Годовой отчет '24

pt

POSI

быть → на шаг впереди

Содержание

О Компании

1.1

Защитники цифрового мира

Positive Technologies — ведущий разработчик инновационных продуктов в области кибербезопасности и первая публичная компания отрасли на Московской бирже.

Уже 23 года мы создаем технологии, которые помогают бизнесу и государству эффективно противостоять цифровым угрозам. Наши продукты и сервисы помогают достичь результативной кибербезопасности и обеспечить реальную защиту компаний от хакерских атак.

Positive Technologies — лидер результативной кибербезопасности. Быть в авангарде для нас — это не просто взгляд в будущее, это умение действовать на опережение. Мы не просто реагируем на угрозы, мы предвосхищаем их, создаем уникальные подходы к защите, которые опережают время и задают новые стандарты для всей отрасли. В условиях, когда кибербезопасность является неотъемлемой частью цифрового мира, мы выходим за рамки традиционной защиты и создаем решения, которые объединяют информационные технологии (ИТ) и информационную безопасность (ИБ).

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.

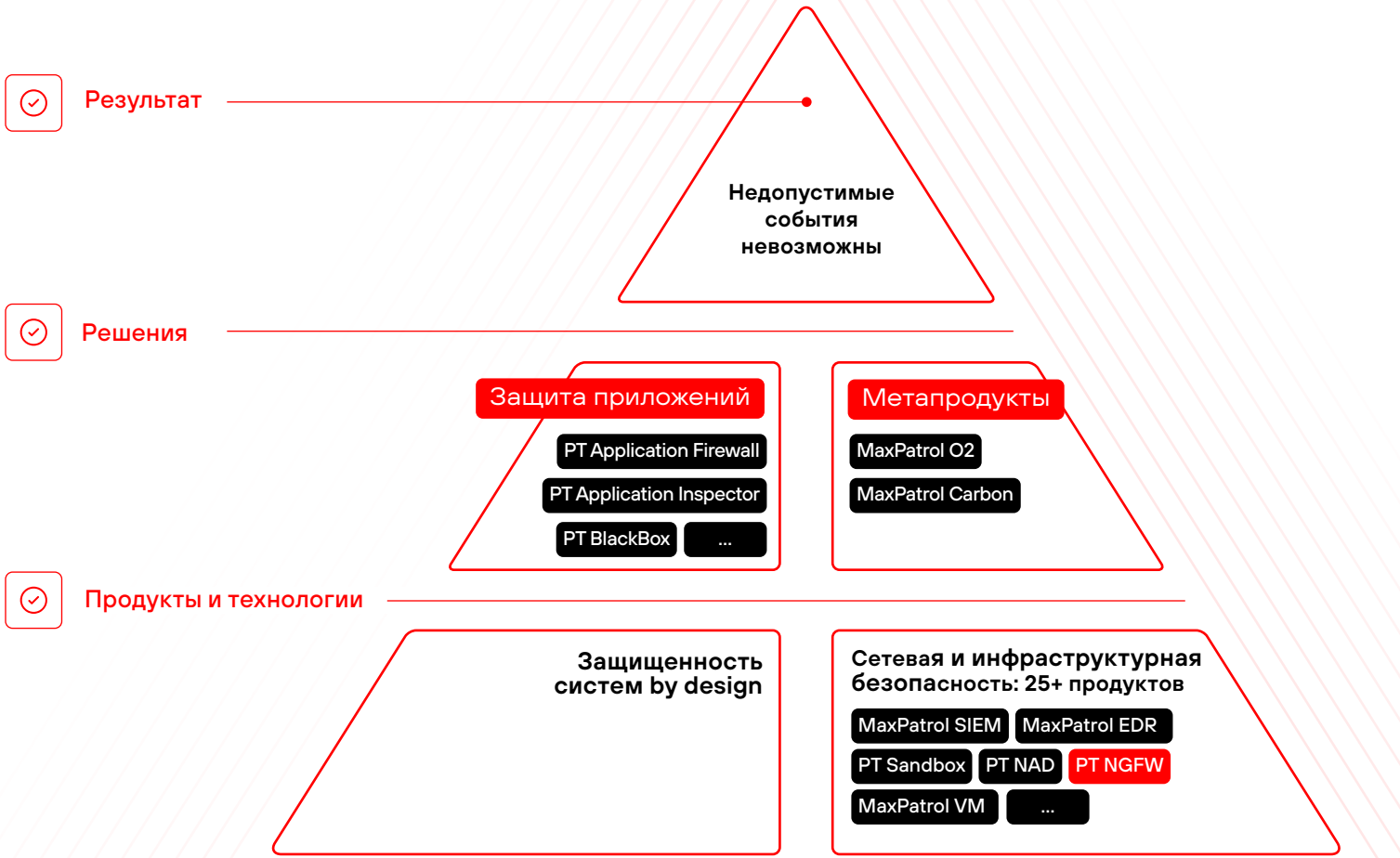
1.2

Быть в авангарде

Наши продукты решают огромный спектр задач в области кибербезопасности: от сканирования инфраструктуры компании и анализа сетевого трафика до защиты от целевых атак и реагирования на них.

Мы закладываем в основу наших продуктов собственные технологии. Именно они обеспечивают результативность и выстраивают непреодолимый барьер для злоумышленников.

Наши продукты и технологии помогают достичь результативной кибербезопасности, сделать недопустимые события невозможными и обеспечить реальную защиту компании от хакерских атак.



Результативная кибербезопасность

Защититься от всех киберугроз невозможно. Все больше организаций привлекает бизнес-ориентированная (результативная) кибербезопасность, задача которой — защитить наиболее важные активы компании и предотвратить наступление недопустимых событий.

«

За последние годы отрасль кибербезопасности трансформировалась и стала одной из самых привлекательных технологических сфер в стране. С одной стороны, окончательно сформировался запрос на доставку реального результата в формате киберзащищенности. С другой — отечественные технологии шагнули на новый уровень развития, который позволяет обеспечивать этот самый результат.

Денис Баранов,
Генеральный директор Positive Technologies

Недопустимые события

Событие, которое возникло в результате кибератаки и делает невозможным достижение операционных и (или) стратегических целей организации или приводит к значительному нарушению ее основной деятельности.

Результативная кибербезопасность

Подход, позволяющий организации (отрасли, государству) достичь состояния защищенности, характеризующегося устойчивостью к кибератакам, и в любой момент на практике подтвердить, что злоумышленник не сможет реализовать недопустимые для организации (отрасли, государства) события.

Фреймворк результативной кибербезопасности

Карта рынка наших продуктов — лидеров в своих сегментах

Security Information & Event Management
MaxPatrol SIEM

Next-Generation Firewall
PT NGFW

Vulnerability Management
MaxPatrol 8 + MaxPatrol VM + XSpider

Static Application Security Testing
PT Application Inspector

Network Traffic Analysis/NDR
PT Network Attack Discovery

Endpoint Detection & Response
MaxPatrol EDR

Web Application Firewall
PT Application Firewall

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

Network Sandboxing
PT Sandbox

Dynamic Application Security Testing
PT BlackBox

Продуктовая линейка Positive Technologies насчитывает более 25 продуктов и решений. Мы являемся лидерами рынка корпоративной кибербезопасности в ключевых технологических нишах.

>25

продуктов и решений

Мы работаем над расширением клиентской базы и продуктовой линейки, фокусируясь на результативности работы наших решений и комплексной защищенности клиентов. Мы выстраиваем с клиентами долгосрочные отношения: уровень продления составляет более 90%.

Рынок кибербезопасности растет

По итогам 2023 года на рынке средств защиты информации (СЗИ) обозначились два лидера — «Лаборатория Касперского» и Positive Technologies. Эти компании занимают схожие доли рынка, значительно опережая остальных участников. При этом динамика изменений демонстрирует разнонаправленные тенденции: доля «Лаборатории Касперского» на рынке постепенно снижается (–1,5 п. п. за год), в то время как Positive Technologies растет (+1,7 п. п. за год).

Цифровизация затрагивает все сферы жизни, делая кибербезопасность неотъемлемым элементом устойчивого развития общества. Киберпреступники постоянно находят уязвимости в системах и сетях, что позволяет им организовывать атаки с серьезными последствиями для бизнеса. В ответ компании вынуждены усиливать защиту, что приводит к росту спроса на надежные решения в области ИБ.

275–300 млрд руб.

объем рынка кибербезопасности в России[1]

2024 год стал важным этапом развития результативной кибербезопасности. В условиях ограниченных ресурсов бизнес вынужден тщательнее подходить к вопросам своей деятельности, оценивая не только действия, но и их эффективность. В сфере кибербезопасности это переосмысление приводит к акценту на достижении конкретного результата. Компании начинают сосредотачиваться на выявлении событий, которые представляют наибольшую угрозу для бизнеса, и выстраивании защиты, направленной на их предотвращение.

10–15 %

рост российского рынка кибербезопасности в 2024 году[2]

По прогнозам Центра стратегических разработок (ЦСР), в ближайшие пять лет рынок кибербезопасности в России вырастет в 2,4 раза — до 715 млрд руб.

Среди основных драйверов роста рынка в ближайшие годы:

- рост числа кибератак;
- массовый уход зарубежных вендоров — практически все иностранные разработчики покинули российский рынок;
- финансовые и нефинансовые меры поддержки отрасли — пониженная ставка налога на прибыль, льготная ставка по кредитам;
- готовность заказчиков к импортозамещению — переход российских компаний на отечественное ПО;
- персональная ответственность — теперь руководители организаций должны отвечать за обеспечение кибербезопасности своих предприятий;
- запрет на использование ПО, ИБ-сервисов и услуг из недружественных государств — с 1 января 2025 года (согласно указу Президента Российской Федерации).

Российские организации сегодня фактически стали полигоном для тестирования новых видов кибероружия и тактик. Это вынуждает компании отходить от формального соответствия регуляторным требованиям и сосредотачиваться на реальной защите, направленной на предотвращение критически опасных событий.

[1] По оценкам Positive Technologies и ЦСР.
[2] По оценкам Positive Technologies.

1.3

Инновации как драйвер роста

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

Сегодня мы стараемся быть максимально гибкими — с точки зрения как организационной структуры, так и того, как мы смотрим на технологии, которым доверяем и в которые верим. Прогресс развивается настолько стремительно, что технологии, еще вчера служившие нашей опорой, сегодня могут стать ограничением. Поэтому мы стараемся построить такую 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.

Мы продолжаем наращивать инвестиции в R&D и убеждены, что это позволит нам обеспечить непрерывность роста масштаба бизнеса Positive Technologies в последующие годы.

В 2024 году объем вложений в разработку новых продуктов, улучшение функциональности существующих решений, а также в технологические и инфраструктурные проекты вырос на 82% по сравнению с прошлым годом, достигнув 9,1 млрд руб.

Мы продолжили усиливать команду, привлекая разработчиков и экспертов в области кибербезопасности.

Видим отдачу от инвестиций, сделанных ранее

Менее чем за два месяца наш новый продукт — межсетевой экран нового поколения PT NGFW — преодолел отметку 1 млрд руб. Массовые отгрузки стартовали 20 ноября 2024 года, и по итогам года общий объем отгрузок PT NGFW составил 1,2 млрд руб. Этот результат подтверждает востребованность решения на рынке и оправдывает вложения в его разработку.

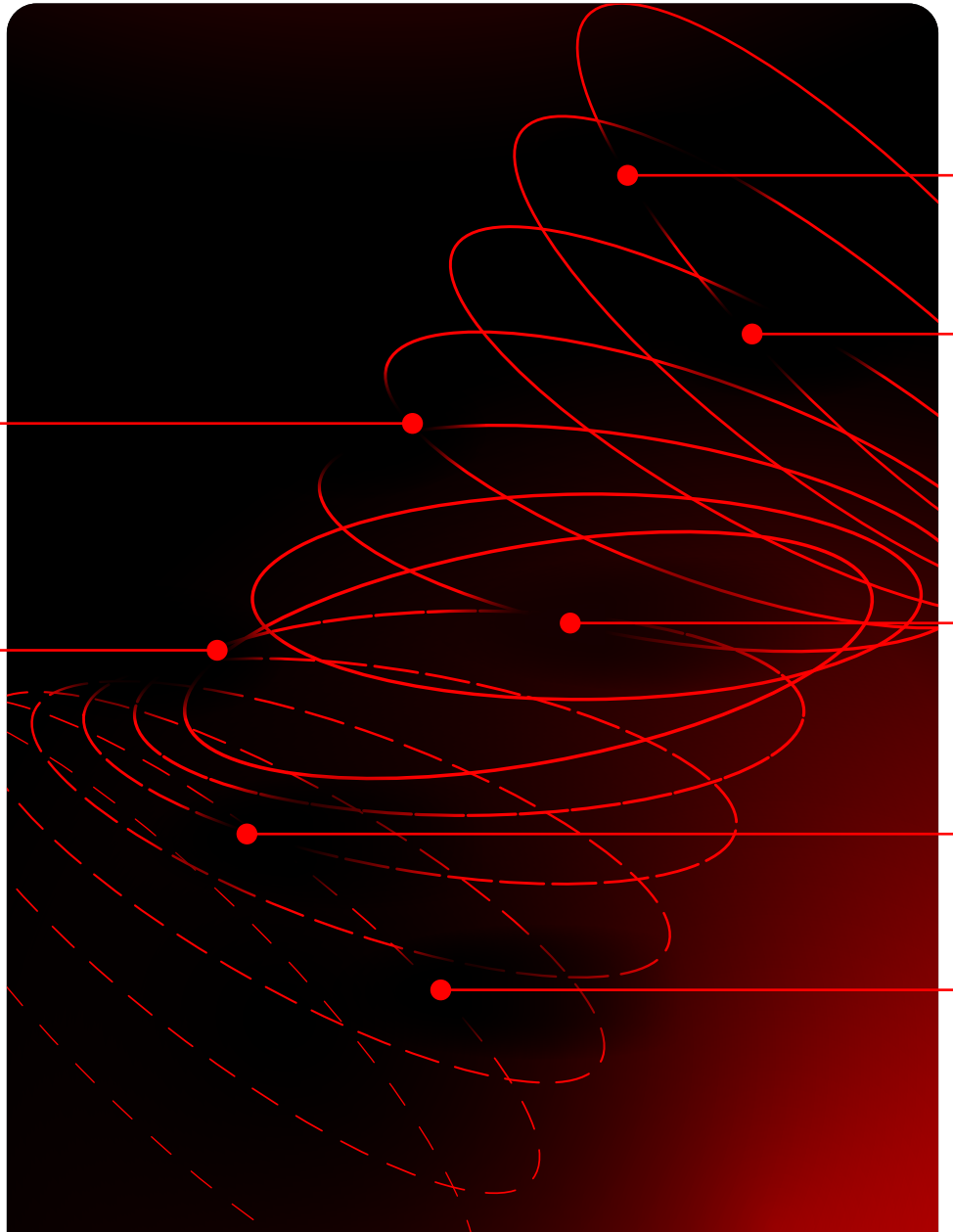
82%

рост расходов на R&D, технологические и инфраструктурные проекты

1,2 млрд руб.

объем отгрузок PT NGFW в 2024 году

Наши новые продукты и перспективные разработки



Метапродукты

MaxPatrol O2 — наш первый метапродукт, который позволяет обнаружить и остановить хакера с минимальным участием человека.

MaxPatrol Carbon — наш второй метапродукт. Помогает достичь киберустойчивости ИТ-инфраструктуры для противодействия атакам хакеров.

Запустили в мае 2024 года

PT NGFW — высокопроизводительный межсетевой экран нового поколения.

Запустили в ноябре 2024 года

PT Knockin — симулятор атак на корпоративную почту для проверки ее защищенности. Продукт за две минуты проверяет, как работают почтовые средства защиты — антивирусы, почтовые шлюзы, песочницы, выдает вердикт о безопасности и формирует рекомендации по улучшению их работы.

Запустили в апреле 2024 года

PT Dephaze — продукт для тестирования на проникновение в автоматическом режиме. Основан на многолетнем опыте Компании в проведении пентестов и знаниях о том, как защищаться от киберугроз.

Продукт доступен с марта 2025 года

PT Maze — сервис по защите мобильных приложений от реверс-инжиниринга.

Анонсировали запуск в марте 2025 года

PT Data Security — единое решение для защиты данных независимо от их типа и места хранения.

Запуск во втором полугодии 2025 года

1.4

Важные достижения года

Запустили **PT NGFW** — высокопроизводительный и надежный межсетевой экран нового поколения, который команда Positive Technologies разрабатывала два года.

- PT NGFW — самый производительный российский межсетевой экран нового поколения: более 300 Гбит/с в режиме L7-фильтрации и более 60 Гбит/с с включенными IPS, антивирусом и URL-фильтрацией, что подтверждено тестированиями в независимой лаборатории Bi.zone[1].
- PT NGFW — первый и пока единственный российский межсетевой экран нового поколения, сертифицированный по требованиям ФСТЭК России к многофункциональным межсетевым экранам уровня сети по четвертому классу защиты[2].
- Две наши аппаратные платформы вошли в единый реестр российской радиоэлектронной промышленности Министерства промышленности и торговли Российской Федерации (Минпромторг России). Программно-аппаратный комплекс (ПАК) PT NGFW на серверах YADRO внесен в единый реестр российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Также мы подали заявления на внесение в реестр ПАК PT NGFW на наших аппаратных платформах и серверах «Тринити».
- PT NGFW выбрали для защиты своей инфраструктуры не только субъекты критической информационной инфраструктуры (КИИ) — крупные финансовые организации, банки, муниципальные органы госуправления и др., но и коммерческие компании, чей выбор традиционно шире, так как не ограничен только российскими решениями.

Рекордный старт продаж

1,2 млрд руб.

всего за 1,5 месяца

Positive Technologies планирует занять не менее половины российского рынка NGFW

100 млрд руб.

наша оценка российского рынка NGFW

[1] Подробнее читайте в протоколе испытаний.
[2] Сертификат ФСТЭК России от 19 ноября 2024 года № 4877.

Нам доверяют защиту мероприятий федерального значения

Результаты работы Positive Technologies на «Играх Будущего»

- Автопилот MaxPatrol O2 впервые работал параллельно с экспертами и автоматически собирал и анализировал все активности в инфраструктуре фиджитал-турнира.
- Технология подтвердила свою зрелость, способность автоматизировать процессы обнаружения действий злоумышленников и их пресечение.

Продукты, которые мы использовали для защиты:

MaxPatrol O2, MaxPatrol SIEM, MaxPatrol EDR, MaxPatrol VM, PT NAD, PT Sandbox, PT Application Firewall

«Игры Будущего»

Positive Technologies выступила ключевым партнером по кибербезопасности первого международного мультиспортивного фиджитал-турнира «Игры Будущего», который прошел с 21 февраля по 3 марта 2024 года в Казани. «Игры Будущего» — это масштабное событие, объединяющее реальный и киберспорт, где классические дисциплины переплетаются с цифровыми, создавая уникальный формат соревнований.

«

Последствия успешных кибератак на инфраструктуру такого крупного мероприятия, как «Игры Будущего», могли бы поставить под удар возможность качественного проведения турнира в непрерывном режиме. Кроме того, они сказались бы на репутации события. Принципы результативной кибербезопасности, а также средства ИБ, многократно проверенные в боевых условиях, позволили нам минимизировать риски атак и создать защищенную среду для организаторов и гостей турнира. Мы рады, что подход Positive Technologies оказался близок и нашим коллегам из сферы фиджитал-спорта.

Алексей Новиков,
Управляющий директор Positive Technologies

425 инцидентов

145 успешных атак

112 уязвимостей

12 критических событий

21 страна

42

международные команды

Международная кибербитва Standoff на ПМЭФ-2024

В 2024 году международная кибербитва Standoff стала частью программы Петербургского международного экономического форума (ПМЭФ). В киберучениях участвовали 42 международные команды. За четыре дня они познакомились с разными инструментами защиты и техниками кибератак, протестировали свои стратегии, а также обменялись знаниями, чтобы в будущем перенести этот опыт на повседневную работу.

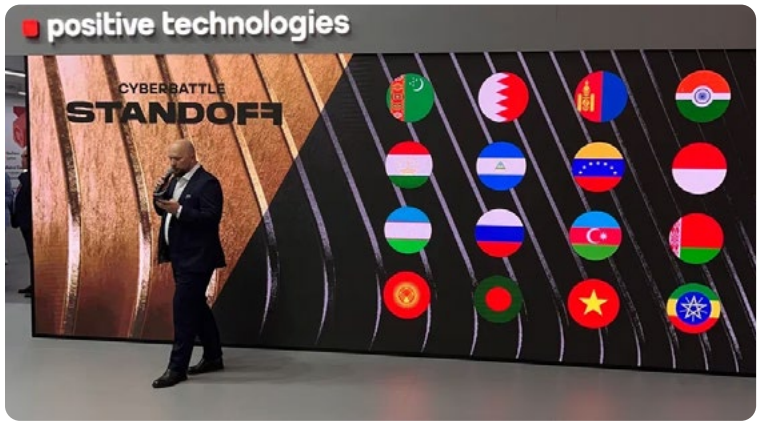
За время киберучений команды защитников обнаружили 425 инцидентов и расследовали 145 успешных атак. Команды атакующих обнаружили 112 уязвимостей и реализовали 12 критических событий.

Всего в кибербитве Standoff на ПМЭФ-2024 приняли участие представители 21 страны, в том числе группы реагирования (CERT) и независимые эксперты и руководители функциональных направлений бизнеса в качестве наблюдателей.

«

Такой международный обмен очень важен, потому что у киберпреступности нет национальности, и сообщество исследователей безопасности не должно замыкаться в границах своих стран. Нужно сообща противостоять этому глобальному вызову.

Алексей Новиков,
Управляющий директор Positive Technologies



138 тыс. посетителей

137 тыс. онлайн-зрителей

400 докладов

500 спикеров

Positive Hack Days 2: городской киберфестиваль в «Лужниках»

С 23 по 26 мая 2024 года спортивный комплекс «Лужники» в Москве стал центром кибербезопасности — здесь прошел международный киберфестиваль Positive Hack Days 2. В течение четырех 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. В профессиональной части выступили более 500 спикеров, которые представили свыше 400 докладов по самым актуальным темам. Обсуждались методы противодействия хакерским атакам и способы реагирования на инциденты, новые техники и векторы атак, эксплуатация уязвимостей, разработка и защита приложений, а также технологии машинного обучения и их безопасность.

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 138 тыс. человек посетили открытую зону, а свыше 137 тыс. зрителей следили за мероприятием онлайн.

>250 зарубежных гостей

из 22 стран

Positive Hack Days 2 стал важным международным событием: впервые на киберфестивале присутствовало более 250 зарубежных гостей, потенциальных партнеров и клиентов, представляющих 22 страны. Это подчеркнуло растущий интерес к передовым решениям в области кибербезопасности и укрепило позиции Positive Technologies на мировой арене.

В рамках Positive Hack Days 2 прошел Молодежный день, где школьники и студенты узнали больше о профессии и возможностях карьеры в сфере кибербезопасности. Кроме того, мы провели День инвестора, предоставив акционерам возможность лично пообщаться с руководством Компании и задать интересующие вопросы.

В 2024 году киберфестиваль вышел за пределы Москвы и проходил в Санкт-Петербурге, Нижнем Новгороде, Иннополисе, а также в Бангкоке в рамках PHDays x HITB Bangkok Hub.

Международное присутствие

36 команд

415 критических атак

Расследование **182** успешных атак

851 инцидент

Кибербитва Standoff 13

Одним из самых главных событий Positive Hack Days 2 стала кибербитва Standoff 13 — масштабное противостояние хакеров и защитников в виртуальном государстве. На киберполигоне была воссоздана инфраструктура реального мира: финансовые организации, транспортные сети, промышленные предприятия и госучреждения.

В ходе кибербитвы команды атакующих пытались найти уязвимости, чтобы проникнуть в ключевые системы и нарушить работу критически важных объектов — от финансовых учреждений до транспортной и энергетической инфраструктуры. В это же время защитники работали над тем, чтобы предотвратить атаки, минимизировать последствия и сохранить стабильность виртуального мира. Впервые в этом году были задействованы сразу два виртуальных государства, что добавило противостоянию еще больше динамики и неожиданных сценариев.

Standoff 13 стала самой масштабной кибербитвой за всю историю. В состязании приняли участие 36 команд — 25 атакующих и 11 защитников (рекордное количество) из пяти стран: России, Малайзии, Франции, Беларуси и Казахстана.

За три дня основного этапа кибербитвы команды атакующих провели 415 критических атак и выявили 617 уязвимостей в инфраструктуре виртуальных государств. Команды защитников расследовали 182 успешные атаки и зафиксировали 851 инцидент, доказывая свою способность противостоять реальным угрозам.

Все события кибербитвы отображались на физическом макете, позволяя зрителям в реальном времени увидеть, как кибератаки могут привести к сходу поездов с рельсов, вызвать аварии на дорогах или спровоцировать техногенную катастрофу и повлечь серьезные последствия для экологии.

Кибербитва Standoff вновь продемонстрировала, что кибератаки — это не что-то абстрактное, а вполне реальные угрозы, способные затронуть экономику, экологию, безопасность городов и нарушить устойчивое развитие общества. Этот уникальный формат не только позволяет моделировать кибератаки в условиях, максимально приближенных к реальности, но и помогает формировать базу знаний, что способствует усилению экспертности наших специалистов и совершенствованию продуктов Positive Technologies.

5 тыс. участников

Молодежный день на Positive Hack Days 2

Молодежный день на Positive Hack Days 2 открыл мир кибербезопасности для тысяч студентов и школьников. 25 мая он одновременно прошел в четырех городах — Москве, Санкт-Петербурге, Нижнем Новгороде и Иннополисе, собрав более 5 тыс. участников.

На площадках «Лужников», ИТМО, Университета Иннополис и других молодежных центров гости узнали, как построить карьеру в сфере кибербезопасности. Представители ведущих ИТ-компаний поделились полезными советами, рассказали о возможностях стажировок и актуальных вакансиях.

Важной частью программы стали воркшопы и интерактивные задания, где участники смогли попробовать себя в роли белых хакеров, специалистов по киберзащите и безопасной разработке. Вместо формальных лекций студентам и школьникам предлагалось решать реальные задачи и определить, какое направление подходит каждому.

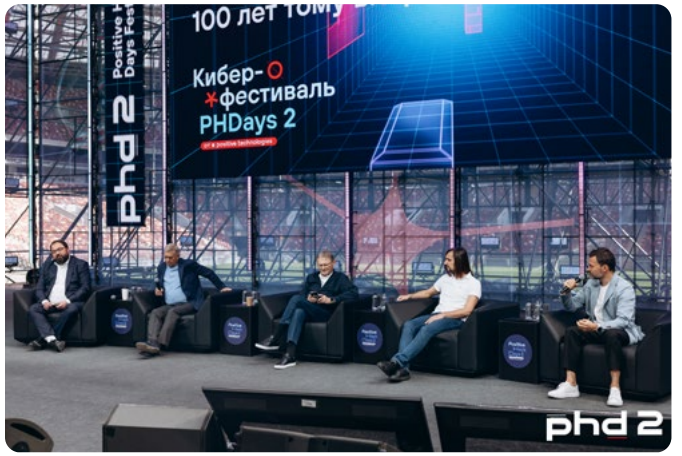
Positive Hack Days является не просто местом встречи профессионалов, а мощным инструментом для развития нашего бизнеса и расширения его возможностей. Мероприятие способствует повышению узнаваемости бренда, укреплению наших позиций лидера на рынке, привлекает новых клиентов и экспертов, что в долгосрочной перспективе положительно сказывается на стоимости акций и на доходах акционеров.

Для чего мы проводим Positive Hack Days

В 2024 году Positive Hack Days проходил уже в 13-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, ориентированным только на 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. Однако из-за ограниченного пространства площадка не смогла вместить всех желающих, поэтому в 2024 году мы пошли дальше и провели киберфестиваль в «Лужниках».



Positive Education — центр обучения Positive Technologies, где практики обучают результативной кибербезопасности

Главные результаты Positive Education в 2024 году

- Открыли новое направление корпоративного обучения
- Запустили международный интенсив для молодых специалистов из стран БРИКС — Positive Hack Camp
- Провели обучение для 5787 компаний в России и 179 компаний в мире (Бразилия, ОАЭ, Мексика, Индонезия)
- Более 60 компаний прошли индивидуальные корпоративные образовательные программы по повышению киберустойчивости организации

Positive Education: развитие результативной кибербезопасности через обучение

С 2023 года мы обучаем компании построению результативной кибербезопасности. Создаем корпоративные программы, усиливаем команды, развиваем культуру кибербезопасности и готовим специалистов, которые способны действовать эффективно в условиях реальных киберугроз.

Наша цель — сократить дефицит квалифицированных кадров и помочь компаниям выстраивать устойчивую и управляемую кибербезопасность.

Основные направления

Наши образовательные программы охватывают весь спектр задач кибербезопасности — от подготовки специалистов до обучения руководителей.

01

Корпоративные программы для бизнеса
Повышаем киберустойчивость организаций через развитие людей. Усиливаем команды, вовлекая в кибербезопасность и развивая необходимые компетенции специалистов.

02

Образовательные программы для профессионалов
Создаем современные программы для специалистов, стремящихся расти в сфере кибербезопасности.

03

Практические тренажеры и продукты для автономного обучения
Разрабатываем симуляционные среды, в которых можно отрабатывать действия в условиях, приближенных к реальности, и учиться в удобном темпе.

04

Программы для управленцев
Помогаем топ-менеджерам выстраивать стратегический подход к ИБ: от понимания рисков до интеграции киберустойчивости в систему управления бизнесом.

05

Курсы по эксплуатации продуктов Positive Technologies
Обучаем клиентов и партнеров эффективной работе с решениями Positive Technologies, чтобы технологии приносили максимальную пользу.

Positive Education

Инициативы

Мы создаем условия для устойчивого роста экспертизы в области кибербезопасности — через развитие людей и партнерства в разных странах.

Сотрудничество с вузами

Развиваем партнерство с 70 вузами в России и за ее пределами. Разрабатываем и проводим учебные программы совместно с преподавателями ведущих университетов: «СберУниверситет», ИТМО, МФТИ, Университет Иннополис, «Сириус».

Подготовка преподавателей по кибербезопасности

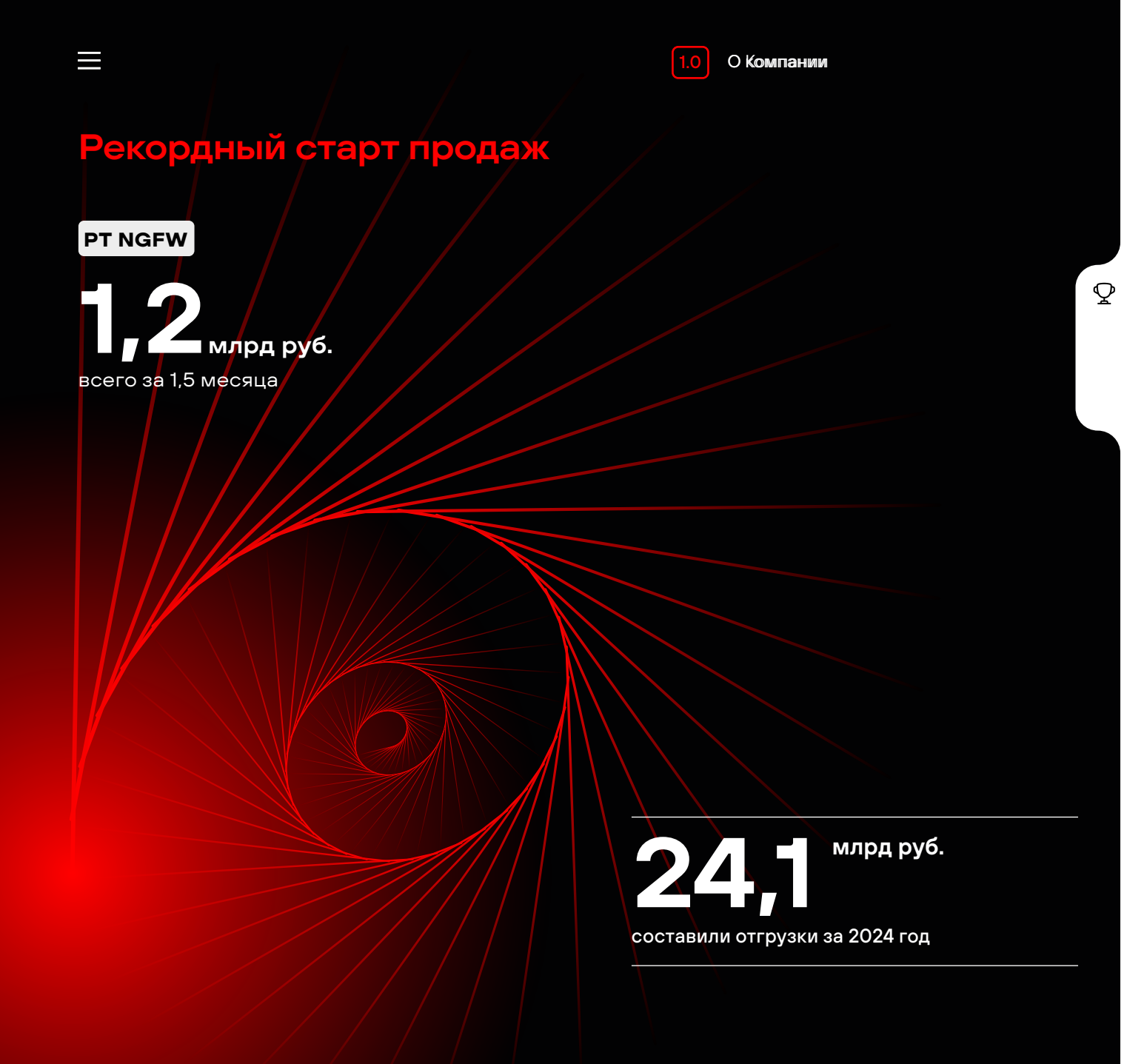
Учим преподавателей вузов, колледжей и школ передовым практикам кибербеза и повышаем качество образовательной системы страны

- При поддержке Минцифры России запущен проект обучения преподавателей — Школа преподавателей по кибербезопасности (ШПК).
- Более 1,7 тыс. преподавателей подали заявку на участие в ШПК и в данный момент продолжают свое обучение.
- С 2024 года проект реализуется в партнерстве с МГТУ им. Н. Э. Баумана.

Международное развитие

Ежегодно проводим интенсивы для молодых специалистов в кибербезе из стран БРИКС.

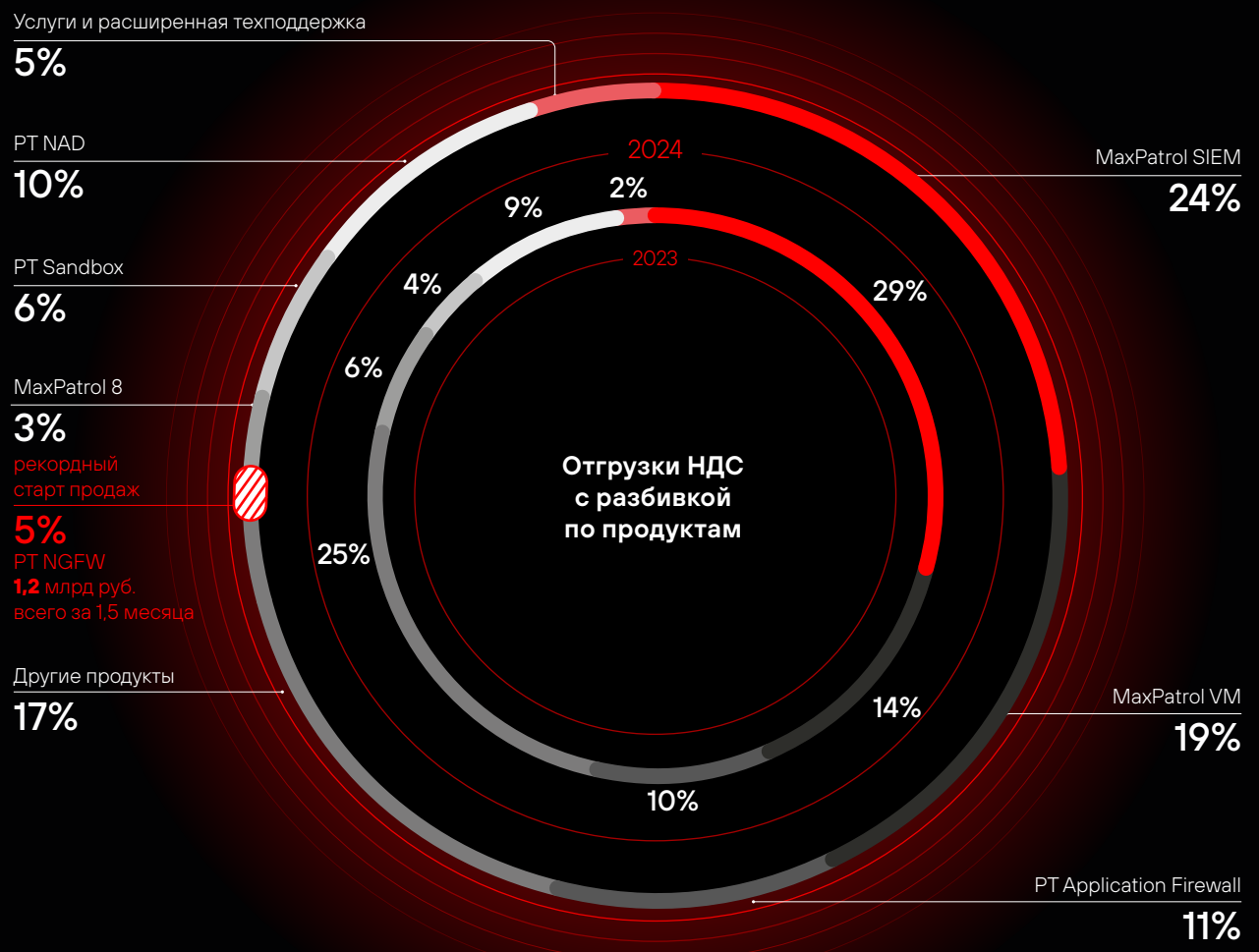
- Развиваем специалистов для индустрии кибербеза в Индонезии (сотрудничаем с университетом SGU, Джакарта) и в ОАЭ (на базе Amity University, Дубаи).
- Positive Hack Camp — международный образовательный проект по кибербезопасности, в котором приняли участие более 70 специалистов из 20 стран мира.
- Positive Hack Talks — международные встречи с локальными сообществами специалистов в области кибербезопасности, объединяющие более 200 участников.



Отгрузки за 2024 год

Итоговый объем оплаченных отгрузок клиентам Компании в 2024 году составил 24,1 млрд руб., что существенно ниже прогнозов и ожиданий менеджмента. Причины расхождения фактических результатов с планами Компании в основном обусловлены внутренним фактором.

В рамках трансформации, которая началась еще в IV квартале прошлого года и во многом уже завершена, Positive Technologies ставит перед собой ключевую цель на 2025 год — вернуться к темпам роста бизнеса, превышающим общую динамику рынка.



Продукты на миллиард

Объем отгрузок шести наших продуктов, а также расширенной технической поддержки преодолел 1 млрд руб.

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

1.5

Привлекательность для инвесторов

MOEX

Expert

АКРА

SMART-LAB.RU

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

- Входим в основные индексы Мосбиржи: IMOEX и РТС
- Регулярно раскрываем финансовую и управленческую отчетность
- Входим в субиндекс пенсионных накоплений
- Акции торгуются в первом котировальном списке
- Высокий рейтинг кредитоспособности — «ruAA» («Эксперт РА»), «AA(RU)» (АКРА)
- Лидер в IR-рейтинге от SMART-LAB, включающем более 200 эмитентов
- Средний объем торгов составил 747 млн руб., показав рост в 7,7 раза в сравнении с первым годом
- Входим в индексы Мосбиржи (широкого рынка, ИТ, малой и средней капитализации, инноваций)
- Наша следующая цель — стать новой голубой фишкой

1.6

Наша география

Россия остается для нас приоритетным рынком, но мы также стремимся занять ключевые позиции на международной арене кибербезопасности. Офисы Positive Technologies работают в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске и Томске. В 2023 году наша первая команда начала работу в ОАЭ, а в 2024 году наши эксперты появились и в других регионах мира. Этот год стал для нас первым полноценным этапом активного развития международного бизнеса в новых геополитических условиях. Мы значительно расширили ресурсы Компании, чтобы эффективно поддерживать проекты зарубежных партнеров и заказчиков, работающих в удаленных регионах и не говорящих на русском языке.

Для Positive Technologies, уже состоявшейся компании на российском ИТ-рынке, смена фокуса с привычных клиентов внутри страны и спроса, вызванного импортозамещением, на удаленные и пока еще не освоенные рынки стала серьезным вызовом. Это потребовало пересмотра подходов, процессов и приоритетов. В 2024 году мы активно работали над укреплением позиций в наших фокусных регионах, наращивали присутствие и адаптировали стратегии под новые условия.

В 2024 году мы значительно укрепили партнерскую сеть: к концу года около 200 локальных дистрибьюторов и интеграторов рассмотрели возможности сотрудничества с Positive Technologies, протестировали наши решения и сосредоточились на обучении своих специалистов. Эти партнеры готовы к совместной работе в 2025 году, что закладывает прочную основу для дальнейшего развития международного бизнеса.

200

партнеров-дистрибьюторов и интеграторов к концу 2024 года

Первые успехи в международных проектах

- Получены референс-проекты в ОАЭ, Катаре, Саудовской Аравии, Тунисе, Египте, Иране, Индонезии, Малайзии, во Вьетнаме и в Мексике.
- Основной спрос — PT NAD, PT Application Inspector, профессиональные сервисы по оценке кибербезопасности.
- MaxPatrol 10, AF Pro и новый NGFW также были выбраны заказчиками.

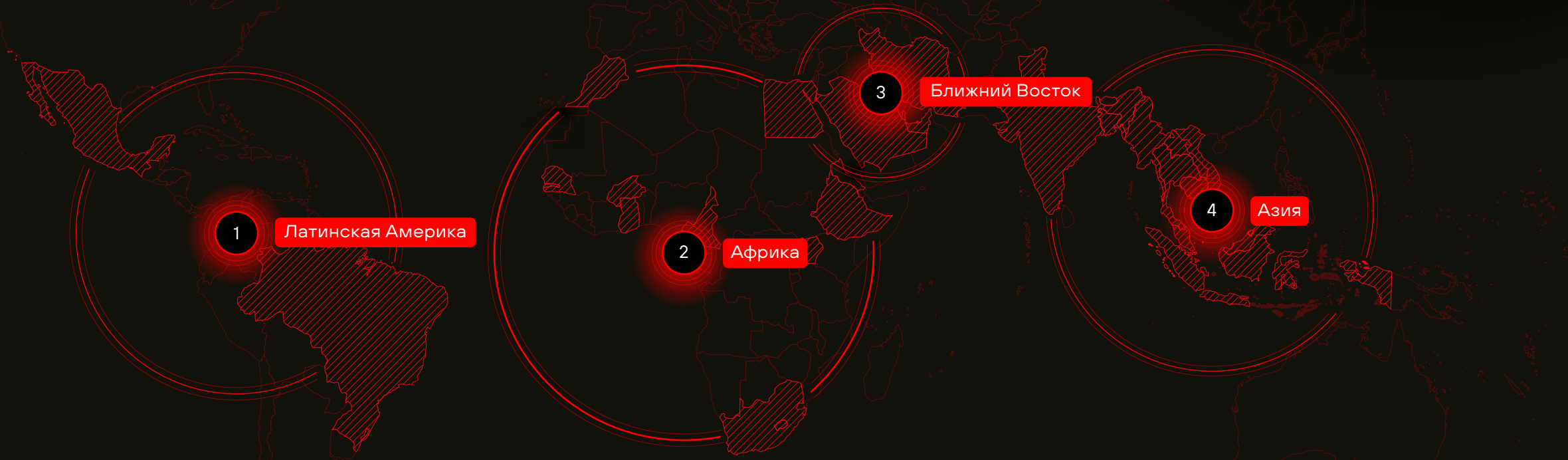
Международные мероприятия

- Positive Hack Days в Москве — более 250 иностранных участников.
- Признание в OIC-CERT благодаря участию Malaysia Cybersecurity в Standoff на Positive Hack Days 2.

Расширение международной команды
У нас появились первые пресейл-инженеры и сейлы в локациях, которые помогают заказчикам общаться с нами на родном языке в удобное время и в очном формате.

Расширение сотрудничества с вузами
SGU, MSU (Индонезия), Amity University (ОАЭ) выбрали Positive Technologies в качестве экспертного партнера по программам подготовки специалистов в сфере кибербезопасности.

Фокусные регионы



1 Латинская Америка
Бразилия, Мексика

2 Африка

3 Ближний Восток
Саудовская Аравия, ОАЭ, Египет

4 Азия
Индонезия, Малайзия, Индия

1.7 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

- 23 года опыта в исследованиях и разработке.
- Организуем ключевые события в профессиональной среде ИБ:
  - Positive Hack Days — ежегодный фестиваль по 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

>500
партнеров — ведущих интеграторов

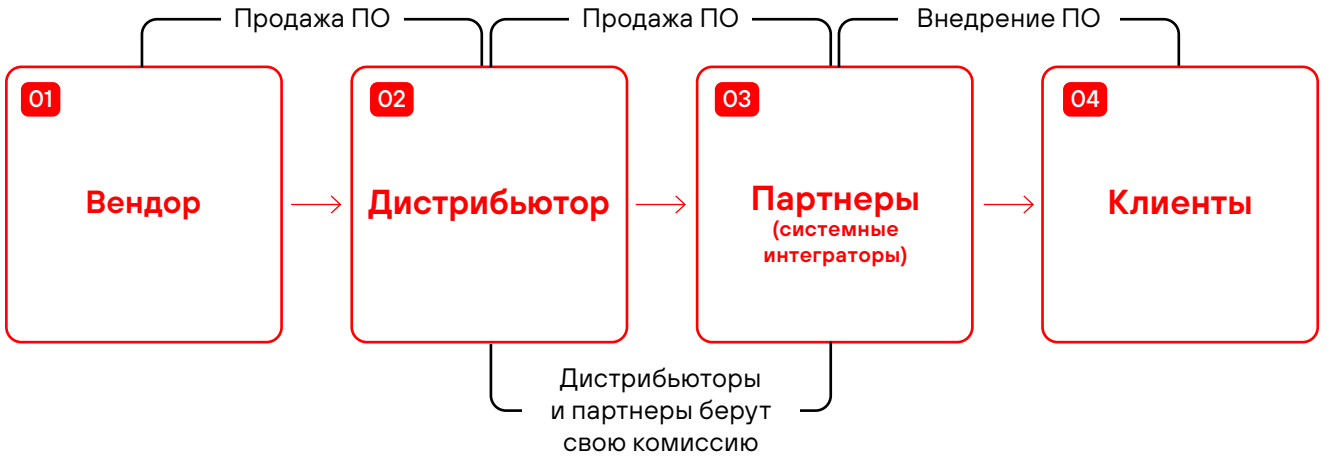
Сильная команда

Ведущие эксперты отрасли и ключевые спикеры в сфере ИБ

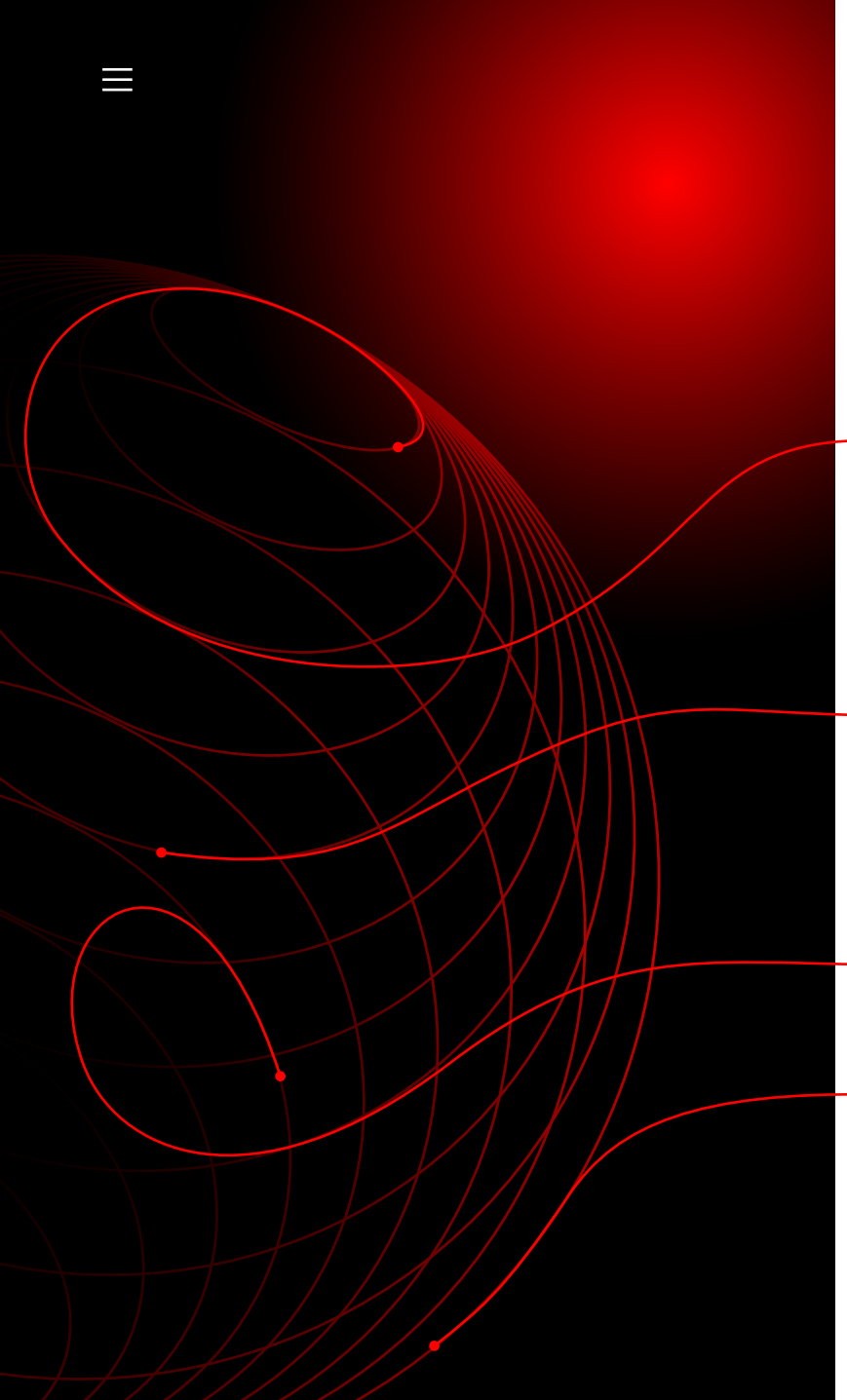
>3100
сотрудников[1]

[1] Данные на декабрь 2024 года.

