросы инвесторов по всей стране и выстраивать доверительные отношения, которые лежат в основе успеха нашей Компании.

6

региональных встреч с инвесторами в партнерстве с банками и брокерами

Годовое заседание Общего собрания акционеров в очном формате

В отчетном году была возобновлена практика проведения годовых заседаний общих собраний акционеров (ГОСА) в очном формате, которые ранее зачастую заменялись заочным голосованием из-за временных законодательных послаблений.

В 2025 году Компания впервые провела ГОСА в очном формате. Встреча прошла 21 мая в «Лужниках» в преддверии киберфестиваля Positive Hack Days. Такой подход позволил инвесторам не только принять участие в официальной части мероприятия, но и лучше понять специфику бизнеса Компании и ИБ-индустрии.

В заседании приняли участие Председатель Совета директоров и топ-менеджмент Компании. Акционеры могли лично заслушать доклады руководителей, задать интересующие вопросы и проголосовать по пунктам повестки непосредственно на площадке. При этом для участников сохранялась полная гибкость: выразить свою позицию можно было как очно, так и дистанционно через систему электронного голосования. Акционеры, не имевшие возможности посетить мероприятие лично, также могли проголосовать заочно в стандартном режиме.

Мы поддерживаем проведение годовых заседаний общих собраний акционеров в очном формате, **видя в них ценную возможность** для открытого диалога с инвесторами и получения оперативной обратной связи.

Общаемся в соцсетях

«Т-Инвестиции»

›140

тыс. подписчиков в «Пульсе»

1-е место

по количеству подписчиков среди эмитентов

«POSItивный инвестор» — ваш персональный гид

Важным помощником для акционеров остается наш чат-бот в Telegram. Этот инструмент предоставляет удобный доступ к актуальной информации о бизнесе Компании в режиме 24/7. Бот помогает лучше понять продуктовую линейку, раскрывает ключевые драйверы роста и финансовые показатели, а также содержит ответы на самые часто задаваемые вопросы. В 2025 году мы полностью актуализировали базу данных чат-бота, чтобы он еще точнее отвечал на запросы нашей инвестиционной аудитории.

Приятно познакомиться!

чат-бот для инвесторов
#POSI

Социальные сети для Positive Technologies — это ключевой канал живой и оперативной связи с инвесторами. Мы выбираем проактивность: не просто транслируем новости, а переводим сложные корпоративные события на понятный язык, раскрываем суть наших продуктов и честно обсуждаем будущее Компании. Для нас важен каждый комментарий и вопрос — мы стремимся быть максимально доступными и поддерживать открытый диалог на всех популярных платформах.

В 2025 году наше присутствие в цифровой среде значительно расширилось. Сегодня мы ведем активный диалог на платформах «Пульс», Telegram (канал It's Positive Investing), Smart-Lab, «БКС Профит», «Импульс» от Market Power (где входим в топ-3 по подписчикам) и в приложении «СберИнвестиции».

В отчетном году Компания вышла в новую независимую соцсеть для инвесторов «Базар». На данный момент наш канал там насчитывает 1,9 тыс. подписчиков и входит в топ-10 лучших каналов площадки. Наличие уникальных авторов и отсутствие привязки сервиса к конкретному банку или брокеру открывают перед Positive Technologies дополнительные возможности для привлечения новой аудитории. Кроме того, в декабре 2025 года мы запустили канал в сообществе «Альфа-Инвестор». Интеграция банка, брокера и медиаканалов «Альфа-Инвестиций» в рамках одной платформы позволяет нам эффективно взаимодействовать с большим количеством розничных инвесторов.

Наш канал в «Пульсе» остается базовой платформой для общения: за год количество подписчиков выросло на 22% и превысило 140 тыс. Это позволило Positive Technologies второй год подряд занять первое место среди всех эмитентов по размеру сообщества на этой площадке.

Наши ключевые онлайн-площадки

«Т-Инвестиции. Пульс»

140,3 +22%
тыс. подписчиков

192
тыс. просмотров

It's Positive Investing

›10,2
тыс. подписчиков

41,5
тыс. просмотров / месяц

Блог PT на SMART-LAB

›86
постов

281
тыс. просмотров

«Альфа-Инвестор» NEW

Канал PT в «БКС Профит»

1,8
тыс. подписчиков

It's Positive Investing

1,86
тыс. подписчиков

«Базар» NEW

1,9
тыс. подписчиков,
топ-10 подписчиков

Инструменты для инвесторов

Датабук

Для профессионального сообщества мы продолжаем выпускать датабук — удобный цифровой сборник ключевых показателей из нашей отчетности. Этот формат значительно упрощает работу аналитиков с цифрами, делая процесс моделирования и оценки бизнеса более эффективным и прозрачным.

Датабук

Сайт для инвесторов

Мы стремимся к тому, чтобы каждый инвестор мог оперативно получать достоверную информацию о деятельности Positive Technologies и оценить привлекательность наших акций. Для этого, помимо основного корпоративного портала, мы развиваем специализированный сайт для инвесторов. На нем в лаконичной форме собраны все необходимые сведения: финансовая отчетность, корпоративные документы, консенсус-прогнозы аналитиков, а также актуальные IR-новости и календарь предстоящих мероприятий. Наша задача — сделать путь к важным данным максимально коротким и простым.

Сайт

Годовой отчет

Годовой отчет для нас не только обязательный формат раскрытия, но и полноценный инструмент коммуникации с рынком. Постоянное совершенствование структуры и визуализации данных позволяет Компании представлять результаты своей деятельности в максимально содержательной и доступной форме. Особое место в системе взаимодействия с инвестиционным сообществом занимает интерактивная версия отчета. Она обеспечивает эффективную навигацию по финансовым и операционным метрикам, превращая сложный анализ данных в интуитивно понятный процесс для каждого участника рынка.

В 2025 году качество раскрытия информации Компанией получило высокую оценку профессионального сообщества. Годовой отчет Positive Technologies стал призером XXVII конкурса годовых отчетов Московской биржи в номинации «Эффективная коммуникация», что подтверждает лидерство в области выстраивания качественного диалога с инвесторами. Кроме того, агентство RAEX присвоило Годовому отчету рейтинг «4 звезды» («Очень высокое качество»), верифицировав соответствие отчетности Компании передовым стандартам прозрачности.

Данные достижения подтверждают правильность выбранного подхода к раскрытию информации. Компания намерена и далее совершенствовать практики прозрачности и развивать инструменты открытого диалога с инвестиционным сообществом.

Годовой отчет

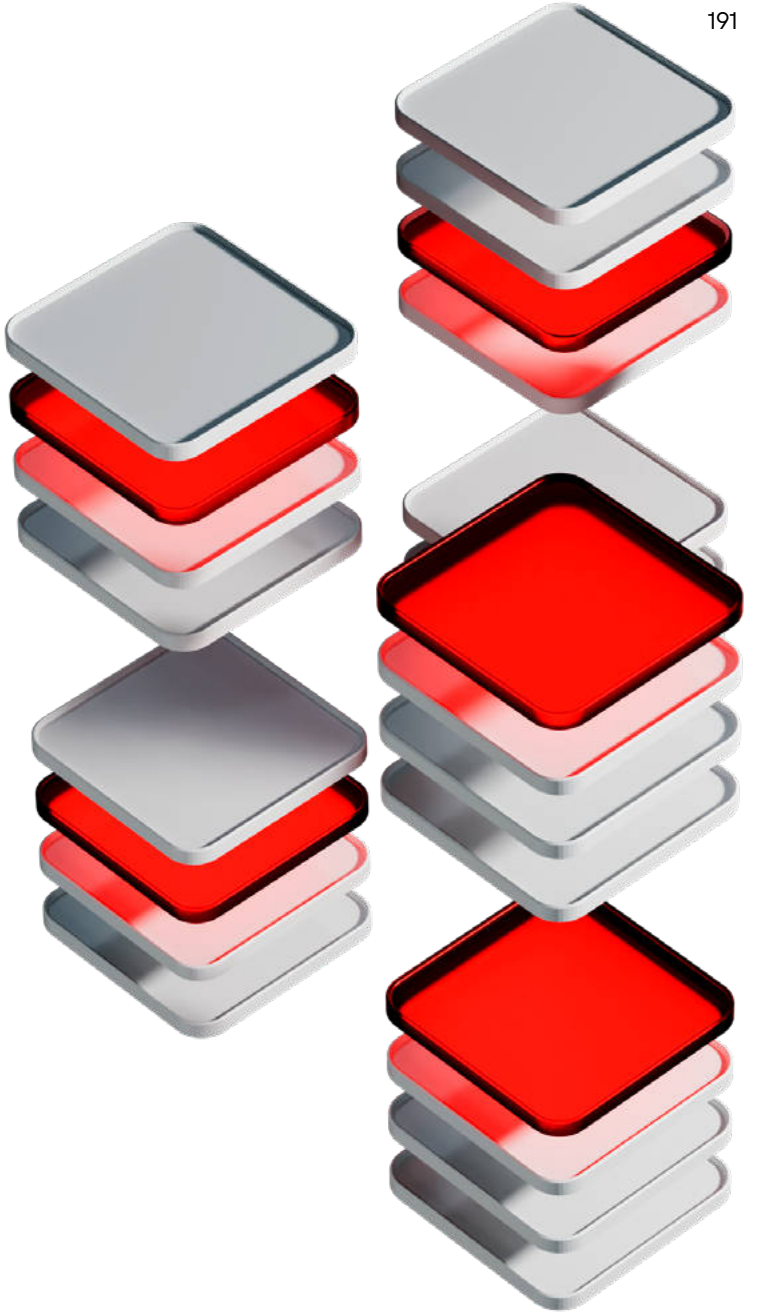
Онлайн-эфиры с топ-менеджментом и IR-директором

Мы активно используем цифровые площадки для поддержания непрерывной связи с инвесторами по всей стране. Участие в прямых эфирах на ведущих инвестиционных платформах стало для нас важным инструментом трансляции ключевых событий и обсуждения глобальных трендов кибербезопасности. Такой формат позволяет топ-менеджерам и IR-директору Positive Technologies не просто делиться новостями, а создавать пространство для честного и открытого диалога в режиме реального времени.

15

онлайн-эфиров и трансляций для инвесторов

В 2025 году мы провели 15 онлайн-эфиров на популярных площадках, таких как РБК, «Финам», «Т-Инвестиции», «Эйлер Аналитические технологии». Каждая встреча была ориентирована на прямой контакт с аудиторией: мы подробно отвечали на вопросы зрителей, разбирали финансовые показатели и делились стратегическими планами развития. Подобная практика открытости помогает нам оперативно реагировать на запросы сообщества, устранять недопонимание и укреплять доверие акционеров, делая Компанию максимально понятной и прозрачной для каждого инвестора.



Делимся опытом с коллегами

Positive Technologies не только совершенствует собственные коммуникации, но и активно участвует в формировании высоких стандартов IR-отрасли в России. Мы убеждены, что развитие культуры открытости среди эмитентов делает весь фондовый рынок более зрелым и привлекательным для инвесторов.

В отчетном году экспертиза нашей Компании легла в основу обновленных отраслевых стандартов. IR-директор Positive Technologies Юрий Мариничев вошел в состав авторов «IR-гида» Московской биржи — фундаментального практического руководства по взаимодействию с инвесторами. Кроме того, Юрий стал одним из спикеров IR-академии Московской биржи, где рассказал о подходах к формированию инвестиционного кейса публичных компаний.

Участие в этих и других профильных мероприятиях позволяет Positive Technologies масштабировать свои наработки и задавать вектор развития для нового поколения публичных технологических компаний.

На протяжении года мы активно делились наработками на крупнейших профессиональных и инвестиционных форумах, способствуя внедрению принципов честного диалога во всем бизнес-сообществе:

1

Форум «Большие данные. ЦОДы и роботизация»

Мы представили взгляд на будущее ИТ-сектора и новые возможности для инвесторов в условиях цифровой трансформации российской экономики.

2

Круглый стол Visiology «Насколько актуально инвестировать в IT?»

При участии ведущих экспертов и инвест-сообщества (модератор — Назар Щетинин, «Вредный инвестор») мы проанализировали реальные драйверы оценки ИТ-бизнеса и перспективы импортозамещения.

3

Smart-lab Conf 2025 (Панельная дискуссия «ТОП IR»)

Совместно с коллегами из крупнейших публичных компаний обсудили важность открытой коммуникации с частными инвесторами как ключевого фактора доверия к эмитенту.

4

M&A Конгресс

В рамках сессии «Критерии успешного pre-IPO и IPO» представили практические рекомендации по подготовке компаний к выходу на биржу в новых рыночных условиях.

5

«IPO SKOLKOVO: капитал для роста»

В рамках мероприятия мы подробно раскрыли уникальный кейс выхода Positive Technologies на фондовый рынок и поделились накопленным опытом публичности.

6

IB Club

Провели глубокое погружение в индустрию кибербезопасности, представив обзор рынка, историю развития Positive Technologies и технологическую карту наших продуктов.

Наши награды

Профессионализм IR-команды Positive Technologies в 2025 году был отмечен высокими оценками ключевых участников рынка. Эксперты выделили открытость Компании к диалогу и готовность предлагать рынку инновационные подходы к раскрытию информации. Успешная реализация планов на фондовом рынке стала важным шагом в укреплении доверия акционеров, подтверждая, что честность и предсказуемость являются главными приоритетами нашей корпоративной культуры.

- Благодарность от Московской биржи
  «За участие в подготовке Руководства для эмитента „Как говорить с инвесторами (IR-гид)“»
  Юрию Мариничеву

- 1-е место в IR-рейтинге российских эмитентов «Смартлаб»
  (третий год подряд)

Cbonds Awards — 2025

- «Лучший IR на российском долговом рынке»
- «Лучшая сделка первичного размещения в сегменте „Информационные технологии"»

«IR премия MOEX Рынок выбирает»

- «Лучший IR-руководитель компании с капитализацией 40–200 млрд рублей»
  3-е место
  Юрий Мариничев

Russia IPO Awards 2025

- «Лучшая команда Investor Relations»

Investment Leaders Award 2025

- «Эмитент акций года в IT»
- «IR-директор года»
  Юрий Мариничев

POSI НА БИРЖЕ

Капитализация и ликвидность

На конец 2025 года стоимость акций Positive Technologies зафиксировалась на уровне 997,0 руб. Отрицательная динамика в размере 50,4% относительно значения прошлого года стала следствием сочетания рыночных факторов и реакции инвесторов на внутренние события Компании.

2025 год оказался непростым для всего российского фондового рынка. Технологический сектор, как наиболее чувствительный к изменению макроэкономических условий и процентных ставок, столкнулся с самым сильным давлением. Падение котировок POSI во многом следовало за общим трендом охлаждения интереса к акциям роста.

Дополнительным сдерживающим фактором стала консервативная оценка инвесторами результатов 2024 года. Отклонение от ранее заявленного гайденса создало временный дефицит доверия, который отразился на рыночной стоимости бумаг.

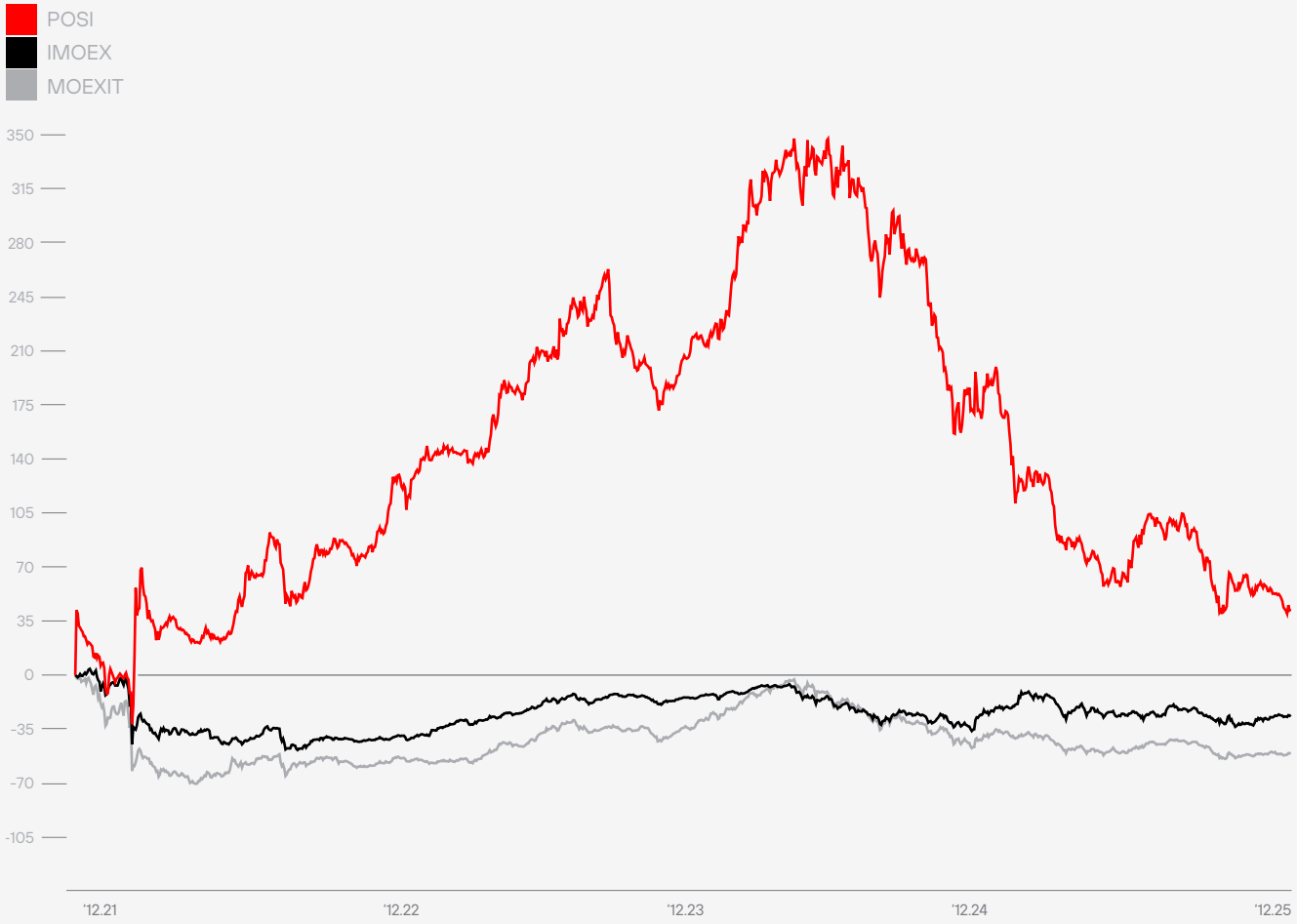
Несмотря на текущую волатильность, капитализация Компании на 30 декабря 2025 года (71,0 млрд руб.) остается выше уровней, зафиксированных при первоначальном выходе на биржу. Мы рассматриваем текущую цену акций как рыночную аномалию, не в полной мере отражающую реальные темпы развития бизнеса.

Наша приоритетная задача — через повышение операционной эффективности и восстановление положительной динамики NIC вернуть рыночную оценку акций в соответствие с фактическим масштабом бизнеса. Мы придерживаемся стратегии долгосрочного роста, где прозрачность результатов является главным драйвером восстановления капитализации.

Сравнительный анализ показывает, что движение акций Positive Technologies в 2025 году во многом определялось общим вектором развития российского фондового рынка и его технологического сегмента. График наглядно демонстрирует высокую корреляцию котировок Компании с отраслевым индексом МосБиржи (MOEXIT), который на протяжении года находился под значительным давлением макроэкономических факторов. В то время как снижение основного индекса МосБиржи (IMOEX) отражало общую рыночную конъюнктуру, более выраженная коррекция акций POSI стала следствием сочетания отраслевого спада и специфической реакции инвесторов на временное отклонение от гайденса по итогам 2024 года. Текущий разрыв в динамике индексов и стоимости наших бумаг мы рассматриваем как временное явление, не в полной мере отражающее фундаментальную стоимость бизнеса и потенциал его дальнейшего роста.

Ликвидность акций Positive Technologies демонстрирует устойчивый рост. За четыре года среднедневной объем торгов составил 536 млн руб. В 2025 году этот показатель вырос до 831 млн руб. — в 8,5 раза больше, чем в первый год размещения, и на 11,3% выше уровня прошлого года. Рост ликвидности подтверждает повышенный интерес инвесторов к акциям Компании и укрепляет ее позиции на фондовом рынке.

Динамика изменения стоимости акций POSI в сравнении с индексами



Акции в индексах Мосбиржи

Основной площадкой для торгов акциями Positive Technologies является Московская биржа. Акции Компании включены в широкий ряд индексов: основные индексы Московской биржи — IMOEX и РТС, а также индекс акций широкого рынка, индекс средней и малой капитализации, индекс информационных технологий, индекс инноваций.

На конец 2025 года акции Positive Technologies входят в 13 индексов, включая основной индекс МосБиржи. Включение в список российских эмитентов с высокой капитализацией и наиболее ликвидными акциями свидетельствует о стабильности финансовых показателей и прибыльности акций Компании, подчеркивая ее надежность и инвестиционную привлекательность.

До 19 декабря 2025 года акции Positive Technologies входили в субиндекс пенсионных накоплений.

Индексы, в которые входят ценные бумаги Positive Technologies на 31 декабря 2025 года

Код	Название индекса
IMOEX	Индекс МосБиржи
IMOEX	Индекс МосБиржи (все сессии)
IMOEXW	Индекс МосБиржи — активное управление
MCXSM	Индекс МосБиржи SMID (средней и малой капитализации)
MOEXIT	Индекс МосБиржи IT
RTSI	Индекс РТС
RTSIT	Индекс РТС IT
RTSSM	Индекс РТС SMID
RUBMI	Индекс РТС широкого рынка
MOEXBMI	Индекс широкого рынка
MOEXINN	Индекс МосБиржи инноваций
IMOEXCNY	Индекс МосБиржи в юанях
MXSHAR	Индекс МосБиржи Исламских инвестиций

POSI на СПБ бирже

Акции Positive Technologies также торгуются на СПБ Бирже. Это расширяет доступ к акциям Positive Technologies для большего числа инвесторов, открывая новые возможности для их приобретения и укрепления позиций Компании на фондовом рынке.

ДИВИДЕНДНАЯ ПОЛИТИКА И ДИВИДЕНДНАЯ ИСТОРИЯ

Мы стремимся к тому, чтобы каждый акционер четко понимал, как формируется доходность его инвестиций. Для Positive Technologies выплата дивидендов — это не просто формальное выполнение обязательств, а подтверждение нашей ответственности перед инвесторами.

В основе нашей дивидендной политики лежит показатель NIC — чистая прибыль без учета капитализируемых расходов. Этот индикатор максимально точно отражает реальный денежный поток Компании. Согласно дивидендной политике, мы направляем на дивиденды от 50 до 100% от значения показателя NIC. Positive Technologies входит в число высокотехнологичных компаний, делающих все возможное для обеспечения дивидендных выплат акционерам.

С 2022 по 2024 год мы планомерно наращивали объем выплат. В 2024 году Компания распределила 6,547 млрд руб. (99,19 руб. на акцию), что в 1,4 раза больше уровня 2023 года и в пять раз — уровня 2022 года.

По итогам 2024 года показатель NIC ушел в отрицательную зону (–2,7 млрд руб.). В строгом соответствии с нашей дивидендной политикой и принципами финансовой устойчивости Компания не осуществляла выплаты по результатам 2024 года.

Прошедший год стал периодом эффективной трансформации. По результатам 2025 года показатель NIC вернулся в положительную зону, что позволило нам рассмотреть возможность распределения прибыли и возвращения к привычной для наших акционеров модели дивидендных выплат. Совет директоров Positive Technologies созвал внеочередное Общее собрание акционеров и рекомендовал принять решение о выплате дивидендов акционерам Компании.
Сумма рекомендованных к выплате дивидендов составляет 2 млрд рублей, или 28,08 руб. на одну акцию. Вопрос об утверждении дивидендов вынесен на рассмотрение внеочередного Общего собраниям акционеров, которое пройдет в форме заочного голосования 6 мая 2026 года.

Дивидендная история Positive Technologies

2022 – дивиденды по итогам 2021 года

340,6 млн руб.
Ноябрь 2022
5,16 ₽ за акцию

950 млн руб.
Май 2022
14,4 ₽ за акцию

2023 – дивиденды по итогам 2022 года

1,04 млрд руб.
Декабрь 2023
15,8 ₽ за акцию

1,25 млрд руб.
Май 2023
18,94 ₽ за акцию

2,5 млрд руб.
Апрель 2023
37,87 ₽ за акцию

2024 – дивиденды по итогам 2023 года

3,122 млрд руб.
Апрель 2024
47,3 ₽ за акцию

3,425 млрд руб.
Май 2024
51,89 ₽ за акцию

2025 - дивиденды по итогам 2024 года не выплачивались

1 За минусом налога на сверхприбыль.

1 На основании решения Общего собрания акционеров Общества от 20 мая 2022 года ранее размещенные 6 000 000 привилегированных акций конвертированы в 6 000 000 обыкновенных акций. В период с 20 мая 2022 года и по конец отчетного периода привилегированные акции в уставном капитале отсутствовали.

2 Промежуточные дивиденды за три месяца 2024 года являются частью дивидендов по итогам 2023 года. Решение о выплате дивидендов из прибыли этого периода носит технический характер: выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам трех месяцев 2023 года.

3 Годовые дивиденды за 2023 год являются частью дивидендов по итогам 2023 года. Выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам 2023 года.

4 Промежуточные дивиденды за девять месяцев 2023 года являются третьей частью дивидендов по итогам 2022 года. Решение о выплате дивидендов из прибыли этого периода носит технический характер, выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам девяти месяцев 2023 года.

5 Промежуточные дивиденды за три месяца 2023 года являются второй частью дивидендов по итогам 2022 года. Решение о выплате дивидендов из прибыли этого периода носит технический характер, выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам трех месяцев 2023 года.

6 Годовые дивиденды за 2022 год являются первой частью дивидендов по итогам 2022 года. Выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам 2022 года.

7 Промежуточные дивиденды за девять месяцев 2022 года являются дополнительными дивидендами за 2021 год. Решение о выплате дивидендов из прибыли этого периода носит технический характер, выплата дивидендов произведена из чистой прибыли Общества по данным бухгалтерской отчетности по итогам девяти месяцев 2022 года.

8 Промежуточные дивиденды за I квартал 2022 года являются выплатами по итогам 2021 года. Решение о выплате дивидендов из прибыли I квартала 2022 года носит технический характер, поскольку акционерам распределена консолидированная прибыль всех компаний Группы, которые подвели финансовые итоги своей деятельности и перечислили дивиденды головной компании в I квартале 2022 года.

9 В связи с выплатой дивидендов по итогам девяти месяцев 2021 года по обыкновенным и привилегированным акциям годовые дивиденды не объявлялись.

Дивидендная история Positive Technologies

Отчетный период	Общий размер объявленных дивидендов, тыс. руб.		Размер дивиденда в расчете на одну акцию, руб.	
	Обыкновенные акции	Привилегированные акции	Обыкновенные акции	Привилегированные акции[1]
Дивидендная история после получения Обществом публичного статуса				
2024 год	Решение о выплате дивидендов Общим собранием акционеров за 2024 год не принималось, дивиденды за указанный период не начислялись и не выплачивались			
Три месяца 2024 года[2]	3 121 800 + 300 960 (дополнительные дивиденды)		47,30 + 4,56 (дополнительные дивиденды)	–
	3 121 800 + 300 960 (дополнительные дивиденды)	–		
2023[3]		3 123 780	47,33	–
	3 123 780	–		
Девять месяцев 2023 года[4]		1 042 800	15,80	–
	1 042 800	–		
Три месяца 2023 года[5]		2 499 420	37,87	–
	2 499 420	–		
2022 год[6]		1 250 040	18,94	–
	1 250 040	–		
Девять месяцев 2022 года[7]		340 560	5,16	–
	340 560	–		
I квартал 2022 года[8]		950 400	14,40	14,40
	864 000	86 400		
2021 год[9]	Годовые дивиденды не объявлялись			
Дивидендная история до получения Обществом публичного статуса (до 13 декабря 2021 года)				
III квартал 2021 года		340 008	54,84	54,84
	329 040	10 968		
2020 год		592 720	95,60	95,60
	573 600	19 120		
2019 год	Решение о выплате дивидендов Общим собранием акционеров за 2017–2019 годы не принималось, дивиденды за указанные периоды не начислялись и не выплачивались			
2018 год				
2017 год				

ДОЛГОВЫЕ ИНСТРУМЕНТЫ

Кредитный рейтинг

Поддержание высокого уровня кредитоспособности Positive Technologies, подтвержденного ведущими национальными агентствами, остается ключевым направлением нашей финансовой стратегии.

В 2025 году независимыми экспертами были проведены плановые пересмотры рейтингов Компании, по итогам которых оценки были сохранены в категории высокого уровня надежности (Double A), что свидетельствует о существенном запасе прочности бизнеса.

В апреле 2025 года агентство АКРА актуализировало кредитный рейтинг Компании на уровне «AA–(RU)» с прогнозом «негативный». Оценка отражает осторожный подход аналитиков к динамике увеличения долговой нагрузки и показателей обслуживания долга в краткосрочном периоде в связи с сохранением жесткой денежно-кредитной политики Банка России во второй половине 2024 года. По мнению агентства, выход Компании на плановые показатели в 2025 году приведет к значительному снижению долговой нагрузки. Также эксперты АКРА отметили сильный бизнес-профиль, лидирующие позиции Positive Technologies на рынке кибербезопасности, высокие показатели рентабельности и ликвидности Компании. В июне 2025 года агентство «Эксперт РА» подтвердило кредитный рейтинг Positive Technologies на уровне «ruAA», прогноз — «развивающийся». Аналитики агентства классифицировали результаты 2024 года как единичный кейс, связанный с макроэкономической ситуацией на фоне ключевой ставки Центрального банка России во втором полугодии, не влияющий на устойчивость и долгосрочный потенциал роста бизнеса. В своем релизе агентство указало на временный характер отклонения операционных показателей от плановых значений и выразило уверенность в способности Positive Technologies восстановить целевую динамику. По мнению экспертов агентства, информационная безопасность является важной частью поддержания работоспособности критически важной инфраструктуры страны, что обеспечивает стабильность спроса на продукты Компании и гарантирует дальнейшее масштабирование бизнеса в среднесрочной перспективе.

В отчетном году Positive Technologies продолжила реализацию мер, направленных на повышение эффективности бизнеса и снижение долговой нагрузки. На этом фоне АКРА в марте 2026 года изменило прогноз по кредитному рейтингу Компании на «позитивный», отразив в своей оценке текущие изменения в кредитном профиле.

Наличие двух актуальных рейтингов категории «АА» **подтверждает статус Positive Technologies как надежного заемщика** и подчеркивает прозрачность системы корпоративного управления.

Для нас принципиально важно не только сохранять, но и последовательно повышать уровень кредитных рейтингов, поэтому мы продолжим работу над укреплением финансового профиля Компании, снижением долговой нагрузки и реализации стратегии роста и масштабирования бизнеса.

Доверие со стороны крупнейших рейтинговых агентств к долгосрочной модели развития Positive Technologies является важным индикатором для инвесторов и обеспечивает стабильный доступ к рынку капитала.

АКРА

AA(ru)	Апрель 2024	прогноз: позитивный
AA-(ru)	Апрель 2025	прогноз: негативный
AA-(ru)	Март 2026	прогноз: позитивный

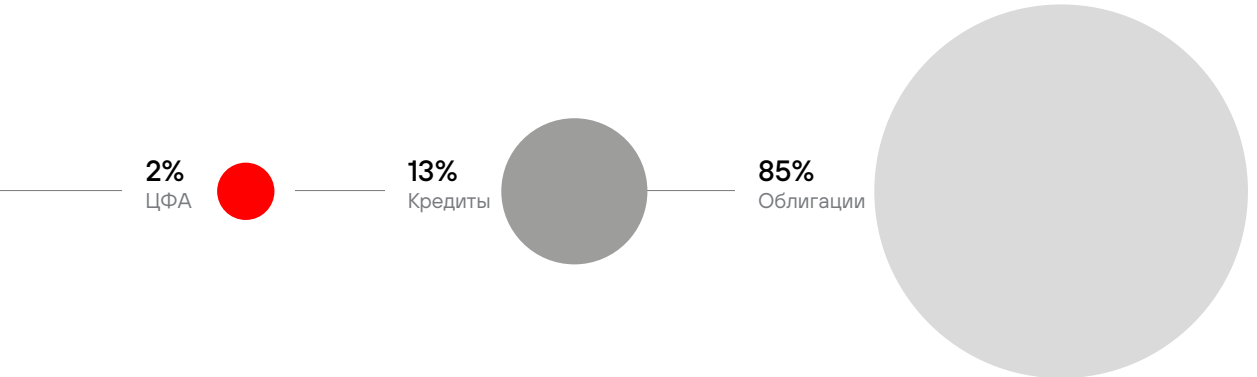
«Эксперт РА»

ruA-	Декабрь 2021	прогноз: позитивный
ruA+	Август 2022	прогноз: позитивный
ruAA	Июль 2023	прогноз: позитивный
ruAA	Июль 2024	прогноз: позитивный
ruAA	Июнь 2025	прогноз: развивающийся

Облигации

В 2025 году Positive Technologies **продолжила реализацию стратегии** по улучшению структуры и показателей долгового портфеля.

Структура долгового портфеля на 31 декабря 2025 года



Ключевым событием стало успешное размещение пятого выпуска облигаций на сумму 10 млрд руб., завершенное 27 июня 2025 года. Высокий уровень доверия со стороны рынка подтвердил финальный этап букбилдинга: общий спрос со стороны институциональных и частных инвесторов превысил объем предложения в 2,5 раза, что дало возможность зафиксировать ставку купона на уровне 18%.

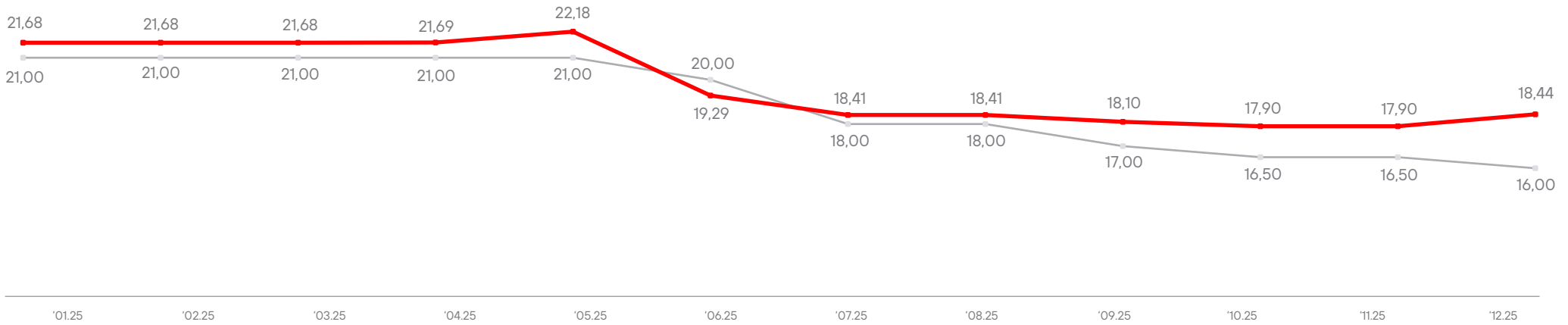
Срок обращения выпуска облигаций 2,8 года позволил Компании реализовать важную стратегическую цель — качественно трансформировать структуру заимствований за счет полного погашения краткосрочных и более дорогих банковских кредитов в составе долга. В результате на 31 декабря 2025 года облигационные займы составляют 85% от суммы задолженности Компании.

Такой подход позволяет минимизировать зависимость от банковского финансирования, оптимизировать расходы на обслуживание долга и обеспечивать гибкое управление ликвидностью Компании в долгосрочной перспективе.

Дисциплина в обслуживании долга, соблюдение интересов кредиторов и инвесторов остаются фундаментальными принципами финансовой стратегии Компании. 3 декабря 2025 года мы в полном объеме погасили выпуск облигаций серии RU000A105JG1, размещенный в декабре 2022 года на сумму 2,5 млрд руб. Своевременная выплата купонов и основной суммы долга подтвердила репутацию Positive Technologies как надежного заемщика на рынке капитала.

На конец отчетного периода инвесторам доступны к приобретению три выпуска облигаций Positive Technologies (эмитент — ПАО «Группа Позитив») с фиксированным и с плавающим купоном, а также цифровые финансовые активы (ЦФА) — современный инструмент инвестирования, недавно предложенный нами рынку.

Динамика средневзвешенной ставки по кредитному портфелю, %



Средневзвешенная ставка по кредитному портфелю Positive Technologies
Ключевая ставка Центрального банка России

45%
Долг с фиксированной ставкой

55%
Долг с плавающей ставкой

1,66
Net Debt / EBITDA LTM

Сведения об облигациях Positive Technologies	RU000A101YV8	RU000A105JG1	RU000A109098	RU000A10AHJ4	RU000A10BWC6
Полное наименование ценной бумаги	Биржевые облигации бездокументарные процентные неконвертируемые с централизованным учетом прав серии 001P-01	Биржевые облигации бездокументарные процентные неконвертируемые с централизованным учетом прав серии 001P-02	Биржевые облигации бездокументарные процентные неконвертируемые с централизованным учетом прав серии 001P-01	Биржевые облигации процентные неконвертируемые бездокументарные серии 001P-02	Биржевые облигации процентные неконвертируемые бездокументарные серии 001P-03
Срок обращений облигаций на бирже	3 года	3 года	3 года	2 года	2,8 года
Дата начала торгов	29 июля 2020 года	7 декабря 2022 года	19 июля 2024 года	27 декабря 2024 года	27 июня 2025 года
Дата погашения	26 июля 2023 года	3 декабря 2025 года	4 июля 2027 года	17 декабря 2026	12 апреля 2028 года
Размер выпуска	500 тыс. облигаций	2,5 млн облигаций	5 млн облигаций	4,8 млн облигаций	10 млн облигаций
Размер ставки купона	11,5% годовых	10,55% годовых	КС + 1,7% годовых	КС + 4% годовых	18%
Первоначальная номинальная стоимость	1 тыс. руб.	1 тыс. руб.	1 тыс. руб.	1 тыс. руб.	1 тыс. руб.
Периодичность выплаты купона	Ежеквартально	Ежеквартально	Каждые 30 дней	Каждые 30 дней	Каждые 30 дней
Уровень листинга	3	3	2	2	2
Статус	Погашен	Погашен	В обращении	В обращении	В обращении

Цифровые финансовые активы

В 2025 году Positive Technologies осуществила дебютный выпуск ЦФА на платформе «А-Токен». Данный шаг стал логичным развитием финансовой стратегии Компании, направленной на диверсификацию источников заимствований путем расширения используемых видов долгового финансирования и оптимизации стоимости краткосрочной ликвидности за счет использования высокотехнологичных финтехрешений.

Параметры выпуска

Ставка:

17,75%

Объем:

400 млн руб.

Срок обращения

1 декабря 2025 года — 1 апреля 2026

Сочетание привлекательной ставки и отсутствие высоких организационных издержек, характерных для классических облигаций, обеспечило значительную экономию на процентных расходах по сравнению с рыночными ставками банковского кредитования.

Заинтересованность розничных инвесторов подтверждена 27 ноября 2025 года — книга заявок была полностью закрыта всего за два часа. Столь высокая скорость размещения за счет активного спроса на ЦФА Компании свидетельствует о значительном доверии к бренду Positive Technologies и готовности рынка к освоению новых цифровых инвестиционных продуктов под надзором Банка России.

Данный опыт стал успешным тестом ЦФА как оперативной и востребованной альтернативы классическим кредитам и облигациям.

Интеграция цифровых активов в общую структуру привлечений Компании позволила предоставить инвесторам дополнительные возможности для участия в росте бизнеса через современные эквиваленты традиционных финансовых инструментов.

Успешный дебют и мгновенный выкуп всего объема размещения подтверждают жизнеспособность ЦФА в качестве источника пополнения оборотного капитала.
Кроме того, выпуск цифровых активов позволяет расширить базу инвесторов.
В будущем Positive Technologies рассматривает возможность дальнейшего использования ЦФА в качестве альтернативного инструмента привлечения финансирования, а также ожидает высокий спрос на цифровые активы, опираясь на подтвержденную финансовую устойчивость, зафиксированную кредитными рейтингами уровней «ruAA» от «Эксперт РА» и «AA–(RU)» от АКРА.

