positive technologies

A**********t 2021

Запомнить меня

pt

POSI

Наша основная задача

— предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу, отраслям и целым государствам

ПОЗИТИВ
ПЕРВОЕ ХАЙТЕК-РАЗМЕЩЕНИЕ
ПЕРВОЕ ПРЯМОЕ РАЗМЕЩЕНИЕ
ПЕРВАЯ КИБЕРБЕЗ-КОМПАНИЯ
НА МОСКОВСКОЙ БИРЖЕ

group.ptsecurity.com

Интерактивная версия отчета Positive Technologies — 2021

Содержание

Мы — Positive Technologies

эмитент ПАО «Группа Позитив»

Positive Technologies — ведущий разработчик продуктов и решений для информационной безопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям. Positive Technologies — первая и единственная публичная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

>1200
человек в команде

20
лет на рынке

>2300
компаний нам доверяют

15
продуктов и решений

80%
крупнейших компаний России — участников рейтинга «Эксперт-400» — наши клиенты

Читайте подробнее о наших продуктах и сервисах на с. 28

RAEX ЭКСПЕРТ РА

ruA-
с позитивным прогнозом
наш кредитный рейтинг от «Эксперт РА»

О нас
Видео

От первого лица

Мы — бесспорный визионер рынка кибербезопасности в России

Кибербезопасность: новые принципы для изменившегося мира

Сегодня российские компании подвергаются беспрецедентному количеству кибератак. Потребность в результативной безопасности сейчас велика как никогда: компании нацелены на получение гарантий невозможности атак с недопустимыми последствиями. Это, в совокупности с массовым уходом зарубежных вендоров, формирует огромный потенциал для роста отечественного рынка кибербезопасности в целом и Positive Technologies в частности.

Денис Баранов,
Генеральный директор
Positive Technologies

Выполнение стратегических целей

В рамках стратегии 2019–2021 годов мы ставили перед собой амбициозные задачи и выполнили их.

Бизнес-стратегия

Удвоение объема продаж каждые 2 года

2021

8 млрд руб.

2020

6 млрд руб.

2019

4 млрд руб.

Подробная информация на сайте

Публичная стратегия

Мы на бирже

Для Positive Technologies **выход на Московскую биржу** — точка синхронизации для всех технологических и бизнес-планов

Positive Technologies — **первая и единственная кибербез-компания на Московской бирже**

Мы — **пионеры прямого листинга**[1]

1391 акционер перед выходом на биржу

>44 тыс. акционеров на середину апреля 2022 года

[1] Прямой листинг (DPO) — это процесс выхода компании на биржу, при котором продаются не новые акции, а уже существующие бумаги акционеров.

Технологическая стратегия

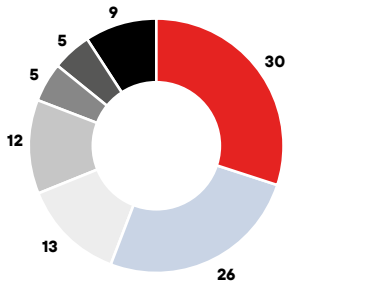
Результативная кибербезопасность

- **Результативная кибербезопасность** — ключевой элемент цифровизации
- **Неизбежная эволюция индустрии ИБ** — автоматизация кибербезопасности и решение задач ИБ одним человеком
- **Недопустимые события на уровне компании**, отрасли и государства должны быть невозможны
- **Технологическая линейка Positive Technologies** — фундамент концепции метапродуктов, практического воплощения идеи результативной кибербезопасности

Наши клиенты

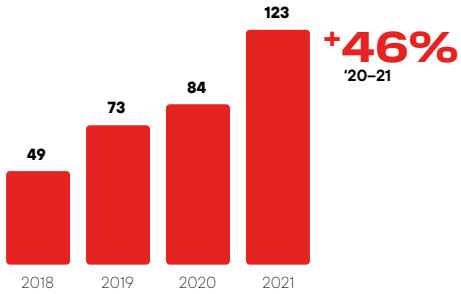
Нашим ключевым сегментом являются крупные корпоративные клиенты.

Распределение клиентов по отраслям в 2021 году, %



- ТЭК
- Государственные структуры
- Банковский сектор
- Промышленность
- Связь и коммуникации
- Информационные услуги
- Остальное

Количество крупных корпоративных клиентов Positive Technologies



Мы расширяем работу со всеми сегментами нашей клиентской базы, сохраняя при этом фокус на работе с крупным корпоративным бизнесом. В 2021 году доля крупных корпоративных клиентов Компании увеличилась до 74%[1].

Большинство клиентов — российские компании. Это минимизирует зависимость от иностранных партнеров и иностранного капитала.

Подробнее о наших клиентах на с. 29

98%
продаж
на территории России

Крупные корпоративные клиенты Positive Technologies

74% доля продаж

123
клиента

Средние корпоративные клиенты Positive Technologies

25% доля продаж

726
клиентов

Средние и малые корпоративные клиенты Positive Technologies

1% доля продаж

1427
клиентов

Наши клиенты представляют ключевые отрасли экономики.

Мы обеспечивали кибербезопасность ключевых мероприятий, которые проводились в России в минувшее десятилетие

- **2013 год** — Универсиада в Казани
- **2014 год** — зимние Олимпийские игры в Сочи
- **2018 год** — чемпионат мира по футболу
- **2018 год** — выборы Президента Российской Федерации
- **2019 год** — Универсиада в Красноярске
- **2020 год** — общероссийское голосование по вопросу одобрения изменений в Конституцию Российской Федерации
- **2021 год** — выборы в Государственную думу Российской Федерации

[1] Крупные корпоративные клиенты — согласно внутренней сегментации клиенты Компании, годовой бюджет которых на ИБ составляет более 30 млн руб.; средние корпоративные клиенты — бюджет на ИБ от 1 млн до 30 млн руб.; средний и малый бизнес — бюджет на ИБ до 1 млн руб. в год.

Наша продуктовая линейка

Динамика продаж наших наиболее быстрорастущих продуктов в 2021 году

+74%
PT Network Attack Discovery

+46%
MaxPatrol SIEM

+46%
PT Application Inspector

+41%
PT Sandbox

Метапродукты

За 20 лет работы мы выработали визионерский подход к созданию своих решений.

В портфеле Positive Technologies 15 продуктов мирового уровня, которые необходимы для построения практической безопасности. Новый класс решений — метапродукты — это переосмысление подхода к построению кибербезопасности, которое позволит предотвращать хакерские атаки в автоматическом режиме до того, как компании будет нанесен недопустимый ущерб на уровне бизнеса и целых отраслей.

MaxPatrol O2
Метапродукт

MaxPatrol O2 автоматически выявляет и предотвращает атаки до того, как будет нанесен неприемлемый для компании ущерб.

Подробнее о метапродуктах на с. 41

Доли наших продуктов на российском рынке ИБ[1]

60–70%
доля MaxPatrol 8 и MaxPatrol VM в сегменте систем управления уязвимостями

30–40%
доля MaxPatrol SIEM в сегменте SIEM

35–40%
доля PT Application Firewall в сегменте межсетевых экранов уровня веб-приложений

20–30%
доля PT ISIM в сегменте безопасности промышленных сетей

10–20%
доля PT Application Inspector в сегменте сканеров исходного кода

Подробнее о наших продуктах на с. 28

[1] Доля рынка продуктов определена экспертами Компании в ценах конечного заказчика и оценки сегментов рынка ИБ России по данным аналитического портала anti-malware.ru.

Признание в глобальном технологическом сообществе

Наши экспертизу и продукты признают во всем мире

- Positive Technologies трижды становилась визионером в исследовании Gartner Magic Quadrant по системам защиты веб-приложений (WAF).
- В 2021 году аналитическая компания IDC включила Positive Technologies в топ-3 мировых вендоров с наибольшим годовым приростом продаж решений класса SIEM.
- Специалисты Компании участвуют в работе технических комитетов Федерального агентства по техническому регулированию и метрологии (Росстандарта) и рабочих групп Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Центрального банка Российской Федерации (Банка России), общественно-государственного объединения «Ассоциация документальной электросвязи» (АДЭ), Международного совета по большим электрическим системам высокого напряжения — СИГРЭ (Conseil International des Grands Réseaux Electriques, CIGRE) и других организаций, оказывают экспертную помощь в формировании требований безопасности.
- За обнаружение критически опасных уязвимостей специалисты Positive Technologies включены в залы славы таких компаний, как Adobe, Apple, AT&T, PayPal, Google, GitLab, IBM, Microsoft, Mastercard, «Яндекс» и Mail.ru.

Positive Technologies объединяет глобальное технологическое комьюнити

phd Positive Hack Days

Positive Hack Days (PHDays) — это самый крупный форум в России по технологической безопасности. Сплав технологий и новейших исследований от ключевых российских и зарубежных экспертов, бизнес- и инвестиционной повестки, связанной с острыми проблемами обеспечения кибербезопасности компаний, отраслей и даже целых государств, и насыщенной конкурсной программы, во время которой этичные хакеры показывают свои силы и соревнуются.

THE STANDOFF

The Standoff — самая масштабная в мире открытая кибербитва, включающая киберучения. В ходе учений команды этичных хакеров находят уязвимости в корпоративной и промышленной ИТ-инфраструктуре, а специалисты по киберзащите нарабатывают опыт предотвращения недопустимых событий.

Подробнее о Positive Hack Days и The Standoff на с. 59

SecurityLab.ru

Топ-10
самых посещаемых ресурсов для сферы ИТ

>3 млн
просмотров в месяц

>400 тыс.
пользователей

Мы создаем площадки для обмена знаниями и опытом людей, заинтересованных в развитии и защите цифрового мира.

2022 год — время возможностей

В начале 2022 года российский рынок ИБ изменился коренным образом. Кибербезопасность и защита от атак стали потребностью номер один для бизнеса и государства. Иностранные вендоры практически полностью ушли с российского рынка, и отечественным игрокам предстоит их заместить. При этом решение о покупке программного обеспечения (ПО) для кибербезопасности принимают уже не только специалисты по ИТ — такие вопросы перешли на уровень первых лиц компаний.

Сегодня многие иностранные вендоры в одностороннем порядке прекращают поддержку своих систем в России, оставляя клиентов фактически без защиты. Компании понимают риски работы с продуктами зарубежных поставщиков ПО и сами начинают превентивно искать замену среди предложений российских разработчиков. Сейчас мы видим повышенный спрос со стороны крупных клиентов на высокопроизводительные, нагруженные инсталляции с большим количеством узлов, и у нас есть решения, сполна покрывающие их потребности, ведь мы полностью были готовы к суверенному спросу на кибербезопасность с 2021 года.

Как мы росли раньше

- Расширяли продуктовую линейку
- Наращивали объемы продаж ключевых продуктов
- Увеличили клиентскую базу за счет представителей новых отраслей

Как мы будем расти в новой реальности

- Работаем с концепцией результативной безопасности: делаем недопустимые события невозможными
- Запускаем новые решения (PT XDR) и метапродукты (MaxPatrol O2)
- Наращиваем количество продуктов у наших клиентов, наша цель — не менее пяти продуктов у каждого клиента

Подробнее о перспективах рынка кибербезопасности на с. 18

20 лет роста

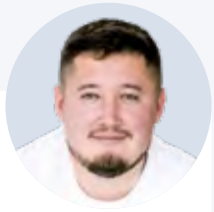
История Positive Technologies — это более 20 лет успешного развития и экспоненциального роста продаж

- 1998 год — Дмитрий Максимов и Евгений Киреев создают сканер уязвимостей XSpider и затем выкладывают его в свободный доступ в сеть.
- 2002 год — начало работы Positive Technologies.
- 2003 год — появляется коммерческая версия XSpider с расширенной функциональностью.
- 2008 год — Компания выпускает универсальное средство автоматизированного анализа защищенности и контроля соответствия стандартам MaxPatrol 8, расширяя пул крупных корпоративных клиентов.
- 2015 год — у Positive Technologies сформирован продуктовый портфель, который позволяет обеспечить защиту от всех распространенных сценариев хакерских атак.
- 2021 год — Компания выходит на Московскую биржу, став пионером прямого листинга в России и единственной публичной компанией на рынке отечественного кибербеза.

Команда профессионалов в ИТ и кибербезопасности

Юрий Максимов
Сооснователь Компании,
Председатель Совета директоров

Максим Пустовой
Операционный директор



Андрей Бершадский
Директор центра компетенции

Владимир Заполянский
Директор по маркетингу и корпоративным коммуникациям

Алла Макарова
Финансовый директор

Максим Филиппов
Директор по развитию бизнеса в России

Борис Симис
Заместитель Генерального директора по развитию бизнеса

Денис Баранов
Генеральный директор

Алексей Андреев
Управляющий директор департамента исследований и разработки

Денис Кораблев
Директор по продуктам

Евгения Гулина
HR-директор

Обращение к инвесторам

«Мы убеждены в том, что рост цифровизации невозможен без активного развития кибербезопасности. И мы видим, что именно недостаточное внимание к обеспечению кибербезопасности — сдерживающий фактор для дальнейшего бума цифровизации.

Юрий Максимов
Председатель Совета директоров Positive Technologies

Обращение сооснователя Компании, Председателя Совета директоров

> Кибербезопасность — это та сфера, где мы очевидно имеем много конкурентных преимуществ, а не догоняем мир.

Уважаемые акционеры, друзья, коллеги!

Мы рады представить вам первый публичный отчет о нашей деятельности в 2021 году. В рамках Отчета мы хотим подвести ключевые итоги года и рассказать о том, как работает, чем живет и куда движется наша Компания. Уверены, что для вас важно понимать, как мы работаем в условиях новой реальности и почему кибербезопасность — потребность первого уровня для всех нас.

Мы убеждены в том, что рост цифровизации невозможен без активного развития кибербезопасности. И мы видим, что именно недостаточное внимание к обеспечению кибербезопасности — сдерживающий фактор для дальнейшего бума цифровизации. Почему мы все не перешли на использование беспилотного транспорта и на улицах по-прежнему встречаются лишь единичные тестовые экземпляры автомобилей без водителей, хотя технологически это давно возможно? В том числе и потому, что велика вероятность, что киберпреступники их взломают и устроят транспортный коллапс с непоправимыми последствиями. Решений, позволяющих обеспечить гарантированную защиту, на рынке недостаточно. И таких примеров, где активное развитие ИБ может стать бустером для цифровизации, масса.

Вторым фактором, который сегодня влияет на переустройство мира, является, конечно же, геополитическая ситуация. Последние месяцы подсветили все слабые места индустрии кибербезопасности в России. В первую очередь, большую зависимость от иностранных компаний — разработчиков и поставщиков ПО. Клиенты, которые делали ставку на них, сегодня лишились возможности обеспечивать защиту своих ИТ-контуров и систем и столкнулись с необходимостью срочно переориентироваться на отечественные продукты и разработки.

Россия стала мишенью номер один для кибератак, которые направлены на самые разные отрасли и компании, от государственных порталов и объектов инфраструктуры до информационных ресурсов и персональных аккаунтов в социальных сетях. Атаки продолжаются по всем направлениям, и здесь максимально важно иметь возможность эффективно им противостоять.

Я уверен, что не только в условиях геополитической турбулентности, но и в дальнейшем отечественные технологии будут занимать в России доминирующую позицию, близкую к 100%. Все возможности и ресурсы для этого у отрасли есть: поддержка со стороны государства, которая выражается в беспрецедентных мерах стимулирования развития нашей отрасли; уникальный практический опыт противодействия хакерским атакам. Мы готовы обеспечить защиту бизнесу, отраслям, государствам — для этого у нас есть все необходимые знания, опыт и технологии.

Безусловно, сейчас наша задача — обеспечить кратно выросший спрос на услуги кибербезопасности в России. Но в то же время в мире быстро растет количество стран, которым принципиально важно иметь цифровой суверенитет. И мы готовы двигаться в этом направлении, помогая обеспечивать независимость и комплексную защиту от киберугроз компаниям и государствам в разных частях света.

Кибербезопасность — это та сфера, где мы очевидно имеем много конкурентных преимуществ, а не догоняем мир. У нас есть лучшие разработчики, лучшие специалисты в области белого хакинга, у нас сформировалась практика постоянной проверки защиты друг друга, построенной на собственных же продуктах силами белых хакеров. В мире так не принято — и это выгодно отличает нас и наш опыт от других.

Изначально мы пришли в бизнес как фанаты своего дела. Сейчас, в ходе подготовки к размещению на бирже, мы окунулись в мир финансов, но, по сути, мы не изменились, мы технари — и живем этим. Мы можем себе позволить не ставить финансовые показатели как самоцель, а продолжать осуществлять нашу мечту, ведь мы делаем, что любим, а это всегда неизбежно приводит к финансовому росту как Компании, так и ее акционеров.

Благодарю вас за оказанное доверие и уверенность в будущем российской отрасли кибербезопасности!

С уважением,
Юрий Максимов
Сооснователь Компании,
Председатель Совета директоров

Обращение к инвесторам

«Прошлый год стал для нас своего рода моментом сборки, который дал нам уверенность в том, что мы можем эффективно работать на нашем рынке, ставить амбициозные стратегические цели и достигать их даже в условиях пандемии, санкций, геополитической турбулентности.

Денис Баранов
Генеральный директор Positive Technologies

Обращение Генерального директора

Уважаемые акционеры и коллеги!

Этим отчетом мы подводим итоги прошлого года и определяем задел на ближайшее будущее. Нам важно, чтобы вы понимали, что и как мы сделали для того, чтобы прийти в ту точку, где находимся сейчас. А главное — чтобы вы знали, к чему мы планируем идти дальше и насколько реализуемы наши планы и идеи.

Прошлый год стал для нас своего рода моментом сборки, который дал нам уверенность в том, что мы можем эффективно работать на нашем рынке, ставить амбициозные стратегические цели и достигать их даже в условиях пандемии, санкций, геополитической турбулентности. В 2021 году мы завершили реализацию нашей трехлетней стратегии, включавшей три главных направления.

Технологии

Мы разработали все технологии, необходимые для защиты компаний в русле концепции результативной кибербезопасности. Сейчас в нашем портфеле порядка 15 продуктов и сервисов, которые в совокупности гарантированно выявляют хакерскую активность до того, как компании будет нанесен недопустимый ущерб. Это стало фундаментом концепции метапродуктов и практической реализации идеи невозможности недопустимых для бизнеса, отрасли или даже государства событий.

Бизнес

Как компания мы перешли к стратегической перспективе при постановке своих финансовых целей, увеличивая продажи в два раза каждые два года — с 2019 по 2021 год рост объема продаж составил 4–6–8 млрд руб.

Публичность

В 2021 году мы прошли точку синхронизации для всех наших планов — и технологических, и бизнесовых — провели размещение на Московской бирже, ориентированное на физических лиц, став первой компанией в отечественной сфере кибербезопасности, акции которой торгуются на бирже. Опыт последних месяцев показал, что наша ставка на частного инвестора и внутренний рынок была единственно верным решением — это позволило нам полностью исключить зависимость от иностранного капитала и существенно повысить надежность наших акций для инвестирования. Сегодня общее число наших инвесторов превышает 44 тыс. Для того чтобы сделать наш бизнес для них максимально прозрачным, мы много усилий прилагаем, делая более понятной для широкого круга инвесторов саму специфику бизнеса в сфере отечественной кибербезопасности, и применяем лучшие мировые практики раскрытия финансовой отчетности.

Обращение Генерального директора

2022-й изменил мир ИТ и ИБ в целом и отношение отдельных компаний к этим направлениям в частности. Низкий уровень защищенности до сих пор был своего рода тормозом на пути развития технологий. Нынешний год в полной мере подсветил все проблемы сложившейся ситуации бизнесу, который осознал, что ИБ — на самом деле один из главных его союзников в развитии. Сегодня российские компании подвергаются беспрецедентному количеству кибератак: хакеры атакуют буквально все — от системообразующих предприятий во всех сегментах экономики до коммерческих компаний, ориентированных на широкий рынок. При этом мы наблюдаем практически полный исход иностранных вендоров из российского сегмента ИБ. В буквальном смысле слова в момент непрекращающихся атак производители ИТ и ряда средств защиты оставили своих клиентов без поддержки и продуктов. На этом фоне кардинально перестраивается весь рынок: запрос на реальный результат и защиту от недопустимых событий актуален в каждом первом случае, а информационная безопасность действительно стала восприниматься как необходимая «оболочка» для любых технологий, гарантирующая работу бизнеса. Все это в совокупности сделало кибербезопасность приоритетом первых лиц компаний и формирует огромный потенциал для роста отечественного рынка кибербезопасности в целом и Positive Technologies в частности.

Мы в полной мере чувствуем эти изменения на себе, потому что находимся в эпицентре событий: нас буквально завалили запросами. Рост запросов на все наши продукты и сервисы обнаружения и отражения хакерских атак в феврале — марте значительно превысил наши ожидания: мы видим, что потребность в результативной безопасности сейчас велика как никогда — компании нацелены на получение гарантий невозможности атак с недопустимыми последствиями. И главная наша задача на данный момент — максимально оперативно удовлетворить возросший спрос и обеспечить надежную защиту нашим клиентам, чьи службы безопасности на практике не справляются с тем шквалом атак, который на них обрушился. Противодействие такому объему атак требует большой и профессиональной команды защиты и реагирования на инциденты. В целом в индустрии общее число таких специалистов сейчас явно недостаточно для защиты всех компаний, которым это требуется. Единственным решением в данной ситуации является создание средств защиты, которые работали бы автоматически, являясь неким автопилотом, работающим без участия человека. Для себя как для вендора мы видим в этом большую стратегическую технологическую задачу — дать рынку этот автопилот, создать метапродукты, ориентированные на обеспечение киберустойчивости организаций. То есть такой инструмент защиты, который позволит с минимальным вовлечением человеческих ресурсов обеспечивать автоматическое решение задач ИБ, ориентированной на гарантированную невозможность недопустимых событий.

С точки зрения бизнесовых задач нашу стратегическую идею можно описать как «постоянное ускорение темпов роста»: если раньше нашим таргетом для самих себя было удвоение бизнеса каждые два года, то теперь мы целимся в ежегодный двукратный рост. С этим показателем неразрывно связана и капитализация Positive Technologies: мы работаем над тем, чтобы капитализация увеличивалась соответственно росту нашего бизнеса.

С уважением,
Денис Баранов
Генеральный директор Positive Technologies

...мы работаем над тем, чтобы капитализация увеличивалась соответственно росту нашего бизнеса.

Борис Симис
Заместитель Генерального директора по развитию бизнеса

Тектонические изменения на российском рынке ИБ

Кибербезопасность обеспечивает защиту ИТ-контура, который включает компьютеры, мобильные устройства, серверы, сети и иные цифровые системы от хакерских атак, несанкционированного доступа и утечек информации.

Цифровизация идет высокими темпами во всем мире, также растет и количество кибератак. Как следствие, увеличиваются расходы на ИБ. Эксперты прогнозируют ежегодный рост глобального рынка кибербезопасности на 15%[1]. По различным данным, российский рынок, который составляет 2–3% от мирового, оценивается в 150 млрд руб. и ежегодно растет в среднем на 20%.

Глобальные затраты на кибербезопасность, трлн долл. США

Конкурентоспособность российских компаний в этой области очень высока. Positive Technologies задает тренды во многих секторах отрасли и определяет вектор развития российского рынка.

Читайте подробнее о наших продуктах и сервисах на с. 28

[1] По данным RiskBased Security.

Кибербезопасность и ее роль в современном мире

Тенденции 2021 года в сфере кибербезопасности

В информационную безопасность приходят управленцы

Отделы информационной безопасности крупных компаний теперь возглавляют менеджеры, которые хорошо знают бизнес и процессы, но не всегда являются экспертами в области ИБ. Государственные компании и крупные корпорации передают ответственность за киберзащиту на уровень топ-менеджеров, теперь это стратегически значимый вопрос, требующий внимания руководителей компаний. Во многих компаниях введена должность ответственного за информационную безопасность (Chief Information Security Officer, CISO) на уровне заместителя генерального директора. В ответ на это мы стремимся создать систему ИБ, понятную любому руководителю или владельцу компании.

> В 2022 году будет запущена программа обучения в сфере кибербезопасности для российских топ-менеджеров на базе школы управления «Сколково» и МТУСИ[1].

Кибербезопасность выходит на биржу

В 2021 году Positive Technologies стала первой компанией из сферы кибербезопасности, которая начала торговаться на Московской бирже. 17 декабря мы разместили акции в режиме прямого листинга. Это знаковое для отрасли событие, которое создает новые возможности для развития и роста конкурентоспособности.

Автоматизация кибербеза

Ключевую роль начинают играть так называемые humanless-технологии защиты, которые требуют вмешательства человека только в критических ситуациях. Сложные продукты, основанные на этих технологиях, позволяют обеспечить результативную кибербезопасность даже в компаниях с минимальным штатом ИТ-экспертов.

Результативная кибербезопасность

Год от года общее число инцидентов растет, атаки усложняются, а их эффективность повышается. Наши новые технологии и продукты ориентированы на идею результативной кибербезопасности, когда защита требует минимум экспертизы и усилий со стороны специалистов, а атаки обнаруживаются автоматически. Оценить результативность можно только путем реального моделирования действий злоумышленников на киберполигонах. В 2021 году мы реализовали более десятка крупных проектов, нацеленных на верификацию событий, которые могут нанести существенный вред компании клиента и являются для нее неприемлемыми.

69%

топ-менеджеров отметили рост киберугроз с начала 2020 по май 2021 года[2]

72%

топ-менеджеров указали, что их компании испытали от 1 до 10 киберинцидентов за год

94%

руководителей намерены продолжать внедрение современных ИТ-решений в своих компаниях

1 Источник: https://www.skolkovo.ru/news/rossijskih-top-menedzherov-nauchat-kiberbezopasnosti/. МТУСИ — Московский технический университет связи и информатики.

2 Источник: исследование Deloitte «Будущее киберпространства в 2021 году», которое проводилось на основе опроса около 600 руководителей высшего звена, занимающихся кибербезопасностью в компаниях с выручкой не менее 500 млн долл. США в год (https://www2.deloitte.com/global/en/pages/risk/articles/future-of-cyber.html).