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 ПО ушедших с рынка зарубежных вендоров

Для общества

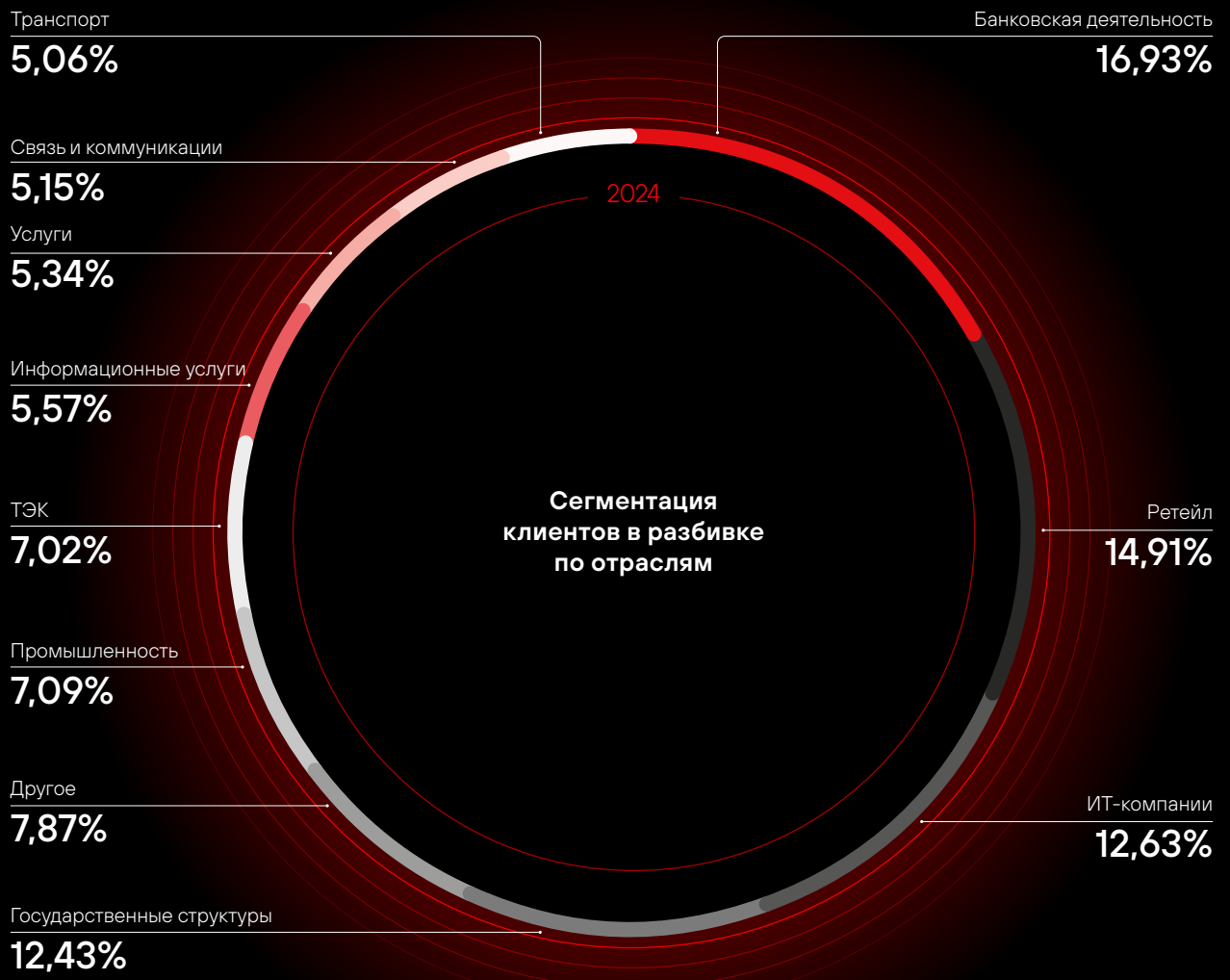
- Обеспечиваем цифровую безопасность страны и цифровой суверенитет
- Защищаем государственные структуры и частные компании, в том числе объекты КИИ, не позволяя злоумышленникам нарушить производственные процессы, вызвать перебои в поставках продовольствия, спровоцировать экологическую катастрофу и привести 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

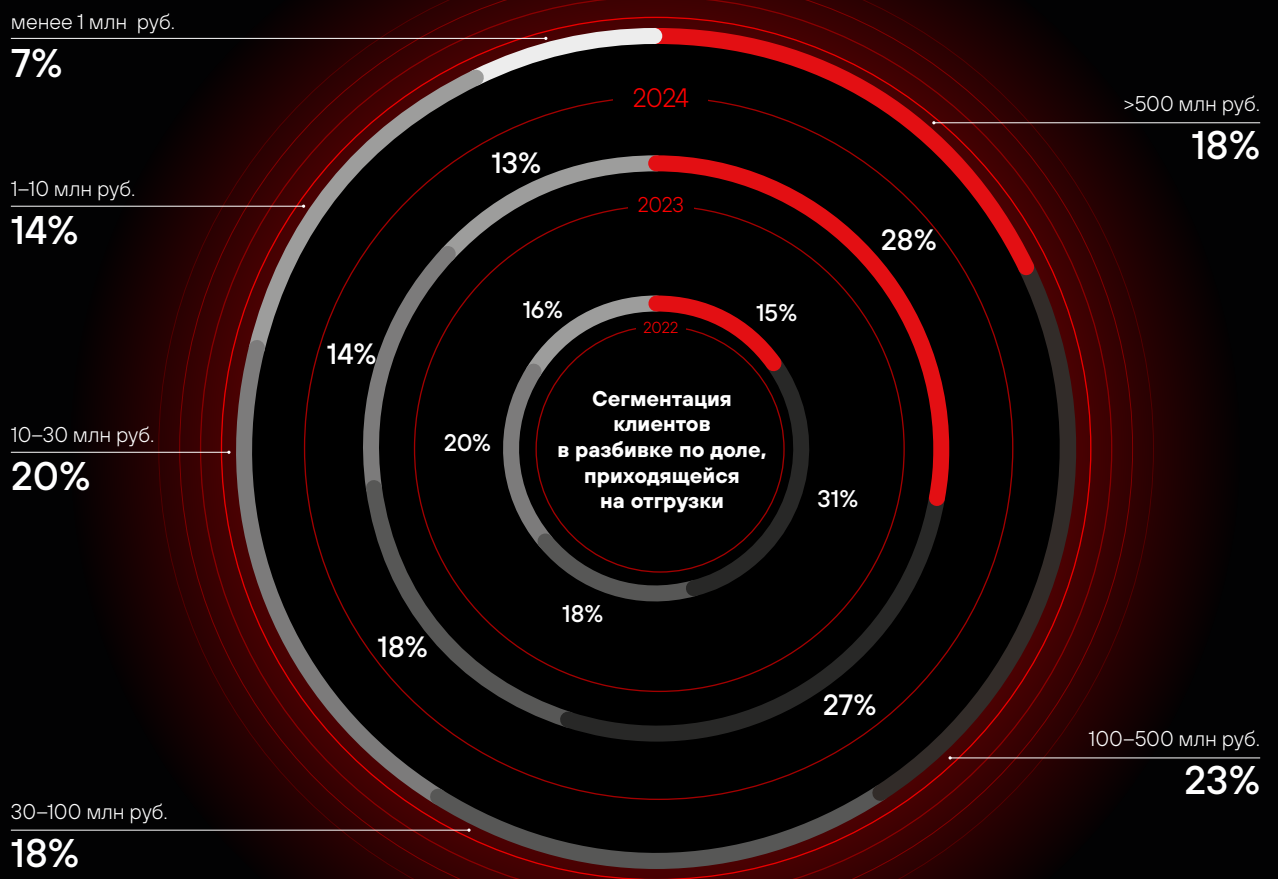
- Восходящая голубая фишка
- Принимаем меры для обеспечения роста капитализации Компании
- Стремимся к регулярной выплате дивидендов
- Делаем наш бизнес и отчетность прозрачными и доступными, формируя новые стандарты работы с инвесторами



1.7

Наши клиенты

Мы помогаем крупным компаниям из всех ведущих отраслей российской экономики. Среди наших клиентов банки (16,93%), ретейл (14,91%), ИТ-компании (12,63%), государственные структуры (12,43%), а также промышленные компании (7,09%). Широкая диверсификация клиентской базы способствует стабильному развитию бизнеса и укреплению позиций Компании.



Диверсификация клиентской базы

Активный рост в сегменте малого и среднего бизнеса

Мы реализуем крупные проекты по построению результативной кибербезопасности.

79 %

доля отгрузок целевому сегменту крупных корпоративных клиентов в 2024 году

Цель на 2025 год

Каждый год мы активно увеличиваем количество наших заказчиков. Это новый мощный вектор развития бизнеса.

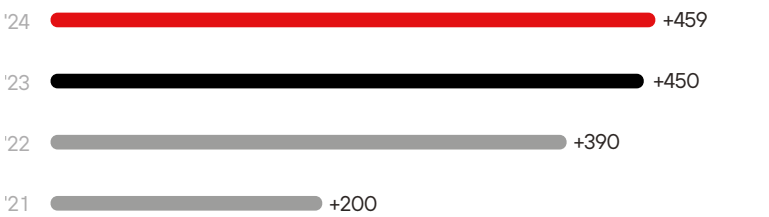
~1,6 тыс.

новых клиентов — цель на 2025 год

Это новый мощный вектор развития бизнеса. По итогам 2024 года к нам присоединилось 459 новых клиентов, а в 2025 году мы ставим перед собой цель привлечь около 1,6 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.

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

Покрытие RAEX-600

Покрытие топ-4000 компаний

Стратегический обзор

2.1

Обращение Генерального директора

Уважаемые совладельцы, клиенты, партнеры!

Этим Отчетом мы подводим итоги 2024 года. Для Positive Technologies минувший год заложил хороший фундамент для роста в будущем, однако финансовые результаты за 2024 год не оправдали наших ожиданий. Фактический результат по отгрузкам оказался существенно ниже наших прогнозов, при этом EBITDA и чистая прибыль остались в положительной зоне. Вместе с тем любые кризисные ситуации — это возможность трезво оценить имеющиеся ресурсы, выявить и устранить причины текущих и будущих проблем, пересобраться и уверенно продолжить двигаться в направлении роста бизнеса и повышения эффективности.

Примерно полгода назад мы обнаружили признаки существенного расхождения фактических результатов с нашими планами и начали анализировать ситуацию, чтобы выявить причины, исправить данный разрыв на текущем этапе и не допускать его в будущем. Мы пришли к выводу, что основные причины — внутренние, а потому исправимы.

В рамках трансформации, которая началась еще в прошлом году и во многом уже завершена, мы ставим перед собой следующие ключевые цели на 2025 год. Во-первых, планируем вернуться к темпам роста бизнеса, превышающим общую динамику рынка. Во-вторых, мы пристально проанализировали бизнес-перспективы каждого направления и скорректировали гипотезы, позволяющие выйти на таргетируемые темпы роста выручки. Параллельно с этим мы приняли более консервативный подход к расходам и формированию бюджета, что позволит нам в перспективе вернуться также и к целевым нормам рентабельности чистой прибыли.

За прошлый год к нам пришло около 1 тыс. новых сотрудников, а за предыдущие два года Компания выросла практически вдвое. После такого экстенсивного роста пришло время для пересборки и анализа результатов каждого подразделения: важно посмотреть вглубь, перенастроить и трансформировать ряд процессов и функций.

В результате этой трансформации мы хотим выйти на плановый рост бизнеса и иметь возможность выплатить дивиденды акционерам по итогам 2025 года. С этой целью Максим Филиппов, Заместитель Генерального директора, вновь возьмет на себя ответственность за продажи на всех рынках присутствия Компании, включая российский периметр. В свою очередь, вся Компания берет на себя жесткие обязательства по повышению эффективности и сдерживанию роста расходов. В то же время мы проследим, чтобы действия Компании не оказывали давления на капитализацию в этом году.

За последние полгода мы уже значимо продвинулись в процессах внутренней трансформации: провели реформу R&D и Центра компетенций, ввели новую роль CPO (продуктовых директоров). В ходе изменений важно сохранить нашу ключевую способность — создавать прорывные продукты и держать фокус на стратегических гипотезах роста Компании. Разработанный в короткие сроки межсетевой экран нового поколения PT NGFW

продемонстрировал рекордный объем отгрузок в 1,2 млрд руб. всего за 1,5 месяца продаж в 2024 году, что подтверждает нашу готовность создавать инновационные продукты мирового уровня. В конце года мы анонсировали решение PT Dephaze, позволяющее запускать автоматические пентесты и без привлечения очень редких специалистов визуализировать способность компаний противостоять хакерским атакам. Кроме того, с запуском нового решения PT Data Security Компания выходит на новый для нее рынок защиты данных.

Positive Technologies движется к максимально полному технологическому портфелю, который включает и технологии защиты конечных устройств. С этой целью мы приобрели долю в белорусской компании «ВИРУСБЛОКАДА». Ее технологии, направленные на обнаружение вредоносной активности, будут интегрированы в наши продукты, а затем появится самостоятельное решение. С этим приобретением, а также с учетом наличия уже работающего решения MaxPatrol EDR мы получаем все необходимое для закрепления на рынке защиты конечных устройств.

В 2024 году Positive Technologies продолжила развивать направление метапродуктов (интеллектуальных решений для комплексной кибербезопасности с минимальным участием человека). Первый продукт этой линейки — MaxPatrol O2 — уже работает в инфраструктуре крупных компаний и начал генерировать выручку. В прошлом году под управлением всего одного специалиста MaxPatrol O2 обнаружил и остановил международную хакерскую группировку у одного из крупных клиентов. Мы также запустили второй метапродукт, MaxPatrol Carbon, который помогает подготовить ИТ-инфраструктуру к отражению атак и обеспечивает непрерывный контроль киберустойчивости, делая невозможным причинение ущерба компании.

За прошлый год мы научились создавать фундамент результативной кибербезопасности в рекордно короткие сроки: за полгода наши клиенты строят ядро своей защиты и выходят на кибериспытания для непрерывной оценки реальной защищенности компании. Мы опробовали подход на заказчиках из разных сфер и в 2025 году будем масштабировать этот опыт с партнерами-интеграторами, чтобы вместе вывести защищенность отраслей на новый уровень.

Мы продолжаем выход на международный рынок: Компания успешно протестировала ряд бизнес-гипотез и определила перспективные регионы, где рассчитывает на достижение значимых результатов в ближайшей перспективе. Наша культурная экспансия в мире вышла на новый уровень. Киберфестиваль Positive Hack Days стал по-настоящему международным: в 2024 году его посетили около 140 тыс. человек, в том числе более 250 зарубежных гостей, партнеров и потенциальных клиентов из 22 стран. Мы впервые провели масштабный Positive Hack Camp для зарубежных специалистов по ИБ в Москве и серию митапов в Индии, во Вьетнаме и в Египте.

Важно отметить, что мы вместе с партнерами продолжаем работать над созданием предложения на страновом уровне, которое включало бы возможность предложить целым государствам способы их защиты от кибератак и построения цифрового суверенитета. Такая идея в нынешних реалиях в мире находит отклик у партнеров из дружественных стран, которые стремятся выстроить безопасную цифровую среду, нарастить способности противостоять атакам на ключевые объекты инфраструктуры и предотвратить недопустимые для них события.

Мы считаем очень важным оставаться компанией, привлекательной для талантливых людей, способных создавать прорывные продукты. Именно поэтому продолжаем развивать концепцию совладения, параметры которой были разработаны в сотрудничестве с инвестиционным сообществом и акционерами Компании. В конце 2024 года завершился ее очередной этап: мы вознаградили акциями Компании около 1,9 тыс. контрибьюторов за вклад в рост нашего бизнеса. Мы благодарны всем за этот диалог, который позволил найти консенсус между задачей развития бизнеса и интересами всех совладельцев, которые вносят свой вклад в изменение будущего кибербезопасности.

Спасибо, что вы с нами!

С уважением,
Денис Баранов,
Генеральный директор Positive Technologies

2.2

Обзор рынка

Кибербезопасность продолжает оставаться одной из наиболее значимых и востребованных отраслей в России, особенно на фоне стремительной цифровизации и растущей необходимости импортозамещения. Все больше компаний осознают критическую важность защиты данных и бизнес-процессов, уделяя этому направлению приоритетное внимание.

2024 год стал важным этапом развития результативной кибербезопасности. В условиях ограниченных ресурсов бизнес вынужден тщательнее подходить к вопросам своей деятельности, оценивая не только действия, но и их эффективность. В сфере кибербезопасности это переосмысление приводит к акценту на достижении конкретного результата. Компании начинают сосредотачиваться на выявлении событий, которые представляют наибольшую угрозу для бизнеса, и выстраивании защиты, направленной на их предотвращение.

Российский рынок

В 2024 году рынок кибербезопасности рос медленнее, чем предполагалось. Изначально Центр стратегических разработок прогнозировал, что среднегодовой темп роста (CAGR) для российских вендоров достигнет 32%. Однако позже этот показатель был скорректирован до 20–25%. По оценке Positive Technologies, реальный рост оказался еще более умеренным и составил всего 10–15%.

Замедление темпов роста связано со следующими факторами.

- В течение года наблюдалось сокращение бюджетов в области ИТ и цифровизации. Компании начали пересматривать свои расходы через призму их реальной экономической или социальной эффективности. Увеличение ключевой ставки сделало кредиты дороже, что вынудило бизнес сосредоточиться на краткосрочных задачах, обеспечивающих быструю отдачу. Такая ситуация повлияла на решения организаций о финансировании долгосрочных проектов, в том числе в сфере кибербезопасности.
- Процесс импортозамещения шел медленнее, чем ожидалось. На рынке не появилось достаточного количества отечественных решений, которые могли бы полноценно заменить зарубежные аналоги. Это привело к пересмотру планов внедрения новых технологий и сокращению связанных с этим бюджетов.

Факторы роста

Рост российского рынка кибербезопасности в 2024 году был обусловлен рядом факторов. Одним из главных стало ускорение процессов импортозамещения. Российские компании перестали рассчитывать на возвращение иностранных вендоров, а действие лицензий на ранее закупленные программные продукты завершилось. Более того, использование зарубежного ПО стало рискованным: обновления могут содержать программные закладки, а отсутствие поддержки свыше двух лет приводит к накоплению уязвимостей, способных открыть доступ злоумышленникам. Эти угрозы уже реализовались в некоторых госорганах и госкорпорациях, что дополнительно подстегнуло спрос на отечественные решения.

Другим важным фактором стал рост числа кибератак. Российские компании фактически превратились в испытательные полигоны для новых видов кибероружия и тактик. Это обстоятельство вынудило разработчиков сосредоточиться на практической кибербезопасности, уходя от формального выполнения регуляторных требований к реальной защите.

В конце года на рынок начала влиять еще одна тенденция — введение оборотных штрафов за утечку персональных данных. Этот шаг по аналогии с событиями 2008 и 2012 годов может стать стимулом для улучшения защиты в 2025 году. Штрафы особенно сильно повлияют на средний бизнес, который будет активнее инвестировать в кибербезопасность. Малые компании, напротив, сталкиваются с нехваткой ресурсов для таких вложений, а крупные игроки, вероятно, предпочтут минимизировать риски через юридическое сопротивление и затягивание разбирательств.

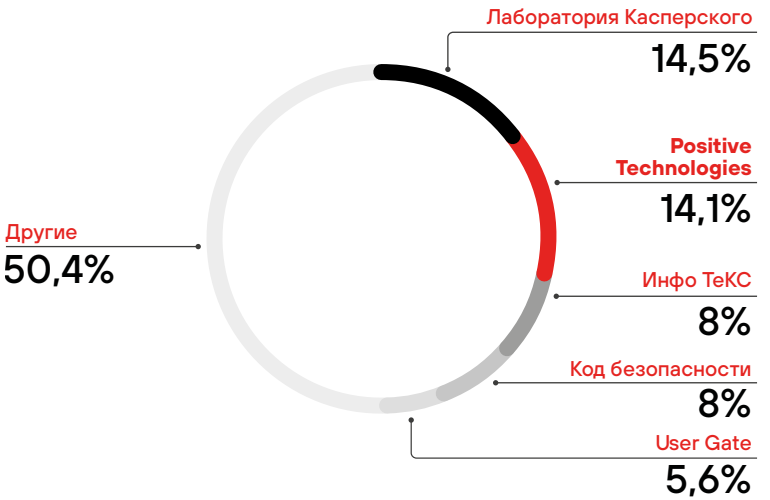
[1] По оценкам Positive Technologies

10–15 %

рост российского рынка кибербезопасности в 2024 году[1]

По итогам 2023 года на рынке средств защиты информации (СЗИ) обозначились два лидера — «Лаборатория Касперского» и Positive Technologies. Эти компании занимают схожие доли рынка, значительно опережая остальных участников. При этом динамика изменений демонстрирует разнонаправленные тенденции: доля «Лаборатории Касперского» на рынке постепенно снижается (–1,5 п. п. за год), в то время как доля Positive Technologies растет (+1,7 п. п. за год).

Доли вендоров средств защиты информации на рынке по результатам 2023 года



23,6 %

Среднегодовой темп прироста рынка ближайшие пять лет[2]

Прогноз: ускорение роста

Российский рынок кибербезопасности продолжает демонстрировать устойчивую динамику роста, опережающую мировые показатели. По данным аналитиков «Центра стратегических разработок» (ЦСР), CAGR рынка в ближайшие пять лет составит 23,6%. Ожидается, что к 2028 году объем рынка достигнет 715 млрд руб., при этом более 95% составят решения российских вендоров.

270–300 млрд руб.

объем рынка кибербезопасности в России[3]

Эксперты Positive Technologies отмечают, что в 2025 году рынок продолжит сохранять умеренные темпы роста, а интерес к решениям в области кибербезопасности останется стабильным. Однако наиболее заметный скачок в развитии отрасли прогнозируется на 2026 год, когда спрос на отечественные решения может значительно усилиться на фоне продолжающихся процессов импортозамещения и ужесточения требований к защите данных.

Анализ рынка

1 По оценкам Positive Technologies.
2 По оценкам Positive Technologies и ЦСР.
3 Исследование российского рынка кибербезопасности ЦСР.

Мировой рынок

Мировой рынок кибербезопасности демонстрирует уверенный рост, и эксперты прогнозируют его дальнейшее развитие в ближайшие годы. По оценкам Statista, к 2025 году объем рынка может достичь 203 млрд долл. США, причем наибольшую долю займут услуги в сфере безопасности с прогнозируемым объемом 103,1 млрд долл. США. Среднегодовой темп прироста с 2025 по 2029 год составит 7,58%, что приведет к увеличению объема рынка до 271,9 млрд долл. США к концу этого периода.

Аналитики Precedence Research отмечают, что в 2023 году объем рынка составлял 238,13 млрд долл. США, а в 2024 году он увеличится до 268,13 млрд долл. США. Согласно прогнозам, к 2034 году рынок кибербезопасности может достичь рекордной отметки 878,48 млрд долл. США. Среднегодовой темп прироста за десятилетие с 2024 по 2034 год оценивается в 12,6%, что подчеркивает стремительное развитие отрасли и возрастающий спрос на решения в области защиты от киберугроз.

Консалтинговая компания Mordor Intelligence приводит похожие оценки: к 2025 году объем рынка составит 234,01 млрд долл. США, а к 2030 году достигнет 424,14 млрд долл. США. Среднегодовой темп прироста в период с 2025 по 2030 год оценивается в 12,63%.

Основными драйверами роста остаются растущая угроза кибератак, включая атаки на критическую инфраструктуру, и увеличивающийся спрос на облачные и ИИ-ориентированные решения. Важное место в кибербезопасности занимают аналитика данных и технологии машинного обучения, которые позволяют компаниям оперативно реагировать на угрозы. Среди наиболее перспективных сегментов — защита облачных решений, а также управление доступом и идентификацией (IAM).

Особое внимание уделяется защите критически важной инфраструктуры, где сложность угроз и их потенциальный ущерб требуют внедрения инновационных стратегий. В то же время все больше компаний фокусируются на создании проактивных и адаптивных систем, которые обеспечивают защиту данных и цифровых активов.

Рост рынка также стимулируется усилением нормативного регулирования в области кибербезопасности. Компании инвестируют в комплаенс-решения, чтобы соответствовать новым требованиям и минимизировать риски.

В регионах присутствия Positive Technologies наблюдается высокий спрос на надежные решения кибербезопасности, что способствует активному росту рынка.

Ближний Восток

На Ближнем Востоке краеугольным камнем является защита критической инфраструктуры от целевых атак. Регион продолжает сталкиваться с изощренными кибератаками, а усиливающиеся со стороны киберпреступников угрозы создают значительные финансовые и репутационные риски для бизнеса. Одним из основных драйверов роста сектора кибербезопасности в регионе также является необходимость соблюдать требования законодательства, регуляторов и соответствовать общемировым фреймворкам.

Растущей угрозой кибератак все больше обеспокоены и в Индонезии, особенно по мере того, как в стране растет число цифровых платформ и сервисов. Региональные инциденты включают в себя утечку данных, использование программ-вымогателей[1], фишинг[2] и более изощренные атаки, такие как advanced persistent threats (APT)[3].

Индия

Для Индии наиболее актуальные задачи кибербезопасности связаны с защитой от утечек конфиденциальной информации (70% от общего числа кибератак на организации) и обеспечением непрерывности бизнес-процессов (к нарушению основной деятельности организаций приводило 13% атак). Высокий темп цифровизации в стране, сопровождающийся ростом количества кибератак (+15% в 2023 году по сравнению с 2022 годом), делает защиту данных и информационных систем первоочередной задачей.

Отрасль кибербезопасности в Индии движется в сторону комплексных решений, объединяющих различные технологии защиты. Учитывая рост инвестиций в цифровизацию, включая облачные технологии и искусственный интеллект, ожидается повышенный спрос на решения для защиты облачных сред, систем IoT[5] и инфраструктуры, связанной с ИИ.

Латинская Америка

В Латинской Америке в настоящее время ощущается острая нехватка специалистов по ИБ — за кибербезопасность отвечают в основном ИТ-службы компаний, поэтому на рынке востребована кибербезопасность как услуга и бизнес MSSP[4] растет очень быстро.

Африка

Глобальные тренды в области кибербезопасности на Африканском континенте — создание SOC[6] и автоматизация процессов. Кроме того, в связи с распространением интернета, развитием телекоммуникационных сетей, а также внедрением цифровых платформ и услуг актуальной для региона является защита веб-ресурсов. Другое востребованное направление — это облачная безопасность, так как крупные игроки предпочитают развертывать облачную инфраструктуру. Уделяют внимание и подготовке национальных кадров по ИБ. Эксперты прогнозируют в регионе рост интереса к автоматизации центров мониторинга кибербезопасности и наращиванию локальной экспертизы, укрепление международного сотрудничества по ведению общей нормативной базы и обмену успешными практиками, а также развитие образовательных инициатив по подготовке профильных специалистов.

1 Программа-вымогатель — вредоносное ПО, которое при проникновении в компьютер шифрует все файлы в ключевых разделах, предлагая затем владельцу заплатить за восстановление доступа к ним.
2 Фишинг (Phishing) — метод мошенничества, когда злоумышленник пытается получить доступ к личной информации, такой как пароли, номера банковских карт и другие конфиденциальные данные, путем подделки электронных сообщений, сайтов, приложений и других форм интернет-коммуникации.
3 APT-атака — это длительная, целенаправленная и скрытая кибератака, при которой злоумышленники получают доступ к информационным системам и остаются незамеченными, чтобы собрать конфиденциальные данные или нанести другой ущерб.
4 MSSP (Managed Security Service Provider) — это внешняя компания (провайдер), которой делегировано управление средствами защиты информации.
5 IoT (Internet of Things, рус. — интернет вещей) — концепция сети передачи данных между физическими объектами («вещами»), оснащенными встроенными средствами для взаимодействия друг с другом или с внешней средой.
6 SOC (Security Operations Center, рус. — 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, для того чтобы как можно оперативнее выявить и устранить угрозу ИБ.

Технологические тренды 2024 года и прогнозы на 2025

2024 год стал годом значительных изменений в подходах к кибербезопасности. Positive Technologies выделила несколько ключевых трендов, которые сформировали повестку рынка и определили направления его развития.

Результативная кибербезопасность

2024 год ознаменовался новым этапом в развитии концепции результативной кибербезопасности. В условиях ограниченных ресурсов бизнес вынужден подходить к вопросам защиты более осознанно, оценивая каждое действие с точки зрения его эффективности. Это переосмысление приводит к концентрации усилий на определении действительно значимых для бизнеса событий и формированию систем защиты, направленных на их предотвращение.

Такой подход не только оптимизирует затраты, но и создает условия для стратегического планирования в области информационной безопасности. Вместо попыток «закрыть все возможные уязвимости», компании делают акцент на критически важных аспектах, минимизируя риски, способные нанести серьезный ущерб.

По данным Positive Technologies, в России растет число компаний, внедряющих эту концепцию. Одной из причин стало то, что с 2022 года страна стала крайне привлекательной целью для киберпреступников, которые стремятся нарушить бизнес-процессы жертв.

Наши достижения результативной кибербезопасности

В отчетном году Positive Technologies перешла к практической реализации концепции результативной кибербезопасности в российском бизнесе и государственных организациях.

На финальной стадии реализации находятся четыре крупных проекта, направленных на повышение уровня защиты. Благодаря экспертной поддержке Positive Technologies наши клиенты получают опыт построения результативной кибербезопасности: как эффективно взаимодействовать с ИТ-функцией и усиливать инфраструктуру, в каких приоритетах развертывать сенсоры и средства защиты, как защищать периметр и компенсировать то, что по объективным причинам защитить невозможно.

> В этом году мы реализовали наш подход к обеспечению киберзащиты, став ключевым партнером по кибербезопасности первого международного мультиспортивного турнира «Игры будущего». Кроме того, Rambler&Co запустила программу APT Bug Bounty (кибериспытания), в которой независимые исследователи безопасности проверяют возможности для реализации недопустимых событий, чтобы проверить киберустойчивость ИТ-систем организации.

Как мы развиваем подход к измерению эффективности ИБ

Positive Technologies активно развивает подходы к измерению эффективности ИБ. Одним из ключевых инструментов в этом направлении стала программа APT Bug Bounty (кибериспытания), которая проходит на платформе Standoff 365. Компания уверена, что такие практики станут стандартом индустрии ИБ.

Целью результативной кибербезопасности является достижение уровня киберустойчивости, при котором злоумышленникам становится невыгодно атаковать инфраструктуру компании за предложенное вознаграждение. Развитие ИБ, таким образом, направлено на повышение этого порога, что достигается благодаря усилению инфраструктуры, внедрению сенсоров для отслеживания действий злоумышленников и совершенствованию процессов реагирования на инциденты. Это требует комплексного подхода — от укрепления (харденинга) инфраструктуры до выстраивания механизмов раннего обнаружения угроз. Одним из этапов построения результативной кибербезопасности должно быть создание такого периметра, который можно взломать только через уязвимости нулевого дня[1] или с помощью методов социальной инженерии[2].

В 2024 году Positive Technologies проделала большую работу, создавая сбалансированный подход к обеспечению кибербезопасности с измеримым результатом (невозможности реализации недопустимых событий). Компания активно вовлекала партнеров, чтобы продвигать эту концепцию на рынок и адаптировать ее к реальным вызовам и задачам бизнеса.

[1] Уязвимость нулевого дня — уязвимость, о которой еще не знают разработчик, производители антивирусов и пользователи.
[2] Социальная инженерия — психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации.

Ассортимент доступных технологий и потребности рынка

В 2024 году на российском рынке кибербезопасности наблюдалось смещение интереса компаний от сложных инфраструктурных решений, требующих длительного внедрения, к продуктам и сервисам, которые позволяют быстро выявлять уязвимости и оценивать киберустойчивость.

К числу наиболее востребованных технологий относятся:

- системы анализа трафика (NTA) — помогают выявлять подозрительную активность в сети;
- межсетевые экраны нового поколения (NGFW) — являются популярным решением на фоне программ импортозамещения;
- превентивная защита почты — решает задачи здесь и сейчас.

Интерес к NGFW подогревается как государством, так и профессиональным сообществом. За последний год число вендоров в этом сегменте выросло в несколько раз, хотя количество качественных продуктов остается ограниченным. В результате на российском рынке возникла перенасыщенность NGFW-решениями. По оценкам, до 35% рынка приходится на продукты этого сегмента, что превышает мировые показатели. Многие компании пытаются занять эту нишу, но сталкиваются с жесткой конкуренцией со стороны крупных игроков. Как результат, менее успешные вендоры будут вынуждены покинуть рынок.

В центре внимания: защита данных и инфраструктуры

Рост числа утечек данных в 2024 году стал катализатором изменений в подходах к защите информации. Становится очевидным, что классические решения, такие как DLP[1], не справляются с современными угрозами.

Компании обращаются к машинному обучению, которое позволяет:

- автоматизировать поиск мест хранения данных;
- проводить их классификацию;
- мониторить попытки несанкционированного доступа.

Существенный рост наблюдается и в сегменте средств защиты приложений. Среди них классические решения, такие как WAF[2] или защита от DDoS-атак[3]. К сегменту относятся также средства безопасной разработки, анализа защищенности и управления уязвимостями. Технологии позволяют правильно реализовать процесс разработки ПО, снизив в нем число уязвимостей, а следовательно — и риски.

Одновременно растет спрос на защиту инфраструктуры. К данному сегменту относятся:

- средства автоматизации и управления инцидентами
- решения по мониторингу событий ИБ;
- платформы сбора и обогащения данных об угрозах.

Дефицит технологий

Несмотря на активное развитие технологий, российский рынок сталкивается с нехваткой решений в нескольких важных направлениях.

Наблюдается дефицит аппаратных решений, что связано с санкциями против отечественной микроэлектроники и сложностями в логистике из Китая и Тайваня. Также на рынке не хватает продуктов для реализации популярной концепции Zero Trust[4] и комплексных инструментов для защиты современных средств коммуникации — от электронной почты до мессенджеров

Не хватает и технологий для защиты искусственного интеллекта, который активно внедряется в государственное управление и бизнес-процессы. Из-за этого остаются без должного контроля доступ к внешним LLM[5] и возможные утечки данных. Несмотря на развитие этой темы в мире, ярко отраженное в программе крупнейшей выставки ИБ RSA Conference, в России похвастаться успехами в этом направлении пока не получается.

К числу острых пробелов рынка можно отнести и решения класса GRC[6], которые необходимы для автоматизации результативной кибербезопасности. Особенно востребованы инструменты вроде новых дашбордов для бизнеса, калькуляторов рисков и потерь, а также систем оценки зрелости процессов.

[1] DLP (Data Leak Prevention) — специализированное ПО, предназначенное для защиты компании от утечек информации.
[2] WAF (Web Application Firewall) — специализированное ПО, которое предназначено для защиты веб-приложений от различных уязвимостей и угроз.
[3] DDoS-атака — распределенная атака типа «отказ в обслуживании», которая является одной из самых распространенных и опасных сетевых атак. В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов.
[4] Zero Trust — концепция безопасности, которая опирается на идею, что никому нельзя доверять по умолчанию. Вместо того чтобы доверять сетям и устройствам внутри компании, Zero Trust предполагает проверку идентичности и авторизацию для доступа к любому ресурсу, а также непрерывный мониторинг действий пользователя.
[5] LLM (large language model, рус. — большая языковая модель) — это языковая модель, состоящая из нейронной сети со множеством параметров (обычно миллиарды весовых коэффициентов и более), обученной на большом количестве неразмеченного текста с использованием обучения без учителя.
[6] GRC (Governance, Risk and Compliance, рус. — управление, риски и соответствие требованиям) — это структурированный способ согласования ИТ с бизнес-целями при управлении рисками и соблюдением всех отраслевых и государственных норм. Оно включает в себя инструменты и процессы, позволяющие объединить управление организацией и управление рисками с технологическими инновациями и их внедрением.

Безопасность станет неотделимым свойством

Одной из долгосрочных тенденций становится внедрение безопасности как неотделимого свойства технологий. Уже сейчас на рынке появляются продукты, сочетающие промышленные и ИТ-решения с встроенной безопасностью. Это напоминает подход, применяемый в разработке ПО, где безопасность интегрируется в процесс разработки. В настоящее время этот тренд только формируется, но он обусловлен жизненной необходимостью и имеет шансы стать одним из ключевых в ближайшем будущем.

Роль ИИ

Искусственный интеллект продолжает укреплять свои позиции, становясь одной из ключевых технологий будущего. Несмотря на то что эта тема уже кажется широко обсуждаемой, интерес к ней только растет: все больше организаций углубляются в изучение и применение ИИ. Существует высокая вероятность, что в ближайшие годы появятся специализированные компании, сосредоточенные исключительно на разработке решений в области ИИ для кибербезопасности и информационных технологий. Эти игроки будут задавать новые стандарты и формировать направления развития отрасли, предлагая инновационные подходы к защите данных и инфраструктуры.

Защита производства

Безопасность производства становится одной из ключевых тем для рынка кибербезопасности, особенно в контексте защиты низовой автоматики. Традиционные подходы к ИБ начинают активно распространяться на новые ниши, включая защиту систем автоматизированного управления технологическими процессами (АСУ ТП).

В условиях продолжающейся цифровизации промышленности появляются новые продукты и платформы, базирующиеся на микросервисных моделях. Эти решения требуют пересмотра принципов их защиты, что открывает огромные перспективы для развития концепций безопасности промышленного производства.

Эта тенденция не только формирует новую нишу для кибербезопасности, но и способствует созданию инновационных продуктов. Интеграция СЗИ с системами управления производством становится необходимостью, помогая минимизировать риски и предотвращать атаки на критически важные процессы.

Именно такие изменения на рынке помогут выстроить более надежные системы защиты, адаптированные под уникальные потребности промышленного сектора.

Багбаунти

Важным трендом 2024 года стал рост популярности багбаунти[1]. Эти программы, которые когда-то интересовали лишь крупные технологические компании, сегодня востребованы в самых разных секторах, включая страхование, логистику, госорганы и букмекерские конторы. В 2024 году багбаунти-платформы значительно расширили свои возможности, отвечая на возрастающий спрос. Positive Technologies прогнозирует удвоение числа компаний, запускающих такие программы, уже в 2025 году. Это связано с тем, что багбаунти предоставляет бизнесу измеримые и осязаемые результаты в области повышения кибербезопасности

Что российский бизнес думает о багбаунти

- Самый честный и эффективный способ проверить свою защищенность.
- Выйти на багбаунти легко, но нужны выстроенные процессы управления уязвимостями.
- Этичные хакеры помогают делать сервисы безопаснее.
- На багбаунти ты платишь не за время и бренд, а за результат.
- Кибериспытания (APT Bug Bounty на платформе Standoff BugBounty) — выбор тех, кто хочет проверить весь внешний периметр и оценить реальный уровень защищенности.
- Багбаунти — для самых умных и эффективных.

Киберполигоны

В 2024 году одним из ключевых трендов в сфере кибербезопасности стал растущий интерес к киберполигонам. Эти уникальные платформы дают возможность моделировать масштабные кибератаки, что в реальных условиях практически невозможно. Такой подход позволяет не только оценивать уязвимости, но и вырабатывать эффективные стратегии защиты в разрезе различных отраслей и государств.

Клиентов, в том числе зарубежных, в основном привлекают on-premise[2]-полигоны. При этом онлайн-версии по-прежнему остаются востребованными как основа для обучения. Компании заинтересованы в создании у себя в стране киберарен, на которых можно проверять цепочки событий и оценивать влияние атак на бизнес-процессы. При этом существующие зарубежные решения позволяют решать только единичные задачи.

С усложнением задач, связанных с моделированием действий множества подразделений и реализацией комплексных сценариев, спрос на гибридные и on-premise-решения продолжает расти. По текущим прогнозам, рынок киберполигонов в России находится в стадии активного формирования и крупные контракты ожидаются уже в 2025–2026 годах.

[1] Багбаунти — программа, с помощью которой пользователи могут получить вознаграждение за нахождение проблем в безопасности сервисов и приложений компании.
[2] On-premise — метод развертывания ПО или приложений, которые устанавливаются и функционируют на собственных серверах и инфраструктуре компании-заказчика.

ХардкорИТ

В 2024 году особое внимание уделялось практическим подходам к усложнению пути атакующих. Новый метод, известный как ХардкорИТ, предполагает трансформацию ИТ-инфраструктуры таким образом, чтобы замедлить продвижение киберпреступников в случае взлома. Такое решение обеспечивает дополнительный уровень защиты и повышает киберустойчивость организаций, делая их инфраструктуру более сложной для атак.

Что такое ХардкорИТ?

ХардкорИТ представляет собой методологию оценки киберустойчивости, основанную на математическом моделировании времени кибератаки (TTA). Концепция возникла как ответ на проблемы, выявленные при проведении пентестов, анализе защищенности и создании систем результативной кибербезопасности. ИТ-инфраструктура — это не только основа для бизнес-процессов, но и зона потенциальных угроз. Ее правильная настройка обеспечивает баланс между эффективностью поддержки бизнеса и возможностью противостоять атакам. Цель ХардкорИТ — достичь такого состояния, при котором время атаки превышает время ее локализации, что позволяет специалистам успешно предотвратить развитие инцидента.

Методология ХардкорИТ позволяет:

- оценивать достижимость целевых систем (TTA) злоумышленниками;
- определять маршруты атак и прогнозировать время до реализации недопустимых событий;
- анализировать параметры инфраструктуры и их влияние на общую киберустойчивость компании.

Практически в каждой компании пентесты выявляют одни и те же слабости в настройке инфраструктуры. За счет них злоумышленник может быстро преодолеть периметр организации, продвинуться к цели и реализовать недопустимое событие. ХардкорИТ помогает устранить такие проблемы, делая системы более устойчивыми к атакам.

Реакция бизнеса

Подход ХардкорИТ вызвал высокий интерес со стороны компаний. После каждого мероприятия, где обсуждаются принципы и результаты методологии, поступает множество запросов на ее применение. Бизнес видит в ХардкорИТ возможность:

- оценивать уровень киберустойчивости и формировать планы по его повышению;
- обосновывать проекты по усилению защиты инфраструктуры;
- мониторить и улучшать KPI служб ИБ.

ХардкорИТ в 2025 году

В 2025 году Positive Technologies продолжит продвижение ХардкорИТ на рынке. Прогнозируется значительное увеличение числа партнеров, которые будут предлагать услуги на основе методологии. Ожидается, что компании начнут активно применять ХардкорИТ для оценки и изменения своей ИТ-инфраструктуры, закладывая средства на эти проекты в бюджеты.

ХардкорИТ станет важной частью комплексных решений Positive Technologies по обеспечению результативной кибербезопасности. В Компании отмечают, что успешное построение защиты невозможно без взаимодействия с отделами ИТ, а методология ХардкорИТ служит эффективным инструментом для достижения этой цели.

Прогнозы на 2025 год: ИИ и экосистемы выйдут на первый план

В 2025 году перед отраслью будут стоять две основные задачи: повышение качества и функциональных возможностей продуктов, а также увеличение комплементарной ценности экосистемы, в которой все сервисы дополняют друг друга. Технологии, которые используются для решения первой задачи, зависят от самого продукта. Например, для повышения качества метапродуктов MaxPatrol Carbon и MaxPatrol O2 необходима оптимизация решения задач на графах и в структурах данных, для MaxPatrol EDR, PT NGFW и PT ISIM — новые эвристические и поведенческие подходы для обнаружения специфических классов атак (технологии сигнатурных методов обнаружения), ML-алгоритмы — для защиты от программ-вымогателей. Значительную роль будут также играть покрытие российских операционных систем, расширение охвата защищаемых типов ИТ-активов и интеграция с облачными поставщиками услуг посредством API.

Реализация второй задачи напрямую зависит от качества интеграции продуктов друг с другом. Для его повышения необходимы единый процесс развертывания ПО, который обеспечивается технологиями Docker и Kubernetes; легковесный агент; сквозные политики; централизованный мониторинг и вариативность конфигураций платформы.

Безусловным трендом 2025 года станут прорывные решения в области искусственного интеллекта. В первую очередь технологии будут применяться для частных задач — для работы с большими массивами данных, обнаружения киберугроз (здесь ожидаем появления новых поведенческих и сигнатурных методов) и расследования инцидентов. Свою роль ИИ сыграет и в решении глобальных вопросов. К ним относится, например, автоматизация работы центров мониторинга безопасности (SOC) — задача, которую уже сегодня можно решать с помощью больших языковых моделей.

Глобальные тренды: интеграция и новые классы решений

На мировом рынке востребованы интегрированные решения, которые объединяют продукты разных вендоров в единую экосистему. Особое внимание уделяется решениям XSPM (Security Posture Management), которые помогают мониторить уязвимости в «облаках», Kubernetes и других инфраструктурах. В России подобных технологий пока почти нет, что открывает возможности для их развития.

Еще один значимый тренд — ITDR (Identity Threat Detection and Response), который расширяет традиционные системы управления учетными записями до мониторинга всего их жизненного цикла. Учитывая важность этого направления, российским компаниям стоит обратить на него внимание.

Кроме того, на мировом рынке кибербезопасности активно развиваются платформенные решения на базе ИИ. Зарубежные компании внедряют инструменты безопасной разработки и автоматизируют проверки защищенности.

В ближайшие годы искусственный интеллект будет все эффективнее применяться и в разработке, у рынка вырастет интерес к интеграциям. В свою очередь, бурный рост числа импортозамещающих решений пойдет на спад. В целом рынок ИТ в России станет более зрелым, а вслед за ним и рынок ИБ.

2.3

Наша стратегия

Positive Technologies стремится к технологическому лидерству в кибербезопасности на мировом уровне, задавая тренды и определяя векторы развития индустрии. Мы расширяем границы традиционной информационной безопасности, создавая связи между ИБ и ИТ, формируем 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

- Укрепление лидерства на российском рынке через разработку инновационных продуктов
- Возвращение к высоким темпам роста за счет повышения эффективности бизнеса и улучшения операционных процессов
- Расширение присутствия на международных рынках

Наши стратегические приоритеты

01
Результативная кибербезопасность: мы делаем недопустимые события невозможными

02
Выпуск продуктов, имеющих конкурентное преимущество в мировом масштабе

03
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 2025 год Компания ставит перед собой конкретную финансовую цель — таргетируемый объем отгрузок в диапазоне 33–38 млрд руб. с плановым показателем 35 млрд руб.

33–35–38

Этот ориентир отражает наши амбиции по дальнейшему развитию бизнеса, укреплению позиций на рынке и расширению ключевых направлений.

При формировании гайденса 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.

Мы продолжаем следовать стратегии технологического лидерства, укрепляя доверие клиентов и партнеров. Наш приоритет — создание передовых решений и сервисов в сфере кибербезопасности, которые помогают бизнесу и государству справляться с современными вызовами.

Наши основные ресурсы — люди и технологии

Сильная и эффективная команда

В 2024 году Positive Technologies продолжила усиливать команду, укрепляя ключевые направления. Мы усилили Центр компетенций, куда пришли профессионалы с глубокой отраслевой экспертизой. Их знания и опыт позволяют Компании уверенно двигаться вперед, решая самые сложные задачи. Сформирована сильная команда продаж, появились новые ключевые роли, включая CPO, которых ранее в Компании не было.

За последние два года 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 продолжаем активно наращивать инвестиции в исследования и разработки (R&D), поскольку убеждены, что именно это обеспечит долгосрочное масштабирование бизнеса и укрепление позиций Компании на рынке кибербезопасности.

В 2024 году объем вложений в разработку новых продуктов, совершенствование существующих решений, а также в технологические и инфраструктурные проекты вырос на 82% по сравнению с прошлым годом, достигнув 9,1 млрд руб. Этот рост — стратегическая необходимость, поскольку инвестиции в технологии формируют будущие конкурентные преимущества Компании.

Мы уверены, что для динамично развивающейся ИБ-компании недоинвестирование в собственное развитие несет гораздо большие риски, чем временный дисбаланс между доходами и расходами. Финансовый разрыв можно компенсировать в моменте, но если упустить возможности для технологического рывка, то Компания теряет отложенную прибыль в будущем, которая кратно превышает текущие вложения.

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

Наши стратегические проекты

Проекты по построению результативной кибербезопасности

РКБ в 2024 году

Технологическая компания

Промышленная компания

Региональное Министерство цифрового развития

Банк

x2 Дополнительные продажи продуктов и услуг

Доверительные, партнерские взаимоотношения с заделом на будущее

Невозможно реализовать недопустимые события на 1–3 млн руб.

РКБ в 2025 году

Быстрый выход на новый уровень киберустойчивости

Определение фокусов | **Кибертрансформация** | **Кибериспытания**

Цель — в максимально короткие сроки обеспечить киберустойчивость для основных недопустимых событий и сформировать ядро безопасности для масштабирования и обеспечения такого состояния, при котором невозможно нанести критический ущерб компании клиента.

Наш метапродукт MaxPatrol O2 в 2024 году доказал свою эффективность в реальных условиях, став ключевым элементом проектов по построению результативной кибербезопасности. Продукт успешно выдержал атаки четырех сильнейших команд, участвовавших в кибербитве Standoff на PHDays, а также помог обеспечить надежную защиту международного фиджитал-турнира «Игры Будущего».

PT NGFW

PT NGFW — высокопроизводительное надежное решение мирового уровня для защиты бизнеса от кибератак.

- Самый производительный российский межсетевой экран нового поколения — более 300 Гбит/с в режиме L7-фильтрации и более 60 Гбит/с с включенными IPS, антивирусом и URL-фильтрацией, что подтверждено тестированиями в независимой лаборатории Bi.zone.
- Первый и пока единственный российский межсетевой экран нового поколения, сертифицированный по требованиям ФСТЭК к многофункциональным межсетевым экранам уровня сети по четвертому классу защиты (сертификат ФСТЭК № 4877 от 19 ноября 2024 года).

Стратегическая цель на 2025 год:
масштабирование отгрузок PT NGFW, а также расширение функционала продукта.

В ноябре 2024 года стартовали массовые отгрузки PT NGFW

1,2 млрд руб
объем отгрузок в 2024 году

260
отгруженных ПАК PT NGFW

- Первая международная продажа
- Самые крупные инсталляции для финансовой отрасли России и крупного продовольственного холдинга

>100
партнеров, в том числе региональных, включили решение в продуктовый портфель. Из них 46 приобрели ПАК NGFW в собственные демофонды

>500
проектов в воронке NGFW

44
российские и 1 зарубежная компания выбрали PT NGFW для защиты своей инфраструктуры

13 дней
самая быстрая продажа

PT Network Attack Discovery (PT NAD)

Продукт для обнаружения сложных сетевых атак и их расследования. Решение точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз. PT NAD знает, что искать в сети.

- Более 300 заказчиков используют PT NAD.
- Наши заказчики с помощью PT NAD нашли более 15 реальных инцидентов.
- В 2024 году выпустили два публичных релиза — 12.0 и 12.1.

Достигли функциональности, которой гордимся:

- увеличение максимальной скорости индексирования в три раза;
- появление пользовательских правил профилирования — нового механизма на основе машинного обучения;
- реализовали ML-алгоритм детектирования приложений в зашифрованном трафике.

PT NAD востребован на международной арене. Входит в топ-3 нашего торгового предложения.

>20

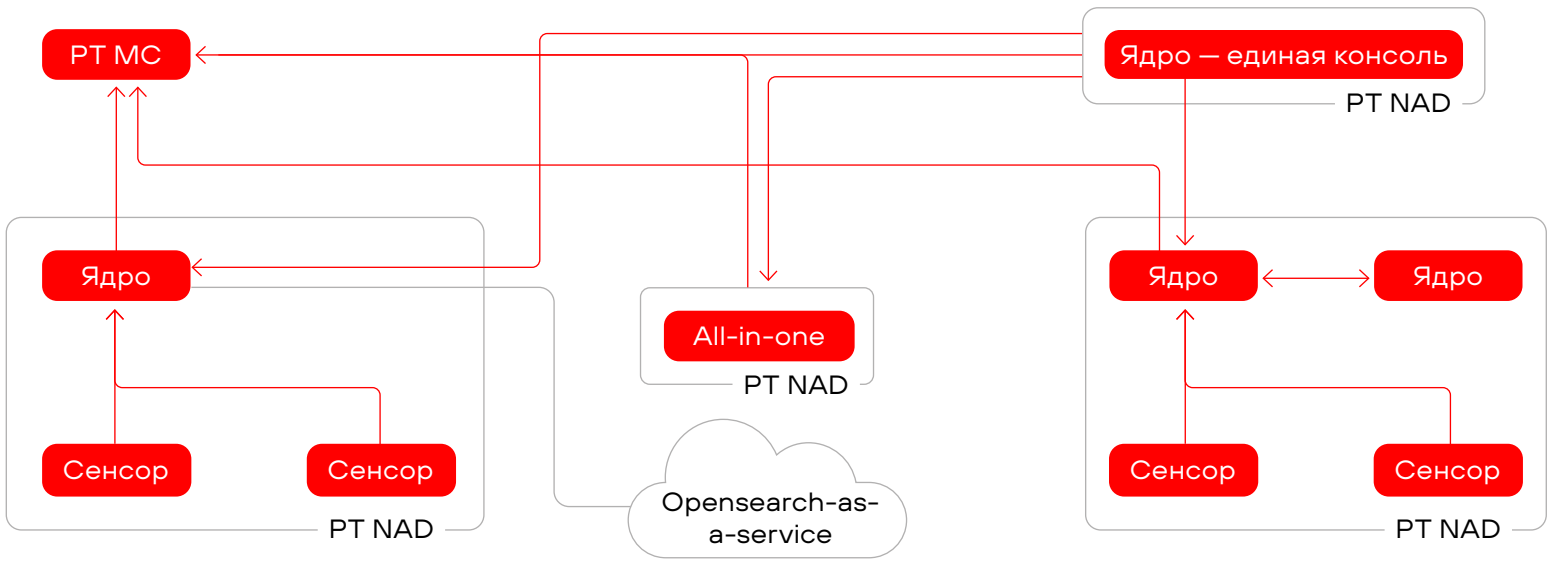
международных пилотных проектов было реализовано за год

3–5

из них находятся на финальной стадии и завершатся покупкой

PT NAD 12.2

Центральная консоль + хранение метаданных в облаке



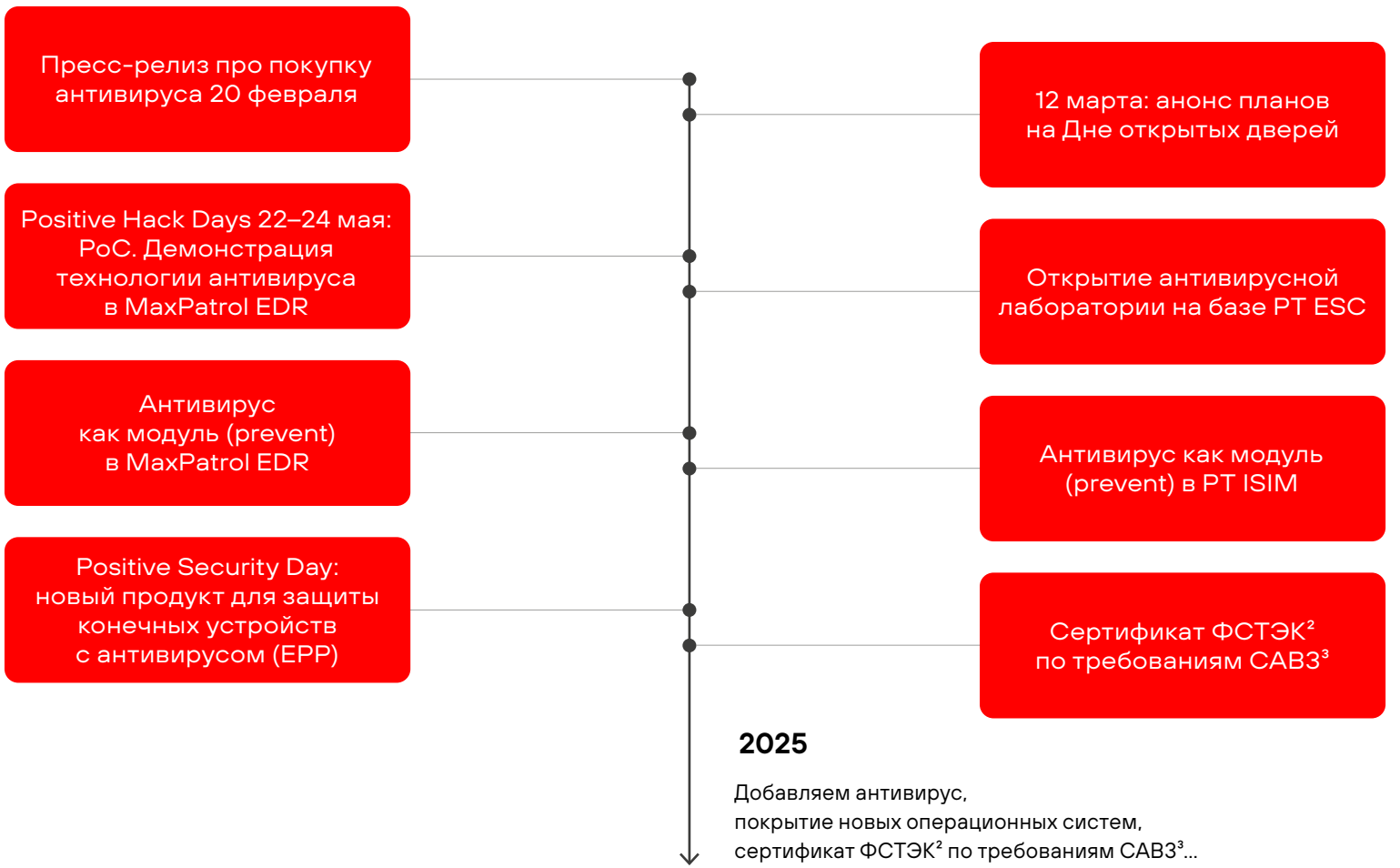
01 Появилась единая консоль, теперь нуже 1 эксперт на 1 клиента

02 Снимает требования к железу за счет облачного хранения

Стратегический вектор 2025 года:
кратное расширение присутствия в крупных холдингах, в том числе за счет продукта PT NAD.

Усиливаем направление защиты конечных устройств[1]

Positive Technologies активно расширяет ключевые направления. В конце 2024 года Компания приобрела долю белорусского вендора «ВИРУСБЛОКАДА», получив экспертизу сильной команды и исключительные права на продукты и технологии. Эти наработки будут интегрированы в решения MaxPatrol EDR, PT ISIM, PT Sandbox и PT NGFW, усиливая их функциональность и эффективность. Кроме того, Positive Technologies планирует выпуск собственного продукта класса EPP (Endpoint Protection Platform), что позволит расширить линейку решений в области защиты конечных устройств и повысить уровень кибербезопасности для клиентов.