АКЦИОНЕРНЫЙ КАПИТАЛ И ПРИНЦИПЫ РАБОТЫ С КАПИТАЛОМ

~71,2 млн

общее количество выпущенных обыкновенных акций Компании

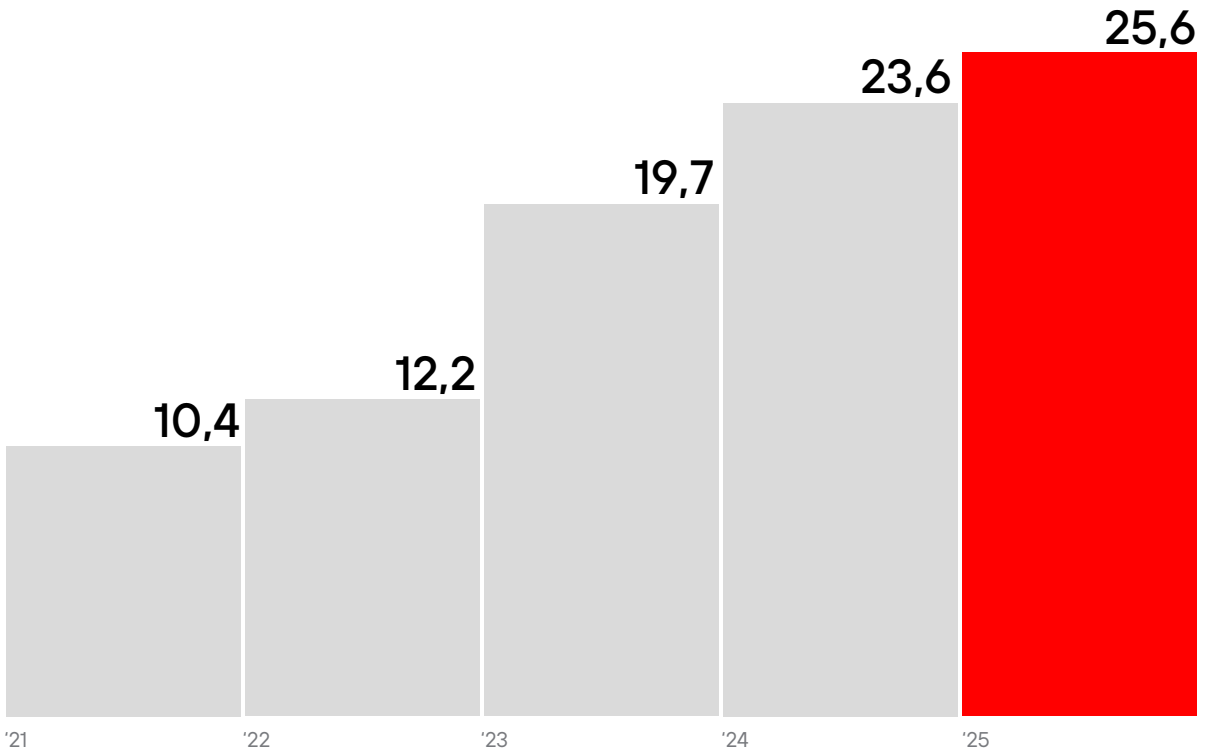
В 2025 году в структуре акционерного капитала Компании произошел ряд незначительных изменений. В декабре 2025 года технически завершилось распределение акций ключевым контрибьюторам, включая топ-менеджмент, внесшим значительный вклад в рост бизнеса и капитализации Компании в 2023 году. Доля квазиказначейских акций снизилась, при этом значение free-float по состоянию на 31 декабря 2025 года составило 25,55%, что на 1,91 п. п. выше показателя прошлого года (23,64%). Эти изменения были обусловлены как распределением акций, так и совершением отдельных сделок с миноритарными пакетами акций вследствие возросшего интереса миноритарных инвесторов к акциям ПАО «Группы Позитив».

ПАО «Группа Позитив» не владеет собственными акциями. Количество акций, находящихся в распоряжении подконтрольных ПАО «Группа Позитив» юридических лиц на 31 декабря 2025 года, составляет 1 197 575 штук (квазиказначейские акции). Общее количество выпущенных обыкновенных акций Компании составляет 71 214 000 штук. Привилегированные акции в уставном капитале отсутствуют.

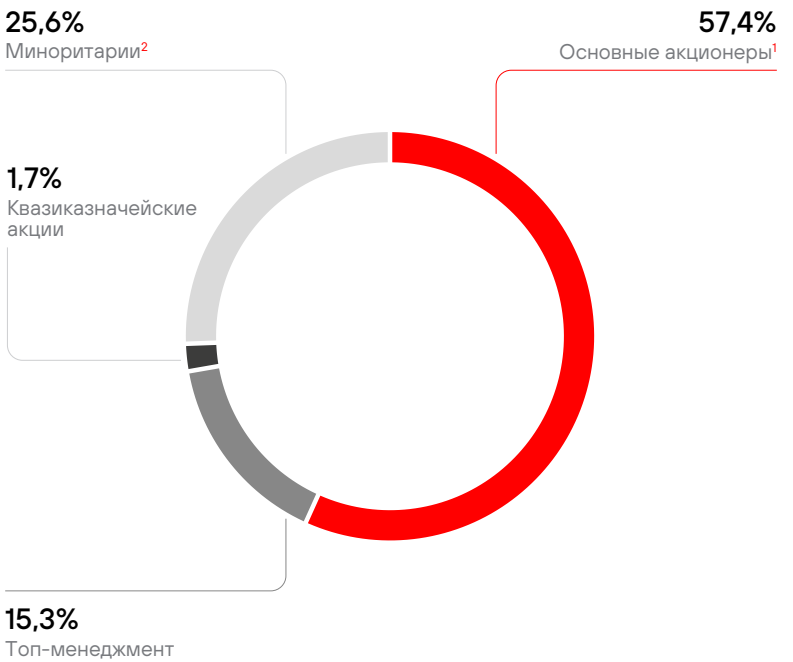
Крупные акционеры Positive Technologies, включая топ-менеджмент Компании, подписали соглашение, которое накладывает долгосрочные ограничения на сделки с подавляющим большинством принадлежащих им акций Компании. Данные ограничения распространяются в том числе на те акции, которые топ-менеджмент получил в рамках Программы стимулирования роста капитализации за вклад в рост бизнеса Компании в 2023 году.

Соглашение поможет сформировать сильное ядро совладельцев среди топ-менеджмента, ориентированных на долгосрочное развитие Компании и заинтересованных в росте финансовых показателей и капитализации. Кроме того, оно позволит снизить риски давления на котировки и избежать резких изменений курса Компании, связанных с возможной продажей крупных пакетов акций.

Доля акций в свободном обращении (free-float),
% от обыкновенных акций



Структура акционерного капитала и количество акций на 31 декабря 2025 года



1 Лица, владеющие 5% и более от уставного капитала.
2 Миноритарные акционеры — более 200 тыс. акционеров — физических и юридических лиц.

Наши акционеры

На момент листинга в декабре 2021 года акционерами Компании являлись ее основатели и около 1,4 тыс. действующих и бывших сотрудников. По результатам первичного прямого листинга акционерами Компании стали еще около 10 тыс. лиц. За четыре года количество владельцев акций выросло примерно в 18 раз. Показательно, что даже на фоне вызовов 2024 года база инвесторов сохранила стабильность: по состоянию на конец 2025 года число акционеров превысило 200 тыс.

Большинство из них — частные инвесторы, причем более 50% держат акции POSI больше года и являются долгосрочными инвесторами. Высокий интерес к акциям Positive Technologies проявляют и институциональные инвесторы — на конец 2025 года среди них было более 170 фондов и юридических лиц. На 31 декабря 2025 года доля институциональных инвесторов составила 6,4% от общего количества акций в обращении, или 24,8% от free-float.

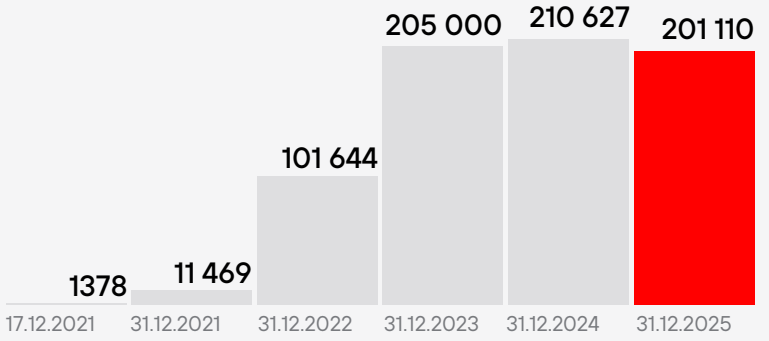
>50%
количество долгосрочных инвесторов, которые держат акции более года

42 года
средний возраст инвесторов

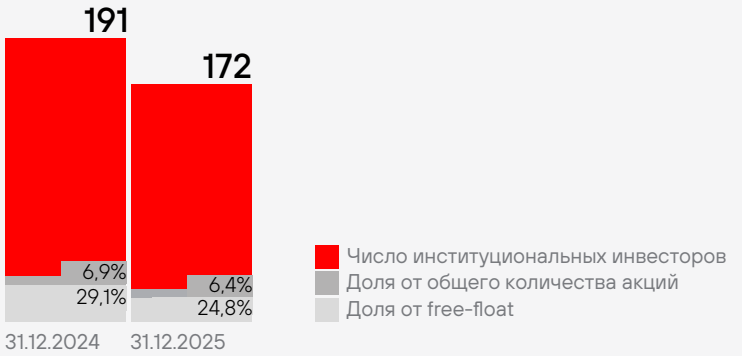
97 лет
самому почтенному

5 лет
самому молодому

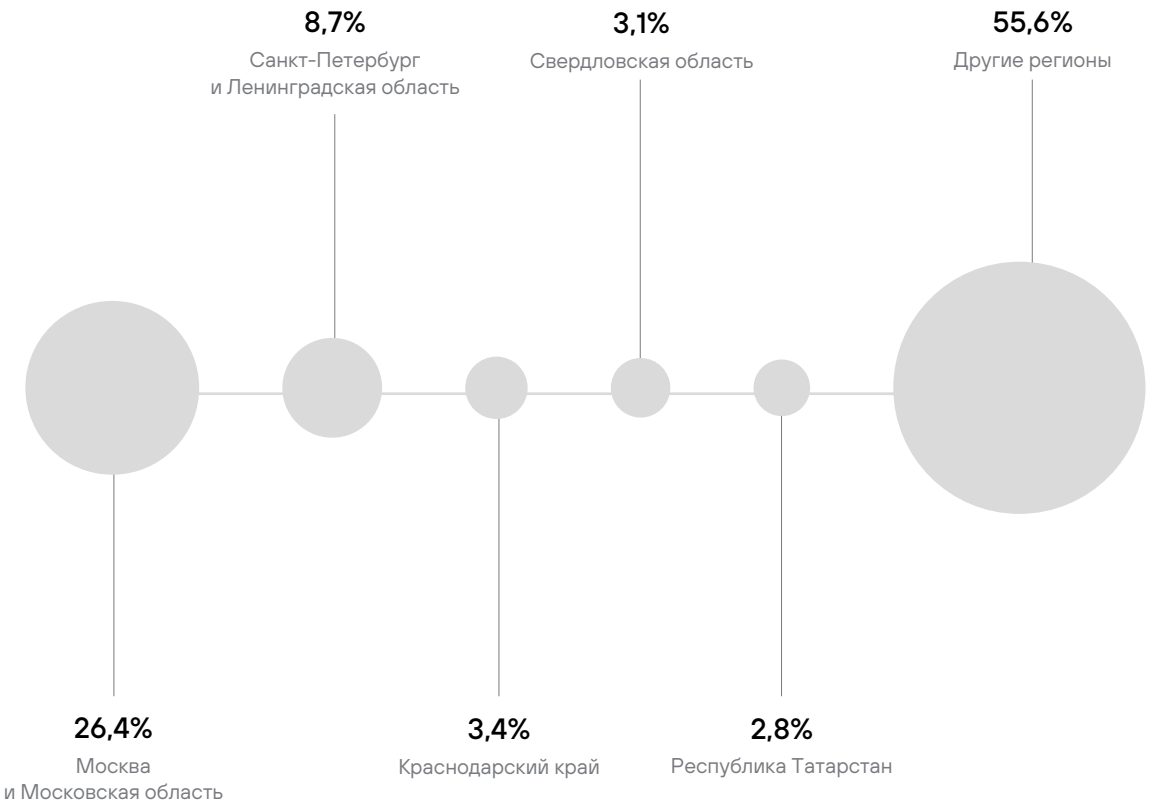
Динамика числа акционеров Positive Technologies, физических и юридических лиц



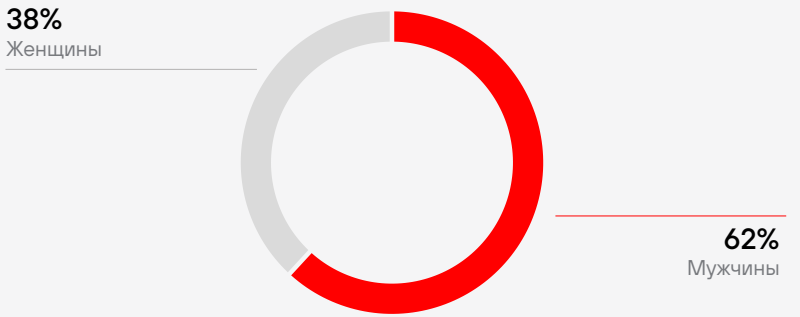
Динамика числа и доли институциональных инвесторов Positive Technologies, фондов и юридических лиц



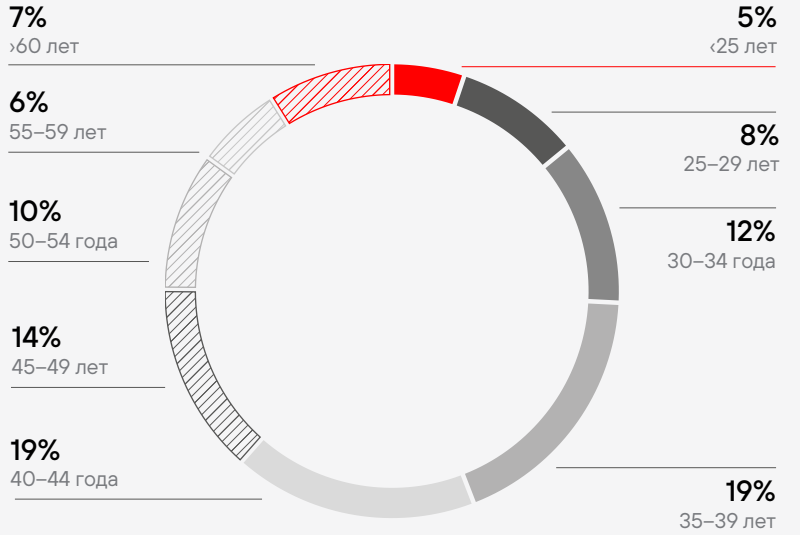
География проживания наших совладельцев



Распределение инвесторов по полу



Распределение инвесторов по возрасту



Принципы работы с капиталом и Программа стимулирования роста капитализации

В 2024 году Positive Technologies разработала комплексный подход к управлению капиталом, включающий принципы работы с капиталом и Программу стимулирования роста капитализации, которая была создана в соответствии с лучшими практиками корпоративного управления.

Политика работы с капиталом подразумевает инвестиции в те направления, которые, как мы верим, позволят стимулировать значительный рост стоимости Компании.

Инвестиции могут быть направлены на Программу стимулирования роста капитализации, проведение сделок M&A с компаниями, комплементарными нашей стратегии в России и в мире, а также капитальные вложения в исследовательские лаборатории, новые офисы, дата-центры и другое. Дополнительно предусмотрена оптимизация структуры долга.

Для реализации этих инициатив формируется резервный фонд акций, источниками финансирования которого выступают дополнительная эмиссия акций, обратный выкуп акций, а также инвестиционное заемное финансирование.

Такие инвестиции не повлияют на дивидендный потенциал Компании, а связанные с ними расходы будут капитализироваться в отчетности по МСФО и управленческим стандартам. Этот подход позволяет сохранить баланс между развитием бизнеса и интересами акционеров.

Одним из инструментов — источников финансирования является допэмиссия. Объем и сроки допэмиссии будут определяться по итогам года с учетом темпов роста бизнеса и капитализации Компании.

- В случае отсутствия роста капитализации допэмиссия проводиться не будет. При наличии роста капитализации объем дополнительного выпуска определяется по формуле.
- Формула предполагает, что на каждый двукратный рост капитализации Компании максимальная величина допэмиссии может составить 15%. В случае если рост капитализации за один год превышает двукратный, допэмиссия будет ограничена 15%.
- После расчета объем выпуска может быть скорректирован в сторону уменьшения в зависимости от потребностей Компании. Увеличение рассчитанного по формуле объема выпуска не допускается.

Согласно формуле, объем дополнительного выпуска в 2024 году составил 7,9% от уставного капитала. Распределение акций контрибьюторам стартовало в конце 2024 года и технически завершилось в декабре 2025 года. По итогам программы акции получили 1900 контрибьюторов.

В 2025 году по итогам 2024 года Компания не проводила дополнительную эмиссию в связи с отсутствием роста капитализации.

Источники финансирования

Дополнительная эмиссия акций

Обратный выкуп акций

Инвестиционное заемное финансирование

Объекты финансирования

Программа стимулирования роста капитализации

Сделки M&A: продукты, технологии, компании, ноу-хау

Капитальные вложения: исследовательские лаборатории, дата-центры

Оптимизация структуры долга

Инвестиции в эти направления позволят стимулировать значительный рост бизнеса и капитализации Компании.

КАЛЕНДАРЬ ИНВЕСТОРА

I квартал

Февраль

- Публикация предварительных данных по отгрузкам за 2025 год
- Форум «Будущее рынка акций» от «Эксперт РА»
- Конференция IPO-2026
- Конференция «Cbonds & Smart-Lab PRO облигации»
- Всероссийский форум по корпоративному управлению от АНД

Март

- IV Российский форум финансового рынка от АКРА
- Инвестиционный форум ВТБ «Россия зовет!» (Екатеринбург)

II квартал

Апрель

- Публикация консолидированной аудированной финансовой отчетности за 2025 год и мероприятие для инвесторов
- Публикация аудированной отчетности за I квартал 2025 года
- Конференция PROFIT

Май

- Годовое заседание Общего собрания акционеров в очном формате
- Investfunds Forum XVII — конференция институциональных инвесторов

Июнь

- ПМЭФ
- Т-Двор
- XVI Российский M&A конгресс
- Smart-Lab Conf (Санкт-Петербург)

III квартал

Июль

- Публикация отчетности за II квартал и шесть месяцев 2026 года

Сентябрь

- IR-форум Московской биржи
- Форум розничных инвесторов

IV квартал

Октябрь

- Smart-Lab Conf (Москва)
- Конференция Investment Leaders Forum

Ноябрь

- Публикация неаудированной отчетности за III квартал и девять месяцев 2026 года
- Конференция PROFIT

Декабрь

- XXIV Российский облигационный конгресс

Календарь инвестора

УСТОЙЧИВОЕ РАЗВИТИЕ

- Принципы устойчивого развития
- Система управления устойчивым развитием
- Наша команда
- Охрана труда и здоровья
- Образование и киберпросвещение
- Благотворительность
- Вклад в экологию

Инициативы, которые меняют мир

Мы стремимся развивать среду, в которой работаем, создавая пространство для диалога в индустрии, укрепляя профессиональное сообщество и поддерживая рост экспертизы.

Образовательные программы и мероприятия Positive Technologies помогают специалистам совершенствовать навыки, делиться опытом и находить единомышленников. При этом мы делаем кибербезопасность более доступной и понятной широкой аудитории, популяризируя сферу и привлекая в нее новые таланты.

- **Positive Education**

  Формируем экспертов, которые делают кибербезопасность результативной

- **Standoff 365**

  Проводим масштабные кибербитвы, прокачиваем скилы на киберполигонах

- **Positive Hack Camp**

  Обучаем практической кибербезопасности на международной арене

- **Positive Hack Days**

  Предоставляем открытую платформу для диалога и развития индустрии

- **Positive Hack Talks**

  Создаем глобальное комьюнити, отвечая на вопросы профессионалов

ПРИНЦИПЫ УСТОЙЧИВОГО РАЗВИТИЯ

В эпоху тотальной цифровизации кибербезопасность перестает быть чисто техническим вопросом и становится базовым условием устойчивого развития общества. Сегодня мир нуждается в новой цифровой архитектуре, которая обеспечит безопасность и независимость. Наша цель — стать теми, кто строит новый мир, где технологии служат людям, не ставя под угрозу их суверенитет и безопасность.

Адаптивность и глобальное присутствие

Более 20 лет Positive Technologies играет важную роль в развитии технологий ИБ. Компания успешно адаптируется к внешним вызовам, совершенствует продукты и сервисы и расширяет географию присутствия. Сегодня продукты и сервисы Positive Technologies востребованы не только в России, мы видим к ним интерес в Латинской Америке, Азии и Африке, а также на Ближнем Востоке.

Технологический суверенитет и инновации

Сегодня наша экосистема включает более 25 продуктов и решений. Мы продолжаем разрабатывать инновационные технологии для защиты от актуальных киберугроз, а также вносим вклад в технологический суверенитет страны, создавая решения, не зависящие от иностранных разработок.

Мы обеспечиваем защиту государственных структур, бизнеса и критической инфраструктуры, помогаем клиентам достичь результативной кибербезопасности и предотвратить угрозы, которые могут повлиять на экономику, экологию и безопасность людей. Кроме того, мы обеспечиваем безопасность знаковых событий — чемпионатов мира по футболу, президентских и региональных выборов, «Игр Будущего», минимизируя риски кибератак в реальном времени.

Популяризация кибербезопасности

В мае 2025 года мы провели в «Лужниках» международный киберфестиваль Positive Hack Days Fest, в котором приняли участие более 150 тыс. человек из 42 стран. Киберфестиваль вновь объединил две программы — для профессионалов и широкой аудитории. В профессиональной части выступили более 500 спикеров с докладами по самым актуальным темам. В открытой зоне развернулся цифровой мегаполис, где гости могли протестировать интерактивные образовательные инсталляции. Мы сделали тему кибербезопасности понятной и доступной широкой аудитории, помогая повысить осведомленность о цифровых угрозах и способах защиты.

Развитие профессионального сообщества

Мы активно развиваем наши образовательные программы: расширяем сотрудничество с вузами, усиливаем корпоративное и профессиональное обучение, масштабируем подготовку преподавателей, проводим обучение по эффективному использованию продуктов Positive Technologies и реализуем международные образовательные инициативы, включая Positive Hack Camp.

КАК МЫ ПОМОГАЕМ ЗАЩИЩАТЬ СУВЕРЕНИТЕТ В ЦИФРОВОМ МИРЕ

Сотрудникам Positive Technologies

- Создаем атмосферу постоянного обучения и развития
- Открываем перспективы для профессионального и карьерного роста
- Заботимся о здоровье сотрудников

Профессионалам отрасли

- Формируем отраслевые стандарты
- Создаем систему профессионального обучения
- Даем возможность совершенствовать практические навыки

Государству и обществу

- Помогаем достичь результативной кибербезопасности на объектах КИИ
- Защищаем мероприятия федерального значения
- Обеспечиваем технологический и цифровой суверенитет
- Укрепляем доверие к технологиям и внедряем инновации
- Создаем рабочие места
- Занимаемся киберпросвещением
- Готовим кадры для индустрии, начиная со школьной скамьи
- Ведем благотворительную деятельность

Нашим клиентам

- Выстраиваем систему результативной кибербезопасности
- Помогаем снизить киберриски
- Помогаем вести стабильный, устойчивый бизнес

СИСТЕМА УПРАВЛЕНИЯ УСТОЙЧИВЫМ РАЗВИТИЕМ

Совет директоров

- Определяет стратегические направления развития
- Отвечает за совершенствование корпоративного управления

Генеральный директор

Отвечает за построение и развитие системы управления устойчивым развитием, контролирует функционирование системы управления охраной труда, работу HR-службы, соблюдение мер по охране окружающей среды

Директор по персоналу

Отвечает за подбор и развитие персонала, разработку мер по охране труда

Директор образовательных программ и проектов

Отвечает за разработку мероприятий в сфере образования и просвещения

Руководители структурных подразделений, отдел охраны труда, HR-служба

Отвечают за управление персоналом на местах, реализацию мер по промышленной безопасности, охране труда и охране окружающей среды в подразделениях Компании, снижение потребления ресурсов и повышение энергоэффективности

НАША КОМАНДА

В 2025 году мы пересмотрели структуру команд, в результате чего часть сотрудников покинула Компанию. Этот процесс позволил нам вернуться к базовым ценностям и ключевым принципам нашей работы: экспертиза, смысл, вовлеченность, создание среды, привлекательной для талантов.

Мы получили ясность в том, какие направления и команды создают максимальную ценность для Компании и разделяют ее миссию — активно работать над продуктами и задачами, которые по-настоящему решают проблему кибербезопасности.

Трансформация дала возможность сосредоточиться на направлениях с реальной перспективой и сильными командами. И мы продолжаем развивать нашу экспертизу и среду, где талантливые люди могут развиваться, экспериментировать и активно вовлекаться в создание продуктов, которые меняют индустрию.

Несмотря на непростой год, мы продолжили привлекать новые кадры. Фокус был не на количестве, а на качестве: мы искали сильных ребят, кто соответствует нашей миссии и разделяет ценности Компании. И несмотря на сложный год, сохраняли способность нанимать более 30% новых сотрудников по внутренним рекомендациям. Важно отметить, что Positive Technologies никогда не имела денежную реферальную программу — нам важно, чтобы люди хотели рекомендовать классных специалистов (друзей и коллег), разделяя наши смыслы и вызовы.

Новые руководители и топ-таланты отмечали, что выбирают Positive Technologies именно за людей вокруг, видение Компании и реальный смысл работы.

Привлекательная среда

Наша цель — строить не просто технологическую и экспертную компанию, а комьюнити, которое притягивает таланты и делает их сильнее.

В 2025 году мы делали акцент на разнообразии управленческих практик и подходов, которые существуют в наших командах. Вместе с руководителями мы создавали обучение на базе реальных кейсов, с которыми сталкиваются тимлиды ежедневно в своей работе: от обратной связи до вопроса, как поддерживать команды в условиях постоянных изменений.
Мы уверены, что такие форматы не просто помогают управлять, а вдохновляют команды на большие идеи и помогают им расти.
Чтобы создавать продукты, которые действительно будут результативными, мы продолжаем вкладываться в развитие ИБ-экспертизы.

В 2025 году в Компании сформировался полноценный учебный трек от погружения в основы кибербезопасности и действия атакующих до внутренних киберучений, где продуктовые команды в течение недели проживают опыт реализации проекта результативной кибербезопасности — от выявления критичных рисков до внедрения наших продуктов, отражения реальных атак и расследования инцидентов.
За прошедший год через этот трек прошли более 300 сотрудников.

В течение года мы активно развивали программы обучения, предоставляя сотрудникам доступ к самым актуальным знаниям и навыкам: успешно запустились и прошли курсы по работе с LLM и алгоритмам. И как всегда, обучение создавалось силами наших сотрудников и ведущих внешних экспертов, которым мы доверяем. Например, курс по работе с LLM был посвящен тому, как повысить эффективность разработки. Спикерами выступали сотрудники, которые уже грамотно и активно применяют LLM в повседневных рабочих задачах. Каждый воркшоп посещали в среднем 200 сотрудников, а количество тех, кто ежедневно использует Positive LLM, выросло в два раза.

Наш подход к обучению формирует в команде уникальную экспертизу на стыке ИБ, ML и алгоритмов и позволяет решать задачи, на которые другие только смотрят.

›300

сотрудников прошли через учебный трек по ИБ за 2025 год

200

сотрудников в среднем посещали каждый воркшоп по работе с LLM

x2

выросло число сотрудников, использующих Positive LLM

Профессиональные и экспертные сообщества

›100

докладов сделали сотрудники Компании в 2025 году на отраслевых мероприятиях

В прошедшем году мы продолжили поддерживать спикеров в Компании: подбирали подходящие площадки, помогали делать заявки на доклады и готовиться к выступлениям. В 2025 году сотрудники Positive Technologies прочитали более 100 докладов на мероприятиях для специалистов по безопасности и разработчиков, включая такие отраслевые конференции, как OFFZONE, ZeroNights, SOC Forum, C++ Russia, Codefest.

Наши сотрудники принимали участие в подкастах и митапах, а также в программных комитетах, формирующих повестку отраслевых событий в ИТ и кибербезопасности (OFFZONE, SOC Forum, «РусКрипто», Southub, SmartData и других). Мы также продолжаем проводить олимпиады по программированию — это неклассические соревнования по решению алгоритмических задач для сотрудников Positive Technologies, студентов и ИТ-специалистов со всего рынка. Для нас это отличная площадка для знакомства, сотворчества и обмена опытом. В 2025 году мы провели две публичные олимпиады и одну камерную — только для сотрудников Компании. Олимпиадное комьюнити в телеграм-канале объединило уже более 660 человек, а мероприятия собирают около 150 участников.

Олимпиады

›660 человек

олимпиадное комьюнити

1

камерная

~150

участников на каждом мероприятии

2

публичные

Наши сотрудники приняли участие в OFFZONE, ZeroNights, SOC Forum, C++ Russia, Codefest, «РусКрипто», Southub, SmartData и других отраслевых мероприятиях.

Таланты и молодежь

В 2025 мы задали себе вопрос: в какую компанию мы бы сами пришли в двадцать лет? Отвечая на него, мы строим такую компанию, в которой молодые специалисты видят не просто работу, а среду для роста и предпринимательства: здесь они учатся у экспертов и получают практические задачи, чтобы развивать продукты и технологии.

За прошедший год мы обновили подходы к приему на стажировку — теперь в Компании есть разные треки для направлений разработки, реверс-инжиниринга, ИБ, ML. Вместо шаблонных практик мы активно используем реальные проекты с наставниками, чтобы студенты сразу вливались в команды и приносили свежий взгляд.

В основе нашей культуры лежит преемственность. Поддержка талантов позволяет нам растить молодых специалистов и руководителей внутри и не терять экспертизу. Это особенно важно в тех направлениях, где готовых талантливых ребят нельзя получить просто из университета. Личное наставничество в таких ситуациях помогает передавать не только навыки, а культуру работы над продуктом и развития бизнеса.

Например, за этот год именно из стажеров у нас собралась команда исследователей безопасности операционных систем, которую возглавляет главный исследователь Александр Попов. Команда Александра уже показывает высокие результаты, а молодые специалисты, выросшие из стажеров, вместе уже готовятся брать к себе новых студентов. Для нас это не просто наем и закрытие ставок, а полноценное «клонирование» талантов с очень редкой и ценной экспертизой.

Внутреннее предпринимательство и рост лидеров: кейс PT NGFW / «ТризТех»

Для Positive Technologies способность к внутреннему предпринимательству — ключ к росту и масштабированию. Мы создаем условия, в которых сотрудники могут запускать новые проекты, тестировать идеи и брать ответственность за развитие направлений, формируя лидеров внутри Компании.

PT NGFW начался как внутренний стартап и в 2024 году стал одним из самых ожидаемых продуктов индустрии, заработав более 1 млрд руб. Чтобы ускорить развитие продукта и масштабировать успех, PT NGFW выделили в отдельную компанию — «ТризТех», CEO которой стал Денис Кораблев. Для сотрудников процессы и поддержка остались прежними, а результаты продукта учитываются в финансовых итогах Positive Technologies.

Кейс PT NGFW / «ТризТех» демонстрирует, как мы растим внутреннее предпринимательство и лидеров: сотрудники получают возможность создавать новые направления, строить команды и управлять продуктами, оставаясь частью корпоративного комьюнити и усиливая экспертизу Компании.

Сейловая трансформация

В 2025 году мы сосредоточились на усилении блока продаж и возвращении способности бизнеса быть бизнесом. Главной задачей стало создание прозрачных процессов и более тесного взаимодействия между командами продуктов и продаж, чтобы они действовали как единая команда.

Мы вернулись к принципу построения планов «от земли», обсуждая их с сейлами и руководителями департаментов, — этот принцип сработал. Люди, отвечающие за поступление денег, делали все возможное, чтобы достичь целей, а Компания поддерживала их во всем и давала все необходимые инструменты.

Пересборка и укрепление R&D позволили создавать успешные кейсы, на которые сейлы могли опираться в работе с рынком. Это укрепило доверие между функциями и показало, что бизнес может работать системно, а не только за счет индивидуальных усилий, повышая предсказуемость результатов и устойчивость Компании в долгосрочной перспективе.

Концепция совладения

Positive Technologies уже более десяти лет развивает систему совладения, когда сотрудники и внешние партнеры могут получить акции Компании за вклад в рост бизнеса: создание сильных команд, запуск новых продуктов, развитие ключевых направлений и любые решения, которые создают значимую ценность для Компании. Такая система помогает выращивать лидеров и привлекать сильных специалистов, которые выступают не исполнителями, а соавторами бизнеса и связывают свою реализацию с результатами Компании. Она стала одним из факторов кратного роста Positive Technologies от небольшой частной структуры до многомиллиардной публичной компании. После выхода на биржу эта система была формализована в Программу стимулирования роста капитализации, где контрибьюторы в рост бизнеса и капитализации Компании получают акции.

Участниками программы на протяжении всего времени становились действующие и бывшие сотрудники, топ-менеджеры, а также внешние специалисты, консультанты и партнеры, которые внесли существенный вклад в рост стоимости бизнеса.

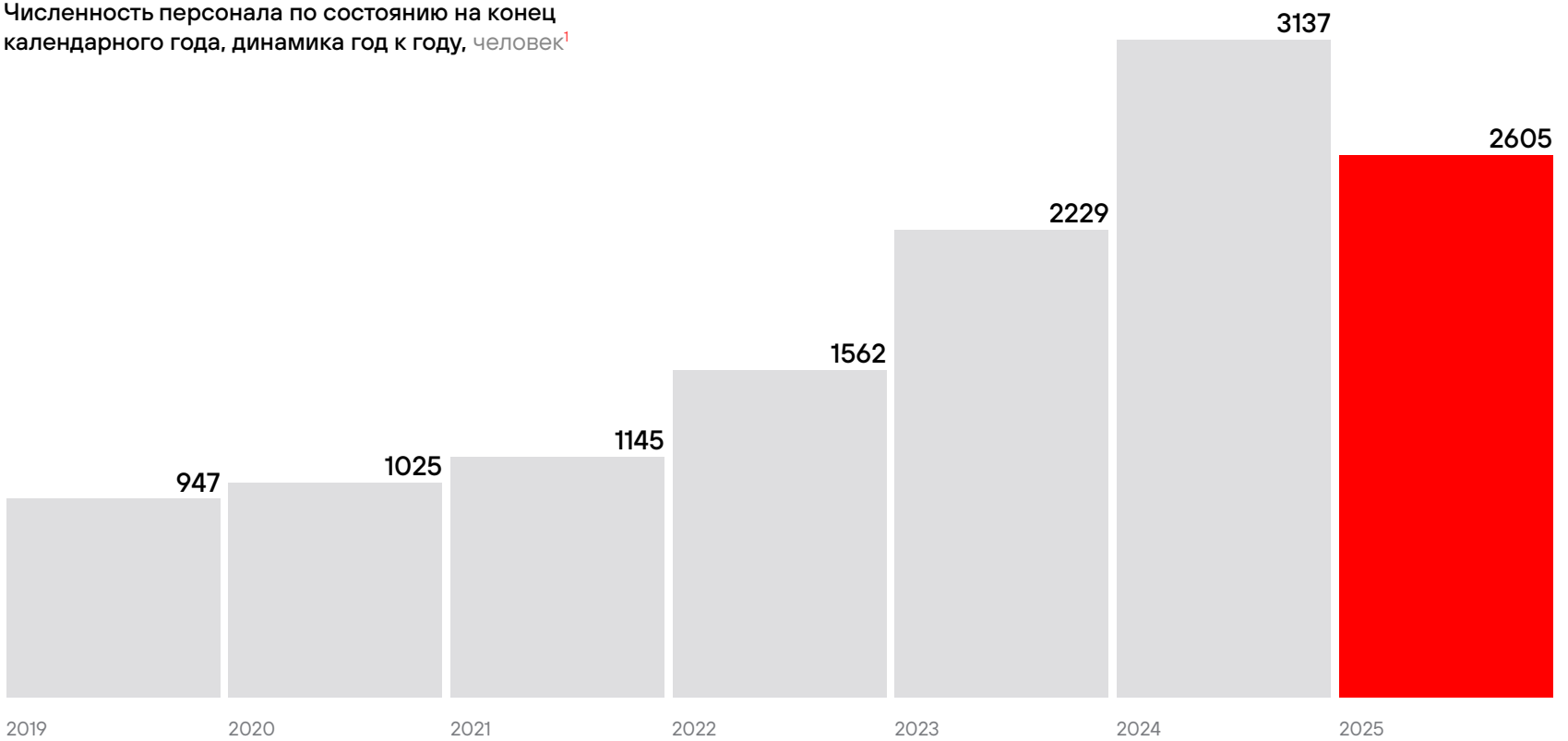
Подробнее про развитие концепции совладения, принципы работы с капиталом и Программу стимулирования роста капитализации читайте в разделе «Взаимодействие с инвесторами: архитектура доверия»

Численность команды

Наша цель — создание сильной и эффективной команды. В течение года к нам присоединились 358 человек. По состоянию на 31 декабря 2025 года в Компании работали 2605 сотрудников. Относительное изменение численности за год составляет – 17%.

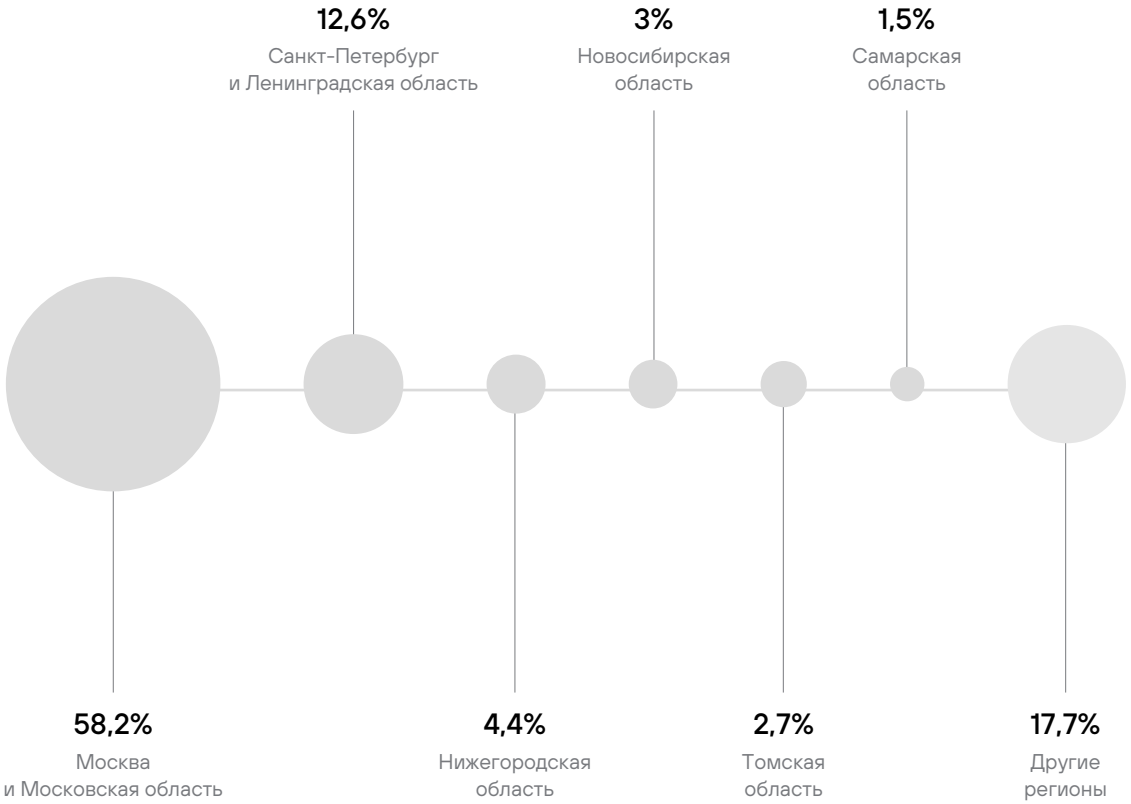
Снижение численности персонала обусловлено реализацией мер по повышению эффективности бизнеса. На фоне снижения объема отгрузок и невыполнения финансовых целей по итогам 2024 года Компания провела масштабную трансформацию бизнеса, одним из ключевых элементов которой был фокус на эффективности. В рамках этой работы Компания ориентировалась на поддержание численности сотрудников на уровне середины 2024 года, продолжая сохранять сопоставимую численность персонала и по состоянию на конец 2025 года.

Численность персонала по состоянию на конец календарного года, динамика год к году, человек[1]

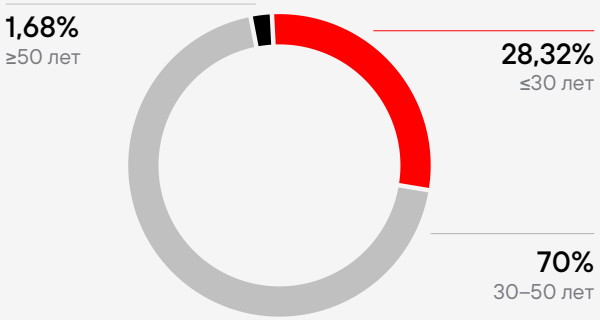


1 За исключением сотрудников, находящихся в декретном отпуске и отпуске по уходу за ребенком, а также стажеров.

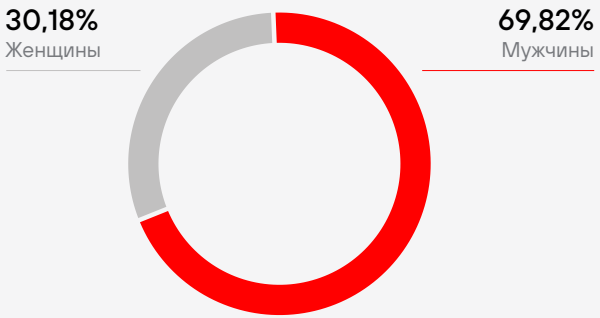
Регионы проживания персонала по состоянию на 31 декабря 2025 года



Возрастная структура персонала по состоянию на 31 декабря 2025 года



Гендерная структура персонала по состоянию на 31 декабря 2025 года



ОХРАНА ТРУДА И ЗДОРОВЬЯ

Мы заботимся о благополучии и здоровье наших сотрудников. Ежегодно мы проводим специальную оценку условий труда (СОУТ) согласно Положению о СУОТ и ежегодным перечням мероприятий.