Рост спроса на bug bounty

Мы считаем, что в 2022 году программы по поиску уязвимостей bug bounty[1] станут более востребованными. Многие российские компании, которые запускали свои программы bug bounty на международных площадках, недавно потеряли к ним доступ. Российские белые хакеры, которые участвовали в подобных программах, осуществляя поиск уязвимостей по заказу зарубежных и российских компаний, теперь не могут на них зарабатывать. Мы готовим площадку для такой программы и планируем запустить ее в 2022 году.

Подробнее об инициативе читайте на сайте

Главные киберугрозы 2021 года

2022

Во время пандемии COVID-19 во всем мире произошел массовый переход к дистанционным технологиям работы, который повлек за собой и рост кибератак. В 2021 году активность злоумышленников продолжала расти.

Увеличение числа атак шифровальщиков[2]

По нашим оценкам, в отчетном году доля атак вирусов-шифровальщиков по отношению ко всем атакам с использованием вредоносного ПО составила около 66%. Чаще всего таким атакам подвергались государственные организации и медицинские учреждения.

Резкий рост онлайн-мошенничества в банковском секторе

От мошенничества с платежными картами и банкоматами злоумышленники перешли к онлайн-мошенничеству — кредитному фроду[3], обходу онлайн-проверок, связанных с технологиями онбординга[4], KYC[5] и противодействия отмыванию средств.

Рост уязвимостей корпоративных сетей

Значительно выросла эксплуатация уязвимостей в корпоративных системах удаленного доступа и решениях аудио- и видеосвязи различных производителей.

Промышленные предприятия чаще подвергались кибератакам

По данным наших аналитиков, в основном это фишинговые рассылки (56%) и хакинг (35%). Доля хакинга в общем количестве атак против промышленных компаний продолжает расти и свидетельствует о низком уровне защищенности предприятий.

Рост числа кибератак с использованием технологий искусственного интеллекта (ИИ)

Были зафиксированы киберпреступления, связанные с технологией deepfake с реалистичной подменой лица и мимики на видео.

Рост интереса хакеров к NFT[6]

1 Программа, с помощью которой пользователи могут получить вознаграждение за нахождение проблем в безопасности сервисов и приложений компании.
2 Вредоносное ПО, которое при проникновении в компьютер шифрует все файлы в ключевых разделах, предлагая затем владельцу заплатить за восстановление доступа к ним.
3 Мошенничество в розничном кредитовании.
4 Процесс привлечения клиента.
5 Процедура идентификации клиента (Know Your Customer, «знай своего клиента»).
6 NFT (от англ. non-fungible token, невзаимозаменяемый токен) — криптографический сертификат цифрового объекта с возможностью передавать сертификат через механизм, применяемый в криптовалютах. Фишинг, направленный на участников процесса покупки или продажи NFT, эксплуатация уязвимостей в смарт-контрактах.

2021

Вызовы в области кибербезопасности 2022 года

Кибербезопасность стала потребностью первого уровня в современных реалиях.

Тренды отрасли в 2022 году

Резко возросшая потребность в цифровом суверенитете стран

Одномоментный уход зарубежных игроков с рынка

Атаки на все отрасли экономики страны

Запрос на кибербезопасность со стороны первых лиц

Запрос на кибербезопасность, ориентированную на результат

Перспективы развития российского рынка кибербезопасности в 2022 году

Российский рынок кибербезопасности стоит на пороге значительных изменений. Иностранные конкуренты покидают рынок, спрос на ИБ постоянно растет, а государство запускает меры поддержки для ИТ-отрасли.

Расширение поддержки ИТ-отрасли государством

В 2020–2021 годах Правительство России приняло значительные меры для стимулирования развития российского ИТ-бизнеса:

- снижение налогов и взносов для ИТ-разработчиков;
- предоставление льготных кредитов и факторинга через уполномоченные банки по ставке от 1 до 5% годовых;
- государственные гранты для ИТ-компаний и стартапов;
- освобождение от НДС операций по реализации прав на использование программных продуктов, которые включены в Единый реестр российского программного обеспечения (ЕРРП);
- упрощение правил предоставления субсидий на НИОКР для ИТ-продукции.

В конце марта 2022 года были приняты новые меры для поддержки ИТ-сектора:

- освобождение ИТ-компаний от налога на прибыль и проверок до 2024 года;
- снижение ставки по льготным кредитам до 3%;
- увеличение сумм грантов;
- отсрочка от службы в армии для сотрудников ИТ-компаний;
- предоставление льготной ипотеки сотрудникам ИТ-компаний;
- согласно Указу Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», госорганам, госкомпаниям и стратегическим предприятиям с 1 января 2025 года запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении России недружественные действия.

В дополнение к этому рассматривается вопрос об упрощении процедур закупок ИТ-продуктов для государственных нужд и стимулировании закупок государственными организациями отечественного ПО.

> **«Мир меняется. В прошлом году мы оценивали рынок кибербезопасности России в 150 млрд руб.**
>
> К концу 2021 года он вырос, по нашей оценке, на 20–25% и составил 190–200 млрд руб. Высвобождаемый рынок за счет ухода западных вендоров я оцениваю в объеме порядка 80 млрд руб., и две трети из них — лицензии, подлежащие, по сути, замене на российские аналоги. Сегодня многие спорят, вырастет рынок или нет. Сейчас вызов не в росте рынка, а в том, чтобы заместить эти 80 млрд руб. на отечественные решения, сделать это качественно, профессионально.
>
> **Максим Филиппов,**
> директор по развитию бизнеса в России и странах СНГ

Новые вызовы

В начале 2022 года мы столкнулись с новой реальностью. Ситуация в экономике в целом и на рынке кибербезопасности в частности резко изменилась в связи с геополитическими событиями. Мы увидели резкий рост кибератак на российские компании и государственные учреждения и массовый уход с нашего рынка иностранных производителей. Кибербезопасность и импортозамещение стали критически важными вопросами в нашей стране.

Для нашей Компании это новый вызов — мы делаем все, чтобы удовлетворить резко выросший спрос на продукты и услуги в нашей отрасли. В I квартале 2022 года наши продажи выросли втрое по сравнению с аналогичным периодом 2021 года. По оценкам Positive Technologies, с уходом западных вендоров объем освободившегося рынка составит около 80 млрд руб.

Наша Компания готова обеспечивать клиентам результативную безопасность. Особую уверенность в этом нам дают метапродукты, которым мы предрекаем большой успех на рынке. Все решения, которые были выпущены нами ранее, были разработаны с прицелом на то, что они дополнят будущие метапродукты и в их составе будут работать как сенсоры, которые автоматически блокируют и устраняют последствия хакерских атак.

Планы Positive Technologies включают:

- **быстрый рост бизнеса в России** на основе предложения клиентам продуктов и решений, обеспечивающих результативную и практическую безопасность. Мы строим ИБ на уровне корпоративных клиентов и масштабируем этот подход на уровне отраслей и страны;
- **работу с международными клиентами,** заинтересованными в построении цифрового суверенитета.

Наша задача в ближайшие месяцы и годы — ответить на новые вызовы и сделать рывок вперед на рынке России и в международном масштабе. Цифровой мир находится на пороге значительных изменений, и мы готовы к этим переменам.

> **Мы хотим конкурировать с сильнейшими компаниями мира, чтобы делать лучшие продукты. У нас есть амбиции выходить на международный рынок.**
>
> **Максим Пустовой,**
> операционный директор

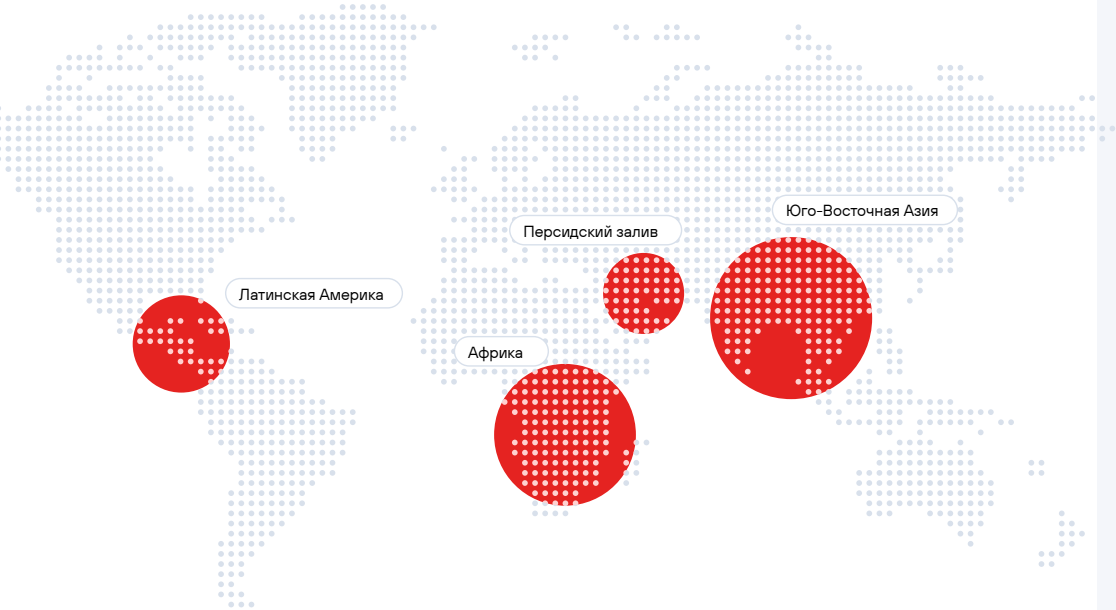
≈80 млрд руб.
высвобождаемый объем рынка (в том числе сервисы)

190–200 млрд руб.
общий объем рынка

Новые вызовы

Международные продажи — новые возможности

Количество стран, нуждающихся в цифровом суверенитете, продолжает увеличиваться на фоне геополитической напряженности и роста числа глобальных киберугроз, и мы готовы им помочь. Интерес к российским разработкам растет в странах Персидского залива, Юго-Восточной Азии, Латинской Америки и Африки.



Усиление конкуренции среди российских компаний и передел рынка

Часть западных вендоров уже покинула российский рынок или приостановила работу на рынке России, и их продукты перестали работать. В связи с этим многие российские компании пересмотрели свою политику в сторону замещения западных продуктов российскими. Широта нашей продуктовой линейки и качество продуктов готовы стать достойной заменой зарубежным альтернативам.

Разработка продуктов, обеспечивающих практическую защиту от кибератак

Клиенты будут стремиться получить реальную практическую безопасность своих информационных сетей. Мы реагируем на их запросы с помощью настройки существующих продуктов и решений и запуска метапродуктов, применение которых гарантирует защиту от наступления недопустимых для клиента событий.

Курс на импортозамещение

Новые возможности на российском рынке в связи с уходом иностранных вендоров на фоне усиления кибератак на российские корпорации и государственные учреждения.

В течение нескольких лет компании приходили к идее реальной защиты ключевой инфраструктуры, а импортозамещение становилось все более важным фактором выбора поставщиков. В 2022 году ситуация достигла апогея в связи с изменениями международной обстановки.

Весной 2022 года западные вендоры начали массово уходить с нашего рынка. Российские компании, которые приобрели иностранное программное обеспечение, столкнулись с отзывом разрешений на использование этого ПО. Те российские предприятия, у которых лицензии на иностранное ПО еще действуют, тревожатся о том, что их могут отозвать в любой момент. Программно-аппаратные комплексы иностранных производителей тоже могут лишиться поддержки.

Согласно нашим данным[1], 72% партнеров нашей Компании озабочены отсутствием аппаратных платформ для решений в области кибербезопасности.

Информационная безопасность — одна из немногих отраслей, в которой возможно полное или практически полное импортозамещение. По нашим оценкам, рост рынка в 2022 году может превысить 20%.

У нас есть многолетний опыт киберзащиты российских компаний, холдинговых структур, компаний с государственным участием, министерств и ведомств.

К 2022 году мы подошли с полной готовностью заместить западные продукты и решения на российском рынке.

[1] Согласно результатам опроса клиентов Компании.

Геополитические изменения и санкции не оказывают влияния на наш бизнес

- Наши решения высокоэффективны, надежны, отличаются высокой конкурентоспособностью, их доля на рынке растет
- Мы полностью независимы от импортных компонентов
- У нас нет зависимости от валютной выручки

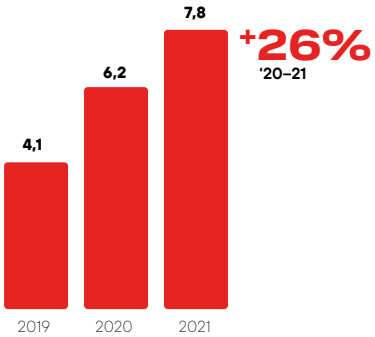
98%
наших доходов
мы получаем внутри страны и в странах СНГ

- Positive Technologies — привлекательный и ответственный работодатель
- Мы — единственная публичная компания из отрасли на российском рынке, число наших инвесторов растет
- Мы не зависим от зарубежного капитала

Выполнение стратегии 2019–2021 годов

Отчетный год был для нас особенным. Мы успешно выполнили все планы, заданные стратегией на период с 2019 по 2021 год, которая предусматривала удвоение бизнеса каждые два года, а конкретно — рост продаж с 4 млрд до 8 млрд руб.

Динамика продаж за 2019–2021 годы, млрд руб.



Выполнение целевых показателей 2021 года

Показатель	Целевой показатель 2021 года	Фактическое выполнение показателя в 2021 году
Количество крупных корпоративных клиентов	100–120	123
Среднее количество продуктов на одного крупного корпоративного клиента	3	3
Доля крупных клиентов, использующих три и более продукта, %	50	49
Продажи[1], млрд руб.	7,5–8	7,8
Выручка, млрд руб.	7–7,5	7,1
Валовая рентабельность, %	85–89	88
EBITDA скорр.[2], млрд руб.	2,5–2,7	2,9
Рентабельность EBITDA скорр., %	35–38	41
Чистая прибыль, млрд руб.	1,5–1,7	1,9
Рентабельность по чистой прибыли, %	20–25	27

[1] Показатель «Объем продаж» означает валовый объем законтрактованных поставок лицензий, оборудования, товаров и услуг в адрес дистрибьютора или конечного покупателя за отчетный период и включает НДС. Данный показатель является управленческой метрикой и определяется как «Выручка за отчетный период с учетом НДС» + «Обязательства по договорам с покупателями на конец отчетного года с учетом НДС» — «Обязательства по договорам с покупателями на начало отчетного периода с учетом НДС».

[2] Не учитывает разовые расходы, связанные с листингом ценных бумаг, в размере 227 млн руб.

Наши цели и планы →

Выполнение целей трехлетней стратегии

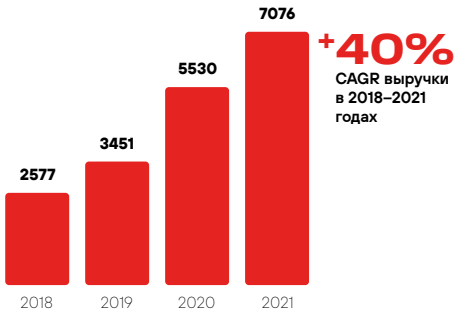
Наша трехлетняя стратегия продаж успешно реализована. В ее рамках мы ставили цель на рост продаж с 2019 по 2021 год в объеме 4–6–8 млрд руб.

Рост внимания к проблемам кибербезопасности и уход с российского рынка западных вендоров открывают перед нами новые возможности для ускоренного роста.

Подробнее о финансовых результатах на с. 70

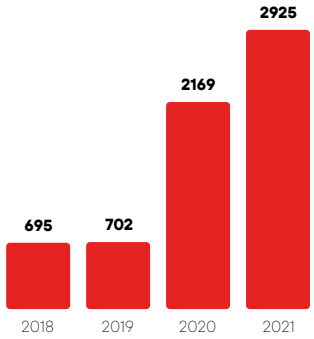
2021

Выручка, млн руб.



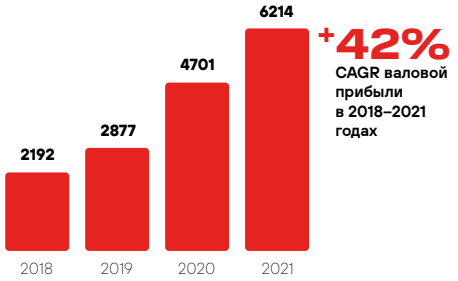
+40%
CAGR выручки в 2018–2021 годах

EBITDA скорр., млн руб.



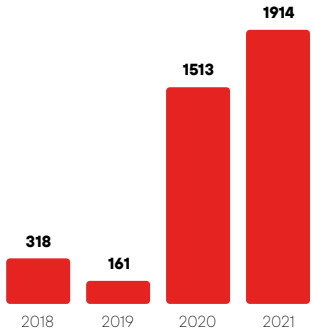
+61%
CAGR EBITDA в 2018–2021 годах

Валовая прибыль, млн руб.



+42%
CAGR валовой прибыли в 2018–2021 годах

Чистая прибыль, млн руб.



+82%
CAGR чистой прибыли в 2018–2021 годах

Наши сотрудники — совладельцы Компании

Перед выходом на биржу Компания вознаградила акциями нынешних и некоторых бывших сотрудников, которые внесли существенный вклад в развитие Positive Technologies. Всего акции в качестве вознаграждения получили около 1,4 тыс. совладельцев.

в 31 раз
выросло число наших акционеров с начала торгов (до 44 тыс.[1])

6,4 млрд руб.
объем торгов акциями Компании за период с 17.12.2021 по 30.04.2022

Модель, при которой почти все сотрудники являются совладельцами Компании, — одна из основ нашей корпоративной культуры.

Подробнее о нашей концепции совладения на с. 48

[1] По данным на апрель 2022 года.

Стратегия роста

Мы движемся вперед в позитивное и высокотехнологичное будущее: делаем мир безопаснее, производим продукты, которые полностью покрывают запросы клиента.

Наши цели

2x
удвоение объема продаж каждый год

2x
рост бизнеса темпами, вдвое превышающими рост рынка

50%+
увеличение доли Компании на рынке до более половины адресуемого рынка

90%
крупнейших компаний России
(из рейтинга «Эксперт РА»)
расширение клиентской базы

в 5–10 раз
увеличение выручки от международных продаж. Выход на рынки Азии, Южной Америки, Ближнего и Среднего Востока

100+
тыс. российских инвесторов
станут нашими акционерами

рост капитализации пропорционально объемам роста бизнеса

обеспечение автоматической защиты от хакеров при помощи метапродуктов

абсолютное лидерство в отдельных категориях продуктов, добавление новых продуктов в линейку

Стратегические целевые показатели на 2022 год

Показатель	Фактическое выполнение показателя в 2021 году	Целевой показатель 2022 года
Продажи[1], млрд руб.	7,8	12–15
Выручка, млрд руб.	7,1	11–14
Валовая рентабельность, %	88	88–90
EBITDA скорр.[2], млрд руб.	2,9	4–6
Рентабельность EBITDA скорр., %	41	40–45
Чистая прибыль, млрд руб.	1,9	3–5
Рентабельность по чистой прибыли, %	27	30–35

Мы достигли наших стратегических целей 2021 года. Часть результатов, например размер чистой прибыли или количество крупных корпоративных клиентов, были выше целевых показателей.

> Добившись таких успехов, мы строим амбициозные планы на будущее. Наша цель — продолжать удваивать наши продажи и расширять бизнес.

1 Показатель «Объем продаж» означает валовый объем законтрактованных поставок лицензий, оборудования, товаров и услуг в адрес дистрибьютора или конечного покупателя за отчетный период и включает НДС. Данный показатель является управленческой метрикой и определяется как «Выручка за отчетный период с учетом НДС» + «Обязательства по договорам с покупателями на конец отчетного года с учетом НДС» — «Обязательства по договорам с покупателями на начало отчетного периода с учетом НДС».

2 Не учитывает разовые расходы, связанные с листингом ценных бумаг, в размере 227 млн руб.

Наши принципы и подходы

Принцип открытости информации и знаний

Мы считаем, что открытость знаний поможет компаниям находить эффективные решения в сфере кибербезопасности и привлекать новые таланты в этой области.

Принцип ответственного разглашения

При исследовании систем на наличие уязвимостей мы всегда сообщаем производителю о найденных уязвимостях, методах обнаружения и использованных инструментах.

Практический подход к кибербезопасности

Мы не просто выполняем стандартные процедуры, а обеспечиваем реальную защиту, отражая хакерские атаки.

В 2020 году наша Компания отказалась от устаревшего подхода, при котором система информационной защиты выявляет инциденты и сообщает о них, а клиент постоянно повышает уровень защиты и нанимает новых сотрудников в отдел ИБ. Мы выбрали подход результативной кибербезопасности.

Результативная кибербезопасность как подход

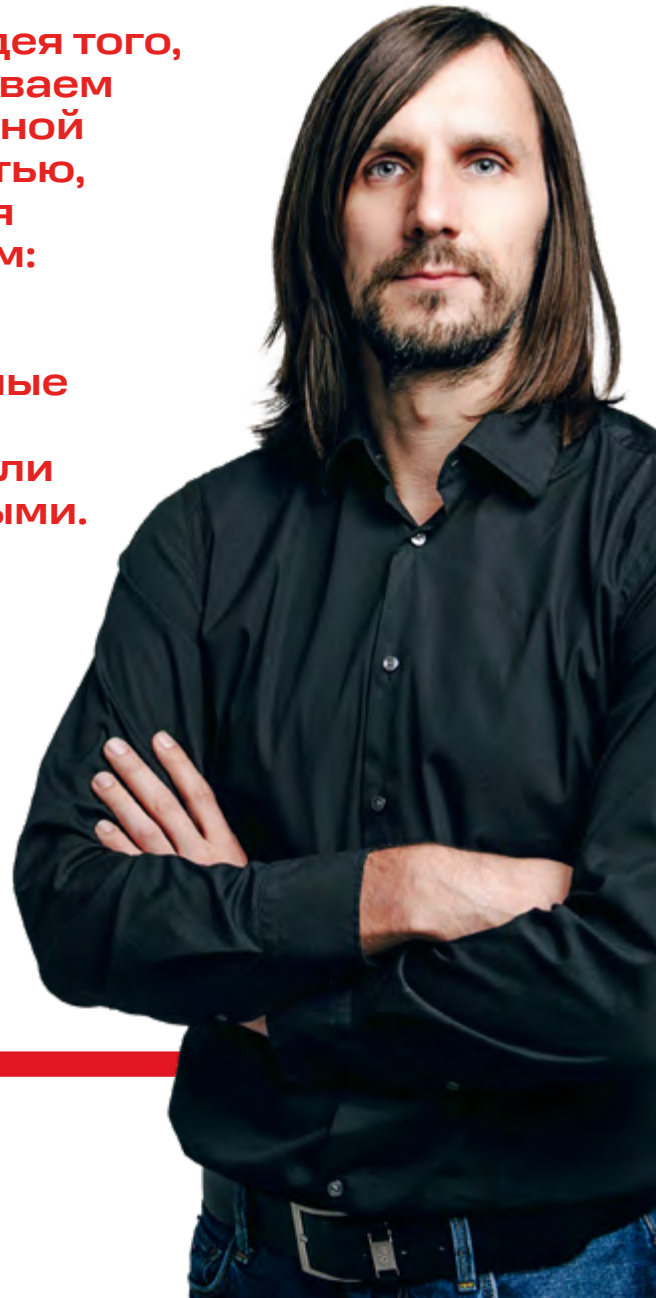
Клиент определяет список недопустимых для бизнеса событий, критически опасных для процессов его компании. С учетом этого знания разрабатывается и устанавливается система защиты. Защищенность информационных систем проверяется с помощью киберучений.

Наши продукты и технологии ориентированы на идею результативной информационной безопасности, когда защита требует минимума экспертизы и усилий специалистов, а кибератаки обнаруживаются автоматически с измеримым эффектом

Мы трансформируем кибербезопасность через подход, ориентированный на результат. Теперь наша технологическая линейка позволяет автоматически обнаружить и остановить хакера до нанесения непоправимого ущерба клиенту.

«Основная идея того, что мы называем результативной безопасностью, заключается в следующем: поставьте цель, чтобы неприемлемые для вас события стали невозможными.

Денис Баранов,
Генеральный директор
Positive Technologies



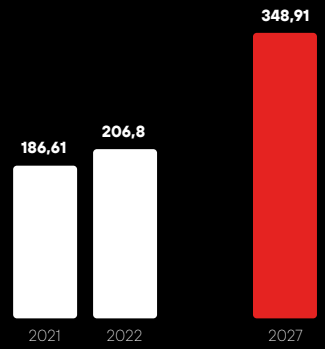
Максим Филиппов
Директор по развитию бизнеса в России

Потенциал российских разработок ИБ на рынке России

Мы уверены, что индустрия ИБ должна перестать быть сдерживающим фактором для развития других отраслей.

Автоматизация кибербезопасности — неизбежная эволюция индустрии ИБ. Сейчас как в России, так и за ее пределами качество и экспертиза российской кибербезопасности говорят сами за себя — мы стали известными на внешнем рынке. Стремительно увеличивающийся глобальный запрос на суверенную кибербезопасность открывает большие возможности в рамках потенциального экспорта и выхода на иностранные рынки.

Объем мирового рынка кибербезопасности[1], млрд долл. США



10,99%

прогнозируемый CAGR совокупного объема мирового рынка кибербезопасности в 2021–2027 годах

[1] По данным исследования ResearchAndMarkets.com https://www.businesswire.com/news/home/20220427005820/en/.

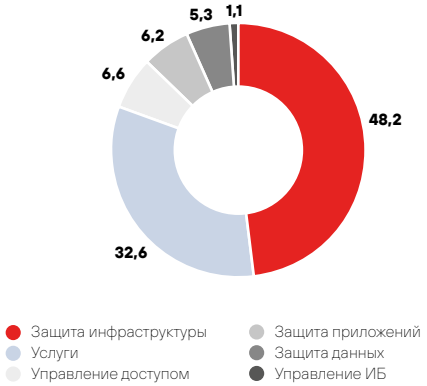
Сегментация российского рынка ИБ

Российский рынок информационной безопасности в 2020 году

По оценке портала Anti-Malware.ru[1], суммарный объем российского рынка ИБ по итогам 2020 года составляет 142,6 млрд руб.