[1] Компьютеры, ноутбуки, рабочие станции, серверы, смартфоны и другие мобильные устройства.
[2] Федеральная служба по техническому и экспортному контролю.
[3] Система сертификации средств защиты информации.

Positive Hack Days

Positive Hack Days — флагманское мероприятие Компании, которое является важным стратегическим инструментом развития нашего бизнеса. Это площадка, где собираются ведущие эксперты, укрепляются партнерства, расширяются возможности и растет узнаваемость бренда. Positive Hack Days привлекает клиентов из России и других стран, помогает продвигать продукты и оказывает прямое влияние на развитие бизнеса.
В 2025 году международный киберфестиваль Positive Hack Days пройдет 22–24 мая в Москве, в «Лужниках».

Международная экспансия

Наша цель — стать первым технологическим гигантом в сфере кибербезопасности с российскими корнями, который уверенно конкурирует с мировыми лидерами. Мы создаем продукты, способные отвечать самым высоким требованиям глобального рынка, и закладываем в них конкурентные преимущества с самого начала. Для нашей команды это не просто работа, а амбициозный вызов — разрабатывать решения, которые соответствуют мировым стандартам и формируют будущее кибербезопасности. Выход на международный уровень — стратегический шаг, который открывает новые возможности для роста и укрепления позиций Компании.

Positive Education

Обучение партнеров и клиентов важный стратегический инструмент масштабирования нашего бизнеса в России и за рубежом. Мы формируем программы по всей продуктовой линейке Компании, доступ к ним могут получить все партнеры и клиенты. Материалы программ регулярно обновляются, чтобы обучение охватывало весь спектр возможностей продуктов и соответствовало актуальным вызовам рынка. Мы создаем высокий уровень знаний в сфере кибербезопасности, который помогает сделать качественные продукты и решения в области ИБ востребованными, что способствует развитию нашего бизнеса.

Развитие команды ключевой приоритет Компании. Мы создаем условия, в которых сотрудники могут постоянно совершенствовать свои навыки, расти как специалисты и вносить вклад в развитие бизнеса. Экспертное обучение помогает им осваивать новые технологии, углублять знания и повышать квалификацию, что напрямую влияет на эффективность работы и конкурентоспособность Компании.

Фокус на эффективности в 2025 году

Пересмотрели подходы к управлению Компанией с точки зрения эффективности и целесообразности

Приостановили рост штата на уровне середины 2024 года

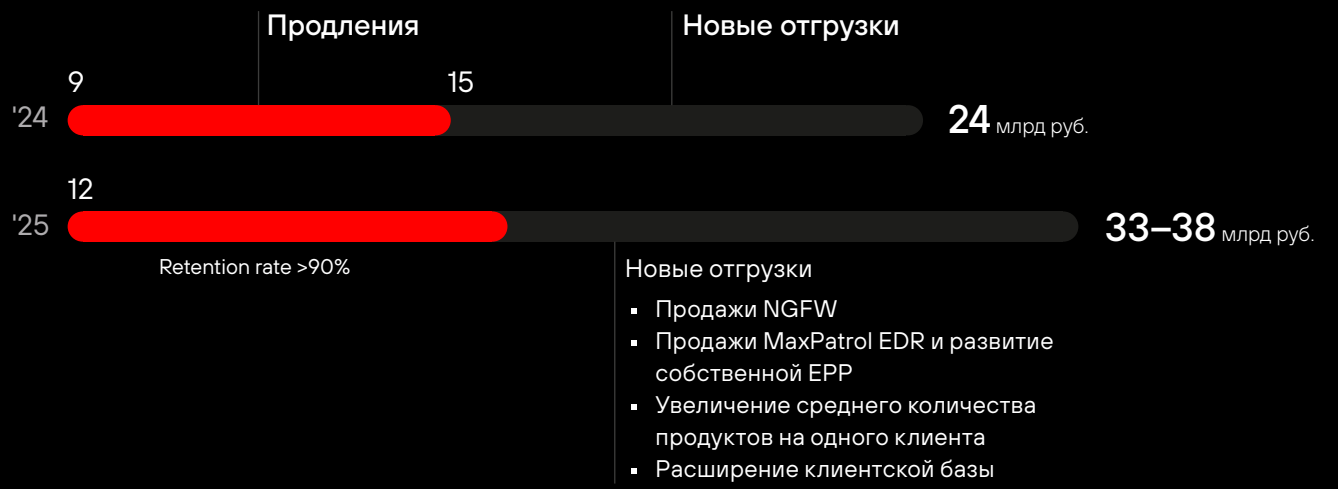
Взяли под жесткий контроль расходы (маркетинг, крупные мероприятия, инфраструктурные проекты; в меньшей степени — инвестиции в R&D)

ОСНОВНЫЕ ФИНАНСОВЫЕ ЦЕЛИ

Возвращение NIC в положительную зону

Возвращение к возможности выплачивать дивиденды

Продления и новые отгрузки в 2025 году



Новые отгрузки

- Продажи NGFW
- Продажи MaxPatrol EDR и развитие собственной EPP
- Увеличение среднего количества продуктов на одного клиента
- Расширение клиентской базы

Фокусные регионы

Латинская Америка
(Бразилия, Мексика)

Азия
(Индонезия, Малайзия, Индия и др.)

Ближний Восток
(Саудовская Аравия, ОАЭ, Египет)

Африка

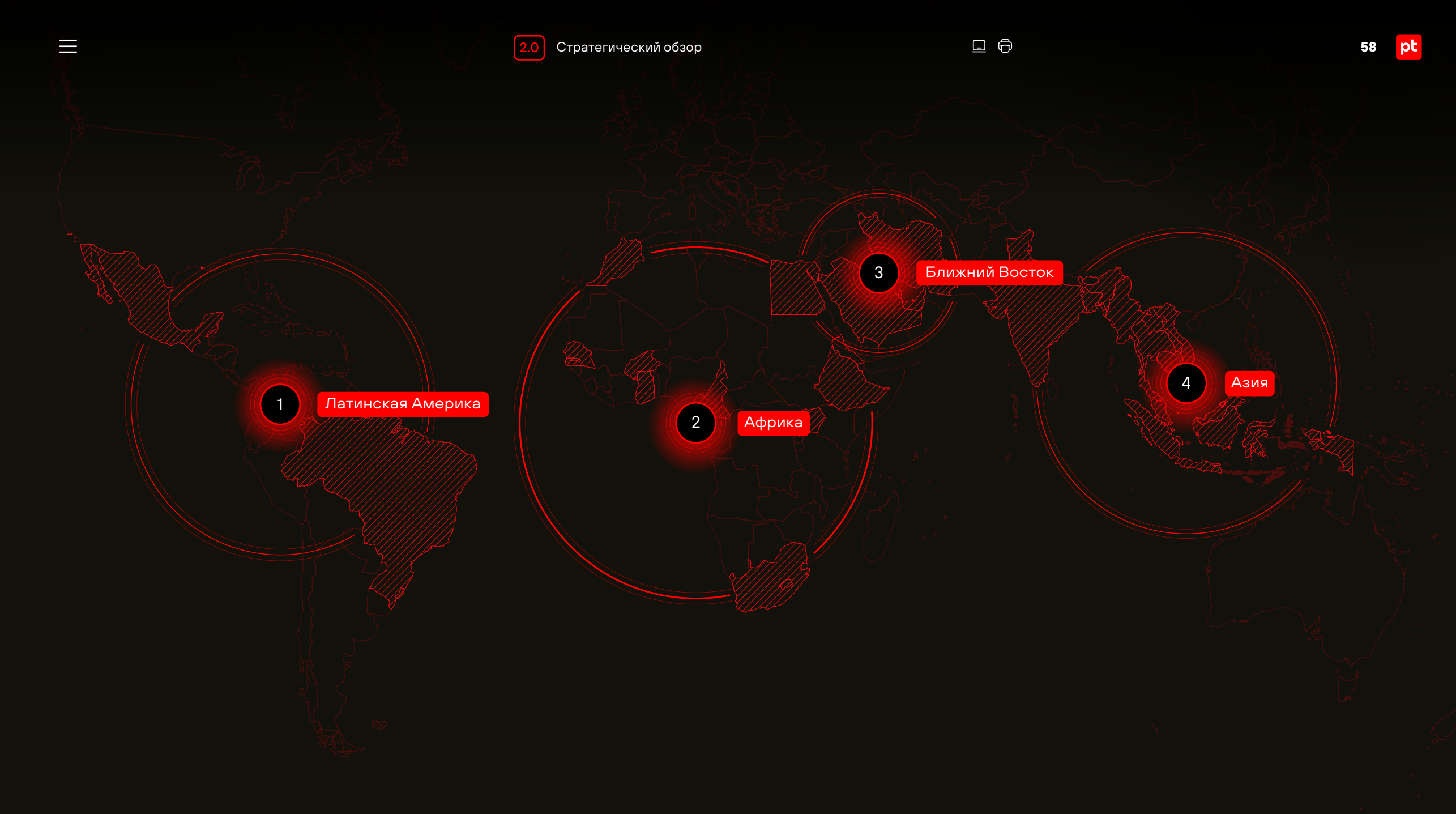
2.4

Международная экспансия

2024 год стал для нас первым полноценным годом активного развития зарубежного бизнеса в новых геополитических условиях. 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.

Для Positive Technologies как зрелой компании на российском ИТ-рынке выход за пределы привычного пространства — это не просто новый этап, а фундаментальная перестройка процессов, приоритетов и подходов к работе. Нам предстояло адаптироваться к требованиям глобального рынка, выстраивать взаимодействие с заказчиками, которые говорят на других языках и работают в иной деловой культуре.

Весь год мы активно исследовали новые регионы, погружаясь в специфику зарубежных рынков. Мы не просто тестировали гипотезы — мы строили фундамент для долгосрочного присутствия в ключевых локациях, укрепляя свои позиции и создавая основу для масштабирования бизнеса на международной арене.

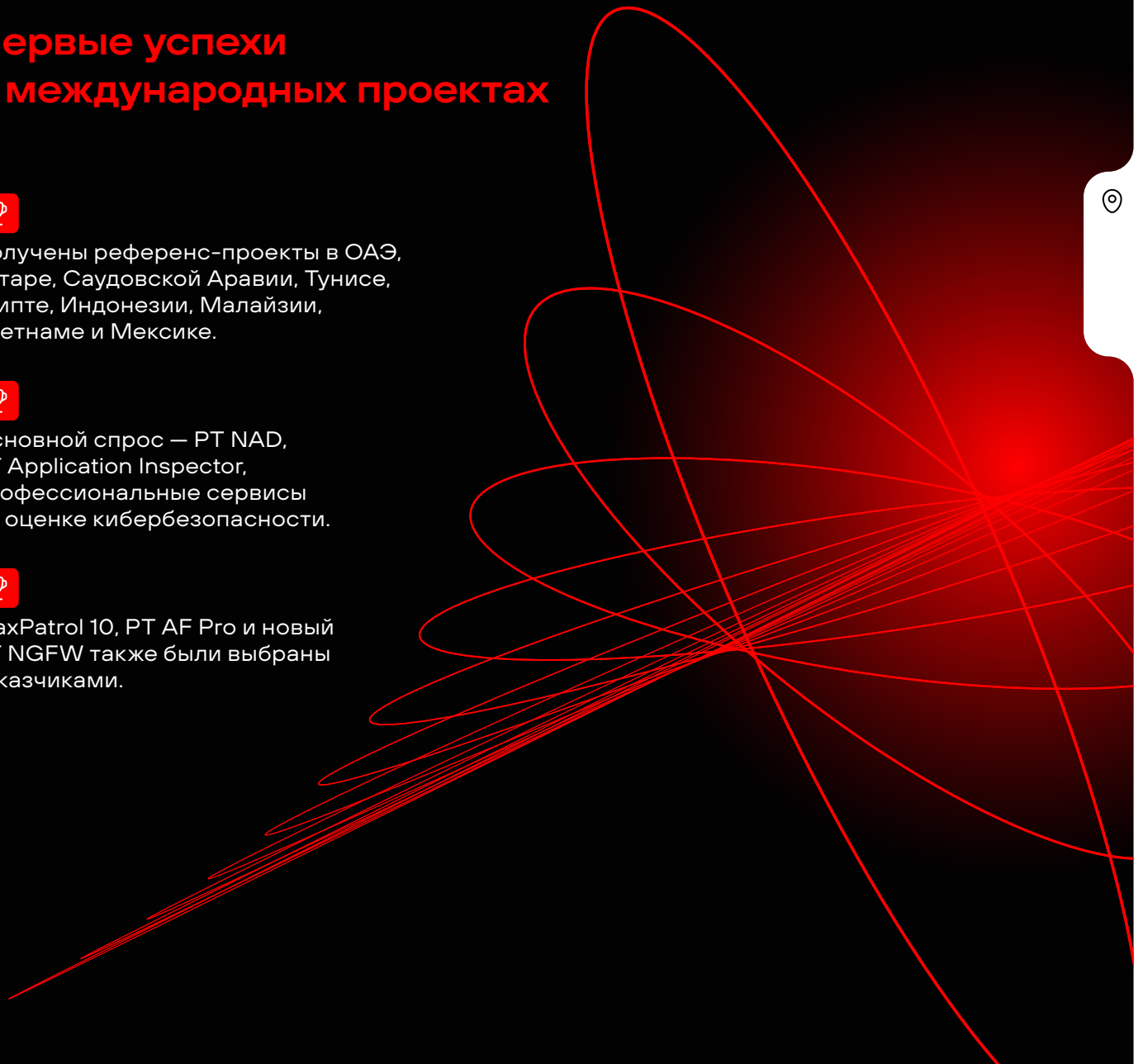

1
Латинская Америка
2
Африка
3
Ближний Восток
4
Азия

Первые успехи в международных проектах

Получены референс-проекты в ОАЭ, Катаре, Саудовской Аравии, Тунисе, Египте, Индонезии, Малайзии, Вьетнаме и Мексике.

Основной спрос — PT NAD, PT Application Inspector, профессиональные сервисы по оценке кибербезопасности.

MaxPatrol 10, PT AF Pro и новый PT NGFW также были выбраны заказчиками.



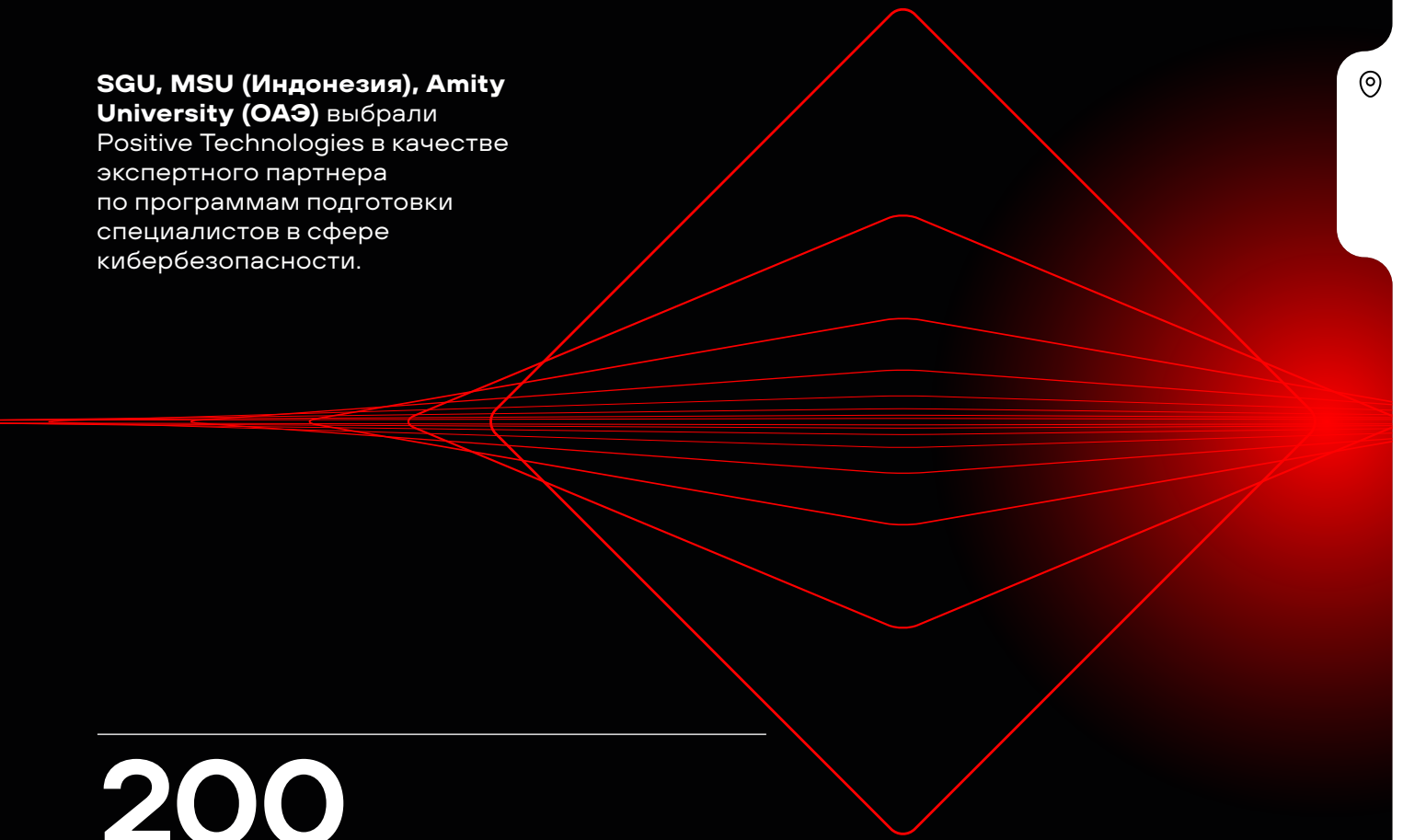
К началу 2024 года наша команда профессионалов и единомышленников сформировала цели и планы по выходу на зарубежные рынки. Мы выстроили активный диалог с локальными партнерами — более 100 компаний, но ключевым вызовом оставалось подтверждение конкурентоспособности наших продуктов и сервисов на глобальном уровне и получение первых референсных проектов.

2024 год мы можем назвать успешным для международного направления Positive Technologies. Мы смогли получить первые референс-проекты в ОАЭ, Катаре, Саудовской Аравии, Тунисе, Египте, Индонезии, Малайзии, Вьетнаме и Мексике, что стало важным шагом в развитии нашего присутствия на международных рынках.

Наибольшим спросом из нашего торгового предложения пользовались PT NAD, PT Application Inspector и наши профессиональные сервисы в области оценки кибербезопасности. Кроме того, в 2024 году мы заключили сделки на поставку нашей платформы MaxPatrol 10 (включает MaxPatrol SIEM, MaxPatrol VM, MaxPatrol EDR, PT NAD и PT Sandbox), а также PT AF Pro и нового решения PT NGFW.

Расширение сотрудничества с вузами

SGU, MSU (Индонезия), Amity University (ОАЭ) выбрали Positive Technologies в качестве экспертного партнера по программам подготовки специалистов в сфере кибербезопасности.



200

партнеров-дистрибьютеров и интеграторов к концу 2024 года

В 2024 году мы достигли значительных успехов в формировании глобальной партнерской сети. На конец года около 200 компаний — локальных дистрибьюторов и интеграторов оценили перспективы сотрудничества с Positive Technologies, протестировали наши продукты и взяли фокус на обучение своих специалистов для совместной работы в 2025 году.

Большую роль в развитии партнерских отношений сыграли мероприятия Positive Education и Центра анализа защищенности, которые позволили участникам глубже познакомиться с нашими технологиями и экспертизой:

- Workshop for FSI — разбор симуляции хакерской атаки в банковской инфраструктуре. Провели в пяти странах.
- Positive Hack Camp — двухнедельный курс по развитию исследовательских навыков. Участники более чем из 20 стран.
- Positive Hack Talks — встречи с локальными комьюнити специалистов в области кибербезопасности. Посетили более 200 человек.

Кульминацией года стало наше флагманское мероприятие Positive Hack Days в Москве, собравшее более 250 потенциальных партнеров и заказчиков из 22 стран.

Подробнее о культурной экспансии Positive Technologies читайте в разделе «Устойчивое развитие», с. 179

Вступление в OIC-CERT

Важным шагом в развитии международного взаимодействия в 2024 году стало наше присоединение к OIC-CERT[1] — ведущей организации, координирующей работу национальных CERT стран, входящих в Organisation of Islamic Cooperation (OIC).

Членство в OIC-CERT стало возможным благодаря участию команды Malaysia Cybersecurity в роли синей команды[2] на киберучениях Standoff, проходивших в рамках Positive Hack Days 2. Полученные в ходе мероприятия положительные рекомендации стали основанием для включения Positive Technologies в международное сообщество киберзащиты.

Взаимодействие с национальными CERT — одно из важных направлений нашей стратегии международной экспансии, и вступление в OIC-CERT открывает новые возможности для укрепления сотрудничества с регуляторами и экспертными сообществами в странах OIC.

Укрепление локального присутствия и развитие клиентского сервиса

В 2024 году благодаря расширению партнерской сети мы получили доступ к новым заказчикам на международных рынках. Для обеспечения качественной поддержки и взаимодействия с клиентами мы усилили команду локальными специалистами, включая пресейл-инженеров и менеджеров по продажам в фокусных регионах. Это позволило нам выстроить более оперативное и удобное взаимодействие с заказчиками — на их родном языке, в удобное время и в очном формате.

[1] Группа OIC-CERT была создана в 2009 году и входит в тройку крупнейших подобных объединений в мире. Членами организации являются более 60 представителей стран Африки, Ближнего Востока, Центральной и Южной Азии. Миссия OIC-CERT — служить платформой для развития потенциала в области кибербезопасности и смягчать последствия кибератак через укрепление глобального сотрудничества.

[2] Команда защитников.

Что дальше

В 2025 году мы планируем закрепить достигнутый успех, фокусируясь на комплексном подходе к кибербезопасности. Основная цель — не просто продвижение отдельных продуктов, а помощь заказчикам в построении полного решения, что включает:

- нашу экспертизу в построении процессов информационной безопасности;
- подготовку специалистов;
- объективную оценку защищенности с помощью наших сервисов.

В 2025 году ключевыми направлениями останутся результативная кибербезопасность, консалтинг по безопасной разработке и реализация проектов национального масштаба, включая создание отраслевых SOC и подготовку специалистов в сфере ИБ.

Развитие партнерской сети

В 2025 году мы актуализируем стратегию работы с партнерами: смещаем фокус с привлечения новых партнеров на развитие совместных проектов с существующими партнерами. Это означает:

- увеличение числа совместных локальных мероприятий с участием наших экспертов;
- углубленную работу с заказчиками через демонстрацию практических результатов;
- выстраивание долгосрочного взаимодействия, направленного на решение реальных бизнес-задач.

Мы продолжаем укреплять позиции Positive Technologies на глобальном рынке, делая акцент на экспертной поддержке, практической эффективности и стратегическом партнерстве.

Продукты, решения, сервисы

3.1

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 экосистемы, 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.

В последние годы особое внимание уделяется все более глубокому использованию машинного обучения (ML) в процессах создания продуктов и экспертизы. Мы активно применяем ML-first-подход, при котором задачу в первую очередь пытаемся решить с помощью ML с самого начала, а не в качестве усиливающего фактора.

ML-first-подход

ML-first-подход — это стратегия разработки, при которой задачи изначально решаются с помощью ML, а не традиционных методов. Если в классическом подходе ML рассматривается как вспомогательный инструмент для оптимизации или усиления существующих процессов, то в ML-first он становится основой с самого начала разработки.

Применение ML-first-подхода позволяет заменить статичные сигнатуры, правила и ручной анализ на самообучающиеся системы, которые могут прогнозировать угрозы, адаптироваться к новым атакам и автоматизировать защиту.

Основные принципы

01

Приоритизация ML — если появляется новая задача, команда сначала рассматривает возможность ее решения через ML, а не традиционную логику.

02

Автоматизация процессов — сокращается участие человека, увеличивается адаптивность моделей.

03

Самообучаемость — системы на основе ML могут улучшаться со временем, анализируя новые данные.

04

Гибкость решений — ML-first позволяет находить неожиданные закономерности и решать проблемы, которые сложно формализовать.

Кросс-функциональные команды функционируют 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.

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 два года 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.

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.

Продукты Positive Technologies лидируют в ключевых ИБ-сегментах

- Security Information & Event Management (MaxPatrol SIEM)
- Vulnerability Management (MaxPatrol VM + MaxPatrol 8 + XSpider)
- Network Traffic Analysis/NDR (PT Network Attack Discovery)
- Web Application Firewall (PT Application Firewall)
- Network Sandboxing (PT Sandbox)
- Next-Generation Firewall (PT NGFW)
- Static Application Security Testing (PT Application Inspector)

Карта рынка наших продуктов — лидеров в своих сегментах

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

Security Information & Event Management
MaxPatrol SIEM

Vulnerability Management
MaxPatrol 8 + MaxPatrol VM + XSpider

Network Traffic Analysis/NDR
PT Network Attack Discovery

Web Application Firewall
PT Application Firewall

Network Sandboxing
PT Sandbox

Next-Generation Firewall
PT NGFW

Static Application Security Testing
PT Application Inspector

Endpoint Detection & Response
MaxPatrol EDR

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

Dynamic Application Security Testing
PT BlackBox

Мы знаем, как

Узнать и защитить

Цель: увеличить время реализации атаки

MaxPatrol Carbon
Навигатор киберустойчивости

MaxPatrol VM
Система для управления уязвимостями

MaxPatrol HCC
Модуль комплаенс-контроля

PT Dephaze
Внутренний автопентест инфраструктуры

PT Knockin
Сервис для проверки защищенности почты

PT Maze
Защита мобильных приложений от реверс-инжиниринга

PT Sandbox
Песочница для обнаружения сложного и неизвестного ВПО

PT BlackBox
Динамический анализатор приложений

PT NGFW
Межсетевой экран нового поколения для высоконагруженных систем

PT Application Firewall
Межсетевой экран уровня веб-приложений

PT Cloud Application Firewall
Облачный межсетевой экран для защиты веб-приложений

PT Application Inspector
Анализатор защищенности приложений

MaxPatrol EDR
Защита конечных устройств от сложных и целевых атак

Проверить киберустойчивость

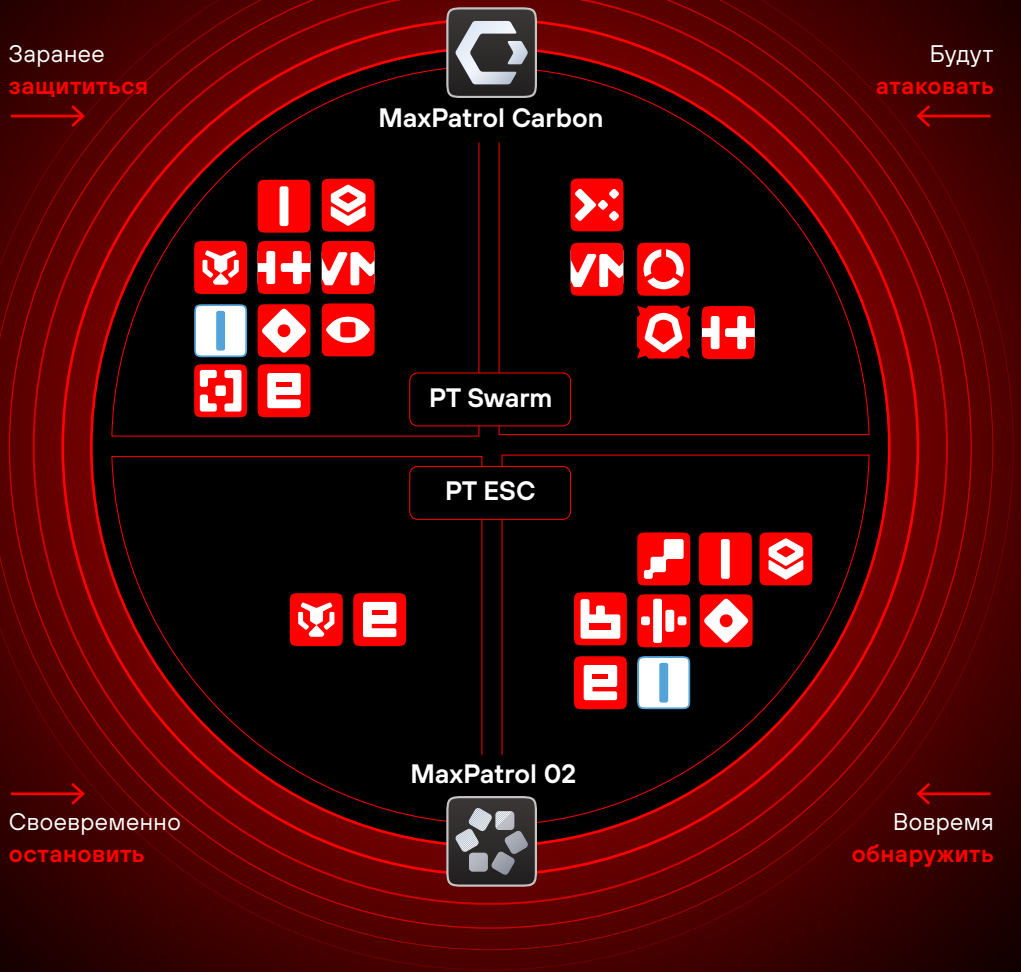
Standoff Bug Bounty

Научить кибербезу

Positive Education

Проверить и прокачать навыки

- Онлайн-симулятор Standoff Cyberbones
- Онлайн-полигон Standoff
- Кибербитва Standoff



Обнаружить и остановить

Цель: увеличить время реализации атаки

MaxPatrol O2
Автопилот для кибербезопасности

PT NGFW
Высокопроизводительный и надежный межсетевой экран нового поколения

PT Application Firewall
Межсетевой экран уровня веб-приложений

PT Cloud Application Firewall
Облачный межсетевой экран для защиты веб-приложений

PT Container Security
Обеспечение безопасности контейнерных сред

MaxPatrol SIEM
Выявление инцидентов ИБ и попыток нарушения киберустойчивости

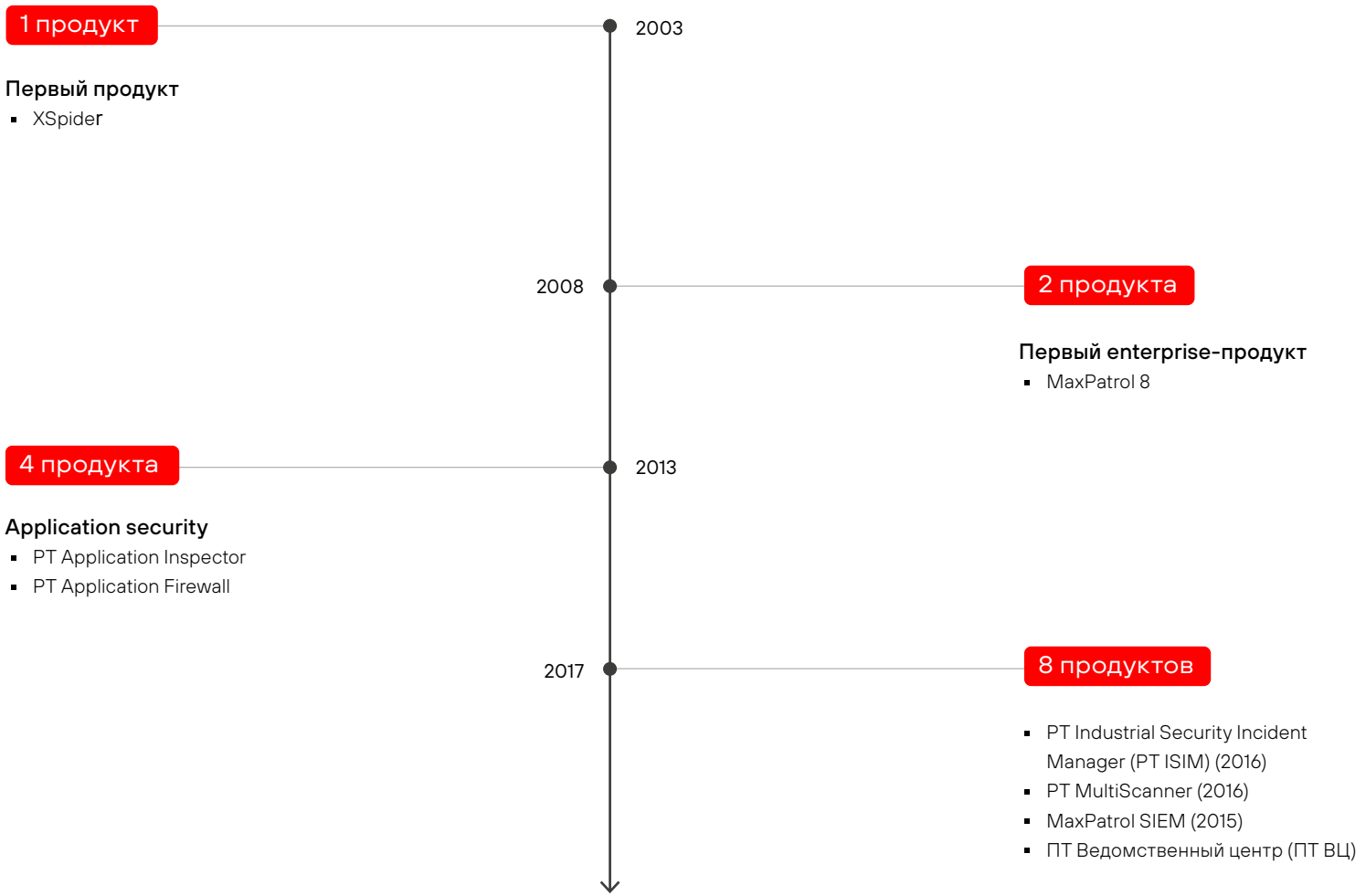
PT Network Attack Discovery
Система поведенческого анализа сетевого трафика

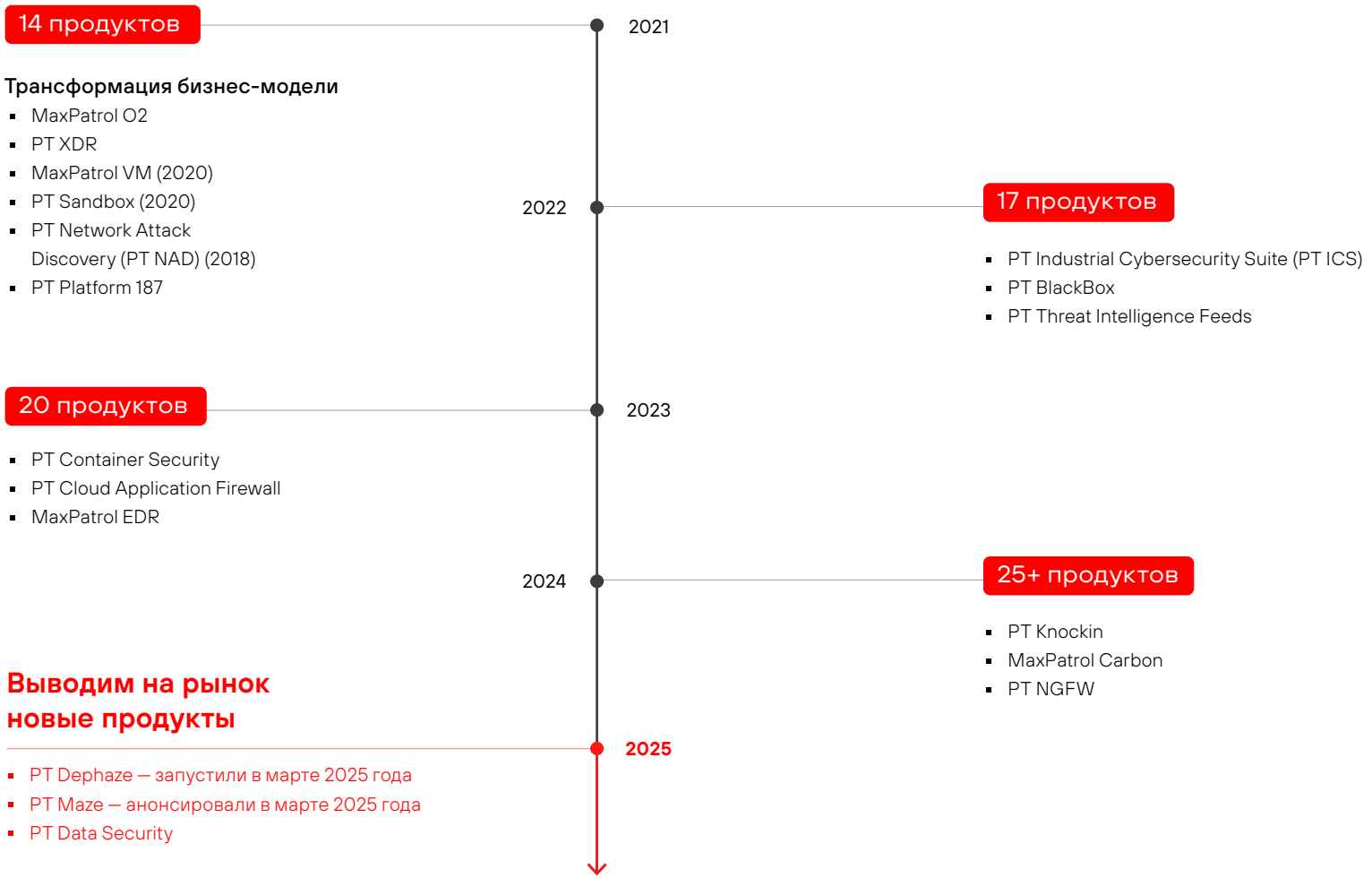
PT Sandbox
Песочница для обнаружения сложного и неизвестного ВПО

MaxPatrol EDR
Защита конечных устройств от сложных и целевых атак

PT ISIM
Система анализа технологического трафика

PT Threat Intelligence Feeds
Потоки данных об угрозах


1 продукт
2003
Первый продукт
XSpider
2008
2 продукта
Первый enterprise-продукт
MaxPatrol 8
4 продукта
2013
Application security
PT Application Inspector
PT Application Firewall
2017
8 продуктов
PT Industrial Security Incident Manager (PT ISIM) (2016)
PT MultiScanner (2016)
MaxPatrol SIEM (2015)
ПТ Ведомственный центр (ПТ ВЦ)


14 продуктов
2021
Трансформация бизнес-модели
MaxPatrol O2
PT XDR
MaxPatrol VM (2020)
PT Sandbox (2020)
PT Network Attack Discovery (PT NAD) (2018)
PT Platform 187
2022
17 продуктов
PT Industrial Cybersecurity Suite (PT ICS)
PT BlackBox
PT Threat Intelligence Feeds
20 продуктов
2023
PT Container Security
PT Cloud Application Firewall
MaxPatrol EDR
2024
25+ продуктов
PT Knockin
MaxPatrol Carbon
PT NGFW
Выводим на рынок новые продукты
2025
PT Dephaze — запустили в марте 2025 года
PT Maze — анонсировали в марте 2025 года
PT Data Security

3.2

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:

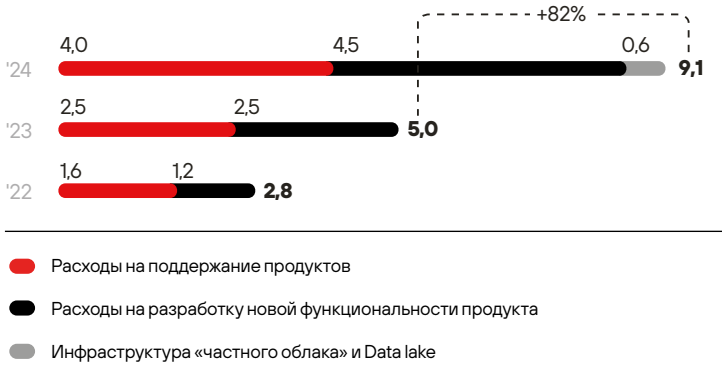
- входят в экспертные организации OIC-CERT[1] и AVAR[2], что способствует борьбе с киберугрозами на международном уровне;
- расследуют самые резонансные инциденты и киберпреступления в России;
- защищают знаковые мероприятия — чемпионат мира по футболу, региональные, федеральные и президентские выборы, «Игры Будущего»;
- исследуют общемировой ландшафт угроз и следят за десятками активных APT-группировок[3]. В том числе наши эксперты обнаруживают деятельность новых группировок, которые проводят тщательно спланированные атаки по всему миру. Эта экспертиза признается коллегами по цеху и активно цитируется в СМИ;
- активно продвигают индустрию ИБ и развивают сообщество. Обеспечивают защиту экосистемы библиотек с открытым исходным кодом для языка Python, создают общедоступные проекты с открытым исходным кодом, активно делятся знаниями, выступая на всех значимых мероприятиях, и пишут статьи в журналы, блоги и СМИ. Наш открытый набор IDS-правил используется большинством популярных сервисов (например, Virustotal, any.run) и большим количеством компаний по всему миру.

[1] Организация исламского сотрудничества объединяет 57 стран Азии, Африки, Европы и Южной Америки. Россия имеет в организации статус наблюдателя с 2005 года.

[2] AVAR была создана в 1998 году как независимая некоммерческая организация для предотвращения распространения вредоносного программного обеспечения (ВПО) и минимизации причиняемого им ущерба путем развития взаимодействия между азиатскими специалистами по защите от ВПО. Ассоциация объединяет выдающихся экспертов из 17 стран и территорий Азиатско-Тихоокеанского региона, в том числе из Китая, Индии, Японии, Южной Кореи, Филиппин, Сингапура, Австралии, США и России.

[3] APT-группировка — это группировка высококвалифицированных хакеров. APT-группировки, как правило, обладают значительными финансовыми ресурсами и техническими возможностями.

Общие R&D-расходы, млрд руб.



Мы продолжаем наращивать инвестиции в R&D и убеждены, что это позволит нам обеспечить непрерывность роста масштаба бизнеса Positive Technologies в последующие годы.

В 2024 году объем вложений в разработку новых продуктов, улучшение функциональности существующих решений, а также в технологические и инфраструктурные проекты вырос на 82% по сравнению с прошлым годом, достигнув 9,1 млрд руб. Основной финансовый эффект от инвестиций, сделанных за последние два года, мы получим в 2025–2026 годах: это существенный вклад в ускорение темпов вывода на рынок новых продуктов и масштабирования бизнеса.

Также мы продолжили усиливать команду за счет привлечения разработчиков и экспертов в области кибербезопасности.

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


PT NGFW


PT Maze


MaxPatrol O2


PT Data Security


PT Knockin


PT Dephaze


MaxPatrol Carbon

3.3

Новые продукты и перспект-ивные разработки

Чтобы поддерживать темпы роста бизнеса, мы активно инвестируем в разработку новых продуктов. Наши наработки воплощают в себе новейшие технологии, определяя дальнейшее развитие отрасли кибербезопасности.

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.

PT NGFW: больше чем импортозамещение

О том, как мы создавали PT NGFW, читайте в материале Positive Research.

«Одна из важнейших задач PT NGFW — это повышение уровня защиты от киберугроз, которых в России за последние два года стало критически много. И он обеспечит эту защиту.

Денис Кораблев,
управляющий директор, директор по продуктам Positive Technologies

100 млрд руб.
наша оценка рынка NGFW в России

Positive Technologies планирует занять не менее половины этого рынка

PT NGFW

Главные достижения 2024 года

- Первый и пока единственный российский межсетевой экран нового поколения сертифицированный по требованиям ФСТЭК к многофункциональным межсетевым экранам уровня сети по четвертому классу защиты (сертификат ФСТЭК от 19 ноября 2024 года № 4877).
- Самый производительный российский межсетевой экран нового поколения — более 300 Гбит/с в режиме L7-фильтрации и более 60 Гбит/с с включенными IPS, антивирусом и URL-фильтрацией, что подтверждено тестированиями в независимой лаборатории Bi.zone (протокол испытаний).
- Две наши аппаратные платформы вошли в единый реестр российской радиоэлектронной промышленности Минпромторга России. ПАК PT NGFW на серверах YADRO внесен в единый реестр российских программ для электронных вычислительных машин и баз данных Минцифры России. Подали заявления на внесение в реестр ПАК PT NGFW на наших аппаратных платформах и серверах «Тринити».
- PT NGFW выбрали для защиты своей инфраструктуры не только субъекты КИИ (крупные финансовые организации, банки, муниципальные органы госуправления и др.), но и коммерческие компании, чей выбор традиционно шире, так как не ограничен только российскими решениями.

Технические характеристики

- Линейка ПАК PT NGFW включает в себя решения как для небольших филиалов (производительность вплоть до 600 Мбит/с), так и для центров обработки данных (производительность 300 Гбит/с в режиме межсетевого экрана и 60 Гбит/с в режиме IPS).
- Централизованная система управления, поддерживающая иерархические структуры групп и правил.
- Собственные механизмы IPS с поддержкой сигнатур от PT Expert Security Center, экспертного подразделения Компании, постоянно анализирующего уязвимости систем и поведение различных группировок.
- Понятный и отзывчивый веб-интерфейс и открытый API.
- Поддержка до 100 тыс. правил безопасности на одно устройство.
- В архитектуре PT NGFW заложено аппаратное разделение ресурсов для плоскости управления и плоскости передачи данных. Это гарантирует управляемость устройства при любых объемах передаваемых данных.
- Отсутствие legacy-кода и регулярные релизы с новыми функциями.
- Кластер Active/Standby: команда разработки продукта пошла по пути лучших мировых практик реализации этой функции. Переключение устройств в кластере проходит максимально быстро, не влияя на уровень защищенности и удобство пользователей.

Также в 2024 году:

- продолжили рассказывать о внутренней кухне разработки в реалити-проекте «PT NGFW за стеклом»;
- начали работу с комьюнити айтишников («ИТ-посиделки»);
- впервые провели хакатон на базе киберполигона Standoff, где участники настраивали PT NGFW, а после этого расследовали атаки;
- запустили регулярный Bootcamp и программу NFR, try & buy, лизинг.

Рекордный старт продаж

1,2 млрд руб.
всего за 1,5 месяца

~300
«пилотов» провели за полгода

PT Dephaze

Внутренний автопентест инфраструктуры.

В 2024 году Positive Technologies объявила о запуске MVP (начальной версии) нового продукта для тестирования на проникновение в автоматическом режиме — PT Dephaze.

Он основан на многолетнем опыте Компании и знаниях о том, как защищаться от киберугроз. Коммерческая версия продукта вышла в марте 2025 года. PT Dephaze непрерывно находит недостатки безопасности инфраструктуры, используя популярный инструментарий, тактики и техники реальных APT-группировок, до того, как злоумышленники реализуют недопустимые для бизнеса события.

Больше чем BAS:

мы выпускаем систему, которая не просто симулирует атаки, как, например, продукты класса BAS[1] (Breach and attack simulation), а реально тестирует инфраструктуру на проникновение, максимально близко к тому, как это делал бы пентестер. С ним вы сможете не только проверить эффективность средств защиты информации, но и увидеть, какими уязвимыми местами злоумышленники воспользуются в первую очередь.

Отличительные характеристики:

- использует технологии искусственного интеллекта, которые значительно ускоряют процесс поиска слабых мест;
- наглядно показывает результаты тестирования на проникновение, позволяя сразу исправить недостатки защиты;
- умеет преднастраивать ограничения для безопасной управляемой атаки;
- построен на гибкой доменной модели, объединяющей в себе лучшие практики решений класса BAS, а также подходов, реализованных в открытых стандартах и opensource-проектах.

Потребности и оценка рынка

Данные Positive Technologies подтверждают востребованность систем класса BAS и автоматического пентеста. Ведь даже компании со зрелым уровнем ИБ проводят анализ защищенности максимум раз в год или по запросу.

По данным ЦСР, потребности компаний в оценке своей защищенности растут из года в год, в 2023 году этот рынок оценивался в 8 млрд руб. Суммарно рынок классических и автопентестов в России, по нашей оценке, составляет более 5 млрд руб.

[1] Системы класса BAS предназначены для имитации кибератак, попыток взлома и проникновения злоумышленника в сеть компании. Подобное моделирование помогает заказчику автоматически протестировать безопасность инфраструктуры и оценить уровень защиты своей организации.

PT Data Security

Единое решение для защиты данных независимо от их типа и места хранения.

В октябре 2024 года мы представили MVP (начальную версию) PT Data Security. Запуск коммерческой версии продукта планируется во втором полугодии 2025 года.

Отличительные характеристики:

- основан на новой концепции защиты данных — Data Security Platform;
- найдет, где располагаются все значимые данные, в каком бы виде они ни были представлены;
- помогает отслеживать состояние инфраструктуры и выявлять критически значимые элементы, которые содержат наиболее чувствительные для бизнеса данные.

В связи с изменениями в российском законодательстве в 2025 году может значительно повыситься внимание к организации защиты персональных данных. В конце ноября 2024 года были приняты поправки, ужесточающие санкции за утечки персональных данных.

Был одобрен законопроект, который существенно увеличивает административную ответственность (в частности, вводятся оборотные штрафы для компаний за повторные утечки — от 1 до 3% годовой выручки) и вводит уголовную ответственность (вплоть до 10 лет лишения свободы) за утечку персональных данных.

Новый перспективный рынок

С выпуском PT Data Security Компания выйдет на новый для себя рынок защиты данных. По оценке ЦСР, отечественный рынок средств защиты данных является самым быстрорастущим сегментом в отрасли. В 2023 году он увеличился на 93% от уровня предыдущего года и достиг отметки 23 млрд руб., составив 12% от общего рынка ИБ.

При этом эксперты Positive Technologies отмечают, что доля сегмента по-прежнему остается низкой и его потенциал не раскрыт. К 2028 году мы планируем занять не менее 50% рынка средств защиты данных, который, по нашим прогнозам, будет оцениваться в половину от всего объема рынка кибербезопасности в России.

PT Knockin

Симулятор атак на корпоративную почту с целью проверки ее защищенности.

Продукт за две минуты проверяет, как работают почтовые средства защиты — антивирусы, почтовые шлюзы, песочницы, выдает вердикт об уровне безопасности и формирует рекомендации по улучшению их работы.

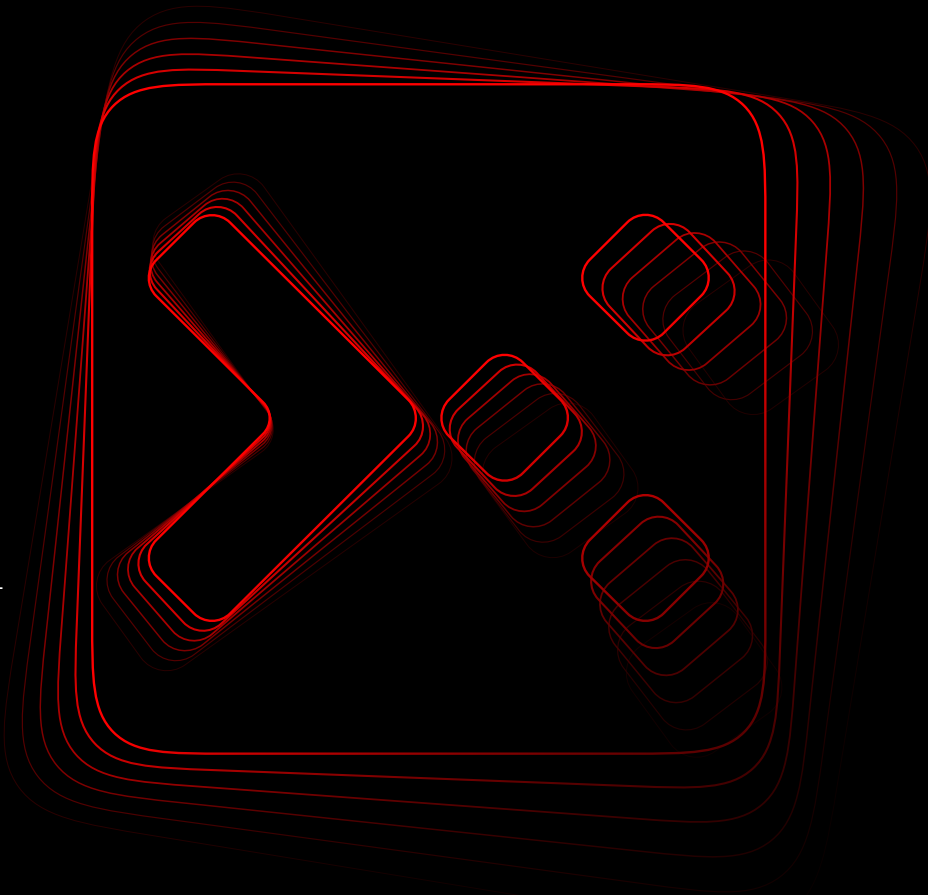
Это единственный сервис на территории России, который может проверить защищенность по почтовому вектору атаки. Аналогов в нашей стране не существует. Мы постоянно обновляем базу семплов (ВПО), придумываем способы запаковки вредоносной активности и улучшаем возможности для гибкой настройки симуляции.

Отличительные характеристики:

- имитирует реальные атаки на почтовый сервер;
- проверяет на самые трендовые вредоносные программы;
- атакует не только файлами, но и ссылками;
- дает рекомендации по улучшению защищенности;
- формирует отчет с оценкой безопасности.

В 2024 году:

- вывели сервис на рынок;
- более 2,7 тыс. компаний со всего мира проверили защиту своей корпоративной электронной почты, из которых 38% относятся к списку Expert RA 600;
- отправили более 200 тыс. писем, содержащих файлы с имитацией зловредного ПО или ссылки на них;
- увеличили количество вариаций атак с 30 на этапе запуска продукта до 3 тыс. в конце года (с учетом возможности запаковки файлов в архивы разных форматов).



PT Maze

Сервис по защите мобильных приложений от реверс-инжиниринга.