Обучение руководителей и специалистов Компании в области охраны труда, электро- и пожарной безопасности и приемам оказания первой помощи проводится в соответствии с требованиями нормативных актов в специализированных учебных центрах.

Для профилактики и предупреждения профессиональных заболеваний мы оснащаем рабочие места персонала современными компьютерами и эргономичной мебелью. В 2025 году в Компании не было зарегистрировано несчастных случаев и профессиональных заболеваний.

ОБРАЗОВАНИЕ И КИБЕРПРОСВЕЩЕНИЕ

Positive Education

Центр практического обучения, созданный на базе экспертизы Positive Technologies.

Центр формирует устойчивые навыки противодействия киберугрозам у специалистов, управленцев и руководителей, помогая организациям выстраивать системную защиту и повышать уровень киберустойчивости.

Результаты 2025 года

- За 2025 год мы усилили компетенции в области ИБ у 14,5 тыс. специалистов благодаря практикумам и образовательным программам центра.
- Проведено обучение для 100+ генеральных директоров, направленное на интеграцию кибербезопасности в стратегию развития компаний, а также 400+ управленцев и представителей органов власти, ресурсоснабжающих организаций и бизнес-объединений.
- 8 тыс. специалистов подтвердили свои компетенции по работе с продуктами Positive Technologies, обеспечивая более эффективное использование технологий защиты в ежедневной практике.
- Провели обучение среди 500 специалистов ИТ и ИБ в Индонезии, ОАЭ, Египте, что усиливает международное присутствие Positive Technologies и способствует развитию локальной экспертизы в каждой из стран.
- Провели глобальную образовательную инициативу Positive Hack Camp, где объединили 90 молодых специалистов из более чем 25 стран Азии, Африки, Ближнего Востока и Латинской Америки.
- Завершили обучение преподавателей из 500 учебных заведений Армении, Беларуси, Казахстана, Киргизии, России и Узбекистана, что позволило масштабировать подготовку специалистов через образовательные системы этих стран.

Деятельность Центра

1

Корпоративное обучение

Positive Education разрабатывает и реализует корпоративные образовательные программы, направленные на повышение киберустойчивости организаций.

Обучение строится с учетом отраслевой специфики, уровня зрелости процессов безопасности и актуального ландшафта угроз. Программы помогают:

- формировать стратегический подход к кибербезопасности на уровне топ-менеджмента;
- развивать практические навыки реагирования на инциденты;
- выстраивать эффективные процессы защиты внутри компаний;
- снижать операционные и репутационные риски.

Отдельное внимание уделяется обучению руководителей — принятые ими решения напрямую влияют на устойчивость бизнеса в условиях растущих киберугроз.

2

Профессиональное обучение

Чтобы повысить кибербезопасность в организациях, мы учим их специалистов строить процессы кибербезопасности системно. Сегодня мы обучаем по следующим корпоративным программам:

- «Управление уязвимостями: от теории к практике»,
- «Безопасность приложений: курс для инженеров»,
- «Безопасность приложений: от хаоса к системному управлению»,
- «Архитектура сетевой безопасности предприятия»,
- «Анализ сетевого трафика: искусство обнаружения атак»,
- «Построение SOC 2.0: от концепции до реализации»,
- «Харденинг ИТ: от дизайна до настроек»,
- «Атаки на АСУ ТП: анализ трафика и защита промышленных систем»,
- «Мониторинг и реагирование на инциденты».

3

Обучение по эффективному использованию продуктов Positive Technologies

Positive Education обеспечивает комплексную подготовку специалистов, работающих с решениями Positive Technologies, помогая организациям максимально реализовать потенциал внедренных технологий кибербезопасности.

Программы обучения охватывают весь жизненный цикл работы с продуктами — от базовой настройки до продвинутых сценариев эксплуатации для повышения качества мониторинга и реагирования.

Обучение позволяет организациям:

- ускорять внедрение решений и сокращать время выхода на целевой уровень защищенности;
- повышать эффективность использования функциональности продуктов;
- снижать риски, связанные с эксплуатационными ошибками;
- формировать внутреннюю экспертизу и уменьшать зависимость от внешних ресурсов.

Деятельность Центра

4

Сотрудничество с вузами

Развиваем партнерство с университетами и помогаем готовить востребованные кадры для рынка кибербезопасности через совместные образовательные проекты и практико-ориентированное обучение. В рамках сотрудничества мы запускаем бакалаврские и магистерские программы, лаборатории и классы для практических занятий, готовим преподавателей и совместно разрабатываем курсы по offensive/defensive security и безопасной разработке.

Взаимодействие помогает:

- сокращать разрыв между академическим образованием и потребностями индустрии ИБ;
- готовить специалистов, способных решать реальные задачи ИБ;
- повышать общий уровень киберустойчивости организаций и государственных систем.

Партнерство с университетами обеспечивает долгосрочное развитие профессионального сообщества и способствует формированию новой генерации экспертов в области кибербезопасности.

5

Развитие культуры кибербезопасности в других странах

Positive Education способствует развитию культуры кибербезопасности за пределами России, поддерживая формирование устойчивых национальных компетенций в области защиты цифровой инфраструктуры.

Реализуем образовательные инициативы для государственных организаций, бизнеса и профессиональных сообществ, передавая практическую экспертизу и современные подходы к противодействию киберугрозам.

Деятельность Positive Education направлена на то, чтобы помочь странам:

- развивать собственные кадровые ресурсы в сфере ИБ;
- повышать устойчивость критически важных систем;
- формировать системный подход к управлению киберрисками;
- укреплять технологическую независимость;
- обеспечить технологический суверенитет.

Международные образовательные проекты Positive Education создают основу для долгосрочного сотрудничества Positive Technologies и способствуют повышению глобального уровня киберустойчивости.

Positive Hack Days

42 страны

были представлены
на фестивале в 2025 году

С 22 по 24 мая 2025 года спортивный комплекс «Лужники» в Москве стал центром кибербезопасности — здесь прошел международный киберфестиваль Positive Hack Days (PHDays Fest). Мероприятие было организовано Компанией при поддержке Минцифры России. Стратегическим партнером выступило Правительство Москвы: поддержку оказывали Комплекс социального развития, Департамент информационных технологий, Департамент предпринимательства и инновационного развития.

В течение трех дней на одной площадке собирались лучшие эксперты, представители министерств и ведомств, топ-менеджеры компаний, разработчики, хакеры и все, кто интересуется защитой цифрового мира.

Фестиваль вновь объединил две программы — для профессионалов и широкой аудитории. Техническая программа включала 26 треков по разным направлениям и 270 докладов, охватывающих ключевые вопросы ИБ. На фестивале выступили свыше 500 спикеров — от начинающих техноэнтузиастов до топовых специалистов, CIO и CISO крупных ИТ-компаний.

В открытой зоне развернулся цифровой мегаполис, где гости могли протестировать интерактивные образовательные инсталляции, узнать о современных киберугрозах и прокачать цифровую грамотность.

Интерес к фестивалю достиг рекордных масштабов: более 150 тыс. человек посетили открытую зону, а свыше 180 тыс. зрителей следили за мероприятием онлайн.

PHDays Fest подтвердил статус значимого международного события, приняв делегации из 42 стран. Ключевой темой межгосударственного диалога стала технологическая кооперация как фундамент цифрового суверенитета. Кроме того, в рамках киберфестиваля мы провели День инвестора, предоставив акционерам возможность лично пообщаться с руководством Компании и задать интересующие вопросы.

›150 тыс. человек

посетили открытую зону фестиваля

›180 тыс. зрителей

онлайн-трансляции

›500 спикеров

Для чего мы проводим Positive Hack Days

В 2025 году Positive Hack Days проходил уже в 14-й раз, преодолев путь от узкоспециализированного мероприятия до масштабного городского киберфестиваля. Ранее в мире кибербезопасности существовали три разрозненных сообщества — хакеры-исследователи, заказчики и регуляторы, которые практически не взаимодействовали. Регуляторы не понимали, как происходит взлом, бизнес жил в своем замкнутом мире, а хакеры обсуждали исследования в узком кругу. Формат конференций тоже был предсказуемым: либо неформальные встречи в баре, либо сухие доклады с трибуны.

Мы решили изменить это и объединить «пиджаки» и «футболки» на одной площадке. С самого начала Positive Hack Days задумывался как место, где сообщество может реализовывать свои идеи, а диалог между всеми участниками индустрии становится открытым и честным.

Долгое время фестиваль оставался камерным событием для профессионалов отрасли, но в 2023 году мы впервые сделали его доступным для всех. Тогда Positive Hack Days прошел в Парке Горького, что стало важным шагом в популяризации кибербезопасности. В 2025 году фестиваль в «Лужниках» закрепил этот успех.

Positive Hack Days является не просто местом встречи профессионалов, а мощным инструментом для развития нашего бизнеса и расширения его возможностей. Мероприятие способствует повышению узнаваемости бренда, укреплению наших позиций лидера на рынке, привлекает новых клиентов и экспертов, что в долгосрочной перспективе положительно сказывается на стоимости акций и на доходах акционеров.

Культурная экспансия

Ключевая составляющая выхода Positive Technologies на глобальную арену.

В конце 2022 года мы перезапустили наш международный бизнес, выбрав фокусные направления развития — это дружественные страны, готовые к сотрудничеству с российскими компаниями. Запуская стратегическое для нас направление, мы были и остаемся уверены в том, что наше международное присутствие должно быть не только операционным, но и в первую очередь интеллектуальным, основанным на технологической и профессиональной культурной экспансии. Именно те специалисты, которые понимают, какая экспертиза заложена в наши технологии, могут непредвзято относиться к продуктам Positive Technologies и возможностям работы с нами.

Positive Hack Camp

Positive Hack Camp — глобальная образовательная инициатива Positive Technologies и Positive Education для начинающих специалистов по кибербезопасности. Наша цель — содействие странам в развитии профессиональных кадров и компетенций для обеспечения их киберсуверенитета и устойчивого цифрового будущего.

В августе 2025 года состоялось второе мероприятие серии. На участие было подано 765 заявок, что более чем в два раза превысило показатели прошлого года. По итогам отборочного тура участниками стали более 90 молодых специалистов с необходимым уровнем ИТ-подготовки из Индии, Индонезии, Малайзии, Вьетнама, Саудовской Аравии, Египта, ОАЭ, Ирана, а также других стран Юго-Восточной Азии, Ближнего Востока, Африки и Латинской Америки.

В течение двух недель ведущие эксперты делились опытом с участниками в рамках интенсивной учебной программы. Помимо обучения и практических занятий, программа включала знакомство с российской культурой. Это способствовало укреплению международных связей и позволило донести наш культурный код до глобального профессионального сообщества. Проект получит продолжение в 2026 году: новая смена Positive Hack Camp пройдет в Москве с 25 июля по 9 августа.

Positive Hack Talks

Positive Hack Talks представляет собой серию открытых международных мероприятий для профессионалов индустрии кибербезопасности. Данная инициатива, запущенная в 2024 году, направлена на формирование глобального экспертного сообщества, обмен актуальными знаниями и совместное противодействие растущим мировым киберугрозам. Первые митапы серии прошли в октябре и ноябре 2024 года в Бангалоре (Индия) и Ханое(Вьетнам).

В 2025 году проект продолжил активное развитие: в феврале в Каире состоялось третье мероприятие, собравшее более 200 участников. Выбор столицы Египта обусловлен стратегическим присутствием бизнеса Компании в регионе через сеть локальных партнеров. Четвертый митап прошел в июле в Джакарте и объединил более 370 специалистов. Индонезия является одной из фокусных стран для развития международного бизнеса Positive Technologies, что подтверждается высоким интересом местного профессионального сообщества к экспертизе Компании. Пятый митап серии состоялся в декабре в Сан-Паулу (Бразилия), его посетили более 170 специалистов. Программа мероприятий объединила признанных экспертов, начинающих исследователей и студентов профильных вузов. В рамках выступлений участники обсудили глобальные тренды индустрии и разобрали реальные кейсы, после чего продолжили профессиональное общение в неформальной обстановке.

Для нас Positive Hack Talks — это важная часть создания глобального комьюнити профессионалов, где можно свободно обмениваться знаниями и вместе работать над тем, чтобы повышать уровень защищенности и противостоять росту числа киберугроз во всем мире.

Сегодня зарубежные страны заинтересованы в импорте не только российских решений в области кибербезопасности, но и наших навыков.

Специалисты Positive Technologies накопили большой объем уникальной экспертизы и готовы делиться опытом с коллегами по всему миру. Для этого мы и проводим Positive Hack Camp — развиваем комьюнити экспертов по кибербезопасности. За две недели, разбирая практические кейсы, молодые специалисты больше узнают о современных подходах к анализу защищенности и научатся применять эти знания для укрепления цифровой безопасности своих государств.

Дмитрий Серебрянников,
директор Positive Technologies
по анализу защищенности

БЛАГОТВОРИТЕЛЬНОСТЬ

В 2025 году на Positive Hack Days Fest действовала благотворительная программа, в рамках которой доступ на закрытую часть мероприятия получали те, кто сделал пожертвование в фонды «Подари жизнь», «Старость в радость» и «Улица мира» на сумму от 1,5 тыс. руб. За время фестиваля было собрано более 12 млн руб. (на 34% больше, чем в 2024 году), а участие в программе приняли 6,2 тыс. человек.

В отчетном году бизнес-консультант по информационной безопасности Positive Technologies Алексей Лукацкий принял участие в благотворительном аукционе от Meet For Charity. Уже более девяти лет эта организация проводит благотворительные аукционы, главные лоты которых — встречи с медийными личностями из разных областей жизни: бизнеса, культуры, спорта, политики, искусства. Средства, полученные за встречу с экспертом Positive Technologies, были направлены в фонд «Провидение».

>12 млн руб. +34%

собрано за время фестиваля Positive Hack Days

6,2 тыс. человек

приняли участие в благотворительной программе

ВКЛАД В ЭКОЛОГИЮ

1

Создание гармоничной среды для продуктивной работы

В основу проектирования офисных пространств Positive Technologies заложен принцип гармоничного взаимодействия сотрудника с окружающей средой. Мы убеждены, что забота о физическом и психологическом комфорте команды является ключевым элементом корпоративной культуры и напрямую влияет на эффективность и качество работы.

2

Забота о здоровье и комфорте

Офис Компании спроектирован как целостная экосистема, ориентированная на благополучие каждого. Мы уделяем особое внимание эргономике: более 30% рабочих мест оборудованы современными регулируемыми по высоте столами, что позволяет сотрудникам выбирать оптимальный режим работы «сидя — стоя». Более 75% рабочих мест имеют прямой доступ к естественному освещению и свободный вид из окна, открывающий перспективу и снижающий зрительное напряжение. Внутреннее искусственное освещение организовано с применением современных решений, обеспечивающих точную цветопередачу и полное отсутствие пульсаций для сохранения здоровья глаз. При этом сотрудники могут самостоятельно и плавно регулировать уровень освещенности на своих рабочих местах. Этот подход не только создает максимально комфортные индивидуальные условия, но и способствует значительному снижению потребления электроэнергии.

3

Биофильный дизайн: природа как источник вдохновения

Все новые и реконструируемые пространства Компании создаются с ориентиром на принципы биоморфного дизайна. Мы стремимся органично интегрировать природу в рабочую среду: в офисе размещено большое количество живых растений, которые улучшают микроклимат и создают свежую, оживленную атмосферу. Этот принцип также находит отражение в использовании форм, текстур и паттернов, имитирующих природные ландшафты, — в плавных линиях интерьера, избегании острых углов, применении натуральных материалов и изображений природы, а также в специально подобранной цветовой палитре, характерной для естественной среды. Такой подход способствует снижению стресса, повышению концентрации и создает ощущение спокойствия и баланса.

4

Экологическая ответственность как ежедневная практика

Осознавая свою ответственность перед окружающим миром, Компания реализует системный подход к управлению ресурсами и отходами. В партнерстве с «Экоцентром Сборка» в офисе налажена система раздельного сбора вторсырья. Отдельно организуется сбор и передача на переработку макулатуры и картона, а также особо опасных отходов — элементов питания (батареек и аккумуляторов). Мы также уделяем внимание рациональному использованию воды: все санузлы оборудованы устройствами слива с регулировкой объема, а краны — аэраторами, что позволяет существенно сократить водопотребление без потери комфорта. Для снижения расхода бумаги внедрены системы электронного документооборота, в том числе кадрового. Таким образом, офис Positive Technologies — это не просто рабочее место, а продуманная среда, где внимание к деталям, забота о здоровье сотрудников и экологические принципы формируют новое качество рабочей атмосферы, направленное на устойчивое развитие и общий успех.

КОРПОРАТИВНОЕ УПРАВЛЕНИЕ

- Принципы и практика корпоративного управления
- Органы управления
- Управление рисками, внутренний контроль и аудит

ПРИНЦИПЫ И ПРАКТИКА КОРПОРАТИВНОГО УПРАВЛЕНИЯ

Система корпоративного управления Positive Technologies нацелена на построение эффективных и прозрачных взаимоотношений между акционерами, членами Совета директоров, менеджментом, а также сотрудниками Компании и иными заинтересованными сторонами.

Принципы и практика корпоративного управления

В области корпоративного управления Компания ставит своей целью соблюдение норм действующего российского законодательства, а также руководствуется правилами листинга Московской биржи и Кодексом корпоративного управления, рекомендованным Банком России. В отношениях с инвесторами мы ставим открытость на первый план. Топ-менеджмент Positive Technologies абсолютно открыт и доступен для коммуникации. Мы формируем новый подход к практикам корпоративного управления и стремимся быть максимально прозрачными и предсказуемыми для стейкхолдеров.

Компания придерживается следующих принципов корпоративного управления:

- равное отношение к акционерам, обеспечение реальной возможности для них осуществлять свои права;
- информационная и финансовая прозрачность для акционеров и инвесторов, своевременное раскрытие полной и достоверной информации;
- подотчетность и ответственность топ-менеджмента перед Советом директоров и акционерами;
- соблюдение интересов и предусмотренных законодательством прав акционеров, инвесторов и всех заинтересованных лиц.

Positive Technologies — группа компаний, которая включает в себя материнскую компанию и ряд дочерних.

Схема элементов системы корпоративного управления ПАО «Группа Позитив»

Административное подчинение
Функциональное подчинение
Отчетность по отдельным вопросам

Заявление Совета директоров о соблюдении Кодекса корпоративного управления

Отчет о соблюдении принципов и рекомендаций Кодекса корпоративного управления

Совет директоров считает соблюдение основных принципов и рекомендаций Кодекса корпоративного управления необходимым инструментом повышения эффективности управления Компанией, нацеленным на обеспечение ее долгосрочного и устойчивого развития. В отчетном периоде оценка соблюдения принципов корпоративного управления проводилась с учетом рекомендаций, указанных в информационном письме Банка России от 27 декабря 2021 года № ИН-06-28/102 «О раскрытии в годовом отчете публичного акционерного общества отчета о соблюдении принципов и рекомендаций Кодекса корпоративного управления».

Меры по совершенствованию корпоративного управления в 2025 году и планы на 2026 год

Основные документы, регламентирующие корпоративное управление Компании

- Устав ПАО «Группа Позитив»
- Положение о Совете директоров
- Положение о Комитете по аудиту
- Положение о Комитете по кадрам и вознаграждениям
- Положение о внутреннем аудите ПАО «Группа Позитив»
- Положение о дивидендной политике ПАО «Группа Позитив»
- Правила внутреннего контроля по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком ПАО «Группа Позитив»

Компания продолжает совершенствовать механизмы корпоративного управления для достижения максимальной прозрачности деятельности. В 2025 году:

- утвержден Проспект ценных бумаг;
- внесены изменения в Программу облигаций;
- утверждены Правила внутреннего контроля Компании по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком в новой редакции;
- актуализирован перечень инсайдерской информации;
- проведена самооценка работы Совета директоров по итогам 2025 года.

В 2025 году Компания вынужденно ограничивала раскрытие информации в соответствии с Постановлением Правительства Российской Федерации от 4 июля 2023 года № 1102. Несмотря на это, Компания раскрывает всю необходимую для инвесторов информацию о финансовых результатах деятельности и планах развития.

В 2026 году Компания будет продолжать работу по поиску способов и совершенствованию системы раскрытия всей ключевой и важной для инвесторов информации о деятельности Компании при сохранении необходимой в сложившихся условиях конфиденциальности.

ОРГАНЫ УПРАВЛЕНИЯ

В Компании выстроена трехуровневая система корпоративного управления. Согласно Уставу, органами управления Компании являются Общее собрание акционеров и Совет директоров, исполнительным органом — Генеральный директор.

Общее собрание акционеров

Общее собрание акционеров является высшим органом управления Компании. Компетенция Общего собрания акционеров определена Федеральным законом от 26 декабря 1995 года № 208-ФЗ «Об акционерных обществах» и Уставом Компании. Компания ежегодно проводит годовое заседание Общего собрания акционеров. Также Компания может проводить внеочередные Общие собрания акционеров.

21 мая 2025 года в Москве, на площадке СК «Лужники», состоялось годовое заседание Общего собрания акционеров Компании, которое впервые проводилось в очном формате. В годовом заседании Общего собрания акционеров приняли участие Председатель Совета директоров, топ-менеджмент и акционеры Компании.

На годовом заседании Общего собрания акционеров Компании были рассмотрены следующие вопросы:

- о распределении прибыли (в том числе о выплате (объявлении) дивидендов) по результатам 2024 года;
- об избрании членов Совета директоров;
- об утверждении аудиторской организации;
- об одобрении сделки, совершенной Компанией.

Акционеры принимали участие в голосовании на заседании с использованием заполненного на бумаге бюллетеня, а также принимали участие в заочном голосовании — используя электронный бюллетень или путем направления заполненного на бумаге бюллетеня и подачи инструкции через депозитарий. Материалы к собранию были заблаговременно размещены на сайте для инвесторов.

Информация для инвесторов на сайте Компании

Совет директоров

Совет директоров является коллегиальным органом управления Компании и осуществляет общее руководство ее деятельностью.

Деятельность Совета директоров определяется Уставом Компании и Положением о Совете директоров. Совет директоров ежегодно избирается Общим собранием акционеров и отчитывается перед ним о своей деятельности. Решения Общего собрания акционеров являются для него обязательными.

Совет директоров играет ключевую роль в системе корпоративного управления Компании. В числе его приоритетных целей — создание эффективной системы обеспечения сохранности средств акционеров и их эффективного использования, снижение рисков инвесторов и Компании.

Он рассматривает вопросы стратегического характера, главные бизнес-вопросы, в том числе:

- определение приоритетных направлений деятельности и стратегии развития Компании;
- назначение единоличного исполнительного органа;
- формирование эффективной системы управления рисками и внутреннего контроля, а также обеспечение эффективной организации и осуществления внутреннего аудита в Компании;
- утверждение документов в области стратегии управления персоналом и системы мотивации;
- обеспечение реализации и защиты прав и законных интересов акционеров Компании;
- обеспечение полноты, точности и достоверности финансовой отчетности Компании.

Независимые директора

В состав Совета директоров входят три независимых директора. Независимость членов Совета директоров подтверждается Комитетом по кадрам и вознаграждениям в соответствии с правилами листинга Московской биржи.

В состав Совета директоров должно быть избрано не менее трех независимых директоров, то есть таких лиц, которые обладают достаточными профессионализмом, опытом и самостоятельностью для формирования собственной позиции, способностью выносить объективные и добросовестные суждения, независимых от влияния исполнительных органов Общества, отдельных групп акционеров или иных заинтересованных сторон. Критерии независимости директоров определяются в соответствии с правилами листинга Московской биржи, а также в соответствии с применимым законодательством. Акционеры Компании при выдвижении кандидатов в Совет директоров должны учитывать, что в качестве независимых директоров не могут быть избраны лица, которые не отвечают признакам независимости.

Независимый директор должен воздерживаться от совершения действий, в результате которых он может перестать быть независимым, а в случае возникновения обстоятельств, в результате которых он перестает быть независимым, должен проинформировать Совет директоров об этих обстоятельствах и о произошедших изменениях. Совет директоров должен обеспечить раскрытие информации об утрате членом Совета директоров статуса независимого директора.

Критерии отбора и преемственность

Членом Совета директоров может быть любое физическое лицо, предложенное акционером или иными лицами и органами управления, обладающими правом в соответствии с законодательством Российской Федерации выдвигать кандидатов в Совет директоров, и избранное Общим собранием акционеров в установленном порядке.

Комитет по кадрам и вознаграждениям проводит предварительную оценку состава Совета директоров Общества с точки зрения:

- профессиональной специализации, опыта, независимости и вовлеченности его членов в работу Совета директоров;
- профессиональной квалификации, соответствия требованиям, установленным законодательством и организатором торгов ценными бумагами, а также критериям независимости кандидатов, выдвинутых в Совет директоров, на основе всей доступной Комитету информации.

Затем Комитет вырабатывает рекомендации Совету директоров в отношении кандидатов для избрания в Совет директоров. Также Комитет по кадрам и вознаграждениям вырабатывает предварительные рекомендации для акционеров в отношении голосования по вопросу избрания кандидатов в Совет директоров Общества.

Введение в должность и обучение членов Совета директоров

Процедура введения в должность и обучения членов Совета директоров включает:

- ознакомление члена Совета директоров с внутренними документами, регулирующими деятельность Компании и ее органов управления, решениями Общего собрания акционеров и Совета директоров;
- ознакомление члена Совета директоров с основными показателями деятельности Компании;
- ознакомление члена Совета директоров со стратегией развития Компании;
- ознакомление независимых членов Совета директоров с дополнительными правами и обязанностями независимых директоров, их функциями и ролями в корпоративной практике Компании;
- ознакомление члена Совета директоров с ответственностью, которая возлагается на него в соответствии с законодательством Российской Федерации, а также в связи с принятыми Компанией обязательствами, в том числе в связи с обращением ценных бумаг Компании на организованных торгах.

Сведения о членах Совета директоров по состоянию на 31 декабря 2025 года

Текущий состав Совета директоров в составе девяти членов был избран решением годового заседания Общего собрания акционеров 21 мая 2025 года и действует до следующего годового заседания Общего собрания акционеров[1].

В состав Совета директоров входят три независимых члена. Независимость директоров, избранных в состав Совета директоров, подтверждена решением Комитета по кадрам и вознаграждениям Совета директоров[2].

Также были переизбраны составы комитетов Совета директоров. Независимые директора вошли в состав Комитета по аудиту и Комитета по кадрам и вознаграждениям, два независимых директора стали председателями комитетов[3].

1 Протокол годового Общего собрания акционеров от 21 мая 2025 года б/н.
2 Протокол Комитета по кадрам и вознаграждениям от 4 апреля 2025 года № 1.
3 Протокол Совета директоров от 10 июня 2025 года № 39.

Отчет о работе Совета директоров в 2025 году

В 2025 году были проведены одно очное и пять заочных заседаний Совета директоров. В рамках заседаний были приняты следующие ключевые решения:

- избран Председатель Совета директоров, утверждены составы комитетов Совета директоров и избраны их председатели;
- утверждены Годовой отчет и годовая бухгалтерская отчетность Компании за 2024 год;
- утвержден годовой бюджет Компании на 2025 год;
- включены кандидаты в список кандидатур для голосования по выборам в Совет директоров Компании на годовом заседании Общего собрания акционеров Компании на 2025 корпоративный год;
- определен порядок проведения годового заседания Общего собрания акционеров Компании по итогам 2024 года;
- выданы рекомендации годовому заседанию Общего собрания акционеров Компании по распределению прибыли и убытков Компании, а также относительно размеров дивиденда по результатам 2024 года по акциям Компании и порядку его выплаты;
- рассмотрен отчет о работе Комитета по аудиту Совета директоров Компании в 2024 году;
- рассмотрен отчет службы внутреннего аудита и службы внутреннего контроля и управления рисками Компании за 2024 год и рекомендации Комитета по аудиту Совета директоров Компании;
- рассмотрены предложения годовому заседанию Общего собрания акционеров Компании по назначению аудиторской организации;
- определен размер оплаты услуг аудиторской организации Компании за 2025 год;
- рассмотрены результаты самооценки работы Совета директоров Компании и его комитетов за 2025 год;
- рассмотрены сделки, совершенные Компанией и ее дочерним обществом;
- утверждены Проспект ценных бумаг, а также изменения в Программу облигаций Компании;
- утверждены Правила внутреннего контроля Общества по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком в новой редакции;
- рассмотрены иные организационные вопросы.

Участие директоров в заседаниях Совета директоров

Дата проведения Совета директоров	Форма принятия решения	Количество директоров, принявших участие / общее количество директоров
07.04.2025	Совместное присутствие	7/9
09.06.2025	Заочное голосование	8/9
10.10.2025	Заочное голосование	9/9
10.12.2025	Заочное голосование	8/9
15.12.2025	Заочное голосование	8/9
22.12.2025	Заочное голосование	9/9

Комитеты при Совете директоров

2

постоянно действующих комитета созданы при Совете директоров.

Комитет по аудиту

Комитет по кадрам и вознаграждениям

Комитет по аудиту

Комитет по аудиту функционирует в Компании с 2021 года.

Основные функции Комитета по аудиту:

- контроль за обеспечением полноты, точности и достоверности бухгалтерской (финансовой) отчетности Компании;
- контроль за надежностью и эффективностью работы системы управления рисками и внутреннего контроля;
- обеспечение независимости и объективности осуществления функций внутреннего и внешнего аудита.

В отчетном году Комитет рассматривал широкий спектр вопросов, в том числе:

- рассмотрение финансовой отчетности, Годового отчета за 2024 год;
- предварительное рассмотрение проекта годового бюджета на 2025 год;
- рассмотрение кандидатуры аудиторской организации и размера оплаты ее услуг на 2025 год;
- утверждение отчета о работе Комитета по аудиту за 2024 год;
- рассмотрение отчета службы внутреннего аудита и службы внутреннего контроля и управления рисками за 2024 год;
- утверждение плана деятельности службы внутреннего аудита Компании и ее бюджета на 2025 год;
- предварительное рассмотрение изменений в ранее утвержденные документы.

Комитет состоит из трех членов, два из которых являются **независимыми директорами.**

Комитеты при Совете директоров

Комитет по кадрам и вознаграждениям

Комитет по кадрам и вознаграждениям функционирует в Компании с 2022 года.

Основные функции Комитета по кадрам и вознаграждениям:

- выработка рекомендаций акционерам по голосованию за кандидатов в Совет директоров: коммуникация с акционерами по данному вопросу;
- выработка рекомендаций Совету директоров в отношении кандидатов на должность Генерального директора, руководителей структурных подразделений, находящихся в его прямом (непосредственном) подчинении, Корпоративного секретаря Компании;
- выработка рекомендаций Совету директоров по определению размера вознаграждения и принципов премирования Корпоративного секретаря Компании;
- проведение процедуры самооценки или внешней оценки Совета директоров и его комитетов, определение приоритетных направлений для усиления состава Совета директоров;
- надзор за внедрением и реализацией политики Общества по вознаграждению и различных программ мотивации.

В отчетном году Комитет рассматривал широкий спектр вопросов, в числе которых:

- выработка рекомендаций акционерам Компании по голосованию за кандидатов в Совет директоров;
- подтверждение независимости членов Совета директоров Компании;
- рассмотрение результатов самооценки работы Совета директоров Компании и его комитетов в 2025 году;
- выработка рекомендаций Совету директоров Компании по вопросу рассмотрения сделки дочернего общества;
- выработка рекомендаций Совету директоров Компании по вопросу вознаграждения Корпоративного секретаря Компании.

Комитет состоит из трех членов, два из которых являются **независимыми директорами.**

Проведение процедуры самооценки работы Совета директоров и комитетов Совета директоров входит в компетенцию Комитета по кадрам и вознаграждениям.

Самооценка и внешняя оценка Совета директоров и комитетов Совета директоров Общества проводятся для анализа эффективности их работы в целом, а также разработки рекомендаций Совету директоров Общества в отношении совершенствования процедур его работы и работы его комитетов.

По итогам 2025 года Обществом была проведена самооценка работы Совета директоров и его комитетов. Результаты самооценки были рассмотрены Комитетом по кадрам и вознаграждениям и на заседании Совета директоров. Самооценка показала, что работа Совета директоров и его комитетов является в достаточной мере эффективной. При этом были выявлены основные направления для повышения эффективности работы Совета директоров Компании.

Генеральный директор

Согласно Уставу, руководство Компанией осуществляет единоличный исполнительный орган — Генеральный директор. Он назначается на должность по решению Совета директоров и подотчетен Совету директоров и Общему собранию акционеров.

К компетенции Генерального директора относится решение всех вопросов текущей деятельности Компании, за исключением вопросов, отнесенных к компетенции Общего собрания акционеров и Совета директоров. Генеральный директор организует деятельность Компании и несет ответственность за ее результаты, обеспечивает выполнение решений Общих собраний акционеров и Совета директоров. Он наделен всей полнотой полномочий, необходимых для осуществления оперативного руководства текущей деятельностью Компании в пределах своей компетенции. С 29 июля 2021 года Генеральным директором Компании является Денис Сергеевич Баранов.

Баранов Денис Сергеевич

Родился в 1985 году.

Окончил Национальный исследовательский университет ИТМО по специальности «прикладная математика».

В начале карьеры разрабатывал веб-приложения в компании Actimind, писал код на Java и C++ в компаниях T-Systems и «Новел-ИЛ».

В 2010 году пришел в Positive Technologies. Занимал должность специалиста, а затем руководителя отдела анализа защищенности веб-приложений. Участвовал в проектировании PT Application Inspector, PT Application Firewall и PT ISIM с самого начала их разработки, после чего отвечал за их развитие.

С 2021 года возглавляет компанию Positive Technologies.

Входит в группу исследователей некоммерческого сообщества SCADA Strangelove, которое специализируется на анализе защищенности промышленных систем управления. Автор ряда исследований в области application security.

Корпоративный секретарь

Корпоративный секретарь является должностным лицом Компании, назначается на должность и освобождается от занимаемой должности Генеральным директором с согласия Совета директоров или по согласованию с ним. Корпоративный секретарь подотчетен Совету директоров и административно подчинен Генеральному директору. Корпоративный секретарь также исполняет функции секретаря Совета директоров.

Компетенции Корпоративного секретаря отражены в Уставе Компании, Положении о Корпоративном секретаре и Положении о Совете директоров, которые формулируют основные квалификационные требования к нему.

С 24 сентября 2024 года Корпоративным секретарем Компании является **Терентьева Ольга Игоревна**.

К функциям Корпоративного секретаря относятся:

- участие в организации подготовки и проведения общих собраний акционеров;
- обеспечение работы Совета директоров и комитетов Совета директоров, организация подготовки и проведения заседаний Совета директоров;
- участие в реализации политики по раскрытию информации, обеспечение хранения корпоративных документов Компании;
- обеспечение взаимодействия Компании с акционерами, владельцами иных эмиссионных ценных бумаг и участие в предупреждении корпоративных конфликтов;
- участие в совершенствовании системы и практики корпоративного управления в Компании;
- обеспечение процедур, обеспечивающих реализацию прав и законных интересов акционеров, контроль за соблюдением и исполнением указанных процедур;
- контроль над раскрытием информации на рынке ценных бумаг.

Терентьева Ольга Игоревна

Родилась в 1991 году.

В 2013 году с отличием окончила Московский государственный юридический университет им. О. Е. Кутафина (МГЮА).

Присоединилась к команде Positive Technologies в декабре 2021 года, имея более чем 10-летний опыт работы в сфере корпоративного управления и сопровождения корпоративных проектов.

До прихода в Positive Technologies Ольга работала с такими эмитентами, как Государственная корпорация «Ростех», ОАО «РЖД», ПАО «Ростелеком», также работала в Коллегии адвокатов города Москвы.

Ольга является сертифицированным корпоративным секретарем Национального объединения корпоративных секретарей.

На 31 декабря 2025 года Ольга владела 274 акциями Компании, что составляет 0,000385% от уставного капитала Компании.

Вознаграждение органов управления

Согласно Положению о Совете директоров за исполнение своих обязанностей члены Совета директоров могут получать денежные вознаграждения и компенсации в порядке и размерах, определенных решением Общего собрания акционеров.

Решение внеочередного Общего собрания акционеров Компании[1] устанавливает размер и порядок выплаты вознаграждений для членов Совета директоров, независимых директоров в составе этого Совета, а также за исполнение обязанностей председателя комитета Совета директоров.

В 2025 году членам Совета директоров выплачивалось вознаграждение за их работу в соответствии с указанным выше решением Общего собрания акционеров Компании.

Генеральному директору выплачивается вознаграждение за выполненную работу. Структура и размер вознаграждения определяются Советом директоров.

1 Протокол от 6 декабря 2021 года № 4.

УПРАВЛЕНИЕ РИСКАМИ, ВНУТРЕННИЙ КОНТРОЛЬ И АУДИТ

Корпоративная система управления рисками, внутреннего контроля и аудита позволяет Компании принимать взвешенные риск-ориентированные решения, нацеленные на предотвращение реализации рисков и устранение негативных последствий в случае их наступления.

Для обеспечения эффективности системы внутреннего контроля и управления рисками в Компании созданы Комитет по аудиту при Совете директоров, служба внутреннего контроля и управления рисками и служба внутреннего аудита.

Система внутреннего контроля и управления рисками в Компании построена на основе модели «трех линий защиты».

1 Менеджмент	Ответственность за внутренний контроль и управление рисками бизнес-процессов
2 Служба внутреннего контроля и управления рисками	Мониторинг и поддержка менеджмента в организации эффективной системы внутреннего контроля и управления рисками
3 Служба внутреннего аудита	Независимая оценка системы внутреннего контроля и управления рисками

Управление рисками и внутренний контроль

Для обеспечения функционирования системы управления рисками в Компании создана служба внутреннего контроля и управления рисками, действующая на основании Политики по управлению рисками и Политики по внутреннему контролю. Руководитель службы функционально и административно подчиняется непосредственно Генеральному директору. Комитет по аудиту осуществляет контроль за эффективностью управления рисками и внутреннего контроля.

Служба внутреннего контроля и управления рисками выполняет следующие основные функции:

- организация и координация процесса управления рисками и внутреннего контроля;
- идентификация и мониторинг рисков и индикаторов рисков, создание и поддержание актуальной карты рисков;
- оценка рисков и выработка предложений по управлению ими совместно с владельцами бизнес-процессов;
- анализ бизнес-процессов и выработка требований по дизайну контрольных процедур, направленных на минимизацию рисков.

Определение уровня принятия решений и приоритетов в управлении рисками происходит по результатам их ранжирования.

При ранжировании используются два основных фактора оценки риска:

- вероятность наступления риска,
- существенность последствий реализации риска.

ОСНОВНЫЕ ПРИНЦИПЫ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

Непрерывность процесса

Заключается в реализации на регулярной основе комплекса упорядоченных процедур управления рисками. Система управления рисками предполагает постоянный процесс обновления и изменения всех ее элементов.

Обоснованность

Система управления рисками предусматривает анализ отношения затрат на снижение вероятности наступления риска к потенциальному ущербу от его реализации.

Информированность

Используется единый канал информирования менеджмента Компании по всему спектру рисков для обеспечения полноты, качества и сопоставимости предоставляемой информации для каждого из уровней принятия решения.

Открытость

Управление рисками предполагает открытое обсуждение как внутри Компании, так и с ключевыми стейкхолдерами.

Ключевые риски и меры по управлению ими

Для минимизации возможных рисков и снижения их возможного негативного влияния Компания проводит комплексную работу по управлению ими. Представленный ниже перечень рисков отражает оценки менеджмента на момент подготовки данного Годового отчета, которые могут со временем меняться. Возникновение новых рисков, о которых менеджменту в настоящий момент неизвестно, или реализация рисков, которые менеджмент в текущий момент считает несущественными, могут также повлиять на бизнес в будущем.

Риск		Меры для снижения возможного негативного влияния
Риски внешней среды	**Экономическая и социальная нестабильность** Экономическая и социальная нестабильность, вызванная влиянием геополитической напряженности, замедлением экономического роста в России и мире, может оказать негативное влияние на достижение стратегических целей Компании. Отрицательное влияние данных факторов на финансовое состояние клиентов может привести к снижению доходов Компании. Нарушения цепочек поставок вследствие существенных санкций и экспортного контроля или экономических ограничений, установленных в отношении России, способны негативно отразиться на показателях эффективности бизнеса	■ Регулярный мониторинг экономической и социальной ситуации, анализ рынков ■ Оперативное операционное реагирование на изменение условий внешней среды ■ Адаптация стратегии развития бизнеса к изменяющимся условиям внешней среды ■ Развитие продаж и инвестиции в увеличение доли Компании на российском рынке ИБ после ухода западных вендоров ■ Разработка продуктов для нужд импортозамещения
	Санкционные риски[1] Введение новых санкций (экономических ограничений в отношении компаний Группы и крупных акционеров, а также вторичных санкций в отношении контрагентов за предоставление товаров или услуг) может негативно повлиять на развитие бизнеса и на достижение стратегических целей Компании	■ Регулярный мониторинг экономических ограничений в отношении Российской Федерации и компаний технологического сектора для минимизации негативных эффектов ■ Диверсификация портфеля поставщиков товаров и услуг
	Риск неблагоприятного изменения нормативно-правовой среды (законодательство, требования регуляторов)	■ Регулярный мониторинг изменений в законодательстве ■ Регулярный анализ соответствия Компании актуальным требованиям ■ Взаимодействие с государственными органами и участие в отраслевых рабочих группах и ассоциациях

1 В 2021 году одна из компаний Группы была включена в «Список SDN».