Positive Technologies оценивает объем адресуемого Компании рынка суммой 60–80 млрд руб. Лидерами российского рынка ИБ являются такие сегменты, как защита инфраструктуры, сервисы безопасности и средства управления доступом. В каждом из этих сегментов есть явно доминирующее направление, обеспечивающее ему передовые позиции: для сервисов это внедрение, для защиты инфраструктуры — сетевая безопасность, а для контроля доступа — средства и системы аутентификации. Устойчивое промежуточное положение занимают средства обеспечения персональной кибербезопасности. Перспективными с точки зрения наращивания долей рынка представляются программные комплексы облачной безопасности, управления рисками, управления безопасностью, безопасности приложений. Можно ожидать, что их востребованность будет расти по мере того, как все большее количество заказчиков будут приходить к активному использованию облачных технологий, мобильных и веб-приложений. Распространенность удаленной работы должна способствовать и росту популярности средств контроля доступа, в том числе для привилегированных пользователей.

Доли основных сегментов российского рынка ИБ в 2020 году, %



Суммарный объем рынка ИБ в 2020 году

142 600
млн руб.

[1] Источник – исследование портала Anti-Malware.ru (https://www.anti-malware.ru/analytics/Market_Analysis/Russian-InfoSec-Market).

Объем российского рынка ИБ по сегментам в 2020 году

Доля 48,2%
68 700
млн руб.
защита инфраструктуры

Доля 32,6%
46 500
млн руб.
услуги ИБ

Доля 6,6%
9400
млн руб.
управление доступом

Доля 6,2%
8900
млн руб.
защита приложений

Доля 5,3%
7600
млн руб.
защита данных

Доля 1,1%
1500
млн руб.
управление ИБ

Прогноз развития российского рынка ИБ

Согласно прогнозу портала Anti-Malware.ru, объем российского рынка ИБ имеет хороший потенциал роста и в среднем **будет увеличиваться на 16–20% в год** до 2023 года.

Высокие темпы будут связаны в первую очередь с низкой насыщенностью и зрелостью рынка. По развитию многих сегментов отечественный рынок ИБ пока отстает от западного (при более высоком уровне внедрения и применения ИТ). Ключевым фактором будет служить необходимость выполнения нормативных требований регуляторов, в первую очередь по цифровизации, защите критической информационной инфраструктуры и импортозамещению. Стремясь выполнить эти требования, бизнес будет закупать и внедрять все больше отечественных или локализованных зарубежных продуктов, включая аппаратные решения российского производства. В коммерческом секторе наиболее заметно в течение ближайших лет будет расти сегмент защиты приложений.

Алексей Андреев
Управляющий директор

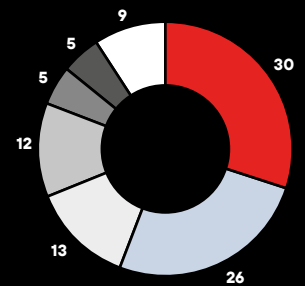
Продукты, решения, сервисы

«Мы работаем с более чем 2300 клиентами, в числе которых крупные компании, финансовые организации, государственные учреждения, промышленные и сервисные компании.

У нас диверсифицированный портфель. Нет такого клиента, уход которого может повлиять на стабильность и устойчивость нашего бизнеса, на наши доходы. ТЭК — 30%; государственные компании — на втором месте, 26%; на третьем — все, что связано с финансами.

Алексей Андреев
Управляющий директор департамента исследований и разработки

Наши клиенты представляют ключевые отрасли экономики



- ТЭК
- Государственные структуры
- Банковская деятельность
- Промышленность
- Связь и коммуникации
- Информационные услуги
- Остальное

80%

российских компаний, включенных в рейтинг «Эксперт-400», пользуются продуктами и услугами Positive Technologies

Продукты Positive Technologies обеспечивают защиту от хакерских атак для предприятия любой отрасли. Наши специалисты — эксперты мирового уровня в вопросах защиты SCADA- и ERP-систем в крупнейших компаниях, а также мобильных и веб-приложений.

Динамика продаж наших продуктов в 2021 году

+74%
PT Network Attack Discovery

+46%
MaxPatrol SIEM

+46%
PT Application Inspector

+41%
PT Sandbox

Наши продукты можно использовать по отдельности, а в совокупности они становятся технологическим фундаментом концептуально нового подхода к защите информационных систем наших клиентов — метаплатформы. Это позволяет в автоматическом режиме выявлять и блокировать действия хакеров.

Доли наших продуктов на российском рынке ИБ

60–70%
доля MaxPatrol 8 и MaxPatrol VM в сегменте систем управления уязвимостями

30–40%
доля MaxPatrol SIEM в сегменте SIEM

35–40%
доля PT Application Firewall в сегменте межсетевых экранов уровня веб-приложений

20–30%
доля PT ISIM в сегменте безопасности промышленных сетей

10–20%
доля PT Application Inspector в сегменте сканеров исходного кода

«На сегодняшний день у нашей Компании 15 продуктов, и в сегменте крупных корпоративных клиентов мы растем.

Каковы наши основные драйверы роста «внутри» клиента? Это, во-первых, увеличение инсталляционной базы одного продукта. И второе, что не менее важно: когда мы продаем тот или иной продукт, мы бьемся за результат, стремимся сделать недопустимые события невозможными. Однозначно никакой одной технологией эту задачу решить нельзя, и мы много вкладываем в то, чтобы продукты Компании работали в симбиозе. Покупая второй и последующие продукты Positive Technologies, клиент получает понятную добавочную ценность по сравнению с использованием этих продуктов в отдельности. Поэтому количество клиентов «внутри» одного заказчика — это для нас немаловажный показатель.

Максим Филиппов,
директор по развитию бизнеса в России

Продукты

Подробнее на с. 31

Наши продукты де-факто являются стандартом по ряду технологических направлений, соответствуют российским и международным стандартам безопасности[1] и признаны глобальными аналитическими агентствами, включая KuppingerCole Analysts AG, Gartner Magic Quadrant и IDC.

[1] В том числе PCI DSS и РС БР ИББС-2,6-2014, приказам ФСТЭК № 17 и 21.

XSpider
Быстрое обнаружение уязвимостей

MaxPatrol 8
Контроль защищенности и соответствие стандартам

MaxPatrol VM
Управление уязвимостями

PT Application Firewall
Безопасность веб-приложений

PT XDR

PT Application Inspector
Анализ защищенности кода веб-приложений

MaxPatrol SIEM
Мониторинг событий ИБ

ПТ Ведомственный центр
Управление инцидентами и взаимодействие с ГосСОПКА

PT Industrial Security Incident Manager
Непрерывная защита АСУ ТП

Построение центра ГосСОПКА

PT Network Attack Discovery
Глубокий анализ сетевого трафика

PT MultiScanner
Многоуровневая защита от вирусных угроз

PT Sandbox
Защита от целевых и массовых атак с применением вредоносного ПО

PT Anti-APT

Подробнее на с. 42

метапродукты

Компания развивает портфель уникальных программных продуктов и систему новых метапродуктов для создания полностью автоматической многоуровневой защиты.

MaxPatrol O2
Автопилот в мире кибербезопасности

Сервисы

Подробнее на с. 40

Наши специалисты знают, как защитить информационные активы клиентов наиболее эффективно и с учетом лучших мировых практик.

Непрерывный анализ защищенности бизнеса

Исследование угроз и уязвимостей аппаратных решений

Расширенная техническая поддержка

Услуги PT Expert Security Center

Уже 20 лет наша основная задача — обнаруживать и останавливать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям.

Решения

Подробнее на с. 39

Наши решения обеспечивают максимальный уровень защищенности и соответствия российским и международным стандартам безопасности.

продукт

MaxPatrol 8

— контроль защищенности и соответствия стандартам

MaxPatrol 8 используется для оценки защищенности информационных систем. Он дает возможность определить, насколько процессы ИБ эффективны, а также обеспечивает их соответствие стандартам и требованиям в этой области.

MaxPatrol 8 располагает мощными механизмами оценки уровня безопасности:

- тестирование на проникновение (PenTest);
- системные проверки (Audit);
- контроль соответствия стандартам (Compliance).

Возможности продукта

- Проводит инвентаризацию информационных ресурсов компании.
- Выявляет уязвимости и ошибки конфигурирования.
- Оценивает соответствие информационных систем требованиям стандартов ИБ и внутренним политикам компании.
- Снижает затраты на аудит и контроль защищенности, сокращает нагрузку на подразделения ИТ и ИБ за счет автоматизации ряда процессов ИБ.

Как работает продукт

Архитектура продукта обеспечивает гибкое масштабирование и позволяет внедрять систему в компаниях любого размера. MaxPatrol 8 можно адаптировать к своей инфраструктуре — выбрать количество серверов, сканеров, установить режимы сканирования.

Как работает продукт
Видео

продукт

MaxPatrol VM

— управление уязвимостями

MaxPatrol VM позволяет выстроить полный цикл управления уязвимостями: от сбора информации об ИТ-активах, выявления и приоритизации уязвимостей по уровню их опасности до контроля их устранения. Система снижает нагрузку на подразделения ИТ и ИБ, автоматизируя большинство рутинных процессов, и повышает эффективность мероприятий по защите. Команда наших экспертов регулярно поставляет информацию о самых опасных трендовых уязвимостях — тех, что нужно устранить в первую очередь.

Возможности продукта

- Помогает выстроить эффективный процесс управления уязвимостями.
- Собирает, обновляет и хранит полную информацию об ИТ-инфраструктуре.
- Выявляет и приоритизирует уязвимости.
- Оперативно выявляет новые опасные уязвимости.
- Позволяет контролировать устранение уязвимостей и отслеживать общее состояние защищенности компании.
- Помогает выстроить эффективное взаимодействие отделов ИТ и ИБ компании в части работы с уязвимостями.

60–70%

доля MaxPatrol VM и MaxPatrol 8 на российском рынке в сегменте управления уязвимостями

Как работает продукт
Видео

продукт

PT Application Firewall

— безопасность веб-приложений

Для защиты компаний от внешних атак мы разработали межсетевой экран уровня веб-приложений PT Application Firewall. Наш продукт позволяет клиентам поддерживать непрерывность бизнес-процессов, снижать риски утечки информации, а также соблюдать требования PCI DSS и других стандартов информационной безопасности.

Возможности продукта

- Блокирует кибератаки, включая атаки L7 DDoS[1] и атаки нулевого дня[2].
- Защищает от угроз из списков OWASP Top 10 и WASC[3].
- Легко устанавливается и быстро встраивается в инфраструктуру[4].
- Адаптируется к защищаемым приложениям.
- Легко интегрируется с продуктами Positive Technologies и другими решениями в области ИБ.

35–40%

доля продукта на российском рынке в сегменте WAF[5]

Как работает продукт
Видео

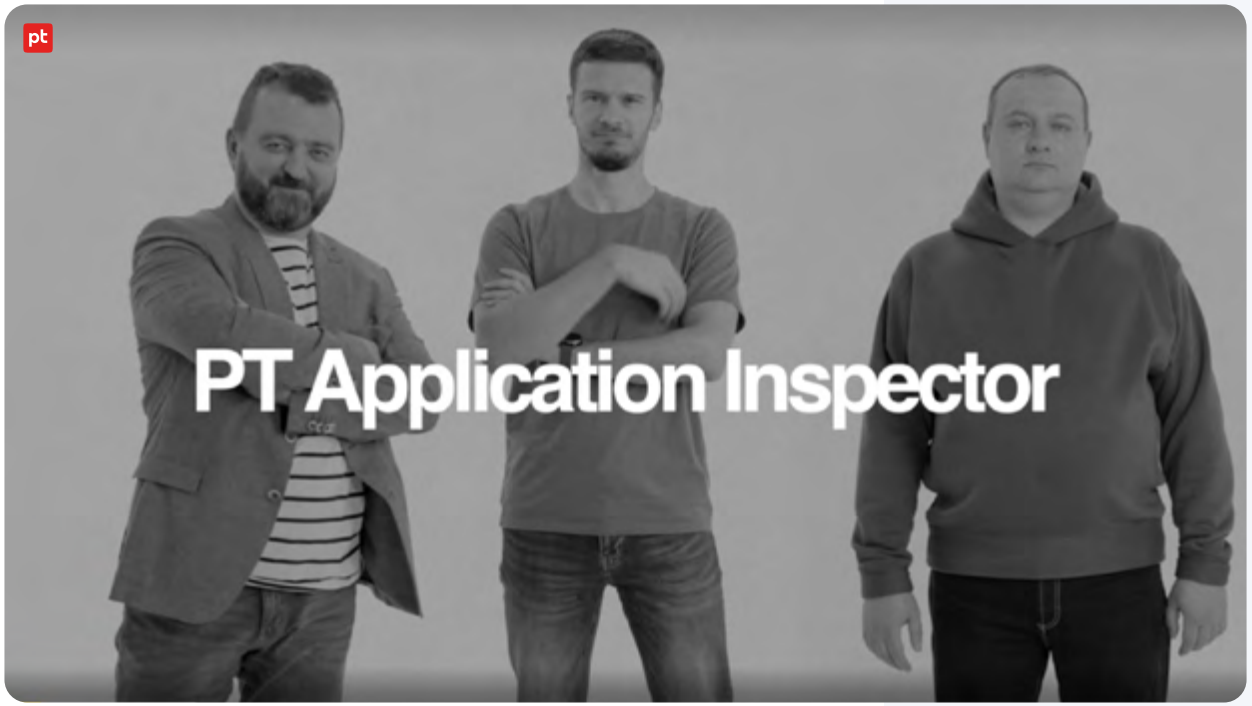
1 Атака, нацеленная непосредственно на приложения, которые работают на сервере.
2 Атака, использующая уязвимость нулевого дня, — уязвимость, о которой еще не знают разработчик, производители антивирусов и пользователи.
3 Отчет об уязвимостях, выпускаемый Open Web Application Security Project (OWASP), открытым проектом по обеспечению безопасности приложений.
4 Классификация угроз в веб-приложениях от Web Application Security Consortium, организации, объединяющей экспертов в области безопасности веб-приложений.
5 Web application firewall — межсетевой экран уровня веб-приложений.

продукт

PT Application Inspector

— анализ защищенности кода веб-приложений

Еще один продукт для защиты приложений клиентов: инструмент для выявления уязвимостей и ошибок в приложениях PT Application Inspector позволяет специалистам по ИБ выявлять и подтверждать уязвимости в исходном коде, а разработчикам — ускорить исправление кода на ранних стадиях разработки. Принцип работы продукта основан на сочетании статического (SAST), динамического (DAST), интерактивного (IAST) методов и анализа сторонних компонентов (SCA).



Возможности продукта

- Точно выявляет и автоматически подтверждает уязвимости приложения.
- Помогает устранять уязвимости на стадии разработки.
- Поддерживает современные методологии разработки (DevSecOps).
- Гибко интегрируется в процесс разработки кода.

10–20%

доля продукта на российском рынке в сегменте сканеров исходного кода

Как работает продукт
Видео

продукт

MaxPatrol SIEM

— мониторинг событий ИБ

MaxPatrol SIEM[1] — система выявления инцидентов ИБ в реальном времени. Она постоянно пополняется знаниями экспертов о способах обнаружения актуальных угроз и адаптируется к изменениям в защищаемой сети. Этот продукт — один из лидеров на российском рынке SIEM.

Возможности продукта

- Знает все об ИТ-инфраструктуре компании, контролирует актуальность данных о ней.
- Регулярно получает свежие экспертные знания для выявления актуальных угроз.
- Отслеживает состояние ИБ в крупных иерархических инфраструктурах.
- Позволяет создавать собственные правила корреляции с помощью гибкого конструктора.
- Контролирует работу источников событий ИБ.
- Оценивает уровень защищенности организации и эффективность процессов ИБ.
- Позволяет сотрудникам центров реагирования на киберугрозы (SOC, security operations center) проводить ретроспективный анализ атак.

30–40%

доля продукта на российском рынке SIEM

Как работает продукт
Видео

[1] SIEM (security information and event management) — анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений, позволяющий реагировать на них до наступления существенного ущерба.

продукт

PT Industrial Security Incident Manager

— непрерывная защита АСУ ТП

Для анализа технологического трафика мы разработали профессиональный продукт класса промышленных NTA/NDR[1] под названием PT Industrial Security Incident Manager (PT ISIM). Это система, которая обеспечивает защиту автоматизированных систем управления технологическим процессом (АСУ ТП) предприятий.

Возможности продукта

- Позволяет находить следы нарушений ИБ в сетях АСУ ТП.
- Выявляет кибератаки, активность вредоносного ПО, неавторизованные действия персонала на ранней стадии.
- Обнаруживает горизонтальное перемещение хакеров в инфраструктуре.
- Осуществляет автоматический ретроспективный анализ трафика.
- Автоматически строит граф развития атаки.
- Обеспечивает соответствие требованиям законодательства.

20–30%

доля продукта на российском рынке в сегменте безопасности промышленных сетей

Как работает продукт
Видео

[1] Система анализа трафика (network traffic analysis / network detection & response).

продукт

PT Network Attack Discovery

— глубокий анализ сетевого трафика

Для выявления атак и их расследования на периметре и внутри сети мы разработали продукт PT Network Attack Discovery. Благодаря ему наши клиенты могут видеть, что происходит в их сетях, определять активность злоумышленников даже в зашифрованном трафике, анализировать атаки и проводить расследования инцидентов.

Возможности продукта

- Информирует об инцидентах и автоматически назначает им уровень опасности.
- Выдает детальную информацию об атаке для правильного реагирования.
- Собирает информацию об угрозах в единой ленте.
- Контролирует происходящее на сетевых узлах.
- Обнаруживает горизонтальное перемещение хакеров в инфраструктуре.
- Осуществляет автоматический ретроспективный анализ трафика.
- Фильтрует сессии с целью поиска вредоносной активности, ошибок конфигурации или индикаторов компрометации.

Как работает продукт

PT Network Attack Discovery захватывает и разбирает сетевой трафик на периметре и в инфраструктуре. Это позволяет выявлять активность злоумышленника и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети.

Как работает продукт
Видео

продукт

PT Sandbox

— защита от целевых и массовых атак с применением вредоносного ПО[1]

Злоумышленники постоянно развивают вредоносное ПО так, чтобы его не обнаруживали обычные средства защиты: антивирусы, межсетевые экраны, IPS[2], почтовые и веб-шлюзы. Для обнаружения продвинутого инструментария атакующих мы разработали PT Sandbox. Это песочница, которая запускает объект (файл или ссылку) в изолированной виртуальной среде, анализирует его действия, определяет, опасен ли он, и блокирует угрозу в случае необходимости.

Как работает продукт
Видео

Возможности продукта

- **Проводит комплексную проверку каждого объекта** — статический и динамический анализ с помощью уникальных правил PT Expert Security Center (PT ESC), а также проверку антивирусами. Правила PT ESC создаются экспертами по итогам расследований инцидентов в реальных компаниях и в ходе исследования деятельности хакерских группировок.
- **Позволяет гибко настраивать виртуальные среды** для анализа и добавлять в них специфическое ПО, которое используется в компании и может стать точкой входа для злоумышленников.
- **Позволяет безопасно провоцировать хакера на активные действия** и выявлять их с помощью приманок в виртуальных средах. Файлы-приманки содержат поддельные учетные записи, файлы конфигурации или другие ценные данные. Процессы-приманки имитируют работу банковского ПО, софта разработчиков, активность пользователей. Продукт выявляет попытки похитить подобные данные или внедриться в процессы.

1 Целевая атака — любое нападение киберпреступников на выбранную ими цель, например, на конкретную компанию, отрасль или группу лиц. Массовая атака — атака с помощью вирусов или других вредоносных программ, направленная на общедоступные цели, в частности на индивидуальных пользователей.
2 Intrusion Prevention System, IPS — система предотвращения вторжений.

решение

PT XDR

— обнаружение и блокирование угрозы в экосистеме одного вендора

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

Как работает продукт
Видео

Возможности решения

- Объединяет все события и контекст из множества систем ИБ, верифицирует сработки и подтверждает факт атаки.
- Автоматически предлагает варианты реагирования на угрозы, проводит лечение заражений, позволяет восстановить работоспособность систем, пострадавших от атаки.
- Снижает требования к ресурсам и компетенциям SOC-команды.

Сервисы

Наши специалисты знают, как защитить информационные активы клиентов наиболее эффективно и с учетом лучших мировых практик.

Непрерывный анализ защищенности бизнеса

Эксперты Positive Technologies помогут своевременно выявить векторы атак на компанию клиента и усовершенствовать стратегию реагирования на инциденты.

- **Pentest 365:** в течение года наши эксперты непрерывно анализируют внешний периметр компании клиента и выявляют слабые места в системе.
- **Эмуляция APT:** в течение трех месяцев наши специалисты имитируют возможные действия злоумышленников, пытаясь получить доступ к важным системам клиента, и выявляют критически опасные бреши в защите.
- **Red team vs blue team:** наши эксперты ведут работы по тестированию на проникновение и имитируют действия хакеров, а специалисты PT Expert Security Center помогают службе ИБ клиента в реагировании на возникающие при этом угрозы.

Исследование угроз и уязвимостей аппаратных решений

Аппаратные уязвимости могут быть использованы для целевых атак и промышленного шпионажа. Мы проводим исследования угроз и уязвимостей аппаратных платформ наших клиентов и предоставляем им рекомендации по предотвращению возможных атак.

Данная услуга включает:

- анализ оборудования на наличие уязвимостей, известных векторов атак и архитектурных ошибок;
- исследование потенциально опасных функциональных возможностей оборудования;
- обнаружение использования стороннего уязвимого ПО и бэкдоров;
- взаимодействие с производителями оборудования для устранения уязвимостей и угроз;
- поддержку и рекомендации в случае выхода обновлений и новых версий прошивок.

Расширенная техническая поддержка

Услуга расширенной технической поддержки включает установку и настройку продуктов Positive Technologies, аудит состояния систем и ПО, а также быстрое реагирование на обращения клиентов.

Услуги PT Expert Security Center

Наш экспертный центр безопасности PT Expert Security Center помогает клиентам обнаруживать, расследовать инциденты ИБ и реагировать на них. Наши специалисты знают, какая хакерская группировка стоит за конкретной атакой. Мы делимся с клиентами способами самостоятельной верификации инцидентов и даем рекомендации для устранения последствий атак.

Подробнее о PT ESC на с. 58

Метапродукты

Концепция результативной кибербезопасности подразумевает, что недопустимые для компании события попросту не происходят. Чтобы масштабировать такой подход на отрасли и государство целиком, кадрами не обойтись — нужны технологии.

MaxPatrol O2 выполняет роль центра мониторинга в компании любого масштаба, работая 24/7. А чтобы управлять им, достаточно одного человека.

Positive Technologies создает метапродукты, которые позволят преодолеть зависимость от экспертов и автоматизировать интеллектуальные и операционные функции службы кибербезопасности. В любых компаниях по всему миру.

Этот подход изменит индустрию и радикально повысит защищенность компаний, а через них — отраслей и государств.

Компания развивает портфель уникальных программных продуктов и систему новых метапродуктов для создания полностью автоматической многоуровневой защиты.

Метапродукты

- **Анализ рисков и угроз**
- **Предотвращение атаки (MaxPatrol O2)**
- **Обеспечение безопасности (Compliance)**
- **Автоматизация безопасности («Оркестратор»)**

2. Остановить атаку

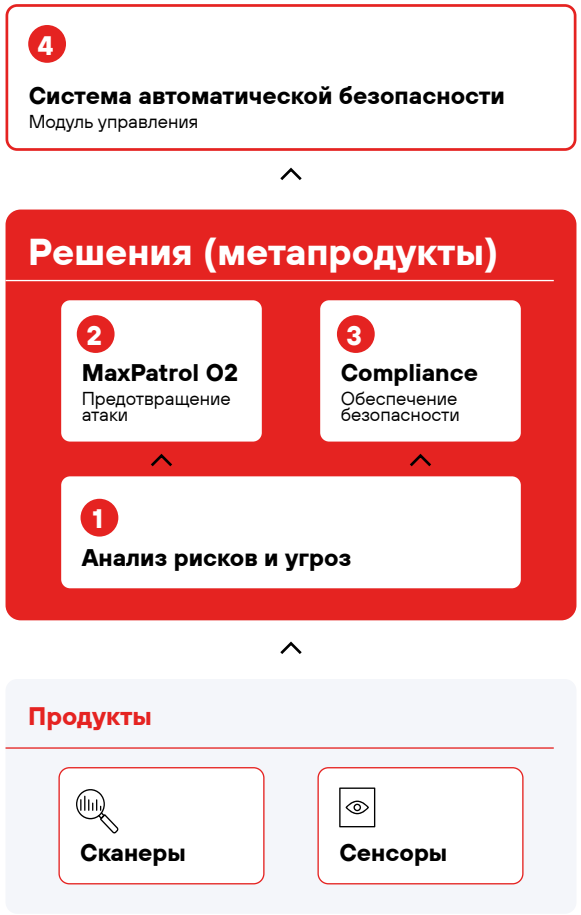
Метапродукт MaxPatrol O2 позволяет автоматически обнаружить и остановить злоумышленника до того, как будет нанесен неприемлемый для компании ущерб.

1. Анализировать угрозы и риски

Динамическое определение векторов атак и возможностей злоумышленника путем объединения и анализа разнородных данных от множества сенсоров и элементов инфраструктуры.

Продукты-сканеры

- **MaxPatrol 8**
- **MaxPatrol VM**
- **PT Application Firewall**
- **PT Application Inspector**



4. Автоматизировать защищенность

Четвертый метапродукт осуществляет автоматическую оркестрацию защитной инфраструктуры для поддержания ее в готовом к отражению хакерских атак состоянии

3. Поддерживать защищенность

Третий метапродукт, Compliance, контролирует защищенность ИТ-инфраструктуры и бизнес-процессов от кибератак. Формирует рекомендации по обеспечению и поддержанию уровня ИБ, обеспечивающего исключение недопустимых событий.