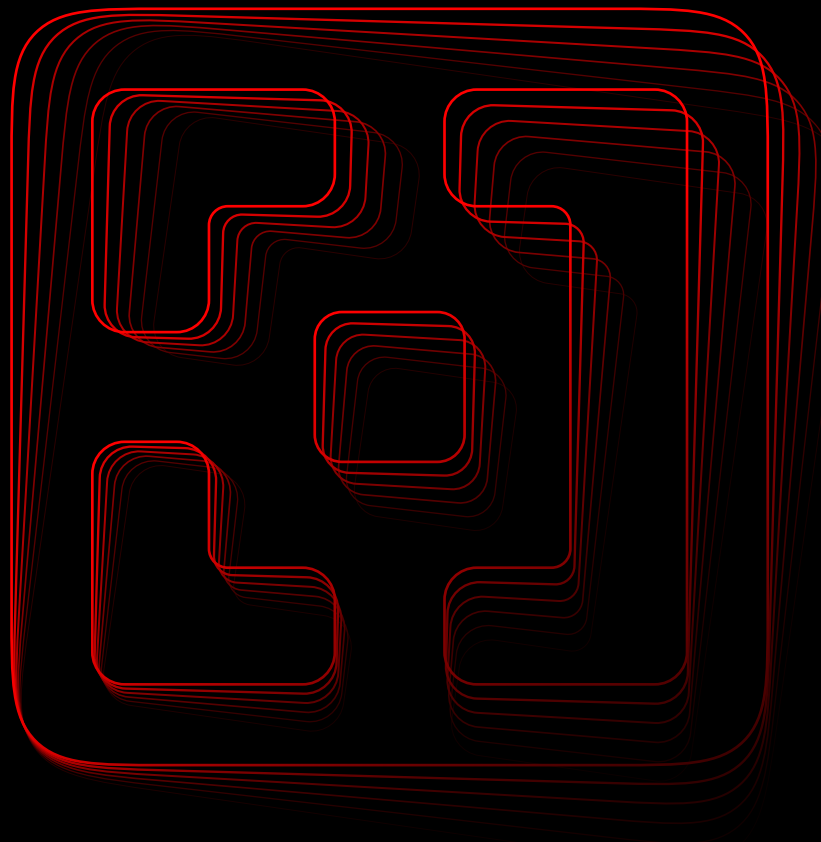
В последние годы в международных рейтингах уязвимостей недостатки, связанные с защитой кода, стабильно движутся вверх. Недостаточная защищенность кода — одна из самых расхожих и критически значимых слабостей приложений на сегодняшний день. Основа PT Maze — многолетний опыт белых хакеров Positive Technologies в анализе защищенности мобильных приложений.

Отличительные характеристики:

- модификация вместо дополнения — PT Maze модифицирует исполняемые файлы приложения, и это основной подход к внедрению защитных механизмов;
- децентрализация — каждый модуль допускает параметризацию и работает независимо, что позволяет распределять защиту внутри приложения;
- SaaS — PT Maze принимает мобильное приложение и модифицирует его на собственном сервере. При этом владельцу приложения доступны все версии модификаций защитными механизмами;
- не требует настройки — мы подготовили стандартные конфигурации защиты, чтобы клиенты могли запустить сервис нажатием одной кнопки, без долгой настройки.

PT Maze поможет защитить приложение от создания клонов и модификаций, несанкционированной разблокировки платных и иных ограниченных функций, поиска уязвимостей и изучения внутреннего устройства третьими сторонами.

Запуск PT Maze анонсировали в марте 2025 года.



MaxPatrol O2

Обнаружение и остановка хакера с минимальным участием человека.

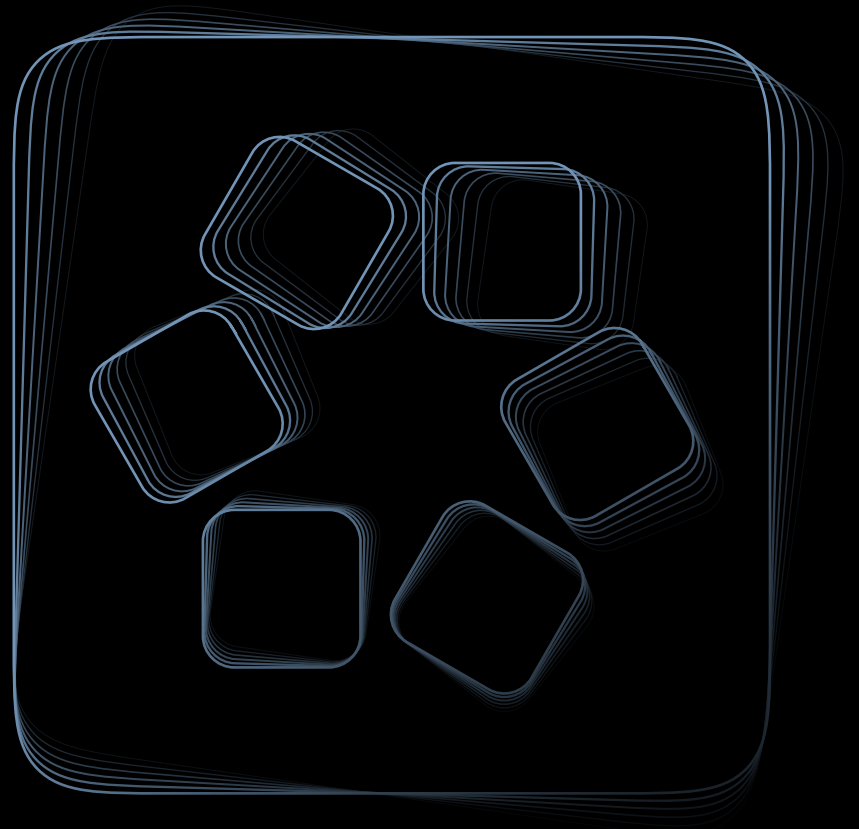
Для того чтобы вовремя обнаружить хакера, пока он не успел нанести неприемлемый ущерб компании, в ИТ-инфраструктуре необходимо по максимуму регистрировать и обрабатывать все подозрительные события. Такая настройка позволит обнаружить даже высококвалифицированные хакерские группировки, но при этом создаст колоссальный поток событий, обработать который в полном объеме не сможет ни один SOC[1].

Метапродукт MaxPatrol O2 берет на себя эту задачу: анализируя десятки и сотни тысяч подозрительных событий, он формирует единицы действительно значимых цепочек активностей. Для верификации выявленных активностей и согласования предложенных сценариев реагирования система привлекает специалистов на несколько минут в день, тем самым снижая время обнаружения и остановки хакерской атаки в 30–50 раз.

[1] Центр мониторинга информационной безопасности (SOC) — структурное подразделение организации, отвечающее за оперативный мониторинг ИТ-среды и реагирование на киберинциденты.

Метапродукты

Positive Technologies продолжает разработку и внедрение метапродуктов, чтобы помочь клиентам достичь результативной кибербезопасности. Мы стремимся избавить ИБ-специалистов от огромного объема технических рутинных операций по мониторингу и противодействию угрозам и передать эти функции нашим метапродуктам. Задачами специалиста по кибербезопасности до момента наступления кибератаки станут анализ потенциальных векторов угроз и своевременное выстраивание защиты. А при обнаружении атаки специалисту будет необходимо верифицировать выявленную активность злоумышленника и запустить сформированный сценарий реагирования, который остановит его прежде, чем он успеет нанести компании непоправимый ущерб.



MaxPatrol O2

ИИ в MaxPatrol O2

В своей работе MaxPatrol O2 использует специальный модуль машинного обучения для оценки аномальности собранных цепочек активностей в инфраструктуре. С помощью заложенных ML-моделей он выявляет нетипичность общей активности процессов, выполняемых командных строк, управляющих воздействий, ресурсов и пр.

Для решения данной задачи используются как предобученные модели машинного обучения, регулярно обновляемые производителем, так и модели, обучающиеся непосредственно на защищаемой ИТ-инфраструктуре.

Отличительные характеристики:

- Защита компании от атак хакеров с помощью одного человека — Автоматическое расследование атаки позволяет исключить все рутинные операции в работе SOC, восстановить хронологию действий злоумышленника и получить все необходимые данные для принятия решения о реагировании. И сделать это все силами одного человека.
- Противодействие хакеру в режиме реального времени — MaxPatrol O2 автоматически генерирует сценарий реагирования на атаку. Оператору остается его верифицировать и нажать одну кнопку для его исполнения.
- Прогнозирование действий атакующих — Технология PT Threat Modeling Engine прогнозирует возможные варианты развития атаки хакера из его текущей точки присутствия с учетом доступа к наиболее критичным активам компании.
- Снижение нагрузки на сотрудников SOC — Автоматизация и машинное обучение позволили в 1,5 тыс. раз снизить нагрузку на аналитиков SOC.

В 2024 году:

- участие в кибербитве StandOff — MaxPatrol O2 шесть часов противостоял четырем лучшим командам хакеров в рамках финала Standoff 13. Белые хакеры пытались реализовать недопустимые события в цифровом двойнике инфраструктуры Positive Technologies, и у них не вышло;
- ряд компаний вышли на киберучения и кибериспытания с использованием для обеспечения защиты MaxPatrol O2;
- MaxPatrol O2 получил отметку, которая подтверждает применение в продукте технологий искусственного интеллекта.

MaxPatrol Carbon

Проактивная подготовка к отражению кибератак.

Метапродукт MaxPatrol Carbon автоматизирует достижения состояния киберустойчивости: анализирует в режиме реального времени, готова ли компания вовремя обнаружить и нейтрализовать возможную кибератаку, рекомендует меры для усиления защиты и снижения рисков из-за действий злоумышленников в инфраструктуре.

Технология моделирования угроз в MaxPatrol Carbon

В MaxPatrol Carbon встроен специальный модуль PT Threat Modeling Engine для моделирования возможностей хакера в инфраструктуре компании. Уникальный алгоритм строит граф возможностей злоумышленника с учетом потенциальных действий атакующих, контекста инфраструктуры и множества параметров, способных повлиять на время, необходимое для реализации атаки (TTA) и ее своевременное обнаружение (TTD).

MaxPatrol Carbon

Отличительные характеристики:

- моделирует кибератаки на критически важные системы — автоматизирует трудоемкий анализ потенциальных маршрутов атак на целевые системы, учитывая время реализации различных действий хакеров в инфраструктуре компании;
- помогает подготовить компанию к отражению кибератак — формирует и объединяет задачи по достижению киберустойчивости, приоритизируя их выполнение в зависимости от влияния на защиту целевых систем и компании в целом;
- улучшает внутреннюю эффективность ИТ и ИБ — позволяет командам ИБ и ИТ сосредоточить ресурсы на самых срочных и критически важных задачах, отслеживать сроки исполнения рекомендаций и контролировать общий ход работ;
- непрерывно контролирует киберустойчивость — комплексно оценивает защищенность целевых систем компании в режиме реального времени и обеспечивает централизованный контроль соответствия требованиям безопасности.

В 2024 году:

- провели и представили исследование состояния готовности российских организаций к противодействию атакам злоумышленников, обозначили основные вопросы в обеспечении киберустойчивости и предложили рекомендации по их решению;
- выпустили коммерческую версию — коммерческий лонч продукта состоялся на международном киберфестивале Positive Hack Days 2;
- развивали технологии — инвестировали в технологии и экспертизу продукта для обеспечения быстрого и максимально точного прогнозирования кибератак для выстраивания эффективного процесса достижения киберустойчивости у наших клиентов;
- первая презентация технологии рынку;
- осуществили первые внедрения.

Интерес к продукту проявляют крупные компании, представляющие различные отрасли (государственный сектор, банковская сфера, промышленность и другие), поскольку на российском рынке отсутствуют решения, способные моделировать и анализировать потенциальные маршруты кибератак с учетом бизнес-рисков. В настоящее время семь проектов находятся на стадии активного внедрения, одновременно с этим мы применяем метапродукт в своей инфраструктуре.

Кроме того, мы помогаем нашим клиентам выстраивать процесс управления активами, так как это одно из ключевых условий для эффективного и успешного использования нашего продукта.


MaxPatrol SIEM


MaxPatrol VM


PT Industrial Security Incident Manager


MaxPatrol HCC


PT Application Inspector


ПТ Ведомственный центр


PT Application Firewall


MaxPatrol EDR


XSpider


PT Threat Intelligence Feeds


PT Multiscanner


PT Container Security


PT Network Attack Discovery


PT Cloud Application Firewall


MaxPatrol 8


PT Sandbox


PT BlackBox

3.4

Зрелые продукты

Многие наши продукты уже стали золотым стандартом в своих технологических сегментах и пользуются заслуженным признанием на рынке.

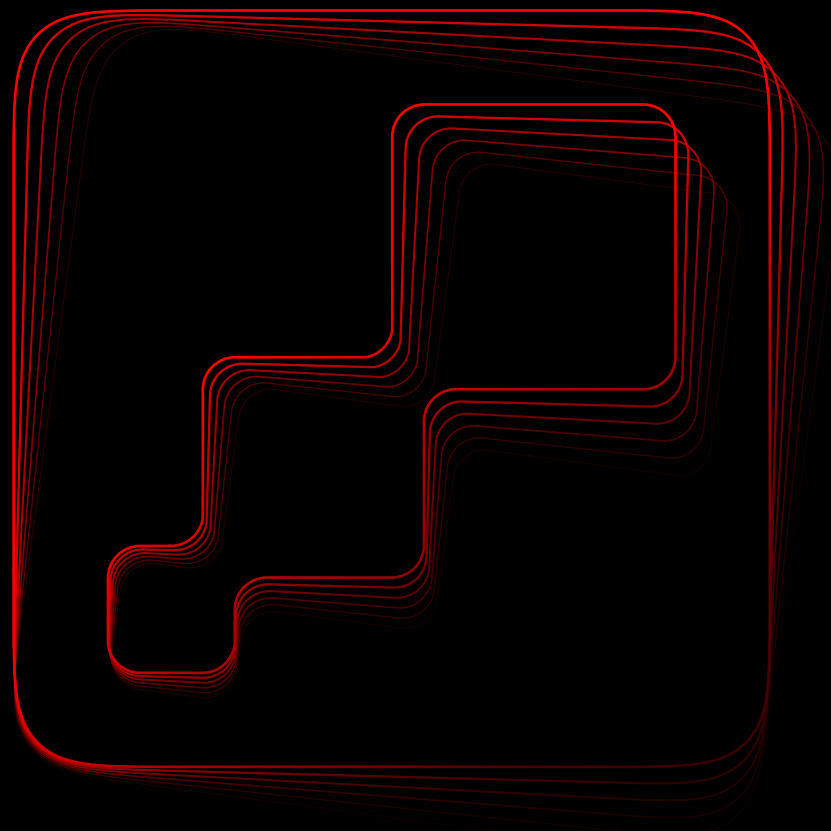
MaxPatrol SIEM

Система непрерывного мониторинга событий кибербезопасности и управления инцидентами. Лидер на российском рынке SIEM[1]-систем и основа крупнейших SOC в России с 2015 года.

Встроенные технологии машинного обучения ML-модуля BAD (Behavioral Anomaly Detection) выявляют неизвестные прежде аномалии.

57%

доля MaxPatrol SIEM в сегменте SIEM[2]



1 Security Information and Event Management — анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений, который позволяет реагировать на них до наступления существенного ущерба.

2 По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса SIEM в 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

MaxPatrol SIEM

Отличительные характеристики

- Результативная SIEM-система, которая обеспечивает качественное обнаружение угроз на потоке более чем из 540 тыс. событий в секунду при использовании всех экспертных правил.
- MaxPatrol SIEM знает, где искать потенциальные угрозы. Обеспечивает полноту аудита инфраструктуры и контроля сбора событий, в том числе с помощью:
  - более 330 поддерживаемых источников событий ИБ;
  - более 9,4 тыс. правил нормализации.
- MaxPatrol SIEM знает, что искать. Высокое качество обнаружения, в том числе целенаправленных атак:
  - более 1,5 тыс. готовых правил корреляции, которые выявляют более 95% всех популярных методов злоумышленников по матрице MITRE (руководство по классификации и описанию кибератак и вторжений);
  - встроенные технологии машинного обучения ML-модуля BAD выявляют неизвестные прежде аномалии.
- Встроенная технология Asset management помогает выявлять недоступность источников, аномалии в распределении потока событий и задержку в получении событий из источников для своевременного реагирования на них.
- MaxPatrol SIEM использует собственную систему управления базами данных (СУБД) LogSpace, разработанную Positive Technologies специально для задач хранения больших объемов информации о событиях из разнообразных источников для нужд подразделений ИБ.

В 2024 году:

- обновили ML-модуль BAD, который теперь не только выдает второе мнение в виде определения уровня риска по событию, но и самостоятельно обнаруживает целенаправленные атаки;
- и тут же показали результат: BAD обнаружил реальных хакеров на реальных киберучениях;
- представили мониторинг источников 2.0, который не дает злоумышленнику обойти систему, используя слепые зоны в мониторинге. Теперь его можно настроить по трем параметрам (контроль активности, потока, задержек) и использовать рекомендации по мониторингу от наших экспертов;
- ускорили работу конвейера обработки событий MaxPatrol SIEM и нормализатор в частности: ожидаемый прирост производительности от 5 до 15% по компонентам;
- значительно повысили производительность СУБД LogSpace, что привело к повышению средней скорости выполнения запросов в клиентских инсталляциях в 5–10 раз. Также новая версия LogSpace доступна для заказчиков со сложной архитектурой благодаря возможности горизонтального масштабирования;
- провели серию вебинаров «Оголяемся технологически», где раскрыли секреты разработки нашей SIEM-системы и подсветили все наши уникальные преимущества и подходы (активоцентричность, СУБД LogSpace, нормализацию, корреляцию, ML-, AI-технологии).

/ Зрелые продукты

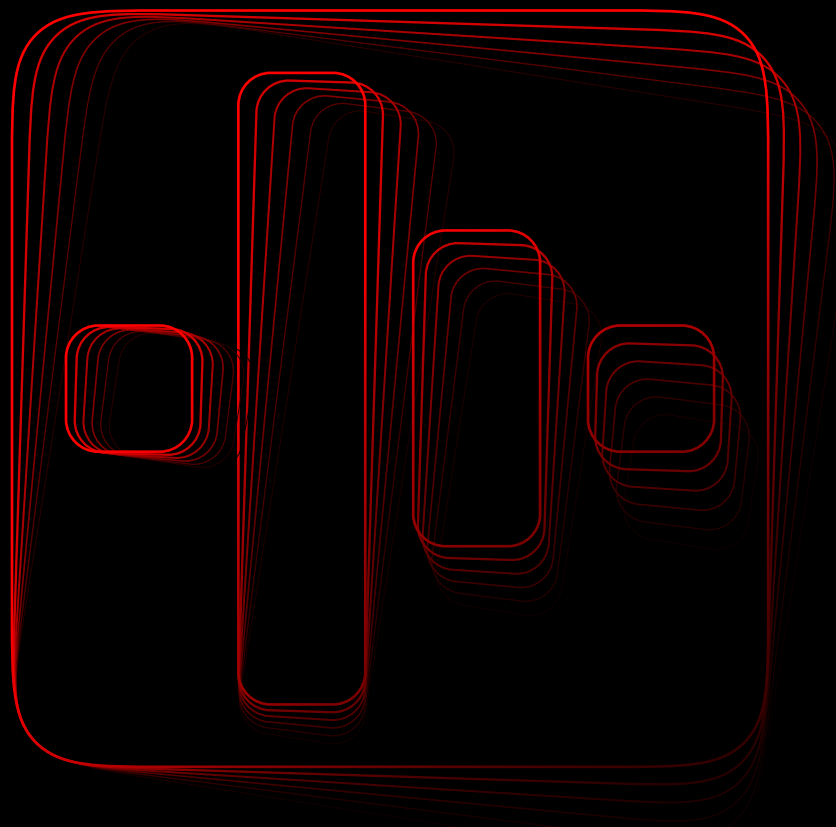
PT Network Attack Discovery

PT Network Attack Discovery (PT NAD) — продукт для обнаружения сложных сетевых атак и их расследования. Решение точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз.
PT NAD знает, что искать в сети.

PT Network Attack Discovery стала первой системой анализа трафика с искусственным интеллектом в реестре российского ПО.

60%
доля PT NAD в сегменте NTA / NDR (не включая Sandbox)[1]

>20
международных пилотных проектов, из которых 3–5 находятся на финальной стадии и завершатся закупкой, было реализовано за год



[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 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

PT Network Attack Discovery

Отличительные характеристики

- Использует эвристические и несигнатурные методы, а также поведенческий анализ для выявления сложных сетевых атак, которые не детектируются сигнатурными методами.
- Обеспечивает эффективное хранение метаданных сетевых соединений и копии сетевого трафика, предоставляя удобный интерфейс для расследования инцидентов и доступа к сырому трафику.
- Осуществляет детальный разбор протоколов (в том числе прикладного уровня), позволяет извлекать и хранить файлы, передаваемые по протоколам прикладного уровня, предоставляя полный сетевой контекст угрозы.
- Автоматический ретроспективный анализ позволяет выявлять новейшие угрозы, информация о которых стала доступна.
- Осуществляет идентификацию узлов путем анализа сетевых сессий, решая проблему контроля теневой инфраструктуры.
- Обеспечивает проверку регламентов ИБ путем выявления слабых паролей и передачи аутентификационных данных в незашифрованном виде, VPN-туннелей, TOR, утилит для удаленного доступа, прокси-серверов, мессенджеров.

В 2024 году:

- более 300 заказчиков используют PT NAD;
- наши заказчики с помощью PT NAD нашли более 15 реальных инцидентов;
- выпустили два публичных релиза — 12.0 и 12.1;
- достигли функциональности, которой гордимся:
  - увеличение максимальной скорости индексирования в три раза,
  - появление пользовательских правил профилирования — нового механизма на основе машинного обучения,
  - реализовали ML-алгоритм детектирования приложений в зашифрованном трафике,
  - обновление экспертных модулей,
  - релиз темной темы;
- провели NetCase Day — наш первый митап честных кейсов по сетевой безопасности. Презентовали фичи нового релиза PT NAD, а также пообщались с ключевыми заказчиками, которые поделились реальным опытом применения продукта;
- выпустили «Исследование и профилирование киберугроз в сетевом трафике российских компаний»;
- провели серию CustDev среди нынешних, бывших и будущих пользователей PT NAD. Результаты глубинного исследования легли в развитие дорожной карты на 2025 год;
- реализована поддержка версии хранилища данных Elasticsearch, благодаря которой система теперь может в три раза быстрее индексировать трафик, а также улучшения для работы операторов и администраторов;
- во время расследования с помощью PT NAD обнаружили и помогли устранить уязвимость нулевого дня в системе видео-конференц-связи VINTEO (BDU:2024–08421, BDU:2024–08422);
- обновили обучающие курсы и получили много положительных отзывов;
- разработали брошюры, чтобы облегчить использование продукта:
  - Справочник по PT NAD для аналитика SOC,
  - Руководство по работе с пользовательскими правилами профилирования в PT NAD,
  - Руководство по передаче трафика в PT NAD,

- Whitepaper с аналитикой по «Исследованию и профилированию киберугроз в сетевом трафике российских компаний в 2023/2024 году».

Международные итоги:

- один из крупных банков благодаря пилоту PT NAD самостоятельно обнаружил атаку APT-группировки на свой платежный шлюз и проследил всю цепочку атаки;
- с использованием PT NAD и экспертизы PT ESC удалось предотвратить атаку на цепочку поставок производителя IoT-устройств в Индонезии;
- вместе с индонезийским партнером Svarnatech и локальным производителем серверов IMV развернули ПАК PT NAD. Стратегическое сотрудничество предполагает до 30 проектов для государственных учреждений;
- успешно провели тестирование совместимости PT NAD в облачных средах AWS и GCP.

MaxPatrol VM

Система управления уязвимостями. Продукт помогает выстроить процесс, результат которого виден, — поддерживает актуальность данных об активах, приоритизирует уязвимости и контролирует их устранение.

«Решение с искусственным интеллектом» в реестре российского ПО

71%

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

12 часов

уникальный для рынка стандарт доставки трендовых уязвимостей, который поддерживает система, тогда как по рекомендациям ФСТЭК России на устранение критичных уязвимостей отводится 24 часа

[1] По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса VM в 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

MaxPatrol VM

Отличительные характеристики:

- позволяет автоматизировать процесс управления уязвимостями;
- в течение 12 часов сообщает о наличии трендовых, по мнению экспертов Positive Technologies, уязвимостей, которыми легко могут воспользоваться злоумышленники;
- благодаря технологии Asset Management (AM, управление уязвимостями) собирает более 3 тыс. параметров ИТ-активов и позволяет провести полную инвентаризацию инфраструктуры;
- технология хранения информации об активах поддерживает актуальные данные об уязвимостях в инфраструктуре без повторных сканирований;
- поддерживает сканирование российского ПО на наличие уязвимостей;
- определяет степень критичности уязвимостей для инфраструктуры, позволяет установить и контролировать сроки устранения наиболее опасных из них;
- обнаруживает уязвимости веб-приложений и Docker-контейнеров, обеспечивая анализ защищенности максимального количества систем в инфраструктуре;
- контролирует состояние безопасности автоматизированных систем управления технологическим процессом (АСУ ТП) благодаря пакету экспертизы для промышленных систем;
- модуль MaxPatrol HCC (host compliance control) в MaxPatrol VM позволяет провести харденинг инфраструктуры и проверить активы на соответствие ключевым требованиям ИБ.

В 2024 году:

- поддержали сканирование веб-приложений и Docker-контейнеров — теперь еще большая часть инфраструктуры может быть просканирована и защищена;
- добавили функционал написания собственных требований безопасности в MaxPatrol HCC. Произошло колоссальное развитие модуля по проверке соответствий требованиям ИБ. Мы даем возможность каждому клиенту написать необходимые проверки для своей инфраструктуры и бизнес-процессов. Это позволяет заказчикам быть на шаг ближе к результативной кибербезопасности;
- добавили функционал AI-поиска в MaxPatrol VM, что ускорило и упростило работу с продуктом. Получили галочку «Решение с искусственным интеллектом» в реестре российского ПО;
- поддержали новое ПО для VM, чем увеличили количество паспортов уязвимостей за год в два раза;
- в несколько раз увеличили скорость доставки информации о трендовых уязвимостях в продукт;
- благодаря ML-алгоритму и команде экспертов ежедневно отслеживали самые опасные уязвимости. Выделили за год 72 трендовые уязвимости. Информация о них регулярно попадала в продукт в течение 12 часов, что является уникальной скоростью для рынка;
- внедрили в продукт агент MaxPatrol EDR. Совместное использование продуктов поможет снизить нагрузку на сетевой сканер MaxPatrol VM, сократить задержки при повторном сканировании и обеспечить оперативную обратную связь об устранении уязвимостей. Это, в числе прочего, позволит получать актуальную информацию с устройств удаленных сотрудников, которые не всегда бывают подключены к сети компании во время сканирования.

MaxPatrol HCC

Инструмент для комплаенс-контроля и харденинга инфраструктуры.

Кроме уязвимостей в коде ПО и ОС, которые обнаруживают решения класса vulnerability management, киберугрозу несет и некорректная настройка систем (например, выдача избыточных прав доступа, наличие открытых портов и интерфейсов). Злоумышленники используют их для проникновения в контур компании и продвижения внутри инфраструктуры. Модуль MaxPatrol HCC проверяет конфигурации систем на соответствие российским и международным стандартам практической ИБ, а также внутренним требованиям компании.

Преимущества:

- приоритизирует риски и определяет требования, соблюдение которых наиболее важно для безопасности компании;
- автоматически оценивает соответствие активов новым требованиям без повторного сканирования;
- позволяет установить в SLA сроки устранения несоответствий требованиям и контролировать изменения в инфраструктуре;
- возможность подключать агенты позволяет сканировать компьютеры сотрудников, в том числе удаленных, а после проверять их на соответствие самым важным требованиям безопасности.

Отличительные характеристики

- Технология Asset Management — позволяет провести полную инвентаризацию сети и собрать данные о параметрах безопасности, а также избавиться от теневых сегментов инфраструктуры.
- Стандарты PT Essentials — разработаны экспертами Positive Technologies, содержат оптимальный набор проверок для повышения уровня защищенности систем.
- Гибкая настройка — позволяет писать кастомные требования безопасности для конкретной компании и создавать из них контролируемые стандарты.

Поможет:

- контролировать соответствие активов важным требованиям безопасности;
- управлять безопасностью конфигураций систем;
- защитить от уязвимостей нулевого дня;
- усилить MaxPatrol VM для полноценного анализа защищенности.

PT Sandbox

Песочница для защиты от сложного и неизвестного ВПО.

Песочница PT Sandbox устанавливается в инфраструктуре и подключается ко множеству источников, обеспечивая своевременное обнаружение неизвестного ВПО и угроз нулевого дня.

Отличительные характеристики

- Единственная песочница, которая обнаруживает сложные новые угрозы на уровне гипервизора, операционной системы и виртуальной машины.
- Легко встраивается в инфраструктуру и контролирует основные каналы передачи файлов и ссылок.
- Адаптируется к особенностям бизнеса, обеспечивая защиту от целенаправленных атак.
- Обеспечивает высокое качество детекта с помощью комбинации статических и поведенческих методов анализа вредоносных программ.

61%

доля PT Sandbox в сегменте Sandbox/Песочницы[1]

В 2024 году:

- ускорили PT Sandbox в девять раз благодаря совокупности новых возможностей, реализованных в течение года (увеличение количества виртуальных машин, параллельно запускаемых на одном узле поведенческого анализа, настройка предварительной фильтрации файлов и очереди на проверку);
- написали более 100 новых правил корреляции (техники) и статических правил (идентификация семейств ВПО и инструментов атакующих), а также более 1 тыс. правил для обнаружения вредоносного сетевого трафика;
- расширили возможности работы со ссылками — продолжаем развивать защиту почты от фишинга и спама.

В условиях постоянно растущего числа киберугроз все большее число компаний понимают, что выгоднее устранять уязвимости на ранних стадиях, чем разбираться с последствиями атак хакеров. Для этого разработчики применяют AppSec-инструменты — они выявляют слабые места в процессе разработки и помогают повысить защищенность ресурса.

[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 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

PT Application Inspector

Инструмент для выявления уязвимостей и тестирования безопасности приложений.

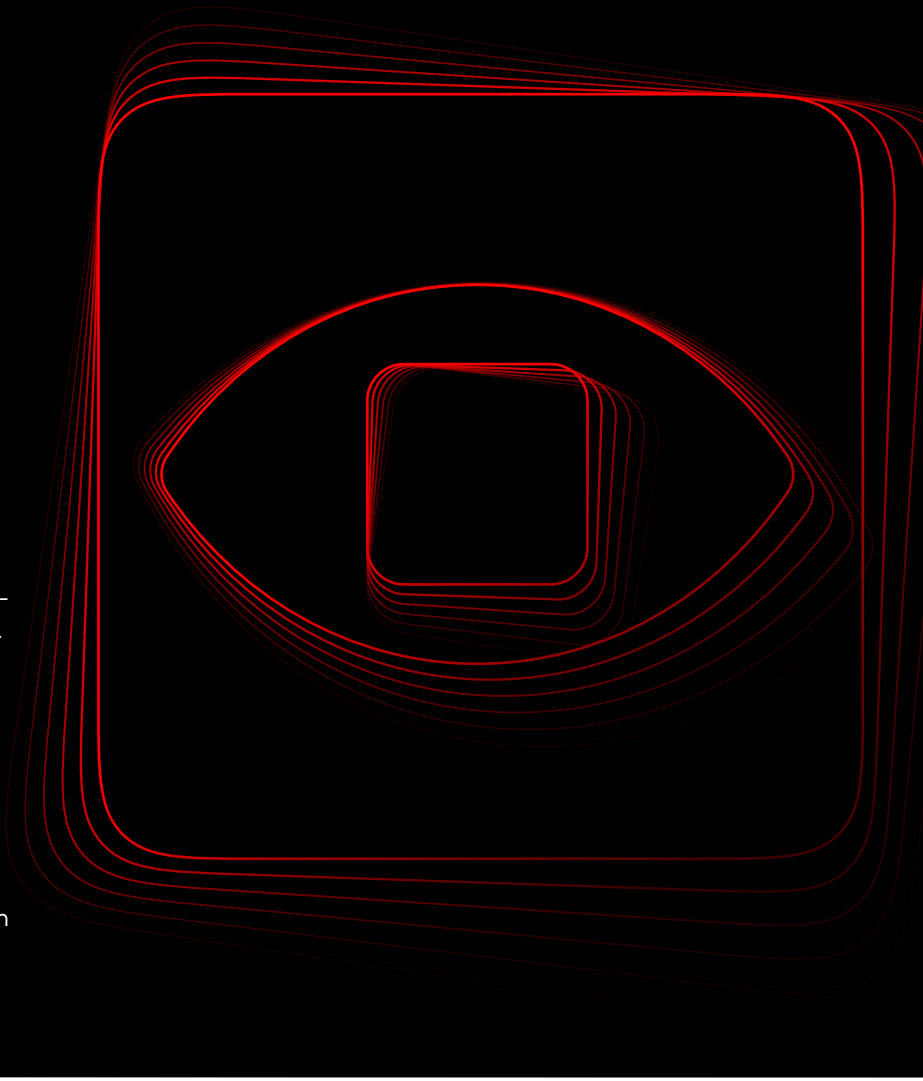
Позволяет специалистам ИТ и ИБ находить слабые места в коде ПО и уязвимости внешних библиотек, а также подтверждать и недокументированные возможности.

В 2024 году:

- выпустили восемь релизов PT Application Inspector и шесть релизов плагинов для IDE;
- сумели поставить продукт в ведущие компании банковской отрасли и поддержали язык разработки смарт-контрактов;
- сделали много полезных фич, таких как мультиязычное сканирование, мастер разбора уязвимостей, удаленное сканирование из плагинов, импорт и экспорт правил анализа;
- почти в три раза увеличили количество загрузок плагинов PT Application Inspector из маркетплейсов.

Отличительные характеристики

- Результаты анализа максимально понятны разработчику: информация об уязвимости содержит диаграмму, иллюстрирующую работу приложения в момент эксплуатации уязвимости.
- Помимо штатного UI продукта, мы реализовали возможность работы с результатами в привычном разработчику виде посредством WebIDE и плагинов для сред разработки.
- Безопасная разработка требует выстраивания диалога между ИБ и R&D. Лицензионная политика продукта позволяет вовлекать разработчиков в этот процесс без дополнительных затрат на лицензии.
- И разумеется, мы понимаем, что анализ кода — это не разовое мероприятие, а часть процесса сборки. Поэтому PT Application Inspector обеспечивает возможность встраивания задачи выявления уязвимостей в конвейер сборки на базе CI-систем.



PT BlackBox

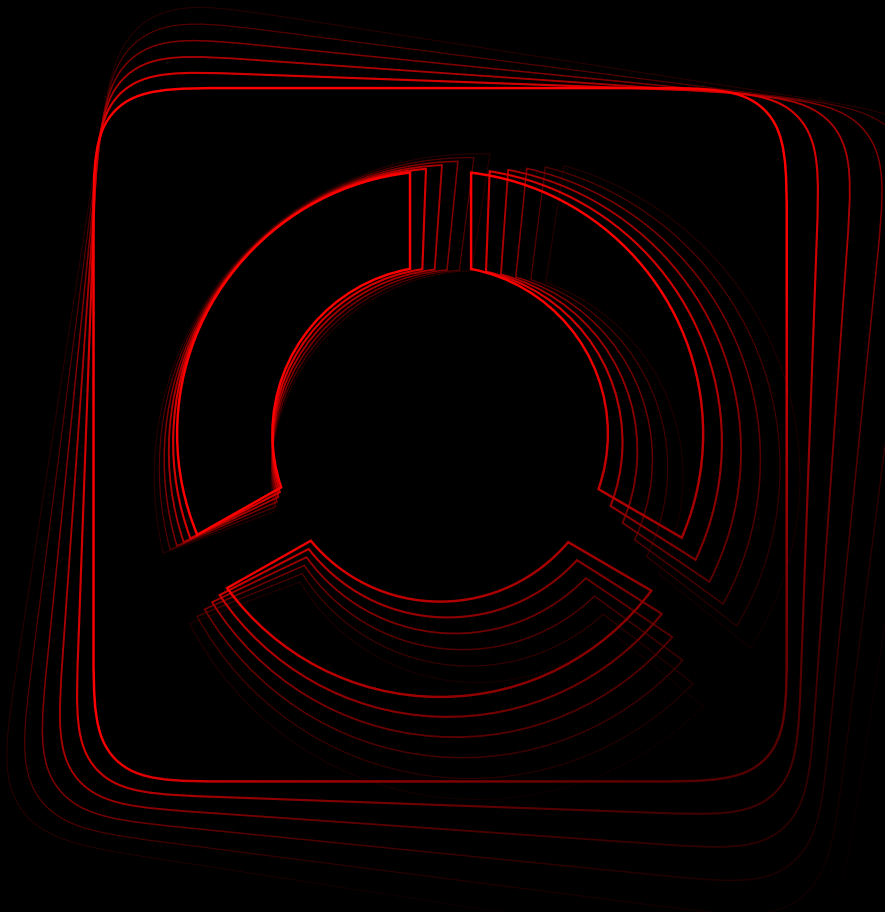
Динамический анализатор защищенности приложений.

Позволяет анализировать защищенность приложений методом черного ящика: сканер имитирует поведение злоумышленника, у которого нет знаний о внутреннем устройстве приложения, что позволяет оценивать защищенность веб-приложения без использования каких-либо исходных данных, кроме адреса веб-цели.

По самым осторожным оценкам аналитиков ЦСР, к 2027 году объем рынка безопасной разработки приблизится к 17,75 млрд руб., увеличившись почти в два раза, а по самым оптимистичным — к 60 млрд руб. (рост в семь раз относительно 2022 года).

В 2024 году:

- перезапустили облачный PT BlackBox Scanner, что дало нашим пользователям пусть ограниченный, но свободный доступ к технологиям для исследования безопасности приложений. Эти данные и обратная связь от пользователей помогли в развитии коммерческой версии продукта;
- коллаборация с PT Cloud Application Firewall открыла глаза многим пользователям на то, что их продукты уязвимы. Это позволило сформировать дополнительный спрос на решения безопасности Positive Technologies;
- выпустили большой релиз продукта 3.0, в котором значительно расширены возможности сканирования и повышена производительность решения. С новой версией сканер переведен на контейнерную архитектуру под управлением Kubernetes, что позволит эффективно внедрять PT BlackBox в компаниях любого размера и адаптировать систему к различным типам нагрузки.



PT Application Firewall

Межсетевой экран уровня веб-приложений.

Не всегда компаниям удается быстро устранить уязвимость в самом приложении, в этих случаях для повышения безопасности системы используются продукты класса WAF (web application firewall). Продукт позволяет защититься от эксплуатации имеющихся уязвимостей без внесения изменений в само приложение.

PT Application Firewall использует движок машинного обучения для точного определения атак класса Shell. Адаптивный анализ поведения пользователей применяется для выявления ботов.

Отличительные характеристики

- Поддержка технологий адаптивного анализа и машинного обучения. PT Application Firewall использует движок машинного обучения для точного определения атак класса Shell. Адаптивный анализ поведения пользователей применяется для выявления ботов.
- Готовые редактируемые шаблоны защиты для популярных веб-фреймворков и приложений. Накопленная экспертиза Positive Technologies позволяет оперативно совместить требования безопасности и модель угроз в шаблоне профиля защиты. Готовые шаблоны для защиты популярных фреймворков и платформ (LAMP, ASP.Net, Apache Struts, NodeJS, «1С Битрикс» и др.) помогают минимизировать время активации защиты и ускорить доставку веб-приложений в продуктивную среду. Имеется возможность создания собственных пользовательских шаблонов для защиты специфичных приложений.
- Настраиваемые лимиты количества обращений за единицу времени к критичным функциям веб-приложений (Rate Limiting). Данная технология применяется для эффективной блокировки активностей типа Brute Force, Credentional Stuffing, Parsing и L7 DOS. Обеспечивает защиту бизнеса от поведенческих кибератак, включая базовую защиту от DDoS.
- Поддержка новых механизмов защиты API. PT Application Firewall способен обнаруживать атаки внутри API благодаря возможности анализа вложенных данных API-запросов. Поддерживаются современные технологии API (например, Graphql API и JWT) и блокировка атак из перечня OWASP API Top-10.

PT Cloud Application Firewall

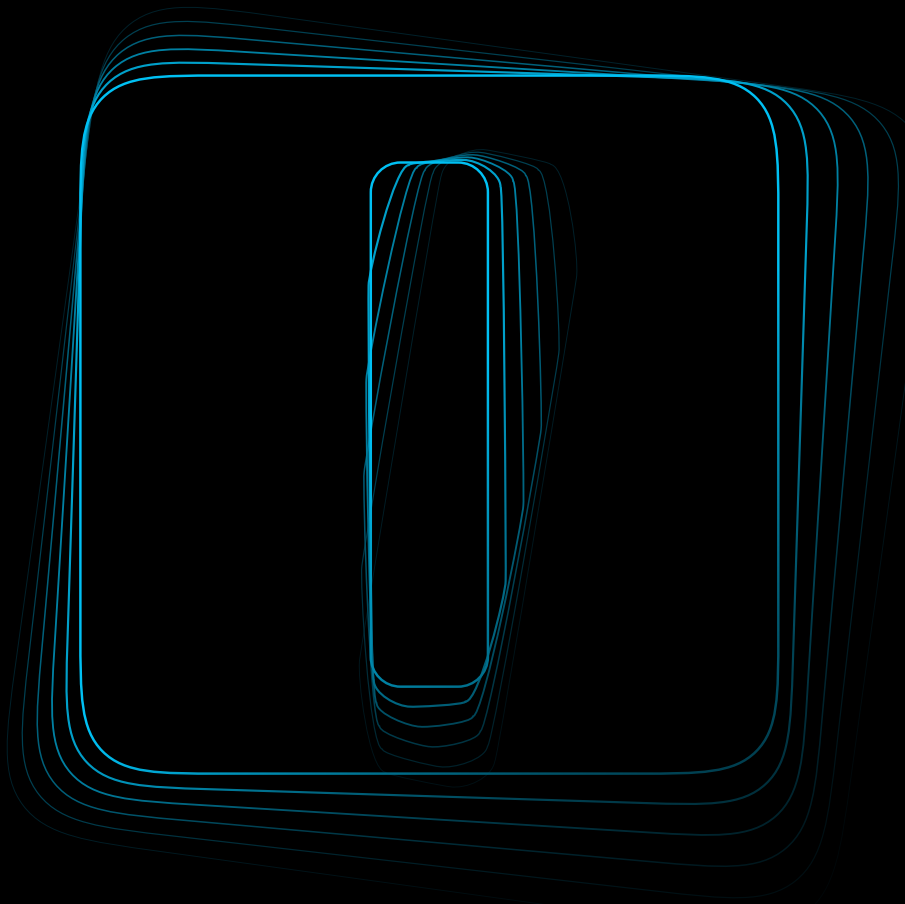
Облачный продукт для защиты веб-приложений.

Отличительные характеристики

- PT Cloud Application Firewall распространяется по подписке: чтобы быстро начать защищать свой ресурс, не нужно приобретать аппаратное обеспечение и нанимать специалистов.
- Все работы по обслуживанию продукта — на стороне доверенного партнера. Эти условия делают PT Cloud Application Firewall максимально выгодным для компаний малого и среднего бизнеса.

В 2024 году:

- +100 новых клиентов;
- 20 технологических партнеров предлагают рынку наши решения;
- услуги на базе решения используется более чем в 15 отраслях.



MaxPatrol EDR

Защита конечных устройств от сложных и целевых атак.

71 %
доля успешных «пилотов»

88
«пилотов» провели в 2024 году (вдвое больше, чем в 2023 году)

Отличительные характеристики

- Использует корреляционный движок на агенте для поведенческого анализа. Такой механизм позволяет обнаруживать целые классы ВПО по их активности без использования сигнатур конкретного образца ВПО, а на события об обнаружении можно назначать действия для автоматического реагирования.
- Автономная работа агента. Это важно для условий, когда агент не подключен к корпоративной сети или интернету. Не менее важно и для организаций, где есть закрытые сегменты, осложнена работа с какими-то внешними серверами и внешними репутационными/сигнатурными базами.
- MaxPatrol EDR позволяет осуществлять автоматическое реагирование на обнаруженные угрозы. Дает возможность гибко управлять сбором данных и правилами реагирования на конечных устройствах.

В 2024 году:

- адаптировали продукт под запросы крупных заказчиков: дали возможность создавать свой экспертный контент;
- позволили сократить затраты на внедрение и настройку продукта, добавив возможность тиражировать политики, обновили экспертные политики;
- расширили возможности продукта, усилив как базовые механики сбора, обнаружения и реагирования, так и дополнительные, необходимые для крупных клиентов: кластеризацию, возможность использования собственных пакетов экспертизы, массовое реагирование;
- добавили управление Windows Audit, конфигурацию сбора аудита для Linux, модуль «Карантин», удаленный Shell и другие возможности;
- расширили покрытие инфраструктуры клиентов, поддержали несколько новых ОС;
- заложили основу для интеграции с целым спектром решений в области ИБ — за счет публичного API-реагирования;
- почти в два раза по сравнению с 2023 годом выросло количество новых, уникальных заказчиков;
- помогали нашему SOC защитить турнир «Игры Будущего»;
- MaxPatrol EDR стал основным инструментом для сбора событий с устройств в проектах, в которых мы работаем совместно с SOC;
- продукт помог заказчикам выстоять на киберучениях;
- дважды участвовали в кибербитве Standoff, дав командам защиты механику реагирования на атаки.

PT Container Security

Инновационное решение для комплексной защиты инфраструктуры гибридного «облака».

Предоставляет набор инструментов для защиты программных продуктов на различных этапах жизненного цикла и дает всем пользователям доступ к экспертизе по ИБ, обеспечивающей лучшие отраслевые стандарты и практики по безопасности контейнеров (контейнер — это программный пакет, который включает в себя все необходимое для запуска ПО: приложение, его зависимости, библиотеки и системные инструменты).

Отличительные характеристики

- Максимальное покрытие цикла безопасной разработки: от анализа используемого инструментария и собираемых образов разрабатываемых приложений до аудита событий внутри кластера.
- Контроль действий, выполняемых в кластере, с возможностью блокировки. Например, для того, чтобы разрешить пользователям ручной запуск команд внутри контейнера в тестовом сегменте и запретить это делать в промышленном.
- Сбор событий безопасности на уровне системных вызовов ядра ОС узла кластера обеспечивает максимум деталей о происходящем и усложняет обход механизмов безопасности злоумышленником.
- Обогащение событий безопасности данными из оркестратора с последующей передачей в SIEM позволяет реализовать полноценный XDR уровня кластера.
- Поддержка политик, разработанных на языках высокого уровня (Go, Python и т. д.) позволяет реализовывать любые сложные сценарии реагирования на события ИБ.

В 2024 году:

- мы стали партнерами с ведущими российскими ИТ-компаниями (VK, Orion Soft, «Флант»);
- активно несли экспертизу по безопасности контейнеров на рынок: участвовали в кибербитве на Positive Hack Days Fest и осеннем Standoff. Продукт отлично показал себя с точки зрения производительности: мы документально подтвердили работу на нагрузке в десятки тысяч EPS (событий в секунду);
- команда проявила себя не только на мероприятиях Positive Technologies — мы представили свои доклады на митапах Bi.Zone и на конференции HighLoad++;
- выпустили три полноценных релиза за год, которые в общей сложности включали в себя более 10 новых фич! Первыми среди разработчиков отечественных систем защиты контейнеров реализовали интерфейс для проведения расследований инцидентов в контейнерах и первыми поддержали интеграцию с отечественным облачным реестром образов Yandex Container Registry;
- совместно с экспертной лабораторией PT Expert Security Center (PT ESC) мы подготовили более 20 детекторов (сигнатур) выявления аномалий в контейнерах и первыми на российском рынке средств защиты контейнеров закрыли 100% матрицы Mitre ATT&CK для контейнеров (Containers Matrix) и провели ее проверку вместе с командой Standoff;
- начали развивать продуктовый подход в разработке и совместно с отделом продуктовых исследований провели два исследования: пользовательского опыта и использования средств контейнеризации.

PT Industrial Security Incident Manager

Система глубокого анализа трафика в промышленных ИТ-инфраструктурах.

Продукт контролирует безопасность технологической сети, позволяет вовремя распознать угрозы кибербезопасности и предотвратить ущерб предприятию.

[1] Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Отличительные характеристики

- Единое окно для мониторинга безопасности всей технологической сети и ее компонентов.
- Использует уникальную базу знаний (PT ISTI), которая содержит данные об угрозах, направленных на российские промышленные компании.
- Поддерживает более 130 промышленных и общесетевых сетевых протоколов.
- Выявляет угрозы на конечных устройствах российского и зарубежного производства, используемых в сети производства.
- Непрерывно контролирует промышленную сеть и видит любые несанкционированные изменения в ней.
- Точно и своевременно обнаруживает следы атакующих во всей инфраструктуре предприятия.
- Эффективен при анализе угроз, расследовании инцидентов и реагировании на кибератаки.
- Помогает закрыть обязательные технические требования для объектов КИИ согласно положениям Федерального закона № 187-ФЗ[1] и Приказа ФСТЭК № 239.
- Не влияет на работу предприятия и бизнес-процессов.

В 2024 году:

- запустили новое поколение продукта — PT ISIM 5. Теперь PT ISIM собирает данные из сетевого трафика и конечных узлов предприятия. Такой подход позволяет вовремя выявить кибератаку независимо от точки проникновения в промышленную сеть. Кроме этого, новое поколение позволяет выявлять отклонения от значимых показателей техпроцессов, обнаруживает компрометацию SCADA-систем и видит потенциально опасные действия персонала;
- представили новый пользовательский интерфейс. Удобно визуализирует собранные данные через дашборд и виджеты. Сокращает время анализа выявленных угроз и ускоряет реагирование на кибератаки. Появилась новая схема технологической сети, в которой показаны вся технологическая инфраструктура, нарушения ее целостности, сетевые взаимодействия и, конечно, самые опасные атаки;
- ускорили PT ISIM в десять раз. Теперь продукт может выявлять кибератаки на сложных видах технологического трафика с большей пропускной способностью, чем раньше.

PT Threat Intelligence Feeds

Уникальные потоки данных об угрозах.

Ландшафт киберугроз постоянно меняется. Отслеживание этих изменений, особенно с учетом специфики отрасли, — сложная задача, требующая серьезных аналитических ресурсов.

PT Threat Intelligence Feeds — потоки данных (фиды) об индикаторах компрометации для информирования команд ИБ об актуальных киберугрозах.

Отличительные характеристики

- Проверенные индикаторы компрометации — получены в ходе расследований реальных атак и исследования деятельности киберпреступных группировок. Кроме того, доступны данные обезличенной телеметрии с инсталляции продуктов Positive Technologies.
- Расширенный контекст — позволяет лучше понять потенциальную угрозу, разработать план ее устранения и повысить скорость реагирования на инциденты.
- Готовые наборы данных — собраны в группы в зависимости от сценариев выявления различных видов угроз.

Преимущества:

- обогащает данными средства защиты и повышает их эффективность, что позволяет обнаруживать и предотвращать атаки на ранних этапах;
- усиливает проактивную защиту от угроз за счет интеграции с продуктами Positive Technologies и средствами защиты информации других вендоров;
- помогает оценить уровень опасности инцидента, потенциальный ущерб компании и приоритизировать задачи реагирования.

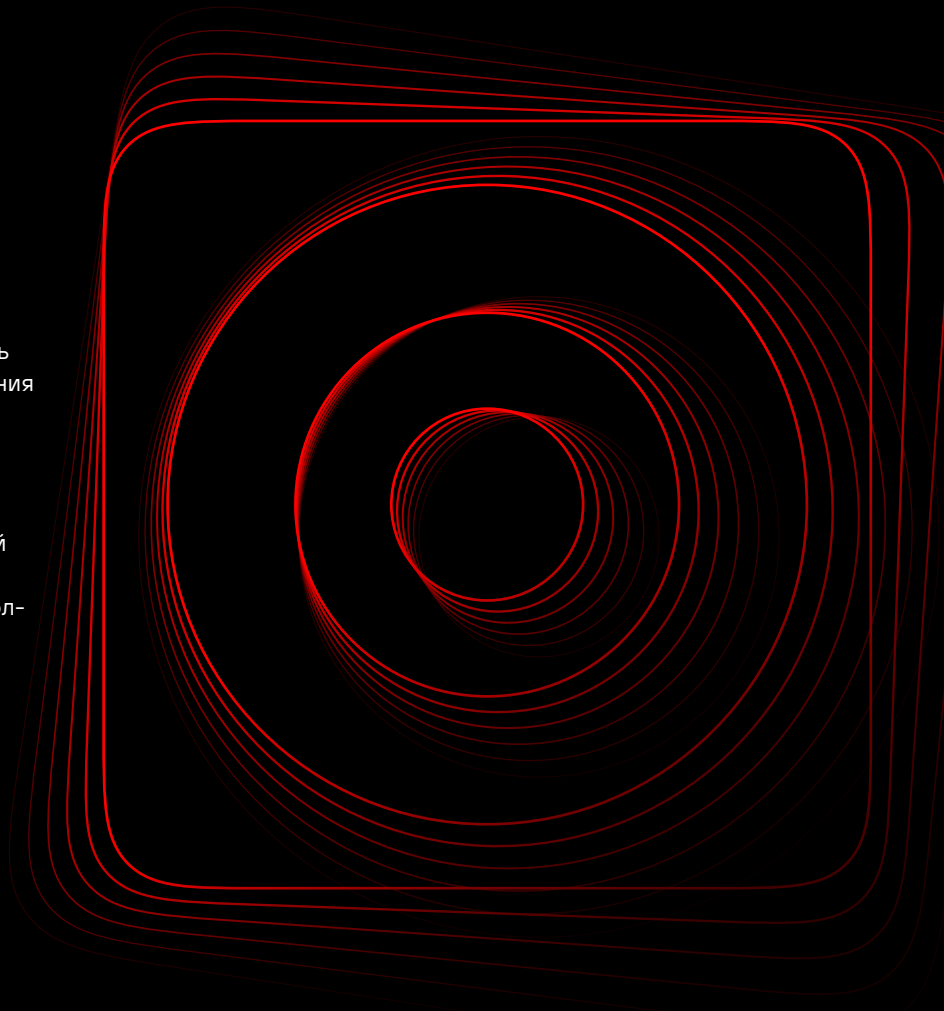
Поможет:

- повысить эффективность средств защиты информации.

PT MultiScanner

PT MultiScanner — система многоуровневой защиты от вредоносных программ. Продукт способен за час анализировать десятки тысяч файлов, которые попадают в корпоративную сеть через сетевой и почтовый трафик, загружаются в веб-приложения и файловые хранилища компании.

Мультивендорная антивирусная защита позволяет использовать обширную базу данных и быстро интегрируется в ИТ-инфраструктуру клиента. PT MultiScanner — единственный продукт в России, который поддерживает три отечественных антивирусных программных модуля, позволяя тем самым выполнять требования регуляторов.