Риск		Меры для снижения возможного негативного влияния
Стратегические риски	Растущая конкуренция, появление новых игроков на рынке кибербезопасности	■ Мониторинг рынка ■ Разработка и создание уникальных инновационных продуктов ■ Улучшение коммерческих условий ■ Инвестирование в цены (эффективное ценообразование, оптимизация расходов) ■ Улучшение клиентского опыта
	Снижение спроса на продукты и услуги Компании из-за сокращения бюджетов заказчиков	■ Мониторинг рынка ■ Инвестирование в цены (эффективное ценообразование, оптимизация расходов)
Операционные риски	Дефицит квалифицированных кадров, отток ИТ-специалистов	■ Предоставление комфортных условий труда и конкурентного уровня заработной платы, льготы для сотрудников ИТ-компаний ■ Мониторинг рынка труда и продвижение Компании ■ Оптимальное развитие ключевых сотрудников ■ Создание резерва для критических ролей
	Прекращение сотрудничества с ключевыми поставщиками программного обеспечения и ИТ-оборудования и дистрибьюторами в связи с объявленными санкциями против России	■ Диверсификация поставщиков программного обеспечения и ИТ-оборудования ■ Выстраивание новых логистических цепочек
Финансовые риски	Валютный риск (риск ухудшения финансовых результатов из-за неблагоприятного изменения курса валют)	■ Заключение долгосрочных расходных договоров с фиксацией цен ■ Заключение доходных договоров в национальной валюте
	Кредитный риск (риск изменения процентных ставок по кредитам и займам, рост долговой нагрузки)	■ Использование долговых инструментов с фиксированной процентной ставкой ■ Проведение мероприятий по рефинансированию и реструктуризации кредитного портфеля ■ Контроль уровня долговой нагрузки

Случаи реализации существенных рисков в 2025 году **не выявлены.**

Компания непрерывно совершенствует систему управления рисками и внутреннего контроля. В течение 2025 года:

- реализована система оперативной отчетности по рискам с использованием инструментов анализа данных;
- проведена оценка рисков по новой методологии;
- доработан аналитический отчет по статусу управления рисками.

Планы Компании на 2026 год включают:

- дальнейшее совершенствование методологии оценки рисков;
- развитие профессиональных компетенций в области управления рисками, получение профессиональных сертификаций.

Внутренний аудит

В Компании действует служба внутреннего аудита — самостоятельное структурное подразделение, функции которого определены Положением о внутреннем аудите.

Руководитель службы внутреннего аудита функционально подчиняется председателю Комитета по аудиту Совета директоров, административно — непосредственно Генеральному директору.

Комитет по аудиту рассматривает и утверждает политики в области внутреннего аудита и план внутреннего аудита, совместно с руководителем службы внутреннего аудита рассматривает и утверждает ресурсы и бюджет внутреннего аудита, дает оценку эффективности деятельности внутреннего аудита.

Служба внутреннего аудита выполняет следующие функции:

- оценка эффективности системы внутреннего контроля, процессов управления рисками и корпоративного управления;
- разработка рекомендаций по совершенствованию процедур внутреннего контроля, управления рисками и корпоративного управления и содействие менеджменту в разработке корректирующих мероприятий по результатам проведенных аудитов;
- мониторинг выполнения рекомендаций по устранению нарушений и недостатков, выявленных по результатам аудитов;
- оказание консультационных услуг.

В своей деятельности служба внутреннего аудита применяет рискориентированный подход.

В течение 2025 года служба внутреннего аудита осуществляла свою деятельность в соответствии с утвержденным планом работы внутреннего аудита. В течение 2025 года совместно со службой управления рисками и внутреннего контроля была проведена переоценка ключевых рисков.

В 2026 году деятельность службы внутреннего аудита будет осуществляться в соответствии со стратегией развития Компании и с учетом необходимости адаптации к динамичным условиям ведения бизнеса по причине нестабильности геополитической и экономической ситуации в мире. Также служба внутреннего аудита планирует дальнейшее совершенствование методологии, внедрение новых подходов и практик, повышение профессиональных компетенций команды внутреннего аудита.

Внешний аудит

Для проведения аудита годовой финансовой отчетности и обзорной проверки полугодовой финансовой отчетности Компания привлекает независимых внешних аудиторов, не связанных имущественными интересами с Компанией или ее акционерами.

Выбор аудиторской организации происходит на основании рекомендаций по канидатуре аудиторской организации Комитета по аудиту Совета директоров Компании. Кандидатура аудиторской организации утверждается на годовом заседании Общего собрания акционеров Компании.

Выбор аудитора Компании для проверки отчетности, составленной в соответствии с МСФО, проводится на конкурсной основе. Выбор проводится посредством тендера. Для целей тендера формируются требования, собираются и сравниваются предложения нескольких аудиторских организаций. Ежегодно происходит подписание нового договора на аудит на основе полученного коммерческого предложения; дополнительно оформляется меморандум по выбору аудитора.

При определении кандидатуры аудитора принимаются во внимание следующие критерии:

- соответствие аудиторской компании и ее сотрудников требованиям, предъявляемым действующим законодательством Российской Федерации к аудиту общественно значимых организаций;
- деловая репутация аудитора;
- наличие опыта работы по аудиту МСФО отчетности;
- наличие опыта работы с компаниями ИТ-отрасли;
- профессионализм рабочей группы, квалификация и опыт специалистов;
- стоимость услуг;
- готовность аудитора работать по установленным Компанией срокам.

Выбор аудитора Компании для проверки отчетности, составленной в соответствии с РСБУ, проводится на конкурсной основе. При определении кандидатуры аудитора принимаются во внимание следующие критерии:

- членство аудиторской организации в саморегулируемой организации аудиторов;
- соответствие аудиторской компании и ее сотрудников требованиям, предъявляемым действующим законодательством Российской Федерации к аудиту общественно значимых организаций;
- в отношении участника на момент проведения конкурса и в период предполагаемого подписания договора на проведение аудита не должны действовать меры воздействия в виде приостановления членства в саморегулируемой организации аудиторов, лишающие участника права заключать новые договоры;
- наличие в аудиторской организации работающих по трудовому договору не менее 10 специалистов, имеющих действующие квалификационные аттестаты аудиторов на право осуществления аудиторской деятельности в области общего аудита, выданные Министерством финансов Российской Федерации в установленном порядке;
- деловая репутация аудитора;
- профессионализм рабочей группы, квалификация и опыт специалистов;
- стоимость услуг;
- готовность аудитора работать по установленным Компанией срокам.

На годовом заседании Общего собрании акционеров 21 мая 2025 года на роль внешнего аудитора (аудиторской организации) Компании за 2025 год было выбрано АО «Юникон».

СВЕДЕНИЯ ОБ АУДИТОРЕ

Полное фирменное наименование:
Юникон Акционерное общество.

Сокращенное фирменное наименование:
Юникон АО.

Идентификационный номер налогоплательщика (ИНН): 7716021332.

Основной государственный регистрационный номер (ОГРН): 1037739271701.

Место нахождения аудитора:
Россия, г. Москва, Варшавское шоссе, д. 125, с. 1, секция 11, 3-й эт., пом. I, ком. 50.

Вознаграждение аудитора
Размер вознаграждения аудитора за услуги по проведению обзорной проверки полугодовой финансовой отчетности составил 2 200 000 (два миллиона двести тысяч) руб. Стоимость услуг по аудиту годовой финансовой отчетности за 2025 год составила 6 200 000 (шесть миллионов двести тысяч) руб. Совокупный размер вознаграждения за аудиторские услуги за 2025 год составил 8 400 000 (восемь миллионов четыреста тысяч) руб. без учета НДС. В течение 2025 года аудитор не оказывал Компании услуги, не связанные с аудитом (неаудиторские услуги).

Противодействие коррупции

В Компании организован почтовый ящик и круглосуточный телефон доверия, предназначенные для приема анонимных сообщений о правонарушениях. Поступающие сообщения обрабатываются по формализованному протоколу. В службе безопасности Компании образована рабочая группа для проведения служебных проверок на основании получаемой информации.

Также Компания на регулярной основе проводит мероприятия по повышению бдительности сотрудников в целях борьбы со злоупотреблениями и коррупционными проявлениями. В ближайшие планы входит организация регулярного обучения ведущих сотрудников Компании актуальным законодательным нормам и лучшим практикам в области противодействия коррупции.

В отчетном году реальных обращений по правонарушениям зафиксировано не было.

Управление конфликтом интересов

В Компании разработаны меры, которые направлены на предупреждение ситуаций, связанных с возможным конфликтом интересов членов Совета директоров и исполнительных органов Компании. Правила управления конфликтом интересов в Компании закреплены в Уставе и Положении о Совете директоров.

В частности, данные документы предусматривают следующие меры:

- при наступлении обстоятельств, в силу которых Генеральный директор и члены Совета директоров могут быть признаны заинтересованными в совершении Компанией сделок, они обязаны доводить до сведения Компании информацию о таких сделках (совершенных или предполагаемых); они также обязаны передавать Компании сведения о подконтрольных организациях и юридических лицах, в органах управления которых они или их близкие родственники занимают должности;
- члены Совета директоров обязаны воздерживаться от действий, которые приведут или могут привести к возникновению конфликта между их интересами и интересами Компании и (или) ее кредиторов;
- независимые директора (у которых отсутствует конфликт интересов) предварительно оценивают существенные корпоративные действия, связанные с возможным конфликтом интересов, а результаты такой оценки предоставляются Совету директоров.

За отчетный год Компанией не выявлено случаев возникновения конфликта интересов у членов Совета директоров и исполнительных органов Компании. Соответствующие сделки в конкретных случаях были надлежащим образом одобрены ответственными органами управления Компании и ее дочерних обществ.

ПРИЛОЖЕНИЯ

- Об Отчете
- Консолидированная отчетность по МСФО
- Отчет о соблюдении принципов и рекомендаций Кодекса корпоративного управления
- Отчет о совершенных (заключенных) крупных сделках
- Отчет о совершенных (заключенных) сделках, в совершении которых имеется заинтересованность
- Раскрытие корпоративной информации
- Контакты

ОБ ОТЧЕТЕ

В настоящем Отчете ПАО «Группа Позитив» (далее также — Компания, Positive Technologies) за 2025 год содержится информация о результатах деятельности ПАО «Группа Позитив» и его дочерних организаций (далее совместно — Группа). Финансовые показатели Компании рассчитаны на основании финансовой отчетности по МСФО за 2025 год, подтвержденной аудиторским заключением и приведенной в приложении к Отчету[1].

Используемые стандарты и рекомендации:

- Федеральный закон от 26 декабря 1995 года № 208-ФЗ «Об акционерных обществах» (ред. от 31 июля 2025 года, с изм. от 25 сентября 2025 года, с изм. и доп., вступ. в силу с 1 сентября 2025 года);
- Федеральный закон от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг»;
- Кодекс корпоративного управления Банка России от 10 апреля 2014 года;
- Положение Центрального банка от 27 марта 2020 года № 714-П «О раскрытии информации эмитентами эмиссионных ценных бумаг» (в ред. от 30 сентября 2022 года);
- Рекомендации по раскрытию публичными акционерными обществами нефинансовой информации, связанной с деятельностью таких обществ (приложение к письму Банка России от 12 июля 2021 года № ИН-06-28/49).

1 Отчет может содержать незначительные неточности в показателях и расчетах, вызванные эффектом округления.

КОНСОЛИДИРОВАННАЯ ОТЧЕТНОСТЬ ПО МСФО

Публичное акционерное общество
«Группа Позитив» и его дочерние организации

Консолидированная финансовая отчетность за год,
закончившийся 31 декабря 2025 года,
и аудиторское заключение независимого аудитора

АУДИТОРСКОЕ ЗАКЛЮЧЕНИЕ НЕЗАВИСИМОГО АУДИТОРА

о раскрываемой консолидированной финансовой отчетности ПАО «Группа Позитив» и его дочерних организаций по итогам деятельности за 2025 год

СОДЕРЖАНИЕ РАСКРЫВАЕМОЙ КОНСОЛИДИРОВАННОЙ ФИНАНСОВОЙ ОТЧЕТНОСТИ

АУДИТОРСКОЕ ЗАКЛЮЧЕНИЕ НЕЗАВИСИМОГО АУДИТОРА

РАСКРЫВАЕМАЯ КОНСОЛИДИРОВАННАЯ ФИНАНСОВАЯ ОТЧЕТНОСТЬ:

Раскрываемый консолидированный отчет о прибыли или убытке и прочем совокупном доходе
Раскрываемый консолидированный отчет о финансовом положении
Раскрываемый консолидированный отчет об изменениях в капитале
Раскрываемый консолидированный отчет о движении денежных средств

ПРИМЕЧАНИЯ К РАСКРЫВАЕМОЙ КОНСОЛИДИРОВАННОЙ ФИНАНСОВОЙ ОТЧЕТНОСТИ:

1. Общие сведения 11
2. Основные положения учетной политики 13
3. Управление финансовыми рисками 23
4. Управление рисками наступления недопустимых событий 29
5. Ключевые бухгалтерские суждения, оценочные значения и допущения 31
6. Сезонность 32
7. Выручка по договорам с покупателями 32
8. Информация по сегментам 33
9. Операционные расходы 34
10. Налог на прибыль 36
11. Прибыль на акцию 37
12. Основные средства 39
13. Нематериальные активы 40
14. Запасы 46
15. Торговая и прочая дебиторская задолженность 46
16. Денежные средства и их эквиваленты 47
17. Финансовые активы 47
18. Капитал и резервы 48
19. Кредиты и займы 48
20. Обязательства по договорам с покупателями 50
21. Торговая и прочая кредиторская задолженность 50
22. Аренда 51
23. Условные обязательства 52
24. Связанные стороны 54
25. События после отчетной даты 55

unicon

Тел: +7 495 797 56 65
Факс: +7 495 797 56 60
reception@unicon.ru
www.unicon.ru

Юникон АО, Россия,
117587, Москва, Варшавское шоссе,
д. 125, стр. 1, секция 11, 3 этаж, пом. I,
комната 50

АУДИТОРСКОЕ ЗАКЛЮЧЕНИЕ НЕЗАВИСИМОГО АУДИТОРА

Акционерам Публичного акционерного общества «Группа Позитив»

Мнение

Мы провели аудит раскрываемой консолидированной финансовой отчетности Публичного акционерного общества «Группа Позитив» (Организация) (ОГРН 5177746006510) и его дочерних организаций (далее совместно - Группа), состоящей из раскрываемого консолидированного отчета о финансовом положении по состоянию на 31 декабря 2025 года, раскрываемого консолидированного отчета о прибыли или убытке и прочем совокупном доходе за 2025 год, раскрываемого консолидированного отчета об изменениях в капитале за 2025 год и раскрываемого консолидированного отчета о движении денежных средств за 2025 год, а также примечаний к раскрываемой консолидированной финансовой отчетности за 2025 год, состоящих из существенной информации об учетной политике и прочей пояснительной информации.

По нашему мнению, прилагаемая раскрываемая консолидированная финансовая отчетность Группы за 2025 год, подготовлена во всех существенных отношениях в соответствии с принципами подготовки, указанными в примечании 2.1 «Основы подготовки финансовой отчетности» к раскрываемой консолидированной финансовой отчетности.

Основание для выражения мнения

Мы провели аудит в соответствии с Международными стандартами аудита (МСА). Наша ответственность в соответствии с этими стандартами описана в разделе «Ответственность аудитора за аудит раскрываемой консолидированной финансовой отчетности» нашего заключения. Мы являемся независимыми по отношению к Группе в соответствии с Правилами независимости аудиторов и аудиторских организаций и Кодексом профессиональной этики аудиторов, принятыми в РФ, и содержащимися в них требованиями независимости, применимыми к аудиту общественно значимых организаций. Нами также выполнены прочие обязанности в соответствии с этими требованиями профессиональной этики. Мы полагаем, что полученные нами аудиторские доказательства являются достаточными и надлежащими, чтобы служить основанием для выражения нашего мнения.

Важные обстоятельства - принципы учета и ограничение использования

Мы обращаем внимание на примечание 2.1 «Основы подготовки финансовой отчетности» к раскрываемой консолидированной финансовой отчетности, в котором описываются принципы подготовки раскрываемой консолидированной финансовой отчетности. Раскрываемая консолидированная финансовая отчетность подготовлена с целью представления консолидированного финансового положения и консолидированных финансовых результатов Группы, раскрытие которых не наносит ущерба Группе и (или) ее контрагентам, иным лицам. Как следствие, данная раскрываемая консолидированная финансовая отчетность может быть непригодна для иной цели.

Раскрываемая консолидированная финансовая отчетность не является полным комплектом консолидированной финансовой отчетностью Группы, составленной в соответствии с Международными стандартами финансовой отчетности (МСФО).

Мы не выражаем модифицированного мнения в связи с этим вопросом.

Прочие сведения

Группа подготовила полную консолидированную финансовую отчетность за год, закончившийся 31 декабря 2025 года, в соответствии с Международными стандартами финансовой отчетности, в отношении которой мы выпустили отдельное аудиторское заключение для акционеров Группы, датированное 6 апреля 2026 года.

Прочая информация

Генеральный директор Организации (руководство) несет ответственность за прочую информацию. Прочая информация включает информацию, содержащуюся в годовом отчете за 2025 год и отчете эмитента за 2025 год, но не включает раскрываемую консолидированную финансовую отчетность и наше аудиторское заключение о ней. Годовой отчет за 2025 год и отчет эмитента за 2025 год, предположительно, будут нам предоставлены после даты настоящего аудиторского заключения.

Наше мнение о раскрываемой консолидированной финансовой отчетности не распространяется на прочую информацию, и мы не будем предоставлять вывод, обеспечивающий в какой-либо форме уверенность в отношении данной информации.

В связи с проведением нами аудита раскрываемой консолидированной финансовой отчетности наша обязанность заключается в ознакомлении с указанной выше прочей информацией, когда она будет нам предоставлена, и рассмотрении вопроса о том, имеются ли существенные несоответствия между прочей информацией и раскрываемой консолидированной финансовой отчетностью или нашими знаниями, полученными в ходе аудита, и не содержит ли прочая информация иных возможных существенных искажений.

Если при ознакомлении с годовым отчетом за 2025 год и отчетом эмитента за 2025 год мы придем к выводу о том, что в них содержится существенное искажение, мы должны довести это до сведения Совета директоров Организации.

Ответственность руководства и Совета директоров Организации за раскрываемую консолидированную финансовую отчетность

Генеральный директор Организации несет ответственность за подготовку указанной раскрываемой консолидированной финансовой отчетности в соответствии с принципами подготовки, указанными в примечании 2.1 «Основы подготовки финансовой отчетности» к раскрываемой консолидированной финансовой отчетности, и за систему внутреннего контроля, которую руководство считает необходимой для подготовки раскрываемой консолидированной финансовой отчетности, не содержащей существенных искажений вследствие недобросовестных действий или ошибок.

При подготовке раскрываемой консолидированной финансовой отчетности руководство несет ответственность за оценку способности Группы продолжать непрерывно свою деятельность, за раскрытие в соответствующих случаях сведений, относящихся к непрерывности деятельности, и за составление отчетности на основе допущения о непрерывности деятельности, за исключением случаев, когда руководство намеревается ликвидировать Группу, прекратить ее деятельность или когда у него отсутствует какая-либо иная реальная альтернатива, кроме ликвидации или прекращения деятельности.

Совет директоров Организации несет ответственность за надзор за подготовкой раскрываемой консолидированной финансовой отчетности Группы.

Ответственность аудитора за аудит раскрываемой консолидированной финансовой отчетности

Наша цель состоит в получении разумной уверенности в том, что раскрываемая консолидированная финансовая отчетность не содержит существенных искажений вследствие недобросовестных действий или ошибок, и в выпуске аудиторского заключения, содержащего наше мнение. Разумная уверенность представляет собой высокую степень уверенности, но не является гарантией того, что аудит, проведенный в соответствии с Международными стандартами аудита, всегда выявляет существенные искажения при их наличии. Искажения могут быть результатом недобросовестных действий или ошибок и считаются существенными, если можно обоснованно предположить, что в отдельности или в совокупности они могут повлиять на экономические решения пользователей, принимаемые на основе этой раскрываемой консолидированной финансовой отчетности.

В рамках аудита, проводимого в соответствии с Международными стандартами аудита, мы применяем профессиональное суждение и сохраняем профессиональный скептицизм на протяжении всего аудита. Кроме того, мы выполняем следующее:

а) выявляем и оцениваем риски существенного искажения раскрываемой консолидированной финансовой отчетности вследствие недобросовестных действий или ошибок; разрабатываем и проводим аудиторские процедуры в ответ на эти риски; получаем аудиторские доказательства, являющиеся достаточными и надлежащими, чтобы служить основанием для выражения нашего мнения. Риск необнаружения существенного искажения в результате недобросовестных действий выше, чем риск необнаружения существенного искажения в результате ошибки, так как недобросовестные действия могут включать сговор, подлог, умышленный пропуск, искаженное представление информации или действия в обход системы внутреннего контроля;

б) получаем понимание системы внутреннего контроля, имеющей значение для аудита, с целью разработки аудиторских процедур, соответствующих обстоятельствам, но не с целью выражения мнения об эффективности системы внутреннего контроля Группы;

в) оцениваем надлежащий характер применяемой учетной политики, обоснованность оценочных значений, рассчитанных руководством, и соответствующего раскрытия информации;

г) делаем вывод о правомерности применения руководством допущения о непрерывности деятельности, а на основании полученных аудиторских доказательств - вывод о том, имеется ли существенная неопределенность в связи с событиями или условиями, в результате которых могут возникнуть значительные сомнения в способности Группы продолжать непрерывно свою деятельность. Если мы приходим к выводу о наличии существенной неопределенности, мы должны привлечь внимание в нашем аудиторском заключении к соответствующему раскрытию информации в раскрываемой консолидированной финансовой отчетности или, если такое раскрытие информации является ненадлежащим, модифицировать наше мнение. Наши выводы основаны на аудиторских доказательствах, полученных до даты нашего аудиторского заключения. Однако будущие события или условия могут привести к тому, что Группа утратит способность продолжать непрерывно свою деятельность;

д) планируем и проводим аудит Группы для получения достаточных надлежащих аудиторских доказательств, относящихся к финансовой информации организаций или подразделений Группы, в качестве основы для формирования мнения о раскрываемой консолидированной финансовой отчетности Группы. Мы отвечаем за руководство, надзор за ходом аудита и проверку работы по аудиту, выполненной для целей аудита Группы. Мы остаемся полностью ответственными за наше аудиторское мнение.

Мы осуществляем информационное взаимодействие с Советом директоров Организации, доводя до его сведения, помимо прочего, информацию о запланированном объеме и сроках аудита, а также о существенных замечаниях по результатам аудита, в том числе о значительных недостатках системы внутреннего контроля, которые мы выявляем в процессе аудита.

Мы также предоставляем Совету директоров Организации заявление о том, что мы соблюдали все соответствующие этические требования в отношении независимости и информировали его обо всех взаимоотношениях и прочих вопросах, которые можно обоснованно считать оказывающими влияние на независимость аудитора, а в необходимых случаях - о соответствующих мерах предосторожности.

Руководитель аудита,
по результатам которого выпущено
аудиторское заключение
независимого аудитора
(руководитель задания по аудиту),
ОРНЗ 22006016065, действующий от
имени аудиторской организации
на основании доверенности
от 18.02.2026 № 40-01/2026-Ю

Ефремов Антон Владимирович

Аудиторская организация:
Юникон Акционерное Общество
117587, Россия, Москва, Варшавское шоссе, дом 125, строение 1, секция 11, 3 эт., пом. I, ком. 50,
ОРНЗ 12006020340

6 апреля 2026 года

Раскрываемый консолидированный отчет о прибыли или убытке и прочем совокупном доходе

за год, закончившийся 31 декабря 2025 г.

В тыс. российских рублей	Примечание	2025 год	2024 год
Выручка	7	**30 881 105**	**24 456 985**
Выручка от реализации лицензий		*26 515 121*	*21 733 480*
Выручка от реализации услуг в области информационной безопасности		*3 139 108*	*2 143 672*
Выручка от реализации программно-аппаратных комплексов		*1 068 685*	*389 722*
Прочая выручка		*158 191*	*190 111*
Себестоимость	9	**(3 694 388)**	**(2 386 332)**
Заработная плата и социальные отчисления		*(847 266)*	*(744 579)*
Амортизация нематериальных активов		*(2 215 478)*	*(1 296 596)*
Стоимость материалов		*(506 448)*	*(187 929)*
Прочие расходы		*(125 196)*	*(157 228)*
Валовая прибыль		**27 186 717**	**22 070 653**
Операционные расходы	9	**(17 854 888)**	**(17 455 816)**
Расходы на исследования и разработки		(4 476 210)	(3 824 016)
Расходы на продажу		(6 199 749)	(4 943 890)
Расходы на отраслевые мероприятия и развитие бизнеса		(2 058 056)	(2 632 508)
Расходы на продвижение и маркетинг		(1 183 813)	(1 487 269)
Общехозяйственные и административные расходы		(3 860 825)	(4 487 625)
Прочие операционные расходы, нетто		(76 235)	(80 508)
Прибыль от операционной деятельности		**9 331 829**	**4 614 837**
Процентные доходы		2 178 887	507 946
Процентные расходы	19	(4 104 777)	(1 225 224)
Прочие финансовые расходы		(23 567)	(48 431)
Прибыль до налогообложения		**7 382 372**	**3 849 128**
Расходы по налогу на прибыль	10	(108 851)	(185 139)
Прибыль за год		**7 273 521**	**3 663 989**
Прибыль, приходящаяся на долю:			
Собственников Компании	11	*7 275 484*	*3 662 039*
Неконтролирующих долей участия		*(1 963)*	*1 950*
Прочий совокупный доход:			
Статьи, которые впоследствии могут быть реклассифицированы в состав прибыли или убытка:			
Эффект пересчета иностранных подразделений в валюту презентации отчетности		4 373	312
Прочий совокупный расход за период		**4 373**	**312**
Общий совокупный доход за период		**7 277 894**	**3 664 301**
Приходящийся на долю:			
Собственников Компании		*7 279 857*	*3 662 351*
Неконтролирующих долей участия		*(1 963)*	*1 950*
Прибыль на акцию, рубли			
Базовая и разводненная прибыль на обыкновенную акцию	11	102,14	51,45

Примечания на стр. с 11 по 55 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет о финансовом положении

по состоянию на 31 декабря 2025 г.

В тыс. российских рублей	Примечание	31 декабря 2025 года	31 декабря 2024 года
АКТИВЫ			
Внеоборотные активы			
Основные средства	12, 22	3 151 183	3 279 653
Нематериальные активы	13	26 251 788	21 457 217
Прочие финансовые активы	17	2 126 409	1 702 400
Отложенные налоговые активы	10	884 421	357 085
		32 413 801	**26 796 355**
Оборотные активы			
Запасы	14	1 674 606	562 415
Торговая и прочая дебиторская задолженность	15	24 153 257	19 135 056
Денежные средства и их эквиваленты	16	2 779 128	6 225 167
		28 606 991	**25 922 638**
ИТОГО АКТИВЫ		**61 020 792**	**52 718 993**
КАПИТАЛ			
Уставный капитал	18	35 607	35 607
Акции в собственности	18	(599)	(2 404)
Нераспределенная прибыль	18	24 303 628	9 491 947
Резерв по платежам, основанным на акциях	18	-	7 536 197
Резерв накопленных курсовых разниц		858	(3 515)
Капитал, приходящийся на долю собственников Компании		**24 339 494**	**17 057 832**
Неконтролирующие доли участия		(13)	1 950
ИТОГО КАПИТАЛ		**24 339 481**	**17 059 782**
ОБЯЗАТЕЛЬСТВА			
Долгосрочные обязательства			
Долгосрочные кредиты и займы	19	15 358 869	10 326 668
Обязательства по договорам с покупателями	20	3 801 281	2 860 901
Отложенные налоговые обязательства	10	685 823	501 307
		19 845 973	**13 688 876**
Краткосрочные обязательства			
Краткосрочные кредиты и займы	19	8 651 361	16 022 157
Обязательства по договорам с покупателями	20	2 475 564	1 770 024
Торговая и прочая кредиторская задолженность	21	5 265 757	4 178 154
Обязательства по налогу на прибыль	10	442 656	-
		16 835 338	**21 970 335**
ИТОГО ОБЯЗАТЕЛЬСТВА		**36 681 311**	**35 659 211**
ИТОГО КАПИТАЛ И ОБЯЗАТЕЛЬСТВА		**61 020 792**	**52 718 993**

Д. Баранов

Генеральный директор

6 апреля 2026

Примечания на стр. с 11 по 55 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет об изменениях в капитале

за год, закончившийся 31 декабря 2025 г.

	Приходящийся на долю собственников Компании							
В тыс. российских рублей	Уставный капитал	Акции в собственности	Нераспределенная прибыль	Резерв по платежам, основанным на акциях	Резерв накопленных курсовых разниц	Итого капитал и резервы	Неконтролирующие доли участия	Итого капитал и резервы
На 1 января 2024 года	**33 000**		**13 171 115**	**-**	**(3 827)**	**13 200 288**	**-**	**13 200 288**
Прибыль за год	-		3 662 039	-	-	**3 662 039**	1 950	**3 663 989**
Прочий совокупный доход:								
Эффект курсовых разниц	-		-	-	312	**312**	**-**	**312**
Итого совокупный доход за 2024 год	**-**	**-**	**3 662 039**	**-**	**312**	**3 662 351**	**1 950**	**3 664 301**
Выкуп собственных акций	-	(443)	(3 300 418)	-	-	**(3 300 861)**		**(3 300 861)**
Эмиссия акционерного капитала	2 607	(2 607)	-	-	-	-	-	-
Сформирован резерв под выплату акциями (Примечание 18)	-	-	-	10 041 948	-	**10 041 948**	**-**	**10 041 948**
Программа «Стимулирование роста»	-	646	2 505 751	(2 505 751)	-	**646**		**646**
Дивиденды	-	-	(6 546 540)	-	-	**(6 546 540)**	-	**(6 546 540)**
На 31 декабря 2024 года	**35 607**	**(2 404)**	**9 491 947**	**7 536 197**	**(3 515)**	**17 057 832**	**1 950**	**17 059 782**
Прибыль за год	-		7 275 484	-	-	**7 275 484**	(1 963)	**7 273 521**
Прочий совокупный доход:								
Эффект курсовых разниц	-		-	-	4 373	**4 373**	**-**	**4 373**
Итого совокупный доход за 2025 год	**-**	**-**	**7 275 484**	**-**	**4 373**	**7 279 857**	**(1 963)**	**7 277 894**
Программа «Стимулирование роста» (Примечание 18)	-	1 805	7 536 197	(7 536 197)	-	**1 805**		**1 805**
На 31 декабря 2025 года	**35 607**	**(599)**	**24 303 628**	**-**	**858**	**24 339 494**	**(13)**	**24 339 481**

Примечания на стр. с 11 по 55 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет о движении денежных средств

за год, закончившийся 31 декабря 2025 г.

В тыс. российских рублей	Примечание	2025 год	2024 год
Движение денежных средств от операционной деятельности			
Прибыль до налогообложения		**7 382 372**	**3 849 128**
Корректировки:			
Чистые финансовые расходы / (доходы)		1 926 989	720 588
Амортизация основных средств	12	733 935	555 452
Амортизация нематериальных активов	13	2 280 194	1 336 554
Движение резервов по ожидаемым кредитным убыткам по дебиторской задолженности	15	14 757	1 118
Расходы по вознаграждению акциями		-	96 250
Курсовые разницы		(3 081)	(6 714)
Убыток от выбытия основных средств и нематериальных активов	12	2 969	18 830
Изменения оборотного капитала		**(3 306 313)**	**(3 146 788)**
Изменение торговой и прочей дебиторской задолженности	15	(5 032 959)	(2 166 966)
Изменение торговой и прочей кредиторской задолженности	21	1 192 919	(704 535)
Изменение обязательств по договорам с покупателями	20	1 645 919	166 442
Изменение запасов	14	(1 112 192)	(441 729)
Поступления денежных средств от основной деятельности		**9 031 822**	**3 424 418**
Проценты уплаченные	19	(3 512 695)	(968 986)
Проценты полученные		1 105 258	480 614
Банковские комиссии и прочие финансовые расходы		(22 467)	(38 446)
Налог на прибыль уплаченный		(2 874)	(11 512)
Денежные средства, полученные от операционной деятельности, нетто		**6 599 044**	**2 886 088**
Движение денежных средств от инвестиционной деятельности			
Денежные средства полученные:			
Займы выданные		80 766	-
Денежные средства уплаченные:			
Приобретение основных средств		(464 065)	(1 422 728)
Создание нематериальных активов		(6 955 103)	(5 139 397)
Покупка нематериальных активов		(200 383)	(109 208)
Займы выданные		(22 000)	(1 704 400)
Приобретение финансового актива		(63 605)	-
Денежные средства, использованные в инвестиционной деятельности, нетто		**(7 624 390)**	**(8 375 733)**
Движение денежных средств от финансовой деятельности			
Денежные средства полученные:			
Получение кредитов и займов	19	13 348 000	26 470 211
Денежные средства уплаченные:			
Дивиденды, выплаченные акционерам Компании		-	(6 546 540)
Погашение кредитов и займов	19	(15 444 181)	(6 300 000)
Платежи по договорам аренды	22	(328 885)	(292 408)
Выкуп собственных акций		-	(3 300 418)
Денежные средства, полученные от / (использованные в) финансовой деятельности, нетто		**(2 425 066)**	**10 030 845**
Эффект от курсовых разниц на остатки денежных средств и их эквивалентов		4 373	312
Изменение денежных средств и их эквивалентов, нетто		**(3 446 039)**	**4 541 512**
Денежные средства и их эквиваленты на начало года	**16**	**6 225 167**	**1 683 655**
Денежные средства и их эквиваленты на конец года	**16**	**2 779 128**	**6 225 167**

Примечания на стр. с 11 по 55 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

1. Общие сведения

Данная раскрываемая консолидированная финансовая отчетность была подготовлена в соответствии с принципами, указанными в пункте 2.1 примечаний за год, закончившийся 31 декабря 2025 года, для ПАО «Группа Позитив» («Компания») и его дочерних компаний («Группа»).

Компания зарегистрирована и находится в Российской Федерации. Компания является публичным акционерным обществом и была создана в соответствии с российским законодательством.

Юридический адрес Компании: 107061, г. Москва, вн.тер.г. муниципальный округ Преображенское, Преображенская пл., д. 8, помещ. 60.

Основное место нахождения Группы: 107061, г. Москва, вн.тер.г. муниципальный округ Преображенское, Преображенская пл., д. 8, помещ. 60.

Дочерние компании ПАО «Группа Позитив», которые были включены в данную консолидированную финансовую отчетность, представлены ниже:

Дочерняя компания	Страна	Вид деятельности	Доля владения на 2025 год	Доля владения на 2024 год
Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102	Россия	Разработка компьютерного программного обеспечения и оказание сопутствующих услуг	100%	100%
	Россия	Продажа компьютерного программного обеспечения, компьютерного оборудования и оказание сопутствующих услуг	100%	100%
		Продажа компьютерного программного обеспечения и оказание сопутствующих услуг	99%	100%
	Россия	Разработка компьютерного программного обеспечения и оказание сопутствующих услуг	99%	99%
	Россия	Предоставление прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению	100%	100%
	Россия	Деятельность административно-хозяйственная комплексная по обеспечению работы организации	100%	100%
	Россия	Разработка компьютерного программного обеспечения	90%	-
	Россия	Разработка компьютерного программного обеспечения	68%	-

Новые компании, вошедшие в периметр консолидации в отчетном периоде, были учреждены непосредственно Группой. *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102).*

По состоянию на 31 декабря 2025 бенефициарным владельцем Группы являлся *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102).*

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Группа разрабатывает, продает и поддерживает широкий спектр инновационных программных продуктов и услуг для ИТ-безопасности, предназначенных для выявления, верификации и нейтрализации реальных бизнес-рисков, которые могут возникать в IT-инфраструктуре предприятий.

Продуктовый портфель Группы включает несколько передовых продуктов, которые позволяют клиентам Группы:

- контролировать защищенность инфраструктуры и своевременно находить в ней уязвимости;
- выявлять инциденты ИБ в инфраструктуре любых масштабов, включая закрытые промышленные системы;
- обнаруживать 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.

Группа оказывает ряд сервисных и консультационных услуг в области кибербезопасности, включая непрерывный анализ защищенности бизнеса, обнаружение, реагирование и расследование сложных инцидентов, мониторинг защищенности корпоративных систем.

Ежегодно Группа проводит собственный научно-практический форум «Positive Hack Days» – одно из крупнейших мероприятий в области информационной безопасности в России и странах СНГ, в котором принимают участие тысячи специалистов в области информационных технологий и информационной безопасности, представители бизнеса и государственных структур, а также студенты. Являясь одной из ведущих компаний отрасли, Группа имеет собственный портал информационной безопасности SecurityLab.ru.

Группа разрабатывает образовательные программы для ведущих университетов и помогает студентам в начале их карьеры: материалы Positive Education, подготовленные экспертами Группы, используются более чем в 50 университетах.

По состоянию на 31 декабря 2025 г. в Группе работало 2 605 человек (на 31 декабря 2024 г. – 3 160), в том числе эксперты мирового уровня по защите ERP, SCADA, веб-приложений и мобильных приложений, в том числе в банковской и телекоммуникационной сферах.

15 апреля 2021 года Управление по контролю за иностранными активами Министерства финансов США («OFAC») внесло дочернюю компанию Группы *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102)* в Список лиц особых категорий и запрещенных лиц («SDN») («Санкции OFAC»). Санкции ограничивают доступ на финансовые и товарные рынки отдельных стран. Группа учитывает последствия санкций в своей деятельности, осуществляет их мониторинг, проводит анализ влияния санкций на финансовое положение и результаты хозяйственной деятельности.

23 июня 2024 года ПАО «Группа Позитив» была включена в 11-й пакет санкций Евросоюза.

На текущий момент введенные в отношении *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102)* санкции

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

не оказали существенного влияния на деятельность Группы, так как подавляющая доля выручки Группы (99%) получена от клиентов из России и стран СНГ. Международные интересы Группы не связаны со странами ЕС и сосредоточены в первую очередь на регионах, готовых работать с организациями из Российской Федерации, в частности - на рынках Латинской Америки, Ближнего Востока, Африки и Юго-Восточной Азии. Кроме того, санкции не повлияли на динамику выручки Группы: в отчетном году рост выручки составил 26%.

2. Основные положения учетной политики

2.1 Основы подготовки финансовой отчетности

Настоящая раскрываемая консолидированная финансовая отчетность составлена руководством Группы на основе полной финансовой отчетности за 2025 год, составленной руководством Группы в соответствии с Международными стандартами финансовой отчетности, путем исключения из нее сведений, раскрытие которых способно нанести ущерб Группе и (или) ее контрагентам (далее - чувствительная информация). Как следствие, данная раскрываемая консолидированная финансовая отчетность может быть непригодна для иной цели. Данная раскрываемая консолидированная финансовая отчетность не является полным комплектом консолидированной финансовой отчетности, составленной в соответствии с Международными стандартами финансовой отчетности. Иные сведения, содержащиеся в полной финансовой отчетности, включены в раскрываемую консолидированную финансовую отчетность структурно и содержательно таким же образом, как в полной консолидированной финансовой отчетности. Решение о составлении раскрываемой консолидированной финансовой отчетности принято руководством Группы на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102. Состав чувствительной информации определен руководством Группы также на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102.

Раскрываемая консолидированная финансовая отчетность подготовлена на основе принципов непрерывности деятельности и оценки по первоначальной стоимости, за исключением случаев, раскрытых в учетной политике ниже.

Подготовка консолидированной финансовой отчетности в соответствии с МСФО требует применения определенных ключевых оценочных суждений. Также требуется, чтобы руководство использовало суждения в процессе применения учетной политики Группы. Области, требующие более высокой степени суждения или сложности, а также области, в которых допущения и оценочные суждения являются ключевыми для консолидированной финансовой отчетности, раскрыты ниже в Примечании 5.

2.2 Основы консолидации

Раскрываемая консолидированная финансовая отчетность включает финансовую отчетность Компании и ее дочерних компаний.

Компания обладает контролем над объектом инвестиций только в том случае, если она:

- обладает полномочиями в отношении объекта инвестиций;
- подвергается рискам, связанным с переменным доходом от участия в объекте

инвестиций, или имеет право на получение такого дохода;

- имеет возможность использовать свои полномочия в отношении объекта инвестиций с целью оказания влияния на величину дохода Компании.

Группа повторно оценивает, контролирует ли она объект инвестиций, если факты и обстоятельства свидетельствуют об изменении одного или нескольких из трех компонентов контроля, перечисленных выше. Консолидация дочерней компании начинается, когда Группа получает контроль над дочерней компанией, и прекращается, когда Группа теряет контроль над дочерней компанией. Активы, обязательства, доходы и расходы дочерней компании, приобретенной или проданной в течение года, включаются в раскрываемую консолидированную финансовую отчетность с даты получения Группой контроля до даты, когда Группа перестает контролировать дочернюю компанию.