Продукты-сенсоры

- **MaxPatrol SIEM**
- **PT Network Attack Discovery**
- **PT MultiScanner**
- **PT Sandbox**

метапродукты

MaxPatrol O2

— автопилот в мире кибербезопасности

MaxPatrol O2 — наш первый метапродукт, в названии которого отражается его функция — обнаружить и остановить хакера.

Продукты Positive Technologies играют роль сенсоров, которые знают обо всем, что происходит в ИТ-инфраструктуре предприятия, тогда как MaxPatrol O2 анализирует полученные от них данные. В момент атаки он определяет точку, где хакер пытается проникнуть в систему, прогнозирует цели атаки и количество шагов до недопустимого события. В отличие от самого квалифицированного эксперта, MaxPatrol O2 делает это за секунды — и тут же останавливает хакера.

MaxPatrol O2 способен заменить центр мониторинга в компании любого масштаба, работая 24/7. А чтобы управлять им, достаточно одного человека.

Как работает продукт
Видео

Максим Пустовой
Операционный директор

Инвестиционная привлекательность

Наши цели

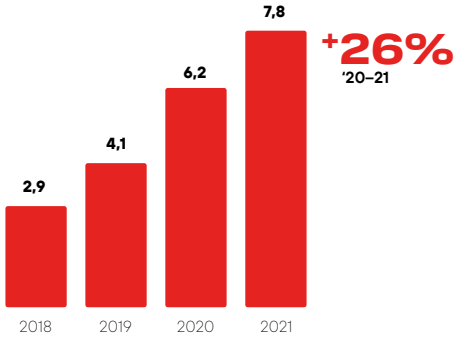
- Увеличение числа акционеров до **100 тыс.**
- **Рост ликвидности** и увеличение объемов торгов
- **Развитие каналов** коммуникаций с инвесторами
- **Запуск мобильного приложения** для совладельцев
- **Раскрытие информации** и финансовой отчетности на ежеквартальной основе
- **Выплата дивидендов** в соответствии с дивидендной политикой
- Увеличение объема **free-float**

Почему наши акции растут

Рост продаж и клиентской базы

Наши продажи растут: в 2021 году их объем вырос на 26% к 2020 году. Число крупных клиентов увеличилось на 46%, а среднее количество проданных продуктов на одного клиента выросло до трех. Клиенты нашей Компании работают в ключевых отраслях экономики (ТЭК, финансы, телекоммуникации и другие), кроме того, среди них немало государственных организаций. По нашим расчетам, интерес этих групп клиентов к нашим продуктам и услугам в ближайшее время повысится.

Рост продаж Positive Technologies, млрд руб.



Рост продаж продуктов Компании в 2021 году

+74%

PT Network Attack Discovery

+46%

MaxPatrol SIEM

+46%

PT Application Inspector

+41%

PT Sandbox

По итогам 2021 года все ключевые продукты Positive Technologies продемонстрировали рост продаж. Мы прогнозируем, что спрос на наши продукты станет еще выше в связи с уходом зарубежных компаний с российского ИТ-рынка.

POSI — акции роста

Акции Positive Technologies вошли в тройку лидеров роста 28–29 марта 2022 года после возобновления торгов на Московской бирже, показав рост на 96% за два дня.

- Рост количества кибератак стимулирует потребность в ИБ. Кибербезопасность становится потребностью первого уровня, на которой не экономят.
- Уход с российского рынка зарубежных вендоров открывает новые перспективы развития перед российскими игроками.
- Positive Technologies — единственная публичная компания на российском рынке ИБ.
- Бизнес Positive Technologies быстро и стабильно растет. Наши акции на Московской бирже, отражая динамику развития Компании, привлекательны для долгосрочных инвестиций.

Дивидендная политика

В отличие от многих технологических компаний роста, мы утвердили дивидендную политику и приступили к ее реализации.

≥50%

чистой прибыли по МСФО

мы планируем выплачивать акционерам

При этом возможен и более высокий коэффициент дивидендных выплат, до 100% от чистой прибыли по МСФО.

Государственная поддержка ИТ-отрасли

Positive Technologies входит в топ-10 разработчиков российского ПО[1]. Российские ИТ-компании пользуются государственными льготами. Эти преимущества позволят нам развиваться еще быстрее.

Льготы для ИТ-компаний в России

0%

налог на прибыль до 2024 года

7,6%[2]

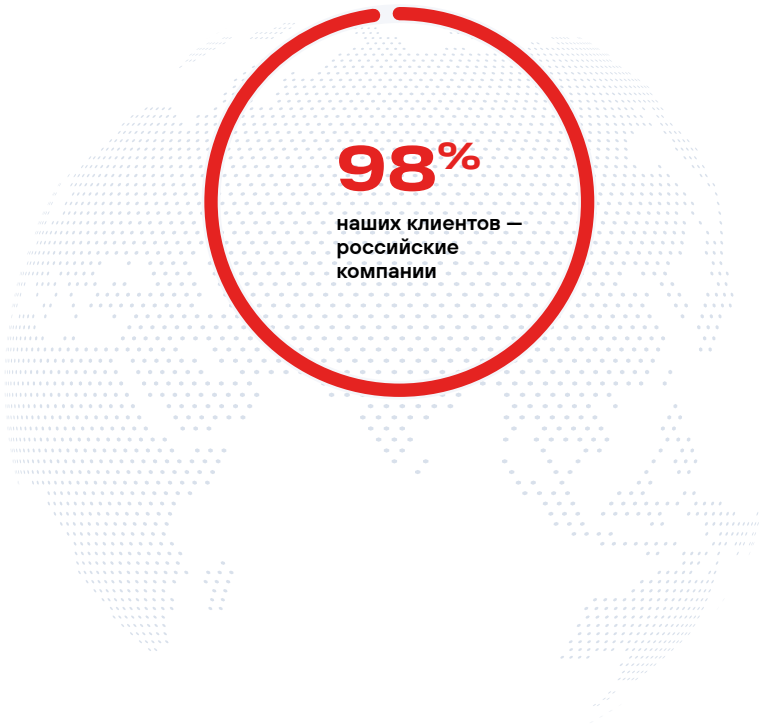
страховые взносы за сотрудников

3%

ставка по кредитам

Меньшая зависимость от геополитической обстановки

Наша Компания в основном работает на внутреннем рынке, 98% наших клиентов — российские компании. В 2021 году мы работали над выстраиванием логистических цепочек и бизнес-процессов таким образом, чтобы не зависеть от импортных компонентов. Теперь мы готовы заменить иностранных вендоров, которые покидают российский рынок.



Первая публичная компания в России из сегмента кибербезопасности

В декабре 2021 года наша Компания стала первой публичной компанией в своем секторе, разместив акции на Московской бирже в режиме прямого листинга. В составе акционеров Компании преимущественно розничные инвесторы. Мы ведем активные коммуникации с нашими инвесторами и стремимся к высокому уровню прозрачности.

6,4
млрд руб.

объем торгов акциями Компании с момента выхода на биржу по 30 апреля 2022 года

1391
инвестор

в день начала торгов

>44
тыс. инвесторов

в апреле 2022 года

1 Данные RAEX (https://raex-a.ru/rankingtable/it/2019/tab2).
2 Общая ставка тарифа без льгот для других компаний составляет 30%.

Больше чем акционер. IR-практики Positive Technologies

Акционерный капитал

Positive Technologies, эмитент ПАО «Группа Позитив», стала первой в России публичной кибербез-компанией и пионером выхода на Московскую биржу в формате прямого листинга (MOEX: POSI). Владельцами значительной части акций Positive Technologies, то есть совладельцами Компании, является большая доля его сотрудников — от топ-менеджмента до линейного персонала. Вместе с тем акции Positive Technologies представляют большой интерес для широкого круга инвесторов.

17 декабря 2021 года на Московской бирже начались торги акциями Компании под тикером POSI. Positive Technologies стала первой и единственной компанией из отрасли кибербезопасности на Московской бирже. Размещению предшествовало дробление акций, которое было произведено с целью возможности привлечения большего числа инвесторов и вознаграждения сотрудников Компании ее акциями. При этом дополнительная эмиссия акций не осуществлялась. Размещение было осуществлено в формате прямого листинга: перед началом торгов часть акций в качестве вознаграждения была передана ключевыми собственниками Компании всем ее действующим и некоторым бывшим сотрудникам, которые внесли значительный вклад в развитие бизнеса Компании и ее продуктов. В результате перед выходом на биржу миноритарными акционерами стали 1,4 тыс. действующих и бывших сотрудников.

За 10 торговых сессий на бирже с 17 по 31 декабря 2021 года количество миноритарных акционеров увеличилось на 10 тыс. и на конец года превысило 11,5 тыс. инвесторов. В 2022 году сохраняются высокие темпы роста количества акционеров. По состоянию на 31 марта 2022 года наш акционерный капитал составлял:

- 60 млн обыкновенных акций;
- 6 млн привилегированных акций.

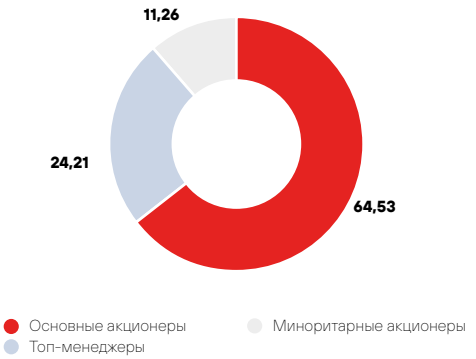
У трех мажоритарных акционеров сосредоточено 64,53% обыкновенных акций:

- Евгений Киреев — 8,74%;
- Дмитрий Максимов — 8,71%;
- Юрий Максимов — 47,08%;

Все привилегированные акции принадлежат одному из основных акционеров.

ПАО «Группа Позитив» и подконтрольные ему юридические лица не имеют обыкновенных акций ПАО в своем распоряжении.

Структура акционерного капитала по состоянию на 31 марта 2022 года, % от обыкновенных акций



Пионер DPO на Московской бирже

Positive Technologies стала первым эмитентом на Московской бирже, разместившим акции в формате DPO (direct public offering). Это формализованный в законодательстве и доступный для эмитентов, но ранее никем из крупных компаний в современной России не использованный вариант прямого выхода на биржу, когда в определенное время акционеры, которых ранее вознаградили акциями, получили возможность продавать их на бирже.

В отличие от IPO (initial public offering), прямой листинг не предполагает участия андеррайтеров. Перед началом торгов акции Компании получили в качестве вознаграждения линейные сотрудники, а также бывшие сотрудники, которые внесли существенный вклад в ее развитие.

С началом торгов для владельцев крупных пакетов акций было установлено ограничение на их продажу (lock-up). Для миноритарных акционеров, напротив, не было ограничений, вместе с тем большая часть новых акционеров быстро осознали потенциал роста своих активов и максимально сохранили их в составе своих инвестиционных портфелей.

Почему мы выбрали формат прямого размещения акций:

- прежде всего мы были сфокусированы на частных инвесторах как движущей силе российского фондового рынка,
- мы не нуждались в привлечении дополнительного капитала и ставили перед собой задачи по повышению узнаваемости бренда, появлению возможности использования акций в качестве инструмента мотивации и вознаграждения сотрудников, привлечения лучших специалистов не только среди специалистов в области ИБ, но и из других профессиональных сфер,
- процесс прямого размещения акций влечет за собой меньше издержек, поскольку не требует участия андеррайтеров, а также может быть реализован в более сжатые сроки,
- курс акций в первые недели после размещения на бирже в значительно меньшей степени подвержен волатильности по сравнению с традиционным IPO.

Вместе с тем прямое размещение акций позволило нам достичь поставленных целей, в том числе сформировать культуру совладения как у менеджмента, так и у линейного персонала Positive Technologies и получить инструмент реальной оценки стоимости Компании.

Концепция совладения

Positive Technologies воплотила в жизнь новую модель совладения Компанией, когда линейные сотрудники вместе с ее основателями и топ-менеджерами владеют бизнесом и чувствуют свою сопричастность к общему делу.

Мотивация с помощью вознаграждения акциями или опционами топ-менеджмента — достаточно распространенная практика на рынке, однако наш подход абсолютно уникален. В декабре 2021 года около 1,2 тыс. действующих сотрудников Компании и еще около 200 ранее работавших специалистов были вознаграждены нашими акциями за свой существенный вклад в ее общее развитие. Акции получили даже те сотрудники, которые уже не работают в Компании.

Мы планируем и дальше практиковать вознаграждение сотрудников путем передачи им акций. Кроме того, концепция совладения предполагает, что акционеры получают возможность принимать активное участие в работе не только в вопросах управления, но и с точки зрения разработки продуктов и решений. Многие акционеры — носители глубокой экспертизы в области ИТ и кибербезопасности, и их знания и опыт позволят открыть дополнительные возможности развития.

~1,2
тыс. действующих сотрудников

и еще

~200
ранее работавших специалистов

были вознаграждены нашими акциями за свой существенный вклад в общее развитие Компании в декабре 2021 года

> **Основная идея нашего выхода на биржу — чтобы люди, которые работают на общий результат, относились к этому делу как к своему.**

Ты владеешь долей в Компании и через свою работу и инициативу влияешь на то, чтобы она становилась круче, ее капитализация росла. Благодаря этому она становится успешнее и стоит дороже, а значит, твои акции стоят больше.

Денис Баранов,
Генеральный директор

Динамика котировок

Технология прямого публичного размещения акций на бирже не предусматривает процедуры букбилдинга, в ходе которой определяется первоначальная цена размещения акций на IPO. В процессе подготовки к размещению акций на Московской бирже их первоначальная цена обсуждалась с консультантами по организации размещения — ИК «Велес Капитал», ФК ITI Capital, БКС. Исходя из их оценок был сформирован целевой коридор по цене размещения акций в диапазоне от 600 до 1 тыс. руб. за акцию. На момент выхода на биржу мы приняли решение установить первоначальную цену на уровне 700 руб. за акцию.

В первый день торгов цена акций стала расти и доходила до отметки 1238,2 руб. за акцию, а цена на закрытии составила 994,8 руб. В последующие месяцы стоимость акций стала постепенно снижаться на фоне обострения внешнеполитической ситуации. Торговую сессию 25 февраля 2022 года акции Positive Technologies закончили на отметке 560,4 руб. за акцию, после чего торги на Московской бирже были приостановлены. В первый же день возобновления торгов 28 марта акции выросли на 40%, несмотря на снижение индекса Московской биржи. 29 марта 2022 года котировки акций повторили максимально допустимый рост в 40%, таким образом, обеспечив суммарное увеличение стоимости акций на 96% за два дня. Кратно, примерно в 15 раз, выросли и объемы торгов, что подтверждает высокий спрос со стороны инвесторов на фоне перспектив существенного расширения бизнеса.

Ход торгов акциями ПАО «Группа Позитив» на Московской бирже

Дивиденды

В отчетном году было принято Положение о дивидендной политике, согласно которому мы планируем обеспечивать стабильную выплату дивидендов по акциям, что является уникальным подходом для высокотехнологичных быстрорастущих компаний.

Согласно Положению о дивидендной политике дивиденды выплачиваются из прибыли, определенной на основе бухгалтерской отчетности по российским стандартам бухгалерской отчетности (РСБУ). При подготовке рекомендаций касательно размера выплачиваемых дивидендов Совет директоров учитывает финансовые показатели, определенные в соответствии с консолидированной отчетностью.

Совет директоров при разработке рекомендаций Общему собранию акционеров относительно величины дивидендных выплат будет стремиться ежегодно направлять на выплату дивидендов максимальный объем скорректированного свободного денежного потока с возможностью корректировки с учетом следующих факторов:

- текущие и прогнозные финансовые результаты деятельности Компании;
- размер нераспределенной прибыли прошлых лет и промежуточной чистой прибыли текущего года;
- планируемые капитальные затраты текущего года и объем инвестиций в развитие бизнеса и финансирование сделок по слиянию и поглощению (M&A);
- достаточность собственного оборотного капитала и доступность внешних источников капитала;
- планируемые программы обратного выкупа акций в целях мотивации персонала;
- уровень долговой нагрузки с учетом показателя «Чистый долг / EBITDA» Adj. LTM:
  - если значение показателя «Чистый долг / EBITDA» Adj. LTM на последнюю отчетную дату, предшествующую дате принятия решения о рекомендации выплаты дивидендов, и на конец года, в котором принимается решение о рекомендации выплаты дивидендов, находится в диапазоне ниже 1,5, то на выплату дивидендов в течение года может быть рекомендовано к направлению до 100% и более скорректированного свободного денежного потока, но не более 100% чистой прибыли периода и (или) нераспределенной прибыли прошлых лет по данным консолидированной отчетности,
  - если значение показателя «Чистый долг / EBITDA» Adj. LTM на последнюю отчетную дату, предшествующую дате принятия решения о рекомендации выплаты дивидендов, и на конец года, в котором принимается решение о рекомендации выплаты дивидендов, находится в диапазоне от 1,5 до 2,5, то на выплату дивидендов в течение года может быть рекомендовано к направлению не более 100% скорректированного свободного денежного потока,
  - если показатель «Чистый долг / EBITDA» Adj. LTM на последнюю отчетную дату, предшествующую дате принятия решения о рекомендации выплаты дивидендов, и на конец года, в котором принимается решение о рекомендации выплаты дивидендов, превышает 2,5, то выплата дивидендов может быть признана нецелесообразной, либо Совет директоров может рекомендовать выплату дивидендов в меньшем размере с учетом прочих значимых факторов текущего и прогнозного финансового состояния Группы.

Мы также ориентируемся на чистую прибыль по международным стандартам финансовой отчетности (МСФО) при определении размера дивидендов и планируем направлять на дивидендные выплаты не менее ее половины. Так, 27 апреля 2022 года решением внеочередного Общего собрания акционеров утверждена выплата дивидендов в общей сумме 950 млн руб., ставка дивиденда на одну акцию — 14,4 руб. При этом чистая прибыль Positive Technologies за 2021 год составила 1,9 млрд руб.

Сведения о дивидендной истории

АО «Группа Позитив» приобрело публичный статус и именуется ПАО «Группа Позитив» с 13 декабря 2021 года. Сведения о дивидендной истории приводятся по АО «Группа Позитив», созданному путем учреждения вновь 27 сентября 2017 года.

27 апреля 2022 года внеочередное Общее собрание акционеров приняло решение о выплате дивидендов акционерам из чистой прибыли ПАО «Группа Позитив» за I квартал 2022 года. Это первая выплата дивидендов после выхода Компании на биржу.

Дивиденды за I квартал 2022 года

Отчетный период	Общий размер объявленных дивидендов, тыс. руб.		Размер дивиденда в расчете на одну акцию[1], руб.	
	Обыкновенные акции	Привилегированные акции	Обыкновенные акции	Привилегированные акции
I квартал 2022 года	950 000		14,4	14,4
	864 000	86 400		

Дивидендная история Positive Technologies до выхода на биржу

Отчетный период	Общий размер объявленных дивидендов, тыс. руб.		Размер дивиденда в расчете на одну акцию[1], руб.	
	Обыкновенные акции	Привилегированные акции	Обыкновенные акции	Привилегированные акции
III квартал 2021 года	340 008		54,84	54,84
	329 040	10 968		
2020 года	592 720		95,60	95,60
	573 600	19 120		
2019 года	Решение о выплате дивидендов Общим собранием акционеров за 2017–2019 годы не принималось, дивиденды за указанные периоды не начислялись и не выплачивались			
2018 года				
2017 года				

[1] Размер дивиденда в расчете на акцию приведен до дробления акций, связанного с приобретением Компанией публичного статуса.

Облигации

29 июля 2020 года дочернее общество Компании разместило дебютный выпуск облигаций на Московской бирже объемом 500 млн руб. Размещение облигаций стало первым шагом Компании к публичности и представлению нашего бизнеса более прозрачным и понятным для инвесторов.

«Позитив Текнолоджиз 001Р-01»
полное наименование ценной бумаги

3 года
срок обращения облигаций на бирже

500 тыс. облигаций
размер выпуска

11,5% годовых
уровень ставки купона

1 тыс. руб.
номинал облигации

Выплата купона осуществляется **ежеквартально**

3-й уровень листинга
присвоен выпуску

26 июля 2023 года
дата погашения облигаций

Ход торгов облигациями дочернего общества ПАО «Группа Позитив» на Московской бирже

Кредитные рейтинги

2 декабря 2021 года рейтинговое агентство «Эксперт РА» присвоило ПАО «Группа Позитив» кредитный рейтинг на уровне ruA– с позитивным прогнозом.

Агентство отметило, что установление позитивного прогноза по рейтингу обусловлено ожиданиями роста масштабов бизнеса и сильными финансовыми показателями Компании по итогам 2021 года, сохранением низкой долговой нагрузки и высокого процентного покрытия, а также улучшением оценки блока корпоративных рисков в результате внедрения лучших практик корпоративного управления и риск-менеджмента в краткосрочной перспективе.

Среди позитивных факторов, оказывающих поддержку рейтингу, агентство указало:

- **Сильные рыночные и конкурентные позиции.**
  На протяжении последних двух лет мы демонстрируем рост выше среднеотраслевого. Наша Компания обладает умеренно-высокой степенью диверсификации портфеля продуктов. Клиентская база насчитывает более 2300 компаний, высоко диверсифицирована по отраслевой принадлежности, доля крупнейшего клиента составляет не более 5% от совокупной выручки. Ввиду отсутствия зависимости от труднозаменимых поставщиков и подрядчиков риски концентрации бизнеса агентством оцениваются как низкие.
- **Низкий уровень долговой нагрузки.**
  Первый коммерческий продукт был запущен в 2004 году, с 2014 года началась активная фаза развития портфеля предоставляемых решений по кибербезопасности, при этом мы росли органически без существенного увеличения долговой нагрузки. Актуальная стратегия развития ориентирована на предоставление комплексных решений для реализации результативной кибербезопасности, основанных на уже разработанных ИТ-продуктах, что в совокупности с ростом доходов не приведет в будущем к увеличению долговой нагрузки. В прогнозных периодах агентство ожидает уровень процентного покрытия выше 10,0x, что по бенчмаркам агентства оценивается как высокое.
- **Тенденция к росту маржинальности бизнеса.**
  Рост инсталляционной базы в дочерних структурах крупных холдинговых организаций и ежегодные отчисления по продлениям и обновлениям уже внедренных продуктов позволяют постоянно наращивать долю продуктов и сервисов в бюджетах проектов на информационную безопасность у заказчиков, что приводит к повышению маржинальности бизнеса. Наши планы предусматривают масштабирование числа продуктов на одного клиента с текущих трех продуктов до пяти-десяти, что позволит обеспечить значительный рост совокупной выручки и EBITDA в будущих периодах. Учитывая отсутствие пропорционального роста затрат на разработку программного обеспечения, агентство ожидает дальнейшего роста показателей рентабельности в среднесрочной перспективе.

Рейтинги кредитоспособности ПАО «Группа Позитив» (по состоянию на 30 апреля 2022 года)

Рейтинговое агентство
«Эксперт РА»

Объект рейтингового действия
ПАО «Группа Позитив»

Действующий рейтинг
ruA–

Прогноз
позитивный

Дата последнего подтверждения/ пересмотра
2 декабря 2021 года

Взаимодействие с акционерами и инвесторами

В своей деятельности мы придерживаемся следующих ключевых принципов, призванных гарантировать интересы акционеров:

- обеспечение реальной возможности для акционеров реализовывать свои права, связанные с участием в деятельности Positive Technologies;
- стратегическое управление Советом директоров деятельностью Компании и эффективный контроль за деятельностью исполнительного органа Компании;
- осуществление исполнительным органом руководства текущей деятельностью в интересах долгосрочного устойчивого развития нашей Компании и получения акционерами выгоды от этой деятельности;
- обеспечение эффективного контроля за финансово-хозяйственной деятельностью с целью защиты прав и законных интересов акционеров.

Для достижения вышеуказанных целей мы своевременно и точно раскрываем информацию по всем существенным вопросам, касающимся нашей деятельности, включая финансовое положение, результаты деятельности, структуру собственности и управления.

Мы делаем это открыто и на регулярной основе: проводим офлайн- и онлайн-мероприятия, совместные эфиры с ключевыми брокерами, Московской биржей и инвестиционными каналами, доносим до наших действующих и потенциальных инвесторов максимально подробную информацию о рынке кибербезопасности, о наших продуктах и решениях, финансовых показателях, перспективах и планах, делимся нашей экспертизой и позитивными новостями из жизни организации.

Мы ведем открытый диалог с нашими акционерами в телеграм-канале инвесторов IT's positive investing и в официальном канале Positive_technologies в социальной сети для инвесторов «Пульс» («Тинькофф Инвестиции»), где нашими подписчиками являются суммарно уже больше 12 тыс. пользователей.

Telegram:
IT's positive investing

Тинькофф Пульс:
Positive_technologies

Раскрытие информации

Мы стремимся следовать основным принципам раскрытия информации, обеспечивая его регулярность и оперативность, доступность информации для акционеров и иных заинтересованных лиц, а также достоверность и полноту ее содержания. Мы соблюдаем требования в области публичного раскрытия информации, предоставляя акционерам и иным заинтересованным лицам возможность получить достоверную информацию о Компании и подконтрольных ей организациях. Компания регулярно и своевременно публикует информацию на собственном сайте и странице ООО «Интерфакс-ЦРКИ».

Страница Компании на сайте «Интерфакс — Центр раскрытия корпоративной информации»

Раздел «Инвесторам» на сайте Компании

Почему Positive Technologies

Мы создаем технологии, которые позволяют предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям, объединяем экспертов с уникальными компетенциями в области разработки и кибербезопасности, даем публичные площадки для обмена знаниями и опытом людей, заинтересованных в развитии и защите цифрового мира

Владимир Заполянский
Директор по маркетингу
и корпоративным коммуникациям

Наша история: 20 лет на рынке кибербезопасности

История Positive Technologies — это история создания надежной системы защиты от хакерских угроз.

'90 '00

1999 год

Интерес к первому нашему продукту — бесплатному сканеру безопасности **XSpider** превысил все ожидания: пользователи скачали его более 300 тыс. раз.

2002 год

Мы основали Positive Technologies, открыли первый офис и запустили консалтинговые услуги.