MaxPatrol 8

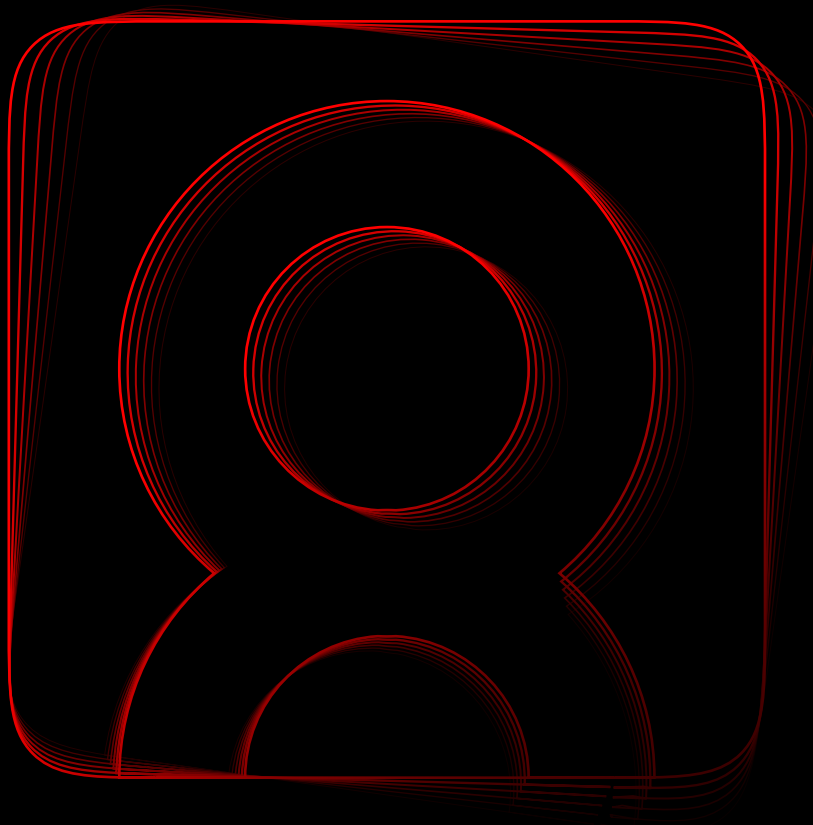
MaxPatrol 8 используется для оценки защищенности информационных систем. В его основе лежат мощные механизмы тестирования на проникновение (PenTest), системных проверок (Audit) и контроля соответствия стандартам (Compliance). Результатом их работы становится объективная оценка уровня безопасности ИТ-инфраструктуры как в целом, так и частных элементов, благодаря чему своевременно обнаруживаются уязвимости и предотвращаются атаки на них.

10%

доля MaxPatrol 8 в сегменте Vulnerability management / управление уязвимостями[1]

Отличительные характеристики:

- продуманная архитектура для покрытия георазпределенных компаний;
- большое количество поддерживаемых сканируемых типов ПО;
- гибкие настройки по сканированию на уязвимости.



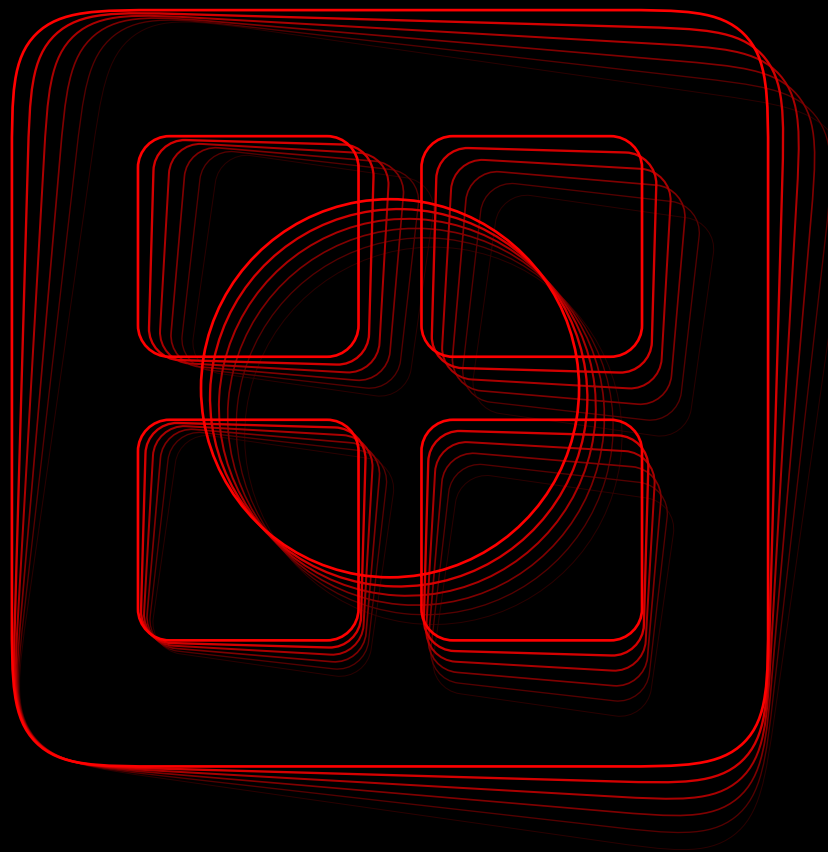
[1] По оценке Компании. Оценка получена на основе анализа данных открытых продаж для российских поставщиков решений класса VM в 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

XSpider

XSpider — профессиональный сканер уязвимостей, который позволяет оценить реальный уровень безопасности ИТ-инфраструктуры компании. Сканер быстро и точно выявляет компоненты сети, находит и анализирует уязвимости, после чего выдает четкие и понятные рекомендации по их устранению. База уязвимостей XSpider постоянно пополняется нашими специалистами, позволяя выявлять новые угрозы, а благодаря автоматизации сканирования оптимизируется работа ИБ-специалистов.

4%

доля XSpider 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 2024 году и не учитывает неофициальные закупки иностранного ПО. Оценка дана в ценах конечного клиента без НДС (если применимо).

ПТ Ведомственный центр

Система «ПТ Ведомственный центр» автоматизирует процесс обработки инцидентов и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и другие отраслевые CERT[1]. Эта функция особенно актуальна для компаний, которым необходимо подключиться к инфраструктуре ГосСОПКА и информировать НКЦКИ об инцидентах. Наш продукт кастомизируется под процессы компании, легко интегрируется в ее ИТ-инфраструктуру и экономит время ИБ-специалистов.

Что такое ГосСОПКА

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, нарушение или прекращение работы которых может крайне негативно повлиять на экономику страны или безопасность граждан. Корпоративный центр ГосСОПКА автоматизирует выявление инцидентов, реагирование на них и взаимодействие с НКЦКИ. В соответствии с Федеральным законом № 187-ФЗ организации здравоохранения, науки, транспорта, связи, энергетики, банковской сферы, горнодобывающей, металлургической и химической промышленности обязаны подключиться к инфраструктуре ГосСОПКА и уведомлять НКЦКИ об обнаруженных компьютерных инцидентах.

[1] Computer Emergency Response Team — группа реагирования на компьютерные инциденты, представляющая собой независимый коллектив экспертов, в список задач которых входят постоянный мониторинг информации о появлении угроз в сфере ИБ, их классификация и нейтрализация.

PT Industrial Cybersecurity Suite

PT XDR

PT Platform 187

PT Anti-APT

Выполнение указа 250

Безопансность объектов КИИ

Построение центра ГосСОПКА

3.5

Наши решения

Разработанные нами решения обеспечивают максимальный уровень защищенности и соответствуют российским и международным стандартам безопасности.

PT Industrial Cybersecurity Suite

Это первое комплексное решение для защиты промышленности от киберугроз, в его составе основные продукты Positive Technologies: PT ISIM, MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, MaxPatrol EDR. В решение также входят полный спектр наших сервисов анализа защищенности промышленных систем и услуги экспертного центра безопасности PT Expert Security Center по обнаружению, реагированию и расследованию сложных инцидентов, связанных с АСУ ТП. Оно позволяет обнаруживать злоумышленника на всех этапах развития атаки в промышленных средах и своевременно реагировать на нее.

Выполнение Указа № 250

Это решение мы разработали для организаций, которые обязаны выполнять требования Указа Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее — Указ № 250). Оно включает продукты Positive Technologies, которые позволяют выполнять основные законодательные требования к обеспечению ИБ[1] и технические требования Указа № 250. Наше решение предотвращает и выявляет атаки на сети клиентов, а также автоматизирует взаимодействие с ГосСОПКА и отраслевыми центрами кибербезопасности.

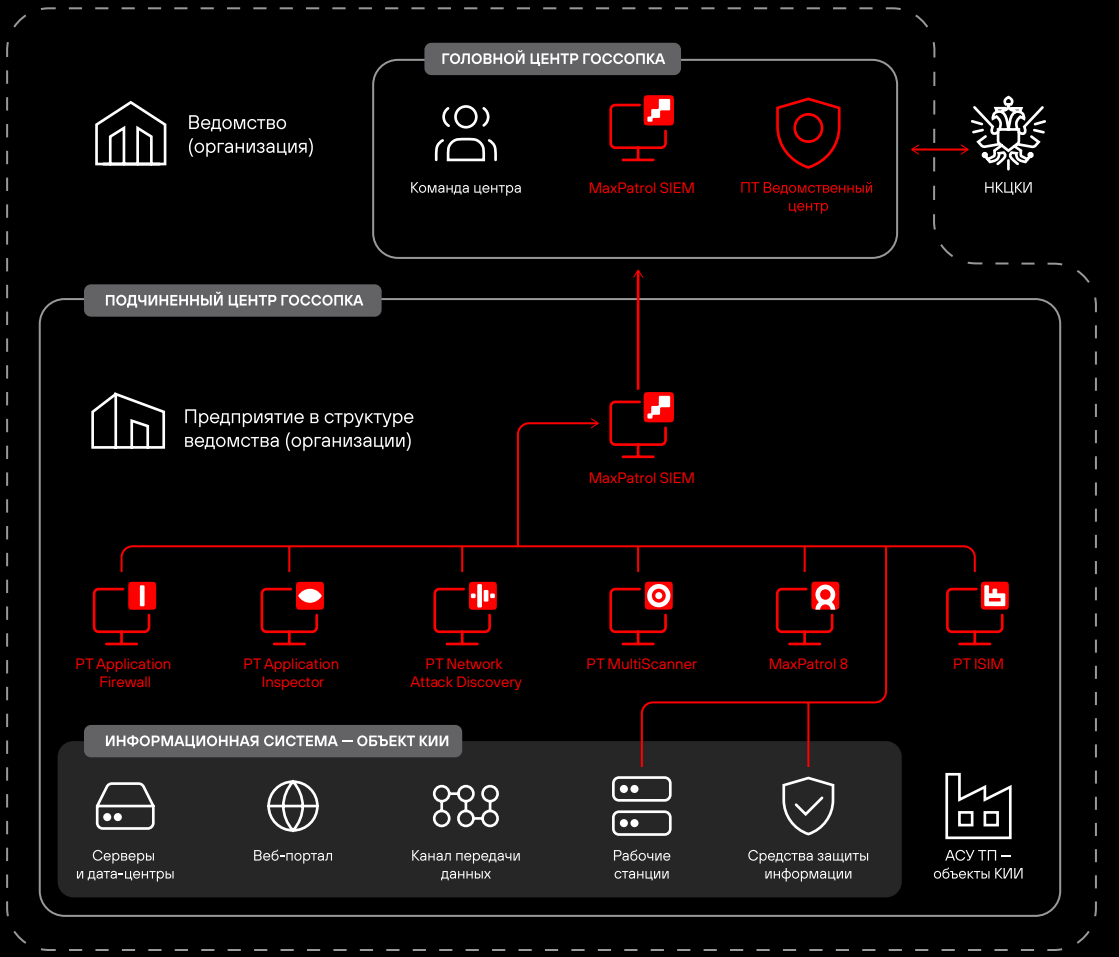
[1] Требования по защите объектов КИИ, информационной системы персональных данных (ИСПДн), государственной информационной системы (ГИС), организаций банковской системы.

Безопасность объектов КИИ

Наше решение объединяет продукты Positive Technologies, которые позволяют соответствовать требованиям по защите объектов КИИ. Система выявляет кибератаки на начальных стадиях и находит не обнаруженные ранее признаки взлома при помощи ретроспективного анализа, непрерывно взаимодействуя с ГосСОПКА в режиме онлайн-чата.

Построение центра ГосСОПКА

Мы предлагаем нашим клиентам поэтапное построение центра ГосСОПКА на основе ключевых продуктов Positive Technologies. Это решение включает и услуги нашего экспертного центра безопасности (PT Expert Security Center): специалисты дополнят команду клиента собственной экспертизой и возьмут на себя сопровождение работы ИБ-подразделений.



PT Platform 187

PT Platform 187 — программно-аппаратный комплекс для реализации мер защиты значимых объектов КИИ в соответствии с требованиями ФСТЭК России и построения ведомственных центров ГосСОПКА согласно требованиям ФСБ России.

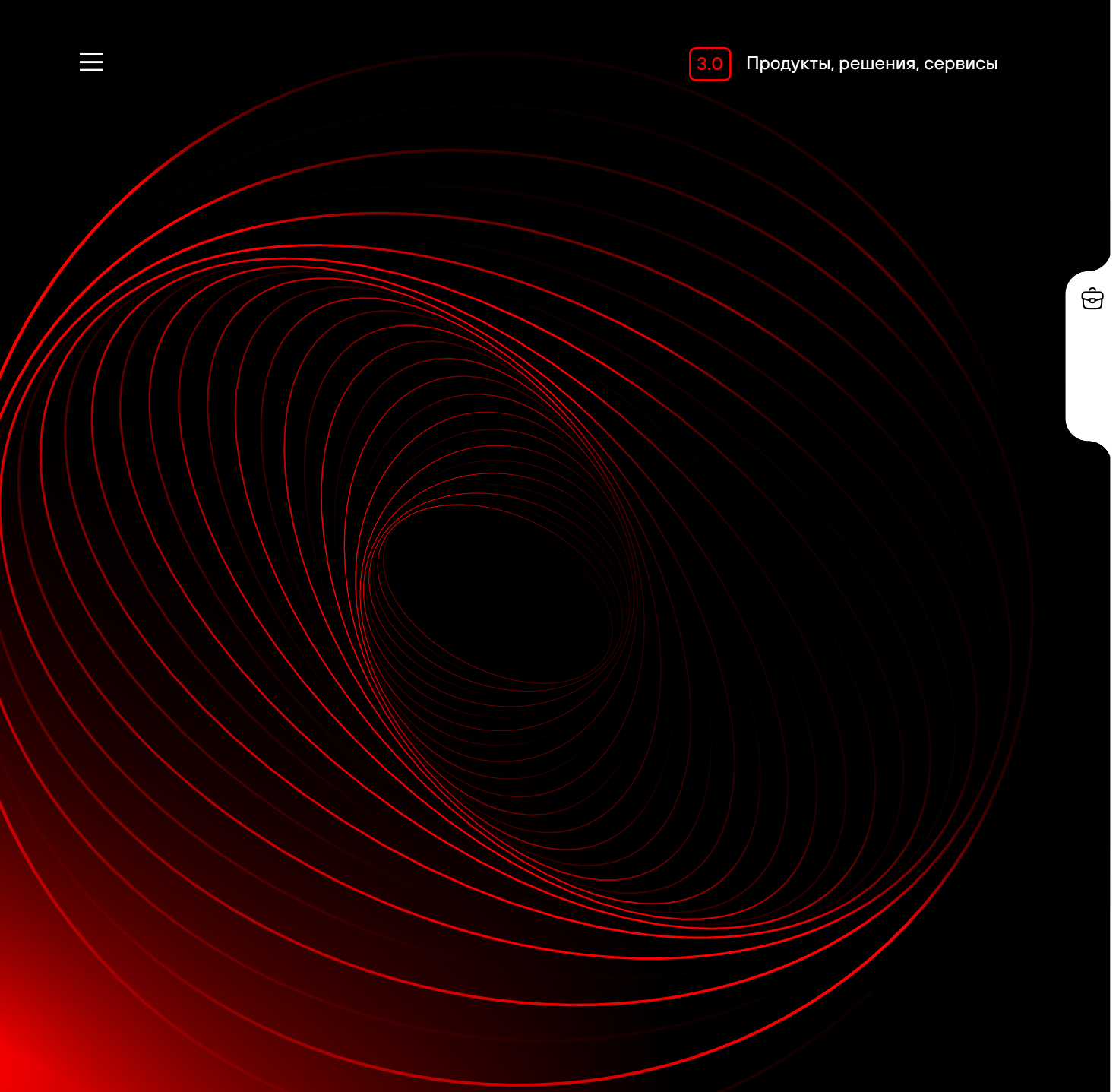
Платформа включает в себя набор технических средств, которые помогают соответствовать основным требованиям законодательства, автоматизируют ИБ-процессы в компании и значительно повышают их эффективность. PT Platform 187 объединяет пять наших ключевых продуктов: MaxPatrol SIEM, MaxPatrol 8, PT Network Attack Discovery, PT MultiScanner и «ПТ Ведомственный центр». Продукты платформы своевременно обновляются для выполнения актуальных требований регуляторов.

PT XDR

PT Extended Detection and Response — система, разработанная для защиты конечных устройств от кибер-угроз. Решение собирает и обогащает данные с рабочих станций и серверов, выполняет статический и динамический анализ угроз как на устройствах, так и во внешних системах, выявляет в ИТ-инфраструктуре организации сложные целевые атаки и позволяет реагировать на них как вручную, так и автоматически.

PT Anti-APT

Комплекс раннего выявления сложных угроз PT Anti-APT защищает клиентов от наиболее актуальных в России угроз, выявляет атаки на Active Directory и противодействует фишингу. Решение помогает оперативно обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования.



3.6

Наши услуги и экспертиза

Услуги для повышения защищенности от киберугроз помогут оценить готовность компании к противостоянию злоумышленникам, оперативно принять меры для защиты от кибератак и устранения их последствий.

Платформа Standoff 365

«

Платформа Standoff 365 — это более 14 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. Здесь они могут ближе познакомиться с разными ИБ-профессиями и прокачать свои скилы.

Алексей Новиков,
управляющий директор Positive Technologies

- **Кибербитва Standoff**
- **Standoff Cyberbones**
- **Онлайн-полигон Standoff**
- **Standoff Bug Bounty**

По итогам игр по кибербезопасности пользователями платформы стали более 600 новых участников, а победители получили не только возможность посетить киберфестиваль PHDays в мае, но и пройти сразу на второй этап стажировки PT Start. В 2025 году мы планируем повторить два сезона игр и расширить базу пользователей Standoff молодыми участниками.

Кибербитва Standoff

Кибербитва Standoff — международные соревнования по кибербезопасности, которые помогают организациям прокачать уровень зрелости своей службы ИБ в условиях интенсивных кибератак, а белым хакерам усовершенствовать свои навыки.

В 2024 году:

- провели три масштабные международные кибербитвы: Standoff 13 во время Positive Hack Days 2, Standoff во время Петербургского международного экономического форума и кибербитву Standoff 14 онлайн в ноябре. Всего в кибербитвах официально приняла участие 141 команда. Это были и синие, и красные[1] команды. В этом году мы активно развивали международное комьюнити — приглашали команды из разных стран. В течение года в кибербитвах, по нашим подсчетам, приняли участие более 1,6 тыс. человек из 40 стран;
- запустили международные игры по кибербезопасности для студентов. На отборочные этапы международных игр пришло около 100 красных и 100 синих студенческих команд, многие из которых ничего не знали про формат Standoff и до этого играли только в CTF[2]. В финале осеннего сезона международных игр — студенческой кибербитве — встретились 50 лучших команд.

Онлайн-полигон Standoff

Онлайн-полигон Standoff — инструмент для регулярной отработки специалистами по ИБ навыков выявления и расследования кибератак. Онлайн-полигон представляет из себя виртуальную ИТ-инфраструктуру типовой компании, доступную онлайн в режиме 24/7.

В течение 2024 года команда работала над обновлением онлайн-полигона Standoff для синих команд. Из важных событий — вывели в продакшен новый модуль регулируемых атак, который симулирует пользовательскую активность, действует на основе сценариев атак крупнейших APT-группировок и является важной частью новой концепции продукта онлайн-полигона.

В первом полугодии 2025 года сможем предложить клиентам Positive Technologies обновленную версию продукта для регулярной прокачки навыков по кибербезопасности.

[1] Синяя команда — команда защитников, красная — команда атакующих.

[2] CTF, Capture the Flag — соревнования в форме командной игры, главная цель которой — захватить «флаг» у соперника в приближенных к реальности условиям. Команды решают прикладные задачи, чтобы получить уникальную комбинацию символов (флаг). Далее участники отправляют флаг в специальную платформу и получают подтверждение, что задача решена верно или стоит попытаться дать ответ еще раз.

Кибериспытания

Positive Technologies активно развивает подходы к измерению эффективности ИБ. Одним из ключевых инструментов в этом направлении стала программа APT Bug Bounty (кибериспытания), которая проходит на платформе Standoff 365. Компания уверена, что такие практики станут стандартом индустрии ИБ.

«

Кибериспытания — это логичное развитие нашей стратегии по защите инфраструктуры медиахолдинга. Мы формируем понимание ее наиболее важных областей и фокусируемся на них. Экспертиза Positive Technologies и платформа Standoff Bug Bounty позволяют расширить «партнерство» с багхантерами для оценки защищенности наиболее ценных активов от целевых атак.

Евгений Руденко,
директор по кибербезопасности Rambler&C

Standoff Bug Bounty

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 2024 году мы активно развивали Standoff Bug Bounty:

- вывели на платформу в три раза больше компаний по сравнению с 2023 годом;
- позволили багхантерам[1] заработать в течение года 95 млн руб. и сдать почти 5 тыс. отчетов;
- привлекли на платформу международных багхантеров;
- Standoff Bug Bounty включена в реестр отечественного ПО;
- провели во Вьетнаме первый международный ивент Standoff Hacks.

С начала 2024 года количество пользователей платформы увеличилось с 8 тыс. до 18 тыс.

Standoff Cyberbones

Standoff Cyberbones — онлайн-симулятор с реальными кейсами, собранными по итогам кибербитв Standoff, где специалисты по ИБ могут расследовать инциденты, чтобы лучше понимать, как выявлять подобные ситуации и реагировать на них в повседневной работе.

В 2024 году команда Standoff запустила новый продукт Standoff Cyberbones, где любой специалист по ИБ может проверить свои практические навыки расследования инцидентов. У продукта есть бесплатная версия для всех желающих, а также расширенная — с большим количеством заданий — для клиентов Positive Technologies.

С момента запуска продукта в сентябре 2024 года более 500 человек успешно расследовали хотя бы один киберинцидент.

[1] Багхантеры — «охотники за уязвимостями», белые хакеры, которые занимаются поиском уязвимостей в ИТ-сетях, системах и приложениях за вознаграждение.

ХардкорИТ

ХардкорИТ — это методология определения путей и времени атаки хакера методом анализа ИТ-инфраструктуры. Она помогает оценить киберустойчивость ИТ-инфраструктуры организации перед атаками, нацеленными на причинение недопустимого ущерба[1]. Основана на математическом моделировании времени кибератак.

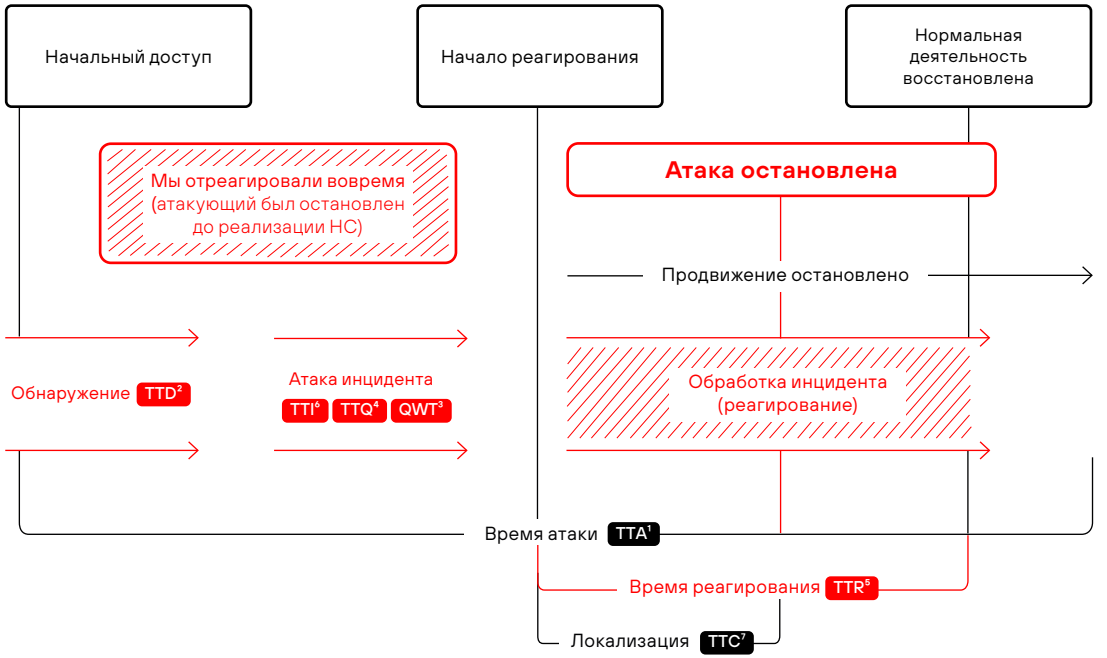
Применение методологии дает бизнесу:

- знание о том, где и зачем нужна ИБ, чтобы тратить ресурсы на защиту только необходимых бизнес-систем;
- знание сценариев, ключевых и целевых систем, что делает процесс защиты более осознанным, точечным и менее затратным;
- определение самых проблемных ИТ-активов ключевых и целевых систем, функциональных областей их работы, на которых нужно сфокусировать ресурсы по защите;
- расчет интуитивно понятных бизнесу метрик кибербезопасности, определение наиболее приоритетных маршрутов злоумышленников для защиты целевых систем, определение готовности противостоять реализации недопустимых событий;
- определение набора инициатив на основе моделирования атак на бизнес-системы, приоритизацию шагов по обеспечению киберустойчивости на основе аналитики моделирования атак;
- формирование программы трансформации, сбалансированной с точки зрения затрат бизнеса для обеспечения состояния киберустойчивости. Программа трансформации создается с учетом инициатив бизнес-стратегии и ИТ-стратегии.

Принцип работы: TTA>TTC

ИТ-инфраструктура — это не только основа для бизнес-процессов, но и зона потенциальных угроз. Ее правильная настройка обеспечивает баланс между эффективностью поддержки бизнеса и возможностью противостоять атакам. Цель ХардкорИТ — достичь такого состояния, при котором время атаки превышает время ее локализации, что позволяет специалистам успешно предотвратить развитие инцидента.

[1] Недопустимый ущерб / недопустимое событие (НС) — полученный в результате кибератаки критический урон, делающий невозможным достижение операционных и (или) стратегических целей или приводящий к значительному нарушению основной деятельности организации.



1 TTA, время реагирования — время реагирования, которое защитники тратят на локализацию, устранение и восстановление. Время отчитывается с момента, когда принято решение, что делать.
2 TTD, время обнаружения — время от момента первоначального доступа агента угрозы в сеть организации до окончания обнаружения атаки.
3 QWT — время ожидания в очереди с момента регистрации инцидента, до его назначения исполнителю или передачи в автоматизированную систему для обработки.
4 TTQ — время верификации, то есть определения легитимности обнаруженной активности (исключение ложноположительного срабатывания).
5 TTR, время атаки — время от первоначального доступа до момента реализации недопустимого события отсчитывается с момента, когда принято решение, что делать.
6 TTI — время оценки, то есть сбора информации об инциденте (о его масштабе, приоритете) и иных необходимых сведений для принятия решения о дальнейшем реагировании (и самого принятия решения о реагировании).
7 TTC, время локализации — время от категоризации инцидента (то есть когда становится ясно, что делать) до окончания локализации (блокирования и изоляции агента угрозы).

Positive Education

Positive Education центр обучения Positive Technologies, где практики обучают результативной кибербезопасности.

Мы запустили направление Positive Education в 2023 году, чтобы ответить на один из ключевых вызовов цифровой эпохи острую нехватку квалифицированных специалистов в сфере информационной безопасности.

К 2023 году в России дефицит ИБ-специалистов составил 45% около 50 тыс. человек. Сегодня кибербезопасность по уровню потребности в специалистах находится там, где была ИТ-отрасль десять лет назад. При этом рынок продолжает расти: кибератаки становятся все сложнее и масштабнее. По данным Positive Technologies, в 2024 году число успешных атак на организации выросло на 5% по сравнению с 2023 годом.Кибербезопасность это стратегическая отрасль и ее развитие начинается с людей. Positive Education это пространство, где соединяются практика, технологии и методология Positive Technologies, чтобы формировать архитекторов кибербезопасности: тех, кто мыслит системно, берет ответственность и способен вести отрасль вперед.

В 2024 году:

- запустили корпоративные и профессиональные программы, которые прошли свыше 15 000 пользователей. Средняя оценка удовлетворенности 4,8 из 5, что отражает высокий уровень качества обучения. Количество обученных специалистов удвоилось по сравнению с 2023 годом. В 2025 году мы продолжим расширять линейку программ;
- провели Positive Hack Camp международный образовательный проект по кибербезопасности, в котором приняли участие более участвовали 70 специалистов из 20 стран мира;
- начали обучение топ-менеджеров в корпоративном формате. Теперь наши программы охватывают сотрудников всех уровней от специалистов до руководителей и управленцев;
- совместно с Минцифры запустили Школу преподавателей кибербеза (ШПК). Более 1 600 преподавателей и преподающих экспертов из 300+ организаций подали заявки и продолжают обучение в рамках проекта.

Наша команда умеет защищать информационные активы клиентов наиболее эффективно и с учетом лучших мировых практик. Услуги в области обеспечения кибербезопасности, которые мы оказываем нашим клиентам, полностью соответствуют законодательным и отраслевым нормам, а также основываются на лучших международных примерах.

Анализ защищенности приложений

Проведение всестороннего анализа приложения для выявления потенциальных уязвимостей, предоставление объективной и независимой оценки его защищенности

Реагирование на инциденты и их расследование

Оперативное восстановление всех обстоятельств инцидента и устранение его последствий

Ретроспективный анализ на выявление следов компрометации

Выявление всех факторов компрометации объектов инфраструктуры организации, ранее не зафиксированных штатными системами защиты

Техническая поддержка

Техническое сопровождение продуктов Positive Technologies

Профессиональные сервисы

Сервисы по управлению продуктами Positive Technologies: от внедрения до модернизации

Финансовые результаты

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.

4.1

Отгрузки и валовая прибыль отгрузок

Мы используем показатель «Отгрузки» — валовый объем заключенных 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 2024 года со сроками оплаты позднее 31 марта 2025 года исключаются из показателя «Отгрузки с НДС»;
- отгрузка сертификатов на абонентское обслуживание (услуги технической поддержки, подписка на услуги анализа инцидентов и др.) 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 и входят в состав себестоимости.

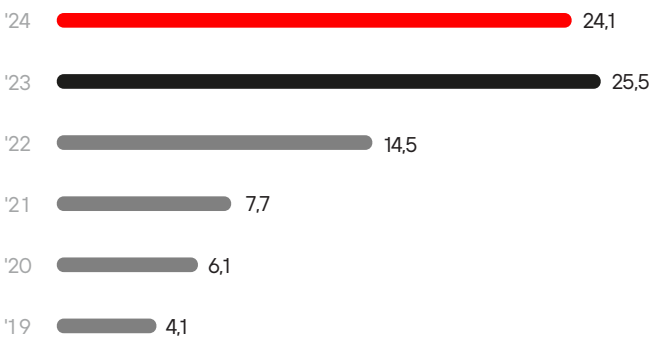
[1] Рибейт — премия за достижение объемов продаж и субсидирование покупателей.

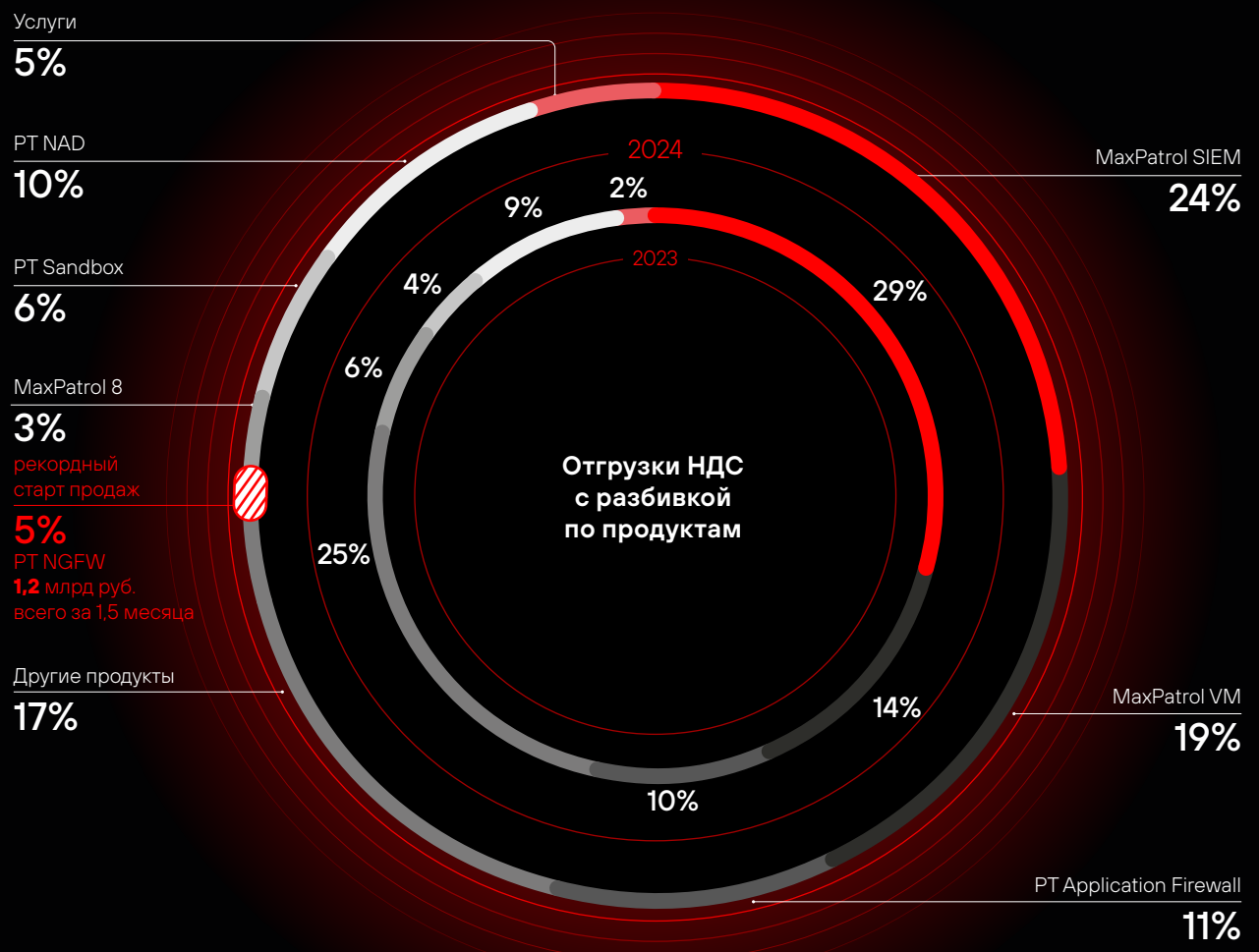
Итоговый **объем оплаченных отгрузок** клиентам Компании в 2024 году составил 24,1 млрд руб., что на 5,7% ниже показателя прошлого года и существенно ниже прогнозов и ожиданий менеджмента. Причины расхождения фактических результатов с планами Компании в основном обусловлены внутренним фактором. В рамках трансформации, которая началась еще в IV квартале прошлого года и во многом уже завершена, Positive Technologies ставит перед собой ключевую цель на 2025 год — вернуться к темпам роста бизнеса, превышающим общую динамику рынка.

+42,5 %

CAGR за пять лет (2019–2024)

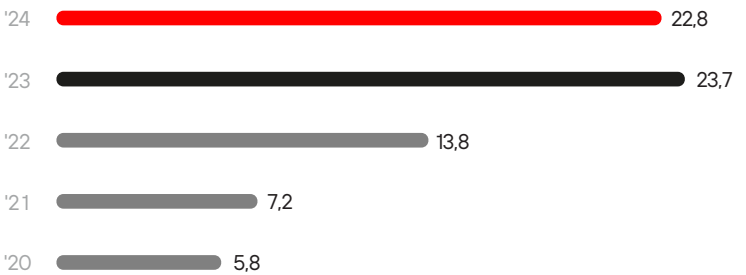
Отгрузки, млрд руб.





В структуре продаж продуктами-лидерами, показавшими наибольший вклад в общий результат, стали MaxPatrol SIEM (24%), MaxPatrol VM (19%), PT Application Firewall (11%) и PT Network Attack Discovery (10%). Новое флагманское решение PT NGFW (Next Generation Firewall, межсетевой экран нового поколения), массовые продажи которого стартовали в ноябре, продемонстрировало рекордный старт: 1,2 млрд руб., или 5% от общего объема отгрузок.

Валовая прибыль отгрузок, млрд руб.



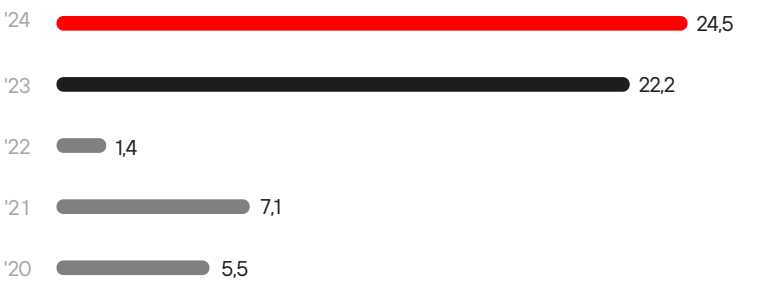
Валовая прибыль отгрузок, представляющая собой отгрузки, уменьшенные на сумму НДС, бонусов партнерам и прочих прямых расходов по итогам 2024 года составила 22,8 млрд руб. (23,7 млрд руб. годом ранее).

4.2

Выручка

Выручка по МСФО увеличилась на 10%, до 24,5 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 2025 года.

Выручка, млрд руб.

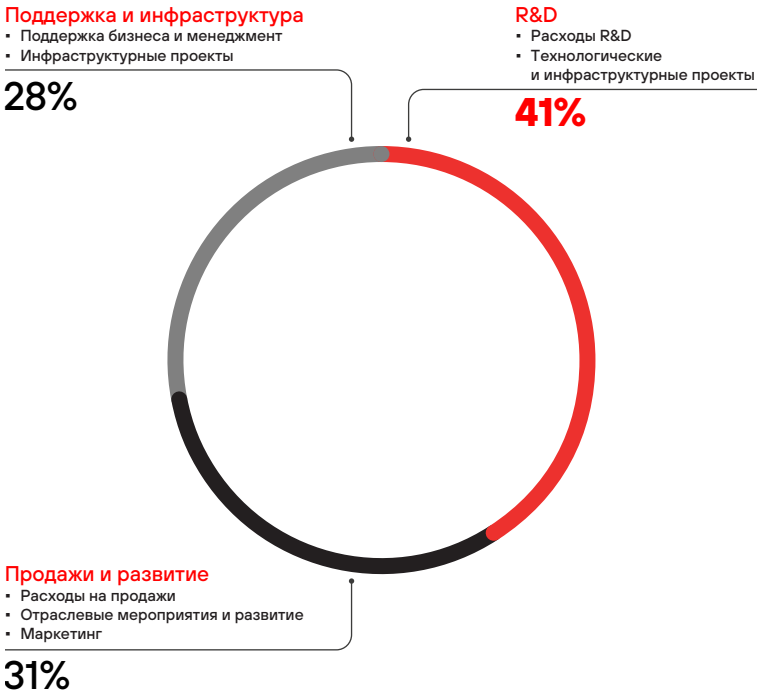


4.3

Операционные расходы

Операционные расходы Компании по итогам года выросли на 60%. В их структуре основную долю (41%) составили расходы на R&D и технологические инфраструктурные проекты, 31% — продажи и развитие, а доля расходов на поддержку бизнеса и инфраструктуры составила 28%.

Структура операционных расходов



4.4

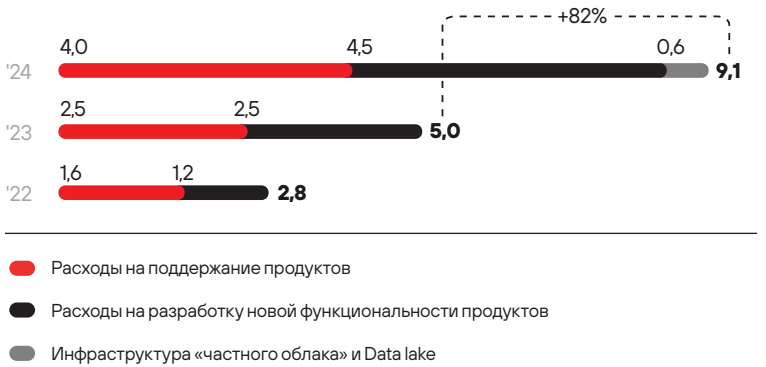
Расходы на разработку и создание нематериальных активов

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., увеличившись на 82%. Вложения, которые мы делаем сейчас в разработку, принесут прибыль в следующих периодах: перед нами стоят задачи по кратному масштабированию бизнеса, выходу в новые технологические и географические сегменты рынка.

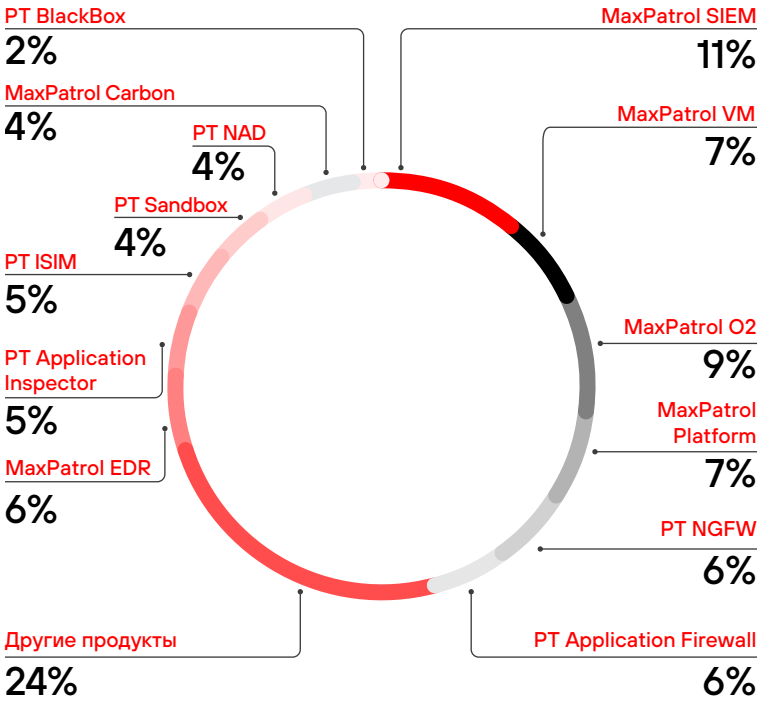
Продукты на разных стадиях жизненного цикла требуют разного объема капитальных затрат. В 2024 году наибольший их объем пришелся на MaxPatrol SIEM, MaxPatrol O2, MaxPatrol VM, PT Application Firewall, PT NGFW.

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

Общие R&D-расходы, млрд руб.



Структура расходов R&D по продуктам



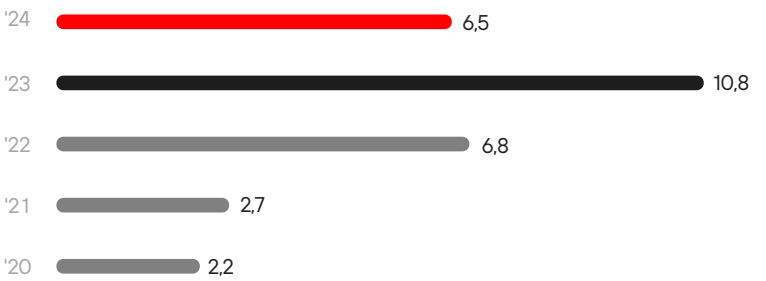
4.5

EBITDA и чистая прибыль

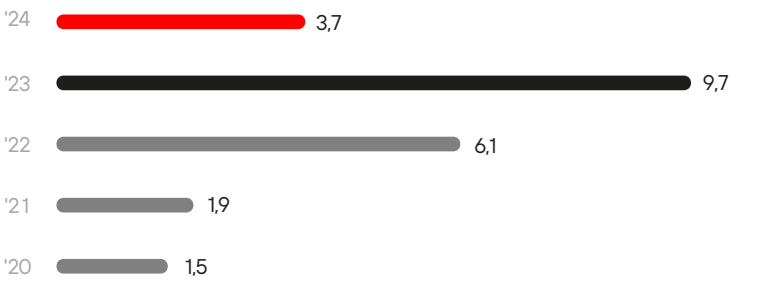
EBITDA Компании составила 6,5 млрд руб. при уровне маржинальности 26%, что является высоким показателем для крупных публичных компаний.

Чистая прибыль за 2024 год составила 3,7 млрд руб. (9,7 млрд руб. годом ранее) при маржинальности на уровне 15%.

EBITDA, млрд руб.



Чистая прибыль, млрд руб.



4.6

EBITDAC и NIC

EBITDAC, управленческий показатель, который отличается от EBITDA на сумму разницы между «Отгрузками» и «Выручкой», а также сумму капитализируемых расходов, составил минус 1,2 млрд руб.

Второй управленческий показатель — NIC.

Принимая во внимание сохранение высокой динамики расходов при отсутствии роста отгрузок, чистая прибыль без учета капитализируемых расходов (NIC) оказалась в отрицательной зоне: чистый убыток по управленческой отчетности составил 2,7 млрд руб.

В 2025 году Компания планирует вернуться к таргетируемым темпам роста бизнеса и рентабельности по чистой прибыли (NIC), что обеспечит возможность выплаты дивидендов по итогам 2025 года.

EBITDAC, млрд руб.

Показатель	2021	2022	2023	2024
EBITDAC, млрд руб.	1,5	5,2	8,9	(1,2)

NIC, млрд руб.

Показатель	2021	2022	2023	2024
NIC, млрд руб.	1,2	5,0	8,7	(2,7)

Подробнее о Дивидендной политике Positive Technologies

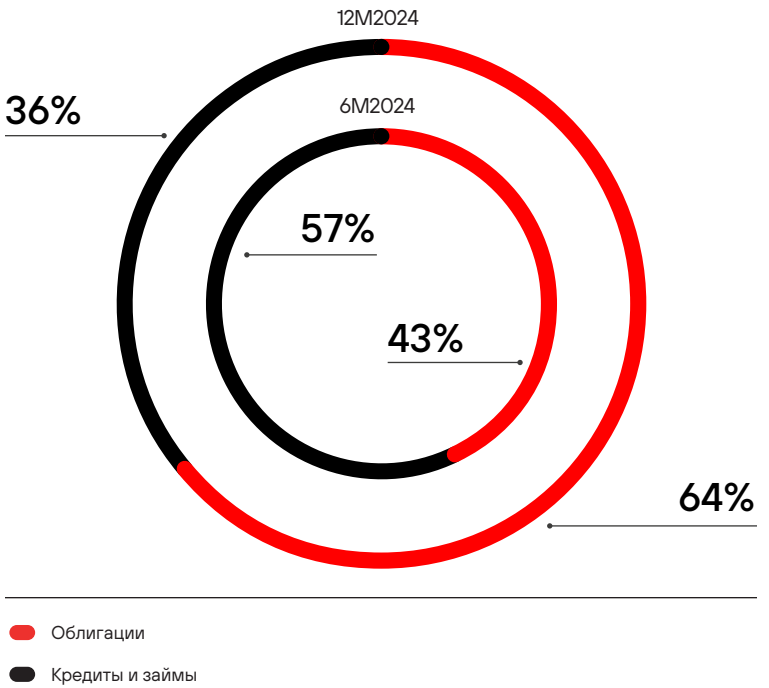
4.7

Долговая нагрузка и управление долгом

Отношение чистого долга к EBITDA по состоянию на конец 2024 года составило 2,97. При этом, по предварительным данным, на конец I квартала 2025 года показатель снизился до более комфортного значения — ниже 1,9. Текущие показатели долговой нагрузки позволяют Компании соблюдать все необходимые ковенанты. На фоне общего увеличения долгового портфеля Positive Technologies существенно улучшила его структуру, снизив зависимость от краткосрочных банковских кредитов. С этой целью в 2024 году были размещены два выпуска облигаций (1, 2), позволяющих Компании привлекать долгосрочное финансирование на более комфортных и предсказуемых условиях. Доля облигаций в общем портфеле заимствований по состоянию на конец отчетного периода составила 64%.

Чистый долг/EBITDA*

Структура чистого долга[1]



* Без арендной задолженности, не применяется МСФО 16.

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

4.8

Основные финансовые результаты 2024 года

Показатель	2021, факт	2022, факт	2023, факт	2024, факт
Отгрузки с НДС, млрд руб.	7,7	14,5	25,5	24,1
Валовая прибыль отгрузок, млрд руб.	7,2	13,8	23,7	22,8
Доля валовой прибыли от отгрузок без НДС, %	97%	98%	95%	95%
EBITDAC, млрд руб.	1,6	5,2	8,9	(1,2)
NIC (чистая прибыль без капитализации расходов), млрд руб.	1,2	5,0	8,7	(2,7)
Рентабельность по NIC, %	16%	35%	35%	–
NIC за вычетом налога на сверхприбыль, млрд руб.		4,8		
Рентабельность по NIC, %		34%		
Корректировка по выручке, млрд руб.	(0,4)	(0,3)	(1,6) [4]	
Капитализируемые расходы, млрд руб.	1,5	1,9	3,5	
Амортизация расходов и прочее, млрд руб.	(0,4)	(0,5)	(0,9)	
МСФО метрики				
Выручка[1], млрд руб.	7,1	13,8	22,2	24,5
EBITDA[2], млрд руб.	2,7	6,8	10,8	6,5
Рентабельность по EBITDA, %	38%	50%	49%	26%
Чистая прибыль, млрд руб.[3]	1,9	6,1	9,7	3,7

1 Выручка = Отгрузки без НДС + Корректировка по выручке — бонусы покупателям.
2 EBITDA = EBITDAC + Корректировка по выручке + Капитализируемые расходы.
3 Чистая прибыль = NIC + Корректировка по выручке + Капитализируемые расходы + Амортизация расходов.
4 Корректировка включает разницу в признании техподдержки на (1,3) млрд руб., пролонгирующихся лицензий на (0,9) млрд руб., а также корректировку на оплаты до 31 марта 2024 года на сумму 0,6 млрд руб.

Разница между управленческой отчетностью и МСФО

	2024 год	2023 год
Отгрузки с НДС	**24,1**	**25,5**
НДС	(0,6)	(0,7)
Отгрузки без НДС	**23,5**	**24,9**
Разницы между отгрузками и выручкой	0,9	(2,6)
▪ разницы в сроках признания техподдержки и пролонгирующихся лицензий	(0,3)	(2,2)
▪ рибейты покупателям	(0,4)	(1,0)
▪ оплаты, не полученные до 31.03.2025 (до 31.03.2024 для 2023 года)	2,1	1,0
▪ оплаты по прошлогодним отгрузкам, полученные после 31.03.2024 (после 31.03.2023 для 2023 года)	(0,5)	(0,4)
Выручка МСФО	**24,5**	**22,2**
EBITDA	**6,5**	**10,8**
Разницы между отгрузками и выручкой, за исключением рибейтов покупателям	(1,3)	1,6
Капитализированные расходы и прочее	(6,4)	(3,5)
EBITDAC	**(1,2)**	**8,9**
Прибыль за период	**3,7**	**9,7**
Разницы между отгрузками и выручкой, за исключением рибейтов покупателям	(1,3)	1,6
Капитализированные расходы и прочее	(6,4)	(3,5)
Амортизация капитализированных расходов, капитализация процентов и прочее	1,4	0,9
NIC	**(2,7)**	**8,7**

Открытый диалог с инвесторами

«

Уважаемые инвесторы!

В современном мире прозрачность является одним из ключевых факторов устойчивости и доверия к публичной компании. Positive Technologies неизменно следует принципам открытости, демонстрируя ответственность перед акционерами, клиентами и обществом. Мы уверены, что только честный диалог и готовность говорить о сложном укрепляют настоящие партнерские отношения.

2024 год был для нас непростым: финансовые результаты не оправдали ожиданий менеджмента. Тем не менее мы верим в потенциал Компании и продолжаем двигаться вперед. В 2025 году Компания планирует вернуться к таргетируемым темпам роста бизнеса и рентабельности по чистой прибыли (NIC), что обеспечит возможность выплаты дивидендов по итогам 2025 года.

Мы благодарим вас за доверие и поддержку. Ваша лояльность особенно ценна в моменты, когда Компания работает над внутренней трансформацией и готовит почву для будущего устойчивого роста.

Спасибо, что вы с нами!

Юрий Мариничев,
директор по связям с инвесторами Positive Technologies

5.1

Завоевываем доверие

2024 год для Positive Technologies стал годом открытого диалога с инвестиционным сообществом. Мы провели ряд масштабных мероприятий для инвесторов, где лично общались с акционерами и аналитиками, отвечали на их вопросы и обсуждали перспективы Компании. Также мы активно участвовали в IR-конференциях, что позволило еще больше укрепить связи с ключевыми участниками инвестиционного рынка.

>20
IR-конференций

>25
онлайн-эфиров

6
встреч с блогерами и инфлюенсерами

7
встреч с финансовыми аналитиками и журналистами

Мы продолжили развивать коммуникацию с инвесторами, уделяя особое внимание нашим каналам в социальных сетях и внедряя новые инструменты для диалога. Наша цель — не просто поддерживать контакт, а задавать высокий стандарт открытости, делая взаимодействие с Компанией комфортным и понятным для каждого акционера.