Все внутригрупповые активы и обязательства, капитал, доходы, расходы и денежные потоки, относящиеся к операциям между участниками Группы, полностью исключаются при консолидации.

Группа относит общий совокупный доход к собственникам материнской компании и неконтролирующим долям, даже если это приводит к отрицательному сальдо неконтролирующих долей.

При необходимости в финансовую отчетность дочерних компаний вносятся корректировки для приведения их учетной политики в соответствие с учетной политикой Группы.

2.3 Основные аспекты учетной политики

Основные аспекты учетной политики, применяемой Группой при подготовке настоящей раскрываемой консолидированной финансовой отчетности, представлены ниже:

2.3.1 Выручка по договорам с покупателями

Выручка – это доходы, которые возникают в ходе обычной деятельности Группы.

Выручка признается в сумме цены операции. Цена операции – это сумма к возмещению, право на которое Группа ожидает получить в обмен на передачу контроля над обещанными товарами или услугами покупателю, за исключением сумм, полученных от имени третьих сторон. Выручка признается за вычетом налога на добавленную стоимость и скидок.

Возмещение, подлежащее уплате покупателю, также включает в себя кредит или другие статьи, которые могут быть зачтены против сумм, причитающихся организации. Группа учитывает такие статьи, подлежащее уплате покупателю, как уменьшение цены операции и, следовательно, выручки.

Выручка признается, когда (или по мере того, как) Группа исполняет обязательство к исполнению путем передачи обещанных товаров или услуг покупателю (то есть, когда покупатель получает контроль над этим товаром или услугой).

Группа использует суждение для признания выручки в момент времени или с течением времени на основе определенного времени передачи контроля над обещанным товаром или услугой.

Выручка от реализации лицензий на ИТ-продукты

Ключевую ценность ИТ-продуктов Группы представляет их функционал, разрабатываемый и поддерживаемый Группой. Данные ИТ-продукты являются сложными решениями, совмещающими комплексный мониторинг сетей и инфраструктуры компаний, управление угрозами и безопасностью. Предлагаемые решения могут работать без обновлений баз данных, а в некоторых случаях клиенты могут поддерживать собственные базы данных угроз и использовать их для обслуживания безопасности продуктов.

Основная часть выручки от продажи лицензий конечным пользователям реализуется через сеть дистрибьюторов и партнеров, в связи с чем могут возникать различия в датах фактического отражения момента передачи лицензии дистрибьюторам и датами начала лицензирования продукта для конечного пользователя. В некоторых случаях Группа продает лицензии напрямую конечным пользователям.

Группа предоставляет право пользования своей интеллектуальной собственностью и учитывает данное обязательство к исполнению в момент времени. Соответствующая выручка признается в момент времени, когда лицензия предоставлена конечному пользователю.

Признание выручки по многолетним контрактам

В некоторых случаях Группа заключает многолетние договоры на реализацию лицензий на ИТ-продукты. Такие договоры заключаются в одной из следующих форм:

- доступ к одной многолетней лицензии;
- доступ к стандартной лицензии сроком на один год с возможностью пролонгации на один год и более.

Независимо от типа договора выручка признается в полной сумме в начале первого лицензионного периода. По условиям договора покупатели не имеют права на возврат лицензии.

Скидки за объем

Группа предоставляет своим покупателям скидки за объем продаж лицензий в рамках договоров. Предоставляемые скидки представляют собой переменное возмещение. Группа применяет метод наиболее вероятной суммы для оценки переменного возмещения. На сумму оцененного переменного возмещения Группа уменьшает сумму выручки, а также признает обязательство к выплате покупателю, которое отражается в составе Прочей кредиторской задолженности в раскрываемом консолидированном отчете о финансовом положении.

Выручка от услуг технической поддержки и мониторинга безопасности

Отдельно от продажи лицензий Группа реализует услуги расширенной техподдержки собственных ИТ-продуктов и мониторинга ИТ-систем (в большинстве случаев совместно с использованием ИТ-продуктов Группы). Такой тип выручки признается линейно в течение срока действия договора, который как правило составляет один год.

Прочие виды выручки Группы

Помимо перечисленных выше Группа имеет следующие виды выручки:

- услуги ИТ-безопасности (выручка признается в момент времени, когда услуги предоставлены);
- реализация программно-аппаратных комплексов (выручка признается в момент поставки комплекса покупателю);
- услуги в области исследований и технологических разработок (выручка признается в момент времени, когда услуги предоставлены);
- организация ИТ-мероприятий (выручка признается в дату проведения мероприятия).

Отложенный доход

Стоимость вознаграждения, получаемого до предоставления услуг по лицензиям или услугам по техподдержке в рамках договоров с покупателями, отражается как отложенный доход и признается в составе выручки по мере предоставления услуг.

Полученная, но не признанная в соответствии с учетной политикой в раскрываемом консолидированном отчете о прибыли или убытке и прочем совокупном доходе выручка отражается в рамках Обязательств по договорам с покупателями в составе раскрываемого консолидированного отчета о финансовом положении.

Группа учитывает отложенный доход, который будет признан в течение последующих 12 месяцев, в составе краткосрочных обязательств по договорам с покупателями, и оставшаяся часть признается в составе долгосрочных.

2.3.2 Функциональная валюта и валюта представления

Раскрываемая консолидированная финансовая отчетность представлена в российских рублях, которые также являются функциональной валютой материнской компании. Для каждой организации Группа определяет функциональную валюту, и статьи, включаемые в финансовую отчетность каждой организации, оцениваются с использованием этой функциональной валюты.

Операции в иностранной валюте и пересчет валют

Операции в иностранной валюте первоначально отражаются компаниями Группы по официальным обменным курсам Центрального Банка Российской Федерации (ЦБ РФ), действующим на дату, когда операция впервые удовлетворяет критериям признания. Монетарные активы и обязательства, выраженные в иностранной валюте, пересчитываются по обменным курсам ЦБ РФ в функциональной валюте, действующим на отчетную дату.

Немонетарные статьи, которые оцениваются по первоначальной стоимости в иностранной валюте, пересчитываются по обменному курсу ЦБ РФ, установленному на дату первоначальных операций. При определении обменного курса, используемого для первоначального признания активов, доходов и расходов (или их частей) при прекращении признания немонетарных активов или немонетарных обязательств, относящихся к авансовому возмещению, датой операции является дата, на которую Группа первоначально признала немонетарный актив или немонетарное обязательство, возникающее в связи с авансовым вознаграждением. Если существуют несколько авансовых платежей, Группа определяет дату транзакции для каждого поступления.

Компании Группы

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Для целей раскрываемой консолидированной отчетности, результаты и финансовое положение всех компаний Группы, функциональная валюта которых отличается от валюты представления, переводятся в валюту представления следующим образом:

i) Активы и обязательства в составе каждого раскрываемого консолидированного отчета о финансовом положении пересчитываются по обменному курсу, действующего на дату данного отчета;

ii) Доходы и расходы для каждого раскрываемого консолидированного отчета о прибыли или убытке и прочем совокупном доходе пересчитываются по среднему обменному курсу; а также

iii) Все курсовые разницы, полученные в результате пересчета, признаются отдельной строкой в составе Капитала.

Курсы российского рубля к основным иностранным валютам, установленные на отчетные даты, и средневзвешенные курсы за соответствующие отчетные периоды приведены ниже:

	31 декабря	
	2025 года	2024 года
Доллар США к Российскому рублю		
На конец года	78,2267	101,6797
Средний за период	83,2108	92,5652
Евро к Российскому рублю		
На конец года	92,0938	106,1028
Средний за период	94,0522	100,2154

2.3.3 Нематериальные активы

Нематериальные активы Группы представлены программными продуктами, созданными самой Группой, а также приобретенными нематериальными активами.

Нематериальные активы, созданные Группой

Стадия исследования

На стадии исследования Группа проводит новые запланированные исследования, предпринимаемые с целью получения новых научных или технических знаний.

Затраты на осуществление стадии исследования в рамках внутреннего проекта подлежат признанию в качестве расходов в момент их возникновения, поскольку Группа еще не может продемонстрировать наличие нематериального актива, который будет приносить вероятные будущие экономические выгоды. На стадии исследования Группа разрабатывает требования к функциональности ИТ-продуктов.

Затраты на исследовательскую деятельность, предпринятую с целью анализа рынка, подтверждения идеи и ее экономическое и техническое обоснование признаются Группой в составе прибыли или убытка за период в момент возникновения.

Стадия разработки

Разработка представляет собой применение результатов исследований или иных знаний при планировании или проектировании производства новых или существенно улучшенных программных продуктов до начала их коммерческого производства или использования.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Группа начинает капитализировать нематериальные активы, являющиеся результатом разработки, когда может продемонстрировать все перечисленное ниже:

- техническая осуществимость завершения разработки нематериального актива и доведение его до состояния, пригодного для использования или продажи;
- намерение завершить разработку нематериального актива и использовать или продать его;
- способность использовать или продать нематериальный актив;
- предполагаемый способ извлечения вероятных будущих экономических выгод;
- наличие рынка сбыта для продукта, получаемого от использования нематериального актива, или самого нематериального актива, или же, если этот актив предназначен для внутреннего использования самой организацией, полезность такого нематериального актива;
- наличие достаточных технических, финансовых и прочих ресурсов для завершения процесса разработки, использования или продажи нематериального актива;
- способность надежно оценить затраты, относящиеся к нематериальному активу в процессе его разработки.

Затраты на нематериальные активы, которые первоначально были признаны в качестве расходов, впоследствии не могут быть признаны в составе себестоимости нематериального актива.

В себестоимость самостоятельно созданного нематериального актива включаются все прямые затраты, необходимые для создания, производства и подготовки этого актива к использованию в соответствии с намерениями руководства.

Группа определяет следующие прямые затраты:

- затраты на вознаграждение работникам (в значении, определенном в МСФО (IAS) 19), возникающие в связи с созданием нематериального актива;
- выплаты, необходимые для регистрации юридического права;
- затраты по займам, непосредственно связанные с приобретением и разработкой «квалифицируемого актива», включаются в стоимость программных продуктов;
- стоимость обязательной и добровольной сертификации программных продуктов;
- другие прямые затраты, необходимые для создания, производства и подготовки этого актива к использованию.

Готовность актива к продаже

Стадия разработки программного продукта заканчивается, когда актив готов к продаже.

Группа определяет программный продукт как готовый к продаже в момент, когда его функциональные области разработаны до той степени, в которой продукт обладает всеми основными характеристиками, присущими программным продуктам того же класса на рынке.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

После первоначального признания нематериальный актив учитывается по первоначальной стоимости за вычетом накопленной амортизации и любых накопленных убытков от обесценения.

Группа использует линейный метод амортизации для программных продуктов и признает амортизационные расходы в составе себестоимости в раскрываемом консолидированном отчете о прибыли или убытке и прочем совокупном доходе.

Срок полезного использования для самостоятельно созданных нематериальных активов оценивается в пределах 5 – 10 лет.

При определении срока полезного использования нематериальных активов учитываются следующие факторы:

- предполагаемое использование этого актива Группой и способность руководящей команды эффективно управлять этим активом;
- обычный жизненный цикл продукта применительно к данному активу и общедоступная информация о расчетных оценках срока полезного использования аналогичных активов, которые используются аналогичным образом;
- техническое, технологическое, коммерческое и другие типы устаревания;
- стабильность отрасли, в которой функционирует указанный актив, и изменения рыночного спроса на продукты или услуги, произведенные активом;
- ожидаемые действия конкурентов или потенциальных конкурентов;
- уровень затрат на поддержание и обслуживание данного актива, требуемых для получения ожидаемых будущих экономических выгод от этого актива, а также способность и готовность Группы обеспечить такой уровень затрат;
- период наличия контроля над данным активом и юридические или аналогичные ограничения по использованию этого актива, например, даты истечения срока соответствующих договоров аренды; а также
- зависимость срока полезного использования соответствующего актива от срока полезного использования других активов Группы.

Группа определяет срок полезного использования на основе как внутренних, так и внешних источников информации.

Срок амортизации и метод начисления амортизации для нематериальных активов с конечным сроком полезного использования пересматриваются не реже, чем раз в год. Если ожидаемый срок полезного использования данного актива отличается от предыдущих расчетных оценок, то срок амортизации корректируется соответствующим образом.

Существенные доработки программных продуктов

Существенные доработки представляют собой изменения программного продукта, которые приводят к увеличению будущих экономических выгод, увеличению срока полезного использования и/или значительному повышению рыночной конкурентоспособности по сравнению с исходным продуктом.

Группа считает доработку существенной на основании следующих данных:

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

- расширение функциональности и/или увеличение продолжительности возможного периода коммерциализации программного продукта в результате разработки данных улучшений;
- значительное увеличение прогнозируемой выручки по функциональным направлениям, если данное улучшение повысит конкурентоспособность продукта на рынке;
- значительное увеличение срока полезного использования по результатам пересмотра.

В случае выявления существенных доработок программного продукта Группа применяет те же правила, как и для признания и последующего учета нематериальных активов.

Обесценение

На каждую отчетную дату Группа оценивает остаточную стоимость своих нематериальных активов на предмет наличия признаков их обесценения. Нематериальные активы в стадии разработки тестируются на предмет обесценения на ежегодной основе. Нематериальные активы, разработка которых завершена, тестируются на обесценение, если события или изменения в обстоятельствах указывают на то, что балансовая стоимость не может быть возмещена. Убыток от обесценения признается, если балансовая стоимость актива превышает его возмещаемую стоимость. Группа определяет возмещаемую стоимость своих программных продуктов на основе принципа ценности от использования.

Прочие нематериальные активы

Прочие нематериальные активы капитализируются в сумме цены покупки нематериального актива, включая импортные пошлины и невозмещаемые налоги на покупку, после вычета торговых скидок и уступок, а также любые затраты, непосредственно относящиеся к подготовке актива к использованию.

2.3.4 Основные средства

Основные средства отражаются по первоначальной стоимости за вычетом накопленной амортизации и накопленных убытков от обесценения, если таковые имеются. Первоначальная стоимость включает затраты, непосредственно связанные с приобретением объектов. Последующие затраты включаются в балансовую стоимость актива или признаются как отдельный актив только когда существует высокая вероятность того, что будущие экономические выгоды, связанные с данным объектом, будут поступать Группе, и стоимость объекта может быть надежно оценена. Все прочие расходы на мелкий ремонт и ежедневное техническое обслуживание отражаются в раскрываемом консолидированном отчете о прибыли или убытке и прочем совокупном доходе в течение финансового периода, в котором они были понесены.

Амортизация рассчитывается линейным методом для списания первоначальной стоимости каждого актива до его ликвидационной стоимости в течение предполагаемого срока эксплуатации объектов основных средств, которая составляет:

Вид основных средств	Срок полезного использования, лет
Мебель	10
Серверы и компьютерное оборудование	От 3 до 7

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Офисное оборудование	От 5 до 7
Прочее	От 3 до 5

Ликвидационная стоимость актива — расчетная сумма, которую организация получила бы на текущий момент от выбытия актива после вычета предполагаемых затрат на выбытие, если бы актив уже достиг конца срока полезного использования и состояния, характерного для конца срока полезного использования. Ликвидационная стоимость актива равна нулю, если Группа планирует использовать актив до конца его физического срока службы.

В конце каждого отчетного периода Руководство оценивает наличие признаков обесценения основных средств. Если такие признаки существуют, Руководство оценивает возмещаемую стоимость, которая определяется как наибольшая из двух величин: справедливой стоимости актива за вычетом затрат на продажу или ценности использования. Балансовая стоимость уменьшается до возмещаемой стоимости, а убыток от обесценения признается в составе прибыли или убытка за отчетный период. Убыток от обесценения актива, признанный в предыдущие отчетные периоды, сторнируется при необходимости, если произошло изменение в оценках, использованных для определения ценности использования актива или его справедливой стоимости за вычетом затрат на выбытие.

Прибыли или убытки от выбытия определяются сравнением выручки от выбытия с балансовой стоимостью и признаются в составе прибылей или убытков за отчетный период по строке «Прочие операционные доходы и расходы».

2.3.5 Затраты по кредитам и займам

Затраты по кредитам и займам, непосредственно связанные с приобретением или разработкой актива, которые занимают длительный промежуток времени, включаются в первоначальную стоимость данного актива. Все другие затраты по кредитам и займам признаются в качестве расходов в том периоде, в котором они возникают. Затраты по кредитам и займам включают проценты и другие расходы Группы, связанные с привлечением заемных средств.

В случае если Группа заимствует средства на общие цели и использует их для приобретения или разработки актива, Группа определяет сумму затрат по заимствованиям к капитализации путем умножения ставки капитализации на сумму затрат на данный актив. Ставка капитализации определяется как средневзвешенное значение затрат по заимствованиям применительно к займам Группы, остающимся непогашенными в течение периода, за исключением займов, полученных специально для приобретения или разработки актива.

2.3.6 Справедливая стоимость

Все активы и обязательства, справедливая стоимость которых оценивается или раскрывается в раскрываемой консолидированной финансовой отчетности, классифицируются в иерархии справедливой стоимости, описанной ниже:

- уровень 1 – цены на аналогичные активы и обязательства, определяемые активными рынками;
- уровень 2 – методы, где все используемые исходные данные, оказывающие существенное влияние на справедливую стоимость, являются наблюдаемыми, прямо или косвенно;

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

- уровень 3 – методы, использующие исходные данные, оказывающие существенное влияние на справедливую стоимость, не основанные на наблюдаемых рыночных данных.

Справедливая стоимость всех финансовых активов и обязательств Группы была оценена с использованием уровня 3 иерархии оценок справедливой стоимости, за исключением денежных средств и их эквивалентов, относящихся к уровням 1 и 2, соответственно. Выпущенные необеспеченные облигации классифицируются как относящиеся к уровню 1.

По состоянию на 31 декабря 2025 и 2024 гг. все финансовые активы и обязательства Группы отражены по амортизированной стоимости. Финансовые инструменты Группы включают денежные средства и их эквиваленты, банковские депозиты, торговую и прочую дебиторскую задолженность, торговую и прочую кредиторскую задолженность, займы и кредиты, и их справедливая стоимость существенно не отличается от их балансовой стоимости.

2.3.7 Обесценение нефинансовых активов

Дополнительная информация об обесценении нефинансовых активов также представлена в следующих примечаниях:

- Ключевые бухгалтерские суждения, оценочные значения и допущения – Примечание 5;
- Основные средства – Примечание 2.3.4;
- Нематериальные активы – Примечание 2.3.3.

На каждую отчетную дату Группа оценивает наличие признаков возможного обесценения актива. Если такие признаки существуют или требуется ежегодное тестирование актива на предмет обесценения, Группа оценивает возмещаемую стоимость актива. Возмещаемая стоимость - наибольшая из двух величин: справедливой стоимости актива за вычетом затрат на продажу и ценности использования.

Убыток от обесценения признается в сумме, на которую балансовая стоимость актива превышает его возмещаемую стоимость. Любые нефинансовые активы, кроме гудвила, которые подверглись обесценению, проверяются на предмет возможного восстановления обесценения на каждую отчетную дату.

2.3.8 Вознаграждения, основанные на акциях

В Группе действует программа, в рамках которой некоторые сотрудники и прочие стороны при росте капитализации Компании получают акции компании. Группа учитывает операции по вознаграждениям, основанным на акциях, в соответствии с МСФО (IFRS) 2 «Выплаты на основе акций».

Группа признает выплаты на основе акций с расчетами долевыми инструментами в составе собственного капитала.

Стоимость вознаграждений, основанных на акциях, расчеты по которым производятся долевыми инструментами, оценивается по справедливой стоимости (за исключением влияния условий перехода прав, отличных от рыночных) на дату предоставления.

Товары или услуги, полученные или приобретенные при операции по выплатам на основе акций могут быть признаны в качестве активов, если отвечают критериям признания активов, либо признаются расходом.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

2.4 Применение новых или пересмотренных стандартов и интерпретаций

Следующая поправка к стандартам вступила в силу в отчетном периоде, начавшемся 1 января 2025 года:

- Ограничения конвертируемости валюты (поправки к МСФО (IAS) 21 «Влияние изменений валютных курсов»;

Данная поправка не оказала существенного влияния на раскрываемую консолидированную финансовую отчетность Группы за 2025 г.

2.5 Стандарты, которые были выпущены, но еще не вступили в силу

Ниже приводятся стандарты и разъяснения, которые были выпущены и применимы к Группе, но еще не вступили в силу на дату выпуска настоящей раскрываемой консолидированной финансовой отчетности. Группа намерена применить эти стандарты с даты их вступления в силу и не ожидает существенного влияния на раскрываемую консолидированную финансовую отчетность Группы от их применения.

Следующие поправки вступают в силу для годовых периодов, начавшихся 1 января 2026 года:

- Поправки к классификации и оценке финансовых инструментов (поправки к МСФО (IFRS) 9 «Финансовые инструменты» и МСФО (IFRS) 7 «Финансовые инструменты: раскрытие информации»);
- Договоры купли-продажи электроэнергии, получаемой из природных источников» (поправки к МСФО (IFRS) 9 и МСФО (IFRS)7).

Следующие стандарты и поправки вступают в силу в отчетном периоде, начинающемся 1 января 2027 года:

- МСФО (IFRS) 18 «Представление и раскрытие информации в финансовой отчетности»;
- МСФО (IFRS) 19 «Непубличные дочерние компании: раскрытие информации».

Группа не применяла досрочно какие-либо стандарты, интерпретации или поправки, которые были выпущены, но еще не вступили в силу, перечисленные выше.

3. Управление финансовыми рисками

Основные финансовые обязательства Группы включают в себя кредиты и займы, обязательства по аренде, торговую и прочую кредиторскую задолженность. Основная цель этих финансовых обязательств - финансирование деятельности Группы. Основные финансовые активы Группы включают в себя торговую дебиторскую задолженность, а также денежные средства и краткосрочные депозиты, которые возникают непосредственно в результате ее деятельности.

Как и все другие компании, Группа подвержена рискам, связанным с использованием финансовых инструментов.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Группа подвержена следующим рискам, связанным с финансовыми инструментами: кредитный риск, рыночный риск и риск ликвидности. Руководство Группы рассматривает и согласовывает политики управления каждым из этих рисков, которые кратко изложены ниже.

3.1 Кредитный риск

Кредитный риск — это риск того, что контрагент не выполнит свои обязательства по финансовому инструменту или контракту с клиентом, что приведет к финансовым убыткам. Группа подвержена кредитному риску, связанному с ее операционной деятельностью (в основном с торговой дебиторской задолженностью), а также с денежными средствами и их эквивалентами, хранящимися в банках.

Торговая дебиторская задолженность

Группа анализирует уровень кредитного риска по контрагентам. Такие риски отслеживаются на возобновляемой основе и подлежат ежегодной или более частой проверке. Руководство Группы регулярно проводит анализ просроченной торговой дебиторской задолженности и отслеживает просроченные остатки. Поэтому руководство считает целесообразным предоставить информацию о сроках погашения и прочую информацию о кредитном риске.

Группа создает резерв под обесценение на основании оценки ожидаемых кредитных убытков за весь срок по всей торговой дебиторской задолженности с использованием упрощенного подхода МСФО (IFRS) 9. Резерв под убытки корректируется с учетом прогнозных факторов, специфичных для должника.

Кредитный риск клиентов управляется каждым бизнес-подразделением в соответствии с установленными политикой, процедурами и контролем Группы, относящимися к управлению кредитным риском клиентов. Группа контролирует уровень принимаемого на себя кредитного риска путем оценки степени риска для каждого контрагента или группы сторон. В целях минимизации кредитного риска руководство разработало и поддерживает классификацию кредитного риска Группы, чтобы классифицировать позиции в соответствии с их степенью риска дефолта. Дефолт по финансовому активу — это когда контрагент не производит платежи, в срок, подлежащий оплате в соответствии с условиями контракта. Группа отдельно оценивает вероятность наступления дефолта контрагента в случае, если задолженность просрочена более чем на 90 дней. Система классификации кредитного риска Группы включает 4 категории:

- Ниже среднего (непросроченная задолженность);
- Средний (задолженность, просроченная менее чем на 30 дней);
- Высокий (задолженность, просроченная на срок от 30 до 90 дней);
- Дефолт (задолженность, просроченная более чем на 90 дней).

Информация о кредитном рейтинге основана на оценочных данных, которые позволяют прогнозировать риск дефолта. При анализе учитываются характер подверженности риску и тип заемщика. Уровни кредитного риска определяются с использованием качественных и количественных факторов, указывающих на риск дефолта.

Уровни кредитного риска разработаны и определены для отражения риска дефолта по мере ухудшения кредитного риска. По мере увеличения кредитного риска разница в риске дефолта между категориями меняется. При первоначальном признании каждый риск

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

применяется на основании доступной информации о контрагенте. Все риски подвергаются мониторингу, в связи с чем уровень кредитного риска обновляется для отражения текущей информации. Применяемые процедуры мониторинга являются как общими, так и адаптированными к типу риска.

Группа отслеживает все финансовые активы, к которым применим резерв на ожидаемые кредитные убытки, чтобы оценить, произошло ли значительное увеличение кредитного риска с момента первоначального признания.

В результате таких действий, выполненных в течение отчётных периодов, руководство считает, что у Группы нет значительного риска убытков, помимо уже отраженного резерва.

Денежные средства и их эквиваленты

Денежные средства и их эквиваленты отражаются по амортизированной стоимости, которая приблизительно совпадает с текущей справедливой стоимостью.

Кредитный риск Группы по денежным средствам и их эквивалентам ограничен, поскольку контрагентами, как правило, являются финансовые учреждения с высокими кредитными рейтингами.

Максимальная подверженность кредитному риску на отчетную дату представляет собой балансовую стоимость каждого класса финансовых активов, раскрытых ниже.

в тыс. российских рублей	Прим.	31 декабря 2025 года	31 декабря 2024 года
Торговая дебиторская задолженность	15	23 802 726	18 206 736
Денежные средства и их эквиваленты	16	2 779 128	6 225 167
Общая максимальная подверженность кредитному риску		**26 581 854**	**24 431 903**

3.2 Рыночный риск

3.2.1 Риск изменения процентных ставок

Риск изменения процентных ставок — это риск того, что справедливая стоимость или будущие потоки денежных средств по финансовому инструменту будут колебаться из-за изменений рыночных процентных ставок. Подверженность Группы риску изменения рыночных процентных ставок в основном связана с долгосрочными долговыми обязательствами Группы с плавающей процентной ставкой.

Группа управляет риском изменения процентных ставок, имея сбалансированный портфель кредитов и займов с фиксированной и переменной ставкой.

По состоянию на 31 декабря 2025 года примерно 45% кредитов и займов Группы имеют фиксированную процентную ставку (на 31 декабря 2024: 27%).

Подверженность Группы изменению процентных ставок несущественна.

3.2.2 Валютный риск

Валютный риск — это риск того, что справедливая стоимость или будущие денежные потоки подвержены колебаниям из-за изменений валютных курсов. Подверженность Группы риску изменения обменных курсов в основном связана с операционной деятельностью Группы (в случае если выручка или расходы выражены в иностранной валюте) и чистыми инвестициями Группы в иностранную дочернюю компанию.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Целью управления валютным риском Группы является минимизация волатильности денежных потоков Группы, возникающих в результате колебаний обменных курсов. Руководство уделяет особое внимание оценке будущих денежных потоков Группы в иностранной валюте и управлению разрывами между притоком и оттоком денежных средств. В настоящее время Группа не использует инструменты хеджирования для управления валютными рисками.

Балансовая стоимость монетарных активов и монетарных обязательств Группы, выраженных в иностранной валюте, на конец отчетного периода представлена следующим образом:

тыс. российских рублей	В долларах США		В Евро		В дирхамах ОАЭ	
	31 декабря 2025 года	31 декабря 2024 года	31 декабря 2025 года	31 декабря 2024 года	31 декабря 2025 года	31 декабря 2024 года
Монетарные финансовые активы	111 123	46 475	11	5 066	-	-
Монетарные финансовые обязательства	(144 035)	(8 834)	(2 588)	(393)	(9 700)	(10 632)
Чистая валютная позиция	**(32 912)**	**37 641**	**(2 577)**	**4 673**	**(9 700)**	**(10 632)**

Подверженность Группы риску изменения валютных курсов несущественна.

3.3 Риск ликвидности

Риск ликвидности — это риск того, что Группа не сможет погасить все обязательства при наступлении срока их погашения.

Позиция ликвидности Группы тщательно отслеживается и управляется. Группа внедрила подробный процесс составления бюджета и прогнозирования денежных средств, чтобы обеспечить наличие достаточных денежных средств для выполнения своих платежных обязательств.

В таблице ниже представлены сроки погашения финансовых обязательств Группы:

31 декабря 2025 года	менее 1 года	1-2 года	2-5 лет	Итого
Торговая кредиторская задолженность	629 343	-	-	**629 343**
Кредиты и займы	3 338 550	19 908 198	-	**23 246 748**
Обязательства по аренде	294 175	390 821	78 486	**763 482**
Итого	**4 262 068**	**20 299 019**	**78 486**	**24 639 573**

31 декабря 2024 года	менее 1 года	1-2 года	2-5 лет	Итого
Торговая кредиторская задолженность	787 225	-	-	**787 225**
Кредиты и займы	15 704 313	9 729 075	-	**25 433 388**
Обязательства по аренде	317 825	399 736	197 877	**915 438**
Итого	**16 809 363**	**10 128 811**	**197 877**	**27 136 051**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

3.4 Управление капиталом

Для целей управления капиталом Группы капитал включает выпущенный капитал, эмиссионный доход и все прочие резервы собственного капитала, относящиеся к акционерам материнской компании. Основная цель управления капиталом Группы — максимизация акционерной стоимости. Группа управляет структурой капитала и вносит коррективы с учетом изменений экономических условий.

Управление капиталом осуществляется посредством контроля руководства за результатами деятельности Группы на основе показателей чистого долга, EBITDA, а также внутренних управленческих показателей EBITDAC и NIC.

Показатель EBITDA — это прибыль или убыток Группы за период, скорректированные на расходы по налогу на прибыль, финансовые доходы и расходы, доходы и расходы от курсовых разниц, износ, амортизацию и выбытие основных средств.

Показатель EBITDA LTM — это прибыль или убыток Группы за 12 месяцев, предшествующих отчетной дате, скорректированные на расходы по налогу на прибыль, финансовые доходы и расходы, доходы и расходы от курсовых разниц, износ, амортизацию и выбытие основных средств.

Чистый долг равен общей сумме долга (не включая обязательства по аренде) за вычетом денежных средств и их эквивалентов, а также банковских депозитов на каждую отчётную дату.

Значения показателей приведены ниже:

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Общая сумма долга	23 246 740	25 433 388
Наличные денежные средства и остатки на счетах в банках	2 779 128	6 225 167
Чистый долг	**20 467 611**	**19 208 221**
EBITDA	12 322 390	6 458 413
Чистый долг/EBITDA	1,66	2,97

EBITDAC – управленческий показатель, который отличается от показателя EBITDA, указанного выше, на:

- Разницы между управленческим показателем «Отгрузки» (см. описание ниже) и Выручкой;
- Сумму капитализированных расходов (см. описание ниже).

NIC – управленческий показатель, который отличается от показателя «Прибыль за период», на:

- Разницы между управленческим показателем «Отгрузки» (см. описание ниже) и «Выручкой»;
- Сумму капитализированных расходов (см. описание ниже);

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

- Амортизацию капитализированных расходов.

Капитализированные расходы - затраты Группы, которые не списываются на финансовый результат сразу, а признаются в качестве актива в отчете о финансовом положении, который впоследствии уменьшается за счет амортизации в течение срока полезного использования, либо списывается в момент, когда был использован в ходе хозяйственной деятельности. К таким затратам относятся: создание продуктов компании, покупка оборудования, мебели, программного обеспечения, запасов (за исключением тех, которые планируется перепродать), долгосрочная аренда и прочие несущественные затраты.

Отгрузки – управленческий показатель, который отражает доходы, возникающие в ходе обычной деятельности Группы, и признаются в сумме цены операции. Все отгрузки признаются в момент подписания акта-приемки с Покупателем и корректируются на дату оплаты (подробнее см. в таблице ниже).

Описание разниц между Отгрузками и Выручкой	Выручка	Отгрузки
Пролонгация существующих у заказчика лицензий	по окончанию срока действия существующей лицензии	по дате отгрузки пролонгированной лицензии
Продажи сертификатов на техническую поддержку и прочие услуги	равномерно в течение срока действия сертификата	одномоментно по дате отгрузки
Премии покупателям	уменьшают сумму выручки	на величину отгрузок не влияют, признаются в составе расходов
Продажи, не оплаченные до 31 марта в году, следующим за отчетным	корректировка не делается	отгрузки отчетного периода, которые не будут оплачены до 31 марта в году, следующим за отчетным, переносятся в следующий отчетный период

Разницы между отгрузками и выручкой за 2025 г. составили (1 711 729) тыс. руб. (2024 г: 937 000 тыс. руб.), как указано в таблице ниже:

в тыс. российских рублей	2025 год	2024 год
Отгрузки с НДС	**33 638 340**	**24 080 419**
НДС	*(1 045 506)*	*(560 434)*
Отгрузки без НДС	**32 592 834**	**23 519 985**
Разницы между отгрузками и выручкой	*(1 711 729)*	*937 000*
Выручка (см. Примечание 7)	**30 881 105**	**24 456 985**

в тыс. российских рублей	2025 год	2024 год
EBITDA	**12 322 390**	**6 458 413**
Разницы между отгрузками и выручкой, за иск. разниц в классификации премий покупателям	*1 181 729*	*(1 327 098)*
Капитализированные расходы и прочее	*(6 380 620)*	*(6 371 879)*
EBITDAC	**7 123 499**	**(1 240 564)**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	2025 год	2024 год
Прибыль за период	**7 273 521**	**3 663 989**
Разницы между отгрузками и выручкой, за искл. разниц в классификации премий покупателям	*1 181 729*	*(1 327 098)*
Капитализированные расходы и прочее	*(6 380 620)*	*(6 371 879)*
Амортизация капитализированных расходов, капитализация процентов и прочее	*656 203*	*1 379 837*
NIC	**2 730 833**	**(2 655 151)**

Цели Группы при управлении капиталом состоят в том, чтобы гарантировать способность Группы продолжать непрерывно свою деятельность, чтобы обеспечивать прибыль для акционеров и выгоды для других заинтересованных сторон, а также поддерживать оптимальную структуру капитала для снижения стоимости капитала. Для поддержания или корректировки структуры капитала Группа может скорректировать сумму дивидендов, выплачиваемых акционерам, вернуть капитал акционерам, выпустить новые акции или продать активы для уменьшения долга. Сумма капитала, которым Группа управляла по состоянию на 31 декабря 2025 года, составляла 24 339 495 тыс. рублей (на 31 декабря 2024: 17 057 832 тыс. рублей).

Руководство Группы ежегодно пересматривает структуру капитала Группы. В рамках этого обзора руководство рассматривает стоимость капитала и риски, связанные с каждым классом капитала. Основываясь на результатах обзора, Группа уравновешивает свою общую структуру капитала за счет выпуска нового долга или погашения существующего долга. Группа контролирует капитал на основе отношения заемных средств к собственному капиталу (не более 1,5:1). Отношение на 31 декабря 2025 года составляет 1:1 (2024: 1,5:1).

4. Управление рисками наступления недопустимых событий

С точки зрения информационной безопасности Группа в первую очередь ориентируется на непрерывность бизнеса, безопасность своих продуктов и сохранность персональных данных сотрудников, клиентов и акционеров. Исходя из этого, топ-менеджментом был выделен перечень Недопустимых событий, вокруг предотвращения которых и строится информационная безопасность Группы.

Для управления рисками наступления Недопустимых событий Группа непрерывно совершенствует свою киберзащиту, учитывая эволюцию угроз и лучшие практики информационной безопасности:

• применяет современные технологии кибербезопасности, используя все свои продукты в промышленной среде. В отчетном периоде были модернизированы системы SIEM (переход на новую базу данных LogSpace), WAF (перевод на PT AF Pro);

• осуществляет проактивный мониторинг информационной безопасности: организовано круглосуточное обнаружение и реагирование на угрозы ИБ, несколько уровней реагирования. Среднее время реагирования на инциденты высокой критичности не превышает 5-ти часов с момента обнаружения, что свидетельствует о высокой скорости реагирования.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

• проводит регулярную оценку, выявление и устранение новых уязвимостей по выстроенному процессу. Проводит тестирования на проникновение (пентест) для оценки защищенности инфраструктуры, сервисов компании, а также выпускаемых продуктов. Активное взаимодействие с продуктовыми командами разработки, возможное благодаря применению продуктов Группы в защите собственной информационной инфраструктуры, позволяет повышать качество и ускорять выпуск новых стабильных релизов.

• на платформе BugBounty опубликованы четыре программы, за 12 месяцев 2025 года выплачено вознаграждение в размере 1 360 тыс. руб.:

- Positive dream hunting - программа по реализации недопустимых событий Positive Technologies, с фондом вознаграждения в 60 000 тыс. руб. За время существования программы ни одно из недопустимых событий в полном или частичном объеме не реализовано;

- Positive bug hunting - программа по поиску уязвимостей в сервисах компании. За 12 месяцев 2025 года принято и рассмотрено 10 отчетов, выплачено 535 тыс. руб.;

- PT Cloud - программа по поиску уязвимостей в экосистеме облачных продуктов для кибер-безопасности от Positive Technologies. Выплачено 145 тыс. руб. по 7 отчетам;

- Продукты Positive Technologies - программа, запущенная в марте 2025 года, нацелена на оценку безопасности продуктов компании. За это время принято 14 отчетов по продуктам, из которых по 10 отчетам внесены ценные исправления. Суммарно по программе было выплачено 680 тыс.руб.;

• реализует организационные меры: регулярное обучение сотрудников по киберигиене и противодействию фишингу, четкие регламенты реагирования на инциденты. В отчетном году 1760 человек прошли обязательное обучение по вопросам кибербезопасности. Обучение включало адаптированные модули для отдельных ролей (например, для сотрудников первой линии технической поддержки и административного персонала);

• проходит регуляторные аудиты для подтверждения права осуществления лицензируемой деятельности (ФСТЭК РФ).

Расходы Группы за отчетный период на обеспечение кибербезопасности составили 135 303 тыс. руб. Данные расходы включают заработную плату сотрудников департамента информационной безопасности и закупку внешних ПО.

Уровень зависимости Группы от сторонних облачных провайдеров и поставщиков ИТ-инфраструктуры оценивается как низкий. Соответственно, риски, связанные с кибератаками на их системы, включая простои или утечки данных, не представляют существенной угрозы для непрерывности операций и экономической устойчивости Группы.

В отчетном периоде Группа продолжила планомерное повышение зрелости системы кибербезопасности в соответствии с требованиями государственных стандартов (ГОСТ),

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

национальных регуляторных требований (НКЦКИ, ФСТЭК). Актуализированы некоторые внутренние нормативные документы по информационной безопасности, введены новые.

5. Ключевые бухгалтерские суждения, оценочные значения и допущения

Группа делает оценки и допущения, которые влияют на отражаемые в отчетности суммы доходов, расходов, активов и обязательств, а также на соответствующие раскрытия информации. Оценки и суждения постоянно анализируются и основываются на опыте руководства и иных факторах, включая ожидания в отношении будущих событий, которые считаются разумными в данных обстоятельствах. Руководство также выносит определенные суждения, помимо тех, которые предполагают оценку, в процессе применения учетной политики. Суждения, которые наиболее существенно влияют на суммы, отражаемые в раскрываемой консолидированной финансовой отчетности, и оценки, которые могут привести к существенной корректировке балансовой стоимости активов и обязательств в течение отчетного периода, включают:

Срок полезного использования нематериальных активов

Основываясь на исторических данных, анализе рынка, сроках полезного использования аналогичных продуктов других компаний и ожидаемых выгодах от потребления активов, руководство оценивает сроки полезного использования самостоятельно созданных нематериальных активов. Срок полезного использования периодически пересматривается, чтобы обеспечить его уместность в связи с изменениями рынка и доработкой продуктов.

За год, закончившийся 31 декабря 2025 года, если бы оцениваемые сроки полезного использования нематериальных активов, созданных Группой, были бы на 10 процентов больше / меньше при неизменности всех прочих переменных, величина амортизации за год уменьшилась / увеличилась бы на 119 342 тыс. руб. (за год, закончившийся 31 декабря 2024 года: на 93 404 тыс. руб.).

Капитализация расходов на разработку

В соответствии с принятой учетной политикой Группа капитализирует затраты на разработку продуктов. Капитализация затрат на разработку продуктов начинается с момента, в котором получено заключение руководства о подтверждении технической и экономической целесообразности продукта, и заканчивается в момент готовности актива к продаже. После того момента, когда актив готов к продаже, Группа может существенно дорабатывать функциональность программного продукта. В периоды существенных доработок затраты на доработку программных продуктов также капитализируются.

Руководство делает допущения относительно момента готовности активов к продаже и периодов значительных доработок программных продуктов.