2003 год

Мы запустили первую коммерческую версию сканера безопасности **XSpider** и успешно вывели ее на рынок. Также мы начали деятельность по анализу защищенности.

2004 год

Мы успешно провели первый тест на хакерское проникновение.

Наша Компания подписала договоры с крупными клиентами — Сбербанком, компанией «ВымпелКом», Министерством обороны Российской Федерации, Магнитогорским металлургическим комбинатом.

2005 год

Мы выполнили первую уникальную работу по анализу кода.

2006 год

Наши специалисты начали разработку системы контроля защищенности и соответствия стандартам **MaxPatrol**.

Стартовал проект по непрерывному тестированию виртуальных площадок компании Masterhost для выявления уязвимостей ПО интернет-проектов.

2007 год

Мы сформировали отдел тестирования ПО.

2008 год

Мы создали партнерскую сеть в России.

В нашей Компании появилась отдельная команда, работающая над проведением тестов на проникновение.

Мы вывели на рынок новую систему контроля защищенности и соответствия стандартам **MaxPatrol 8**, ставшую наиболее востребованным продуктом года.

Positive Technologies вошла в топ-10 самых быстрорастущих российских ИТ-компаний в сфере защиты информации[1].

Мы запустили обучающие курсы по сертификации уровня владения основными возможностями системы **MaxPatrol Enterprise Edition**.

2009 год

В Компании был создан исследовательский центр.

[1] По версии CNews.

'10

2010 год

Мы подписали новые контракты с крупными клиентами, включая «МегаФон», МТС, «Ростелеком», «Газпром нефть», «Газпромбанк», «Росбанк».

2011 год

Были запущены регулярные бесплатные вебинары по ИБ.

Учебный центр «Информзащита» получил статус авторизованного учебного центра Positive Technologies.

Мы организовали первый международный форум по кибербезопасности **Positive Hack Days**.

2012 год

Наша Компания открыла офис в Санкт-Петербурге.

Мы запустили образовательные инициативы — конкурс **PHDays Young School** и программу **Positive Education**.

География форума **Positive Hack Days** расширилась от Владивостока до Калининграда и от Индии до Туниса.

2013 год

Мы вывели на рынок новые продукты и решения: **PT Application Inspector** и **PT Application Firewall**.

Наша Компания стала лидером в рейтинге самых быстрорастущих компаний сегмента Security and Vulnerability Management[1] и заняла третье место на российском рынке ПО для безопасности.

2014 год

Наш продукт **PT Application Firewall** был использован во время Олимпиады в Сочи для круглосуточной защиты порталов ВГТРК.

Positive Technologies включили в отчеты аналитического агентства Gartner.

Мы заняли третье место на отечественном рынке продуктов для защиты информации[2].

Наша Компания вошла в список 20 наиболее быстрорастущих ИТ-компаний 2013 года[3].

2015 год

Мы открыли офисы в Новосибирске, Томске и Нижнем Новгороде.

Наш продукт **PT Application Firewall** был включен в рейтинг аналитического агентства Gartner.

Наша Компания стала визионером рейтинга Gartner.

2016 год

Мы открыли офис в Самаре.

Наша Компания вывела на российский рынок новые продукты: **PT ISIM**, **PT MultiScanner**, **MaxPatrol SIEM**.

2017 год

Мы запустили новые продукты и решения: **PT Application Firewall Cloud DDoS Protection** и **PT Security Intelligence Portal**.

Совместный продукт Positive Technologies и «Бомбардье Транспортейшн (Сигнал)» был признан лучшим отраслевым решением[3].

Наша Компания вновь вошла в рейтинг Gartner в качестве визионера.

2018 год

Мы выпустили новые продукты: **PT ISIM freeView Sensor**, **PT Network Attack Discovery**, **PT Platform 187** и **MaxPatrol SIEM 4.0**.

Наша Компания обеспечила защиту информационных ресурсов на чемпионате мира по футболу 2018 года.

Доля продукта **MaxPatrol SIEM** на российском рынке выросла до 25%.

2019 год

Мы вывели на рынок новые продукты и решения: **PT Application Inspector Enterprise**, **PT ISIM Sensor** и **PT ISIM View Point**.

Positive Technologies обеспечила защиту ИТ-систем во время Универсиады-2019 в Красноярске.

Наша Компания вошла в число участников программы для разработчиков средств защиты Microsoft Active Protections.

1 По данным аналитической компании International Data Corporation.
2 По данным CNews.
3 По версии Global CIO.

'20

2020 год

Мы запустили новые продукты: **PT Network Attack Discovery**, **PT Sandbox**.

Наша Компания была включена в топ-20 крупнейших российских групп и компаний в области информационно-коммуникационных технологий (ИКТ), а также в топ-10 разработчиков ПО[1].

Мы стали одной из десяти крупнейших компаний России в сфере защиты информации и одним из трех крупнейших вендоров России в сфере защиты информации[2].

2021 год

Наша Компания анонсировала решения нового поколения — метапродукты, полностью ориентированные на результативную кибербезопасность.

Мы провели открытые киберучения на действующей инфраструктуре Positive Technologies и испытание первого метапродукта **MaxPatrol O2** в условиях, приближенных к реальным.

Состоялось бета-тестирование **The Standoff 365** — первой в России онлайн-платформы для проведения полноценных киберучений в режиме 24 часа в сутки и 365 дней в году.

Positive Technologies вышла на биржу путем прямого листинга и стала первой в России публичной компанией из отрасли кибербезопасности.

Объем продаж нашей Компании составил 7,8 млрд руб., что на 26% больше, чем в 2020 году. Таким образом, успешно реализована трехлетняя стратегия, которая была ориентирована на увеличение продаж с 2019 по 2021 год в объеме с 4 млрд до 8 млрд руб.

Юбилейный **PHDays 10** собрал более 2,5 тыс. гостей, а за самой масштабной в мире открытой кибербитвой **The Standoff** онлайн наблюдали свыше 65 тыс. человек.

Мы представили новые продукты и решения: **PT XDR**, **MaxPatrol VM**.

Positive Technologies заняла 15-е место в рейтинге 30 самых дорогих компаний Рунета, составленном Forbes.

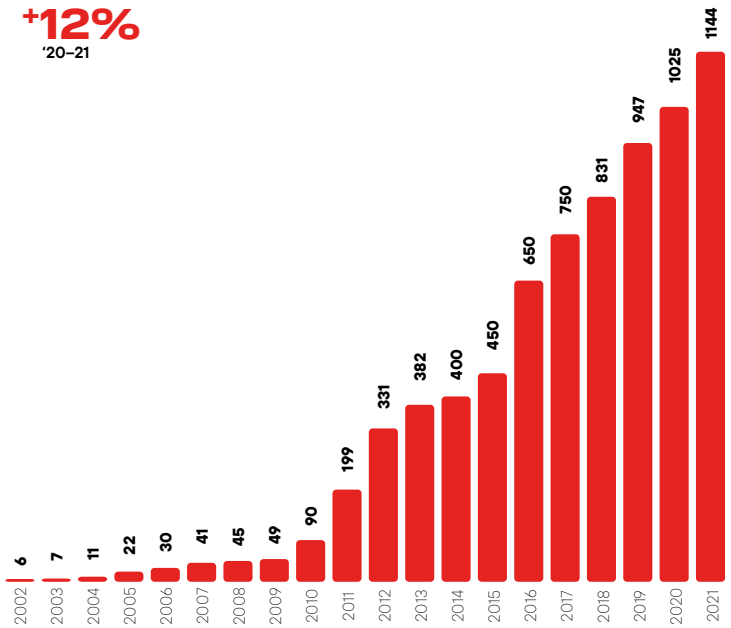
Компания вошла в топ-20 крупнейших российских компаний в области ИКТ, а также в топ-10 разработчиков ПО по версии «Эксперт РА».

Компания заняла 11-е место в списке крупнейших компаний России в сфере защиты информации, а также вошла в десятку крупнейших российских вендоров в сфере защиты информации по версии CNews Analytics.

Продукт **MaxPatrol SIEM** вошел в топ-20 мировых SIEM-систем по оценке IDC. Доля MaxPatrol SIEM на российском рынке SIEM составляет более 40%.

Positive Technologies вошла в тройку мировых вендоров с наиболее высоким годовым приростом продаж **SIEM-решений** (85%) по оценке IDC. Рейтинговое агентство «Эксперт РА» присвоило Компании рейтинг кредитоспособности на уровне «ruA-» с позитивным прогнозом.

Рост числа сотрудников Positive Technologies с 2002 по 2021 год, человек

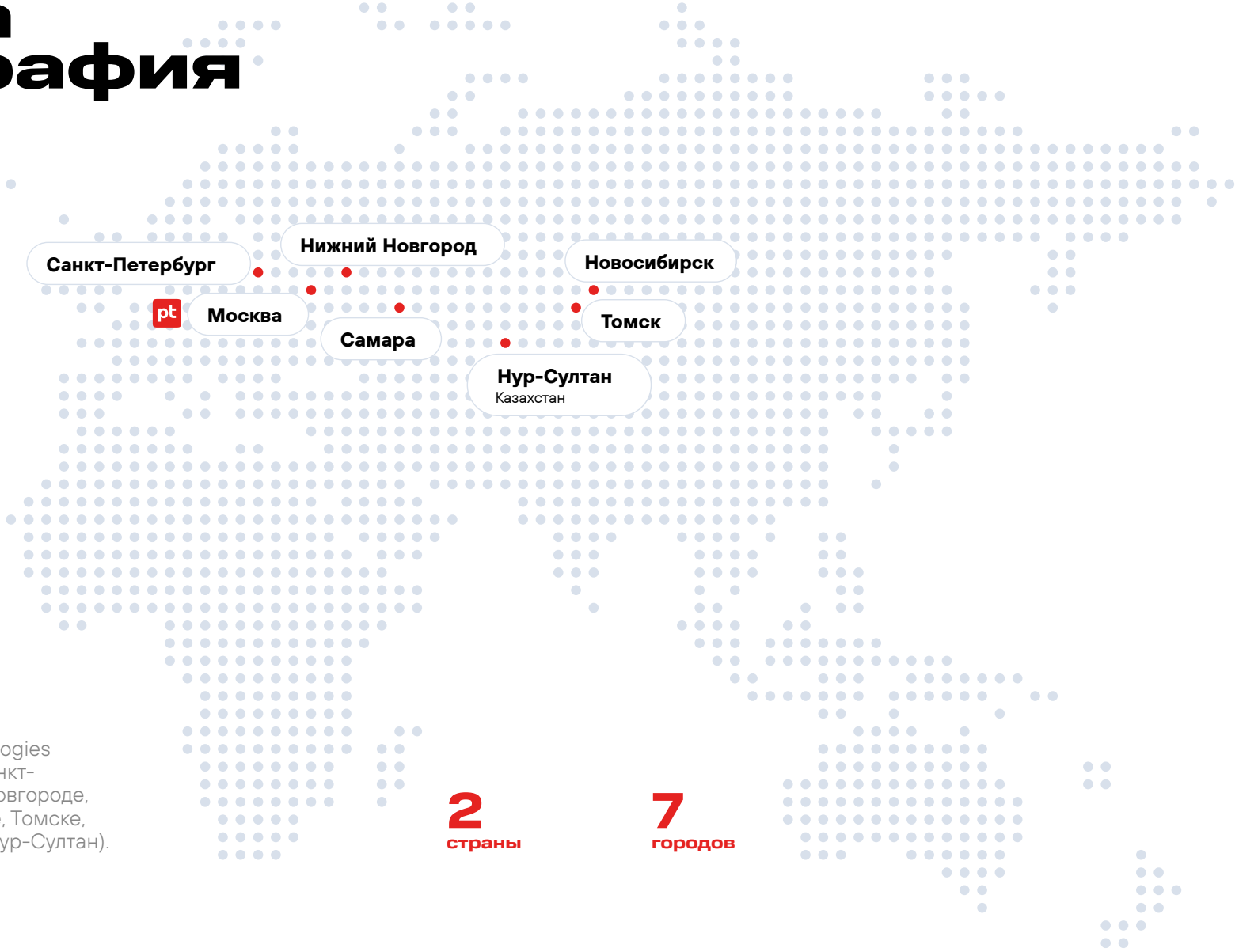


В последние годы с ростом числа киберугроз уровень ответственности за принятие решений в этой области перешел к первым лицам компаний. Рынок потребовал от нас принципиально нового подхода к безопасности: критически важные процессы должны быть защищены от любых угроз.

Для решения этой задачи мы разрабатываем продукты, которые объединены в единую метаплатформу. Они автоматически обмениваются информацией, чтобы выявлять и блокировать действия хакеров и вывести защиту информационных систем на новый уровень.

1 По версии РА «Эксперт».
2 По версии CNews Analytics.

Наша география



Офисы Positive Technologies работают в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске, Томске, а также в Казахстане (Нур-Султан).

2 страны

7 городов

Наша экспертиза

PT Expert Security Center

Для успешной работы служб ИБ обычно используются автоматизированные средства защиты. Но иногда этого недостаточно.

Чтобы предоставить нашим клиентам больше возможностей по выявлению угроз и противодействию им, в 2015 году мы создали экспертный центр безопасности — PT Expert Security Center. В нем работают почти 200 экспертов в сфере ИБ, проводится около 50 расследований в год.

Услуги PT ESC

Контроль периметра
Advanced Border Control — услуга, в рамках которой наши эксперты оперативно оповещают клиентов о выявлении на узлах сетевого периметра уязвимостей и дают рекомендации по их устранению.

Ретроспективный анализ событий ИБ
По запросу клиента мы проводим анализ событий ИБ и выявляем пропущенные инциденты. Затем мы передаем ему экспертное заключение о степени опасности обнаруженных инцидентов, их влиянии на ИТ-инфраструктуру, а также рекомендации по минимизации ущерба.

Экспертная поддержка при реагировании на инцидент
Мы всегда готовы прийти на помощь службам ИБ и ИТ-отделам наших клиентов. Специалисты PT ESC подключаются удаленно или выезжают к клиенту и оперативно решают возникшую проблему.

Анализ инцидента ИБ
Мы проводим полное расследование инцидента по просьбе клиента: выясняем уровень опасности события, устанавливаем, какое вредоносное ПО использовалось, определяем границы и степень поражения.

Комплексное расследование инцидентов ИБ
По запросам клиентов мы проводим всестороннее и глубокое расследование инцидентов, восстанавливая их хронологию и предоставляя развернутые рекомендации в области кибербезопасности.

PT SWARM[1]

PT SWARM — это команда из более чем 60 экспертов в сфере offensive security[2].

Мы проводим:

- тестирование на проникновение,
- анализ защищенности приложений,
- работы по проектам социальной инженерии,
- аудит беспроводных сетей, банкоматов и POS-терминалов.

100+
проектов
ежегодно

250+
уязвимостей
выявлено в ПО

60
крупнейших производителей

Наши эксперты признаны во всем мире и находятся в залах славы разных компаний.

Наши эксперты в области защиты SCADA- и ERP-систем, веб-приложений, банковских и телекоммуникационных технологий ведут исследования и тестирования на проникновение, анализируют угрозы и уязвимости. Специалисты центра включены в залы славы Adobe, Apple, AT&T, PayPal, Google, GitLab, IBM, Microsoft, Mastercard, «Яндекс» и Mail.ru.

1 SWARM — security weakness advanced research and modeling.
2 Подход к информационной защите на основе модели, подразумевающей взлом, при которой необходимо найти слабые места и усилить их, а также сократить время реагирования до минимума.

Positive Hack Days

Positive Hack Days (PHDays) — ежегодная конференция, посвященная вопросам ИБ, которую мы проводим в Москве с 2011 года.

phd Positive Hack Days

На PHDays выступают российские и зарубежные разработчики, эксперты по ИБ и хакеры, проходят мастер-классы и лабораторные практикумы.

PHDays поднимает самые актуальные вопросы ИБ:

- инновации в области взлома информационных систем и методов практической безопасности,
- подходы к ИБ в эпоху интернета вещей,
- защита критически важной инфраструктуры,
- организация физической безопасности информационных ресурсов,
- противодействие мошенничеству и киберпреступности,
- выявление и расследование инцидентов ИБ,
- создание и совершенствование продуктов ИБ,
- развитие методов безопасной разработки программного обеспечения (SSDL).

The Standoff

The Standoff — это крупнейшие в мире открытые киберучения, которые мы проводим ежегодно.

Мы воссоздаем производственные цепочки, бизнес-сценарии и технологический ландшафт различных отраслей экономики на киберполигоне, а ведущие специалисты в области нападения и защиты борются за ресурсы виртуальной копии мира.

Участие в The Standoff позволяет:

- оценить последствия кибератак в виртуальной среде
- получить знания и навыки выявления кибератак и противодействия им
- изучить сценарии реагирования
- понять взаимосвязи кибербезопасности и бизнеса

The Standoff
Видео

Работодатель мечты

Мы развиваем среду, в которой сотрудники занимаются любимым интересным делом в команде лучших экспертов и единомышленников, чувствуя себя причастными к развитию результативной кибербезопасности.

Positive Technologies — это уникальная среда, в которой есть амбициозные задачи и особые, новые форматы их решения:

- у нас можно менять индустрию и делать невозможное возможным;
- в Компании работают вместе очень разные люди и достигают результата. Каждый из нас — эксперт в своей области, но вместе мы создаем новые конструкции;
- у нас люди растут очень быстро, потому что у нас много смыслов и вызовов. Новички становятся экспертами за два года;
- мы — сильнейшие «технари» индустрии, у нас интересные задачи;
- мы — белые хакеры. Мы знаем лучше всех, как ломать, и поэтому знаем, как защищать;
- наше DPO — лучшая в индустрии модель мотивации ключевых людей Компании, возможность собирать лучших специалистов рынка;
- Positive Technologies — это не один генеральный директор, это команда сильных и ярких ключевых людей.

Мы помогаем людям расти в Компании, развиваться и становиться лучшими в своих областях, раскрывать свои уникальные таланты максимально. Строим открытые коммуникации, чтобы все понимали стратегию Компании, актуальную повестку бизнеса и привносили свой вклад в развитие Компании. Хорошие условия работы — база, которая помогает сосредоточиться на деле и не думать о мелочах. Мы никогда не останавливаемся в совершенствовании условий нашей работы.

Наша Компания работает в узкоспециализированной отрасли, что определяет специфику работы с людьми. На рынке мало высококвалифицированных специалистов, и ведущие компании конкурируют между собой за лучших профессионалов. Из-за этого подбор сотрудников усложняется. Тем не менее из 200 экспертов высочайшего класса в сфере ИБ, которые есть сейчас в России, около 80 работают в Positive Technologies.

Исторически в нашей Компании распространена практика, когда сотрудники строят карьеру, развиваясь с линейных позиций до уровня топ-менеджмента. Поэтому у менеджеров Positive Technologies обширные компетенции в ИБ.

Важный элемент нашей корпоративной культуры — концепция совладения. Для Компании важно, чтобы сотрудники были не просто наемными работниками, а воспринимали бизнес Positive Technologies как собственное дело. В 2021 году Компания вознаградила сотрудников акциями, и в дальнейшем мы планируем сохранять эту практику.

Еще одна важная особенность нашей Компании — открытость менеджмента любого уровня к неформальному общению с персоналом. Благодаря такому подходу Компания сохраняет гибкость и может быстро адаптироваться к меняющимся условиям.

«Позитив — это люди.

Мы наблюдаем в СМИ большой ажиотаж по поводу оттока ИТ-кадров за рубеж. По себе мы видим, что из 1,2 тыс. сотрудников нашей Компании около 2% временно переехали за рубеж, оставаясь работать в Компании и планируя вернуться. В то же время на рынке из-за ухода глобальных вендоров освобождается немало опытных специалистов. У нас сейчас есть около 300 вакансий, и мы рассчитываем, что многие талантливые люди присоединятся к нам, и мы станем еще сильнее.

Евгения Гулина,
HR-директор

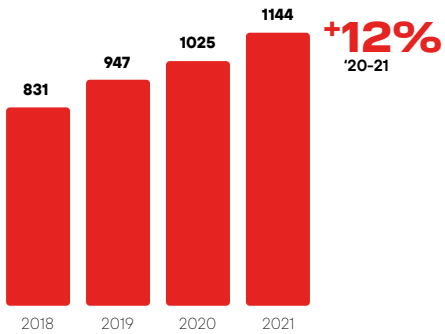
Численность и структура персонала

Бизнес Компании стремительно растет, поэтому численность персонала Positive Technologies увеличивается год от года.

В 2021 году штат вырос на 12% и на конец года составил 1144 человека. Текучесть персонала в 2021 году составила около 20%. Этот показатель вырос за последний год в связи с тенденциями рынка и выходом из паузы, образовавшейся во время пандемии. Многие специалисты в области разработки стали получать международные офферы с удаленным форматом работы.

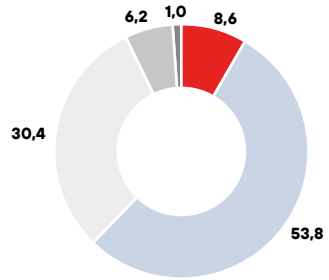
При этом мы отметили приток возврата сотрудников в Компанию. В 2021 году 3% вакансий было закрыто бывшими сотрудниками, которые вернулись работать в Компанию. Этот показатель быстро растет и уже по итогам I квартала 2022 года составил 8%.

Численность персонала по состоянию на 31 декабря 2021 года



По гендерному составу в штате Компании преобладают мужчины (72%). Доля мужчин на руководящих должностях чуть выше — 77%. Компания предоставляет сотрудникам равные возможности развития вне зависимости от пола. Мужчины и женщины имеют равные права при приеме на работу и равные возможности построения карьеры.

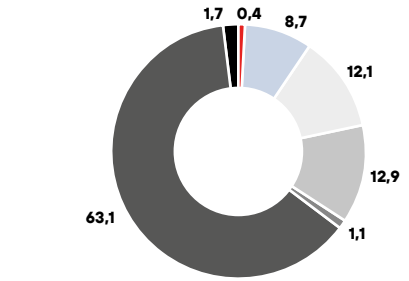
Возрастная структура персонала по состоянию на 31 декабря 2021 года, %



<35 лет

Positive Technologies — молодая компания: возраст 62% персонала не превышает 35 лет

Регионы проживания персонала по состоянию на 31 декабря 2021 года, %



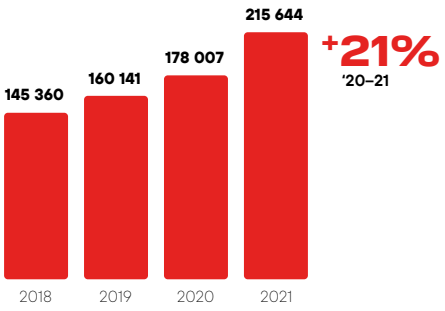
Специфика бизнес-процессов Positive Technologies позволяет командам взаимодействовать удаленно. У нас развит гибридный формат работы — сотрудник может выбрать работу в офисе или удаленно, или совмещать оба варианта. Компания географически распределена, 9% персонала проживают и работают в регионах, где нет наших офисов.

Финансовая и нефинансовая мотивация

Важнейшими факторами мотивации для нас всегда были амбициозные задачи Компании и команда единомышленников. Мы создаем в Компании среду, в которой людям интересно работать и расти за счет решения сложнейших задач, которые мы ставим перед собой.

Большие достижения в работе отражаются на материальной составляющей мотивации сотрудников. Мы постоянно мониторим заработные платы на рынке, участвуем в обзорах и соответственно повышаем вознаграждение сотрудников. Размер повышения определяется индивидуально и зависит от ситуации на рынке труда и оценки личной эффективности сотрудника. За три года средняя зарплата в Компании выросла на 48%.

Средняя заработная плата, руб.



Помимо заработной платы, в Positive Technologies существует проектное премирование. Также Компания предоставляет сотрудникам социальный пакет. В него входят:

- **добровольное медицинское страхование** и страхование выезжающих за рубеж для всех сотрудников;
- **изучение английского языка** с индивидуальными репетиторами и языковыми школами;
- **возмещение затрат** на переезд;
- **компенсация** оплаты занятий спортом.

Наравне с материальной мотивацией наша Компания уделяет много внимания созданию системы нематериальной мотивации и обеспечению комфортных условий работы. В офисе регулярно работают порядка 20% персонала. Для них мы предоставляем удобные рабочие пространства с зонами отдыха и спортивными зонами.

Мы совершенствуем программы премирования и разрабатываем систему долгосрочной мотивации сотрудников акциями, ее внедрение запланировано на 2022 год.

Мы заботимся о базовых элементах мотивации, которые должны создавать комфортную среду для сотрудников, чтобы они могли сосредоточиться на любимом деле и не думать о мелочах. С 2022 года мы ввели дополнительные льготы:

- теперь ДМС можно пользоваться с первого дня работы в Компании;
- расширена программа компенсации затрат на занятия спортом и ее размеры увеличены на 15%;
- мы развиваем среду для общения коллектива в формате клубов по интересам. Сейчас в Компании действует больше 10 клубов: спортивные клубы по разным направлениям, книжный и киноклуб, клуб настольных игр и шахматный.

Обучение персонала

Компетенции персонала — главное конкурентное преимущество Компании, поэтому мы помогаем нашим людям учиться, пополняя багаж знаний и навыков.

Для этого мы используем следующие инструменты:

- обязательное обучение — сертификацию сотрудников для подтверждения экспертизы;
- профессиональное обучение — приобретение технических или управленческих компетенций;
- участие в конференциях как в качестве докладчиков, так и в качестве слушателей;
- внутренним тренером может стать любой сотрудник, который готов делиться востребованными знаниями и умениями;
- часть обучения организуется через внешних провайдеров с привлечением самых интересных спикеров;
- в Компании есть учебный портал, на котором размещаются тренинги по продуктам и курсы менеджеров.

В 2021 году затраты Компании на обучение составили 40,45 млн руб. В 2022 году мы планируем расширить программы внутреннего обучения, больше делиться уникальными знаниями и подходами в работе, которые смогли сделать Компанию успешной. Также мы продолжим участвовать в конференциях, чтобы сотрудники оставались в курсе последних инноваций.

Охрана труда и здоровья сотрудников

Забота о здоровье сотрудников и обеспечение здоровых условий труда — один из приоритетов Компании в области управления персоналом.