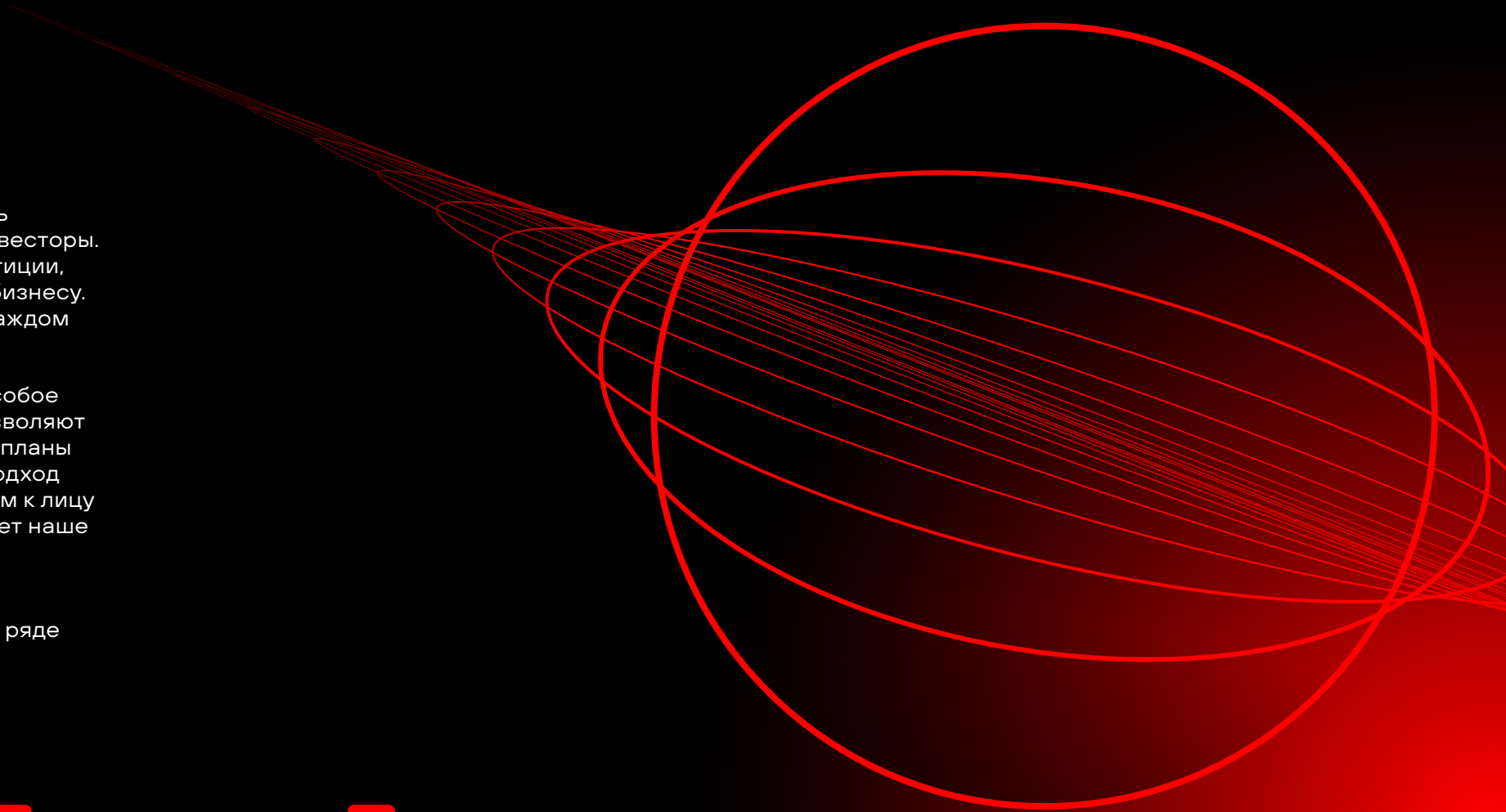
Мы стремимся к тому, чтобы бизнес Positive Technologies был прозрачным и доступным для всех участников инвестиционного сообщества, а не только для специалистов в области кибербезопасности. Это позволяет нам выстраивать отношения и укреплять доверие среди широкого круга инвесторов.

Наша главная цель — сформировать сообщество лояльных инвесторов, которые не только понимают перспективы бизнеса, но и разделяют нашу миссию и ценности. Вместе мы создаем крепкий фундамент для устойчивого роста и развития Компании.

→ **IR на «Играх Будущего»**

→ **День инвестора в «Лужниках»**

Лицом к инвестору



Среди акционеров Positive Technologies есть как розничные, так и институциональные инвесторы. Для нас их вложения — это не просто инвестиции, а доверие, которое они оказывают нашему бизнесу. Мы это ценим и стараемся оправдывать в каждом аспекте своей работы.

Живое общение с акционерами занимает особое место в нашей стратегии. Такие встречи позволяют не только отвечать на вопросы и обсуждать планы Компании, но и находить индивидуальный подход к каждому инвестору. Взаимодействие лицом к лицу помогает лучше понять друг друга, что делает наше сотрудничество крепче и эффективнее.

В 2024 году Positive Technologies в качестве организатора и партнера приняла участие в ряде крупномасштабных мероприятий.

День инвестора в «Лужниках»
«Игры Будущего»
Лидеры неформального общения

День инвестора в 2024 году

+75% год к году

~700 участников очной сессии

›5 тыс. пользователей смотрели онлайн-трансляцию мероприятия

+506% год к году

~9,7 тыс. посетителей инвестиционного стенда

День инвестора в «Лужниках»

Инновации, кибербезопасность и честный диалог с инвесторами — и все это Positive Hack Days 2.

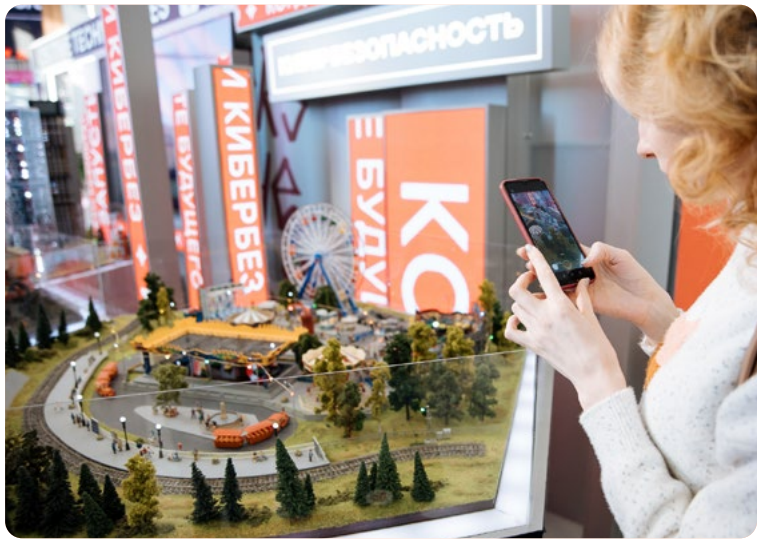
С 23 по 26 мая 2024 года спорткомплекс «Лужники» стал центром крупнейшего события года в области кибербезопасности — фестиваля Positive Hack Days 2. Открытую часть мероприятия за четыре дня посетило более 138 тыс. человек.

Одним из ключевых событий фестиваля стал День инвестора Positive Technologies, предоставивший акционерам уникальную возможность встретиться с руководством Компании и погрузиться в атмосферу кибербезопасности. Посетители могли пройтись по цифровому мегаполису, познакомиться с интерактивными образовательными инсталляциями, понаблюдать за ходом кибербитвы Standoff и поучаствовать в увлекательных квестах.

На официальной части мероприятия топ-менеджеры Компании представили стратегию технологического развития, рассказали о факторах роста бизнеса, поделились планами по международной экспансии, а также раскрыли детали принципов работы с капиталом.

Однако День инвестора Positive Technologies — это не только презентации и выступления. Мы создали пространство для живого общения, где акционеры смогли задать вопросы, обсудить идеи и получить ответы напрямую от руководства.

Также в течение четырех дней киберфестиваля любой желающий мог посетить наш POSItивный стенд и оценить перспективы инвестиций в кибербезопасность. Формат мероприятия позволил создать теплую и неформальную атмосферу, что особенно ценят наши акционеры.



«Игры Будущего»

С 21 февраля по 3 марта 2024 года в Казани прошел международный фиджитал-турнир «Игры Будущего», официальным партнером по кибербезопасности которого выступила Positive Technologies.

«Игры Будущего» — это масштабное спортивное событие, объединяющее спорт, науку и технологии, где классические дисциплины переплетаются с цифровыми, создавая уникальный формат соревнований.

Во время «Игр Будущего» зрители и участники соревнований получили уникальную возможность заглянуть в мир кибербезопасности на стенде Positive Technologies. Здесь можно было увидеть макет киберполигона Standoff 365 — площадки, где ежедневно отрабатываются навыки противодействия киберугрозам, — и узнать, как работают системы защиты в реальных условиях.

Для гостей стенд стал не только образовательной, но и интерактивной зоной, где можно было повысить уровень своей киберграмотности и узнать больше об инвестиционном потенциале акций Positive Technologies. Одним из самых популярных развлечений на стенде стал кибервелотренажер, где участники ставили собственные рекорды, одновременно «запуская» акции POSI в космос.

В рамках «Игр Будущего» Positive Technologies организовала встречу с инвесторами и акционерами POSI. На официальной части мы рассказали гостям о нашем пути на бирже, поделились ключевыми достижениями за два года, а также обсудили с аналитиками, как поддержка крупных мероприятий влияет на рост инвестиционной привлекательности компаний. Особое внимание уделили теме кибербезопасности крупных мероприятий. Мы объяснили, как участие в подобных проектах укрепляет имидж Компании и доверие со стороны инвесторов.

Не обошлось и без неформальной части в непринужденной атмосфере. Мы организовали захватывающий ИТ-квиз, где гости проверили свои знания и узнали много нового о мире технологий. Настоящей изюминкой вечера стало выступление иллюзиониста, который впечатлил гостей магическими трюками. Однако главным на встрече, конечно, было живое общение: ответы на вопросы, обмен идеями и возможность лично обсудить волнующие темы с представителями Компании.

Лидеры неформального общения

Мы активно укрепляем связь с инвесторами и аналитиками, используя разные форматы общения. Одним из ярких событий стал ИТ-пикник, прошедший 17 августа в парке «Коломенское», где мы встретились с инвесторами в неформальной обстановке.

В июле 2024 года мы провели POSI Summer Day, где познакомили инвестиционных аналитиков и блогеров с продуктовой линейкой. Также наше инвестсообщество получило возможность посещения продуктовых мероприятий Компании, в частности Positive Security Day и лонч NGFW, прошедших в октябре и ноябре соответственно.

Кроме того, для гостей мы открыли двери нашего офиса, организовав экскурсии, посвященные знакомству с внутренними рабочими процессами Компании. Аналитики и блогеры получили возможность пообщаться с топ-менеджментом Positive Technologies, задать вопросы и узнать больше о наших планах и достижениях. Такие встречи помогают создавать атмосферу доверия и открытости, что является важной частью нашей корпоративной культуры.

ИТ-пикник

Positive Security Day

«Т-Инвестиции»

Более 115 тыс. подписчиков в «Пульсе»

1-е место по количеству подписчиков среди эмитентов

Ставка на соцсети

Мы стремимся быть ближе к нашим инвесторам, обеспечивая открытость и прозрачность в общении. В основе IR-коммуникаций Positive Technologies лежит честный и проактивный подход.

Мы открыто делимся планами Positive Technologies как публичной компании, даем простые и понятные пояснения к ключевым новостям и существенным фактам, рассказываем о наших продуктах и событиях в мире кибербезопасности.

Важной частью этого диалога является внимание к вопросам и комментариям пользователей. Мы стараемся быть максимально доступными, чтобы каждый мог получить ответы от представителей Компании.

Мы представлены на всех ключевых платформах и адаптируем контент под каждую соцсеть, учитывая интересы аудитории. Например, пользователи «Пульса» ценят оперативность и полный охват новостей, в то время как аудитория SMART-LAB предпочитает получать только ключевые новости от эмитента.

Быть там, где удобно нашим инвесторам, и вести диалог на актуальных площадках — один из главных приоритетов Positive Technologies.

В 2024 году наш канал в «Пульсе» сохранил статус базовой платформы для взаимодействия с инвесторами: количество подписчиков за год выросло на 78% и превысило 115 тыс., что вывело нас на первое место среди эмитентов по этому показателю. Аудитория нашего телеграм-канала It's Positive Investing демонстрирует стабильный рост — за год она увеличилась на 45%. Также мы активно развиваем блог на платформе SMART- LAB и канал в «БКС Профит». В отчетном году мы значительно расширили свое присутствие в соцсетях, запустив каналы в «СберИнвестициях» и новой платформе «Импульс», где уже заняли первое место по количеству просмотров.

Чат-бот — POSIтивный инвестор

В 2024 году Positive Technologies сделала еще один шаг навстречу акционерам, запустив чат-бот «POSIтивный инвестор» в «Телеграме». Этот инструмент стал важным дополнением к работе нашей IR-команды, предоставляя инвесторам удобный и доступный способ получать актуальную информацию о Компании.

«POSIтивный инвестор» помогает акционерам лучше понять бизнес Positive Technologies. Чат-бот дает последовательное представление о продуктах Компании, раскрывает ключевые драйверы роста и делится финансовыми показателями. Кроме того, он отвечает на самые часто задаваемые вопросы, делая взаимодействие с Компанией еще более прозрачным и доступным.

Наши ключевые онлайн-площадки

«Т-Инвестиции. Пульс»

115,1 тыс. подписчиков
+78% к 2023 году

222 тыс. просмотров

Телеграм-канал It's Positive Investing

>11,3 тыс. подписчиков
+45% к 2023 году

129 тыс. просмотров в месяц

Блог PT на SMART-LAB

122 поста

66 тыс. просмотров

Канал PT в «БКС Профит»

1,6 тыс. подписчиков

YouTube-канал It's positive investing

1,6 тыс. подписчиков

Честный диалог топ-менеджеров и IR-директора с инвестсообществом

Мы активно взаимодействуем с инвестиционным сообществом, участвуя в эфирах на ведущих инвестиционных платформах. На этих встречах мы делимся ключевыми событиями из жизни Компании, рассказываем о тенденциях в сфере ИБ и отвечаем на вопросы зрителей, создавая пространство для открытого диалога.

В 2024 году мы провели около 25 онлайн-эфиров на таких площадках, как «Финам», «МКБ Инвестиции», «Газпромбанк Инвестиции» и др. Такой формат позволил нам не только делиться актуальной информацией, но и укреплять доверие инвесторов.

Доверие через доступность

Сайт для инвесторов

Мы стараемся, чтобы наши инвесторы могли легко и быстро получать актуальную информацию о Positive Technologies и ее акциях из надежных источников. Для этого, помимо основного сайта Компании, мы создали специализированный сайт для инвесторов. На его страницах в лаконичной и доступной форме представлены ключевые данные, которые делают нашу Компанию привлекательной с точки зрения инвестиций.

На сайте можно найти и скачать финансовые отчеты и корпоративные документы, ознакомиться с оценками аналитиков, прочитать актуальные IR-новости, узнать о предстоящих мероприятиях для инвесторов.

Лицом к аналитикам: датабук

В 2024 году Positive Technologies сделала еще один шаг к открытости, начав выпускать датабук — удобный сборник данных из нашей отчетности. Этот формат позволяет аналитикам легко работать с ключевыми показателями Компании. Введение датабука укрепляет доверие и делает взаимодействие с аналитическим сообществом еще более эффективным.

Сайт для инвесторов | Годовой отчет | Интерактивный годовой отчет

Годовой отчет

Мы активно работаем над тем, чтобы наши годовые отчеты были не только содержательными, но и визуально привлекательными. Для нас это важный инструмент, с помощью которого мы доносим ключевые идеи бизнеса, рассказываем о миссии Компании и ее продуктах.

В 2024 году наши старания получили высокую оценку: годовой отчет Positive Technologies стал призером XXVII конкурса годовых отчетов Московской биржи в номинации «Лучший годовой отчет: инвестиционная привлекательность». Он также вошел в шорт-листы номинаций «Выбор розничных инвесторов» и Гран-при «Лучший годовой отчет компании с капитализацией от 40 до 200 млрд рублей».

Кроме того, наш интерактивный годовой отчет занял третье место в номинации «Лучший дизайн интерактивного годового отчета» на конкурсе RAEX. Это признание подчеркивает качество нашей работы и внимание к деталям.

Мы гордимся достигнутыми результатами и продолжаем совершенствовать коммуникации с инвесторами, создавая удобные и понятные инструменты, которые помогают им принимать осознанные инвестиционные решения.

Investfunds Award
«Лучший IR»

Investment Leaders Award — 2024
«Лучшая стратегия взаимодействия с инвесторами»

1-е место в IR-рейтинге российских эмитентов «Смартлаб»

Russia IPO Awards
«Лучшая команда Investor Relations»

Cbonds
«Лучший IR на российском долговом рынке»

Investment Leaders Award — 2024
«Лучший директор по связям с инвесторами» Юрий Мариничев

«Топ-1000 российских менеджеров»
«IR-директор года» Юрий Мариничев

Делимся опытом

Positive Technologies активно делится опытом и знаниями с инвестиционным сообществом. IR-директор Юрий Мариничев выступил одним из главных спикеров IR-академии Московской биржи, где подробно рассказал о подходах к созданию инвестиционного кейса Компании. Его выступление стало ценным источником информации для специалистов, желающих глубже понять, как успешно развивать и продвигать инвестиционные проекты.

В отчетном году Юрий Мариничев также принял участие в конференции корпоративных клиентов «2024 Moex Pro Active — Московская биржа для бизнеса» и ряде других крупных мероприятий. На этих площадках он поделился опытом выхода Positive Technologies на биржу в уникальном для российского рынка формате прямого листинга, что вызвало значительный интерес у участников.

Наш опыт неклассического IPO был подробно освещен в журнале Cbonds Review. Мы открыто делимся своей уникальной практикой, чтобы показать, как нестандартные подходы могут помочь компаниям эффективно работать на фондовом рынке.

Ключевые достижения IR-команды в 2024 году

В 2024 году Positive Technologies получила высокую оценку от экспертов и участников рынка за прозрачность в коммуникациях с инвесторами, последовательность в реализации планов на фондовом рынке и способность находить нестандартные решения. Эти качества стали основой для укрепления доверия и долгосрочных отношений с акционерами, подтверждая нашу приверженность открытости и инновационному подходу.

5.2

2024 год в цифрах и фактах

Дивидендные выплаты

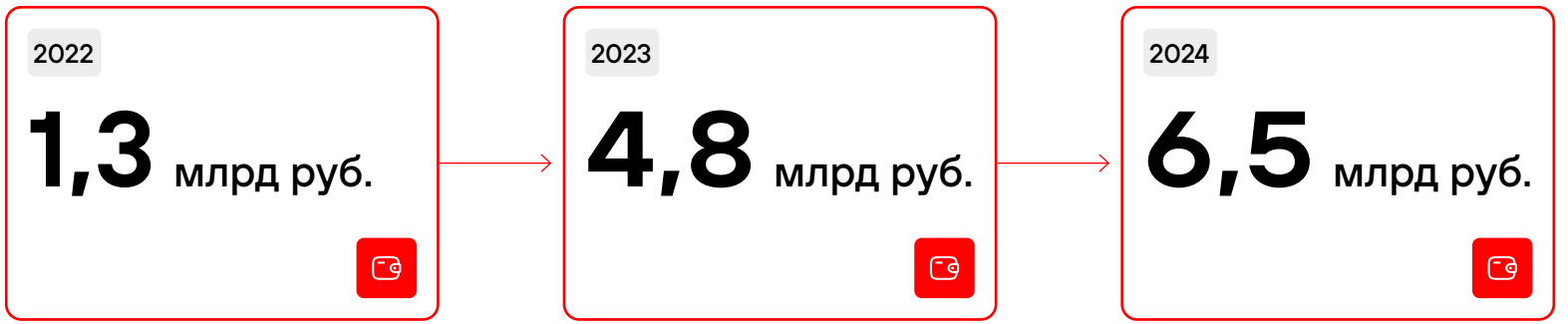
Мы придерживаемся принципа прозрачности во всех аспектах взаимодействия с акционерами, включая выплату дивидендов. Наша задача — обеспечить полное понимание инвесторами принципов формирования дивидендных выплат.

Positive Technologies входит в число высокотехнологичных компаний, делающих все возможное для обеспечения дивидендных выплат акционерам.

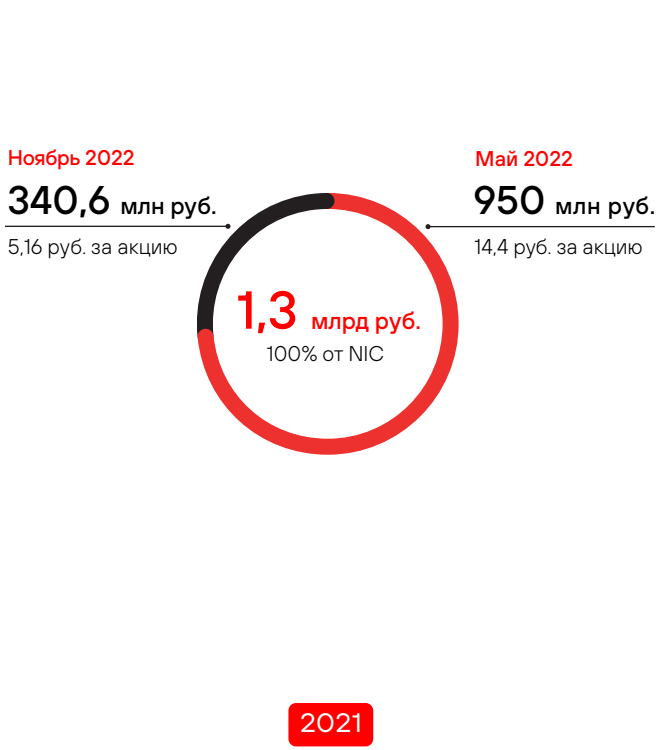
В 2022–2024 годах выплата дивидендов осуществлялась в несколько этапов. В 2024 году было произведено две выплаты, общая сумма которых составила 6,547 млрд руб., или 99,19 руб. на одну акцию. Этот результат превышает показатель 2023 года в 1,4 раза (4,8 млрд руб.) и в пять раз больше суммы дивидендов, выплаченных в 2022 году (1,3 млрд руб.).

Основой для расчета дивидендов служит показатель NIC — чистая прибыль без учета капитализируемых расходов. В соответствии с нашей дивидендной политикой на выплаты направляется от 50 до 100% NIC. В 2024 году общая сумма дивидендов составила 75% этого показателя за 2023 год.

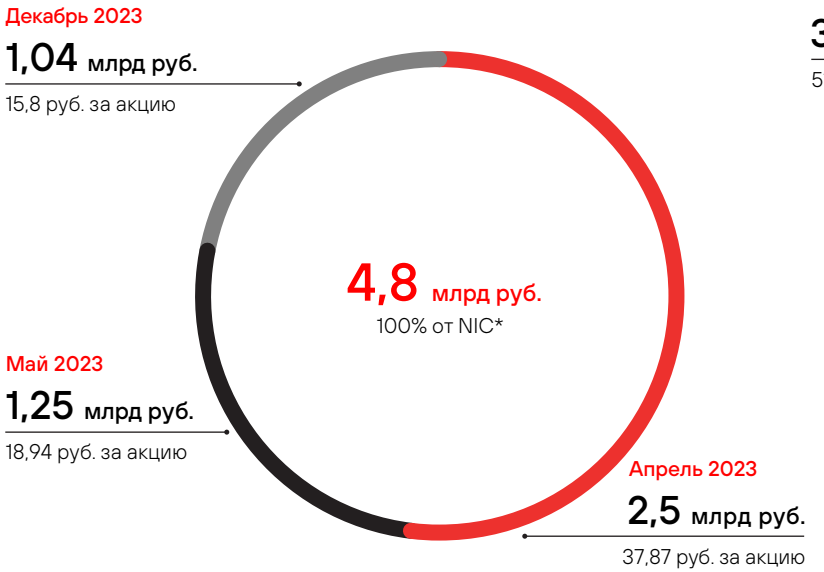
Дивидендная история Positive Technologies



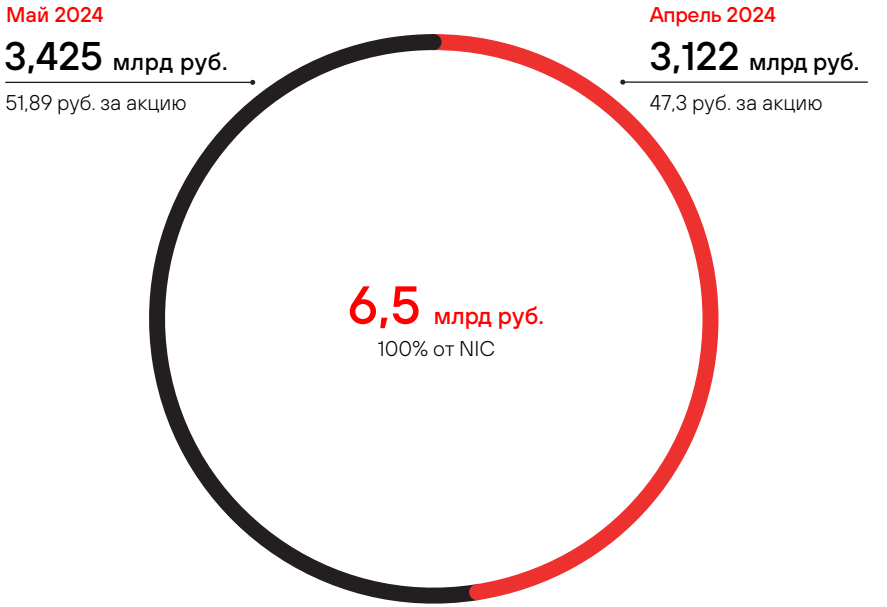
Дивиденды по итогам года



2021



2022



2023

* За минусом спецналога на сверхприбыль.

Дивидендная история Positive Technologies

Отчетный период	Общий размер объявленных дивидендов, тыс. руб.		Размер дивиденда в расчете на одну акцию, руб.	
	Обыкновенные акции	Привилегированные акции[1]	Обыкновенные акции	Привилегированные акции[1]
Дивидендная история после получения обществом публичного статуса				
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				

1 С 11 августа 2022 года количество обыкновенных акций Общества составляет 66 000 000 штук. 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.

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.

Акции в индексах Мосбиржи

На конец 2024 года акции Positive Technologies входят в 14 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.

В 2024 году Московская биржа включила акции Positive Technologies в субиндекс акций пенсионных накоплений. В него входят эмитенты, в акции которых могут вкладываться средства пенсионных фондов.

Во всем мире пенсионные фонды являются важнейшими участниками фондового рынка, долгосрочно инвестирующими в бумаги наиболее перспективных эмитентов для обеспечения высокого возврата на капитал в рамках программы пенсионных накоплений. Субиндекс является ориентиром для российских пенсионных фондов, инвестирующих в ценные бумаги.

Включение в него акций Positive Technologies показывает, что высокое доверие может привлечь новый тип инвесторов в капитал Компании, а пенсионным фондам это поможет обеспечить долгосрочный рост пенсионных накоплений граждан России.

В 2024 году эмитента ПАО «Группа Позитив» признали соответствующим требованиям Правил листинга ПАО «Московская Биржа» в части критериев инновационности. Решение было принято Экспертным советом рынка инноваций и инвестиций (РИИ), его пересмотр проводится каждые три года.

Таким образом, наши ценные бумаги продолжают входить в сектор РИИ, предоставляя возможность привлекать акционеров, ориентированных на инвестиции в ИТ-сектор. Такое признание подчеркивает наш статус инновационной компании и способствует укреплению позиций на рынке.

POSI на «СПБ Бирже»

Акции POSI с 6 ноября 2024 года включены в список ценных бумаг, допущенных к торгам на Санкт-Петербургской 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.

СПБ БИРЖА

Индексы, в которые входят ценные бумаги Positive Technologies на 31 декабря 2024 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
EPSI	Субиндекс акций активов пенсионных накоплений
IMOEXCNY	Индекс МосБиржи в юанях
MXSHAR	Индекс МосБиржи исламских инвестиций

Оценка акций Positive Technologies инвестбанками и независимыми аналитиками

Дата оценки	Команда аналитиков	Целевая цена акции	Рекомендация
03.12.2024	ФИНАМ	2904 руб.	Покупать
15.08.2024	Альфа Банк	4100 руб.	Покупать
26.07.2024	Invest Heroes	5176 руб.	Покупать
24.07.2024	Aigenis	4341 руб.	
23.07.2024	ИФК «Солид»	3700 руб.	
07.06.2024	ФИНАМ	2904 руб.	Держать
17.05.2024	РынкиДеньгиВласть	4080 руб.	
17.04.2024	ФИНАМ	3700 руб.	
16.04.2024	Тинькофф Инвестиции	2900 руб.	Держать
11.04.2024	Газпромбанк	3500 руб.	Покупать
10.04.2024	ИФК «Солид»	3700 руб.	
05.04.2024	РынкиДеньгиВласть	3620 руб.	
13.03.2024	Ренессанс Капитал	2800 руб.	Держать
11.03.2024	ИФК «Солид»	3290 руб.	
07.03.2024	Тинькофф Инвестиции	2300 руб.	Держать
06.03.2024	ПСБ	2630 руб.	Покупать
28.02.2024	БКС	2300 руб.	
20.02.2024	ПСБ	2630 руб.	Не исключен пересмотр

Расширяем аналитическое покрытие акций

Positive Technologies придает большое значение взаимодействию с независимыми экспертами — аналитиками и представителями инвестиционных банков. Для нас важно получать внешнюю экспертную оценку, которая помогает взглянуть на бизнес со стороны и подтверждает нашу прозрачность и открытость.

Наши акционеры

40 лет – средний возраст инвесторов

96 лет самому почтенному

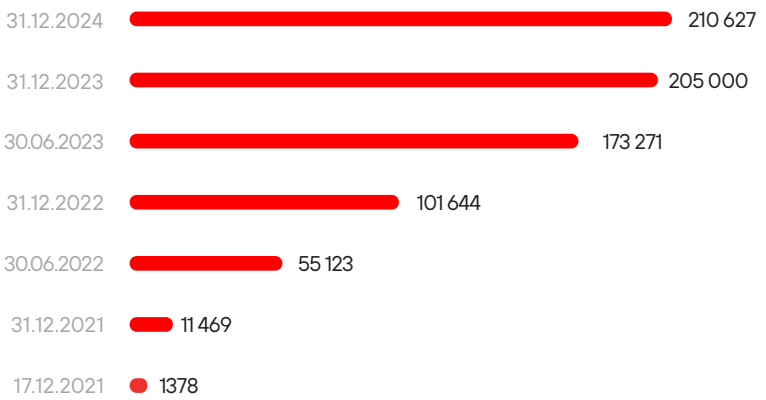
5 лет самому молодому

59,3%

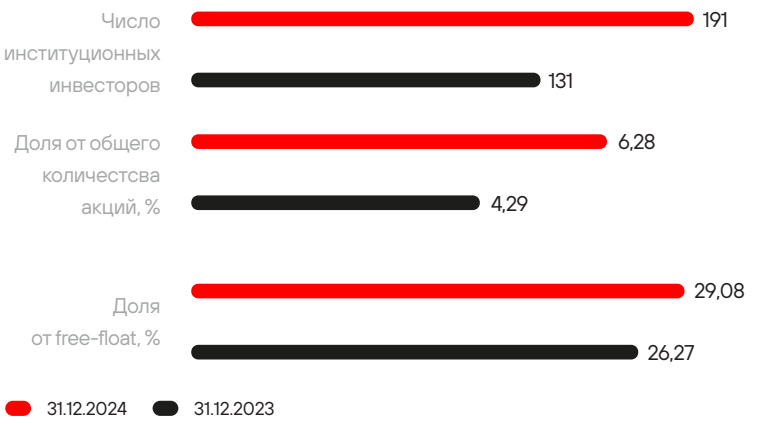
количество долгосрочных инвесторов, которые держат акции более года

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 три года количество владельцев акций выросло более чем в 18 раз.
С начала 2024 года число наших акционеров увеличилось на 2,7% и превысило 210 тыс. Большинство из них — частные инвесторы, причем 59,3% держат акции POSI больше года и являются долгосрочными инвесторами. Высокий интерес к акциям Positive Technologies проявляют и институциональные инвесторы — на конец 2024 года среди них был 191 фонд и юридическое лицо, прирост по сравнению с декабрем 2023 года составил 46%. На 31 декабря 2024 года доля институциональных инвесторов составила 6,87% от общего количества акций в обращении, или 29,08% от free-float.

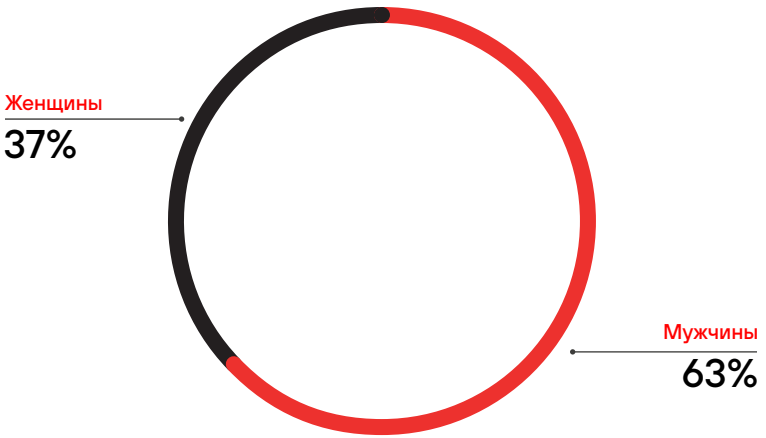
Динамика роста числа акционеров Positive Technologies, физических и юридических лиц



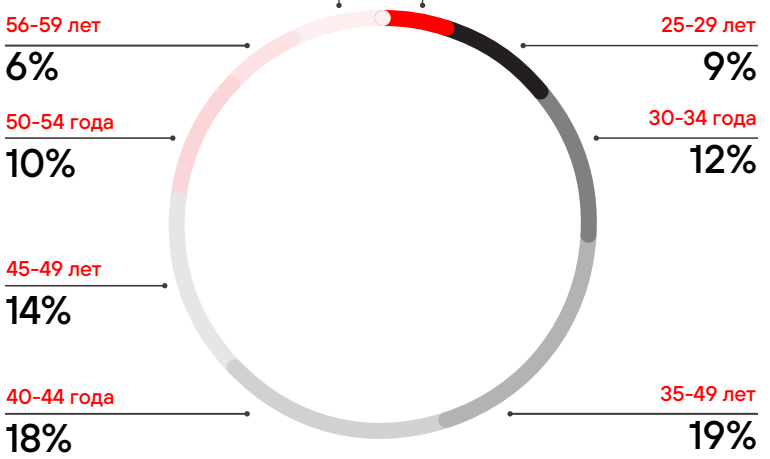
Динамика роста числа и доли институциональных инвесторов Positive Technologies, фондов и юридических лиц



Распределение инвесторов по полу

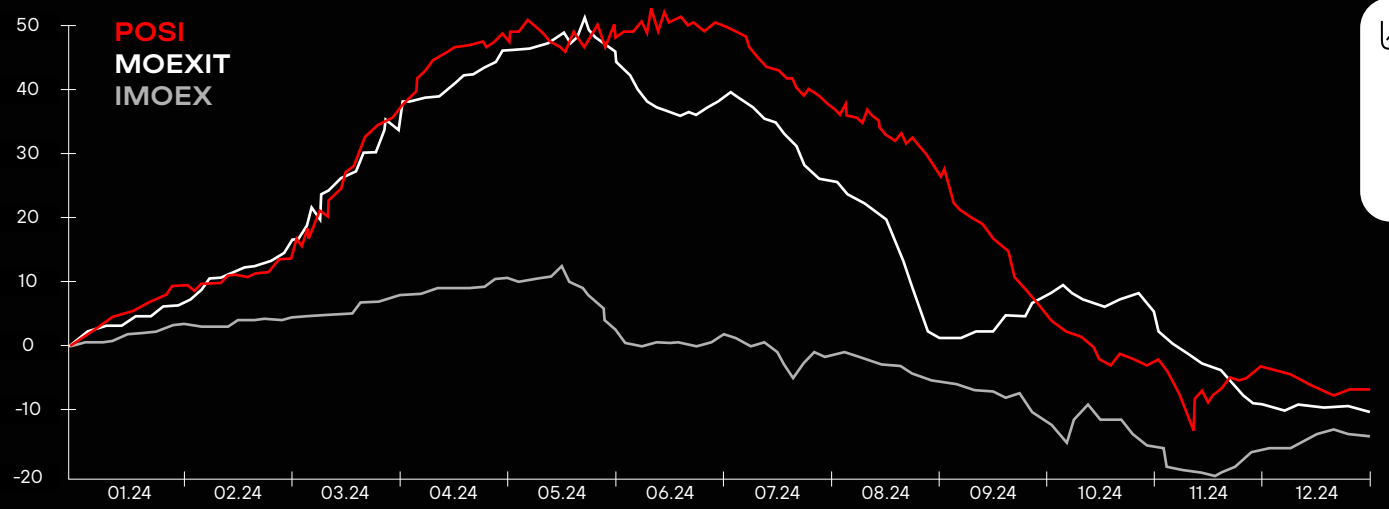


Распределение инвесторов по возрасту



География проживания наших совладельцев

Динамика изменения стоимости акций POSI в сравнении с индексами



Ликвидность акций Positive Technologies демонстрирует устойчивый рост. За три года среднедневной объем торгов составил 441 млн руб. В 2024 году этот показатель вырос до 747 млн руб. — в 7,7 раза больше, чем в первый год размещения, и на 67% выше уровня прошлого года. Рост ликвидности подтверждает повышенный интерес инвесторов к акциям Компании и укрепляет ее позиции на фондовом рынке.

2590,38 руб.

средневзвешенная стоимость акций за 2024 год

Капитализация и ликвидность

Капитализация Positive Technologies на конец 2024 года составила 143,1 млрд руб., увеличившись на 210% с момента размещения.

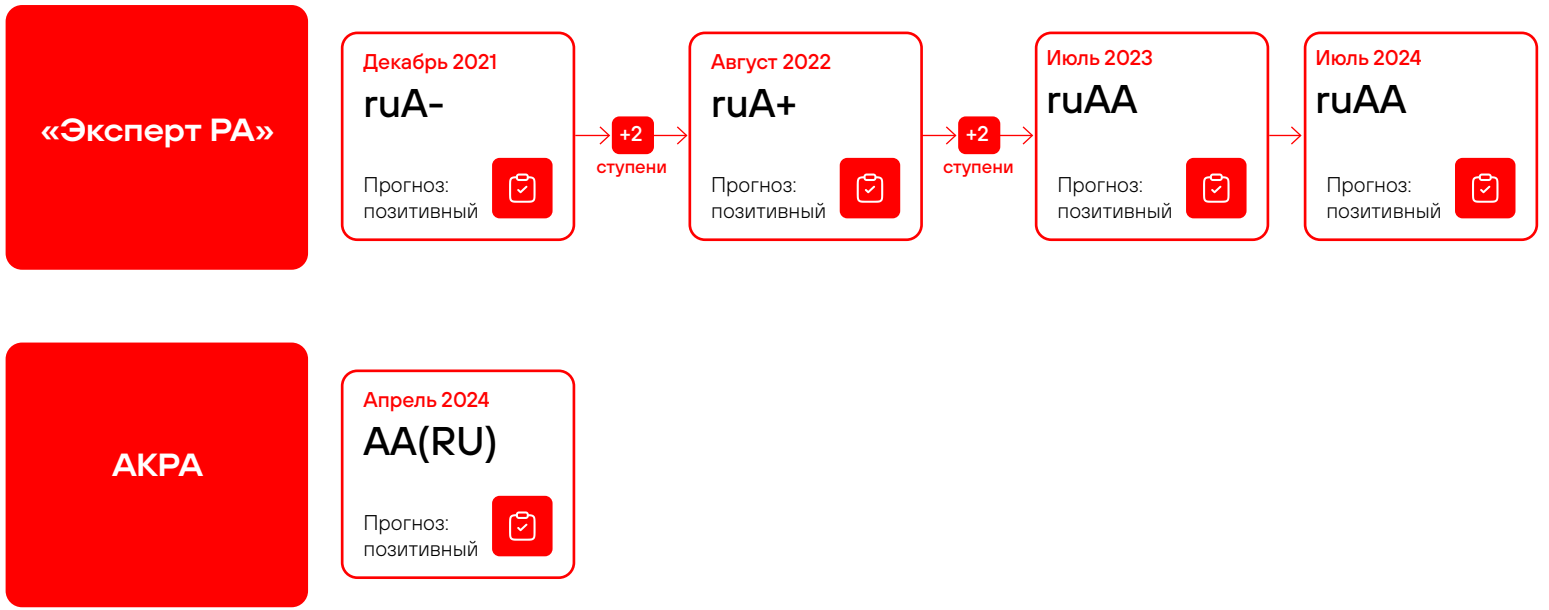
В отчетном году котировки акций Positive Technologies продемонстрировали разнонаправленную динамику. В первом полугодии наблюдался уверенный рост стоимости акций, который достиг своего пика 3 июля 2024 года. В этот день котировки обновили исторический максимум, достигнув в моменте отметки 3200 руб., а капитализация Компании превысила 211,2 млрд руб.

Однако во втором полугодии под влиянием макроэкономических факторов и ужесточения денежно-кредитной политики фондовый рынок оказался под давлением, что привело к снижению котировок ИТ-компаний. На 30 декабря 2024 года стоимость акций Positive Technologies составила 2009,6 руб., что практически соответствует показателю прошлого года (2013,4 руб.).

Несмотря на волатильность акций, Positive Technologies сохраняет долгосрочную цель по пропорциональному соответствию котировок и темпов роста бизнеса Компании.

Средневзвешенная стоимость акций за год составила 2590,38 руб., что на 23,4% выше средневзвешенной стоимости акций за 2023 год.

Кредитный рейтинг



В 2024 году Positive Technologies получила высокую оценку своей финансовой устойчивости и корпоративного управления от ведущих рейтинговых агентств. Аналитическое кредитное рейтинговое агентство (АКРА) присвоило Компании кредитный рейтинг «AA(RU)» со стабильным прогнозом, что свидетельствует о ее высокой кредитоспособности, финансовой устойчивости и развитой системе корпоративного управления. Данный рейтинг получен Компанией впервые.

Также в 2024 году рейтинговое агентство «Эксперт РА» подтвердило наш рейтинг кредитоспособности на уровне «ruAA» со стабильным прогнозом. Это является важным показателем надежности и репутации Positive Technologies как устойчивой и ответственной компании.

Особое внимание агентства уделили низкому уровню корпоративных рисков. Такой результат стал возможен благодаря нашей информационной прозрачности, высокому качеству управления, продуманной стратегии и эффективной системе риск-менеджмента.

Высокие кредитные рейтинги способствуют не только привлечению долгового финансирования на более комфортных условиях, но и росту привлекательности Компании для инвесторов.

Повышаем надежность долгового портфеля

В 2024 году Positive Technologies успешно провела два размещения облигаций, подтвердив высокий уровень доверия со стороны инвесторов и устойчивость своей финансовой стратегии.

19 июля 2024 года Positive Technologies успешно завершила размещение третьего выпуска облигаций на сумму 5 млрд руб. Ставка купона была установлена на уровне ключевой ставки Центрального банка России плюс 170 базисных пунктов, что оказалось ниже ранее заявленного ориентира. Такой уровень спреда доступен лишь наиболее качественным и надежным эмитентам, что подтверждает высокий уровень доверия к Компании.

Размещение вызвало значительный интерес среди институциональных и частных инвесторов с общим спросом, вдвое превышающим объем предложения. Это стало результатом высокого уровня надежности и финансовой устойчивости Компании, ее динамично развивающегося бизнеса с низкой долговой нагрузкой, высокой маржинальностью, а также развитого корпоративного управления и активного взаимодействия с инвесторами. Облигации имеют номинал 1 тыс. руб., срок обращения — три года, выплата купона каждые 30 дней.

Средства, полученные от размещения облигаций, направлены на реализацию задач по диверсификации и повышению устойчивости кредитного портфеля, а также на пополнение оборотных средств.

27 декабря 2024 года мы успешно провели размещение четвертого выпуска облигаций, направленного на улучшение структуры долгового портфеля Компании. Объем выпуска составил 4,8 млрд руб., номинал одной облигации — 1 тыс. руб., а срок обращения — два года.

По результатам формирования книги заявок Positive Technologies зафиксировала высокий спрос со стороны институциональных и частных инвесторов. Фактический объем размещения превысил изначально планируемый более чем в 1,5 раза.

Кроме того, Московская биржа включила облигации четвертого выпуска в сектор РИИ, который освобождает инвесторов от уплаты НДФЛ при владении ценными бумагами более года.

Рейтинговое агентство «Эксперт РА» присвоило облигациям третьего и четвертого выпусков высокий кредитный рейтинг — «ruAA».

Сведения об облигациях Positive Technologies	**RU000A101YV8**	**RU000A105JG1**	**RU000A109098**	**RU000A10AHJ4**
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
Срок обращений облигаций на бирже	Три года	Три года	Три года	Два года
Дата начала торгов	29 июля 2020 года	7 декабря 2022 года	19 июля 2024 года	27 декабря 2024 года
Дата погашения	26 июля 2023 года	3 декабря 2025 года	4 июля 2027 года	17 декабря 2026 года
Размер выпуска	500 тыс. облигаций	2,5 млн облигаций	5 млн облигаций	4,8 млн облигаций
Размер ставки купона	11,5% годовых	10,55% годовых	КС + 1,7% годовых	КС + 4% годовых
Первоначальная номинальная стоимость	1 тыс. руб.	1 тыс. руб.	1 тыс. руб.	1 тыс. руб.
Периодичность выплаты купона	Ежеквартально	Ежеквартально	Каждые 30 дней	Каждые 30 дней
Уровень листинга	3	3	2	2
Статус	Погашен	В обращении	В обращении	В обращении

5.3

Принципы работы с капиталом и программа стимулирования роста капитализации

Positive Technologies ставит перед собой амбициозные цели по кратному росту бизнеса. Достичь таких масштабов только за счет органического роста невозможно — нужны дополнительные ресурсы и вложения.

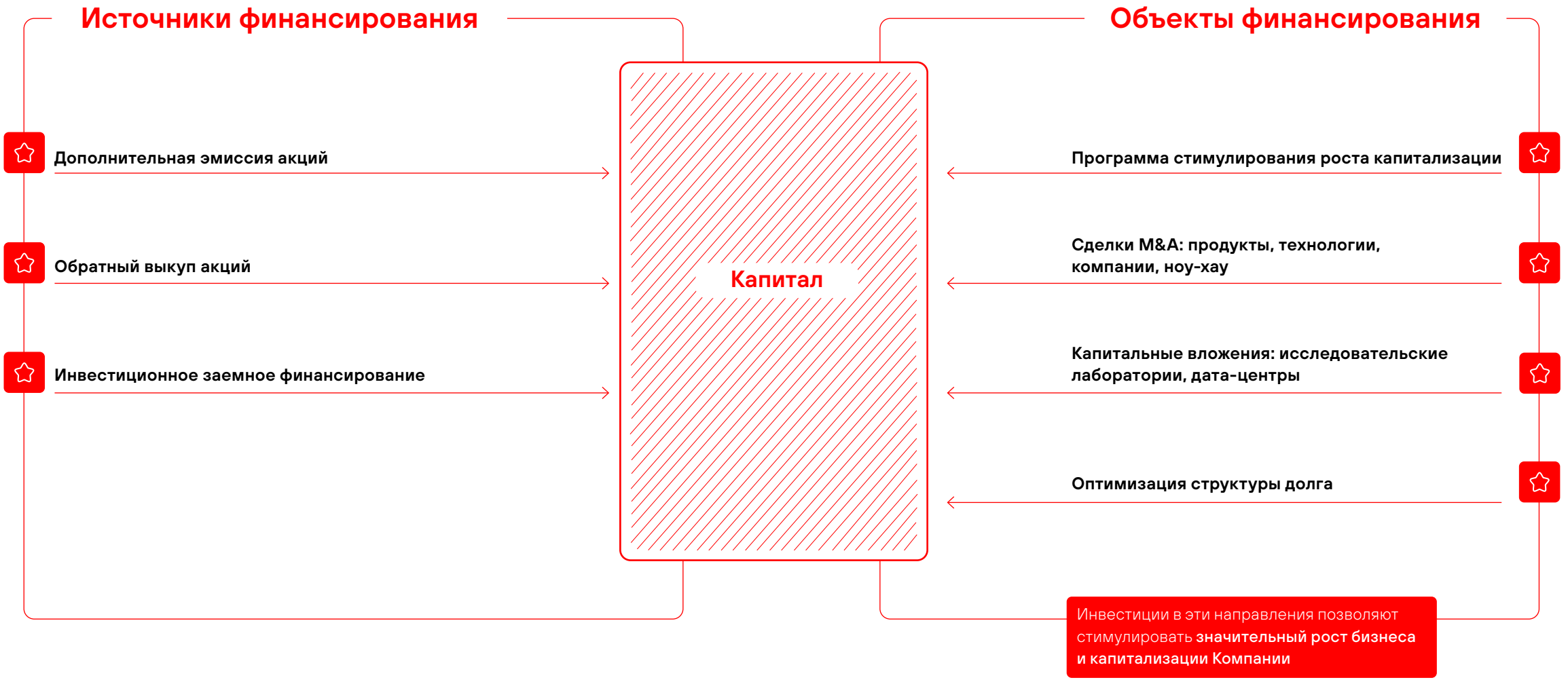
В 2024 году Positive Technologies разработала комплексный подход к управлению капиталом, включающий принципы работы с капиталом и программу стимулирования роста капитализации, которая была создана в соответствии с лучшими практиками корпоративного управления.

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 др. 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.


Источники финансирования
Дополнительная эмиссия акций
Обратный выкуп акций
Инвестиционное заемное финансирование
Капитал
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 позволяют стимулировать значительный рост бизнеса и капитализации Компании

Параметры допэмиссии

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.

По итогам 2023 года капитализация Компании увеличилась на 59%, что по формуле предполагало возможность выпуска акций на 8,4% от уставного капитала. Однако Компания приняла решение снизить объем допэмиссии.

Объем дополнительного выпуска в 2024 году составил 7,9% от уставного капитала и в основном был направлен на реализацию программы стимулирования роста капитализации Компании. Этот выпуск стал единственным в 2024 году и учитывал рост капитализации за 2023 год. Рост капитализации до 2023 года не учитывался и не будет учитываться в последующих допэмиссиях.

Участниками программы стимулирования роста капитализации стали 1880 контрибьюторов.

7,9%

составил дополнительный выпуск акций в 2024 году

Продолжаем реализацию идеи совладения

Ноябрь 2021

Рассказали об успешном опыте стимулирования роста капитализации Компании через передачу акций контрибьюторам — 1

Декабрь 2021

Подтвердили планы проводить допэмиссию. Прорабатываем программу стимулирования роста капитализации, планируем при каждом двукратном росте капитализации выпускать до 25% новых акций — 2

Октябрь 2023

Объявили планы по разработке структуры и запуску дополнительной эмиссии акций. Напомнили инвестиционному сообществу о целях и смыслах программы — кратно масштабировать бизнес, увеличивая капитализацию и обеспечивая сменяемость поколений.

Подтвердили планы проводить допэмиссию в размере до 25% на каждый двукратный рост капитализации — 3

7 марта 2024

Конкретизировали параметры дополнительной эмиссии: от 0 до 15% в зависимости от роста капитализации, бизнеса Компании и потребности в капитале. 15% — максимальный объем допэмиссии при удвоении капитализации в течение года — 4

9 апреля 2024

Подвели итоги года и подробно рассказали о планах допэмиссии — 5

24 мая 2024

Рассказали об основных принципах работы с капиталом и объяснили, как это позволит стимулировать значительный рост бизнеса — 6

4 октября 2024

Совет директоров утвердил программу стимулирования роста капитализации Компании — 7

7 ноября 2024

Общее собрание акционеров приняло решение о размещении дополнительного выпуска акций в размере 7,9% от уставного капитала Компании — 8

28 декабря 2024

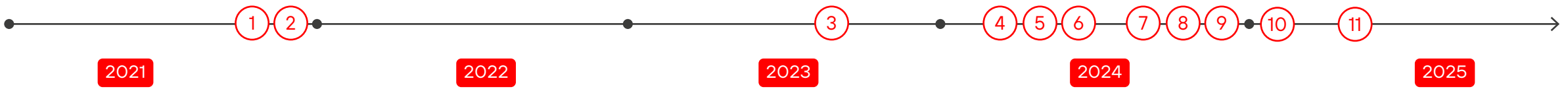
Банк России зарегистрировал итоги дополнительного выпуска акций: в результате допэмиссии количество акций увеличилось на 5,2 млн штук — 9

30 декабря 2024 — 31 января 2025

Positive Technologies распределила часть выпущенных акций между контрибьюторами, внесшими существенный вклад в развитие Компании — 10

Апрель 2025

Акции дополнительного выпуска объединены с основным и допущены до торгов на Московской бирже — 11



Акционерный капитал Positive Technologies

В 2024 году в составе акций, находящихся в свободном обращении (free-float) произошел ряд изменений, которые способствовали росту free-float до 23,64% по сравнению с декабрем 2023 года (19,7%). Среди таких событий — дополнительная эмиссия акций, увеличение доли институциональных акционеров, отдельные сделки с миноритарными пакетами акций. Также в отчетном году Компания проводила обратный выкуп акций.

Одним из ключевых событий стало завершение дополнительной эмиссии акций 28 декабря 2024 года. В результате количество акций увеличилось на 5,2 млн штук.

ПАО «Группа Позитив» не владеет собственными акциями. Количество акций, находящихся в распоряжении подконтрольных ПАО «Группа Позитив» юридических лиц на 31 декабря 2024 года, составляет 5 022 712 штук.

Общее количество выпущенных обыкновенных акций Компании составляет 71 214 000 штук. Привилегированные акции в уставном капитале отсутствуют.

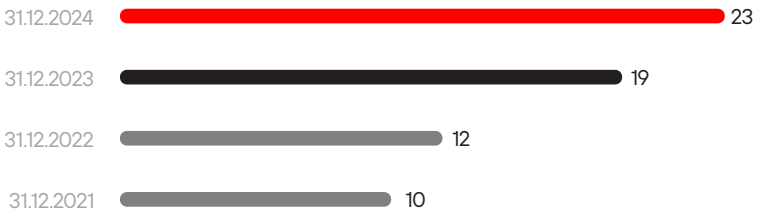
~71,2 млн

общее количество выпущенных обыкновенных акций Компании

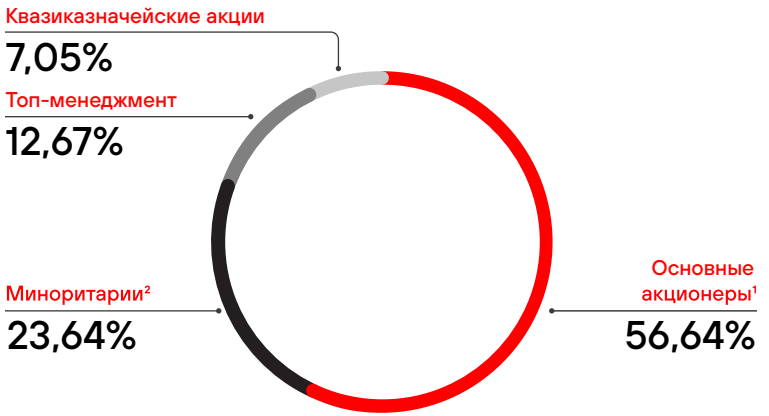
[1] Лица, владеющие 5% и более от уставного капитала.

[2] «Миноритарные акционеры» — более 210 тыс. акционеров — физических и юридических лиц.