В период существенных доработок продукта Группа исключает из капитализированных затрат исправление ошибок и доработки ранее реализованной функциональности программного продукта и признает их расходами текущего периода в составе расходов на исследования и разработку. При определении суммы затрат, исключаемой из капитализации, Группа применяет оценочное суждение, основанное на экспертном мнении команды разработки.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

За год, закончившийся 31 декабря 2025 года, если бы сумма затрат, исключаемая из капитализации, была на 10 процентов больше / меньше при неизменности всех прочих переменных, сумма капитализированных затрат в состав нематериальных активов за год уменьшилась / увеличилась бы на 42 152 тыс. руб. (за год, закончившийся 31 декабря 2024 года: на 39 922 тыс. руб.).

Группа ежегодно оценивает индикаторы обесценения завершенных нематериальных активов и проводит тесты на предмет обесценения, если они обнаружены, а также проводит тесты на обесценение нематериальных активов на стадии разработки. Тесты на обесценение нематериальных активов основаны на чистой приведенной стоимости денежных потоков, связанных с этими активами. Расчет данного показателя зависит от оценок будущих денежных потоков, включая долгосрочные темпы роста, ожидаемые выгоды от актива и соответствующую ставку дисконтирования, которая будет применяться к будущим денежным потокам. Более подробная информация об этих оценках представлена в Примечании 13.

6. Сезонность

Результаты операционной деятельности Группы носят сезонный характер, что по большей части связано с планированием бюджета заказчиков. Доходы Группы, как правило, увеличиваются во второй половине года. Это объясняется тем, что большая часть заказов обычно закрываются к концу календарного года из-за календарного цикла планирования и бюджетирования в Российской Федерации. Вследствие этого результаты операционной деятельности Группы в течение финансового года могут быть не сбалансированы.

7. Выручка по договорам с покупателями

В следующей таблице выручка по договорам с покупателями разбита по основным категориям и срокам признания выручки.

	2025 год		2024 год	
	Сроки признания выручки		Сроки признания выручки	
в тыс. российских рублей	в момент времени	с течением времени	в момент времени	с течением времени
Выручка от реализации лицензий на ИТ-продукты	**26 515 121**	**-**	**21 733 480**	**-**
Выручка от реализации программно-аппаратных комплексов	**994 857**	**73 828**	**329 936**	**59 786**
Выручка от реализации услуг в области информационной безопасности	**1 392 505**	**1 746 603**	**988 941**	**1 154 731**
Выручка от услуг ИТ-безопасности	1 208 874	-	622 360	-
Выручка от услуг технической поддержки и мониторинга безопасности	-	1 746 603	-	1 154 731
Выручка от услуг в области исследований и технологических разработок	16 707	-	80 263	-
Выручка от прочих услуг	166 924	-	286 318	-
Прочая выручка	**158 191**	**-**	**190 111**	**-**
Итого выручка	**29 060 674**	**1 820 431**	**23 242 468**	**1 214 517**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

8. Информация по сегментам

Операционные сегменты определяются как компоненты предприятия, по которым доступна отдельная финансовая информация и которые регулярно оцениваются руководством при принятии решения о распределении ресурсов и оценке результатов деятельности. Руководство определило, что Группа организована как один отчетный операционный сегмент и работает в нем.

Выручка Группы в основном связана с продажей лицензий на ИТ-продукты, разработанные Группой, услуг технической поддержки, компьютерного оборудования и услуг ИТ-безопасности. Группа продает свою продукцию в основном через партнеров-дистрибьюторов, а также напрямую клиентам Группы.

В течение 2025 примерно 75% выручки Группы было получено через пять крупных дистрибьюторов (в течение 2024 примерно 82% выручки Группы было получено через четырех крупных дистрибьюторов), в то время как конечными пользователями ИТ-продуктов Группы являются крупные и средние предприятия различных отраслей.

Количество конечных пользователей (без пользователей XSpider) в 2025 составило 1 966, в 2024 – 1 748. В связи с этим, руководство Группы считает, что риск операционной концентрации не является существенным. По состоянию на 31 декабря 2025 года непогашенная дебиторская задолженность этих покупателей составляла 20 817 292 тыс. рублей (на 31 декабря 2024: 16 097 592 тыс. рублей). Большая часть выручки приходится на клиентов из Российской Федерации: 96% в 2025 (в 2024: 96%).

Продукцию Группы можно разделить на четыре основные продуктовые линейки. Общая выручка по продуктовым линейкам за годы, закончившиеся 31 декабря 2025 и 2024, представлена в Примечании 7.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

9. Операционные расходы

Операционные расходы Группы за 2025 год классифицируются по характеру затрат в таблице ниже.

в тыс. российских рублей	Себестоимость	Расходы на исследования и разработки	Общие и администра-тивные расходы	Расходы на отраслевые мероприятия и развитие бизнеса	Расходы на продажу	Расходы на продвижение и маркетинг	Прочие операционные расходы, нетто	2025 год
Заработная плата	765 993	3 383 687	1 949 876	529 816	5 032 882	453 101	-	**12 115 355**
Социальные отчисления	81 273	353 303	304 224	46 694	425 469	37 179	-	**1 248 142**
Амортизация нематериальных активов	2 215 478	26 596	23 755	1 873	11 242	1 248	-	**2 280 192**
Расходы на мероприятия	-	-	-	1 350 007	422 969	-	-	**1 772 976**
Стоимость материалов	506 448	23 529	92 357	121 055	-	-	-	**743 389**
Амортизация основных средств	-	232 229	463 455	4 990	29 935	3 327	-	**733 936**
Маркетинговые расходы	-	-	-	-	-	640 308	-	**640 308**
Услуги связи и дата-центров	-	233 074	251 819	-	-	2	-	**484 895**
Профессиональные услуги	-	86 236	224 705	-	42 719	18 474	-	**372 134**
Расходы на программное обеспечение	-	81 368	151 060	3 621	21 720	18 763	-	**276 532**
Расходы на аренду и содержание помещений	-	-	254 503	-	163	-	-	**254 666**
Командировочные расходы	-	30 757	31 040	-	155 408	8 876	-	**226 081**
Курсовые разницы, нетто	-	-	-	-	-	-	(3 082)	**(3 082)**
Прочие расходы/ доходы, нетто	125 196	25 431	114 031	-	57 242	2 535	79 317	**403 752**
Итого	**3 694 388**	**4 476 210**	**3 860 825**	**2 058 056**	**6 199 749**	**1 183 813**	**76 235**	**21 549 276**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Операционные расходы Группы за 2024 год классифицируются по характеру затрат в таблице ниже.

в тыс. российских рублей	Себестоимость	Расходы на исследования и разработки	Общие и администра-тивные расходы	Расходы на отраслевые мероприятия и развитие бизнеса	Расходы на продажу	Расходы на продвижение и маркетинг	Прочие операционные расходы, нетто	2024 год
Заработная плата	713 581	3 119 252	1 915 633	614 055	3 735 119	433 958	-	**10 531 598**
Социальные отчисления	30 998	118 684	87 971	20 765	117 884	19 192	-	**395 494**
Амортизация нематериальных активов	1 296 596	7 982	30 918	-	1 058	-	-	**1 336 554**
Расходы на мероприятия	-	-	-	1 763 487	792 930	-	-	**2 556 417**
Стоимость материалов	187 929	35 628	258 334	123 149	-	-	-	**605 040**
Амортизация основных средств	12 307	74 683	435 084	4 542	25 479	3 358	-	**555 453**
Маркетинговые расходы	-	-	-	-	-	972 430	-	**972 430**
Услуги связи и дата-центров	-	75 005	263 786	-	-	-	-	**338 791**
Профессиональные услуги	117 913	189 900	260 725	-	37 416	34 035	-	**639 989**
Расходы на программное обеспечение	1 961	51 151	244 469	17 161	47 831	11 640	-	**374 213**
Расходы на аренду и содержание помещений	10 795	112	505 853	3 084	14 699	2 001	-	**536 544**
Командировочные расходы	281	139 107	123 145	86 251	144 182	1 903	-	**494 869**
Курсовые разницы, нетто	-	-	-	-	-	-	(6 714)	**(6 714)**
Прочие расходы/ доходы, нетто	13 971	12 512	361 707	14	27 292	8 752	87 222	**511 470**
Итого	**2 386 332**	**3 824 016**	**4 487 625**	**2 632 508**	**4 943 890**	**1 487 269**	**80 508**	**19 842 148**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

10. Налог на прибыль

Расходы по налогу на прибыль включают следующее:

в тыс. российских рублей	2025 год	2024 год
Текущий налог	451 671	857
Отложенный налог	(342 820)	184 282
Прочее	-	-
Итого налог на прибыль за отчетный период	**108 851**	**185 139**

С 1 января 2021 года в рамках реализации инициатив развития цифровой экономики в российское налоговое законодательство были включены льготы для ИТ-компаний, заключающиеся в снижении ставки по налогу на прибыль с 20% до 3% и установлении пониженных ставок по социальным взносам при соблюдении компанией определенных критериев. Кроме того, в рамках комплексного пакета мер поддержки ИТ-отрасли, принятого в марте 2022 г., ставка налога на прибыль на период 2022 – 2024 гг. для таких компаний снижена до 0%, а также действует мораторий на плановые проверки надзорными органами. Компании Группы *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102)* применяют перечисленные льготы. Ставка налога на прибыль, применимая к остальным компаниям Группы, преимущественно составляет 25% в 2025 году (20% в 2024 году). С 1 января 2025 года для ИТ-компаний введена ставка налога на прибыль в размере 5%. По этой ставке рассчитаны отложенные налоговые активы и обязательства.

Дивиденды, полученные от большинства дочерних компаний Группы, подлежат налогообложению по ставке налога на прибыль 0% в соответствии с применимым налоговым законодательством.

Ниже приводится сверка ожидаемых и фактических налоговых расходов.

в тыс. российских рублей	2025 год	2024 год
Прибыль до налогообложения	**7 382 372**	**3 849 128**
Теоретические расходы по налогу на прибыль по ставке, установленной законодательством	1 845 593	769 826
Эффект от применения пониженной ставки налогообложения для ИТ-компаний	(1 689 985)	(522 050)
Эффект от не вычитаемых расходов для применяемых ставок налогообложения	(46 757)	(62 637)
Прочие разницы	-	-
Итого налог на прибыль за отчетный период	**108 851**	**185 139**

Различия между МСФО и российским законодательством в области налогообложения приводят к возникновению временных разниц между балансовой стоимостью активов и обязательств для целей финансовой отчетности и их налоговой базой.

в тыс. российских рублей	1 января 2025 года	Начислено в прибыли или убытке	31 декабря 2025 года
Налоговый эффект от вычитаемых временных разниц и налоговых убытков, перенесенных на будущие периоды			
Обязательства по договорам с покупателями	113 569	23 230	136 799
Торговая и прочая кредиторская задолженность	140 281	30 545	170 826

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	1 января 2025 года	Начислено в прибыли или убытке	31 декабря 2025 года
Налоговый эффект от вычитаемых временных разниц и налоговых убытков, перенесенных на будущие периоды			
Займы и кредиты	28 153	(7 664)	20 489
Торговая и прочая дебиторская задолженность	12 263	16 314	28 577
Налоговые убытки, перенесенные на будущие периоды	62 819	464 911	527 731
Признанный отложенный налоговый актив	**357 085**	**527 336**	**884 421**

в тыс. российских рублей	1 января 2024 года	Начислено в прибыли или убытке	31 декабря 2024 года
Налоговый эффект от вычитаемых временных разниц и налоговых убытков, перенесенных на будущие периоды			
Обязательства по договорам с покупателями	159 666	(46 097)	113 569
Торговая и прочая кредиторская задолженность	83 748	56 533	140 281
Займы и кредиты	19 367	8 786	28 153
Торговая и прочая дебиторская задолженность	9 072	3 191	12 263
Налоговые убытки, перенесенные на будущие периоды	6 773	56 046	62 819
Признанный отложенный налоговый актив	**278 626**	**78 459**	**357 085**

По состоянию на 31 декабря 2025 года Группа накопила налоговые убытки в размере 2 264 879 тыс. рублей (вычитаемая временная разница в размере 527 731 тыс. руб.) (на 31 декабря 2024: 314 095 тыс. рублей (вычитаемая временная разница в размере 62 819 тыс. руб.)), которые в основном возникли в Российской Федерации. Эти убытки могут быть зачтены против будущей налогооблагаемой прибыли дочерних компаний, в которых возникли убытки и в отношении которых были признаны отложенные налоговые активы.

в тыс. российских рублей	1 января 2025 года	Начислено в прибыли или убытке	31 декабря 2025 года
Налоговый эффект от налогооблагаемых временных разниц			
Нематериальные активы	422 290	169 548	591 838
Основные средства	79 017	14 968	93 985
Торговая и прочая дебиторская задолженность	-	-	-
Признанное налоговое отложенное обязательство	**501 307**	**184 516**	**685 823**

в тыс. российских рублей	1 января 2024 года	Начислено в прибыли или убытке	31 декабря 2024 года
Налоговый эффект от налогооблагаемых временных разниц			
Нематериальные активы	200 472	221 818	422 290
Основные средства	34 885	44 132	79 017
Торговая и прочая дебиторская задолженность	3 209	(3 209)	-
Признанное налоговое отложенное обязательство	**238 566**	**262 741**	**501 307**

11. Прибыль на акцию

Базовая прибыль на акцию рассчитывается путем деления прибыли или убытка, приходящегося на долю держателей обыкновенных и привилегированных акций Группы, на средневзвешенное количество обыкновенных и привилегированных акций в обращении в течение отчетного периода.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Компания не имеет обыкновенных акций с потенциально разводняющим эффектом, следовательно, разводненная прибыль на акцию равна базовой прибыли на акцию.

Прибыль на акцию рассчитывается следующим образом:

в тыс. российских рублей	2025 год	2024 год
Прибыль за год	7 273 521	3 663 989
Средневзвешенное количество акций в обращении (шт.)	71 214 000	71 214 000
Базовая и разводненная прибыль на акцию (выражена в рублях на акцию)	**102,14**	**51,45**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

12. Основные средства

в тыс. российских рублей	Активы в форме права пользования	Серверы и компьютерное оборудование	Офисное оборудование	Мебель	Прочее	Итого
Первоначальная стоимость на 1 января 2024 года	**1 208 624**	**1 408 343**	**119 683**	**35 176**	**143 467**	**2 915 293**
Накопленная амортизация	**(613 931)**	**(432 192)**	**(22 030)**	**(7 976)**	**(70 773)**	**(1 146 902)**
Остаточная стоимость на 1 января 2024 года	**594 693**	**976 151**	**97 653**	**27 200**	**72 694**	**1 768 391**
Поступления	157 057	1 330 159	325 020	90 340	118 333	**2 020 909**
Модификация договоров аренды	334 783	-	-	-	-	**334 783**
Выбытия	-	(408 940)	(2 972)	(101)	-	**(412 013)**
Начисленная амортизация	(248 234)	(247 477)	(22 669)	(5 184)	(31 888)	**(555 452)**
Выбытие амортизации	-	120 787	2 174	74	-	**123 035**
Первоначальная стоимость на 31 декабря 2024 года	**1 700 464**	**2 329 562**	**441 731**	**125 415**	**261 800**	**4 858 972**
Накопленная амортизация	**(862 165)**	**(558 882)**	**(42 525)**	**(13 086)**	**(102 661)**	**(1 579 319)**
Остаточная стоимость на 31 декабря 2024 года	**838 299**	**1 770 680**	**399 206**	**112 329**	**159 139**	**3 279 653**
Первоначальная стоимость на 1 января 2025 года	**1 700 464**	**2 329 562**	**441 731**	**125 415**	**261 800**	**4 858 972**
Накопленная амортизация	**(862 165)**	**(558 882)**	**(42 525)**	**(13 086)**	**(102 661)**	**(1 579 319)**
Остаточная стоимость на 1 января 2025 года	**838 299**	**1 770 680**	**399 206**	**112 329**	**159 139**	**3 279 653**
Поступления	17 055	510 685	12 804	21 744	22 966	**585 254**
Модификация договоров аренды	62 539	-	-	-	-	**62 539**
Выбытия	(39 771)	(18 209)	(8 350)	(398)	(9 453)	**(76 181)**
Начисленная амортизация	(240 753)	(371 818)	(49 495)	(13 363)	(58 506)	**(733 935)**
Выбытие амортизации	13 550	8 872	1 795	183	9 453	**33 853**
Первоначальная стоимость на 31 декабря 2025 года	1 740 287	2 822 038	446 185	146 761	275 313	**5 430 584**
Накопленная амортизация	(1 089 368)	(921 828)	(90 225)	(26 266)	(151 714)	**(2 279 401)**
Остаточная стоимость на 31 декабря 2025 года	**650 919**	**1 900 210**	**355 960**	**120 495**	**123 599**	**3 151 183**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

13. Нематериальные активы

в тыс. российских рублей	Нематериальные активы, созданные Группой, прошедшие стадию разработки	Нематериальные активы, созданные Группой, находящиеся на стадии разработки	Прочие нематери-альные активы	Итого
Остаточная стоимость на 1 января 2024 года	**6 165 200**	**1 279 207**	**99 161**	**7 543 568**
Первоначальная стоимость на 1 января 2024 года	**8 454 603**	**1 279 207**	**164 869**	**9 898 679**
Накопленная амортизация на 1 января 2024 года	**(2 289 403)**	**-**	**(65 708)**	**(2 355 111)**
Поступления	10 439 624	4 762 554	34 369	15 236 547
Начисленная амортизация	(1 279 194)	-	(57 360)	(1 336 554)
Реклассификация в НМА, прошедшие стадию разработки	665 514	(665 514)	-	-
Выбытие НМА	-	-	(78 480)	(78 480)
Списание амортизации	-	-	92 136	92 136
Остаточная стоимость на 31 декабря 2024 года	**15 991 144**	**5 376 247**	**89 826**	**21 457 217**
Первоначальная стоимость на 31 декабря 2024 года	**19 559 741**	**5 376 247**	**120 758**	**25 056 746**
Накопленная амортизация на 31 декабря 2024 года	**(3 568 597)**	**-**	**(30 932)**	**(3 599 529)**
Поступления	3 751 753	3 210 408	108 651	7 070 812
Начисленная амортизация	(2 219 929)	-	(41 880)	(2 261 809)
Реклассификация в НМА, прошедшие стадию разработки	-	-	-	-
Выбытие НМА	-	-	(29 029)	(29 029)
Списание амортизации	-	-	14 597	14 597
Остаточная стоимость на 31 декабря 2025 года	**17 522 968**	**8 586 655**	**142 165**	**26 251 788**
Первоначальная стоимость на 31 декабря 2025года	**23 311 494**	**8 586 655**	**200 380**	**32 098 529**
Накопленная амортизация на 31 декабря 2025 года	**(5 788 526)**	**-**	**(58 215)**	**(5 846 741)**

Нематериальные активы, созданные Группой, включают продукты следующих видов:

1) Системы мониторинга событий информационной безопасности

Продукты Группы, которые обеспечивают процесс проверки событий безопасности, получаемых от различных источников в режиме реального времени. Источниками событий могут быть антивирусные системы, журналы операционных систем, сканеры анализа защищенности инфраструктуры, сетевое оборудование и другие источники, расположенные в инфраструктуре организации.

Группа имеет следующие продукты для мониторинга событий информационной безопасности:

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

- MaxPatrol SIEM - программное обеспечение, предназначенное для мониторинга событий безопасности и автоматического выявления хакерских атак;
- PT Application Firewall - современное решение для защиты веб-приложений от известных и неизвестных атак, включая OWASP Top 10, автоматизированные атаки, атаки на стороне клиента и атаки нулевого дня. В 2015 и 2016 году продукт вошел в рейтинг аналитического агентства Gartner – Magic Quadrant for Web Application Firewalls (магический квадрант Гартнера для межсетевых экранов прикладного уровня) как «визионер» рынка на мировом уровне;
- PT Application Firewall PRO – обновленная архитектура классического PT Application Firewall, которая даёт возможности установки в распределенной инфраструктуре и гибкого масштабирования под любую нагрузку, использующая инструменты глубокого машинного обучения;
- PT Cybersecurity Intelligence - платформа для управления знаниями об угрозах, автоматически нормализующая и обогащающая индикаторы компрометации для выявления массовых, целенаправленных и отраслевых атак;
- Sandbox - передовая песочница, позволяющая защищать компанию от целевых и массовых атак с применением современного вредоносного ПО;
- PT NGFW — межсетевой экран для защиты корпоративной сети передачи данных, относится к классу межсетевых экранов нового поколения, предлагающих расширенные возможности для фильтрации трафика;
- PT Incident Processing Center – мониторинговая система информационных ресурсов, взаимодействующая с клиентами по обнаруженным инцидентам для передачи инструкции для оперативного реагирования;
- PT NAD - система глубокого анализа сетевого трафика (NTA) для выявления атак на периметре и внутри сети;
- PT Industrial Security Incident Manager - система управления инцидентами кибербезопасности АСУ ТП;
- ГТ Ведомственный центр - продукт, который автоматизирует процесс обработки инцидентов и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и другие отраслевые CERT;
- Прочие продукты.

В таблице ниже приведено изменение стоимости нематериальных активов, входящих в данную группу:

в тыс. российских рублей	Нематериальные активы, прошедшие стадию разработки	Нематериальные активы, находящиеся на стадии разработки
Остаточная стоимость на 1 января 2024 года	**4 155 573**	**465 053**
Первоначальная стоимость на 1 января 2024 года	**5 642 806**	**465 053**
Накопленная амортизация на 1 января 2024 года	**(1 487 233)**	**-**
Поступления	6 822 394	2 732 680
Начисленная амортизация	(899 710)	-
Реклассификация в НМА, прошедшие стадию разработки	214 831	(214 831)

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	Нематериальные активы, прошедшие стадию разработки	Нематериальные активы, находящиеся на стадии разработки
Остаточная стоимость на 31 декабря 2024 года	**10 293 088**	**2 982 902**
Первоначальная стоимость на 31 декабря 2024 года	**12 680 031**	**2 982 902**
Накопленная амортизация на 31 декабря 2024 года	**(2 386 943)**	**-**
Поступления	2 291 044	1 495 754
Начисленная амортизация	(1 489 384)	-
Остаточная стоимость на 31 декабря 2025 года	**11 094 748**	**4 478 656**
Первоначальная стоимость на 31 декабря 2025 года	**14 971 075**	**4 478 656**
Накопленная амортизация на 31 декабря 2025 года	**(3 876 327)**	**-**

Остаточный срок полезного использования таких продуктов на 31 декабря 2025 года находится в диапазоне от 2 до 10 лет, на 31 декабря 2024 года – от 2 до 10 лет.

2) Системы для анализа защищенности информационных систем

Продукты Группы, которые обеспечивают процесс проверки инфраструктуры организации на наличие возможных уязвимостей сетевого периметра, виртуальной инфраструктуры, вызванных в том числе ошибками конфигурации, а также программного обеспечения и исходного кода приложений. При анализе защищенности проверяется безопасность различных информационных систем, как внутренних, так и внешних.

Группа имеет следующие продукты данного класса:

- MaxPatrol 8 - система контроля уязвимостей и соответствия стандартам. Признана продуктом года в категории Vulnerability Management (Вулнерабилити Менеджмент) на церемонии вручения британской премии Cyber Security Awards в 2016 году;
- MultiScanner - многопоточная система выявления вредоносного контента;
- MaxPatrol VM – система для управления уязвимостями, позволяющая ранжировать потенциальные угрозы по уровню их опасности для бизнес-процессов;
- XSpider - сканер безопасности;
- PT Application Inspector - инструмент для выявления уязвимостей и ошибок в приложениях, поддерживающий процесс безопасной разработки;
- Прочие продукты.

В таблице ниже приведено изменение стоимости нематериальных активов, входящих в данную группу:

в тыс. российских рублей	Нематериальные активы, прошедшие стадию разработки	Нематериальные активы, находящиеся на стадии разработки
Остаточная стоимость на 1 января 2024 года	**1 418 267**	**156 865**
Первоначальная стоимость на 1 января 2024 года	**2 160 246**	**156 865**
Накопленная амортизация на 1 января 2024 года	**(741 979)**	**-**
Поступления	2 685 573	448 501
Начисленная амортизация	(266 527)	-

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	Нематериальные активы, прошедшие стадию разработки	Нематериальные активы, находящиеся на стадии разработки
Реклассификация в НМА, прошедшие стадию разработки	58 332	(58 332)
Остаточная стоимость на 31 декабря 2024 года	**3 895 645**	**547 034**
Первоначальная стоимость на 31 декабря 2024 года	**4 904 151**	**547 034**
Накопленная амортизация на 31 декабря 2024 года	**(1 008 506)**	**-**
Поступления	808 642	631 535
Начисленная амортизация	(504 369)	-
Остаточная стоимость на 31 декабря 2025 года	**4 199 918**	**1 178 569**
Первоначальная стоимость на 31 декабря 2025 года	**5 712 793**	**1 178 569**
Накопленная амортизация на 31 декабря 2025 года	**(1 512 875)**	**-**

Остаточный срок полезного использования таких продуктов на 31 декабря 2025 года находится в диапазоне от 3 до 6 лет, на 31 декабря 2024 года – от 3 до 6 лет.

3) Метапродукты

Метапродукты представлены продуктами Группы, которые образуют систему защиты, сфокусированную на невозможности реализовать недопустимые последствия и работающую полностью в автоматическом режиме.

Группа имеет следующие продукты данного класса:

- O2 – платформа, выполняющая роль центра мониторинга ИБ 24/7 в автоматическом режиме и останавливает хакера до наступления недопустимых для бизнеса последствий;
- Carbon – система, анализирующая возможные сценарии атак на компанию, формирует и контролирует выполнение требований к IT-инфраструктуре, которые не позволят злоумышленнику добраться до критически важных активов или существенно усложнят его путь.

В таблице ниже приведено изменение стоимости нематериальных активов, входящих в данную группу:

в тыс. российских рублей	Нематериальные активы, находящиеся на стадии разработки
Первоначальная стоимость на 1 января 2024 года	**657 289**
Накопленная амортизация на 1 января 2024 года	**-**
Остаточная стоимость на 1 января 2024 года	**657 289**
Поступления	1 327 267
Остаточная стоимость на 31 декабря 2024 года	**1 984 556**
Первоначальная стоимость на 31 декабря 2024 года	**1 984 556**
Накопленная амортизация на 31 декабря 2024 года	**-**
Поступления	797 578
Остаточная стоимость на 31 декабря 2025 года	**2 782 134**
Первоначальная стоимость на 31 декабря 2025 года	**2 782 134**
Накопленная амортизация на 31 декабря 2025 года	**-**

4) Прочие решения Группы

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Группа имеет следующие продукты данного класса:

- PT Standoff Cyber Polygon – это виртуальная копия нашего мира, в которой воссозданы производственные цепочки, бизнес-сценарии и технологический ландшафт, характерные для различных отраслей экономики, где исследователи безопасности смогут исследовать прототипы потенциальных уязвимостей;
- Прочие продукты.

В таблице ниже приведено изменение стоимости нематериальных активов, входящих в данную группу:

в тыс. российских рублей	Нематериальные активы, прошедшие стадию разработки	Нематериальные активы, находящиеся на стадии разработки
Первоначальная стоимость на 1 января 2024 года	**651 551**	-
Накопленная амортизация на 1 января 2024 года	**(60 190)**	-
Остаточная стоимость на 1 января 2024 года	**591 361**	-
Поступления	931 658	254 105
Начисленная амортизация	(112 958)	-
Реклассификация в НМА, прошедшие стадию разработки	2 122	(2 122)
Выбытие НМА	-	-
Списание амортизации	-	-
Обесценение НМА	-	-
Остаточная стоимость на 31 декабря 2024 года	**1 412 183**	**251 983**
Первоначальная стоимость на 31 декабря 2024 года	**1 585 331**	**251 983**
Накопленная амортизация на 31 декабря 2024 года	**(173 148)**	-
Поступления	652 064	285 544
Начисленная амортизация	(226 176)	-
Остаточная стоимость на 31 декабря 2025 года	**1 838 071**	**537 527**
Первоначальная стоимость на 31 декабря 2025 года	**2 237 395**	**537 527**
Накопленная амортизация на 31 декабря 2025 года	**(399 324)**	-

На отчетную дату Группа проводит тестирование на обесценение нематериальных активов, находящихся на стадии разработки, а также нематериальных активов, по которым на отчетную дату осуществляется существенная доработка. По состоянию на 31 декабря 2025 и 2024 гг. руководство проверило нематериальные активы, созданные Группой, на предмет возможного обесценения. По состоянию на 31 декабря 2025 года и 31 декабря 2024 года признаков обесценения выявлено не было.

Для тестирования на предмет обесценения Группа определила возмещаемую стоимость каждого отдельного программного продукта Группы. В этих расчетах используются прогнозы движения денежных средств, основанные на финансовом прогнозе, утвержденном руководством на следующий финансовый год, и с учетом реализации долгосрочного прогноза. Денежный поток от выручки рассчитывается исходя из темпов роста ИТ-рынка аналогичных продуктов Группы в России. Сроки прогноза, используемые в моделях и охватывающие 5-7 лет, приведены до точки безубыточности программного продукта, которые могут быть меньше расчетного срока полезного использования актива. Допущения, используемые для расчета денежных потоков от продуктов Группы, основаны на прогнозируемых доходах, операционных расходах и других соответствующих факторах, включая сумму капитальных затрат.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Ставка дисконтирования до налогообложения, применяемая к прогнозам денежных потоков в зависимости от стадии их разработки, колеблется от 20% до 26%.

Руководство считает, что любое разумно возможное изменение ключевых допущений, описанных выше, не приведет к превышению балансовой стоимости активов над их возмещаемой стоимостью. Оценки будущих дисконтированных денежных потоков и результаты тестирования на предмет обесценения нематериальных активов, созданных Группой, отличаются особой чувствительностью в следующих областях:

- снижение будущего запланированного объема продаж. По оценкам Группы, повышение данного фактора на 5% не приведет к обесценению;
- повышение ставки дисконтирования. По оценкам Группы, повышение данного фактора на 1% не приведет к обесценению;
- повышение будущего запланированного объёма административных и коммерческих расходов. По оценкам Группы, повышение данного фактора на 5% не приведет к обесценению.

В 2025 году следующие расходы были капитализированы как нематериальные активы: расходы на персонал – 5 077 106 тыс. рублей (2024: 13 945 031 тыс. рублей); профессиональные услуги – 136 906 тыс. рублей (2024: 310 517 тыс. рублей).

Капитализированные затраты по займам в 2025 году составляют 1 619 647 тысяч рублей (в 2024: 823 384 тыс. рублей). Эффективная ставка капитализации затрат по займам составила 20,2% в 2025 году (2024: 16,2%).

По результатам 2025 года Группа произвела справедливую оценку нематериальных активов доходным методом, которая была подтверждена независимым оценщиком. МСФО стандарты не позволяют признавать нематериальные активы, по которым отсутствует активный рынок, по переоцененной стоимости. Однако, учитывая, что продукты, созданные группой, имеют высокую маржинальность, и их оценка по затратному методу не отражает реальную суть бизнеса, справедливая оценка таких продуктов является важным управленческим показателем. Произведенная оценка справедливой стоимости нематериальных активов позволяет заключить, что возмещаемая стоимость значительно превышает их балансовую стоимость.

	31 декабря 2025 года		31 декабря 2024 года	
в тыс. российских рублей	Остаточная стоимость нематериальных активов, созданных Группой (МСФО оценка)	Справедливая стоимость нематериальных активов, созданных Группой (экспертная оценка)	Остаточная стоимость нематериальных активов, созданных Группой (МСФО оценка)	Справедливая стоимость нематериальных активов, созданных Группой (экспертная оценка)
Продукты, которые активно продаются на рынке либо по которым прошел ряд успешных пилотов	17 287 770	70 400 000	15 960 641	69 000 000
Прочие продукты	8 964 018	Не оценивались	5 496 576	Не оценивались

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

14. Запасы

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Товарно-материальные ценности	1 662 724	559 929
Прочее	11 882	2 486
Итого запасы	**1 674 606**	**562 415**

15. Торговая и прочая дебиторская задолженность

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Торговая дебиторская задолженность	23 802 726	18 206 736
Резерв под ожидаемые кредитные убытки	(9 781)	(13 292)
Итого финансовая торговая дебиторская задолженность, нетто	***23 792 945***	***18 193 444***
Авансы выданные	249 072	827 683
НДС к возмещению	43 426	26 517
Переплаты по налогам	1 109	10 974
Прочая дебиторская задолженность	78 555	76 438
Резерв под ожидаемые кредитные убытки	(11 850)	-
Итого нефинансовая торговая и прочая дебиторская задолженность, нетто	***360 312***	***941 612***
Итого	**24 153 257**	**19 135 056**

В таблице ниже представлена торговая дебиторская задолженность по срокам возникновения:

	31 декабря 2025 года		31 декабря 2024 года	
в тыс. российских рублей	Торговая дебиторская задолженность	Резерв под ожидаемые кредитные убытки	Торговая дебиторская задолженность	Резерв под ожидаемые кредитные убытки
Не просроченная	23 528 713	-	18 015 281	-
Просроченная менее 30 дней	263 683	-	138 213	-
Просроченная 30 – 90 дней	90	-	12 861	-
Просроченная более 90 дней	10 240	(9 781)	40 381	(13 292)
Итого	**23 802 726**	**(9 781)**	**18 206 736**	**(13 292)**

В следующей таблице поясняются изменения резерва под ожидаемые кредитные убытки по торговой и прочей дебиторской задолженности в рамках упрощенной модели ожидаемых кредитных убытков между началом и концом отчетного периода:

в тыс. российских рублей	Итого резерв под ожидаемые кредитные убытки
На 1 января 2024 года	**12 174**
Начисленный за период резерв под ожидаемые кредитные убытки	2 552
Восстановленный за период резерв под ожидаемые кредитные убытки	(1 434)
На 31 декабря 2024 года	**13 292**
На 1 января 2025 года	**13 292**
Начисленный за период резерв под ожидаемые кредитные убытки	14 757

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	Итого резерв под ожидаемые кредитные убытки
На 1 января 2024 года	**12 174**
Восстановленный за период резерв под ожидаемые кредитные убытки	(6 417)
На 31 декабря 2025 года	**21 632**

16. Денежные средства и их эквиваленты

в тыс. российских рублей	Рубли	Доллары США	Евро	Прочее	31 декабря 2025 года
Наличные денежные средства и остатки на счетах в банках	179 481	-	-	276	**179 757**
Депозиты	2 573 790	-	-	25 581	**2 599 371**
Итого денежные средства и их эквиваленты	**2 753 271**	**-**	**-**	**25 857**	**2 779 128**

в тыс. российских рублей	Рубли	Доллары США	Евро	Прочее	31 декабря 2024 года
Наличные денежные средства и остатки на счетах в банках	457 471	-	-	314	**457 785**
Депозиты	5 750 000	-	-	17 382	**5 767 382**
Итого денежные средства и их эквиваленты	**6 207 471**	**-**	**-**	**17 696**	**6 225 167**

Все остатки на банковских счетах и депозиты не являются просроченными или обесцененными. В таблице ниже представлены данные по остаткам на счетах в банках и банковских депозитов в разрезе кредитного качества:

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Рейтинг от AAA	14 354	6 141 362
Рейтинг от AA- до AA+	2 710 884	64 492
Рейтинг от A- до A+	-	1 617
Прочее	53 890	17 696
Итого	**2 779 128**	**6 225 167**

Указанный выше анализ сделан на основе кредитных рейтингов, присвоенных независимыми рейтинговыми агентствами Эксперт РА и АКРА.

По состоянию на 31 декабря 2025 года, 31 декабря 2024 года все денежные средства и их эквиваленты отнесены к Стадии 1 по кредитному качеству и подвержены минимальному кредитному риску в соответствии с МСФО (IFRS) 9. Сумма резерва под ожидаемые кредитные убытки по состоянию на 31 декабря 2025, 31 декабря 2024 незначительна и не была отражена в настоящей раскрываемой консолидированной финансовой отчетности.

17. Финансовые активы

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Долгосрочные финансовые активы		
Займы, выданные связанным сторонам	2 040 692	1 702 400

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Прочие финансовые активы	85 717	-
Итого долгосрочные финансовые активы	**2 126 409**	**1 702 400**

18. Капитал и резервы

По состоянию на 31 декабря 2025 и 31 декабря 2024 гг. уставный капитал представлен капиталом материнской компании ПАО «Группа Позитив».

Общее количество разрешенных к выпуску обыкновенных акций на 31 декабря 2025 и 31 декабря 2024 составляет 71 214 000 акций с номинальной стоимостью 0,5 рублей за акцию.

На 31 декабря 2024 года Группа создала резерв по платежам, основанным на акциях, в соответствии с Программой стимулирования роста на общую сумму 10 041 948 тыс. руб. (5 180 000 шт. по рыночной цене 1 938,6 руб. за 1 акцию на дату утверждения программы) под будущую выдачу акций сотрудникам и прочим сторонам.

На 31 декабря 2024 года часть акций была передана получателям (1 292 557 шт. по рыночной цене 1 938,6 руб. за 1 акцию на дату утверждения приказа), вследствие чего резерв по платежам, основанным на акциях, был уменьшен на 2 505 751 тыс. руб. На 31 декабря 2025 года вся сумма была передана получателям в сумме 10 041 948 тыс. руб. (5 180 000 шт. по рыночной цене 1 938,6 руб. за 1 акцию на дату утверждения программы), вследствие чего был использован весь резерв по платежам, основанным на акциях.

19. Кредиты и займы

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Долгосрочные обязательства		
Выпущенные необеспеченные облигации	14 889 553	9 729 055
Обязательства по аренде (Примечание 22)	469 316	597 613
	15 358 869	**10 326 668**
Краткосрочные обязательства		
Обеспеченные банковские кредиты	3 048 042	9 964 582
Обязательства по цифровым финансовым активам	405 836	-
Займы, полученные от связанных сторон	-	3 160 434
Обязательства по аренде (Примечание 22)	294 175	317 825
Выпущенные необеспеченные облигации	4 903 308	2 579 316
	8 651 361	**16 022 157**
Итого	**24 010 230**	**26 348 825**

Вид	Процентная ставка	Срок погашения	Задолженность на 31 декабря 2025 года
Выпущенные необеспеченные облигации с фиксированной процентной ставкой	18%	2028	10 034 514
Выпущенные необеспеченные облигации с плавающей процентной ставкой	Ключевая ставка ЦБ РФ + 1,7%-4%	2026-2027	9 758 347
Обязательства по цифровым финансовым активам	17,75%	2026	405 836

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Обеспеченные банковские кредиты с плавающей процентной ставкой	Ключевая ставка ЦБ РФ + 1,4%-2,95%	2026	3 048 042
Обязательства по аренде (Примечание 22)	8,63–21,1%	2026-2030	763 491
Итого			**24 010 230**

Вид	Процентная ставка	Срок погашения	Задолженность на 31 декабря 2024 года
Выпущенные необеспеченные облигации	10,55%	2025	2 519 514
Выпущенные необеспеченные облигации	Ключевая ставка ЦБ РФ + 1,7%-4%	2026-2027	9 788 857
Необеспеченные займы	Ключевая ставка+2,65%	2028	3 160 434
Обеспеченные банковские кредиты с плавающей процентной ставкой	Ключевая ставка ЦБ РФ + 1,4%-2,97%	2025	6 691 491
Обеспеченные банковские кредиты с фиксированной процентной ставкой	19,7%-19,9%	2025	3 273 091
Обязательства по аренде (Примечание 22)	8,63–21,1%	2025-2030	915 438
Итого			**26 348 825**

Облигации обращаются на фондовом рынке ММВБ. Внешнее краткосрочное финансирование привлекается Группой с целью поддержание ликвидности ввиду сезонного характера основной выручки и денежного потока от нее.

Банковские кредиты обеспечены поручительствами связанных сторон и дочерних компаний.

Выпущенные Группой цифровые финансовые активы (ЦФА) удостоверяют права их держателей на получение денежных средств от Группы в установленном объеме и в предусмотренные сроки. Остаток обязательств по выпущенным ЦФА на отчетную дату отражает сумму задолженности Группы перед инвесторами по таким инструментам.