Во время пандемии COVID-19 мы перевели всех сотрудников, присутствие которых в офисе не было необходимо для функционирования бизнес-процессов, на удаленный режим работы. Персонал, продолжавший работать из офиса, был обеспечен средствами индивидуальной защиты (маски, хирургические перчатки), дезинфицирующими салфетками, санитайзерами, а офисные помещения оборудовали рециркуляторами.

6,5
млн руб.

Компания затратила на услуги по регулярному тестированию сотрудников на COVID-19

Охрана труда

В Компании проводится специальная оценка условий труда (СОУТ) согласно Положению о СОУТ[1] и ежегодным планам мероприятий. На 1001 рабочем месте (охват 100% по состоянию на февраль 2021 года) проведен инструментальный контроль (измерение) и оценка электромагнитного поля от ПЭВМ. Затраты на эти мероприятия составили 451 тыс. руб.

Обучение руководителей и специалистов Компании мерам по охране труда и технике безопасности проводится дистанционно в АНО ДПО «ТехноПрогресс» на базе образовательной платформы Courson с персональным контролем прохождения обучения и проверки пройденного материала. Периодичность обучения — один раз в три года. Обучение проходят 100% сотрудников. Не проходят обучение сотрудники, работающие удаленно. В 2021 году обучение прошли 219 человек.

Для профилактики профзаболеваний в Компании проводятся следующие мероприятия: оснащение рабочих мест современными компьютерами и эргономичной мебелью, организация мест для активного отдыха, специальные места для перерывов в работе, комфортные кухни и кофе-поинты. Случаев профессиональных заболеваний в Компании в 2021 году не зарегистрировано.

23,7
млн руб.

затраты Компании на добровольное медицинское страхование персонала в 2021 году (см. подробнее выше)

[1] Утверждено приказом от 9 января 2019 года № 02-ОД.2019.

Система управления устойчивым развитием

«Смысл нашей деятельности — обеспечение безотказной работы инфраструктуры для комфортной жизни человека, устойчивой работы бизнеса и безопасности страны.
Наш основной вклад в развитие общества — в том, что мы делаем недопустимые события невозможными.

Евгения Гулина
HR-директор

Принципы устойчивого развития

Деятельность Positive Technologies напрямую связана с обеспечением безопасности компаний, инфраструктуры, государственных и корпоративных сервисов, с выполнением важной социальной функции.

Безотказное функционирование процессов, основанных на информационных технологиях, обеспечивают системы кибербезопасности. Социальная ответственность нашей Компании заключается в том, чтобы с помощью наших разработок не позволить хакерам нарушить функционирование цифровых процессов, будь то работа онлайн-банка, системы городских светофоров или реактора на атомной станции.

Также Компания способствует развитию профессионального сообщества специалистов в области ИБ и стремится сделать сферу ИБ более прозрачной для широкой аудитории.

Система управления устойчивым развитием

Совет директоров

Определяет стратегические направления развития

Отвечает за совершенствование корпоративного управления

Генеральный директор

- Контролирует функционирование системы управления охраной труда, работу HR-службы, соблюдение мер по охране окружающей среды

Директор по персоналу

- Отвечает за подбор и развитие персонала, разработку мер по охране труда

Директор образовательных программ и проектов

- Отвечает за разработку мероприятий в сфере образования и просвещения

Руководители структурных подразделений, отдел охраны труда, HR-служба

- Отвечают за управление персоналом на местах, реализацию мер по промышленной безопасности, охране труда и охране окружающей среды в подразделениях Компании, снижение потребления ресурсов и повышение энергоэффективности

Просвещение и образование

Наша Компания на протяжении многих лет стремится развивать профессиональное сообщество специалистов по кибербезопасности и знакомить с проблемами ИБ широкую общественность. Positive Technologies регулярно проводит целый ряд мероприятий, известных в индустрии кибербезопасности не только в России, но и за ее пределами.

Своими мероприятиями мы стараемся охватить всех, кому может быть интересна тематика ИБ. Мы не делаем различий по гендерному или географическому признаку и проводим целый ряд мероприятий для людей с ограниченными возможностями здоровья.

Результатом наших мероприятий является повышение осведомленности населения, в том числе детей, о проблемах кибербезопасности, привлечение в отрасль заинтересованных людей, которые хотят развиваться в сфере ИБ, а также привлечение новых кадров в нашу Компанию.

Просветительские проекты

Стажировка для студентов вузов в формате летней практики

Positive Technologies предлагает студентам ведущих вузов России пройти стажировку в Компании с возможностью последующего трудоустройства. Среди партнеров Компании — Московский институт электроники и математики им. А. Н. Тихонова, Московский институт электронной техники, Московский энергетический институт, Московский автомобильно-дорожный государственный технический университет, Университет ИТМО (Санкт-Петербург), Томский государственный университет систем управления и радиоэлектроники.

Компания собирает группы студентов со всей России, чтобы не только передать им теоретические знания, но и научить на практике использовать технологии Компании. По окончании стажировки студенты становятся специалистами, которым можно предложить трудоустройство в Positive Technologies или рекомендовать на вакансии в команды ИБ наших заказчиков.

Студенческая практика в Positive Technologies в 2021 году

55 студентов
прошли стажировку

34 студента
были трудоустроены

19 из них
ранее не имели официального трудового стажа

27 из 34 трудоустроенных
продолжают работать по настоящее время

Выступления экспертов Компании перед студентами программы НТИ в ДВФУ

На базе Дальневосточного федерального университета в партнерстве с нашей Компанией запущена образовательная программа Positive Education. В рамках сотрудничества мы передаем вузу лицензии на наши продукты и проводим подготовку преподавателей по тематике ИБ.

20
студентов

участников олимпиады по кибербезопасности НТО — слушатели курса Positive Education

Проведение мастер-классов для московских школьников

Эксперты Positive Technologies совместно с «КиберКлубом» проводят мероприятия для учеников московских школ. Программа лекций и мастер-классов, посвященных вопросам кибербезопасности, была рассчитана на полный учебный день. Мы приглашали к участию детей в возрасте от 10 до 16 лет. Дети младшего возраста в игровой механике узнавали правила кибергигиены, для них были разработаны различные интерактивные задания. Для участников постарше — а это было порядка 200 учеников классов с углубленным изучением информатики — мы провели лекции по вопросам кибербезопасности и профориентации. Ведущим одного из мастер-классов стал сотрудник «хакерского» направления в Компании. Он пришел в Positive Technologies, когда учился на первом курсе Высшей школы экономики, и на мастер-классе поделился опытом, как устроиться в нашу Компанию и совмещать обучение и работу, а также чем интересна работа в сфере кибербезопасности.

Конкурс студенческих докладов на The Standoff

В рамках киберучений The Standoff мы проводим конкурс студенческих докладов. В ноябре 2021 года 30 студентов из России и СНГ прислали свои заявки на участие, содержащие информацию о проектах, которые они реализуют в вузе или самостоятельно. Экспертное жюри Positive Technologies оценило эти материалы и выбрало 18 работ. Участники конкурса сделали доклады в рамках деловой программы The Standoff, которые затем были размещены на платформе кибербитвы. Победителей конкурса определили с помощью онлайн-голосования. Сейчас трое участников проходят стажировку в Компании с перспективой дальнейшего трудоустройства.

Подробнее о The Standoff
на с. 59

Детский день на PHDays

В рамках форума Positive Hack Days мы проводим детский день. Мероприятие направлено на погружение детей в возрасте от 10 до 16 лет в правила личной безопасности через игровые механики. В 2021 году в мероприятии приняли участие 75 подростков в возрасте от 10 до 14 лет, и более 100 — в возрасте от 14 до 16 лет.

175
подростков

приняли участие в детском дне

Подробнее о Positive Hack Days
на с. 59

Обучение детей с ограниченными возможностями здоровья правилам личной безопасности

Данный проект Positive Technologies реализовала совместно с партнером — командой «Мир уникальных геймеров». В 2021 году мы провели две встречи с молодыми людьми с ограниченными возможностями здоровья, которые увлекаются кибериграми. В них приняли участие больше 60 геймеров. В рамках этих мероприятий мы рассказывали ребятам о цифровой безопасности с учетом специфики их увлечений.

60
геймеров

приняли участие во встрече

Проведение соревнований в формате capture the flag для студентов с ограниченными возможностями здоровья

Наша Компания провела два раунда онлайн-соревнований в формате capture the flag для студентов с ограниченными возможностями здоровья. В первом из них приняли участие шесть человек, во втором — уже 12. На следующем мероприятии, которое запланировано на вторую половину текущего года, мы собираемся провести онлайн-соревнование capture the flag для ребят с ограниченными возможностями здоровья в общероссийском масштабе.

Выступление по тематике инфобезопасности для детей — участников «Кванториума» во Владивостоке

Детский технопарк «Кванториум» в городе Владивостоке сам обратился к Positive Technologies с предложением провести лекцию для детей и осветить в ней вопросы безопасности в интернете.

30
детей

стали слушателями выступления наших экспертов

Проведение мастер-класса «Как прийти в ИБ» для студентов летней школы МЭИ

Наша Компания на протяжении многих лет сотрудничает с летней «Школой молодого инженера» Московского энергетического института. Специалисты Positive Technologies читают лекции для студентов и проводят соревнования в формате capture the flag. В отчетном году мастер-класс Positive Technologies был посвящен вопросам профориентации: как студенту выбрать стажировку, компанию для работы, как пройти собеседование. В мастер-классе участвовали 15 студентов, и один из них пришел на стажировку в Компанию.

15
студентов

участвовали в мастер-классе

Обучение преподавателей вузов актуальным практикам ИБ

Наряду со студентами преподаватели вузов также нуждаются в актуальных знаниях и навыках в сфере ИБ. Специалисты Positive Technologies регулярно проводят встречи с педагогическим составом ведущих вузов. В течение 2021 года во встречах со специалистами нашей Компании приняли участие 55 преподавателей из 17 вузов по всей России.

Проект SecurityLab.ru

Мы создали и поддерживаем информационный портал SecurityLab.ru — один из самых популярных российских интернет-ресурсов по тематике кибербезопасности. На портале мы ежедневно рассказываем о событиях в области защиты информации, интернет-праве и новых технологиях.

Топ-10

самых посещаемых ресурсов для сферы ИТ

>3 млн

просмотров в месяц

>400 тыс.

пользователей

Информационный портал SecurityLab.ru

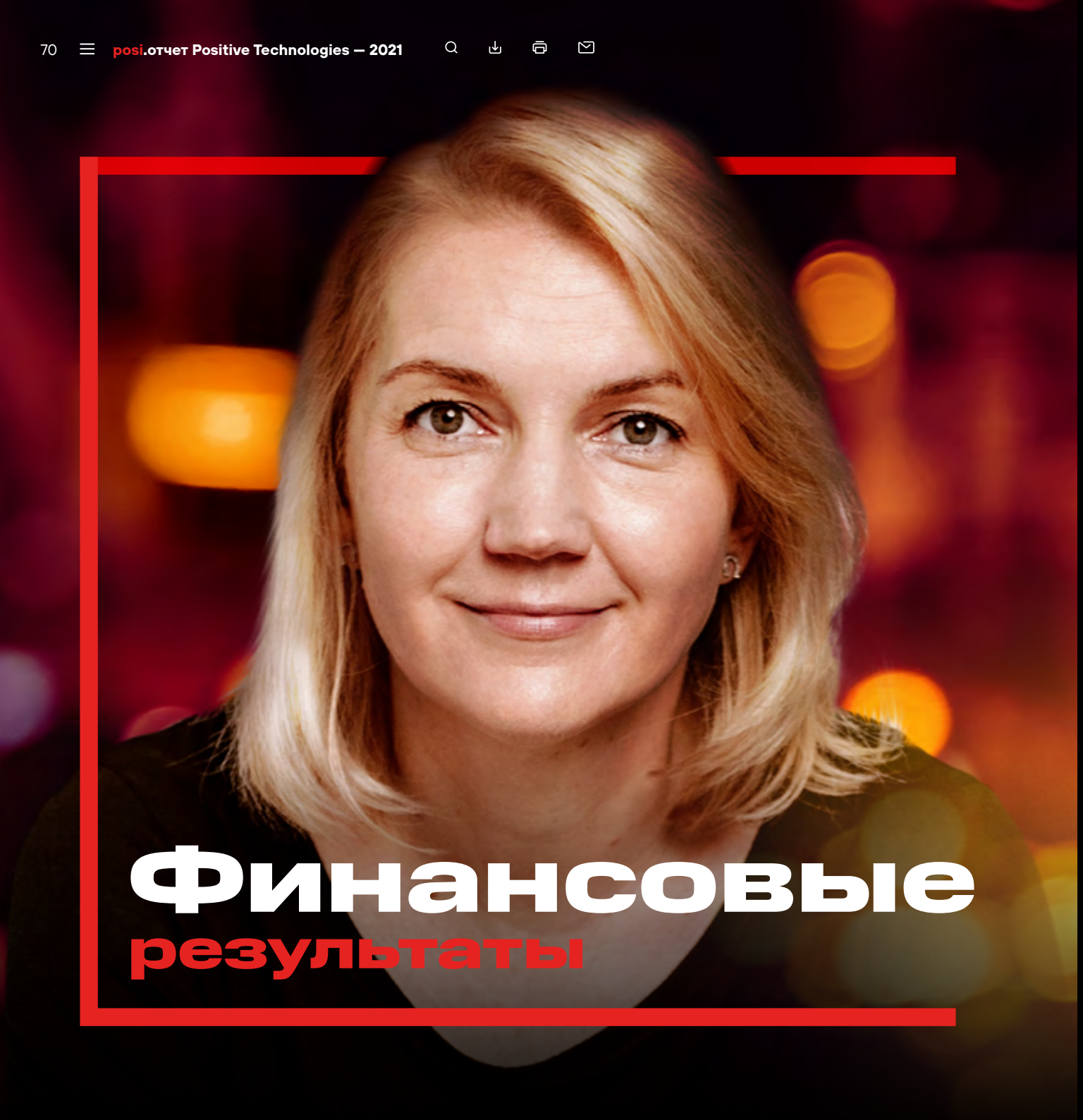
Пилотный проект по подбору персонала

Частью нашей программы развития профессионального сообщества является помощь нашим клиентам в подборе специалистов по кибербезопасности. Компания оказывает данную услугу на безвозмездной основе.

Мы заинтересованы в том, чтобы обеспечением ИБ в российских компаниях занимались высококвалифицированные профессионалы. Специалистам по кадрам в компаниях, для которых ИБ не является основным бизнесом, трудно определить профессиональный уровень кандидатов на такие узкоспециализированные вакансии, и мы готовы рекомендовать специалистов, которые в настоящее время находятся в поиске работы.

Пилотный проект по подбору персонала запущен Positive Technologies в сентябре отчетного года. За четыре месяца (с сентября по декабрь) к нам обратилось 15 организаций с запросами о подборе специалиста или целого отдела. Мы порекомендовали нашим партнерам 60 резюме для рассмотрения.

С 2022 года подбор персонала в сфере ИБ приобретает статус официальной услуги Positive Technologies, и она всегда будет оказываться вплоть до закрытия вакансии. Эта услуга останется бесплатной: нам важно, чтобы на стороне клиента работали профессионалы.



Финансовые результаты

Наш среднегодовой исторический темп роста выручки опережает рост рынка ИБ в два раза. По итогам 2021 года он составил 40%.

Основной драйвер — продажа лицензий на разработанные нами продукты и услуги в области ИБ, которые совокупно составляют 96% от общей выручки. При этом по итогам 2021 года рост лицензионной выручки составил 39%, а рост выручки от услуг в области ИБ — 32%.

Алла Макарова
Финансовый директор

Ключевые финансовые показатели

В отчетном году Компания продемонстрировала быстрый рост по всем ключевым финансовым показателям, существенно обгоняя рынок.

Динамика финансовых показателей Positive Technologies по МСФО, млн руб.

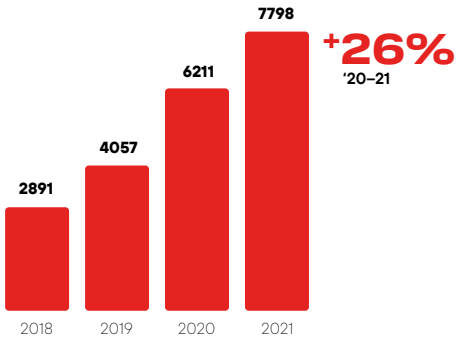
Показатель	2018	2019	2020	2021	Изменение 2021/2020, %
Выручка	2577	3451	5530	7076	28
Валовая прибыль	2192	2877	4701	6214	32
EBITDA скорр.	695	702	2169	2925	35
Чистая прибыль	318	161	1513	1914	27

[1] Данный показатель является управленческой метрикой и определяется как «Выручка за отчетный период с учетом НДС» + «Обязательства по договорам с покупателями на конец отчетного периода с учетом НДС» — «Обязательства по договорам с покупателям на начало отчетного периода с учетом НДС».

Продажи[1]

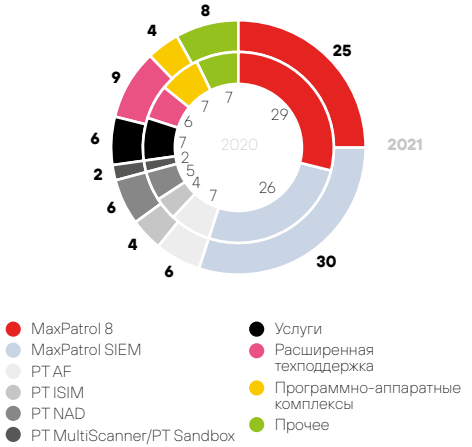
Один из ключевых показателей нашей работы — продажи, то есть валовый объем законтрактованных поставок лицензий и услуг в адрес дистрибьютора или конечного покупателя за отчетный период, включая НДС. Следует отметить, что не весь объем продаж признается в отчетном периоде, часть будет признана как выручка будущих периодов.

Продажи, млн руб.



CAGR продаж Positive Technologies в 2018–2021 годах составлял 39%, что существенно больше, чем у российского рынка кибербезопасности в целом (15–20% ежегодно). По итогам отчетного года продажи Компании составили 7,8 млрд руб., что на 26% больше результатов 2020 года.

Структура продаж продуктов, %



В сегментации продаж по портфелю продуктов больше половины объема обеспечивают MaxPatrol 8 и MaxPatrol SIEM (55% суммарно в 2021 году). При этом MaxPatrol SIEM впервые опередил наш продукт MaxPatrol 8 и вышел на первое место с долей 30%.

Вместе с тем растет диверсификация продаж за счет расширения линейки продуктов и увеличения количества продуктов на одного клиента.

Выручка и валовая прибыль

Динамика выручки и валовой прибыли в целом повторяют кривую роста продаж. CAGR выручки Positive Technologies в 2018–2021 годах составлял 40%, CAGR валовой прибыли в этот же период — 42%.

Основной рост пришелся на выручку от реализации лицензий на использование ПО, которая составила 6 млрд руб. (+39% к результатам прошлого года), и выручку от оказания услуг в области ИБ, которая составила 771 млн руб. (+32%). Снижение выручки от реализации программно-аппаратных комплексов более чем в два раза связано с концентрацией Компании на продаже ключевых продуктов и сервисов и передаче данного сегмента как непрофильного для Компании на сторону партнеров.

Уверенный рост выручки Компании, существенно превышающий темпы роста рынка в прошлом году на 15–20%, говорит о востребованности продуктов и услуг Positive Technologies и возможности дальнейшего органического роста, а также об увеличении количества продаж за счет масштабирования проектов ИБ у ключевых заказчиков и активной работе с новыми клиентами и партнерами, в том числе на фоне растущего спроса на кибербезопасность.

Увеличение валовой прибыли и валовой рентабельности — результат существенного роста выручки от реализации лицензий (+39%) и услуг в области ИБ (+32%) как более высокомаржинальных направлений бизнеса. Также влияние на валовую прибыль оказало изменение структуры себестоимости: на фоне общего несущественного роста себестоимости продаж на 3,9% снизилась себестоимость оборудования и материалов по причине снижения объемов выручки от продажи программно-аппаратных комплексов.

До 7,1 млрд руб.

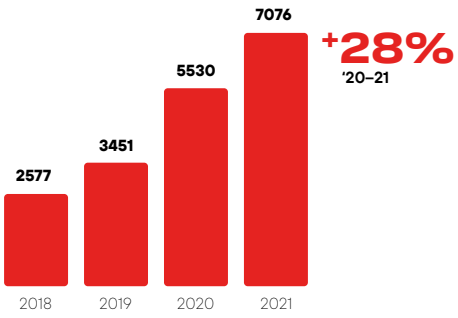
выручка Компании по итогам 2021 года выросла на 28% относительно прошлого года

6,2 млрд руб.

составила валовая прибыль по итогам 2021 года, она увеличилась на 32% относительно прошлого года

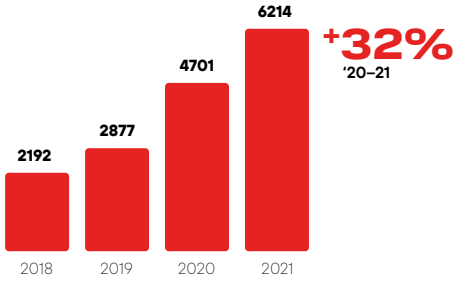
Показатель валовой рентабельности продолжил рост и увеличился до 88%, по сравнению с 85% годом ранее.

Выручка, млн руб.



Структура выручки в 2021 году, %

Валовая прибыль, млн руб.



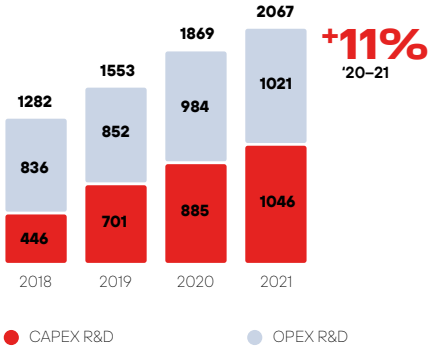
Расходы на R&D и создание нематериальных активов

Основа нашего бизнеса — производимое нами ПО. Общие расходы на R&D — сумма затрат, списываемых в расходы, и капитализируемых затрат на R&D — является наиболее адекватной метрикой активности Компании в сфере исследований и разработок. Мы капитализируем собственную разработку по каждому продукту в зависимости от стадии жизненного цикла, на котором он находится. За 2018–2021 годы средняя доля капитализируемых расходов на создание продуктов Positive Technologies составила 45% от общих расходов на R&D.

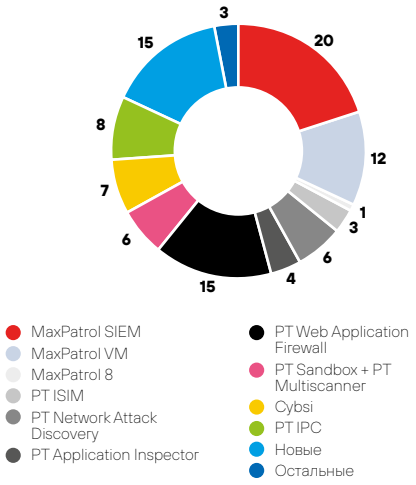
Мы активно развиваем продуктовую линейку, поэтому увеличиваем расходы на разработку: CAGR расходов на R&D в 2018–2021 годах составил 17%.

Объем капитальных затрат зависит от стадии жизненного цикла продукта. В отчетном году больше всего капитальных затрат потребовали наш самый продаваемый продукт MaxPatrol SIEM и новая разработка MaxPatrol VM.

Общие расходы на R&D, млн руб.



Структура CAPEX R&D по продуктам, %



EBITDA и чистая прибыль

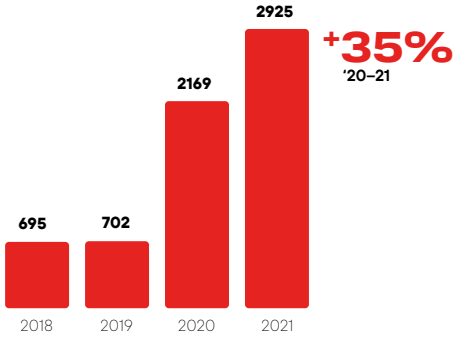
На мировом рынке кибербезопасности не так много публичных компаний имеют положительные показатели EBITDA и чистой прибыли. Молодые ИТ-компании обычно активно инвестируют в развитие, но на протяжении многих лет остаются убыточными. Зрелые игроки со сформированным продуктовым портфелем и большой клиентской базой ведут прибыльный бизнес, но уже не могут развиваться двузначными темпами. На этом фоне Positive Technologies выделяется сочетанием быстрого роста с высокой рентабельностью.

Показатель EBITDA по результатам 2021 года составил 2,7 млрд руб. и увеличился на 24% год к году. Рентабельность EBITDA составила 38% и осталась на уровне прошлого года.

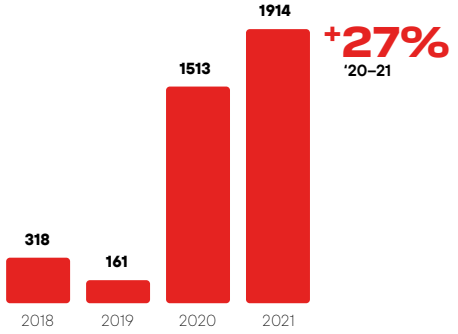
Для расчета финансовой эффективности Компания также использует показатель EBITDA, скорректированный на сумму единоразовых расходов, связанных с размещением на бирже. Скорректированный показатель EBITDA составляет 2,9 млрд руб., рентабельность по EBITDA — 41%. Это один из лучших показателей для аналогичных компаний не только в России, но и в мире.

Чистая прибыль за 2021 год составила 1,9 млрд руб. Рост по сравнению с предыдущим годом — 27%. Рентабельность по чистой прибыли осталась на высоком уровне в 27%. Традиционно в связи с характерной сезонностью выручки существенное влияние на итоговую чистую прибыль оказали результаты IV квартала.

EBITDA скорр., млн руб.



Чистая прибыль, млн руб.