Доля акций в свободном обращении (free-float), % от обыкновенных акций



Структура акционерного капитала и количество акций на 31 декабря 2024 года



5.4 Календарь инвестора

I квартал

Февраль

Событие
Публикация предварительных данных по отгрузкам за 2024 год

II квартал

Апрель

Событие
Публикация консолидированной аудированной финансовой отчетности за 2024 год

Апрель

Событие
Итоги года: мероприятие для инвесторов

Апрель

Событие
Positive Technologies на PROFIT CONF 2024

Апрель

Событие
Публикация аудированной отчетности за I квартал 2025 года

Май

Событие
Годовое Общее собрание акционеров

Май

Событие
День инвестора на киберфестивале Positive Hack Days

Июнь

Событие
Positive Technologies на Smart-Lab Conf (Санкт-Петербург)

III квартал

Июль

Событие
Публикация отчетности за II квартал и шесть месяцев 2025 года

IV квартал

Октябрь

Событие
Positive Technologies на Smart-Lab Conf (Москва)

Ноябрь

Событие
Публикация неаудированной отчетности за III квартал и девять месяцев 2025 года

Ноябрь

Событие
Positive Technologies на PROFIT CONF 2024

Устойчивое развитие

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

Positive Hack Days

Предоставляем открытую платформу для диалога и развития индустрии

Standoff

Прокачиваем скилы на киберполигоне

Positive Hack Talks

Создаем глобальное комьюнити, отвечая на вопросы профессионалов

Positive Hack Camp

Обучаем практической кибербезопасности на международной арене

6.1

Принципы устойчивого развития

С развитием цифровых технологий растет и число киберпреступлений, что делает кибербезопасность необходимым 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

Positive Technologies уже 23 года играет ключевую 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 киберзащиту мероприятий федерального значения, таких как «Игры Будущего» и Петербургский международный экономический форум.

Популяризация кибербезопасности

В мае 2024 года мы провели в «Лужниках» международный киберфестиваль Positive Hack Days 2, который 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, открываем новые направления профессионального обучения, запустили школу преподавателей кибербезопасности и международную программу по практической кибербезопасности 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

Нашим клиентам

- Выстраиваем систему результативной кибербезопасности
- Помогаем снизить киберриски
- Помогаем вести стабильный, устойчивый бизнес

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

Система управления устойчивым развитием

6.2

Люди Positive Technologies

Мы верим, что успех Компании создают люди. Наша команда — это не просто сотрудники, а сообщество увлеченных профессионалов и реальных контрибьюторов, которых объединяет стремление разрабатывать передовые технологии и двигать отрасль вперед.

В Positive Technologies работают люди, которые фанатично любят свое дело, смело берутся за сложные вызовы и создают инновационные продукты мирового уровня. Они не просто выполняют свою работу, а прикладывают усилия по принципу disrupt, что невозможно уложить в рамки обычных трудовых обязанностей, это уже скорее прямой и реальный вклад в развитие бизнеса, определяющий его будущее.

Мы делаем все, чтобы каждый контрибьютор мог реализовать свой потенциал, развиваться и чувствовать поддержку коллег. Для нас Компания — это не просто место работы, а общее дело, которым мы гордимся.

Продолжаем строить компанию совладения

Мы верим в идею совладения Компанией контрибьюторами и последовательно продолжаем вознаграждать их за вклад в развитие бизнеса Positive Technologies. Наша программа стимулирования роста капитализации основана на анализе уже достигнутых результатов. Мы ретроспективно оцениваем успехи Компании, выделяем значимые события, ключевые проекты и продукты, которые достигли новых высот. Особое внимание мы уделяем людям, которые сделали рост Компании возможным. Для нас важно понимать, как вклад прошлого формирует сегодняшний успех и закладывает основу для будущего развития.

Перед выходом на биржу в декабре 2021 года топ-менеджеры Компании распределили акции среди всех контрибьюторов, в том числе внешних экспертов, которые внесли значительный вклад в ее успех. Сейчас мы продолжаем эту традицию. Мы провели глубокий ретроспективный анализ и вознаградили акциями Компании 1880 контрибьюторов.

Подробнее о программе стимулирования роста капитализации читайте в разделе «Открытый диалог с инвесторами», с. 155

Создаем среду для интеллектуалов и экспертов

Наша цель — собрать в команде сильных профессионалов и создать для них условия, в которых интересно браться за сложные задачи и экспериментировать. Мы создаем среду, в которой сотрудники могут развиваться, делиться опытом, иметь доступ к обучению современным технологиям и находить поддержку руководителя и коллег.

В 2024 году мы уделили особое внимание развитию управленческих навыков. Для этого мы организовали воркшопы, направленные на формирование сильных команд и создание условий для их роста. Всего мы провели 64 воркшопа, 25 из которых прошли в регионах. В них приняли участие около 450 руководителей: они получили практические инструменты и узнали о новых подходах к управлению.

В течение года мы активно развивали программы обучения, предоставляя сотрудникам доступ к самым актуальным знаниям и навыкам. Так, успешно запустились и прошли курсы по AI и ML, безопасной разработке и ИБ. При этом значительная часть обучения была организована силами наших сотрудников и ведущих внешних экспертов, которым мы доверяем.

В 2024 году одним из ключевых направлений для нас стало **экспертное обучение продуктовых команд**. Безопасность — одна из ключевых метрик разработки. Исправлять уязвимости постфактум — долго и дорого, поэтому мы делаем ставку на профилактику: интеграцию методов и инструментов безопасной разработки на всех этапах создания продукта. Именно с этой целью мы запустили курс по безопасной разработке, который создал и ведет наш эксперт Владимир Кочетков. Обучение длится 21 неделю, и сейчас участники уже преодолели экватор. На каждое занятие стабильно приходит более 120 человек, а сообщество слушателей в чате выросло до 250 участников.

Чтобы создавать продукты, которые действительно будут результативными, разработчикам важно говорить на одном языке, понимать основы кибербезопасности, методы хакеров и принципы работы наших продуктов. Именно поэтому мы разработали учебный курс для погружения в ИБ. В пилотной группе приняли участие более 100 человек, и интерес к теме подтвердил его актуальность. В следующем году мы планируем, что обучение ИБ станет частью онбординга для всех, кто приходит в Positive Technologies создавать продукты.

В 2024 году мы запустили ряд внутренних экспериментальных проектов, которые помогли командам лучше понять бизнес, прочувствовать его процессы изнутри и получить реальный опыт использования продуктов.

Один из таких проектов — киберучения. В течение недели продуктовые команды погрузились в захватывающий процесс реализации **проекта результативной кибербезопасности**. Участники прошли полный цикл от общения с заказчиком и выявления критичных рисков до внедрения наших продуктов, отражения реальных атак хакеров и расследования инцидентов.

Такие инициативы помогают не только лучше понять бизнес, но и укрепляют взаимодействие внутри Компании, создавая по-настоящему сплоченную команду. Для нас важно, что в результате команды продуктов лучше поняли, как мыслит и действует хакер, и что важно учитывать не только в стратегии развития своего продукта, но и в кросс-продуктовом бэклоге. Мы верим, что наши сотрудники выбирают Positive Technologies, потому что здесь они могут работать рядом с сильными профессионалами, у которых есть чему научиться.

120+ участников
посещают курс по безопасной разработке

450 руководителей
приняли участие в воркшопах по формированию сильных команд

>100 сотрудников
прошли курс по основам кибербезопасности

В 2024 году мы запустили внутри Компании формат научно-популярных лекций — встреч, где сложные темы объясняются простым и понятным языком. Это не просто образовательные мероприятия, а возможность вдохновиться, узнать о новых трендах, пообщаться с экспертами Positive Technologies и приглашенными спикерами.

>1000

сотрудников посетили научно-популярные лекции в 2024 году

В течение года прошло девять встреч, на которых мы обсуждали машинное обучение в медицине, стратегии хакеров и защиту от атак, а также нейросети и большие языковые модели. Мы уверены, что обмен знаниями — это ключ к развитию, и будем продолжать делиться интересными кейсами и опытом.

«

Идея сделать обзорный рассказ о наших продуктах давно витала в воздухе. За почти шесть лет в Компании я не раз замечал, что даже коллеги, работающие здесь не первый год, не всегда четко понимают, как именно наши продукты защищают от хакерских атак. Но еще важнее было создать целостную картину — изложить ее так, чтобы каждый сотрудник, независимо от должности, мог легко разобраться в сути нашей работы. Ведь мы делаем одно большое дело, и важно, чтобы и технари, и нетехнари одинаково хорошо понимали, ради чего все это и как наши усилия превращаются в реальную защиту. Во время выступления я чувствовал, что аудитория действительно вовлечена. Это стало особенно заметно во время секции вопросов и ответов — коллеги задавали по-настоящему важные и продуманные вопросы. Приятным сюрпризом стали отклики от тех, кто смотрел лекцию онлайн. Коллеги из отдела продаж попросили запись — они не успели подключиться с самого начала, но хотели досмотреть. Пресейл-команда запросила презентацию, чтобы похожим образом объяснять заказчикам, как взаимодействуют разные классы продуктов. А еще поступили предложения по развитию этой лекции в более широкий формат, чтобы донести наши знания до еще большего числа людей.

Антон Кутепов,
руководитель направления развития инициатив ИБ-сообществ

Развиваем профессиональные сообщества внутри и вовне

Одна из наших ключевых целей — формирование активного комьюнити талантливых специалистов как внутри Компании, так и за ее пределами. Каждый новый шаг в обучении и развитии — это эксперимент, который приносит реальные результаты: новые идеи, нестандартные решения и развитие предпринимательского подхода внутри Компании.

Олимпиады по программированию

В 2024 году мы запустили олимпиады по программированию, и мы приглашаем участвовать не только сотрудников, но и их друзей, коллег из других компаний. Формат предполагает, что каждый участник может подумать над решением сложной задачи, узнать какие-то лучшие практики от коллег и пообщаться с близкими по духу людьми.

Олимпиады помогают прокачивать навыки решения нестандартных задач и находить новые подходы в программировании. Мы верим, что способность смотреть на свои повседневные задачи под другим углом открывает больше возможностей сделать прорывной продукт.

Важная часть Олимпиад — комьюнити. Подготовка к олимпиадам включает тренировочные сессии по алгоритмам, которые стали важной частью нашей системы внутреннего обучения.

3 олимпиады

прошло в 2024 году

458 человек

приняли участие в олимпиадах

«

По большому счету разработка так устроена, что в ней можно долгое время работать, быть успешным и при этом иметь кучу ограничений и не знать очень много интересного. При этом ты создаешь, пишешь код, делаешь продукты, но они недостаточно эффективны, недостаточно быстрые, недостаточно красивые и т. д. Что может получить человек, который сюда приходит? Он может понять, в каких областях ему не хватает знаний или по крайней мере какие вещи ему надо освоить. Но самое главное, что это все-таки не про знания, а про прокачку именно думалки. То есть олимпиады — это про придумать, это про додумать и т. д. А программисты — это люди, которые... Ну вот я говорю, в моем детстве программисты — это были те, кто математику знает лучше математиков, физику лучше физиков, еще и программирует. На самом деле вот этот скил — додумать, докрутить, досчитать, вот это все — он выделяет и всегда выделял, например, отечественных инженеров относительно международных. Просто потому, что вот этот скил-сет — он еще с советской школы шел. И очень хочется, чтобы люди поняли, о чем это.

Денис Кораблев,

управляющий директор, директор по продуктам Positive Technologies

Работаем с техническими сообществами

Мы активно взаимодействуем с профессиональными сообществами: наши эксперты выступают на ведущих технических мероприятиях. В 2024 году наши спикеры приняли участие более чем в 110 конференциях, где делились знаниями и опытом.

Наши эксперты являются членами программных комитетов конференций и отраслевых событий в ИТ и кибербезопасности.

Positive Hack Days

Площадка для знакомства и общения технических специалистов. В этом году мы расширили технический блок на Positive Hack Days, организовав четыре дня насыщенной программы с участием 64 спикеров из ИТ-индустрии. Количество технической аудитории в докладной части фестиваля выросло с 6 до 15%, достигнув **3,5 тыс. человек**.

в 110+ конференциях

приняли участие спикеры Positive Technologies

3,5 тыс. человек

техническая аудитория фестиваля Positive Hack Days в 2025 году

Молодежные и образовательные программы. PT Start

В 2024 году мы продолжили поддерживать молодых специалистов, помогая им сделать первые шаги в индустрии кибербезопасности и ИТ. Мы провели две волны набора, предоставляя возможность пройти отбор, углубить знания и получить реальный опыт работы. В результате 41 молодой специалист вступил в команду Positive Technologies. Помимо этого, для развития сообщества среди стажеров мы также проводили митапы, куда приглашали наших спикеров — экспертов из R&D и ИБ.

Результаты программы PT Start в 2024 году

Волна 2024.1

- **3** тыс. заявок
- **1,3** тыс. участников прошли первый этап
- **250** человек вышли на второй этап (интенсивы с командами)
- **70** стажеров получили оплачиваемую стажировку

Волна 2024.2

- **2735** заявок
- **1,5** тыс. участников прошли первый этап
- **144** человека вышли на второй этап (интенсивы с командами)
- **20** стажеров получили оплачиваемую стажировку

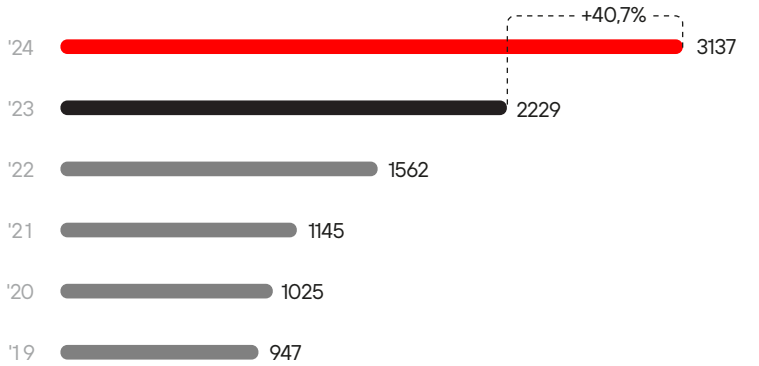
Программы для школьников

- В 2024 году мы запустили проект Back to School. В рамках инициативы наши сотрудники подготовили материалы, которые можно использовать для проведения уроков по основам кибербезопасности в школах.
- Проводим уроки по профессиям в сфере кибербезопасности в рамках проекта ШПК.
- Проводим практику для областного технолицея им. В. И. Долгих совместно с командой MP VM.
- Проводим экскурсии для школ с ИТ-уклоном, где рассказываем про специфику работы в ИТ и ИБ, приглашая молодых ребят к себе в офис.

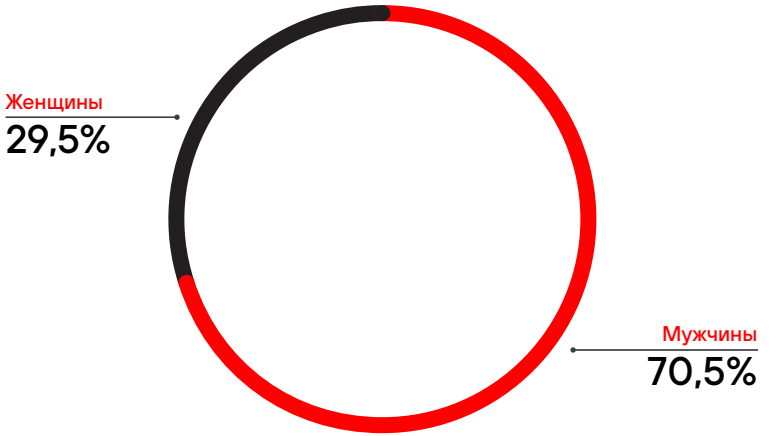
Численность команды

Наша цель — создание сильной и эффективной команды.
В течение года к нам присоединились 908 человек. По состоянию на 31 декабря 2024 года в Компании работали 3137 сотрудников.

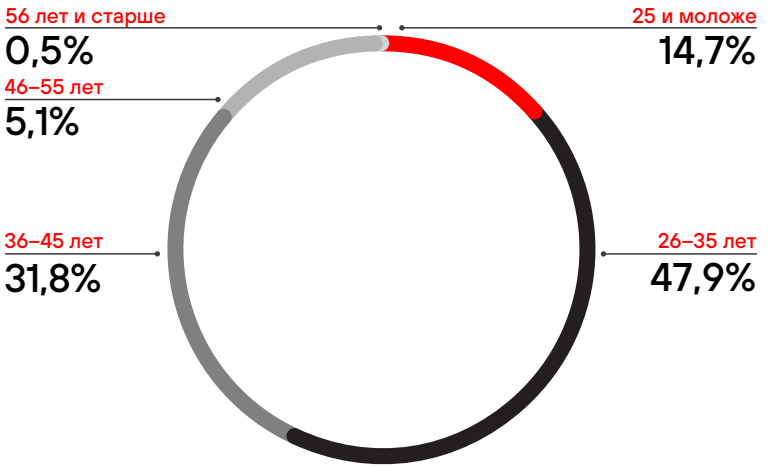
Численность персонала, динамика год к году,[1] человек



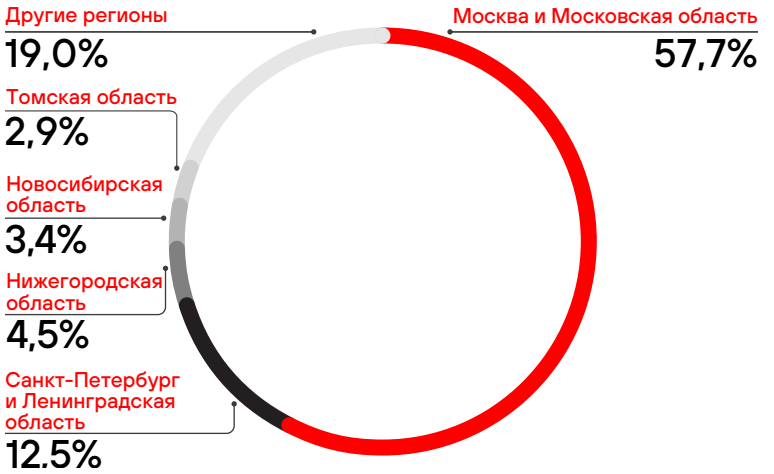
Гендерная структура персонала по состоянию на 31 декабря 2024 года



Возрастная структура персонала по состоянию на 31 декабря 2024 года



Регионы проживания персонала по состоянию на 31 декабря 2024 года



[1] За исключением сотрудников, находящихся в декретном отпуске и отпуске по уходу за ребенком, а также стажеров.

Делаем все, чтобы сотрудникам было удобно на рабочем месте

С ростом количества сотрудников вырос и наш офис. Мы открыли новые площади, сделали их комфортными и создали там уникальные условия для работы команд в соответствии с их предпочтениями.

6.3

Охрана труда и здоровья

Мы заботимся о благополучии и здоровье наших сотрудников. Каждый год мы проводим специальную оценку условий труда (СОУТ) согласно Положению о СУОТ[1] 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. Обучение ведется как заочно (дистанционно), так и очно на базе образовательных платформ Courson и 1ППА, его проходят 100% сотрудников[2].

Для профилактики и предупреждения профессиональных заболеваний мы оснащаем рабочие места персонала современными компьютерами и эргономичной мебелью. Кроме того, мы организовали в офисах места для активного отдыха и установили обязательные перерывы в работе. В 2024 году в Компании не было зарегистрировано несчастных случаев и профессиональных заболеваний.

[1] Утверждено приказом от 9 января 2019 года № 02-ОД.2019.
[2] Кроме сотрудников, работающих удаленно.

Positive Education

Positive Education — центр обучения Positive Technologies, где практики обучают результативной кибербезопасности. В 2024 году мы начали развивать экспертизу не только в России, но и в других странах мира.

6.4

Образование и киберпросвещение

Развиваем результативную кибербезопасность через обучение

Сегодня Positive Education

01

Реализует образовательные программы по построению эффективной информационной безопасности в организациях для профильных команд и топ-менеджмента.

02

Обучает партнеров и клиентов по всему миру эффективному использованию продуктов Positive Technologies для масштабирования бизнеса и повышения его устойчивости.

03

Помогает молодым специалистам определиться с профессиональным треком и освоить современные подходы к кибербезопасности, привлекая к обучению ведущих преподавателей как в России, так и за рубежом.

Positive Education — уникальные подходы

01

Внедрение обучения в рабочие процессы
Используем гибкие форматы (очно, онлайн, с отрывом и без отрыва от работы), внедряем профессиональное развитие в повседневную практику.

02

Фокус на практике и реальные задачи
Все программы создаются с участием специалистов, ежедневно работающих с инцидентами ИБ, кибератаками и защитой инфраструктуры.

03

Сильная методология и структура
Курсы и программы построены на проверенных подходах, учитывают уровень подготовки специалистов и цели компании.

04

Развитие культуры кибербезопасности
Формируем понимание важности обеспечения кибербезопасности у руководителей и специалистов всех подразделений.

Что дальше?

Мы продолжаем расширять и улучшать наши образовательные программы, стремясь сделать обучение кибербезопасности доступным и эффективным для всех желающих. В планах — запустить новые курсы, развить партнерские отношения с образовательными учреждениями и компаниями, а также внедрить современные технологии в процесс обучения.

Программы обучения

Для нас кибербезопасность — это не только развитие собственных компетенций и продуктов. Это еще и масштабирование нашего опыта для прогресса навыков в индустрии — так мы создаем синергию, которая позволяет кибербезопасности расти глобально.

Positive Technologies — лидер результативной безопасности. Мы обладаем передовой экспертизой в этой области и стремимся делиться ею с теми, кто заинтересован в кибербезопасности. Для этого мы создаем образовательные программы в партнерстве с ключевыми экспертами индустрии и ведущими вузами страны.

Корпоративное обучение

Мы помогаем компаниям выстраивать результативную кибербезопасность через обучение собственных команд. Наши корпоративные программы — это практика, направленная на развитие ключевых компетенций: от формирования базового понимания основ кибербезопасности до построения устойчивых процессов выявления угроз, реагирования на инциденты и управления уязвимостями — всего, что лежит в основе результативной ИБ.

Обучение проводится в удобном формате и с учетом специфики бизнеса, уровня подготовки сотрудников и целей компании. Мы обучаем специалистов, которые уже сегодня отвечают за цифровую безопасность, и формируем команды, готовые к угрозам завтрашнего дня.

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»;
- «Анализ сетевой безопасности»;
- «Анализ сетевого трафика»;
- «Построение SOC 2.0»;
- «Харденинг ИТ: от дизайна до настроек».

Обучение топ-менеджмента

Мы адаптируем программы Positive Education под задачи организаций, составляя учебные треки под конкретную роль или подбирая комплексное решение.

Также мы развиваем сотрудничество с ведущими бизнес-школами по формированию корпоративных программ для управленческих ролей компаний. Наша цель — сформировать понимание у топ-менеджеров, как кибербезопасность влияет на бизнес-результаты и устойчивость организаций. В рамках обучения управленческого состава мы запустили открытую программу для генеральных директоров «Информационная безопасность бизнеса» в партнерстве со «СберУниверситетом», которую прошли уже более 60 менеджеров организаций.

Развитие компетенций

Мы стремимся кратно увеличить число качественных специалистов и создаем программы повышения квалификации в сотрудничестве с партнерами и ведущими российскими вузами.

Запустившиеся программы в 2024 году:

- программа повышения квалификации для специалистов SOC совместно с Центральным университетом и «Т-Банком», которую прошли уже 60 человек из 50 компаний и получили удостоверение о повышении квалификации.
- первая на российском рынке программа по повышению квалификации для специалистов по безопасной разработке и администраторов средств защиты информации совместно с Физтех-школой прикладной математики и информатики Московского физико-технического института (ФПМИ МФТИ), по которой обучились уже более 50 человек.
- программа по кибербезопасности, разработанная совместно с Национальным исследовательским ядерным университетом МИФИ, где Positive Technologies выступила индустриальным партнером.

Развитие экспертизы в магистратуре

Еще одно важное направление развития профессионалов — запуск магистерских программ в рамках флагманских партнерств с ключевыми вузами в области обучения кибербезопасности. Так, в 2024 году мы открыли магистерские программы:

- на базе Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (ИТМО), цель которой — подготовка архитекторов в области ИБ, обладающих навыками аналитиков SOC и ML, для стран БРИКС;
- по направлению «Кибербезопасность» совместно с Университетом Иннополис, которая вобрала в себя лучшие практики кибербезопасности;
- по разработке безопасной КИИ, где партнерами выступили «Сириус» и наши партнеры из индустрии. В рамках программы студенты смогут пройти стажировку в Positive Technologies и других крупных компаниях.

6757

российских партнеров мы обучили и сертифицировали по нашим продуктам

179

зарубежных партнеров мы обучили, 29 из них прошли сертификацию

Партнерам и клиентам

Один из способов развития и масштабирования нашего бизнеса в России и за рубежом — это обучение партнеров и клиентов результативному использованию наших продуктов. Мы организуем программы по всей продуктовой линейке Компании, доступ к ним могут получить все партнеры и клиенты. Материалы программ регулярно обновляются, чтобы обучение позволило овладеть полным спектром возможностей продукта.

Среди тех, кто проходит обучение по продуктам Positive Technologies, — почти 11 тыс. сотрудников партнеров и дистрибьюторов и 5,8 тыс. заказчиков, при этом ежегодно количество проходящих обучение удваивается.

Сегодня в Компании действуют более 35 программ продуктового обучения, четыре из них — для международных партнеров. В 2024 году наши пользователи зарегистрировались на обучение 115 тыс. раз и оценили его на 4,8 из 5 баллов.

Студентам и преподавателям

Мы обучаем молодых профессионалов и преподавателей передовым практикам кибербезопасности как в России, так и за рубежом, чтобы качественно повысить образование в области ИБ.

Для студентов мы создаем специализированные курсы и школы, проводим открытые лекции и митапы в университетах и на отраслевых мероприятиях, запускаем совместные образовательные программы с компаниями-партнерами. Дополнительно предоставляем онлайн-тренажер PT EdTechLab для практики отражения кибератак.

Совместно с преподавателями вузов и ведущими специалистами индустрии мы организуем и проводим программы подготовки по востребованным направлениям. Также создаем специальные образовательные проекты для талантливых преподавателей, чтобы они могли обучать актуальным знаниям и технологиям.

Сотрудничество с вузами

Развивая образование в области кибербезопасности, мы укрепляем сотрудничество с 70 вузами не только в России, но и за ее пределами. Так, в 2024 году Компания подписала соглашение о сотрудничестве с SGU (Джакарта, Индонезия) и Amity University (Дубай, ОАЭ). Совместно с ними Positive Technologies будет готовить специалистов по результативному построению кибербезопасности.

Школа преподавателей кибербезопасности

Уже второй год Школа преподавателей кибербезопасности помогает погрузить действующих преподавателей в актуальную повестку кибербезопасности. В первом потоке мы обучили чуть менее 1 тыс. преподавателей российских вузов и ссузов, а в 2024 году запустили новый при поддержке Минцифры России и в партнерстве с Московским государственным техническим университетом (МГТУ) им. Н. Э. Баумана. На программу записалось более 1,7 тыс. участников со всей страны и близлежащего зарубежья, среди которых преподаватели вузов, ссузов и школьные учителя информатики. После прохождения программы участники также получают удостоверение о повышении квалификации.

В рамках программы участники проходят обучение по направлениям:

- актуальные методы атак и защиты, применимые в реальной практике;
- безопасная разработка с учетом уязвимостей и рисков;
- ИТ-база для понимания архитектуры и процессов информационной безопасности;
- прикладной подход к построению результативной кибербезопасности в организациях;
- этичный хакинг и методы тестирования на проникновение;
- безопасность в сферах искусственного интеллекта и web3;
- расследование инцидентов и реагирование на кибератаки;
- карьерные треки и профессиональное развитие в ИБ.

Для закрепления навыков участники используют тренажер PT EdTechLab с реалистичными сценариями атак и задач, приближенными к повседневной практике специалистов.

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.

В 2024 году мы запустили ряд проектов, чтобы внести свой вклад в развитие глобального комьюнити.

Positive Hack Camp

В августе 2024 года мы провели первую смену международного буткемпа по основам наступательной кибербезопасности (белый хакер) — это первая инициатива такого рода в России.

Мы пригласили в кемп более 70 участников из 20 стран. В течение 12 дней молодые специалисты не только учились и практиковались с ведущими экспертами в области белого хакинга, но и узнавали культуру нашей страны, что позволило укрепить и донести до международного сообщества наш культурный код.

Культурная экспансия

«

Мы накопили огромный опыт и готовы делиться им с иностранными специалистами. Наша миссия — сформировать глобальное равноправное сообщество экспертов в сфере кибербезопасности, чтобы обмениваться знаниями, вместе противостоять растущим киберугрозам и повышать уровень защищенности во всем мире.

Дмитрий Серебрянников,
директор по анализу защищенности Positive Technologies

Positive Hack Talks: расширяем границы кибербезопасности

В 2024 году мы запустили Positive Hack Talks — международную серию встреч для всех, кто увлечен кибербезопасностью. От студентов и начинающих специалистов до опытных экспертов, готовых делиться знаниями, — наши митапы объединяют профессионалов со всего мира.

В октябре 2024 года состоялся первый митап Positive Hack Talks. Он прошел в Индии, в Бенгалуру. Выбор места для старта проекта не случаен: Индия — один из мировых лидеров с точки зрения экономического роста и цифровизации, а Бенгалуру — один из ведущих технологических центров мира, своего рода Кремниевая долина Южной Азии.

Презентации спикеров доступны на сайте митапа

Среди докладчиков — эксперты Positive Technologies, специалисты из России и местные профессионалы. Участники обсуждали безопасность блокчейна, багбаунти и защиту от современных киберугроз.

Митап стал отличной площадкой для обмена опытом между экспертами из разных стран.

В ноябре мы продолжили международный тур: второй Positive Hack Talks прошел в Ханое (Вьетнам) и собрал более 200 участников.

На митапе выступили восемь ведущих экспертов, а участники смогли не только послушать доклады, но и лично пообщаться с профессионалами отрасли.

В 2025 году Positive Hack Talks продолжит расширять границы. Мы планируем новые митапы в разных странах, чтобы создать глобальное сообщество специалистов, обмениваться знаниями и вместе противостоять растущему числу киберугроз.

6.5

Благотворительность

В 2024 году на киберфестивале Positive Hack Days действовала благотворительная программа, в рамках которой доступ на закрытую часть мероприятия получали те, кто сделал пожертвование в фонд «Подари жизнь» на сумму от 1 тыс. руб. Во время проведения фестиваля было собрано около 9 млн руб., а участие в программе приняли 7 тыс. человек.

~9 млн руб.

помог собрать Positive Hack Days на благотворительность

В 2025 году Positive Hack Days расширяет инициативу: теперь для получения билета на закрытую часть фестиваля можно будет сделать пожертвование не только в фонд «Подари жизнь», но и в фонды «Старость в радость» и «Улица мира». Минимальная сумма пожертвования для получения билета составит 1,5 тыс. руб.

Таким образом, Positive Hack Days продолжает объединять кибер-сообщество не только ради технологий, но и для добрых дел.

6.6

Вклад в экологию

Московский офис Positive Technologies находится в бизнес-центре «ПРЕО 8» класса А, где применяются современные технологии для снижения нагрузки на окружающую среду.

Экологические инициативы в бизнес-центре «ПРЕО 8»

- Озеленение крыши — на техническом этаже высажен газон, улучшающий качество воздуха и повышающий энергоэффективность здания.
- Озеленение территории — рядом с офисом посажены клены, которые делают пространство более уютным и способствуют улучшению экологии.
- Раздельный сбор отходов — организован сбор картона для переработки.
- Безопасная утилизация — ртутные лампы утилизируются с соблюдением экологических стандартов.
- Энергосбережение: используется светодиодное освещение и энергосберегающее лифтовое оборудование Kone.

В 2024 году Positive Technologies продолжил развивать экологические инициативы, направленные на сокращение отходов и повышение энергоэффективности.

- В московском офисе Компании установлены урны для раздельного сбора мусора. Отходы разделяются на вторсырье (пластик, стекло, упаковка и другие перерабатываемые материалы) и смешанные, которые выбрасываются стандартным способом в контейнер на территории бизнес-центра. Вторсырье передается партнерской компании «Собиратор» для переработки.
- Организован сбор использованных батареек, что позволяет безопасно утилизировать опасные элементы.
- Для снижения расхода бумаги внедрены системы электронного документооборота, в том числе кадрового.

Чтобы повысить энергоэффективность, в 2024 году в московском офисе Positive Technologies были открыты новые пространства, которые спроектированы и реализованы с применением светодиодного освещения. Его можно индивидуально регулировать для групп рабочих мест.

Все эти шаги помогают нам уменьшать нагрузку на окружающую среду и делать работу Компании более экологичной.

Корпоративное управление

7.1

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

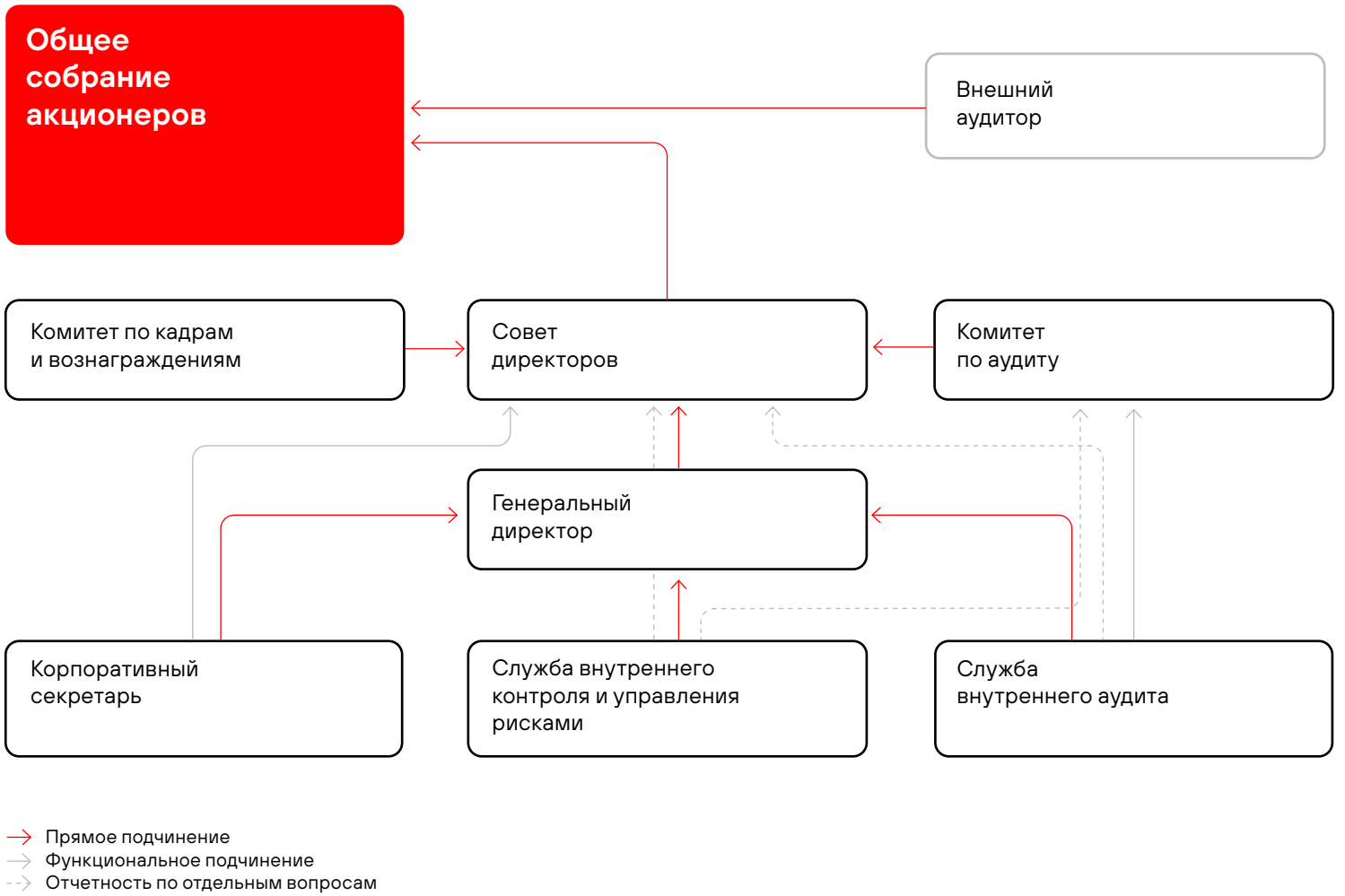
В области корпоративного управления Компания ставит своей целью соблюдение норм действующего российского законодательства, а также руководствуется правилами листинга Московской биржи и Кодексом корпоративного управления, рекомендованным Банком России. В отношениях с инвесторами мы ставим открытость на 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.

Схема элементов системы корпоративного управления ПАО «Группа Позитив»

Positive Technologies — группа компаний, которая включает в себя материнскую компанию и ряд дочерних



Заявление Совета директоров о соблюдении 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 № ИН06-28/102 «О раскрытии в годовом отчете публичного акционерного общества отчета о соблюдении принципов и рекомендаций Кодекса корпоративного управления».

Отчет о соблюдении принципов и рекомендаций Кодекса корпоративного управления

Меры по совершенствованию корпоративного управления в 2024 году и планы на 2025 год

Компания продолжает совершенствовать механизмы корпоративного управления для достижения максимальной прозрачности деятельности. В 2024 году:

- проведена работа по актуализации Устава Компании в связи с внесением в него положений об объявленных акциях, изменениями действующего корпоративного законодательства и с целью оптимизации отдельных корпоративных процедур в Компании;
- разработаны и утверждены основные принципы работы с капиталом;
- разработана и утверждена программа стимулирования роста капитализации;
- актуализирован перечень инсайдерской информации Компании;
- по итогам 2024 года была проведена первая самооценка работы Совета директоров.

В 2024 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 2025 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.

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»

7.2

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 Общее собрание акционеров. Также она может проводить внеочередные Общие собрания акционеров.

В 2024 году годовое Общее собрание акционеров было проведено 14 мая[1]. На нем были рассмотрены вопросы:

- о распределении прибыли (в том числе о выплате (объявлении) дивидендов) по результатам 2023 года;
- о выплате (объявлении) дополнительных дивидендов по результатам I квартала 2024 года;
- об избрании членов Совета директоров;
- об утверждении аудиторской организации;
- об определении количества, номинальной стоимости, категории (типа) объявленных акций и прав, предоставляемых этими акциями;
- об утверждении Устава Компании в новой редакции.

Также в течение отчетного периода Компания провела три внеочередных Общих собрания акционеров: 9 апреля[2], 10 июля[3], 7 ноября[4].

На указанных собраниях акционерами рассматривались вопросы о выплате (объявлении) дивидендов по результатам I квартала отчетного, 2024 года, о распределении (оставлении нераспределенной) остатка чистой прибыли Общества по итогам 2022 года, а также были рассмотрены вопросы об увеличении уставного капитала Компании путем размещения дополнительных акций Компании посредством закрытой подписки. Акционеры могли принимать участие в голосовании с использованием электронного бюллетеня, а также путем направления заполненного на бумаге бюллетеня и подачи инструкции через депозитарий. Материалы собраний Компания заблаговременно размещает на сайте для инвесторов.

Информация для инвесторов на сайте Компании

1 Протокол годового Общего собрания акционеров от 15 мая 2024 года б/н.
2 Протокол внеочередного Общего собрания акционеров от 10 апреля 2024 года № 1.
3 Протокол внеочередного Общего собрания акционеров от 11 июля 2024 года № 2.
4 Протокол внеочередного Общего собрания акционеров от 7 ноября 2024 года № 3.

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 2024 года

Текущий состав Совета директоров в составе девяти членов был избран решением годового Общего собрания акционеров 14 мая 2024 года и действует до следующего годового 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 15 мая 2024 года б/н.
[2] Протокол Комитета по кадрам и вознаграждениям от 5 апреля 2024 года № 1.
[3] Протокол Совета директоров от 7 июня 2024 года № 31.

Отчет о работе Совета директоров в 2024 году

В 2024 году были проведены одно очное и девять 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;
- назначен новый Корпоративный секретарь Компании;
- утверждены Годовой отчет и годовая бухгалтерская отчетность Компании за 2023 год;
- выданы рекомендации Общему собранию акционеров о выплате дивидендов по итогам 2023 года и I квартала отчетного года;
- утвержден годовой бюджет Компании на 2024 год;
- утверждены основные принципы работы с капиталом Общества;
- утверждена программа стимулирования роста капитализации Компании, определены основные направления действий Компании для ее реализации;
- утвержден документ, содержащий условия размещения дополнительных акций Компании на основании решения Общего собрания акционеров Общества об увеличении уставного капитала, и приняты иные необходимые в связи с проведением дополнительной эмиссии акций решения.

Участие директоров в заседаниях Совета директоров

Дата проведения Совета директоров	Форма принятия решения	Количество директоров, принявших участие / общее количество директоров
04.03.2024	Заочное голосование	9/9
14.03.2024	Заочное голосование	9/9
08.04.2024	Заседание	9/9
06.06.2024	Заочное голосование	9/9
02.07.2024	Заочное голосование	9/9
11.07.2024	Заочное голосование	9/9
23.09.2024	Заочное голосование	9/9
04.10.2024	Заочное голосование	9/9
07.11.2024	Заочное голосование	9/9
25.12.2024	Заочное голосование	9/9

Комитеты при Совете директоров

При Совете директоров созданы два постоянно действующих комитета:
- 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;
- предварительное рассмотрение годового бюджета;
- рассмотрение кандидатуры аудитора;
- рассмотрение оценки текущего статуса развития системы внутреннего контроля и управления рисками, а также плана развития системы управления рисками Компании;
- утверждение плана деятельности Службы внутреннего аудита Компании и ее бюджета.

Комитет состоит из трех членов, два из которых являются независимыми директорами.

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 по назначению Корпоративного секретаря;
- выработка рекомендаций акционерам Компании по голосованию за кандидатов в Совет директоров;
- подтверждение независимости членов Совета директоров;
- рассмотрение программы стимулирования роста капитализации.

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 2024 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 Общества.

Баранов
Денис Сергеевич

Генеральный директор

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.

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.

Сазыкина
Юлия Сергеевна

Корпоративный секретарь

Родилась в 1982 году.

Окончила юридический факультет Московского государственного университета им. М. В. Ломоносова.

Имеет более чем 19-летний опыт работы в сфере корпоративного управления и корпоративных проектов. До прихода в Positive Technologies возглавляла корпоративное управление в группе компаний OZON с листингом на Nasdaq и Московской бирже, а также в ПАО «Уралкалий» с листингом на Лондонской бирже (и последующим делистингом) и Московской бирже.

Была главой юридической службы международного семейного офиса. Более восьми лет работала в международном юридическом консалтинге в сфере корпоративных проектов и сделок на рынках капитала, таких как публичные предложения ценных бумаг, публичные слияния и поглощения.

На 23 сентября 2024 года акциями Компании не владела.

С 24 сентября 2024 года Корпоративным секретарем Компании является Терентьева Ольга Игоревна.

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.

Терентьева
Ольга Игоревна

Корпоративный секретарь

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 ГК «Ростех», ГК ОАО «РЖД», ГК ПАО «Ростелеком», также работала в Коллегии адвокатов города Москвы.

Ольга является сертифицированным корпоративным секретарем Национального объединения корпоративных секретарей.

На 31 декабря 2024 года владела 274 акциями Компании, что составляет 0,000385% от уставного капитала Компании.

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.

До 23 сентября 2024 года включительно Корпоративным секретарем Компании являлась Сазыкина Юлия Сергеевна.

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 2024 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.

7.3

Управление рисками, внутренний контроль и аудит

Корпоративная система управления рисками, внутреннего контроля и аудита позволяет Компании принимать взвешенные рискориентированные 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».

01

Менеджмент
Ответственность за внутренний контроль и управление рисками бизнес-процессов

02

Служба внутреннего контроля и управления рисками
Мониторинг и поддержка менеджмента в организации эффективной системы внутреннего контроля и управления рисками

03

Служба внутреннего аудита
Независимая оценка системы внутреннего контроля и управления рисками

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.

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.

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 в 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».

Случаи реализации существенных рисков в 2024 году не выявлены.

Компания непрерывно совершенствует систему управления рисками и внутреннего контроля. В течение 2024 года:

- доработана методология управления рисками с фокусом на недопустимые события;
- актуализирован процесс оценки рисков по новой методологии;
- запущен аналитический отчет по статусу управления рисками.

Планы Компании на 2025 год включают:

- развитие системы оперативной отчетности по рискам с использованием инструментов анализа данных;
- дальнейшее совершенствование методологии оценки рисков;
- развитие профессиональных компетенций в области управления рисками, получение профессиональных сертификаций.

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

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 2024 года служба внутреннего аудита осуществляла свою деятельность в соответствии с утвержденным планом работы внутреннего аудита.
В течение 2024 года совместно со службой управления рисками и внутреннего контроля была проведена переоценка ключевых рисков.

В 2025 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

Согласно Уставу для проверки и подтверждения годовой финансовой отчетности Компании Общее собрание акционеров ежегодно утверждает аудитора, не связанного имущественными интересами с Компанией или ее акционерами.

Назначение внешнего аудитора Компании, его переизбрание и отстранение относятся к компетенции Комитета по аудиту Совета директоров. Комитет рассматривает кандидатов на эту должность, оценивает их независимость и объективность, определяет размер вознаграждения внешнего аудитора, следит за соблюдением внешним аудитором принципов оказания и совмещения услуг по аудиту и сопутствующих услуг в области ведения и подготовки бухгалтерской (финансовой) отчетности.

Внешним аудитором консолидированной финансовой отчетности Компании за 2024 год было выбрано АО «Юникон» (ОГРН 1037739271701, юридический адрес: 117587, г. Москва, Варшавское ш., 125, стр. 1, секция 11, 3 эт., пом. I, ком. 50).

Противодействие коррупции

В Компании организованы 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.

Приложения

8.1

Об Отчете

В настоящем Отчете ПАО «Группа Позитив» (далее также — Компания, Positive Technologies) за 2024 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 2024 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» (с изменениями и дополнениями, вступившими в силу с 1 января 2023 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);
- Рекомендации по раскрытию в годовом отчете публичного акционерного общества информации о вознаграждении членов Совета директоров (наблюдательного совета), членов исполнительных органов и иных ключевых руководящих работников публичного акционерного общества (письмо Банка России от 11 декабря 2017 года № ИН-06-28/57);
- Руководство для эмитента Московской биржи «Как соответствовать лучшим практикам устойчивого развития» (2024).

Этот Отчет подготовлен на основе информации, доступной Компании на дату его составления. В нем могут содержаться заявления прогнозного характера, которые отражают ожидания руководства Компании в отношении будущих результатов ее деятельности, но в силу того, что они относятся к будущим событиям, эти заявления содержат в себе значительную долю неопределенности. Компания не дает гарантий в отношении того, что фактические результаты ее деятельности будут соответствовать результатам или показателям, содержащимся в каких-либо заявлениях прогнозного характера в настоящем Отчете.

[1] Отчет может содержать незначительные неточности в показателях и расчетах, вызванные эффектом округления.

8.2

Консолидированная отчетность по МСФО

АУДИТОРСКОЕ ЗАКЛЮЧЕНИЕ НЕЗАВИСИМОГО АУДИТОРА

о раскрываемой консолидированной финансовой отчетности Публичного акционерного общества «Группа Позитив» и его дочерних организаций по итогам деятельности за 2024 год

СОДЕРЖАНИЕ РАСКРЫВАЕМОЙ КОНСОЛИДИРОВАННОЙ ФИНАНСОВОЙ ОТЧЕТНОСТИ

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 2024 года, раскрываемого консолидированного отчета о прибыли или убытке и прочем совокупном доходе, раскрываемого консолидированного отчета об изменениях в капитале и раскрываемого консолидированного отчета о движении денежных средств за год, закончившийся на указанную дату, а также примечаний к раскрываемой консолидированной финансовой отчетности за 2024 год, включая краткий обзор основных положений учетной политики и прочую пояснительную информацию.

По нашему мнению, прилагаемая раскрываемая консолидированная финансовая отчетность Группы за год, закончившийся 31 декабря 2024 года, 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 соответствующими Международному кодексу этики профессиональных бухгалтеров (включая Международные стандарты независимости), разработанному Советом по международным стандартам этики для профессиональных бухгалтеров, и нами 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

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).

Исправления в раскрываемой консолидированной финансовой отчетности

Мы обращаем внимание на примечание 2.2 «Исправления в финансовой отчетности» к раскрываемой консолидированной финансовой отчетности, в котором раскрыта информация о том, что данная раскрываемая консолидированная финансовая отчетность заменяет первоначально представленную раскрываемую консолидированную финансовую отчетность от 4 апреля 2025 года.

Мы не выражаем модифицированного мнения в связи с этими вопросами.

Прочие сведения

Консолидированная финансовая отчетность и наше заключение о данной отчетности

Группа подготовила полную консолидированную финансовую отчетность за год, закончившийся 31 декабря 2024 года, в соответствии с Международными стандартами финансовой отчетности, в отношении которой мы выпустили отдельное аудиторское заключение для акционеров Организации, датированное 4 апреля 2025 года.

Замена первоначально выданного аудиторского заключения

Данное аудиторское заключение по раскрываемой консолидированной финансовой отчетности заменяет первоначально выданное аудиторское заключение по раскрываемой консолидированной финансовой отчетности от 4 апреля 2025 года.

Прочая информация

Генеральный директор Организации (руководство) несет ответственность за прочую информацию. Прочая информация включает информацию, содержащуюся в годовом отчете за 2024 год и отчете эмитента за 2024 год, но не включает раскрываемую консолидированную финансовую отчетность и наше аудиторское заключение о ней.

Наше мнение об раскрываемой консолидированной финансовой отчетности не распространяется на прочую информацию, и мы не предоставляем вывода, обеспечивающего 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 прочей информацией и рассмотрении вопроса о том, имеются ли существенные несоответствия между прочей информацией и раскрываемой консолидированной финансовой отчетности или нашими знаниями, полученными в ходе аудита, и не содержит ли прочая информация иных возможных существенных искажений. Если на основании проведенной нами работы мы приходим к выводу о том, что такая прочая информация содержит существенное искажение, мы обязаны сообщить об этом факте.

Мы не выявили никаких фактов, которые необходимо отразить в нашем заключении.

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 01.01.2024 № 8-01/2024-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

10 декабря 2025 года

Раскрываемый консолидированный отчет о прибыли или убытке и прочем совокупном доходе

за год, закончившийся 31 декабря 2024 г.

В тыс. российских рублей	Приме-чание	2024 год	2023 год
Выручка	5	**24 456 985**	**22 212 552**
Выручка от реализации лицензий		*21 733 480*	*20 149 706*
Выручка от реализации услуг в области информационной безопасности		*2 143 672*	*1 737 155*
Выручка от реализации программно-аппаратных комплексов		*389 722*	*187 739*
Прочая выручка		*190 111*	*137 952*
Себестоимость	7	**(2 386 332)**	**(1 459 417)**
Заработная плата и социальные отчисления		*(744 579)*	*(666 479)*
Амортизация нематериальных активов		*(1 296 596)*	*(652 341)*
Стоимость материалов		*(187 929)*	*(36 765)*
Прочие расходы		*(157 228)*	*(103 832)*
Валовая прибыль		**22 070 653**	**20 753 135**
Операционные расходы	7	**(17 455 816)**	**(10 930 553)**
Расходы на исследования и разработки		(3 824 016)	(2 309 325)
Расходы на продажу		(4 943 890)	(3 615 686)
Расходы на отраслевые мероприятия и развитие бизнеса		(2 632 508)	(1 218 831)
Расходы на продвижение и маркетинг		(1 487 269)	(1 149 245)
Общехозяйственные и административные расходы		(4 487 625)	(2 595 595)
Прочие операционные расходы, нетто		(80 508)	(41 871)
Прибыль от операционной деятельности		**4 614 837**	**9 822 582**
Процентные доходы		507 946	244 961
Процентные расходы	17	(1 225 224)	(148 086)
Прочие финансовые расходы		(48 431)	(28 374)
Прибыль до налогообложения		**3 849 128**	**9 891 083**
Расходы по налогу на прибыль	8	(185 139)	(194 871)
Прибыль за год		**3 663 989**	**9 696 212**
Прибыль, приходящаяся на долю:			
Собственников Компании	9	*3 662 039*	*9 696 212*
Неконтролирующих долей участия		*1 950*	*-*
Прочий совокупный доход:			
Статьи, которые впоследствии могут быть реклассифицированы в состав прибыли или убытка:			
Эффект пересчета иностранных подразделений в валюту презентации отчетности		312	(1 604)
Прочий совокупный расход за период		**312**	**(1 604)**
Общий совокупный доход за период		**3 664 301**	**9 694 608**
Приходящийся на долю:			
Собственников Компании		*3 662 351*	*9 694 608*
Неконтролирующих долей участия		*1 950*	*-*
Прибыль на акцию, рубли			
Базовая и разводненная прибыль на обыкновенную акцию	9	51,45	146,91

Примечания на стр. с 12 по 54 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет о финансовом положении

по состоянию на 31 декабря 2024 г.

В тыс. российских рублей	Приме-чание	31 декабря 2024 года	31 декабря 2023 года
АКТИВЫ			
Внеоборотные активы			
Основные средства	10, 20	3 279 653	1 768 391
Нематериальные активы	11	21 457 217	7 543 568
Прочие финансовые активы	15	1 702 400	-
Отложенные налоговые активы	8	357 085	278 626
		26 796 355	**9 590 585**
Оборотные активы			
Запасы	12	562 415	120 686
Торговая и прочая дебиторская задолженность	13	19 135 056	16 969 208
Денежные средства и их эквиваленты	14	6 225 167	1 683 655
		25 922 638	**18 773 549**
ИТОГО АКТИВЫ		**52 718 993**	**28 364 134**
КАПИТАЛ			
Уставный капитал	16	35 607	33 000
Акции в собственности	16	(2 404)	-
Нераспределенная прибыль		9 491 947	13 171 115
Резерв по платежам, основанным на акциях	16	7 536 197	-
Резерв накопленных курсовых разниц		(3 515)	(3 827)
Капитал, приходящийся на долю собственников Компании		**17 057 832**	**13 200 288**
Неконтролирующие доли участия		1 950	-
ИТОГО КАПИТАЛ		**17 059 782**	**13 200 288**
ОБЯЗАТЕЛЬСТВА			
Долгосрочные обязательства			
Долгосрочные кредиты и займы	17	10 326 668	2 873 631
Обязательства по договорам с покупателями	18	2 860 901	3 180 663
Отложенные налоговые обязательства	8	501 307	238 566
Торговая и прочая кредиторская задолженность	19	-	134 971
		13 688 876	**6 427 831**
Краткосрочные обязательства			
Краткосрочные кредиты и займы	17	16 022 157	2 803 441
Обязательства по договорам с покупателями	18	1 770 024	1 283 820
Торговая и прочая кредиторская задолженность	19	4 178 154	4 643 268
Обязательства по налогу на прибыль	8	-	5 486
		21 970 335	**8 736 015**
ИТОГО ОБЯЗАТЕЛЬСТВА		**35 659 211**	**15 163 846**
ИТОГО КАПИТАЛ И ОБЯЗАТЕЛЬСТВА		**52 718 993**	**28 364 134**

Д. Баранов

Генеральный директор

10 декабря 2025

Примечания на стр. с 12 по 54 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет об изменениях в капитале

за год, закончившийся 31 декабря 2024 г.