В таблице ниже представлены движения обязательств по финансовой деятельности в течение 2024 и 2025 годов:

в тыс. российских рублей	Кредиты и займы	Обязательства по аренде	Выпущенные облигации	Обязательства по цифровым финансовым активам	Итого
Обязательства по финансовой деятельности на 1 января 2025 года	**13 125 016**	**915 438**	**12 379 316**	**-**	**26 419 770**
Денежные потоки	***(11 602 579)***	***(328 885)***	***4 062 891***	***400 000***	***(7 468 573)***
Получение кредитов и займов	3 043 000	-	9 905 000	400 000	**13 348 000**
Погашение основного долга	(12 944 181)	(201 443)	(2 298 557)	-	**(15 444 181)**
Погашение процентов	(1 701 398)	(127 442)	(3 543 552)	-	**(5 372 392)**

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	Кредиты и займы	Обязательства по аренде	Выпущенные облигации	Обязательства по цифровым финансовым активам	Итого
Неденежные изменения	*1 525 605*	*176 938*	*3 350 654*	*5 836*	*5 059 033*
Начисление процентов	1 525 605	127 397	3 350 654	5 836	5 009 492
Новые договоры аренды	-	17 055	-		17 055
Выбытие договоров аренды	-	(30 053)	-	-	(30 053)
Модификации договоров аренды	-	62 539	-	-	62 539
Обязательства по финансовой деятельности на 31 декабря 2025 года	**3 048 042**	**763 491**	**19 792 861**	**405 836**	**24 010 230**

в тыс. российских рублей	Кредиты и займы	Обязательства по аренде	Выпущенные облигации	Итого
Обязательства по финансовой деятельности на 1 января 2024 года	**2 525 924**	**633 058**	**2 518 090**	**5 677 072**
Денежные потоки	*9 421 245*	*(292 408)*	*9 039 130*	*18 167 967*
Получение кредитов и займов	16 744 181	-	9 726 030	26 470 211
Погашение основного долга	(6 300 000)	(209 276)	-	(6 509 276)
Погашение процентов	(1 022 936)	(83 132)	(686 900)	(1 792 968)
Неденежные изменения	*1 177 847*	*574 788*	*751 151*	*2 503 786*
Начисление процентов	1 177 847	83 132	751 151	2 012 130
Новые договоры аренды	-	95 381	-	95 381
Модификации договоров аренды	-	396 275	-	396 275
Обязательства по финансовой деятельности на 31 декабря 2024 года	**13 125 016**	**915 438**	**12 308 371**	**26 348 825**

20. Обязательства по договорам с покупателями

На 1 января 2024 года	**4 464 483**
Отражено в отчете о прибыли или убытке в течение отчетного года	(3 284 427)
Отнесено на будущие периоды в течение отчетного года	3 450 869
На 31 декабря 2024 года	**4 630 925**
На 1 января 2025 года	**4 630 925**
Отражено в отчете о прибыли или убытке в течение отчетного года	(3 347 247)
Отнесено на будущие периоды в течение отчетного года	4 993 167
На 31 декабря 2025 года	**6 276 845**

21. Торговая и прочая кредиторская задолженность

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Резервы по заработной плате	2 821 428	2 025 568
Прочая кредиторская задолженность	659 461	401 380

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	31 декабря 2025 года	31 декабря 2024 года
Торговая кредиторская задолженность	629 343	787 225
Налоги к уплате	583 958	362 760
Кредиторская задолженность по текущей заработной плате, включая соответствующие налоги	414 819	540 150
Авансы полученные	156 748	61 071
Итого краткосрочная кредиторская задолженность	*5 265 757*	*4 178 154*
Долгосрочная кредиторская задолженность	-	-
Итого долгосрочная кредиторская задолженность	-	-
Итого торговая и прочая кредиторская задолженность	**5 265 757**	**4 178 154**

22. Аренда

Группа выступает в качестве арендатора по договорам аренды офисных помещений.

Следующая арендуемая недвижимость является существенной для Группы:

- офисные помещения, расположенные по адресу: г. Москва, Преображенская площадь, 8;
- складские помещения, расположенные по адресу: г. Москва, ул. Электрозаводская, 24;
- офис, расположенный по адресу: г. Санкт-Петербург, ул. Итальянская, 17.

Срок аренды прямо устанавливается в договорах аренды без опционов на продление либо досрочное расторжение. Срок истечения договоров аренды варьируется от 2025 до 2028 года. Будущие арендные платежи были дисконтированы по ставке 8,63 – 21,1% в 2025 году, 8,63 – 13,77% – в 2024 году.

Группа также имеет договоры аренды офисных и складских помещений на срок до 12 месяцев. Группа применяет освобождение от признания «краткосрочной аренды» для этих договоров аренды.

Движение активов в форме права пользования в течение 2024 – 2025 гг. представлено в рамках раскрытия по Основным средствам в Примечании 12.

Обязательства по аренде:

в тыс. российских рублей	2024 год
На 1 января 2024 года	**633 058**
Поступления	95 381
Модификация договоров аренды	396 275
Выкуп лизингового оборудования	-
Платежи	(292 408)
Начисление процентов	83 132
На 31 декабря 2024 года	**915 438**
в том числе:	
Долгосрочные обязательства по аренде	*597 613*
Краткосрочные обязательства по аренде	*317 825*

в тыс. российских рублей	2025 год
На 1 января 2025 года	**915 438**
Поступления	17 055

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

в тыс. российских рублей	2025 год
На 1 января 2025 года	**915 438**
Выбытие	(30 053)
Модификация договоров аренды	62 539
Платежи	(328 885)
Начисление процентов	127 397
На 31 декабря 2025 года	**763 491**
в том числе:	
Долгосрочные обязательства по аренде	*469 316*
Краткосрочные обязательства по аренде	*294 175*

Анализ сроков погашения обязательств по аренде представлен в Примечании 3.

23. Условные обязательства

Условия ведения операционной деятельности Группы

Большая часть операций Группы происходит в России. Россия продолжает экономические реформы и развитие своей правовой, налоговой и нормативной базы в соответствии с требованиями рыночной экономики. Будущая стабильность российской экономики во многом зависит от этих реформ и изменений, а также от эффективности экономических, финансовых и монетарных мер, предпринимаемых правительством.

Начиная с февраля 2022 года произошел рост геополитической напряженности в связи с обострением конфликта вокруг Украины, создавший существенные риски для экономики РФ и приведший к значительным колебаниям курсов валют и снижению стоимости российских активов на финансовых рынках, снижению суверенного рейтинга России, расширению санкций со стороны США, стран ЕС и ряда других стран в отношении физических и юридических лиц в Российской Федерации. Введенные экономические санкции предусматривают в том числе частичное блокирование золотовалютных резервов ЦБ РФ, ограничение доступа РФ к мировому рынку капитала, ограничение на совершение инвестиций и расчетов в долларах США и Евро, отключение работы системы SWIFT для отдельных российских банков, ограничение на проведение операций с международными клиринговыми организациями, вызывающие разрушение устоявшихся платежных цепочек, возникновение затруднений с платежами в долларах США и Евро, неплатежи (задержки плановых платежей) по ценным бумагам.

В ответ на указанные риски и санкции Правительство Российской Федерации и Банк России приняли комплекс стабилизационных мер для обеспечения макроэкономической устойчивости и стабильности экономики и финансовой системы РФ, в том числе временное введение запретов на ряд операций с нерезидентами и расчеты в долларах США и Евро, повышение ключевой ставки ЦБ РФ, введение обязательной продажи валютной выручки, временную приостановку биржевых торгов, ограничение раскрытия определенной статистической информации о макроэкономических показателях, а также финансовой и нефинансовой информации организаций.

Банк России в целях стабилизации экономической ситуации и снижения инфляционного давления на экономику неоднократно пересматривал в 2024 году величину ключевой ставки. Ключевая ставка ЦБ РФ на начало года составляла 21%, на 31.12.2025 года ключевая ставка ЦБ РФ составляла 16%.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Руководство Группы не в состоянии предвидеть все возможные изменения, способные оказать влияние на российскую экономику, и соответственно, эффект на будущее финансовое положение Группы. Однако руководство Группы считает нужным отметить несколько важных факторов:

1. ПАО «Группа Позитив» разместило свои акции на Московской бирже и не зависит от иностранного капитала. Модель размещения акций на бирже была изначально ориентирована на российских физических лиц. ПАО «Группа Позитив» – единственная публичная технологическая компания из сектора кибербезопасности в РФ. На конец отчетного периода среди инвесторов уже около 200 000 российских физических лиц. В текущей ситуации акции компании становятся сильным защитным активом с перспективой роста.

2. Подавляющая часть клиентов компаний Группы – российские организации. Доля выручки Группы за счет нерезидентов РФ составила около 1%. Таким образом, компания не имеет риска потери клиентов и выручки, а имеет достаточный уровень стабильности даже в сложившейся ситуации.

3. Росту спроса на решения, обеспечивающие кибербезопасность, способствуют следующие факторы:

- наблюдается значительный рост числа кибератак на органы власти, бизнес и промышленные объекты экономики РФ;
- с 31 марта 2022 запрещена закупка зарубежного программного обеспечения для использования на значимых объектах критической информационной инфраструктуры, а с 1 января 2025 года запрещается использование зарубежного программного обеспечения на таких объектах;
- вводится ответственность первых лиц организаций за обеспечение их информационной безопасности.

Налогообложение

Российское налоговое, валютное и таможенное законодательство, которое было принято или, по существу, вступило в силу на конец отчетного периода, допускает возможность неоднозначных толкований в применении к операциям и деятельности Группы.

Следовательно, интерпретация руководством законодательства, применимого к операциям и деятельности Группы, и официальная документация, подтверждающая налоговые позиции, могут быть оспорены налоговыми органами. Налоговое администрирование в России постепенно укрепляется, в том числе повышается риск проверки налоговых операций без четкой деловой цели или с контрагентами, не соблюдающими налоговые правила. Финансовые периоды остаются открытыми для проверки властями в отношении налогов в течение трех календарных лет, предшествующих году, когда было принято решение о проверке. При определенных обстоятельствах обзоры могут охватывать более длительные периоды времени.

Существует вероятность, что регулирующие органы в области трудового законодательства могут оспорить методы бухгалтерского учета, которые они никогда раньше не оспаривали. Таким образом, могут быть начислены значительные дополнительные штрафы и обязательства. Невозможно определить суммы претензий по претензиям, которые могли быть, но на самом деле не были поданы, или оценить вероятности неблагоприятного исхода. Иски по вопросам, которые не были поданы, могут быть предъявлены независимо от срока их давности.

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Эти изменения и последние тенденции в применении и толковании некоторых положений российского налогового законодательства указывают на то, что налоговые органы могут занять более жесткую позицию в своем толковании этого законодательства и проверке налоговых деклараций. Следовательно, существует вероятность, что операции и методы бухгалтерского учета, которые не оспаривались в прошлом, могут быть оспорены в будущем.

Руководство считает, что Группа в значительной степени соблюдает налоговое и иное законодательство, регулирующее ее деятельность в России и других налоговых юрисдикциях. Однако остается риск того, что соответствующие органы могут занять разные позиции в отношении вопросов толкования, или что судебная практика может негативно повлиять на позиции, занятые Группой, и влияние на финансовое положение Группы, если регулирующим органам удастся отстоять свою позицию, может быть значительным.

24. Связанные стороны

В ходе обычной деятельности Группа заключает сделки со связанными сторонами по продаже товаров и услуг, а также в связи с заключением соглашений о финансировании с компаниями Группы. Операции со связанными сторонами обычно совершаются на стандартных коммерческих принципах.

Остатки по операциям со связанными сторонами по состоянию на 31 декабря 2025 года и 31 декабря 2024 года представлены ниже:

Займы выданные

в тыс. российских рублей	31.12.2025		31.12.2024	
	Основной долг с учетом капитализированных процентов	**Проценты**	**Основной долг с учетом капитализированных процентов**	**Проценты**
Займы выданные	2 034 372	6 320	1 702 400	24 457
	2 034 372	**6 320**	**1 702 400**	**24 457**

Займы полученные

в тыс. российских рублей	31.12.2025		31.12.2024	
	Основной долг	**Проценты**	**Основной долг**	**Проценты**
Займы полученные	-	-	(3 144 181)	(16 254)
	-	**-**	**(3 144 181)**	**(16 254)**

Информация по изменению балансовой величины займов, выданных и полученных от связанных сторон, представлена ниже:

в тыс. российских рублей	**2025 год**	**2024 год**
На 1 января 2025 года	**1 433 578**	**-**
Денежные потоки:		
Займы выданные		
Выдано займов	-	(1 702 400)
Возвращено займов	80 766	-

Примечания к раскрываемой консолидированной финансовой отчетности за год, закончившийся 31 декабря 2025 г.

Выплачено процентов	4 541	-
Займы полученные		
Получено займов	-	3 144 181
Возвращено займов	(3 144 181)	-
Выплачено процентов	(310 075)	(53 876)
Неденежные потоки:		
Начислено процентов по займам выданным	(399 142)	(24 457)
Начислено процентов по займам полученным	293 821	70 130
На 31 декабря 2025 года	**(2 040 692)**	**1 433 578**

Вознаграждения ключевому управленческому персоналу

К ключевому управленческому персоналу относятся ключевые руководители Группы и члены Совета директоров. За годы, закончившиеся 31 декабря 2025 и 2024 гг., общая сумма вознаграждения ключевому управленческому персоналу, включенная в общие и административные расходы, составила 590 110 тыс. руб. и 446 084 тыс. руб. соответственно, включая социальные взносы. По состоянию на 31 декабря 2025 и 2024 гг. задолженность перед ключевым управленческим персоналом составляет 97 810 тыс. руб. и 99 119 тыс. руб. соответственно.

25. События после отчетной даты

После отчетной даты Группа объявила о намерениях направить на выплату дивидендов в общей сумме 2 млрд руб. Окончательное решение будет принято после утверждения финансовых результатов. Обязательство по выплате дивидендов в настоящей отчетности на отчетную дату не признано.

ОТЧЕТ О СОБЛЮДЕНИИ ПРИНЦИПОВ И РЕКОМЕНДАЦИЙ КОДЕКСА КОРПОРАТИВНОГО УПРАВЛЕНИЯ

Настоящий отчет о соблюдении принципов и рекомендаций Кодекса корпоративного управления был рассмотрен Советом директоров публичного акционерного общества «Группа Позитив» (далее — **Общество**) на заседании 7 апреля 2026 года.

Совет директоров подтверждает, что приведенные в настоящем отчете данные содержат полную и достоверную информацию о соблюдении Обществом принципов и рекомендаций Кодекса корпоративного управления за 2025 отчетный год.

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
1.1	**Общество должно обеспечивать равное и справедливое отношение ко всем акционерам при реализации ими права на участие в управлении обществом**			
1.1.1	Общество создает для акционеров максимально благоприятные условия для участия в общем собрании, условия для выработки обоснованной позиции по вопросам повестки дня общего собрания, координации своих действий, а также возможность высказать свое мнение по рассматриваемым вопросам	1. Общество предоставляет доступный способ коммуникации с обществом, такой как горячая линия, электронная почта или форум в сети Интернет, позволяющий акционерам высказать свое мнение и направить вопросы в отношении повестки дня в процессе подготовки к проведению общего собрания. Указанные способы коммуникации были организованы обществом и предоставлены акционерам в ходе подготовки к проведению каждого общего собрания, прошедшего в отчетный период	Соблюдается	
1.1.2	Порядок сообщения о проведении общего собрания и предоставления материалов к общему собранию дает акционерам возможность надлежащим образом подготовиться к участию в нем	1. В отчетном периоде сообщение о проведении общего собрания акционеров размещено (опубликовано) на сайте общества в сети Интернет не позднее чем за 30 дней до даты проведения общего собрания, если законодательством не предусмотрен больший срок. 2. В сообщении о проведении собрания указаны документы, необходимые для допуска в помещение. 3. Акционерам был обеспечен доступ к информации о том, кем предложены вопросы повестки дня и кем выдвинуты кандидаты в совет директоров и ревизионную комиссию общества (в случае, если ее формирование предусмотрено уставом общества)	Соблюдается	
1.1.3	В ходе подготовки и проведения общего собрания акционеры имели возможность беспрепятственно и своевременно получать информацию о собрании и материалы к нему, задавать вопросы исполнительным органам и членам совета директоров общества, общаться друг с другом	1. В отчетном периоде акционерам была предоставлена возможность задать вопросы членам исполнительных органов и членам совета директоров общества в период подготовки к собранию и в ходе проведения общего собрания. 2. Позиция совета директоров (включая внесенные в протокол особые мнения (при наличии) по каждому вопросу повестки общих собраний, проведенных в отчетный период, была включена в состав материалов к общему собранию. 3. Общество предоставляло акционерам, имеющим на это право, доступ к списку лиц, имеющих право на участие в общем собрании, начиная с даты получения его обществом во всех случаях проведения общих собраний в отчетном периоде	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
1.1.4	Реализация права акционера требовать созыва общего собрания, выдвигать кандидатов в органы управления и вносить предложения для включения в повестку дня общего собрания не была сопряжена с неоправданными сложностями	1. Уставом общества установлен срок внесения акционерами предложений для включения в повестку дня годового общего собрания, составляющий не менее 60 дней после окончания соответствующего календарного года. 2. В отчетном периоде общество не отказывало в принятии предложений в повестку дня или кандидатов в органы общества по причине опечаток и иных несущественных недостатков в предложении акционера	Соблюдается	
1.1.5	Каждый акционер имел возможность беспрепятственно реализовать право голоса самым простым и удобным для него способом	1. Уставом общества предусмотрена возможность заполнения электронной формы бюллетеня на сайте в сети Интернет, адрес которого указан в сообщении о проведении общего собрания акционеров	Соблюдается	
1.1.6	Установленный обществом порядок ведения общего собрания обеспечивает равную возможность всем лицам, присутствующим на собрании, высказать свое мнение и задать интересующие их вопросы	1. При проведении в отчетном периоде общих собраний акционеров в форме собрания (совместного присутствия акционеров) предусматривалось достаточное время для докладов по вопросам повестки дня и время для обсуждения этих вопросов, акционерам была предоставлена возможность высказать свое мнение и задать интересующие их вопросы по повестке дня. 2. Обществом были приглашены кандидаты в органы управления и контроля общества и предприняты все необходимые меры для обеспечения их участия в общем собрании акционеров, на котором их кандидатуры были поставлены на голосование. Присутствовавшие на общем собрании акционеров кандидаты в органы управления и контроля общества были доступны для ответов на вопросы акционеров. 3. Единоличный исполнительный орган, лицо, ответственное за ведение бухгалтерского учета, председатель или иные члены комитета совета директоров по аудиту были доступны для ответов на вопросы акционеров на общих собраниях акционеров, проведенных в отчетном периоде. 4. В отчетном периоде общество использовало телекоммуникационные средства для обеспечения дистанционного доступа акционеров для участия в общих собраниях либо советом директоров было принято обоснованное решение об отсутствии необходимости (возможности) использования таких средств в отчетном периоде	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 соблюдается частично. В заседании годового Общего собрания акционеров Общества принимали участие два кандидата в члены Совета директоров Общества. Присутствовавшие на Общем собрании акционеров кандидаты в органы управления и контроля Общества были доступны для ответов на вопросы акционеров. В соответствии с Постановлением Правительства Российской Федерации от 04.07.2023 № 1102 информация о членах Совета директоров Общества публично не раскрывается. Генеральный директор Общества был избран в 2021 году на пять лет. Он регулярно участвует в онлайн- и офлайн-мероприятиях для акционеров и доступен для ответов на вопросы акционеров. Общество продолжит применять практику участия в Общих собраниях акционеров Общества кандидатов в органы управления и контроля Общества. Критерий 3 соблюдается частично. В годовом заседании Общего собрания акционеров Общества принимали участие Председатель Совета директоров Общества и представители топ-менеджмента Общества. Практика участия Генерального директора Общества, Главного бухгалтера Общества, членов комитета Совета директоров Общества и иных лиц не применялась. Генеральный директор Общества и топ-менеджмент Общества регулярно участвуют в онлайн- и офлайн-мероприятиях для акционеров и доступны для ответов на вопросы акционеров (с актуальным перечнем можно ознакомиться на странице «Календарь инвестора» на официальном сайте Общества в сети Интернет). Общество планирует продолжать применять практику участия в Общих собраниях акционеров Общества Генерального директора Общества и топ-менеджмента Общества в 2026 году. Критерий 4 соблюдается

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
1.2	**Акционерам предоставлена равная и справедливая возможность участвовать в прибыли общества посредством получения дивидендов**			
1.2.1	Общество разработало и внедрило прозрачный и понятный механизм определения размера дивидендов и их выплаты	1. Положение о дивидендной политике общества утверждено советом директоров и раскрыто на сайте общества в сети Интернет. 2. Если дивидендная политика общества, составляющего консолидированную финансовую отчетность, использует показатели отчетности общества для определения размера дивидендов, то соответствующие положения дивидендной политики учитывают консолидированные показатели финансовой отчетности. 3. Обоснование предлагаемого распределения чистой прибыли, в том числе на выплату дивидендов и собственные нужды общества, и оценка его соответствия принятой в обществе дивидендной политике, с пояснениями и экономическим обоснованием потребности в направлении определенной части чистой прибыли на собственные нужды в отчетном периоде были включены в состав материалов к общему собранию акционеров, в повестку дня которого включен вопрос о распределении прибыли (в том числе о выплате (объявлении) дивидендов)	Соблюдается	
1.2.2	Общество не принимает решение о выплате дивидендов, если такое решение, формально не нарушая ограничений, установленных законодательством, является экономически необоснованным и может привести к формированию ложных представлений о деятельности общества	1. В Положении о дивидендной политике общества, помимо ограничений, установленных законодательством, определены финансовые/экономические обстоятельства, при которых обществу не следует принимать решение о выплате дивидендов	Соблюдается	
1.2.3	Общество не допускает ухудшения дивидендных прав существующих акционеров	1. В отчетном периоде общество не предпринимало действий, ведущих к ухудшению дивидендных прав существующих акционеров	Соблюдается	
1.2.4	Общество стремится к исключению использования акционерами иных способов получения прибыли (дохода) за счет общества, помимо дивидендов и ликвидационной стоимости	1. В отчетном периоде иные способы получения лицами, контролирующими общество, прибыли (дохода) за счет общества, помимо дивидендов (например, с помощью трансфертного ценообразования, необоснованного оказания обществу контролирующим лицом услуг по завышенным ценам, путем замещающих дивиденды внутренних займов контролирующему лицу и (или) его подконтрольным лицам) не использовались	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
1.3	**Система и практика корпоративного управления обеспечивают равенство условий для всех акционеров — владельцев акций одной категории (типа), включая миноритарных (мелких) акционеров и иностранных акционеров, и равное отношение к ним со стороны общества**			
1.3.1	Общество создало условия для справедливого отношения к каждому акционеру со стороны органов управления и контролирующих лиц общества, в том числе условия, обеспечивающие недопустимость злоупотреблений со стороны крупных акционеров по отношению к миноритарным акционерам	1. В течение отчетного периода лица, контролирующие общество, не допускали злоупотреблений правами по отношению к акционерам общества, конфликты между контролирующими лицами общества и акционерами общества отсутствовали, а если таковые были, совет директоров уделил им надлежащее внимание	Соблюдается	
1.3.2	Общество не предпринимает действий, которые приводят или могут привести к искусственному перераспределению корпоративного контроля	1. Квазиказначейские акции отсутствуют или не участвовали в голосовании в течение отчетного периода	Соблюдается	
1.4	**Акционерам обеспечены надежные и эффективные способы учета прав на акции, а также возможность свободного и необременительного отчуждения принадлежащих им акций**			
1.4	Акционерам обеспечены надежные и эффективные способы учета прав на акции, а также возможность свободного и необременительного отчуждения принадлежащих им акций	1. Используемые регистратором общества технологии и условия оказываемых услуг соответствуют потребностям общества и его акционеров, обеспечивают учет прав на акции и реализацию прав акционеров наиболее эффективным образом	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.1	**Совет директоров осуществляет стратегическое управление обществом, определяет основные принципы и подходы к организации в обществе системы управления рисками и внутреннего контроля, контролирует деятельность исполнительных органов общества, а также реализует иные ключевые функции**			
2.1.1	Совет директоров отвечает за принятие решений, связанных с назначением и освобождением от занимаемых должностей исполнительных органов, в том числе в связи с ненадлежащим исполнением ими своих обязанностей. Совет директоров также осуществляет контроль за тем, чтобы исполнительные органы общества действовали в соответствии с утвержденными стратегией развития и основными направлениями деятельности общества	1. Совет директоров имеет закрепленные в уставе полномочия по назначению, освобождению от занимаемой должности и определению условий договоров в отношении членов исполнительных органов. 2. В отчетном периоде комитет по номинациям (назначениям, кадрам) рассмотрел вопрос о соответствии профессиональной квалификации, навыков и опыта членов исполнительных органов текущим и ожидаемым потребностям общества, продиктованным утвержденной стратегией общества. 3. В отчетном периоде советом директоров рассмотрен отчет (отчеты) единоличного исполнительного органа и коллегиального исполнительного органа (при наличии) о выполнении стратегии общества	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 не соблюдается. В Обществе не образован коллегиальный исполнительный орган. Генеральный директор Общества был избран в 2021 году сроком на пять лет. При рассмотрении результатов деятельности Общества у членов Совета директоров Общества не возникало вопросов о соответствии профессиональной квалификации, навыков и опыта Генерального директора Общества текущим потребностям Общества. В связи с этим соответствующий вопрос не выносился на рассмотрение Комитета по кадрам и вознаграждениям Совета директоров Общества. Вопрос о соответствии профессиональной квалификации, навыков и опыта Генерального директора Общества (кандидата на должность Генерального директора Общества) будет рассмотрен в 2026 году при истечении срока полномочий действующего Генерального директора Общества либо в случае поступления соответствующего запроса от членов Совета директоров Общества. Критерий 3 частично соблюдается. В Обществе не образован коллегиальный исполнительный орган. Совет директоров Общества не утверждал стратегию Общества в виде отдельного документа. Такое решение вызвано высокой скоростью изменения внешней среды в сфере информационных технологий — основной сферы деятельности Общества. Соответственно, в Обществе отсутствует практика формирования отчета Генерального директора о выполнении стратегии Общества. Перспективные задачи и цели Общества определяются и утверждаются Советом директоров Общества в рамках определения годового бюджета Общества. Исполнение перспективных задач и целей Общества контролируется Советом директоров Общества при утверждении годового отчета Общества, консолидированной финансовой отчетности Общества, а также при утверждении бюджета Общества на очередной год. Общество намерено внедрить практику отчетов Генерального директора Общества Совету директоров Общества о выполнении стратегии Общества, когда это будет соответствовать масштабам и целям деятельности Общества
2.1.2	Совет директоров устанавливает основные ориентиры деятельности общества на долгосрочную перспективу, оценивает и утверждает ключевые показатели деятельности и основные бизнес-цели общества, оценивает и одобряет стратегию и бизнес-планы по основным видам деятельности общества	1. В течение отчетного периода на заседаниях совета директоров были рассмотрены вопросы, связанные с ходом исполнения и актуализации стратегии, утверждением финансово-хозяйственного плана (бюджета) общества, а также рассмотрением критериев и показателей (в том числе промежуточных) реализации стратегии и бизнес-планов общества	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.1.3	Совет директоров определяет принципы и подходы к организации системы управления рисками и внутреннего контроля в обществе	1. Принципы и подходы к организации системы управления рисками и внутреннего контроля в обществе определены советом директоров и закреплены во внутренних документах общества, определяющих политику в области управления рисками и внутреннего контроля. 2. В отчетном периоде совет директоров утвердил (пересмотрел) приемлемую величину рисков (риск-аппетит) общества либо комитет по аудиту и (или) комитет по рискам (при наличии) рассмотрел целесообразность вынесения на рассмотрение совета директоров вопроса о пересмотре риск-аппетита общества	Соблюдается	
2.1.4	Совет директоров определяет политику общества по вознаграждению и (или) возмещению расходов (компенсаций) членам совета директоров, исполнительным органам общества и иным ключевым руководящим работникам общества	1. В обществе разработана, утверждена советом директоров и внедрена политика (политики) по вознаграждению и возмещению расходов (компенсаций) членов совета директоров, исполнительных органов общества и иных ключевых руководящих работников общества. 2. В течение отчетного периода советом директоров были рассмотрены вопросы, связанные с указанной политикой (политиками)	Частично соблюдается	Критерий 1 частично соблюдается. Общим собранием акционеров Общества утвержден порядок вознаграждения и возмещения расходов (компенсаций) членов Совета директоров Общества. Совет директоров Общества рассматривает вопросы об утверждении размера вознаграждения Генерального директора Общества, Корпоративного секретаря Общества, руководителя службы внутреннего аудита Общества. Кроме того, Совет директоров Общества контролирует вопросы, связанные с вознаграждением и возмещением расходов (компенсаций) Генерального директора Общества и иных ключевых руководящих работников Общества при утверждении годового бюджета Общества. Общество рассматривает возможность разработки и утверждения Советом директоров Общества единой политики по вознаграждению и возмещению расходов (компенсаций) ключевым руководящим работникам Общества. Критерий 2 частично соблюдается. В отчетном году Советом директоров Общества рассматривался и утверждался годовой бюджет Общества. В годовой бюджет Общества включены сведения о вознаграждениях и компенсациях членов Совета директоров Общества, Генерального директора Общества и иных ключевых работников Общества
2.1.5	Совет директоров играет ключевую роль в предупреждении, выявлении и урегулировании внутренних конфликтов между органами общества, акционерами общества и работниками общества	1. Совет директоров играет ключевую роль в предупреждении, выявлении и урегулировании внутренних конфликтов. 2. Общество создало систему идентификации сделок, связанных с конфликтом интересов, и систему мер, направленных на разрешение таких конфликтов	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.1.6	Совет директоров играет ключевую роль в обеспечении прозрачности общества, своевременности и полноты раскрытия обществом информации, необременительного доступа акционеров к документам общества	1. Во внутренних документах общества определены лица, ответственные за реализацию информационной политики	Частично соблюдается	Критерий 1 частично соблюдается. Акции Общества были допущены до торгов на Московской бирже в декабре 2021 года. К настоящему моменту информационная политика Общества в виде единого формализованного документа не утверждена. При этом в Положении о корпоративном секретаре Общества Корпоративный секретарь Общества определен в качестве ответственного лица за надлежащей организацией и эффективным функционированием системы раскрытия Обществом информации, а также за обеспечением доступа акционеров к информации Общества
2.1.7	Совет директоров осуществляет контроль за практикой корпоративного управления в обществе и играет ключевую роль в существенных корпоративных событиях общества	1. В течение отчетного периода совет директоров рассмотрел результаты самооценки и (или) внешней оценки практики корпоративного управления в обществе	Соблюдается	
2.2	**Совет директоров подотчетен акционерам общества**			
2.2.1	Информация о работе совета директоров раскрывается и предоставляется акционерам	1. Годовой отчет общества за отчетный период включает в себя информацию о посещаемости заседаний совета директоров и комитетов каждым из членов совета директоров. 2. Годовой отчет содержит информацию об основных результатах оценки (самооценки) качества работы совета директоров, проведенной в отчетном периоде	Частично соблюдается	Критерий 1 частично соблюдается. Общество было вынуждено ограничить публичный доступ к информации о членах Совета директоров Общества в соответствии с Постановлением Правительства Российской Федерации от 04.07.2023 № 1102. В связи с этим информация о посещаемости заседаний Совета директоров Общества раскрыта в Годовом отчете обезличенно. Общество рассмотрит возможность включения в годовой отчет Общества информации о посещаемости заседаний Совета директоров Общества и комитетов каждым из членов Совета директоров Общества после возобновления практики раскрытия информации о членах Совета директоров Общества. Критерий 2 соблюдается
2.2.2	Председатель совета директоров доступен для общения с акционерами общества	1. В обществе существует прозрачная процедура, обеспечивающая акционерам возможность направления председателю совета директоров (и, если применимо, старшему независимому директору) обращений и получения обратной связи по ним	Соблюдается	
2.3	**Совет директоров является эффективным и профессиональным органом управления общества, способным выносить объективные независимые суждения и принимать решения, отвечающие интересам общества и его акционеров**			
2.3.1	Только лица, имеющие безупречную деловую и личную репутацию и обладающие знаниями, навыками и опытом, необходимыми для принятия решений, относящихся к компетенции совета директоров, и требующимися для эффективного осуществления его функций, избираются членами совета директоров	1. В отчетном периоде советом директоров (или его комитетом по номинациям) была проведена оценка кандидатов в совет директоров с точки зрения наличия у них необходимого опыта, знаний, деловой репутации, отсутствия конфликта интересов и так далее	Частично соблюдается	Критерий 1 частично соблюдается. В отчетном году Комитетом по кадрам и вознаграждениям Совета директоров Общества были утверждены результаты оценки соответствия критериям независимости кандидатов в члены Совета директоров Общества. Совет директоров Общества единогласно утвердил список кандидатов в члены Совета директоров Общества, подтвердив наличие у них необходимого опыта, знаний, деловой репутации отсутствия конфликта интересов и так далее

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.3.2	Члены совета директоров общества избираются посредством прозрачной процедуры, позволяющей акционерам получить информацию о кандидатах, достаточную для формирования представления об их личных и профессиональных качествах	1. Во всех случаях проведения общего собрания акционеров в отчетном периоде, повестка дня которого включала вопросы об избрании совета директоров, общество представило акционерам биографические данные всех кандидатов в члены совета директоров, результаты оценки соответствия профессиональной квалификации, опыта и навыков кандидатов текущим и ожидаемым потребностям общества, проведенной советом директоров (или его комитетом по номинациям), а также информацию о соответствии кандидата критериям независимости согласно рекомендациям 102–107 Кодекса и информацию о наличии письменного согласия кандидатов на избрание в состав совета директоров	Частично соблюдается	Критерий 1 частично соблюдается. Публичный доступ к информации о членах Совета директоров Общества в отчетном году был ограничен в соответствии с Постановлением Правительства Российской Федерации от 04.07.2023 № 1102. В связи с этим акционерам не предоставлялась подробная информация, рекомендованная Кодексом, о кандидатах в члены Совета директоров Общества при подготовке к проведению Общего собрания акционеров Общества. В том числе не предоставлялись биографические сведения о кандидатах в Совет директоров Общества. При этом акционерам предоставлялась информация о наличии письменного согласия кандидатов на избрание в состав Совета директоров Общества. Советом директоров при принятии решения об утверждении списка кандидатов для избрания в Совет директоров Общества принималось во внимание соответствие профессиональной квалификации, опыта и навыков кандидатов текущим и ожидаемым потребностям Общества. Комитетом по кадрам и вознаграждениям Совета директоров Общества были утверждены результаты оценки соответствия критерия независимости кандидатов в члены Совета директоров Общества
2.3.3	Состав совета директоров сбалансирован, в том числе по квалификации его членов, их опыту, знаниям и деловым качествам, и пользуется доверием акционеров	1. В отчетном периоде совет директоров проанализировал собственные потребности в области профессиональной квалификации, опыта и навыков и определил компетенции, необходимые совету директоров в краткосрочной и долгосрочной перспективе	Соблюдается	
2.3.4	Количественный состав совета директоров общества дает возможность организовать деятельность совета директоров наиболее эффективным образом, включая возможность формирования комитетов совета директоров, а также обеспечивает существенным миноритарным акционерам общества возможность избрания в состав совета директоров кандидата, за которого они голосуют	1. В отчетном периоде совет директоров рассмотрел вопрос о соответствии количественного состава совета директоров потребностям общества и интересам акционеров	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.4	**В состав совета директоров входит достаточное количество независимых директоров**			
2.4.1	Независимым директором признается лицо, которое обладает достаточными профессионализмом, опытом и самостоятельностью для формирования собственной позиции, способно выносить объективные и добросовестные суждения, независимые от влияния исполнительных органов общества, отдельных групп акционеров или иных заинтересованных сторон. При этом следует учитывать, что в обычных условиях не может считаться независимым кандидат (избранный член совета директоров), который связан с обществом, его существенным акционером, существенным контрагентом или конкурентом общества или связан с государством	1. В течение отчетного периода все независимые члены совета директоров отвечали всем критериям независимости, указанным в рекомендациях 102–107 Кодекса, или были признаны независимыми по решению совета директоров	Соблюдается	
2.4.2	Проводится оценка соответствия кандидатов в члены совета директоров критериям независимости, а также осуществляется регулярный анализ соответствия независимых членов совета директоров критериям независимости. При проведении такой оценки содержание преобладает над формой	1. В отчетном периоде совет директоров (или комитет по номинациям совета директоров) составил мнение о независимости каждого кандидата в совет директоров и представил акционерам соответствующее заключение. 2. За отчетный период совет директоров (или комитет по номинациям совета директоров) по крайней мере один раз рассмотрел вопрос о независимости действующих членов совета директоров (после их избрания). 3. В обществе разработаны процедуры, определяющие необходимые действия члена совета директоров в том случае, если он перестает быть независимым, включая обязательства по своевременному информированию об этом совета директоров	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 не соблюдается. Состав Совета директоров Общества был избран Общим собранием акционеров Общества 21.05.2025. Комитет по кадрам и вознаграждениям Совета директоров Общества утвердил результаты оценки соответствия критериям независимости кандидатов в Совет директоров Общества при их избрании. Необходимости пересматривать вопрос о независимости не возникало. В Обществе разработаны процедуры, определяющие необходимые действия члена Совета директоров Общества в том случае, если он перестает быть независимым, включая обязательство по информированию об этом Общество и Совет директоров Общества. Кроме того, в течение года Общество проверяет сохранение статуса независимости у независимых членов Совета директоров Общества в соответствии с требованиями Московской биржи. Соответствующая информация передается на Московскую биржу. Общество планирует рассматривать вопрос о независимости действующих членов Совета директоров Общества в случае получения информации об изменении статуса члена Совета директоров Общества, влияющего на независимость такого члена Совета директоров Общества, в соответствии с внутренними документами Общества. Критерий 3 соблюдается
2.4.3	Независимые директора составляют не менее одной трети избранного состава совета директоров	1. Независимые директора составляют не менее одной трети состава совета директоров	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.4.4	Независимые директора играют ключевую роль в предотвращении внутренних конфликтов в обществе и совершении обществом существенных корпоративных действий	1. Независимые директора (у которых отсутствовал конфликт интересов) в отчетном периоде предварительно оценивали существенные корпоративные действия, связанные с возможным конфликтом интересов, а результаты такой оценки предоставлялись совету директоров	Соблюдается	
2.5	**Председатель совета директоров способствует наиболее эффективному осуществлению функций, возложенных на совет директоров**			
2.5.1	Председателем совета директоров избран независимый директор, либо из числа избранных независимых директоров определен старший независимый директор, координирующий работу независимых директоров и осуществляющий взаимодействие с председателем совета директоров	1. Председатель совета директоров является независимым директором, или же среди независимых директоров определен старший независимый директор. 2. Роль, права и обязанности председателя совета директоров (и, если применимо, старшего независимого директора) должным образом определены во внутренних документах общества	Частично соблюдается	Критерий 1 не соблюдается. Председатель Совета директоров является неисполнительным директором, избран единогласно всеми членами Совета директоров в связи с глубокими знаниями в области основной деятельности Общества. Председатель Совета директоров обладает профессионализмом и значительным опытом работы на руководящих должностях, безупречной деловой и личной репутацией. Среди независимых директоров не определен старший независимый директор. При этом все независимые директора имеют равные права осуществлять взаимодействие с Председателем Совета директоров. Общество рассмотрит необходимость определения старшего независимого директора в случае поступления таких предложений от членов Совета директоров Общества или если такая потребность выяснится иным образом, в том числе по результатам проведенной самооценки работы Совета директоров Общества. Критерий 2 соблюдается
2.5.2	Председатель совета директоров обеспечивает конструктивную атмосферу проведения заседаний, свободное обсуждение вопросов, включенных в повестку дня заседания, контроль за исполнением решений, принятых советом директоров	1. Эффективность работы председателя совета директоров оценивалась в рамках процедуры оценки (самооценки) качества работы совета директоров в отчетном периоде	Соблюдается	
2.5.3	Председатель совета директоров принимает необходимые меры для своевременного предоставления членам совета директоров информации, необходимой для принятия решений по вопросам повестки дня	1. Обязанность председателя совета директоров принимать меры по обеспечению своевременного предоставления полной и достоверной информации членам совета директоров по вопросам повестки заседания совета директоров закреплена во внутренних документах общества	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.6	**Члены совета директоров действуют добросовестно и разумно в интересах общества и его акционеров на основе достаточной информированности, с должной степенью заботливости и осмотрительности**			
2.6.1	Члены совета директоров принимают решения с учетом всей имеющейся информации, в отсутствие конфликта интересов, с учетом равного отношения к акционерам общества, в рамках обычного предпринимательского риска	1. Внутренними документами общества установлено, что член совета директоров обязан уведомить совет директоров, если у него возникает конфликт интересов в отношении любого вопроса повестки дня заседания совета директоров или комитета совета директоров, до начала обсуждения соответствующего вопроса повестки. 2. Внутренние документы общества предусматривают, что член совета директоров должен воздержаться от голосования по любому вопросу, в котором у него есть конфликт интересов. 3. В обществе установлена процедура, которая позволяет совету директоров получать профессиональные консультации по вопросам, относящимся к его компетенции, за счет общества	Соблюдается	
2.6.2	Права и обязанности членов совета директоров четко сформулированы и закреплены во внутренних документах общества	1. В обществе принят и опубликован внутренний документ, четко определяющий права и обязанности членов совета директоров	Соблюдается	
2.6.3	Члены совета директоров имеют достаточно времени для выполнения своих обязанностей	1. Индивидуальная посещаемость заседаний совета и комитетов, а также достаточность времени для работы в совете директоров, в том числе в его комитетах, проанализирована в рамках процедуры оценки (самооценки) качества работы совета директоров в отчетном периоде. 2. В соответствии с внутренними документами общества члены совета директоров обязаны уведомлять совет директоров о своем намерении войти в состав органов управления других организаций (помимо подконтрольных обществу организаций), а также о факте такого назначения	Соблюдается	
2.6.4	Все члены совета директоров в равной степени имеют возможность доступа к документам и информации общества. Вновь избранным членам совета директоров в максимально возможный короткий срок предоставляется достаточная информация об обществе и о работе совета директоров	1. В соответствии с внутренними документами общества члены совета директоров имеют право получать информацию и документы, необходимые членам совета директоров общества для исполнения ими своих обязанностей, касающиеся общества и подконтрольных ему организаций, а исполнительные органы общества обязаны обеспечить предоставление соответствующей информации и документов. 2. В обществе реализуется формализованная программа ознакомительных мероприятий для вновь избранных членов совета директоров	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.7	**Заседания совета директоров, подготовка к ним и участие в них членов совета директоров обеспечивают эффективную деятельность совета директоров**			
2.7.1	Заседания совета директоров проводятся по мере необходимости, с учетом масштабов деятельности и стоящих перед обществом в определенный период времени задач	1. Совет директоров провел не менее шести заседаний за отчетный год	Соблюдается	
2.7.2	Во внутренних документах общества закреплен порядок подготовки и проведения заседаний совета директоров, обеспечивающий членам совета директоров возможность надлежащим образом подготовиться к его проведению	1. В обществе утвержден внутренний документ, определяющий процедуру подготовки и проведения заседаний совета директоров, в котором в том числе установлено, что уведомление о проведении заседания должно быть сделано, как правило, не менее чем за пять дней до даты его проведения. 2. В отчетном периоде отсутствующим в месте проведения заседания совета директоров членам совета директоров предоставлялась возможность участия в обсуждении вопросов повестки дня и голосовании дистанционно — посредством конференц- и видео-конференц-связи	Соблюдается	
2.7.3	Форма проведения заседания совета директоров определяется с учетом важности вопросов повестки дня. Наиболее важные вопросы решаются на заседаниях, проводимых в очной форме	1. Уставом или внутренним документом общества предусмотрено, что наиболее важные вопросы (в том числе перечисленные в рекомендации 168 Кодекса) должны рассматриваться на очных заседаниях совета директоров	Соблюдается	
2.7.4	Решения по наиболее важным вопросам деятельности общества принимаются на заседании совета директоров квалифицированным большинством или большинством голосов всех избранных членов совета директоров	1. Уставом общества предусмотрено, что решения по наиболее важным вопросам, в том числе изложенным в рекомендации 170 Кодекса, должны приниматься на заседании совета директоров квалифицированным большинством, не менее чем в 3/4 голосов, или же большинством голосов всех избранных членов совета директоров	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.8	**Совет директоров создает комитеты для предварительного рассмотрения наиболее важных вопросов деятельности общества**			
2.8.1	Для предварительного рассмотрения вопросов, связанных с контролем за финансово-хозяйственной деятельностью общества, создан комитет по аудиту, состоящий из независимых директоров	1. Совет директоров сформировал комитет по аудиту, состоящий исключительно из независимых директоров. 2. Во внутренних документах общества определены задачи комитета по аудиту, в том числе задачи, содержащиеся в рекомендации 172 Кодекса. 3. По крайней мере один член комитета по аудиту, являющийся независимым директором, обладает опытом и знаниями в области подготовки, анализа, оценки и аудита бухгалтерской (финансовой) отчетности. 4. Заседания комитета по аудиту проводились не реже одного раза в квартал в течение отчетного периода	Частично соблюдается	Критерий 1 не соблюдается. Большинство членов Комитета по аудиту Совета директоров Общества являются независимыми директорами. Его возглавляет независимый директор. Присутствие исполнительного директора в составе Комитета по аудиту позволяет оперативно получать необходимую информацию и пояснения независимым членам Комитета. При этом независимые директора имеют большинство и, соответственно, возможность самостоятельно принимать решения. Указанная практика соответствует требованиям Правил листинга Московской биржи. В среднесрочной перспективе Общество не видит необходимости пересматривать сложившуюся практику. Критерии 2 и 3 соблюдаются. Критерий 4 не соблюдается. Компетенция Комитета по аудиту Совета директоров Общества установлена Положением о Комитете по аудиту Совета директоров Общества. Заседания комитета проводятся при возникновении необходимости рассмотрения вопросов, относящихся к его компетенции. В 2025 году заседания проводились реже одного раза в квартал. В 2026 году Общество планирует перейти на ежеквартальные заседания Комитета по аудиту в тестовом режиме
2.8.2	Для предварительного рассмотрения вопросов, связанных с формированием эффективной и прозрачной практики вознаграждения, создан комитет по вознаграждениям, состоящий из независимых директоров и возглавляемый независимым директором, не являющимся председателем совета директоров	1. Советом директоров создан комитет по вознаграждениям, который состоит только из независимых директоров. 2. Председателем комитета по вознаграждениям является независимый директор, который не является председателем совета директоров. 3. Во внутренних документах общества определены задачи комитета по вознаграждениям, включая в том числе задачи, содержащиеся в рекомендации 180 Кодекса, а также условия (события), при наступлении которых комитет по вознаграждениям рассматривает вопрос о пересмотре политики общества по вознаграждению членов совета директоров, исполнительных органов и иных ключевых руководящих работников	Частично соблюдается	Критерий 1 не соблюдается. Большинство членов Комитета по кадрам и вознаграждениям Совета директоров Общества являются независимыми директорами. Его возглавляет независимый директор. Присутствие исполнительного директора в составе Комитета по кадрам и вознаграждениям Совета директоров Общества позволяет оперативно получать необходимую информацию и пояснения независимым членам комитета. При этом независимые директора имеют большинство и, соответственно, возможность самостоятельно принимать решения. Указанная практика соответствует требованиям Правил листинга Московской биржи. Общество не видит необходимости пересматривать сложившуюся практику в среднесрочной перспективе. Критерии 2 и 3 соблюдаются