При этом CAGR EBITDA (скорр.) в 2018–2021 годах достиг значения +61%, а CAGR чистой прибыли в этом же периоде +82%.

Долговая нагрузка и управление долгом

Наибольший объем выручки мы получаем в IV квартале, а наши расходы, из которых около 80% составляют затраты на персонал, равномерно распределены в течение года. В II и III кварталах мы используем заемные средства для пополнения оборотного капитала, поэтому наша задача — удовлетворить потребность Компании в ликвидности в периоды сезонного снижения выручки и дебиторской задолженности.

Объем кредитов и займов Компании на конец 2021 года составил 1957 млн руб., увеличившись на 67% по сравнению с 2020 годом.

Это произошло в связи с расширением бизнеса и, как следствие, возникновением потребности в увеличении оборотного капитала. При этом доля краткосрочных займов увеличилась с 19 до 66% в связи с более выгодными условиями по таким кредитам. 90% кредитов и займов оформлены по фиксированным ставкам, что снижает зависимость от изменения ключевой ставки. Коэффициент соотношения чистого долга к EBITDA составил 0,44, что значительно ниже среднерыночных показателей. При этом в планах Компании поддерживать данный коэффициент на комфортном уровне — не выше 1,5.

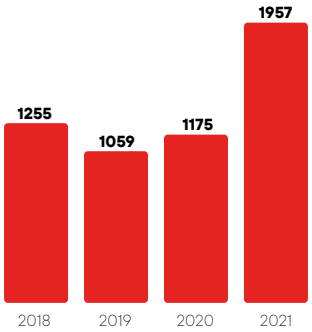
Мы работаем с несколькими опорными банками из топ-10, а также в 2020 году выпустили облигационный заем. Большинство наших кредитных линий — долгосрочные, но внутри них мы получаем транши на срок 12–18 месяцев.

0,44x

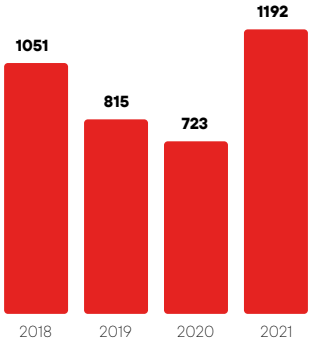
соотношение «Чистый долг / EBITDA»

Компания получает выручку в рублях, и долговой портфель полностью представлен рублевыми кредитами и займами.

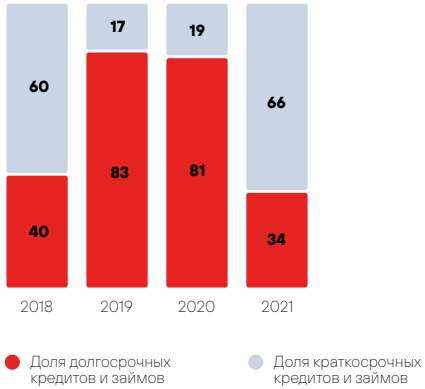
Кредиты и займы, млн руб.



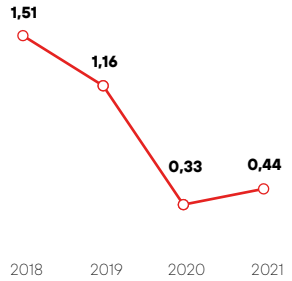
Чистый долг, млн руб.



Соотношение долгосрочных и краткосрочных кредитов и займов, %



Net Debt / EBITDA



Наши цели

2022 год открывает перед Positive Technologies новые возможности для роста. Компания ставит перед собой амбициозные финансовые цели на следующий отчетный период.

Наши минимальные ожидания по EBITDA на текущий год — 4 млрд руб., а реальная цель — удвоить показатель 2021 года. Чистая прибыль также должна вырасти, потому что наши расходы по большей части уже сформированы. Это прежде всего расходы на оплату труда. Наш штат в этом году вырастет, но увеличение фонда оплаты труда будет значительно меньше, чем та цель, которую мы ставим по росту продаж. Все это должно сыграть в нашу пользу, на увеличение нашей рентабельности, эффективности. Мы ожидаем, что по итогу года наша чистая прибыль будет не ниже 30–35% от выручки, это от 3 млрд до 5 млрд руб.

Алла Макарова,
финансовый директор

Показатель	2021	2022 (цель)
Продажи, млрд руб.	7,8	12–15
Выручка, млрд руб.	7,1	11–14
Валовая рентабельность, %	88	88–90
Скорр. показатель EBITDA, млрд руб.	2,9	4–6
Рентабельность по скорр. EBITDA, %	41	40–45
Чистая прибыль, млрд руб.	1,9	3–5
Рентабельность по чистой прибыли, %	27	30–35

Корпоративное управление

Как компания, недавно вышедшая на биржу, Positive Technologies особое внимание уделяет развитию корпоративного управления. Его структура уже претерпела серьезные изменения в связи с приобретением публичного статуса.

В 2022 году мы продолжим совершенствовать систему корпоративного управления, ориентируясь на требования регуляторов, а также на лучшие мировые и российские практики.

Марина Кан
Корпоративный секретарь

Принципы и практика корпоративного управления

Как компания, недавно вышедшая на биржу, Positive Technologies особое внимание уделяет развитию корпоративного управления. Его структура уже претерпела серьезные изменения в связи с приобретением публичного статуса. В 2022 году мы продолжим совершенствовать систему корпоративного управления, ориентируясь на требования регуляторов, а также на лучшие мировые и российские практики.

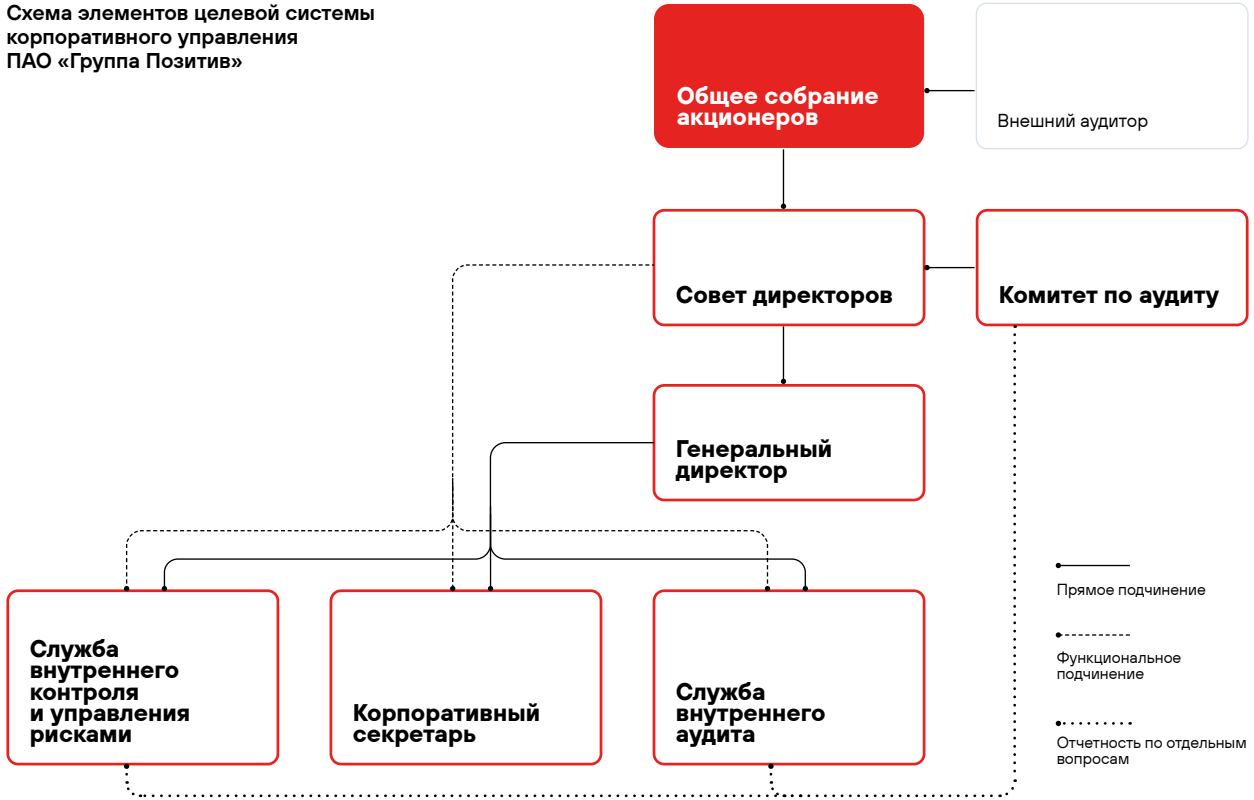
Цель корпоративного управления в Компании — построение эффективных и прозрачных взаимоотношений между акционерами, членами Совета директоров, исполнительным органом, сотрудниками и иными заинтересованными сторонами.

Компания придерживается следующих принципов корпоративного управления:

- равное отношение к акционерам и соблюдение их прав;
- информационная и финансовая прозрачность;
- подотчетность и ответственность Совета директоров и топ-менеджмента Компании перед акционерами.

Выстраивая систему корпоративного управления, Компания ставит своей целью соблюдение норм действующего российского законодательства, а также принципов Кодекса корпоративного управления, которые считает своим ориентиром для формирования наилучшей управленческой практики. В текущем году Компания провела самооценку соблюдения требований Кодекса корпоративного управления. Далее Компания, руководствуясь Положением о Совете директоров, планирует ежегодно проводить самооценку, а раз в три года — оценку с привлечением независимой организации.

Схема элементов целевой системы корпоративного управления ПАО «Группа Позитив»



Заявление Совета директоров о соблюдении Кодекса корпоративного управления

Совет директоров считает соблюдение основных принципов и рекомендаций Кодекса корпоративного управления действенным инструментом повышения эффективности управления Компанией, нацеленным на обеспечение ее долгосрочного и устойчивого развития.

В отчетном периоде оценка соблюдения принципов корпоративного управления проводилась с учетом рекомендаций, указанных в информационном письме Банка России от 27 декабря 2021 года № ИН-06-28/102 «О раскрытии в годовом отчете публичного акционерного общества отчета о соблюдении принципов и рекомендаций кодекса корпоративного управления».

Отчет о соблюдении принципов и норм Кодекса корпоративного управления приведен в приложении на сайте Компании

Меры по совершенствованию корпоративного управления в 2021 году и планы на 2022 год

Актуальная структура корпоративного управления сейчас трансформируется в связи с приобретением Компанией публичного статуса.

В отчетном году в Компании:

- избран новый состав Совета директоров, расширенный до семи членов. Два члена нового состава Совета директоров отвечают критериям независимости;
- сформирован Комитет по аудиту Совета директоров, состоящий из трех членов, два из которых являются независимыми директорами;
- избран Корпоративный секретарь;
- созданы служба внутреннего контроля и управления рисками и служба внутреннего аудита;
- разработаны и утверждены внутренние документы, регулирующие вопросы корпоративного управления. В частности, приняты Положение о Совете директоров, Положение о внутреннем аудите, Положение о Комитете по аудиту, Положение о дивидендной политике, Положение о Корпоративном секретаре, Правила внутреннего контроля по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком.

Компания в 2022 году продолжит развитие системы корпоративного управления с соблюдением норм действующего российского законодательства и принципов Кодекса корпоративного управления. Среди запланированных мер:

- актуализация действующих нормативных документов;
- разработка и утверждение новых внутренних нормативных документов, регулирующих информационную политику, вопросы организации и проведения общих собраний акционеров Компании;
- разработка плана и методологии оценки Совета директоров, закрепление их в соответствующем нормативном документе и утверждение для последующего внедрения.

Планируется унифицировать корпоративные процедуры во всей Группе компаний, а также внедрить дополнительные процедуры внутреннего контроля, работы с рисками и способами их контроля и минимизации возможных последствий.

Страница Компании на сайте «Интерфакс — Центр раскрытия корпоративной информации»

Органы управления

Наш приоритет — эффективное взаимодействие между участниками и органами управления. Согласно Уставу, органами управления Компании являются Общее собрание акционеров, Совет директоров и Генеральный директор (единоличный исполнительный орган).

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. На нем решаются вопросы об избрании Совета директоров, утверждении аудитора, о распределении прибыли (в том числе выплате дивидендов) и убытков по результатам отчетного периода. Также Компания может проводить внеочередные общие собрания акционеров.

В 2021 корпоративном году было проведено шесть общих собраний акционеров Компании, в том числе одно годовое и пять внеочередных. Все общие собрания акционеров проводились в форме совместного присутствия, решения принимались путем очного голосования. На них были рассмотрены вопросы по выплате дивидендов, избранию Генерального директора Компании, утверждению Устава и изменений к нему, утверждению внутренних документов Компании и так далее.

Общие собрания акционеров Компании в 2021 году

01.03.2021

Годовое Общее собрание акционеров, 1 марта 2021 года, протокол б/н

- Утвердить годовой отчет Компании за 2020 год.
- Утвердить годовую бухгалтерскую отчетность (финансовую) за 2020 год.
- Распределить прибыль (в том числе выплатить дивиденды) и убытки по результатам 2021 года.
- Избрать Совет директоров.
- Избрать ревизора.
- Утвердить аудитора Компании.

29.07.2021

Внеочередное Общее собрание акционеров, 29 июля 2021 года, протокол б/н

- Избрать единоличный исполнительный орган.

18.08.2021

Внеочередное Общее собрание акционеров, 18 августа 2021 года, протокол № 1

- Произвести дробление размещенных обыкновенных акций Компании[1].
- Произвести дробление размещенных привилегированных акций Компании[2].
- Внести изменения в решение о выпуске обыкновенных акций АО «Группа Позитив», связанные с изменением количества и номинальной стоимости соответствующих акций Компании в рамках дробления размещенных обыкновенных акций.
- Внести изменения в решение о выпуске привилегированных акций АО «Группа Позитив», связанные с изменением количества и номинальной стоимости соответствующих акций Компании в рамках дробления размещенных привилегированных акций.

[1] Государственный регистрационный номер выпуска 1-01-85307-H, зарегистрирован 13 ноября 2017 года на основании ст. 74 Федерального закона от 26 декабря 1995 года № 208-ФЗ «Об акционерных обществах».

[2] Государственный регистрационный номер выпуска 2-01-85307-H, зарегистрирован 13 ноября 2017 года на основании ст. 74 Федерального закона от 26 декабря 1995 года № 208-ФЗ «Об акционерных обществах».

13.09.2021

Внеочередное Общее собрание акционеров, 13 сентября 2021 года, протокол № 2

- Отменить решения о дроблении размещенных обыкновенных и привилегированных акций Компании (протокол от 18 августа 2021 года № 1).
- Внести изменения в решение о выпуске обыкновенных акций Компании, связанных с изменением количества и номинальной стоимости соответствующих акций при дроблении.
- Внести изменения в решение о выпуске привилегированных акций Компании, связанных с изменением количества и номинальной стоимости соответствующих акций при дроблении.
- Внести изменения в Устав Компании в части объема прав по привилегированным акциям.
- Внести изменений в решение о выпуске привилегированных акций Компании, связанных с изменением объема прав по привилегированным акциям.

11.10.2021

Внеочередное Общее собрание акционеров, 11 октября 2021 года, протокол № 3

- Внести в Устав АО «Группа Позитив» изменения в связи его приведением в соответствие с требованиями, установленными для публичного акционерного общества. В связи с внесением указанных изменений утвердить Устав АО «Группа Позитив» в новой редакции (редакция № 2).
- Внести в Устав АО «Группа Позитив» изменения, содержащие указание на то, что Компания является публичным акционерным обществом, посредством утверждения новой редакции Устава и утвердить Устав ПАО «Группа Позитив» в третьей редакции.
- Выплатить (объявить) дивиденды по результатам девяти месяцев отчетного года по обыкновенным акциям Компании.
- Выплатить (объявить) дивиденды по результатам девяти месяцев отчетного года по привилегированным акциям Компании.

06.12.2021

Внеочередное Общее собрание акционеров, 6 декабря 2021 года, протокол № 4

- Досрочно прекратить полномочия членов Совета директоров Компании.
- Определить количественный состав Совета директоров — 7 человек.
- Избрать членов Совета директоров Компании.
- Установить размер вознаграждения членам Совета директоров Компании за исполнение ими своих обязанностей.
- Утвердить Положение о Совете директоров.
- Внести изменение в Устав Компании (редакция № 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 действенной 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 и вознаграждения Генерального директора Компании;
- обеспечение реализации и защиты прав и законных интересов акционеров Компании;
- обеспечение полноты, точности и достоверности финансовой отчетности Компании.

Организация и руководство работой Совета директоров осуществляется Председателем Совета директоров. Он избирается большинством голосов из числа членов Совета директоров.

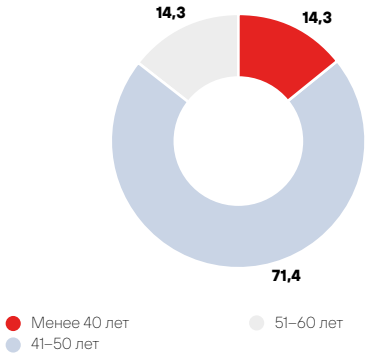
Кандидаты в Совет директоров избираются с учетом их профессиональных навыков, опыта и деловой репутации, личных качеств. В состав Совета директоров должно быть избрано не менее двух независимых директоров, то есть таких лиц, которые обладают достаточными профессионализмом, опытом и самостоятельностью для формирования собственной позиции, способностью выносить объективные и добросовестные суждения, независимые от влияния исполнительных органов Компании, отдельных групп акционеров или иных заинтересованных сторон. Критерии независимости директоров определяются в соответствии с правилами листинга Московской биржи, а также в соответствии с законодательством. Дополнительно независимость членов Совета директоров подтверждается решением Совета директоров.

Сведения о членах Совета директоров по состоянию на 31 декабря 2021 года

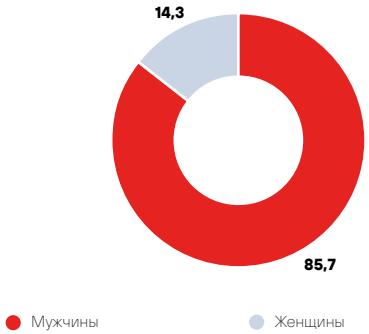
Текущий состав Совета директоров в количестве семи человек, двое из которых — независимые директора, был избран решением внеочередного Общего собрания акционеров 6 декабря 2021 года (протокол от 6 декабря 2021 года № 4) и действует до следующего годового Общего собрания акционеров. Независимость директоров, избранных в состав Совета директоров, подтверждена решением Совета директоров (протокол от 21 января 2022 года № 12). Также независимые директора вошли в состав Комитета по аудиту, один из независимых директоров стал его председателем.

Председатель Совета директоров является неисполнительным директором и мажоритарным владельцем акций Компании, он избран единогласно всеми членами Совета директоров.

Возраст членов Совета директоров,
% от общего состава



Гендерный состав Совета директоров,
% от общего состава



Среди ключевых компетенций членов Совета директоров можно выделить:

- стратегический менеджмент (разработка и внедрение стратегии);
- отраслевой опыт (опыт работы в публичных компаниях);
- ИТ, цифровизация, киберриски (опыт построения, внедрения);
- построение систем мотивации;
- управление рисками, внутренний контроль, внутренний аудит;
- аудит, финансы, контроллинг;
- операции и непрерывное совершенствование;
- опыт работы на посту Генерального директора компании (не меньше среднего бизнеса) или высших руководящих должностях (уровень CEO минус один).

Изменения в составе Совета директоров в 2021 году

С начала отчетного года до 1 марта 2021 года Совет директоров Компании работал в следующем составе (протокол годового Общего собрания акционеров Компании от 15 июля 2020 года):

- Максимов Юрий Владимирович,
- Киреев Евгений Вячеславович,
- Максимов Дмитрий Владимирович,
- Пустовой Максим Владимирович,
- Симис Борис Борисович.

1 марта 2021 года решением годового Общего собрания акционеров Компании (протокол годового Общего собрания акционеров Компании от 1 марта 2021 года) избран новый Совет директоров в составе:

- Максимов Юрий Владимирович,
- Киреев Евгений Вячеславович,
- Максимов Дмитрий Владимирович,
- Пустовой Максим Владимирович,
- Симис Борис Борисович.

6 декабря 2021 года решением внеочередного Общего собрания акционеров (протокол внеочередного Общего собрания акционеров Компании от 6 декабря 2021 года № 4) избран текущий состав Совета директоров.

Краткие биографические сведения о членах Совета директоров по состоянию на 31 марта 2022 года

47,08%
обыкновенных акций Компании на 31 марта 2022 года

Максимов Юрий Владимирович

Председатель Совета директоров

Окончил физический факультет Московского государственного университета им. М. В. Ломоносова.

С 1996 по 2004 год работал в компании «Октава+» (российском разработчике прецизионной измерительной техники), где управлял проектами в области информационных технологий и информационной безопасности. В 2002 году стал одним из основателей Positive Technologies, где с 2004 года занимал должность технического директора, а в 2007 году стал Генеральным директором. Под руководством Юрия Positive Technologies вырос до международного уровня, став одним из лидеров в области комплексной защиты крупных информационных систем от киберугроз.

3,28%
обыкновенных акций Компании на 31 марта 2022 года

Баранов Денис Сергеевич

В 2008 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 Positive Technologies пришел в 2010 году. Занимал должность специалиста, а затем руководителя в отделе 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 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.

8,74%
обыкновенных акций Компании на 31 марта 2022 года

Киреев Евгений Вячеславович

В 1987 году окончил химический факультет Московского государственного университета им. М. В. Ломоносова.

До 1991 года работал младшим научным сотрудником. С 1991 по 2001 год трудился в компании «Агама» сначала разработчиком ПО, потом техническим, а затем и генеральным директором. В 2001–2002 годах был начальником отдела разработки программного продукта в компании Golden Telecom.

Один из создателей и руководителей проекта «Апорт» (1995–2001 годы), который под управлением Евгения превратился в одну из наиболее известных и технологичных поисковых систем в России 1990-х годов.

В 2002 году совместно с Дмитрием и Юрием Максимовыми основал Positive Technologies, где занимал должности Генерального директора, директора по развитию. В настоящее время — член Совета директоров Positive Technologies. Участвовал в решении всех ключевых вопросов работы и развития Компании, на начальном этапе финансировал ее работу.

8,71%
обыкновенных акций Компании на 31 марта 2022 года

Максимов Дмитрий Владимирович

Окончил факультет электроники и системотехники Московского государственного университета леса (МГУЛ) по специальности «Вычислительные машины, комплексы, системы и сети».

Карьеру программиста начал в 1995 году в Министерстве путей сообщения России. С 1997 по 2000 год работал в крупном российском банке — программировал и занимался вопросами информационной безопасности. Увлечение информационной безопасностью подтолкнуло Дмитрия к разработке утилит для сканирования удаленных компьютеров. Набор подобных утилит в 1998 году был собран в первую версию сканера XSpider.

В 2000 году, когда серверы поисковой системы «Апорт» пострадали от взломов и руководитель проекта Евгений Киреев пригласил к сотрудничеству специалистов по информационной безопасности, среди откликнувшихся был и Дмитрий Максимов. В том же году он присоединился к команде поисковика и обеспечивал информационную безопасность проекта.

Краткие биографические сведения о членах Совета директоров по состоянию на 31 декабря 2021 года

0,02%
обыкновенных акций Компании
на 31 марта 2022 года

Рыбак Даниил Александрович

Независимый директор

В 1992 году окончил Московский институт радиотехники, электроники и автоматики (МИРЭА) по специальности «Прикладная математика», получил социологическое образование в Высшей школе социальных наук (EHESS) в Париже. Прошел ряд краткосрочных учебных программ бизнес-школ IMD, INSEAD и Stanford GSB. С 2015 по 2017 год был членом Ассоциации независимых директоров.

Партнер международной консалтинговой компании Odgers Berndtson. Занимается подбором, оценкой и развитием руководителей с 2001 года. Отраслевая экспертиза Даниила включает в себя опыт работы с крупнейшими технологическими и ИТ-компаниями, системными интеграторами, инвестиционными и коммерческими банками, фондами прямых инвестиций, международными консалтинговыми компаниями.

До прихода в Odgers Berndtson участвовал в создании и управлении компаниями в области разработки ПО, корпоративных информационных систем, систем электронной коммерции. Занимал должность советника по инвестиционной политике в крупном системном интеграторе.

С 2012 года — сертифицированный коуч руководителей высшего звена Berkeley Executive Coaching Institute. Сертифицированный эксперт по методологиям оценки руководителей высшего звена: Human Asset Review, LeaderFit, Hogan Assessment Systems, MBTI.

Присоединился к команде ПАО «Группа Позитив» в 2021 году.

Не владела
акциями Компании
на 31 марта 2022 года

Саркисян Карина Суреновна

Независимый директор

Кандидат экономических наук. Имеет степень магистра экономики по специализации «Международные валютно-кредитные и финансовые отношения» Финансового университета при Правительстве Российской Федерации. Преподаватель кафедры экономической безопасности и управления рисками факультета экономики и бизнеса того же университета. Имеет степень MBA Венского университета экономики и бизнеса (Wirtschaftsuniversität Wien) по специализации «Контроллинг и финансы».

Профессиональный опыт — более 20 лет. Работала на руководящих позициях в аудиторских компаниях «большой четверки» — «Эрнст энд Янг» и «Делойт и Туш СНГ». Последние восемь лет занимала руководящие посты в крупнейших российских компаниях: работала заместителем директора — начальником управления внутреннего контроля департамента планирования, управления эффективностью, развития инвестиций в разведке и добыче в компании «Роснефть» и директором по внутреннему контролю и комплаенсу в торговой сети «Перекресток». С 2018 года — директор по управлению рисками и внутреннему контролю «Почты России».

Ключевые направления работы: внутренний контроль, внутренний аудит, управление бизнес-рисками, оптимизация бизнес-процессов, комплаенс, проектная деятельность.

Имеет опыт внедрения требований международных бирж, включая Нью-Йоркскую, Лондонскую, Итальянскую и Гонконгскую фондовые биржи. Реализовала ряд проектов по внутреннему контролю в России, Украине, Казахстане, Нидерландах и Великобритании.

Присоединилась к команде ПАО «Группа Позитив» в 2021 году.