В тыс. российских рублей	Приходящийся на долю собственников Компании: 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 2023 года	**33 000**		**8 267 163**	**-**	**(2 223)**	**8 297 940**	**-**	**8 297 940**
Прибыль за год			9 696 212	-	-	**9 696 212**	**-**	**9 696 212**
Прочий совокупный доход:								
Эффект курсовых разниц	-		-	-	(1 604)	**(1 604)**	**-**	**(1 604)**
Итого совокупный доход за 2023 год	**-**		**9 696 212**	**-**	**(1 604)**	**9 694 608**	**-**	**9 694 608**
Дивиденды	-		(4 792 260)	-	-	**(4 792 260)**	-	**(4 792 260)**
На 31 декабря 2023 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	-	-	-	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 (см. Примечание 16)	**35 607**	**(2 404)**	**9 491 947**	**7 536 197**	**(3 515)**	**17 057 832**	**1 950**	**17 059 782**

Примечания на стр. с 12 по 54 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

Раскрываемый консолидированный отчет о движении денежных средств

за год, закончившийся 31 декабря 2024 г.

В тыс. российских рублей	Примечание	2024 год	2023 год
Движение денежных средств от операционной деятельности			
Прибыль до налогообложения		**3 849 128**	**9 891 083**
Корректировки:			
Чистые финансовые расходы / (доходы)		720 588	(96 875)
Амортизация основных средств	10	555 452	357 400
Амортизация нематериальных активов	11	1 336 554	674 069
Движение резервов по ожидаемым кредитным убыткам по дебиторской задолженности	13	1 118	(16 154)
Расходы по вознаграждению акциями		96 250	-
Курсовые разницы		(6 714)	(6 802)
Убыток от выбытия основных средств и нематериальных активов	10	18 830	19 014
Изменения оборотного капитала		**(3 146 788)**	**(5 221 371)**
Изменение торговой и прочей дебиторской задолженности	13	(2 166 966)	(10 026 058)
Изменение торговой и прочей кредиторской задолженности	19	(704 535)	2 543 614
Изменение обязательств по договорам с покупателями	18	166 442	2 200 254
Изменение запасов	12	(441 729)	60 819
Поступления денежных средств от основной деятельности		**3 424 418**	**5 600 364**
Проценты уплаченные	17	(968 986)	(130 976)
Проценты полученные		480 614	246 147
Банковские комиссии и прочие финансовые расходы		(38 446)	(28 375)
Налог на прибыль уплаченный		(11 512)	(226 973)
Денежные средства, полученные от операционной деятельности, нетто		**2 886 088**	**5 460 187**
Движение денежных средств от инвестиционной деятельности			
Денежные средства уплаченные:			
Приобретение основных средств		(1 422 728)	(614 449)
Создание нематериальных активов		(5 139 397)	(2 873 909)
Покупка нематериальных активов		(109 208)	(72 694)
Займы выданные		(1 704 400)	-
Денежные средства, использованные в инвестиционной деятельности, нетто		**(8 375 733)**	**(3 561 052)**
Движение денежных средств от финансовой деятельности			
Денежные средства полученные:			
Получение кредитов и займов	17	26 470 211	2 700 000
Денежные средства уплаченные:			
Дивиденды, выплаченные акционерам Компании		(6 546 540)	(4 792 260)
Погашение кредитов и займов	17	(6 300 000)	(2 064 281)
Платежи по договорам аренды	20	(292 408)	(179 555)
Выкуп собственных акций		(3 300 418)	-
Денежные средства, полученные от / (использованные в) финансовой деятельности, нетто		**10 030 845**	**(4 336 096)**
Эффект от курсовых разниц на остатки денежных средств и их эквивалентов		312	(1 604)
Изменение денежных средств и их эквивалентов, нетто		**4 541 512**	**(2 438 565)**
Денежные средства и их эквиваленты на начало года	**14**	**1 683 655**	**4 122 220**
Денежные средства и их эквиваленты на конец года	**14**	**6 225 167**	**1 683 655**

Примечания на стр. с 12 по 54 составляют неотъемлемую часть данной раскрываемой консолидированной финансовой отчетности

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 2024 года, для ПАО «Группа Позитив» (до 13 декабря 2021 – АО «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 раскрываемую консолидированную финансовую отчетность, представлены ниже:

Дочерняя компания	Страна	Вид деятельности	Доля владения на 2024 год	Доля владения на 2023 год
Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102		Разработка компьютерного программного обеспечения и оказание сопутствующих услуг	100%	100%
		Продажа компьютерного программного обеспечения, компьютерного оборудования и оказание сопутствующих услуг	100%	100%
		Продажа компьютерного программного обеспечения и оказание сопутствующих услуг	99%	100%
		Разработка компьютерного программного обеспечения и оказание сопутствующих услуг	99%	99%
		Предоставление прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению	100%	100%
		Деятельность административно-хозяйственная комплексная по обеспечению работы организации	100%	100%

По состоянию на 31 декабря 2024 и 31 декабря 2023 гг. бенефициарным владельцем Группы являлся *(Сведения не раскрываются на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102)*.

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 2024 г. в Группе работало 3 160 человек (на 31 декабря 2023 г. – 2 285), 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 2023 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 не оказали существенного влияния на деятельность Группы, так как подавляющая доля выручки Группы (99%) получена от клиентов из России и стран СНГ. Кроме того, санкции не повлияли на динамику выручки Группы: в отчетном году рост выручки составил 10%.

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 2024 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 4.

2.2 Исправления в финансовой отчетности

Ранее Группа не раскрывала данные о дочерних компаниях в раскрываемой консолидированной финансовой отчетности на основании Постановлений Правительства РФ от 28.09.2023 №1587, от 04.07.2023 №1102 во избежание возможных санкций. Банк России уточнил требования в отношении раскрываемой информации, в результате чего, по решению руководства Группы, в раскрываемую консолидированную финансовую отчетность были внесены изменения.

В данной раскрываемой консолидированной финансовой отчетности учтена позиция Банка России, а именно в раздел 1 «Общие сведения» пояснений к раскрываемой консолидированной финансовой отчетности добавлена информация о видах деятельности дочерних компаний и долях владения дочерними компаниями.

Данная раскрываемая консолидированная финансовая отчетность заменяет первоначально представленную раскрываемую консолидированную финансовую отчетность от 4 апреля 2025 года.

2.3 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.

2.4 Основные аспекты учетной политики

Основные аспекты учетной политики, применяемой Группой при подготовке настоящей раскрываемой консолидированной финансовой отчетности, представлены ниже:

2.4.1 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 и 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.

2.4.2 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

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	
	2024 года	**2023 года**
Доллар США к Российскому рублю		
На конец года	101,6797	89,6883
Средний за период	92,5652	85,2466
Евро к Российскому рублю		
На конец года	106,1028	99,1919
Средний за период	100,2154	92,2406

2.4.3 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.

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.

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:

- 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.

2.4.4 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
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».

2.4.5 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.

2.4.6 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;
- 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 2024 и 2023 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.

2.4.7 Обесценение нефинансовых активов

Дополнительная информация об обесценении нефинансовых активов также представлена в следующих примечаниях:

- Ключевые бухгалтерские суждения, оценочные значения и допущения – Примечание 4;
- 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.

2.4.8 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.

2.5 Применение новых или пересмотренных стандартов и интерпретаций

Следующие поправки к стандартам вступили в силу в отчетном периоде, начавшемся 1 января 2024 года:

- «Классификация обязательств как краткосрочных или долгосрочных» (поправка к МСФО (IAS) 1 «Представление финансовой отчетности»);
- «Долгосрочные обязательства с ковенантами» (поправка к МСФО (IAS) 1 «Представление финансовой отчетности»);
- «Обязательства по аренде при продаже и обратной аренде» (поправка к МСФО (IFRS) 16 «Аренда»);
- «Соглашения о финансировании поставщиков» (поправки к МСФО (IAS) 7 «Отчеты о движении денежных средств» и МСФО (IFRS) 7 «Финансовые инструменты: раскрытие информации»).

Данные поправки не оказали существенного влияния на раскрываемую консолидированную финансовую отчетность Группы за 2024 г.

2.6 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.

- «Ограничения конвертируемости валют» (поправка к МСФО (IAS) 21 «Влияние изменений валютных курсов»), вступает в силу 1 января 2025 года;
- «Классификация и оценка финансовых инструментов» (поправки к МСФО (IFRS) 9 «Финансовые инструменты» и МСФО (IFRS) 7 «Финансовые инструменты: раскрытие информации»);
- «Презентация и раскрытие финансовой отчетности» (стандарт МСФО (IFRS) 18), вступает в силу 1 января 2027 года;
- «Дочерние компании без публичной отчетности: раскрытие информации» (стандарт МСФО (IFRS) 19), вступает в силу 1 января 2027 года.

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.

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 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 2024 года	31 декабря 2023 года
Торговая дебиторская задолженность	13	18 206 736	16 687 967
Денежные средства и их эквиваленты	14	6 225 167	1 683 655
Общая максимальная подверженность кредитному риску		**24 431 903**	**18 371 622**

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 2024 года примерно 27% кредитов и займов Группы имеют фиксированную процентную ставку (на 31 декабря 2023: 70%).

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.

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 2024 года	31 декабря 2023 года	31 декабря 2024 года	31 декабря 2023 года	31 декабря 2024 года	31 декабря 2023 года
Монетарные финансовые активы	46 475	6 379	5 066	4 749	-	7 570
Монетарные финансовые обязательства	(8 834)	(322)	(393)	-	(10 632)	(528)
Чистая валютная позиция	**37 641**	**6 057**	**4 673**	**4 749**	**(10 632)**	**7 042**

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 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**

31 декабря 2023 года	менее 1 года	1-2 года	2-5 лет	Итого
Торговая кредиторская задолженность	326 263	-	-	**326 263**
Кредиты и займы	-	5 044 014	-	**5 044 014**
Обязательства по аренде	259 424	176 716	196 918	**633 058**
Итого	**585 687**	**5 220 730**	**196 918**	**6 003 335**

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 за последние 12 месяцев.

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.

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 2024 года	31 декабря 2023 года
Общая сумма долга	25 433 388	5 044 072
Наличные денежные средства и остатки на счетах в банках	6 225 167	1 683 655
Чистый долг	**19 208 221**	**3 360 417**
EBITDA	6 458 413	10 825 677
Чистый долг/EBITDA	2,97	0,3

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)
- 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 2024 г. составили 937 000 тыс. руб. (2023 г: (2 639 790) тыс. руб.), как указано в таблице ниже:

в тыс. российских рублей	2024 год	2023 год
Отгрузки с НДС	**24 080 419**	**25 529 319**
НДС	*(560 434)*	*(676 977)*
Отгрузки без НДС	**23 519 985**	**24 852 342**
Разницы между отгрузками и выручкой	*937 000*	*(2 639 790)*
Выручка (см. Примечание 5)	**24 456 985**	**22 212 552**

в тыс. российских рублей	2024 год	2023 год
EBITDA	**6 458 413**	**10 825 677**
Разницы между отгрузками и выручкой, за искл. разниц в классификации премий покупателям	*(1 327 098)*	*1 640 733*
Капитализированные расходы и прочее	*(6 371 879)*	*(3 546 610)*
EBITDAC	**(1 240 564)**	**8 919 800**

в тыс. российских рублей	2024 год	2023 год
Прибыль за период	**3 663 989**	**9 696 212**
Разницы между отгрузками и выручкой, за искл. разниц в классификации премий покупателям	*(1 327 098)*	*1 640 733*
Капитализированные расходы и прочее	*(6 371 879)*	*(3 546 610)*
Амортизация капитализированных расходов, капитализация процентов и прочее	*1 379 837*	*949 321*
NIC	**(2 655 151)**	**8 739 656**

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 2024 года, составляла 17 057 832 тыс. рублей (на 31 декабря 2023: 13 200 288 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 2024 года составляет 1,5:1 (2023: 0,4:1).

4. 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 2024 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 93 404 тыс. руб. (за год, закончившийся 31 декабря 2023 года: на 57 628 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.

За год, закончившийся 31 декабря 2024 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 39 922 тыс. руб. (за год, закончившийся 31 декабря 2023 года: на 21 423 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 11.

5. Выручка по договорам с покупателями

В следующей таблице выручка по договорам с покупателями разбита по основным категориям и срокам признания выручки.

	2024 год		2023 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	**21 733 480**	**-**	**20 149 706**	**-**
Выручка от реализации программно-аппаратных комплексов	**329 936**	**59 786**	**40 497**	**147 242**
Выручка от реализации услуг в области информационной безопасности	**988 941**	**1 154 731**	**807 336**	**929 819**
Выручка от услуг ИТ-безопасности	622 360	-	686 234	-
Выручка от услуг технической поддержки и мониторинга безопасности	-	1 154 731	-	929 819
Выручка от услуг в области исследований и технологических разработок	80 263	-	3 750	-
Выручка от прочих услуг	286 318	-	117 352	-
Прочая выручка	**190 111**	**-**	**137 952**	**-**
Итого выручка	**23 242 468**	**1 214 517**	**21 135 491**	**1 077 061**

6. 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 2024 примерно 82% выручки Группы было получено через четырех крупных дистрибьюторов (в течение 2023 примерно 76% 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 в 2024 составило 2 876, в 2023 – 2 700. В связи с этим, руководство Группы считает, что риск операционной концентрации не является существенным. По состоянию на 31 декабря 2024 года непогашенная дебиторская задолженность этих покупателей составляла 16 097 592 тыс. рублей (на 31 декабря 2023: 15 674 405 тыс. рублей). Большая часть выручки приходится на клиентов из Российской Федерации: 96% в 2024 (в 2023: 99%).

Продукцию Группы можно разделить на четыре основные продуктовые линейки. Общая выручка по продуктовым линейкам за годы, закончившиеся 31 декабря 2024 и 2023, представлена в Примечании 5.

7. Операционные расходы

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**
Расходы на мероприятия	-	-	-	1 763 487	792 930	-	-	**2 556 417**
Амортизация нематериальных активов	1 296 596	7 982	30 918	-	1 058	-	-	**1 336 554**
Маркетинговые расходы	-	-	-	-	-	972 430	-	**972 430**
Профессиональные услуги	117 913	189 900	260 725	-	37 416	34 035	-	**639 989**
Услуги связи и дата-центров	-	75 005	263 786	-	-	-	-	**338 791**
Командировочные расходы	281	139 107	123 145	86 251	144 182	1 903	-	**494 869**
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**
Амортизация основных средств	12 307	74 683	435 084	4 542	25 479	3 358	-	**555 453**
Стоимость материалов	187 929	35 628	258 334	123 149	-	-	-	**605 040**
Курсовые разницы, нетто	-	-	-	-	-	-	(6 714)	**(6 714)**
Прочие расходы, 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 2024 г.

Операционные расходы Группы за 2023 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	2023 год
Заработная плата	634 743	1 821 388	1 262 913	354 764	3 148 397	318 161	-	**7 540 366**
Социальные отчисления	31 736	66 024	63 703	11 459	81 191	14 995	-	**269 108**
Расходы на мероприятия	-	-	-	647 600	178 291	-	-	**825 891**
Амортизация нематериальных активов	652 341	6 680	12 863	-	2 185	-	-	**674 069**
Маркетинговые расходы	-	-	-	-	1 836	757 082	-	**758 918**
Профессиональные услуги	82 222	176 039	262 441	-	32 576	39 174	-	**592 452**
Услуги связи и дата-центров	-	105 169	90 320	-	1 127	-	-	**196 616**
Командировочные расходы	-	45 374	48 508	27 910	45 812	-	-	**167 604**
Расходы на программное обеспечение	4 623	21 577	130 798	1 020	8 303	1 026	-	**167 347**
Расходы на аренду и содержание помещений	-	4	164 595	3 059	43 087	13 046	-	**223 791**
Амортизация основных средств	-	49 866	249 417	5 729	46 628	5 761	-	**357 401**
Стоимость материалов	36 765	10 118	196 223	167 290	-	-	-	**410 396**
Курсовые разницы, нетто	-	-	-	-	-	-	(6 802)	**(6 802)**
Прочие расходы, нетто	16 987	7 086	113 814	-	26 253	-	48 673	**212 813**
Итого	**1 459 417**	**2 309 325**	**2 595 595**	**1 218 831**	**3 615 686**	**1 149 245**	**41 871**	**12 389 970**

Операционные расходы, которые были отражены по строке «Маркетинговые и коммерческие расходы» в раскрываемом консолидированном отчете о прибыли или убытке и прочем совокупном доходе за 2023 год были перегруппированы и разделены на следующие строки: «Расходы на отраслевые мероприятия и развитие бизнеса», «Расходы на продажу» и «Расходы на продвижение и маркетинг».

8. Налог на прибыль

Расходы по налогу на прибыль включают следующее:

в тыс. российских рублей	2024 год	2023 год
Текущий налог	857	20 833
Отложенный налог	184 282	3 087
Прочее	-	170 951
Итого налог на прибыль за отчетный период	**185 139**	**194 871**

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 20% в 2024 году (20% в 2023 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	2024 год	2023 год
Прибыль до налогообложения	**3 849 128**	**9 891 083**
Теоретические расходы по налогу на прибыль по ставке, установленной законодательством	769 826	1 978 217
Эффект от применения пониженной ставки налогообложения для ИТ-компаний	(522 050)	(1 873 492)
Эффект от не вычитаемых расходов для применяемых ставок налогообложения	(62 637)	(80 805)
Прочие разницы	-	170 951
Итого налог на прибыль за отчетный период	**185 139**	**194 871**

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 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

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			
Налоговые убытки, перенесенные на будущие периоды	6 773	56 046	62 819
Признанный отложенный налоговый актив	**278 626**	**78 459**	**357 085**

в тыс. российских рублей	1 января 2023 года	Начислено в прибыли или убытке	31 декабря 2023 года
Налоговый эффект от вычитаемых временных разниц и налоговых убытков, перенесенных на будущие периоды			
Обязательства по договорам с покупателями	17 761	141 905	159 666
Торговая и прочая кредиторская задолженность	11 252	72 496	83 748
Займы и кредиты	55 341	(35 974)	19 367
Торговая и прочая дебиторская задолженность	22 894	(13 822)	9 072
Налоговые убытки, перенесенные на будущие периоды	19 657	(12 884)	6 773
Признанный отложенный налоговый актив	**126 905**	**151 721**	**278 626**

По состоянию на 31 декабря 2024 года Группа накопила налоговые убытки в размере 314 095 тыс. рублей (вычитаемая временная разница в размере 62 819 тыс. руб.) (на 31 декабря 2023: 33 865 тыс. рублей (вычитаемая временная разница в размере 6 773 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 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**

в тыс. российских рублей	1 января 2023 года	Начислено в прибыли или убытке	31 декабря 2023 года
Налоговый эффект от налогооблагаемых временных разниц			
Нематериальные активы	21 886	178 586	200 472
Основные средства	61 488	(26 603)	34 885
Торговая и прочая дебиторская задолженность	384	2 825	3 209
Признанное налоговое отложенное обязательство	**83 758**	**154 808**	**238 566**

9. 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.

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	2024 год	2023 год
Прибыль за год	3 663 989	9 696 212
Средневзвешенное количество акций в обращении (шт.)	71 213 997	66 000 000
Базовая и разводненная прибыль на акцию (выражена в рублях на акцию)	**51,45**	**146,91**

10. 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 2023 года	**969 792**	**777 507**	**89 699**	**20 880**	**97 204**	**1 955 082**
Накопленная амортизация	**(579 632)**	**(282 471)**	**(49 672)**	**(6 868)**	**(26 591)**	**(945 234)**
Остаточная стоимость на 1 января 2023 года	**390 160**	**495 036**	**40 027**	**14 012**	**70 613**	**1 009 848**
Поступления	426 769	533 937	65 603	15 168	46 263	**1 087 740**
Модификация договоров аренды	42 099	-	-	-	-	**42 099**
Выбытия	(112 931)	(20 206)	(35 619)	(872)	-	**(169 628)**
Начисленная амортизация	(192 704)	(111 031)	(7 794)	(1 689)	(44 182)	**(357 400)**
Выбытие амортизации	98 891	20 824	35 436	581	-	**155 732**
Выкуп лизингового оборудования (первоначальная стоимость)	(117 105)	117 105	-	-	-	**-**
Выкуп лизингового оборудования (накопленная амортизация)	59 514	(59 514)	-	-	-	**-**
Первоначальная стоимость на 31 декабря 2023 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 31 декабря 2023 года	**594 693**	**976 151**	**97 653**	**27 200**	**72 694**	**1 768 391**
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**

11. 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 2023 года	**2 659 824**	**2 434 636**	**80 179**	**5 174 639**
Первоначальная стоимость на 1 января 2023 года	**4 501 452**	**2 434 636**	**124 708**	**7 060 796**
Накопленная амортизация на 1 января 2023 года	**(1 723 250)**	**-**	**(44 529)**	**(1 767 779)**
Накопленное обесценение на 1 января 2023 года	**(118 378)**	**-**	**-**	**(118 378)**
Поступления	1 618 235	1 384 603	45 279	3 048 117
Начисленная амортизация	(652 890)	-	(21 179)	(674 069)
Реклассификация в НМА, прошедшие стадию разработки	2 540 032	(2 540 032)	-	-
Обесценение НМА	118 378	-	-	118 378
Выбытие НМА	(205 116)	-	(5 118)	(210 234)
Списание амортизации	86 737	-	-	86 737
Остаточная стоимость на 31 декабря 2023 года	**6 165 200**	**1 279 207**	**99 161**	**7 543 568**
Первоначальная стоимость на 31 декабря 2023 года	**8 454 603**	**1 279 207**	**164 869**	**9 898 679**
Накопленная амортизация на 31 декабря 2023 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 2024года	**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)**

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:

- 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 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;
- ПТ 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**
Первоначальная стоимость на 1 января 2023 года	**2 986 467**	**1 376 135**
Накопленная амортизация на 1 января 2023 года	**(1 067 741)**	-
Остаточная стоимость на 1 января 2023 года	**1 918 726**	**1 376 135**
Поступления	1 061 055	684 202
Начисленная амортизация	(419 492)	-
Реклассификация в НМА, прошедшие стадию разработки	1 595 284	(1 595 284)
Остаточная стоимость на 31 декабря 2023 года	**4 155 573**	**465 053**
Первоначальная стоимость на 31 декабря 2023 года	**5 642 806**	**465 053**
Накопленная амортизация на 31 декабря 2023 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)
Остаточная стоимость на 31 декабря 2024 года	**10 293 088**	**2 982 902**

в тыс. российских рублей	**Нематериальные активы, прошедшие стадию разработки**	**Нематериальные активы, находящиеся на стадии разработки**
Первоначальная стоимость на 31 декабря 2024 года	**12 680 031**	**2 982 902**
Накопленная амортизация на 31 декабря 2024 года	**(2 386 943)**	-

Остаточный срок полезного использования таких продуктов на 31 декабря 2024 года находится в диапазоне от 2 до 10 лет, на 31 декабря 2023 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 (Валнерабилити 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**
Первоначальная стоимость на 1 января 2023 года	**1 309 870**	**431 210**
Накопленная амортизация на 1 января 2023 года	**(568 771)**	-
Остаточная стоимость на 1 января 2023 года	**741 099**	**431 210**
Поступления	367 376	208 655
Начисленная амортизация	(173 208)	-
Реклассификация в НМА, прошедшие стадию разработки	483 000	(483 000)
Остаточная стоимость на 31 декабря 2023 года	**1 418 267**	**156 865**
Первоначальная стоимость на 31 декабря 2023 года	**2 160 246**	**156 865**
Накопленная амортизация на 31 декабря 2023 года	**(741 979)**	-
Поступления	2 685 573	448 501
Начисленная амортизация	(266 527)	-
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**

в тыс. российских рублей	**Нематериальные активы, прошедшие стадию разработки**	**Нематериальные активы, находящиеся на стадии разработки**
Накопленная амортизация на 31 декабря 2024 года	**(1 008 506)**	-

Остаточный срок полезного использования таких продуктов на 31 декабря 2024 года находится в диапазоне от 3 до 6 лет, на 31 декабря 2023 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, анализирующя 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 2023 года	**265 033**
Накопленная амортизация на 1 января 2023 года	-
Остаточная стоимость на 1 января 2023 года	**265 033**
Поступления	392 256
Остаточная стоимость на 31 декабря 2023 года	**657 289**
Первоначальная стоимость на 31 декабря 2023 года	**657 289**
Накопленная амортизация на 31 декабря 2023 года	-
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	-

4) Прочие решения Группы

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 2023 года	**205 116**	**362 257**
Накопленная амортизация на 1 января 2023 года	**(86 738)**	**-**
Накопленное обесценение на 1 января 2023 года	**(118 378)**	**-**
Остаточная стоимость на 1 января 2023 года	**-**	**362 257**
Поступления	189 804	99 490
Начисленная амортизация	(60 190)	-
Реклассификация в НМА, прошедшие стадию разработки	461 747	(461 747)
Выбытие НМА	(205 116)	-
Списание амортизации	86 737	-
Обесценение НМА	118 378	-
Остаточная стоимость на 31 декабря 2023 года	**591 361**	**-**
Первоначальная стоимость на 31 декабря 2023 года	**651 551**	**-**
Накопленная амортизация на 31 декабря 2023 года	**(60 190)**	**-**
Поступления	931 658	254 105
Начисленная амортизация	(112 958)	-
Реклассификация в НМА, прошедшие стадию разработки	2 122	(2 122)
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)**	**-**

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 2024 и 2023 гг. руководство проверило нематериальные активы, созданные Группой, на предмет возможного обесценения. По состоянию на 31 декабря 2024 года и 31 декабря 2023 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.

Ставка дисконтирования до налогообложения, применяемая к прогнозам денежных потоков, зависит от активов и стадии их разработки следующим образом:

Стадия разработки	**Ставка дисконтирования**
Обоснование концепции	20%-30%
Разработка после обоснования концепции	20%-25%
Готовность актива к продаже	17%
Разработка после готовности актива к продаже	17%

Указанная в таблице выше стадия «Обоснование концепции» является моментом времени, когда исследовательские работы завершены и Группа планирует приступить к разработке ИТ-продукта. На данном этапе составляется финансовая модель по продукту для целей обоснования экономической целесообразности разработки ИТ-продукта.

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 на 5% не приведет к обесценению;
- повышение ставки дисконтирования на 1% не приведет к обесценению;
- повышение будущего запланированного объёма административных и коммерческих расходов на 5% не приведет к обесценению.

В 2024 году следующие расходы были капитализированы как нематериальные активы: расходы на персонал – 13 945 031 тыс. рублей (2023: 2 451 073 тыс. рублей); профессиональные услуги – 310 517 тыс. рублей (2023: 240 849 тыс. рублей); прочие операционные расходы – 6 163 тыс. рублей (2023: 2 508 тысяч рублей).

Капитализированные затраты по займам в 2024 году составляют 823 384 тысяч рублей (в 2023: 300 833 тыс. рублей). Эффективная ставка капитализации затрат по займам составила 16,2% в 2024 году (2023: 9,5%).

В течение 2023 и 2024 годов Группа пересмотрела ожидаемый срок полезного использования нематериальных активов в результате значительных улучшений программных продуктов, которые приведут к уменьшению амортизационных отчислений за годы, закончившиеся 31 декабря 2023 года и 31 декабря 2024 года соответственно.

По результатам 2024 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 2024 года		31 декабря 2023 года	
в тыс. российских рублей	Остаточная стоимость нематериальных активов, созданных Группой (МСФО оценка)	Справедливая стоимость нематериальных активов, созданных Группой	Остаточная стоимость нематериальных активов, созданных Группой (МСФО оценка)	Справедливая стоимость нематериальных активов, созданных Группой
Продукты, которые активно продаются на рынке либо по которым прошел ряд успешных пилотов	15 960 641	69 000 000	5 436 144	87 000 000
Прочие продукты	5 496 576	Не оценивались	2 107 424	Не оценивались

12. Запасы

в тыс. российских рублей	31 декабря 2024 года	31 декабря 2023 года
Товарно-материальные ценности	559 929	118 887
Прочее	2 486	1 799
Итого запасы	**562 415**	**120 686**

13. Торговая и прочая дебиторская задолженность

в тыс. российских рублей	31 декабря 2024 года	31 декабря 2023 года
Торговая дебиторская задолженность	18 206 736	16 687 967
Резерв под ожидаемые кредитные убытки	(13 292)	(12 174)
Итого финансовая торговая дебиторская задолженность, нетто	***18 193 444***	***16 675 793***
Авансы выданные	827 683	158 985
НДС к возмещению	26 517	9 361
Переплаты по налогам	10 974	7 769
Прочая дебиторская задолженность	76 438	117 300
Итого нефинансовая торговая и прочая дебиторская задолженность, нетто	***941 612***	***293 415***
Итого	**19 135 056**	**16 969 208**

В таблице ниже представлена торговая дебиторская задолженность по срокам возникновения:

	31 декабря 2024 года		31 декабря 2023 года	
в тыс. российских рублей	Торговая дебиторская задолженность	Резерв под ожидаемые кредитные убытки	Торговая дебиторская задолженность	Резерв под ожидаемые кредитные убытки
Не просроченная	18 015 281	-	16 539 092	-
Просроченная менее 30 дней	138 213	-	105 510	-
Просроченная 30 – 90 дней	12 861	-	2 706	-
Просроченная более 90 дней	40 381	(13 292)	40 659	(12 174)
Итого	**18 206 736**	**(13 292)**	**16 687 967**	**(12 174)**

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 2023 года	**38 192**
Начисленный за период резерв под ожидаемые кредитные убытки	-
Восстановленный за период резерв под ожидаемые кредитные убытки	(26 018)
На 31 декабря 2023 года	**12 174**
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**

14. Денежные средства и их эквиваленты

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**

в тыс. российских рублей	Рубли	Доллары США	Евро	Прочее	31 декабря 2023 года
Наличные денежные средства и остатки на счетах в банках	1 067 162	550	14	2 663	**1 070 389**
Депозиты	600 000	-	-	13 266	**613 266**
Итого денежные средства и их эквиваленты	**1 667 162**	**550**	**14**	**15 929**	**1 683 655**

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 2024 года	31 декабря 2023 года
Рейтинг от AAA	6 141 362	112 867
Рейтинг от AA- до AA+	64 492	1 549 223
Рейтинг от A- до A+	1 617	769
Прочее	17 696	20 796
Итого	**6 225 167**	**1 683 655**

Указанный выше анализ сделан на основе кредитных рейтингов, присвоенных независимыми рейтинговыми агентствами Эксперт РА и АКРА.

По состоянию на 31 декабря 2024 года, 31 декабря 2023 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 2024, 31 декабря 2023 незначительна и не была отражена в настоящей раскрываемой консолидированной финансовой отчетности.

15. Финансовые активы

в тыс. российских рублей	31 декабря 2024 года	31 декабря 2023 года
Долгосрочные финансовые активы по амортизированной стоимости		
Займы, выданные связанным сторонам	1 702 400	-
Итого долгосрочные финансовые активы по амортизированной стоимости	**1 702 400**	**-**

16. Капитал и резервы

По состоянию на 31 декабря 2024 и 31 декабря 2023 гг. уставный капитал представлен капиталом материнской компании ПАО «Группа Позитив».

Общее количество разрешенных к выпуску обыкновенных акций на 31 декабря 2024 составляет 71 213 997 акций с номинальной стоимостью 0,5 рублей за акцию и на 31 декабря 2023 составляет 66 000 000 акций с номинальной стоимостью 0,5 рублей за акцию.

6 апреля 2023 года акционеры утвердили выплату дивидендов по результатам 12 месяцев 2022 года в размере 2 499 420 тыс. руб., выплата состоялась 18 апреля 2023 года.

12 мая 2023 года акционеры утвердили выплату дивидендов по результатам 12 месяцев 2022 года в размере 1 250 040 тыс. руб., выплата состоялась 24 мая 2023 года.

29 ноября 2023 года акционеры утвердили выплату дивидендов по результатам 9 месяцев 2023 года в размере 1 042 800 тыс. руб., выплата состоялась 5 декабря 2023 года.

9 апреля 2024 года акционеры утвердили выплату дивидендов по результатам 12 месяцев 2023 года в размере 3 121 800 тыс. руб., выплата состоялась 23 апреля 2024 года.

15 мая 2024 года акционеры утвердили выплату дивидендов по результатам 12 месяцев 2023 года в размере 3 123 780 тыс. руб., выплата состоялась 28 мая 2024 года.

15 мая 2024 года акционеры утвердили выплату дополнительных дивидендов по результатам 12 месяцев 2023 года в размере 300 960 тыс. руб., выплата состоялась 28 мая 2024 года.

С 19 июля 2024 по 14 августа 2024 года Группа совершила операции обратного выкупа собственных акций на общую сумму 3 300 418 тыс. руб. (1 101 272 шт. по рыночной цене 2 996,9 руб. за 1 акцию).

7 ноября 2024 года произошло дополнительное размещение акций ПАО «Группа Позитив» в количестве 5 214 000 штук номинальной стоимостью 0,5 рубля каждая.

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.

17. Кредиты и займы

в тыс. российских рублей	31 декабря 2024 года	31 декабря 2023 года
Долгосрочные обязательства		
Выпущенные необеспеченные облигации	9 729 055	2 500 000
Обязательства по аренде (Примечание 20)	597 613	373 631
	10 326 668	**2 873 631**
Краткосрочные обязательства		
Обеспеченные банковские кредиты	9 964 582	2 525 924
Займы, полученные от связанных сторон	3 160 434	-
Обязательства по аренде (Примечание 20)	317 825	259 427
Выпущенные необеспеченные облигации	2 579 316	18 090
	16 022 157	**2 803 441**
Итого	**26 348 825**	**5 677 072**

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 20)	8,63–21,1%	2024-2030	915 438
Итого			**26 348 825**

Вид	Процентная ставка	Срок погашения	Задолженность на 31 декабря 2023 года
Выпущенные необеспеченные облигации	10,55%	2024	2 518 090
Обеспеченные банковские кредиты с плавающей процентной ставкой	Ключевая ставка ЦБ РФ + 1,4%	2024	1 523 212
Обеспеченные банковские кредиты с фиксированной процентной ставкой	16,5%	2024	1 002 712
Обязательства по аренде (Примечание 20)	8,63–13,77%	2023-2028	633 058
Итого			**5 677 072**

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.

В таблице ниже представлены движения обязательств по финансовой деятельности в течение 2023 и 2024 годов:

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**

в тыс. российских рублей	Кредиты и займы	Обязательства по аренде	Выпущенные облигации	Итого
Обязательства по финансовой деятельности на 1 января 2023 года	**1 491 284**	**405 765**	**2 900 164**	**4 797 213**
Денежные потоки	***911 891***	***(228 262)***	***(659 504)***	***24 125***
Получение кредитов и займов	2 700 000	-	-	**2 700 000**
Погашение основного долга	(1 689 281)	(179 555)	(375 000)	**(2 243 836)**
Погашение процентов	(98 828)	(48 707)	(284 504)	**(432 039)**
Неденежные изменения	***122 749***	***455 555***	***277 430***	***855 734***
Начисление процентов	122 749	48 707	277 430	**448 886**
Новые договоры аренды	-	422 340	-	**422 340**
Выкуп лизингового оборудования	-	(57 591)	-	**(57 591)**
Модификации договоров аренды	-	42 099	-	**42 099**
Обязательства по финансовой деятельности на 31 декабря 2023 года	**2 525 924**	**633 058**	**2 518 090**	**5 677 072**

18. Обязательства по договорам с покупателями

На 1 января 2023 года	**2 264 229**
Отражено в отчете о прибыли или убытке в течение отчетного года	(1 852 818)
Отнесено на будущие периоды в течение отчетного года	4 053 072
На 31 декабря 2023 года	**4 464 483**
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**

19. Торговая и прочая кредиторская задолженность

в тыс. российских рублей	31 декабря 2024 года	31 декабря 2023 года
Резервы по заработной плате	2 025 568	2 526 648
Прочая кредиторская задолженность	401 380	948 051
Налоги к уплате	362 760	494 102
Торговая кредиторская задолженность	787 225	326 263
Кредиторская задолженность по текущей заработной плате, включая соответствующие налоги	540 150	314 327
Авансы полученные	61 071	33 877
Итого краткосрочная кредиторская задолженность	***4 178 154***	***4 643 268***
Долгосрочная кредиторская задолженность	-	134 971
Итого долгосрочная кредиторская задолженность	***-***	***134 971***
Итого торговая и прочая кредиторская задолженность	**4 178 154**	**4 778 239**

20. 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.

В 2023 году количество арендуемых помещений значительно возросло в связи с расширением бизнеса и существенным приростом численности персонала.

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 2024 году, 8,63 – 13,77% – в 2023 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 2023 – 2024 гг. представлено в рамках раскрытия по Основным средствам в Примечании 10.

Обязательства по аренде:

в тыс. российских рублей	2023 год
На 1 января 2023 года	**405 765**
Поступления	422 340
Модификация договоров аренды	42 099
Выкуп лизингового оборудования	(57 591)
Платежи	(228 262)
Начисление процентов	48 707

в тыс. российских рублей	2023 год
На 31 декабря 2023 года	**633 058**
в том числе:	
Долгосрочные обязательства по аренде	*373 631*
Краткосрочные обязательства по аренде	*259 427*

в тыс. российских рублей	2024 год
На 1 января 2024 года	**633 058**
Поступления	95 381
Модификация договоров аренды	396 275
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*

Анализ сроков погашения обязательств по аренде представлен в Примечании 3.

21. 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, 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 16%, на 31.12.2024 года ключевая ставка ЦБ РФ составляла 21%.

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.

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.

22. 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 2024 года и 31 декабря 2023 года представлены ниже:

в тыс. российских рублей	**31.12.2024**		**31.12.2023**	
	Тело	**Проценты**	**Тело**	**Проценты**
Займы выданные	1 702 400	24 457	-	-
Займы полученные	(3 144 181)	(16 254)	-	-
	(1 441 781)	**8 203**	**-**	**-**

Информация по изменению балансовой величины займов, выданных и полученных от связанных сторон, представлена ниже:

в тыс. российских рублей	**2024 год**	**2023 год**
На 1 января 2024 года	-	-
Денежные потоки:		
Займы выданные		**-**
Выдано займов	(1 702 400)	-
Займы полученные		
Получено займов	3 144 181	-
Выплачено процентов	(53 876)	-
Неденежные потоки:		
Начислено процентов по займам выданным	(24 457)	-
Начислено процентов по займам полученным	70 130	-
На 31 декабря 2024 года	**1 433 578**	-

Вознаграждения ключевому управленческому персоналу

К ключевому управленческому персоналу относятся ключевые руководители Группы и члены Совета директоров. За годы, закончившиеся 31 декабря 2024 и 2023 гг., общая сумма вознаграждения ключевому управленческому персоналу, включенная в общие и административные расходы, составила 446 084 тыс. руб. и 403 043 тыс. руб. соответственно, включая социальные взносы. По состоянию на 31 декабря 2024 и 2023 гг. задолженность перед ключевым управленческим персоналом составляет 99 119 тыс. руб. и 152 687 тыс. руб. соответственно.

23. События после отчетной даты

20.02.2025 Группа приобрела долю белорусского вендора «ВИРУСБЛОКАДА» и намерена совершенствовать технологию антивирусной защиты для внедрения в существующие продукты, а также для запуска самостоятельного решения этого класса уже в текущем году.

8.3

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 2025 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 2024 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)	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 не соблюдается. В отчетном периоде Общество не проводило Общих собраний акционеров Общества в форме совместного присутствия. В связи с этим в сообщениях о проведении собраний не были указаны документы, необходимые для допуска в помещение. В сообщениях о проведении собраний указывался почтовый адрес, по которому акционеры могли направить бюллетень для голосования, а также адрес страницы в сети Интернет, на которой акционеры могли заполнить электронную форму бюллетеня. В 2025 году Общество планирует проводить годовое Общее собрание акционеров в форме совместного присутствия. В сообщении о проведении указанного собрания планируется указать документы, необходимые для допуска в помещение. Критерий 3 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
1.1.3	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	Частично соблюдается	Критерий 1 частично соблюдается. В отчетном периоде Общество не проводило Общих собраний акционеров в форме совместного присутствия. В связи с этим у акционеров отсутствовала возможность задать очные вопросы Генеральному директору Общества и членам Совета директоров Общества непосредственно в ходе проведения Общих собраний акционеров. При этом акционеры могут задать интересующие их вопросы по электронной почте, направив письмо по адресу shareholder@ptsecurity.com, информация о котором размещена на сайте Общества в сети Интернет. Кроме того, в отчетном году проводились очные и онлайн-мероприятия для акционеров, на которых они могли задать интересующие их вопросы топ-менеджменту Общества, в том числе Генеральному директору Общества (с актуальным перечнем можно ознакомиться на странице «Календарь инвестора» на официальном сайте Общества в сети Интернет). В социальных сетях и каналах, в мессенджерах Общества акционерам предоставлена возможность высказать свое мнение и задать интересующие их вопросы по повестке дня Общих собраний акционеров Общества, любой иной информации Общества, а также общаться с менеджментом Общества и между собой. Общество планирует применять практику ответов на вопросы акционеров членами Совета директоров Общества и Генеральным директором Общества после возобновления практики проведения очного формата Общих собраний акционеров Общества начиная с 2025 года. Критерий 2 частично соблюдается. В отчетном периоде Совет директоров Общества выражал свою позицию по вопросам, связанным с распределением прибыли Общества. Такие позиции были включены в состав материалов к Общим собраниям акционеров Общества, на которых рассматривались соответствующие вопросы. Позиция Совета директоров по каждому вопросу повестки дня Общих собраний акционеров Общества, проведенных в отчетном году, Советом директоров Общества не утверждалась. В случае утверждения Советом директоров Общества позиции по вопросам повестки дня Общих собраний акционеров Общества, такая позиция будет включена в состав материалов к Общим собраниям акционеров Общества. Начиная с 2024 года Общество включает в состав материалов к Общим собраниям акционеров Общества пояснительную записку по каждому вопросу повестки дня Общего собрания акционеров Общества. Критерий 3 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	

№	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
1.1.6	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 частично соблюдается. В отчетном периоде Общество не проводило Общих собраний акционеров Общества в форме совместного присутствия. В связи с этим при проведении Общих собраний акционеров практика докладов не применялась. Обществом организованы различные каналы связи с акционерами. Организуются онлайн- и офлайн-мероприятия для акционеров (с актуальным перечнем можно ознакомиться на странице «Календарь инвестора» на официальном сайте Общества в сети Интернет). На таких мероприятиях предоставляется актуальная информация о результатах деятельности Общества, а также о вопросах, стоящих перед Обществом, в том числе вынесенных на рассмотрение Общего собрания акционеров Общества, акционерам предоставлена возможность высказать свое мнение и задать вопросы. В социальных сетях Общества акционерам предоставлена возможность высказать свое мнение и задать интересующие их вопросы по повестке дня Общих собраний акционеров Общества. Кроме того, любой акционер Общества имеет возможность отправить свои предложения и вопросы на специальный адрес электронной почты: shareholder@ptsecurity.com, информация о котором размещена на официальном сайте Общества в сети Интернет. Общество планирует применять практику докладов и предоставлять акционерам возможность высказать свое мнение и задать вопросы после возобновления практики очного формата проведения Общих собраний акционеров Общества начиная с 2025 года. Критерий 2 соблюдается частично. В отчетном периоде Общество не проводило Общих собраний акционеров Общества в форме совместного присутствия. В связи с этим при проведении Общих собраний акционеров Общества практика участия в Общем собрании акционеров Общества кандидатов в органы управления и контроля Общества не применялась. 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. Критерий 3 соблюдается частично. В отчетном периоде Общество не проводило Общих собраний акционеров Общества в форме совместного присутствия. В связи с этим при проведении Общих собраний акционеров Общества практика участия в них Генерального директора Общества, Главного бухгалтера Общества, членов 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 применять практику участия в Общих собраниях акционеров Общества Генерального директора Общества и топ-менеджмента Общества начиная с 2025 года. 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	

№	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
1.2.4	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	
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 сфере 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 намеренно внедрить практику отчетов Генерального директора Общества Совету директоров Общества о выполнении стратегии Общества, когда это будет соответствовать масштабам и целям деятельности Общества

№	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
2.1.2	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	Частично соблюдается	Критерий 1. Частично соблюдается. В течение отчетного периода на заседанях Совета директоров Общества были рассмотрены вопросы, связанные с утверждением годового бюджета Общества, а также отдельные вопросы, касающиеся стратегии Общества в отдельных направлениях его деятельности. Совет директоров Общества не утверждал стратегию Общества в виде отдельного документа. Такое решение вызвано высокой скоростью изменения внешней среды в сфере информационных технологий основной сфере 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 намеренно внедрить практику утвреждения стратегии Общества в качестве отдельного документа, когда это будет соответствовать масштабам и целям деятельности Общества
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	Частично соблюдается	Критерий 1 соблюдается. Критерий 2 пока не соблюдается. В отчетном периоде Совет директоров Общества не пересматривал приемлемую величину рисков Общества. Совет директоров Общества определяет и утверждает перспективные задачи и цели Общества, а также методы их достижения 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, при утверждении бюджета Общества на очередной год, а также при принятии решения о выплате дивидендов. Промежуточные критерии и показатели исполнения перспективных задач и целей Общества анализируются при рассмотрении вопроса о рекомендации Общему собранию акционеров Общества размера дивиденда по акциям за три и девять месяцев отчетного года. При рассмотрении указанных вопросов Совет директоров Общества учитывает допустимые риски Общества. В отчентном году служба внутреннего контроля и управления рисками Общества внедрила систему управления рисками Общества на основе недопустимых событий («НС»). В 2025 году Советом директоров будет рассмотрен отчет службы внутреннего аудита и службы внутреннего контроля и управления рисками за 2024 год и рекомендации Комитета по аудиту Совета директоров Общества по развитию системы внутреннего аудита. На основании этого отчета Обществом будут сделаны выводы о необходимости пересмотра приемлемой величины рисков Общества

№	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
2.1.4	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	
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 к торгам 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 лица, ответственного за надлежащую организацию и эффективное функционирование системы раскрытия Обществом информации, а также за обеспечение доступа акционеров к информации Общества. Общество планирует разработать информационную политику Общества в качестве единого формализованного документа в среднесрочной перспективе
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	

№	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
2.2	**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 во втором квартале отчетного года. 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	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
2.3.2	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. Общество планирует возобновить практику предоставления акционерам подробной информации о кандидатах в члены Совета директоров Общества после возобновления практики раскрытия информации о членах 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	

№	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
2.4.2	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 14.05.2024. 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 Общества и Совета 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 Московской бирже. 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	
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	

№	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
2.5	**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	

№	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
2.6.4	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	
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	

№	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
2.7.3	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	
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 2024 году заседания проводились реже одного раза в квартал. Общество будет применять практику ежеквартального созыва Комитета по аудиту Совета директоров Общества в случае, если такая необходимость будет обнаружена членами Совета директоров Общества, в том числе в ходе самооценки его деятельности, и (или) если возникнут вопросы, которые необходимо рассмотреть на заседании

№	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
2.8.2	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
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	

№	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
2.8.4	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	
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

№	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
2.9	**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. По итогам отчетного года была проведена самооценка работы Совета директоров Общества. Такая самооценка включала оценку работы комитетов и Совета директоров Общества в целом. Индивидуальная оценка каждого члена Совета директоров Общества в отчетном году не проводилась. Общество планирует рассмотреть вопрос о включении в процедуру самооценки индивидуальной оценки каждого члена Совета директоров Общества в среднесрочной перспективе. 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 не соблюдается. Общество осуществило публичное размещение ценных бумаг на Московской бирже 17.12.2021. В настоящее время Совет директоров проводит самооценку работы Совета директоров Общества. Практику проведения независимой оценки качества работы Совета директоров Общества планируется внедрить 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	

№	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
4.1.2	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 вознаграждения, наиболее адекватно отвечающую стратегическим целям Общества. Топ-менеджмент Общества проводит публичные обсуждения такой системы вознаграждения 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 ее (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	

№	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
4.2.2	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 отсутствует отдельный внутренний документ, предусматривающий предоставление акций 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	Частично соблюдается	Критерий 1 частично соблюдается. Общество не внедряло программу долгосрочной мотивации для членов исполнительных органов и иных ключевых руководящих работников Общества с использованием акций Общества. При этом в Обществе внедрена программа стимулирования роста капитализации Общества. Такая программа предусматривает возможность, в том числе, предоставления акций Общества контрибьюторам, которые внесли вклад в рост стоимости программных продуктов Группы и/или рыночной капитализации Общества. Контрибьюторами могут быть любые лица. Программа предусматривает, что с отдельными контрибьюторами могут быть заключены соглашения, предусматривающие мораторий на последующую продажу контрибьютором полученных акций в течение ограниченного срока (локап)

№	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
4.3.3	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	
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	

№	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
5.1.3	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 внутреннего аудита в состав Годового отчета Общества в среднесрочной перспективе

№	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	**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	
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	

№	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	**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 Общества, находится в процессе разработки. После завершения разработки соответствующей политики планируется, что Совет директоров периодически будет оценивать ее актуальность
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

№	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	**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 текущих 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 рассматривали 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, в связи с положениями 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	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	**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	
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	

№	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
7.1.3	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 не соблюдается. В течение отчетного периода Обществом были совершены существенные корпоративные действия до завершения процедуры одобрения их осуществления. Совершение таких действий объясняется необходимостью быстрого реагирования на меняющиеся условия в высококонкурентной среде. Информация о таких действиях раскрывается в соответствии с правилами, установленными действующим законодательством, в том числе когда это требуется, направляется акционерам при подготовке к годовому Общему собранию акционеров Общества. В случае совершения Обществом существенных корпоративных действий до завершения процедуры их осуществления Общество проводит процедуру последующего одобрения таких действий. При этом в вопросах соблюдения процедуры одобрения существенных корпоративных действий Общество строго соблюдает действующее законодательство
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 топ-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 членаСовета 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

8.4

Отчет о совершенных (заключенных) крупных сделках[1]

В течение отчетного периода Обществом не совершались крупные сделки.

[1] Утвержден в составе Годового отчета ПАО «Группа Позитив» за 2024 год, утвержденного решением Совета директоров ПАО «Группа Позитив» 7 апреля 2025 года (протокол от 7 апреля 2025 года № 38).

8.5

Отчет о совершенных (заключенных) сделках, в совершении которых имеется заинтересованность[1]

[1] Утвержден в составе Годового отчета ПАО «Группа Позитив» за 2024 год, утвержденного решением Совета директоров ПАО «Группа Позитив» 7 апреля 2025 года (протокол от 7 апреля 2025 года № 38).

Сделка	Стороны сделки	Существенные условия сделки	Заинтересованные лица
Договор займа № 1 от 17.07.2024	(Сведения не раскрываются на основании Постановлений Правительства РФ от 04.07.2023 №1102, от 28.09.2023 №1587)	**Сумма займа:** 5 000 000 000 (пять миллиардов) рублей. **Срок займа:** 3 (три) года с даты выдачи займа, возврат суммы займа осуществляется в соответствии с графиком погашения задолженности (приложение к договору). **Процентная ставка:** заем является процентным. За пользование займом Заемщик обязуется уплатить в пользу Займодавца проценты в размере ключевой ставки Банка России, действующей в период действия договора, увеличенной на 1,8% (одна целая восемь десятых процента) годовых. Ключевая ставка определяется в соответствии с данными, размещенными на официальном сайте Центрального банка Российской Федерации. В случае изменения ключевой ставки Банка России новый расчет процентной ставки по договору вступает в силу в соответствующую дату вступления в силу новой ключевой ставки Банка России (при этом за периоды, предшествующие периоду, когда действует новая процентная ставка, проценты начисляются по ранее действовавшим ставкам, применимым в соответствующих периодах). Проценты по займу выплачиваются ежемесячно. **Условия предоставления суммы займа:** предоставление суммы займа осуществляется Займодавцем в течение 2 (двух) рабочих дней с даты подписания договора займа. **Условия досрочного возврата суммы займа:** Заемщик вправе в любой момент досрочно вернуть сумму займа, полученную по сделке, полностью или в части, без каких-либо штрафов или аналогичных сборов. **Целевое использование займа:** заем может быть использован Заемщиком для любых целей	(Сведения не раскрываются на основании Постановлений Правительства РФ от 04.07.2023 №1102, от 28.09.2023 №1587)

Сделка	Стороны сделки	Существенные условия сделки	Заинтересованные лица
Договор займа № 2 от 27.12.2024	(Сведения не раскрываются на основании Постановлений Правительства РФ от 04.07.2023 №1102, от 28.09.2023 №1587)	**Предмет сделки:** Займодавец обязуется предоставить Заемщику денежные средства (заем), а Заемщик обязуется возвратить Займодавцу заем в соответствии с условиями договора займа. **Сумма займа:** 4 800 000 000 (четыре миллиарда восемьсот миллионов) рублей. **Срок займа:** заем предоставляется Заемщику на срок до 26.12.2026. **Процентная ставка:** заем является процентным. За пользование займом Заемщик обязуется уплатить в пользу Займодавца проценты в размере ключевой ставки Банка России, действующей в период действия договора, увеличенной на 4% (четыре процента) годовых. В случае изменения ключевой ставки Банка России новый расчет процентной ставки по договору вступает в силу на 7-й (седьмой) календарный день с даты вступления в силу новой ключевой ставки Банка России (при этом за периоды, предшествующие периоду, когда действует новая процентная ставка, проценты начисляются по ранее действовавшим ставкам, применимым в соответствующих периодах). Ключевая ставка определяется в соответствии с данными, размещенными на официальном сайте Центрального банка Российской Федерации (http://www.cbr.ru/). Проценты по займу выплачиваются ежемесячно в соответствии с графиком, изложенным в Приложении № 1 к Договору займа. **Условия предоставления суммы займа:** предоставление суммы займа осуществляется Займодавцем в течение 2 (двух) рабочих дней с даты подписания договора займа. **Условия досрочного возврата суммы займа:** Заемщик вправе в любой момент досрочно вернуть сумму займа, полученную по сделке, полностью или в части, без каких-либо штрафов или аналогичных сборов. Согласие Займодавца на досрочный возврат суммы займа полностью или по частям не требуется. **Целевое использование займа:** заем может быть использован Заемщиком для любых целей	(Сведения не раскрываются на основании Постановлений Правительства РФ от 04.07.2023 №1102, от 28.09.2023 №1587)

8.6

Раскрытие корпоративной информации

Раскрытие информации на сайте ПАО «Группа Позитив»

Страница Компании на сайте «Интерфакс-ЦРКИ»

8.7

Контакты

Публичное акционерное общество «Группа Позитив»

ИНН 7718668887
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.: 8 (800) 500-31-44
Email: shareholder@ptsecurity.com

Юрий Мариничев,
директор по связям с инвесторами
Тел.: +7 (985) 761-84-63
Email: ymarinichev@ptsecurity.com

Ольга Терентьева,
Корпоративный секретарь
Email: corporatesecretary@ptsecurity.com