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.8.3	Для предварительного рассмотрения вопросов, связанных с осуществлением кадрового планирования (планирования преемственности), профессиональным составом и эффективностью работы совета директоров, создан комитет по номинациям (назначениям, кадрам), большинство членов которого являются независимыми директорами	1. Советом директоров создан комитет по номинациям (или его задачи, указанные в рекомендации 186 Кодекса, реализуются в рамках иного комитета), большинство членов которого являются независимыми директорами. 2. Во внутренних документах общества определены задачи комитета по номинациям (или соответствующего комитета с совмещенным функционалом), включая в том числе задачи, содержащиеся в рекомендации 186 Кодекса. 3. В целях формирования совета директоров, наиболее полно отвечающего целям и задачам общества, комитет по номинациям в отчетном периоде самостоятельно или совместно с иными комитетами совета директоров или уполномоченное подразделение общества по взаимодействию с акционерами организовал взаимодействие с акционерами, не ограничиваясь кругом крупнейших акционеров, в контексте подбора кандидатов в совет директоров общества	Соблюдается	
2.8.4	С учетом масштабов деятельности и уровня риска совет директоров общества удостоверился в том, что состав его комитетов полностью отвечает целям деятельности общества. Дополнительные комитеты либо были сформированы, либо не были признаны необходимыми (комитет по стратегии, комитет по корпоративному управлению, комитет по этике, комитет по управлению рисками, комитет по бюджету, комитет по здоровью, безопасности и окружающей среде и др.)	1. В отчетном периоде совет директоров общества рассмотрел вопрос о соответствии структуры совета директоров масштабу и характеру, целям деятельности и потребностям, профилю рисков общества. Дополнительные комитеты либо были сформированы, либо не были признаны необходимыми	Соблюдается	
2.8.5	Состав комитетов определен таким образом, чтобы он позволял проводить всестороннее обсуждение предварительно рассматриваемых вопросов с учетом различных мнений	1. Комитет по аудиту, комитет по вознаграждениям, комитет по номинациям (или соответствующий комитет с совмещенным функционалом) в отчетном периоде возглавлялись независимыми директорами. 2. Во внутренних документах (политиках) общества предусмотрены положения, в соответствии с которыми лица, не входящие в состав комитета по аудиту, комитета по номинациям (или соответствующий комитет с совмещенным функционалом) и комитета по вознаграждениям, могут посещать заседания комитетов только по приглашению председателя соответствующего комитета	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
2.8.6	Председатели комитетов регулярно информируют совет директоров и его председателя о работе своих комитетов	1. В течение отчетного периода председатели комитетов регулярно отчитывались о работе комитетов перед советом директоров	Частично соблюдается	Критерий 1 частично соблюдается. В текущем отчетном году Совет директоров рассматривал отчет Комитета по аудиту. Отчет Комитета по кадрам и вознаграждениям в текущем году не рассматривался. Комитеты Совета директоров Общества рассматривали необходимые вопросы в рамках своей компетенции. По результатам рассмотрения таких вопросов необходимые рекомендации выносились на рассмотрение Совета директоров Общества. Общество планирует возобновить практику отчетов Комитета по кадрам и вознаграждениям в среднесрочной перспективе
2.9	**Совет директоров обеспечивает проведение оценки качества работы совета директоров, его комитетов и членов совета директоров**			
2.9.1	Проведение оценки качества работы совета директоров направлено на определение степени эффективности работы совета директоров, комитетов и членов совета директоров, соответствия их работы потребностям развития общества, активизацию работы совета директоров и выявление областей, в которых их деятельность может быть улучшена	1. Во внутренних документах общества определены процедуры проведения оценки (самооценки) качества работы совета директоров. 2. Оценка (самооценка) качества работы совета директоров, проведенная в отчетном периоде, включала оценку работы комитетов, индивидуальную оценку каждого члена совета директоров и совета директоров в целом. 3. Результаты оценки (самооценки) качества работы совета директоров, проведенной в течение отчетного периода, были рассмотрены на очном заседании совета директоров	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 частично соблюдается. Служба внутреннего аудита Общества проводит оценку работы Совета директоров Общества, такая оценка не включает индивидуальную оценку каждого члена Совета директоров Общества. В 2026 году была проведена самооценка работы Совета директоров и комитетов по результатам 2025 года. Такая самооценка включает оценку работы комитетов и оценку работы Совета директоров Общества в целом. В настоящее время Общество не планирует введения практики индивидуальной оценки каждого члена Совета директоров Общества. Критерий 3 соблюдается
2.9.2	Оценка работы совета директоров, комитетов и членов совета директоров осуществляется на регулярной основе не реже одного раза в год. Для проведения независимой оценки качества работы совета директоров не реже одного раза в три года привлекается внешняя организация (консультант)	1. Для проведения независимой оценки качества работы совета директоров в течение трех последних отчетных периодов по меньшей мере один раз обществом привлекалась внешняя организация (консультант)	Не соблюдается	Критерий 1 частично соблюдается. Общество осуществило публичное размещение ценных бумаг на Московской бирже 17.12.2021. В 2026 году была проведена самооценка работы Совета директоров и комитетов по результатам 2025 года. Практику проведения независимой оценки качества работы Совета директоров Общества планируется внедрить впоследствии при расширении масштаба деятельности Общества в долгосрочной перспективе
3.1	**Корпоративный секретарь общества обеспечивает эффективное текущее взаимодействие с акционерами, координацию действий общества по защите прав и интересов акционеров, поддержку эффективной работы совета директоров**			
3.1.1	Корпоративный секретарь обладает знаниями, опытом и квалификацией, достаточными для исполнения возложенных на него обязанностей, безупречной репутацией и пользуется доверием акционеров	1. На сайте общества в сети Интернет и в годовом отчете представлена биографическая информация о корпоративном секретаре (включая сведения о возрасте, образовании, квалификации, опыте), а также сведения о должностях в органах управления иных юридических лиц, занимаемых корпоративным секретарем в течение не менее чем пяти последних лет	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
3.1.2	Корпоративный секретарь обладает достаточной независимостью от исполнительных органов общества и имеет необходимые полномочия и ресурсы для выполнения поставленных перед ним задач	1. В обществе принят и раскрыт внутренний документ — положение о корпоративном секретаре. 2. Совет директоров утверждает кандидатуру на должность корпоративного секретаря и прекращает его полномочия, рассматривает вопрос о выплате ему дополнительного вознаграждения. 3. Во внутренних документах общества закреплено право корпоративного секретаря запрашивать, получать документы общества и информацию у органов управления, структурных подразделений и должностных лиц общества	Соблюдается	
4.1	**Уровень выплачиваемого обществом вознаграждения достаточен для привлечения, мотивации и удержания лиц, обладающих необходимой для общества компетенцией и квалификацией. Выплата вознаграждения членам совета директоров, исполнительным органам и иным ключевым руководящим работникам общества осуществляется в соответствии с принятой в обществе политикой по вознаграждению**			
4.1.1	Уровень вознаграждения, предоставляемого обществом членам совета директоров, исполнительным органам и иным ключевым руководящим работникам, создает достаточную мотивацию для их эффективной работы, позволяя обществу привлекать и удерживать компетентных и квалифицированных специалистов. При этом общество избегает большего, чем это необходимо, уровня вознаграждения, а также неоправданно большого разрыва между уровнями вознаграждения указанных лиц и работников общества	1. Вознаграждение членов совета директоров, исполнительных органов и иных ключевых руководящих работников общества определено с учетом результатов сравнительного анализа уровня вознаграждения в сопоставимых компаниях	Соблюдается	
4.1.2	Политика общества по вознаграждению разработана комитетом по вознаграждениям и утверждена советом директоров общества. Совет директоров при поддержке комитета по вознаграждениям обеспечивает контроль за внедрением и реализацией в обществе политики по вознаграждению, а при необходимости — пересматривает и вносит в нее коррективы	1. В течение отчетного периода комитет по вознаграждениям рассмотрел политику (политики) по вознаграждениям и (или) практику ее (их) внедрения, осуществил оценку их эффективности и прозрачности и при необходимости представил соответствующие рекомендации совету директоров по пересмотру указанной политики (политик)	Не соблюдается	Критерий 1 не соблюдается. Учитывая динамичность развития сферы деятельности Общества, в настоящее время Общество разрабатывает систему мотивации, наиболее адекватно отвечающую стратегическим целям Общества. Топ-менеджмент Общества проводит публичные обсуждения такой системы мотивации и получает обратную связь от акционеров и иных стейкхолдеров. По результатам такой работы в случае, если это будет признано эффективным, планируется разработать политику (политики) по вознаграждениям и осуществить их внедрение. Срок реализации разработки и внедрения таких политик в Обществе пока не определен
4.1.3	Политика общества по вознаграждению содержит прозрачные механизмы определения размера вознаграждения членов совета директоров, исполнительных органов и иных ключевых руководящих работников общества, а также регламентирует все виды выплат, льгот и привилегий, предоставляемых указанным лицам	1. Политика (политики) общества по вознаграждению содержит (содержат) прозрачные механизмы определения размера вознаграждения членов совета директоров, исполнительных органов и иных ключевых руководящих работников общества, а также регламентирует (регламентируют) все виды выплат, льгот и привилегий, предоставляемых указанным лицам	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
4.1.4	Общество определяет политику возмещения расходов (компенсаций), конкретизирующую перечень расходов, подлежащих возмещению, и уровень обслуживания, на который могут претендовать члены совета директоров, исполнительные органы и иные ключевые руководящие работники общества. Такая политика может быть составной частью политики общества по вознаграждению	1. В политике (политиках) по вознаграждению или в иных внутренних документах общества установлены правила возмещения расходов членов совета директоров, исполнительных органов и иных ключевых руководящих работников общества	Соблюдается	
4.2	**Система вознаграждения членов совета директоров обеспечивает сближение финансовых интересов директоров с долгосрочными финансовыми интересами акционеров**			
4.2.1	Общество выплачивает фиксированное годовое вознаграждение членам совета директоров. Общество не выплачивает вознаграждение за участие в отдельных заседаниях совета или комитетов совета директоров. Общество не применяет формы краткосрочной мотивации и дополнительного материального стимулирования в отношении членов совета директоров	1. В отчетном периоде общество выплачивало вознаграждение членам совета директоров в соответствии с принятой в обществе политикой по вознаграждению. 2. В отчетном периоде обществом в отношении членов совета директоров не применялись формы краткосрочной мотивации, дополнительного материального стимулирования, выплата которого зависит от результатов (показателей) деятельности общества. Выплата вознаграждения за участие в отдельных заседаниях совета или комитетов совета директоров не осуществлялась	Соблюдается	
4.2.2	Долгосрочное владение акциями общества в наибольшей степени способствует сближению финансовых интересов членов совета директоров с долгосрочными интересами акционеров. При этом общество не обуславливает права реализации акций достижением определенных показателей деятельности, а члены совета директоров не участвуют в опционных программах	1. Если внутренний документ (документы) — политика (политики) по вознаграждению общества — предусматривает (предусматривают) предоставление акций общества членам совета директоров, должны быть предусмотрены и раскрыты четкие правила владения акциями членами совета директоров, нацеленные на стимулирование долгосрочного владения такими акциями	Соблюдается	В Обществе не предусмотрен документ, предоставляющий акции членам Совета директоров
4.2.3	В обществе не предусмотрены какие-либо дополнительные выплаты или компенсации в случае досрочного прекращения полномочий членов совета директоров в связи с переходом контроля над обществом или иными обстоятельствами	1. В обществе не предусмотрены какие-либо дополнительные выплаты или компенсации в случае досрочного прекращения полномочий членов совета директоров в связи с переходом контроля над обществом или иными обстоятельствами	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
4.3	**Система вознаграждения членов исполнительных органов и иных ключевых руководящих работников общества предусматривает зависимость вознаграждения от результата работы общества и их личного вклада в достижение этого результата**			
4.3.1	Вознаграждение членов исполнительных органов и иных ключевых руководящих работников общества определяется таким образом, чтобы обеспечивать разумное и обоснованное соотношение фиксированной части вознаграждения и переменной части вознаграждения, зависящей от результатов работы общества и личного (индивидуального) вклада работника в конечный результат	1. В течение отчетного периода одобренные советом директоров годовые показатели эффективности использовались при определении размера переменного вознаграждения членов исполнительных органов и иных ключевых руководящих работников общества. 2. В ходе последней проведенной оценки системы вознаграждения членов исполнительных органов и иных ключевых руководящих работников общества совет директоров (комитет по вознаграждениям) удостоверился в том, что в обществе применяется эффективное соотношение фиксированной части вознаграждения и переменной части вознаграждения. 3. При определении размера выплачиваемого вознаграждения членам исполнительных органов и иным ключевым руководящим работникам общества учитываются риски, которое несет общество, с тем чтобы избежать создания стимулов к принятию чрезмерно рискованных управленческих решений	Частично соблюдается	Критерий 1 частично соблюдается. В рамках одобрения бюджета на очередной год Совет директоров Общества определяет основные направления развития Общества. Достижение установленных целей учитывается при определении размера переменного вознаграждения Генерального директора Общества и иных ключевых руководящих работников Общества. Критерий 2 частично соблюдается. В отчетном году Совет директоров Общества провел оценку системы вознаграждения Корпоративного секретаря Общества. Совет директоров Общества (Комитет по вознаграждениям Совета директоров Общества) не проводил оценку системы вознаграждения Генерального директора Общества и иных ключевых работников Общества, за исключением Корпоративного секретаря Общества. Полномочия Генерального директора Общества истекают в 2026 году. Не позднее указанного года Советом директоров Общества будет проведена оценка системы вознаграждения Генерального директора Общества. Критерий 3 соблюдается
4.3.2	Общество внедрило программу долгосрочной мотивации членов исполнительных органов и иных ключевых руководящих работников общества с использованием акций общества (опционов или других производных финансовых инструментов, базисным активом по которым являются акции общества)	1. В случае если общество внедрило программу долгосрочной мотивации для членов исполнительных органов и иных ключевых руководящих работников общества с использованием акций общества (финансовых инструментов, основанных на акциях общества), программа предусматривает, что право реализации таких акций и иных финансовых инструментов наступает не ранее чем через три года с момента их предоставления. При этом право их реализации обусловлено достижением определенных показателей деятельности общества	Соблюдается	
4.3.3	Сумма компенсации («золотой парашют»), выплачиваемая обществом в случае досрочного прекращения полномочий членам исполнительных органов или ключевых руководящих работников по инициативе общества и при отсутствии с их стороны недобросовестных действий, не превышает двукратного размера фиксированной части годового вознаграждения	1. Сумма компенсации («золотой парашют»), выплачиваемая обществом в случае досрочного прекращения полномочий членам исполнительных органов или ключевым руководящим работникам по инициативе общества и при отсутствии с их стороны недобросовестных действий, в отчетном периоде не превышала двукратного размера фиксированной части годового вознаграждения	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
5.1	**В обществе создана эффективно функционирующая система управления рисками и внутреннего контроля, направленная на обеспечение разумной уверенности в достижении поставленных перед обществом целей**			
5.1.1	Советом директоров общества определены принципы и подходы к организации системы управления рисками и внутреннего контроля в обществе	1. Функции различных органов управления и подразделений общества в системе управления рисками и внутреннего контроля четко определены во внутренних документах / соответствующей политике общества, одобренной советом директоров	Соблюдается	
5.1.2	Исполнительные органы общества обеспечивают создание и поддержание функционирования эффективной системы управления рисками и внутреннего контроля в обществе	1. Исполнительные органы общества обеспечили распределение обязанностей, полномочий, ответственности в области управления рисками и внутреннего контроля между подотчетными им руководителями (начальниками) подразделений и отделов	Соблюдается	
5.1.3	Система управления рисками и внутреннего контроля в обществе обеспечивает объективное, справедливое и ясное представление о текущем состоянии и перспективах общества, целостность и прозрачность отчетности общества, разумность и приемлемость принимаемых обществом рисков	1. В обществе утверждена антикоррупционная политика. 2. В обществе организован безопасный, конфиденциальный и доступный способ (горячая линия) информирования совета директоров или комитета совета директоров по аудиту о фактах нарушения законодательства, внутренних процедур, кодекса этики общества	Соблюдается	
5.1.4	Совет директоров общества предпринимает необходимые меры для того, чтобы убедиться, что действующая в обществе система управления рисками и внутреннего контроля соответствует определенным советом директоров принципам и подходам к ее организации и эффективно функционирует	1. В течение отчетного периода совет директоров (комитет по аудиту и (или) комитет по рискам (при наличии)) организовал проведение оценки надежности и эффективности системы управления рисками и внутреннего контроля. 2. В отчетном периоде совет директоров рассмотрел результаты оценки надежности и эффективности системы управления рисками и внутреннего контроля общества и сведения о результатах рассмотрения включены в состав годового отчета общества	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 частично соблюдается. Для целей оценки надежности и эффективности управления рисками и внутреннего контроля в Обществе проводится внутренний аудит. Результаты внутреннего аудита Общества не включались в состав Годового отчета Общества, однако предоставлялись акционерам в составе материалов для подготовки к годовому Общему собранию акционеров Общества. Общество рассмотрит возможность включения результатов рассмотрения в состав годового отчета Общества в среднесрочной перспективе
5.2	**Для систематической независимой оценки надежности и эффективности системы управления рисками и внутреннего контроля, и практики корпоративного управления общество организовывает проведение внутреннего аудита**			
5.2.1	Для проведения внутреннего аудита в обществе создано отдельное структурное подразделение или привлечена независимая внешняя организация. Функциональная и административная подотчетность подразделения внутреннего аудита разграничены. Функционально подразделение внутреннего аудита подчиняется совету директоров	1. Для проведения внутреннего аудита в обществе создано отдельное структурное подразделение внутреннего аудита, функционально подотчетное совету директоров, или привлечена независимая внешняя организация с тем же принципом подотчетности	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
5.2.2	Подразделение внутреннего аудита проводит оценку надежности и эффективности системы управления рисками и внутреннего контроля, а также оценку корпоративного управления, применяет общепринятые стандарты деятельности в области внутреннего аудита	1. В отчетном периоде в рамках проведения внутреннего аудита дана оценка надежности и эффективности системы управления рисками и внутреннего контроля. 2. В отчетном периоде в рамках проведения внутреннего аудита дана оценка практики (отдельных практик) корпоративного управления, включая процедуры информационного взаимодействия (в том числе по вопросам внутреннего контроля и управления рисками) на всех уровнях управления общества, а также взаимодействия с заинтересованными лицами	Соблюдается	
6.1	**Общество и его деятельность являются прозрачными для акционеров, инвесторов и иных заинтересованных лиц**			
6.1.1	В обществе разработана и внедрена информационная политика, обеспечивающая эффективное информационное взаимодействие общества, акционеров, инвесторов и иных заинтересованных лиц	1. Советом директоров общества утверждена информационная политика общества, разработанная с учетом рекомендаций Кодекса. 2. В течение отчетного периода совет директоров (или один из его комитетов) рассмотрел вопрос об эффективности информационного взаимодействия общества, акционеров, инвесторов и иных заинтересованных лиц и целесообразности (необходимости) пересмотра информационной политики общества	Частично соблюдается	Критерий 1 частично соблюдается. Информационная политика в виде отдельного формализованного письменного документа, утвержденного Советом директоров Общества, находится в процессе разработки. Рекомендации Кодекса в части информационной политики учтены при разработке Положения о Корпоративном секретаре Общества. В отчетном году Общество было вынуждено ограничить раскрываемую информацию в соответствии с Постановлением Правительства Российской Федерации от 04.07.2023 № 1102. Обществом соблюдаются установленные действующим законодательством требования о раскрытии информации. Топ-менеджмент Общества проводит регулярные очные и онлайн-встречи с инвесторами. Дополнительно Общество разъясняет инвесторам детали своей деятельности в социальных сетях. В настоящее время Общество разрабатывает единую информационную политику с учетом текущей внешней среды. Такую политику планируется подготовить в среднесрочной перспективе. Критерий 2 не соблюдается. Информационная политика в виде отдельного формализованного письменного документа, утвержденного Советом директоров, в Обществе находится в процессе разработки. После завершения разработки соответствующей политики планируется, что Совет директоров периодически будет оценивать ее актуальность

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
6.1.2	Общество раскрывает информацию о системе и практике корпоративного управления, включая подробную информацию о соблюдении принципов и рекомендаций Кодекса	1. Общество раскрывает информацию о системе корпоративного управления в обществе и общих принципах корпоративного управления, применяемых в обществе, в том числе на сайте общества в сети Интернет. 2. Общество раскрывает информацию о составе исполнительных органов и совета директоров, независимости членов совета и их членстве в комитетах совета директоров (в соответствии с определением Кодекса). 3. В случае наличия лица, контролирующего общество, общество публикует меморандум контролирующего лица относительно планов такого лица в отношении корпоративного управления в обществе	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 частично соблюдается. Информация о Генеральном директоре раскрывается Обществом. Иных исполнительных органов в Обществе не образовано. В соответствии с положениями Постановления Правительства Российской Федерации от 04.07.2023 № 1102 Общество ограничило публичное раскрытие информации о членах Совета директоров Общества. При этом Общество рассылает информацию о кандидатах акционерам Общества в составе материалов к соответствующему собранию, включая информацию о независимости кандидатов в члены Совета директоров Общества. Общество планирует возобновить практику полного раскрытия информации о составе Совета директоров Общества, независимости членов Совета директоров Общества и их членстве в комитетах Совета директоров Общества после изменения внешних условий. Критерий 3 частично соблюдается. Контролирующий акционер Общества не публикует меморандум контролирующего лица относительно планов такого лица в отношении корпоративного управления в Обществе. При этом контролирующий акционер Общества проводит публичные онлайн-выступления, на которых разъясняет инвесторам и иным заинтересованным лицам планы в отношении корпоративного управления в Обществе
6.2	**Общество своевременно раскрывает полную, актуальную и достоверную информацию об обществе для обеспечения возможности принятия обоснованных решений акционерами общества и инвесторами**			
6.2.1	Общество раскрывает информацию в соответствии с принципами регулярности, последовательности и оперативности, а также доступности, достоверности, полноты и сравнимости раскрываемых данных	1. В обществе определена процедура, обеспечивающая координацию работы всех структурных подразделений и работников общества, связанных с раскрытием информации или деятельность которых может привести к необходимости раскрытия информации. 2. В случае если ценные бумаги общества обращаются на иностранных организованных рынках, раскрытие существенной информации в Российской Федерации и на таких рынках осуществляется синхронно и эквивалентно в течение отчетного года. 3. Если иностранные акционеры владеют существенным количеством акций общества, то в течение отчетного года раскрытие информации осуществлялось не только на русском, но также на одном из наиболее распространенных иностранных языков	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
6.2.2	Общество избегает формального подхода при раскрытии информации и раскрывает существенную информацию о своей деятельности, даже если раскрытие такой информации не предусмотрено законодательством	1. В информационной политике общества определены подходы к раскрытию сведений об иных событиях (действиях), оказывающих существенное влияние на стоимость или котировки его ценных бумаг, раскрытие сведений о которых не предусмотрено законодательством. 2. Общество раскрывает информацию о структуре капитала общества в соответствии с рекомендацией 290 Кодекса в годовом отчете и на сайте общества в сети Интернет. 3. Общество раскрывает информацию о подконтрольных организациях, имеющих для него существенное значение, в том числе о ключевых направлениях их деятельности, о механизмах, обеспечивающих подотчетность подконтрольных организаций, полномочиях совета директоров общества в отношении определения стратегии и оценки результатов деятельности подконтрольных организаций. 4. Общество раскрывает нефинансовый отчет — отчет об устойчивом развитии, экологический отчет, отчет о корпоративной социальной ответственности или иной отчет, содержащий нефинансовую информацию, в том числе о факторах, связанных с окружающей средой (в том числе экологические факторы и факторы, связанные с изменением климата), обществом (социальные факторы) и корпоративным управлением, за исключением отчета эмитента эмиссионных ценных бумаг и годового отчета акционерного общества	Частично соблюдается	Критерий 1 не соблюдается. Информационная политика в виде отдельного формализованного письменного документа, утвержденного Советом директоров, находится в процессе разработки. Топ-менеджмент Общества проводит регулярные очные и онлайн-встречи с инвесторами. Дополнительно Общество разъясняет инвесторам детали своей деятельности в социальных сетях. В настоящее время Общество разрабатывает единую информационную политику с учетом внешних условий. Такую политику планируется разработать в среднесрочной перспективе. Критерий 2 частично соблюдается. Общество раскрывает информацию о структуре капитала Общества в сокращенном объеме по сравнению с рекомендацией 290 Кодекса в соответствии с положениями Постановления Правительства Российской Федерации от 04.07.2023 № 1102. Общество планирует вернуться к практике раскрытия информации о структуре капитала Общества в соответствии с рекомендацией 290 Кодекса после изменения соответствующих внешних условий. Критерий 3 частично соблюдается. Общество раскрывает информацию о подконтрольных организациях, имеющих для него существенное значение, в сокращенном объеме в соответствии с положениями Постановления Правительства Российской Федерации от 04.07.2023 № 1102. Общество планирует вернуться к практике раскрытия подробной информации о подконтрольных организациях, имеющих для него существенное значение, после изменения соответствующих внешних условий. Критерий 4 не соблюдается. Общество не раскрывает нефинансовый отчет — отчет об устойчивом развитии, экологический отчет, отчет о корпоративной социальной ответственности или иной отчет, содержащий нефинансовую информацию. При этом Общество регулярно проводит образовательные и социальные мероприятия, информация о которых раскрывается в пресс-релизах Общества. Годовой отчет Общества содержит сведения о социальной политике Общества. В настоящее время Общество рассматривает вопрос о внедрении практики раскрытия нефинансового отчета. Соответствующая практика будет внедрена при увеличении масштабов деятельности Общества в долгосрочной перспективе
6.2.3	Годовой отчет, являясь одним из наиболее важных инструментов информационного взаимодействия с акционерами и другими заинтересованными сторонами, содержит информацию, позволяющую оценить итоги деятельности общества за год	1. Годовой отчет общества содержит информацию о результатах оценки комитетом по аудиту эффективности процесса проведения внешнего и внутреннего аудита. 2. Годовой отчет общества содержит сведения о политике общества в области охраны окружающей среды, социальной политике общества	Частично соблюдается	Критерий 1 частично соблюдается. В отчетном году Совет директоров Общества и Комитет Совета директоров Общества не рассматривал отдельно вопрос об эффективности процесса проведения внешнего аудита. Вопрос об эффективности внешнего аудита рассматривается в рамках вопросов об утверждении бухгалтерской (финансовой) отчетности Общества и консолидированной финансовой отчетности Общества, а также при рассмотрении кандидатуры внешнего аудитора на очередной год. Критерий 2 соблюдается

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
6.3	**Общество предоставляет информацию и документы по запросам акционеров в соответствии с принципами равнодоступности и необременительности**			
6.3.1	Реализация акционерами права на доступ к документам и информации общества не сопряжена с неоправданными сложностями	1. В информационной политике (внутренних документах, определяющих информационную политику) общества определен необременительный порядок предоставления по запросам акционеров доступа к информации и документам общества. 2. В информационной политике (внутренних документах, определяющих информационную политику) содержатся положения, предусматривающие, что в случае поступления запроса акционера о предоставлении информации о подконтрольных обществу организациях общество предпринимает необходимые усилия для получения такой информации у соответствующих подконтрольных обществу организаций	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 не соблюдается. Информационная политика в виде отдельного формализованного письменного документа, утвержденного Советом директоров, находится в процессе разработки. В отчетном году Общество было вынуждено ограничить раскрытие информации о подконтрольных Обществу организациях, имеющих для него существенное значение, согласно положениям Постановления Правительства Российской Федерации от 04.07.2023 № 1102. В случае поступления запроса от акционера о предоставлении информации о таких организациях Общество будет рассматривать каждый такой запрос индивидуально для обеспечения баланса между открытостью и необходимым в сложившихся условиях уровнем конфиденциальности. В настоящее время Общество разрабатывает единую информационную политику с учетом текущих внешних условий. Такую политику планируется разработать в среднесрочной перспективе
6.3.2	При предоставлении обществом информации акционерам обеспечивается разумный баланс между интересами конкретных акционеров и интересами самого общества, заинтересованного в сохранении конфиденциальности важной коммерческой информации, которая может оказать существенное влияние на его конкурентоспособность	1. В течение отчетного периода общество не отказывало в удовлетворении запросов акционеров о предоставлении информации либо такие отказы были обоснованными. 2. В случаях, определенных информационной политикой общества, акционеры предупреждаются о конфиденциальном характере информации и принимают на себя обязанность по сохранению ее конфиденциальности	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 частично соблюдается. Информационная политика в виде отдельного формализованного письменного документа, утвержденного Советом директоров, находится в процессе разработки. Акционеры предупреждаются о конфиденциальном характере информации и принимают на себя обязанность по сохранению ее конфиденциальности путем подписания соглашения о конфиденциальности размещенном на сайте Общества
7.1	**Действия, которые в значительной степени влияют или могут повлиять на структуру акционерного капитала и финансовое состояние общества и, соответственно, на положение акционеров (существенные корпоративные действия), осуществляются на справедливых условиях, обеспечивающих соблюдение прав и интересов акционеров, а также иных заинтересованных сторон**			
7.1.1	Существенными корпоративными действиями признаются реорганизация общества, приобретение 30 и более процентов голосующих акций общества (поглощение), совершение обществом существенных сделок, увеличение или уменьшение уставного капитала общества, осуществление листинга и делистинга акций общества, а также иные действия, которые могут привести к существенному изменению прав акционеров или нарушению их интересов. Уставом общества определен перечень (критерии) сделок или иных действий, являющихся существенными корпоративными действиями, и такие действия отнесены к компетенции совета директоров общества	1. Уставом общества определен перечень (критерии) сделок или иных действий, являющихся существенными корпоративными действиями. Принятие решений в отношении существенных корпоративных действий уставом общества отнесено к компетенции совета директоров. В тех случаях, когда осуществление данных корпоративных действий прямо отнесено законодательством к компетенции общего собрания акционеров, совет директоров предоставляет акционерам соответствующие рекомендации	Соблюдается	

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
7.1.2	Совет директоров играет ключевую роль в принятии решений или выработке рекомендаций в отношении существенных корпоративных действий, совет директоров опирается на позицию независимых директоров общества	1. В обществе предусмотрена процедура, в соответствии с которой независимые директора заявляют о своей позиции по существенным корпоративным действиям до их одобрения	Соблюдается	
7.1.3	При совершении существенных корпоративных действий, затрагивающих права и законные интересы акционеров, обеспечиваются равные условия для всех акционеров общества, а при недостаточности предусмотренных законодательством механизмов, направленных на защиту прав акционеров, — дополнительные меры, защищающие права и законные интересы акционеров общества. При этом общество руководствуется не только соблюдением формальных требований законодательства, но и принципами корпоративного управления, изложенными в Кодексе	1. Уставом общества с учетом особенностей его деятельности к компетенции совета директоров отнесено одобрение, помимо предусмотренных законодательством, иных сделок, имеющих существенное значение для общества. 2. В течение отчетного периода все существенные корпоративные действия проходили процедуру одобрения до их осуществления	Частично соблюдается	Критерий 1 частично соблюдается. Компетенция Совета директоров Общества в части одобрения сделок предусмотрена Уставом Общества в соответствии с требованиями действующего законодательства. Учитывая характер деятельности Общества, Общество не видит необходимости пересматривать сложившуюся практику в среднесрочной перспективе. Критерий 2 соблюдается
7.2	**Общество обеспечивает такой порядок совершения существенных корпоративных действий, который позволяет акционерам своевременно получать полную информацию о таких действиях, обеспечивает им возможность влиять на совершение таких действий и гарантирует соблюдение и адекватный уровень защиты их прав при совершении таких действий**			
7.2.1	Информация о совершении существенных корпоративных действий раскрывается с объяснением причин, условий и последствий совершения таких действий	1. В случае если обществом в течение отчетного периода совершались существенные корпоративные действия, общество своевременно и детально раскрывало информацию о таких действиях, в том числе о причинах, условиях совершения действий и последствиях таких действий для акционеров	Частично соблюдается	Критерий 1 частично соблюдается. В отчетном периоде Общество было вынуждено ограничить раскрытие информации в соответствии с Постановлением Правительства Российской Федерации от 04.07.2023 № 1102. В связи с этим информация о существенных корпоративных действиях раскрывалась Обществом в ограниченном объеме. Общество планирует вернуться к практике полного раскрытия информации о существенных корпоративных действиях при изменении соответствующих внешних условий

№	Принципы корпоративного управления	Критерии оценки соблюдения принципа корпоративного управления	Статус соответствия принципу корпоративного управления	Объяснения отклонения от критериев оценки соблюдения принципа корпоративного управления
1	2	3	4	5
7.2.2	Правила и процедуры, связанные с осуществлением обществом существенных корпоративных действий, закреплены во внутренних документах общества	1. Во внутренних документах общества определены случаи и порядок привлечения оценщика для определения стоимости имущества, отчуждаемого или приобретаемого по крупной сделке или сделке с заинтересованностью. 2. Внутренние документы общества предусматривают процедуру привлечения оценщика для оценки стоимости приобретения и выкупа акций общества. 3. При отсутствии формальной заинтересованности члена совета директоров, единоличного исполнительного органа, члена коллегиального исполнительного органа общества или лица, являющегося контролирующим лицом общества, либо лица, имеющего право давать обществу обязательные для него указания, в сделках общества, но при наличии конфликта интересов или иной их фактической заинтересованности, внутренними документами общества предусмотрено, что такие лица не принимают участия в голосовании по вопросу одобрения такой сделки	Частично соблюдается	Критерий 1 не соблюдается. Внутренние документы Общества предусматривают процедуру привлечения независимого оценщика для определения стоимости имущества в случаях, предусмотренных действующим законодательством. Для остальных случаев в целях оперативного принятия решений при определении стоимости имущества, отчуждаемого или приобретаемого по крупной сделке или сделке с заинтересованностью, используются процедуры, предусмотренные действующим законодательством. Совет директоров Общества при определении стоимости соответствующего имущества руководствуется заключениями, подготовленными менеджментом Общества. Общество в целях сохранения возможности оперативного осуществления хозяйственной деятельности в условиях быстро меняющейся внешней среды не планирует в среднесрочной перспективе расширять перечень случаев привлечения независимого оценщика для определения цены имущества, отчуждаемого по крупной сделке или сделке с заинтересованностью. Критерий 2 соблюдается. Критерий 3 соблюдается частично. Во внутренних документах Общества напрямую не закреплена обязанность члена Совета директоров, Генерального директора Общества, лица, являющегося контролирующим лицом Общества, воздерживаться от голосования по вопросам одобрения сделок, в которых при отсутствии формальной заинтересованности у такого лица имеется конфликт интересов или фактическая заинтересованность в совершении такой сделки. При этом Положение о Совете директоров Общества регламентирует вопросы конфликта интересов Совета директоров Общества. Члены Совета директоров Общества обязаны сообщать Обществу и Совету директоров Общества о наличии конфликта интересов. Членам Совета директоров Общества, формально не заинтересованным в совершении сделки при наличии конфликта интересов, не рекомендуется участвовать в голосовании по соответствующему вопросу. По вопросам порядка одобрения сделок Общество строго руководствуется требованиями действующего законодательства

Отчет о совершенных (заключенных) крупных сделках[1]

В течение отчетного периода Компанией не совершались крупные сделки.

Отчет о совершенных (заключенных) сделках, в совершении которых имеется заинтересованность[2]

В течение отчетного периода Компанией не совершались сделки, в совершении которых имелась заинтересованность.

1 Утвержден в составе Годового отчета ПАО «Группа Позитив» за 2025 год, утвержденного решением Совета директоров ПАО «Группа Позитив» 7 апреля 2026 года (протокол от 7 апреля 2026 года № 46).
2 Утвержден в составе Годового отчета ПАО «Группа Позитив» за 2025 год, утвержденного решением Совета директоров ПАО «Группа Позитив» 7 апреля 2026 года (протокол от 7 апреля 2026 года № 46).

Раскрытие корпоративной информации

Раскрытие информации на сайте ПАО «Группа Позитив»

Страница Компании на сайте «Интерфакс-ЦРКИ»

Контакты

Публичное акционерное общество «Группа Позитив»

ИНН 9718077239
КПП 771801001

Юридический адрес: 107061, г. Москва, Преображенская пл., 8, пом. 60.

Почтовый адрес: 107061, г. Москва, Преображенская пл., 8.

Сайт: group.ptsecurity.com/ru
Тел.: +7 (495) 744-01-44

По общим вопросам
Тел.: +7 (495) 540-53-28
Email: info-group@ptsecurity.com

Для акционеров и инвесторов
Тел.: +7 (495) 744-01-44
Email: shareholder@ptsecurity.com