5,45%
обыкновенных акций Компании
на 31 марта 2022 года

Симис Борис Борисович

Окончил физико-технический факультет Московского института электронной техники.

До прихода в Positive Technologies более 10 лет работал в интеграторе «Инфосистемы Джет», где прошел путь от инженера до руководителя центра информационной безопасности.

С 2008 года отвечает за развитие бизнеса и работу с партнерами и ключевыми заказчиками в Positive Technologies. Борис — признанный эксперт ИТ-рынка: он часто выступает с докладами на профильных мероприятиях, создает специализированные курсы по системам управления ИБ, участвует в разработке отраслевых стандартов.

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. 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 соблюдение и исполнением указанных процедур.

Не владела
акциями Компании
на 31 марта 2022 года

Кан Марина Борисовна

Корпоративный секретарь

С отличием окончила Нижегородскую правовую академию по специальности «Юриспруденция». Имеет степень MBA немецкой Академии экономики и управления AFW (AFW Wirtschaftsakademie Bad Harzburg GmbH) совместно с РАНХиГС по программе «Евроменеджмент». Имеет сертификат Ассоциации по противодействию отмыванию денежных средств (ACAMS).

До прихода в Компанию работала в крупных компаниях металлургической и телеком-индустрий. В течение последних 11 лет работала в ПАО «ВымпелКом» (бренд «Билайн», в настоящее время — Veon) и АО «Компания ТрансТелеКом» (входит в холдинг ОАО «РЖД»), где занимала должности корпоративного секретаря, руководителя департамента корпоративного управления. Марина выстраивала работу совета директоров и комитетов, обеспечивала построение системы корпоративного управления и ее автоматизацию, лидировала в ключевых проектах по реструктуризации холдингов, разрабатывала систему делегирования полномочий, внутренних нормативных документов, комплексно руководила корпоративно-правовой поддержкой дочерних компаний холдинга (100+ юридических лиц, включая JV и различные юрисдикции).

Присоединилась к Positive Technologies в 2021 году после 15 лет успешной карьеры в крупных международных и российских компаниях.

Решением Совета директоров (протокол от 10 декабря 2021 года № 11) Корпоративным секретарем Компании избрана Кан Марина Борисовна.

Отчет о работе Совета директоров в 2021 году

В 2021 году Советом директоров было проведено 11 заседаний, одно из них — в заочной форме. В рамках заседаний:

- рассмотрен ряд вопросов в области внутреннего аудита, системы управления рисками и внутреннего контроля, корпоративного управления;
- принято обращение с заявлением о листинге обыкновенных акций Компании;
- утвержден проспект ценных бумаг;
- одобрена программа приобретения размещенных Компанией обыкновенных акций;
- рассмотрены рекомендации по порядку распределения прибыли и дивидендов;
- утверждена промежуточная бухгалтерская отчетность;
- рассмотрены кандидатуры для избрания в Совет директоров;
- избран Корпоративный секретарь;
- утверждены основополагающие документы: Положение о Комитете по аудиту, Положение о внутреннем аудите, Положение о Корпоративном секретаре и другие.

Участие директоров в заседаниях Совета директоров

С 01.01.2021 по 01.03.2021

Состав Совета директоров с 01.01.2021 по 01.03.2021	Участие в заседаниях / количество проведенных заседаний
Максимов Юрий Владимирович	1/1
Максимов Дмитрий Владимирович	1/1
Киреев Евгений Вячеславович	1/1
Симис Борис Борисович	1/1
Пустовой Максим Владимирович	1/1

С 01.03.2021 по 06.12.2021

Состав Совета директоров с 01.03.2021 по 06.12.2021	Участие в заседаниях / количество проведенных заседаний
Максимов Юрий Владимирович	10/10
Максимов Дмитрий Владимирович	5/10
Киреев Евгений Вячеславович	10/10
Симис Борис Борисович	10/10
Пустовой Максим Владимирович	10/10

С 06.12.2021 по 31.12.2021

Состав Совета директоров с 06.12.2021 по 31.12.2021	Участие в заседаниях / количество проведенных заседаний
Максимов Юрий Владимирович	1/1
Максимов Дмитрий Владимирович	1/1
Киреев Евгений Вячеславович	1/1
Симис Борис Борисович	1/1
Баранов Денис Сергеевич	1/1
Саркисян Карина Суреновна	1/1
Рыбак Даниил Александрович	1/1

Комитеты при Совете директоров

10 декабря 2021 года решением Совета директоров (протокол от 10 декабря 2021 года № 11) сформирован Комитет по аудиту Совета директоров, призванный содействовать эффективному выполнению Советом директоров функций контроля финансово-хозяйственной деятельности Компании. Работу Комитета регламентирует Положение о Комитете по аудиту Совета директоров.

Комитет формирует рекомендации Совету директоров по ряду вопросов и не является органом управления Компании. В частности, в функции Комитета по аудиту входят:

- контроль обеспечения полноты, точности и достоверности финансовой отчетности;
- контроль надежности и эффективности функционирования системы управления рисками и внутреннего контроля;
- обеспечение независимости и объективности внутреннего и внешнего аудита;
- контроль эффективности системы оповещения о потенциальных случаях недобросовестных действий сотрудников и третьих лиц, а также об иных нарушениях.

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

- Карина Саркисян — председатель Комитета (независимый директор);
- Даниил Рыбак — независимый директор;
- Борис Симис — член Совета директоров.

Генеральный директор

Согласно Уставу Компании, ею руководит 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 и решения соответствующих вопросов, не отнесенных к компетенции Общего собрания акционеров и Совета директоров.

С 29 сентября 2017 года по 29 июля 2021 года должность Генерального директора Компании занимал Юрий Владимирович Максимов.

Решением внеочередного Общего собрания акционеров Компании (протокол от 29 июля 2021 года) Генеральным директором Компании назначен Денис Сергеевич Баранов. Он также входит в состав Совета директоров Компании.

Вознаграждение органов управления

Согласно Положению о Совете директоров членам Совета директоров при исполнении ими обязанностей членов Совета директоров могут выплачиваться вознаграждения и компенсации в порядке и размерах, определенных решением Общего собрания акционеров. В соответствии с решением внеочередного Общего собрания акционеров Компании (протокол от 6 декабря 2021 года № 4) за исполнение членами Совета директоров Компании своих обязанностей установлен размер и порядок выплаты вознаграждений для каждого из независимых директоров — членов Совета директоров Компании, а также для каждого из независимых директоров — членов Совета директоров Компании при исполнении таким членом Совета директоров обязанностей председателя комитета Совета директоров Компании.

В 2021 году члены Совета директоров Компании не получали вознаграждение за исполнение обязанностей в Совете директоров.

Корпоративная структура Компании

ПАО «Группа Позитив»

материнская компания

Информация не раскрывается на основании Постановлений Правительства России от 4 апреля 2019 года № 400, 12 марта 2022 года № 351

100%

АО «Позитивные Технологии»

Россия

Продажа компьютерного программного обеспечения, компьютерного оборудования и оказание сопутствующих услуг

100%

ООО «Прорывные технологии»

Россия

Разработка компьютерного программного обеспечения и оказание сопутствующих услуг

100%

АО «Актив совладельцев»

Россия

Предоставление прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению

100%

ТОО «Позитивные технологии»

Казахстан

Продажа компьютерного программного обеспечения и оказание сопутствующих услуг

Управление рисками, внутренний контроль и аудит

Создание и эффективное функционирование системы внутреннего контроля и управления рисками направлены на обеспечение разумной уверенности в достижении стоящих перед Компанией целей и позволяют обеспечить надлежащий контроль за деятельностью Компании, а также ее эффективность.

Система внутреннего контроля и управления рисками в Компании построена на основе модели трех линий защиты.

Для обеспечения эффективности системы внутреннего контроля и управления рисками в Компании созданы Комитет по аудиту при Совете директоров, служба внутреннего контроля и управлениями рисками и служба внутреннего аудита.

Третья линия защиты

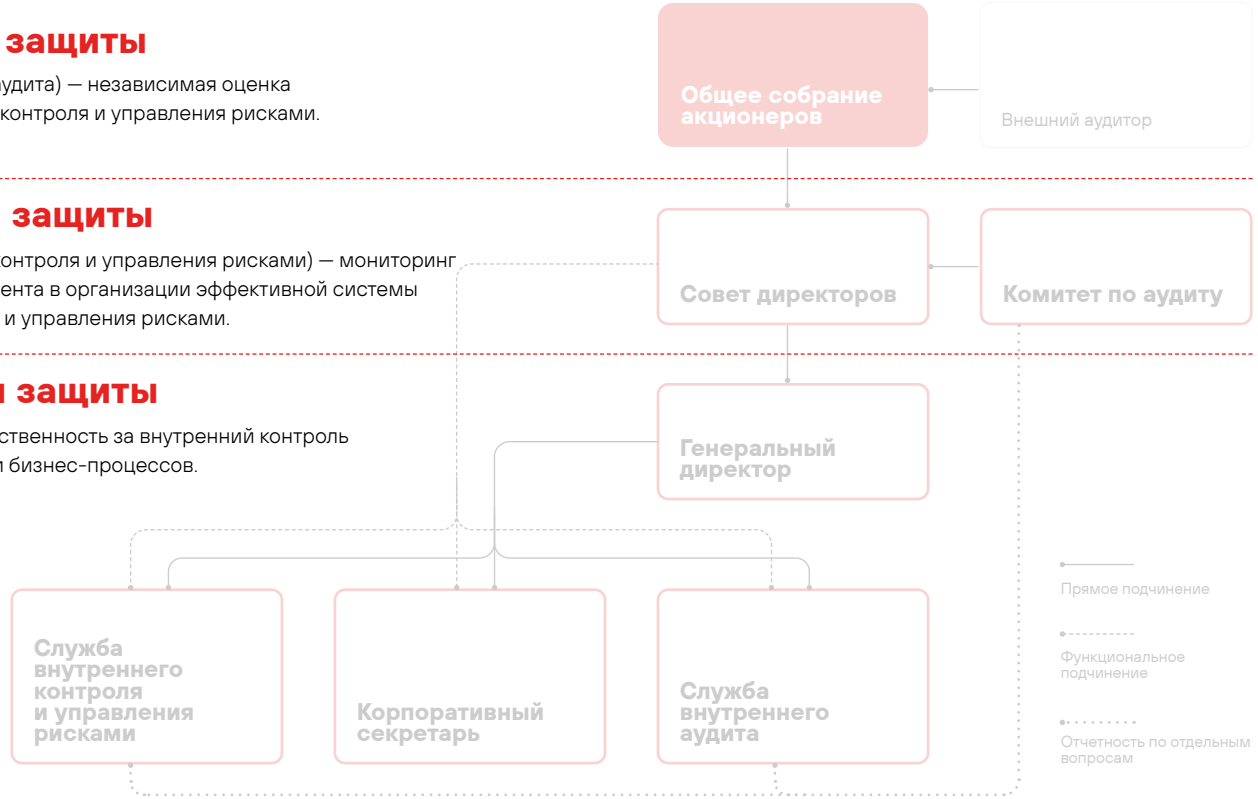
- (служба внутреннего аудита) — независимая оценка системы внутреннего контроля и управления рисками.

Вторая линия защиты

- (служба внутреннего контроля и управления рисками) — мониторинг и поддержка менеджмента в организации эффективной системы внутреннего контроля и управления рисками.

Первая линия защиты

- (менеджмент) — ответственность за внутренний контроль и управление рисками бизнес-процессов.



Комитет по аудиту

Комитет по аудиту является коллегиальным совещательным органом Совета директоров. Комитет создан в 2021 году в целях содействия эффективному выполнению функций Совета директоров в вопросах контроля финансово-хозяйственной деятельности Компании. В своей деятельности члены Комитета руководствуются действующим законодательством и Положением о Комитете по аудиту.

Функциями Комитета по аудиту являются:

- контроль обеспечения полноты, точности и достоверности бухгалтерской (финансовой) отчетности Компании;
- контроль надежности и эффективности системы управления рисками и внутреннего контроля;
- обеспечение независимости и объективности внутреннего и внешнего аудита;
- надзор за обеспечением эффективности функционирования системы оповещения о потенциальных случаях недобросовестных действий сотрудников и третьих лиц и иных нарушениях в Компании.

Комитет по аудиту состоит из трех членов:

- **Саркисян Карина Суреновна** — председатель Комитета, член Совета директоров, независимый директор;
- **Рыбак Даниил Александрович** — член Совета директоров, независимый директор;
- **Симис Борис Борисович** — член Совета директоров, исполнительный директор.

В 2022 году основной целью Комитета по аудиту является обеспечение эффективного функционирования системы внутреннего контроля и управления рисками, внутреннего аудита и внешнего аудитора и осуществление надзора за качеством их деятельности.

Служба управления рисками и внутреннего контроля

Служба управления рисками и внутреннего контроля является самостоятельным структурным подразделением Компании и действует на основании Политики по управлению рисками и Политики по внутреннему контролю. Руководитель службы функционально и административно подчиняется непосредственно Генеральному директору.

Служба управления рисками и внутреннего контроля 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 рисками совместно с владельцами бизнес-процессов;
- **анализ бизнес-процессов** и выработка требований по дизайну контрольных процедур.

В 2022 году Компания планирует развивать и совершенствовать систему управления рисками и внутреннего контроля.

Служба внутреннего аудита

Служба внутреннего аудита является самостоятельным структурным подразделением, которое действует на основании Положения 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**.

Основные цели и задачи службы внутреннего аудита на 2022 год включают:

- **формирование сильной команды** внутреннего аудита с широким спектром профессиональных навыков и глубоким пониманием бизнес-процессов;
- **развитие и совершенствование методологии** внутреннего аудита;
- **выполнение плана аудитов**, сосредоточенных на высокоприоритетных областях и адресующих существенные риски, в том числе включение пунктов ESG-повестки в план аудитов.

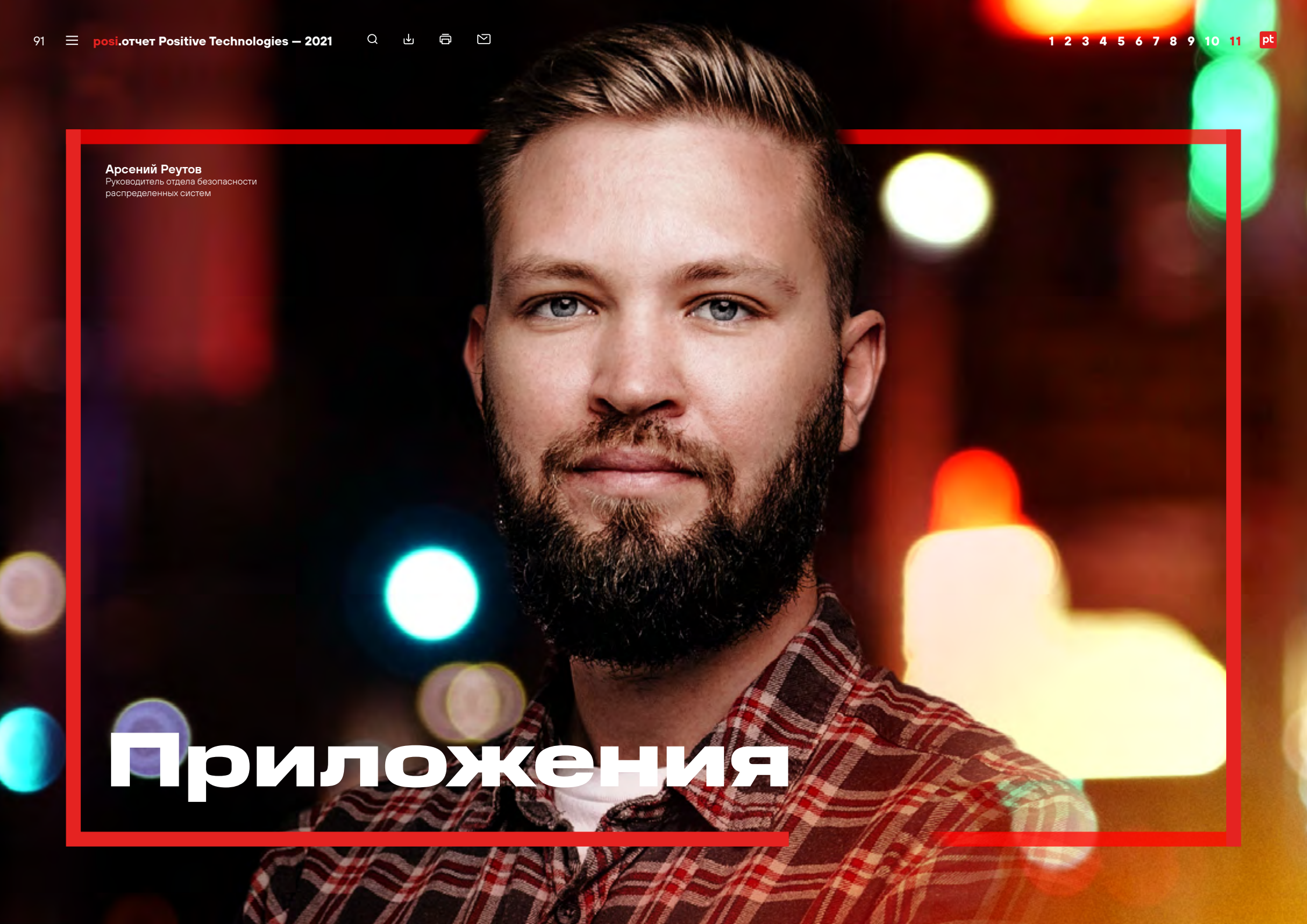
Внешний аудит

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.

Функция по формированию предложения по назначению, переизбранию и отстранению внешнего аудитора Компании возложена на Комитет по аудиту Совета директоров. Комитет рассматривает и оценивает кандидатов и вознаграждение внешнего аудитора, включая независимость и объективность, контроль соблюдения принципов оказания и совмещения оказываемых внешним аудитором услуг по аудиту и сопутствующих аудиту услуг в области ведения и подготовки бухгалтерской (финансовой) отчетности.

Внешним аудитором консолидированной финансовой отчетности Компании за 2021 год было выбрано:

АО «Юникон»
г. Москва, Варшавское шоссе, д. 125, с. 1, секция 11, 3 эт., пом. I, ком. 50.



Арсений Реутов
Руководитель отдела безопасности распределенных систем

Приложения

Об Отчете

В настоящем Отчете ПАО «Группа Позитив» (далее также — Компания, Positive Technologies) за 2021 год содержится информация о результатах деятельности ПАО «Группа Позитив» и его дочерних организаций (далее совместно — Группа), перечень которых приведен в консолидированной финансовой отчетности по МСФО за период с 1 января по 31 декабря 2021 года.

Финансовые показатели Компании рассчитаны на основании финансовой отчетности по МСФО за 2021 год, подтвержденной аудиторским заключением и приведенной в приложении к отчету. Используемые стандарты и рекомендации:

- Федеральный закон от 26 декабря 1995 года № 208-ФЗ «Об акционерных обществах»;
- Федеральный закон от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг» (с изменениями и дополнениями, вступившими в силу с 1 декабря 2021 года);
- Кодекс корпоративного управления Банка России от 10 апреля 2014 года;
- Положение Банка России от 27 марта 2020 года № 714-П «О раскрытии информации эмитентами эмиссионных ценных бумаг»;
- 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: как соответствовать лучшим практикам устойчивого развития (Московская биржа).

Данный Отчет подготовлен на основе информации, доступной Компании на дату составления Отчета.

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, содержат в себе значительную долю неопределенности.

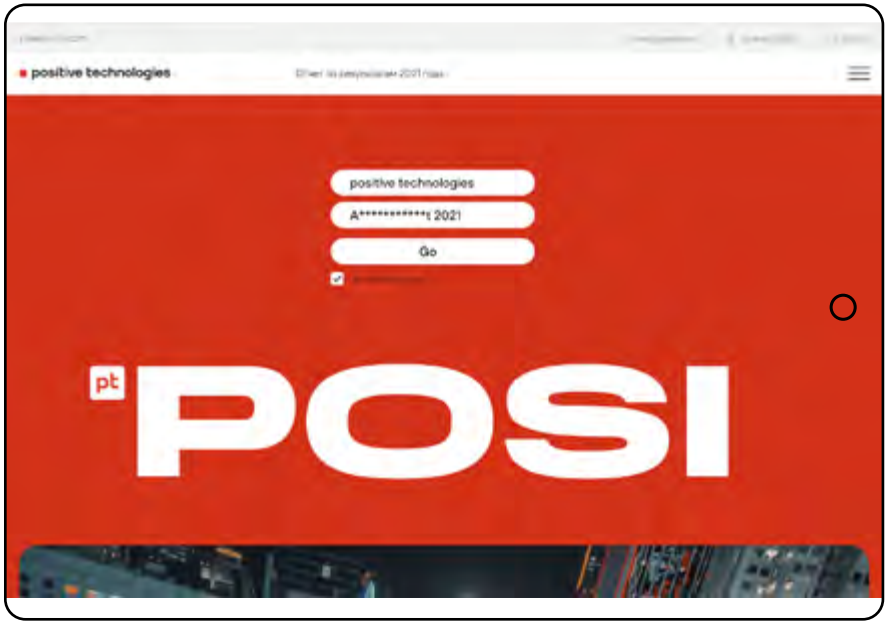
Компания не дает гарантий в отношении того, что фактические результаты ее деятельности будут соответствовать результатам или показателям, содержащимся в любых заявлениях прогнозного характера в настоящем Отчете.

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

Консолидированная отчетность по МСФО

Доступно в интерактивной версии Отчета по ссылке

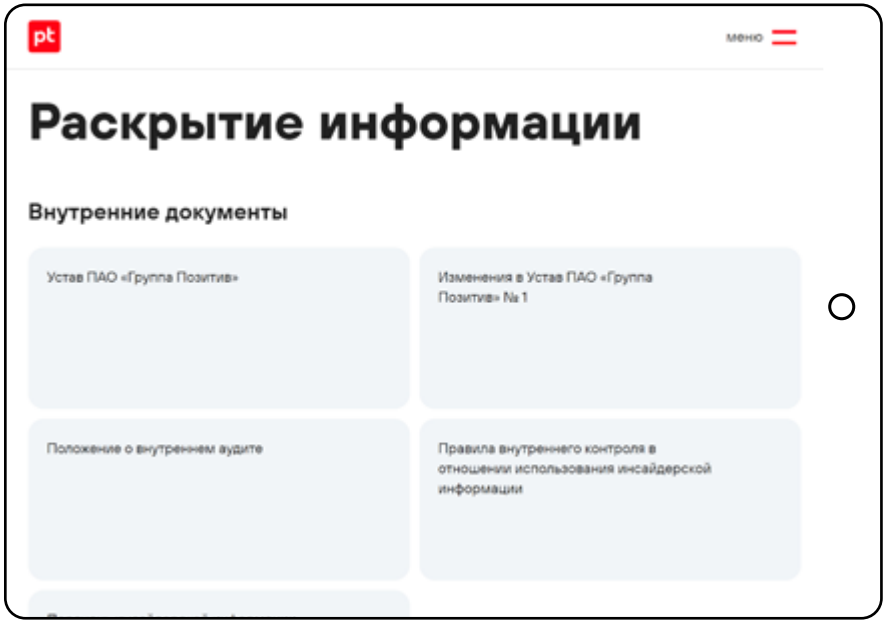
https://ar2021.ptsecurity.com/pdf/ar/ru/applications/consolidated-reporting.pdf



Раскрытие корпоративной информации

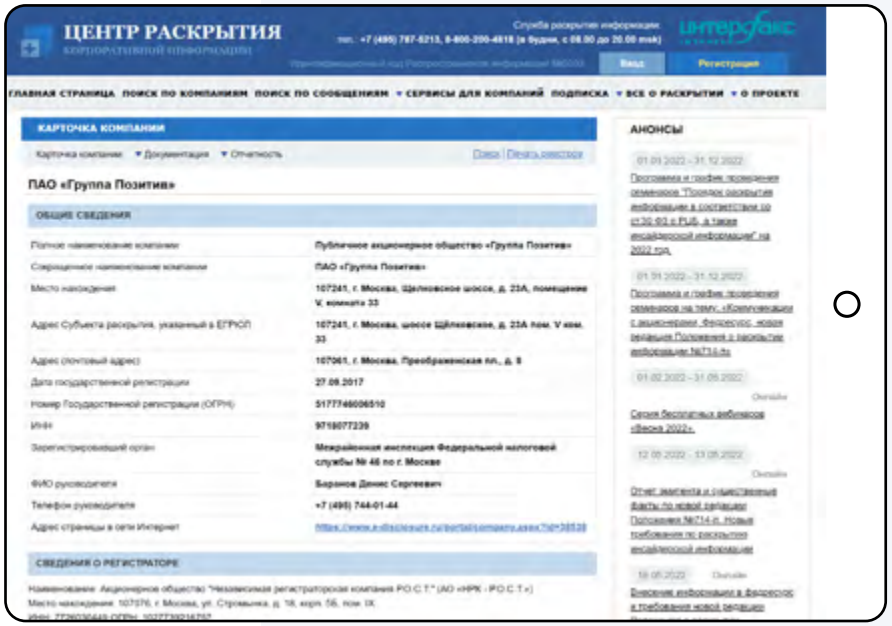
Раскрытие информации на сайте ПАО «Группа Позитив»

https://group.ptsecurity.com/ru/disclosure/



Страница Компании на сайте «Интерфакс-ЦРКИ»

https://e-disclosure.ru/portal/company.aspx?id=38538



Реквизиты и контакты

Публичное акционерное общество «Группа Позитив»

ИНН 9718077239

КПП 771801001

Юридический адрес:
107241, Москва, Щелковское ш., д. 23А, пом. V, комн. 33

Почтовый адрес:
107061, Москва, Преображенская пл., д. 8

Сайт:
https://group.ptsecurity.com/ru

Тел.:
+7 (495) 744-01-44

Контакты для акционеров и инвесторов

Отдел по связям с инвесторами

Тел.:
8-800-500-32-47

IR-contacts@ptsecutity.com
shareholder@ptsecurity.com

Юрий Мариничев
директор по связям с инвесторами

Тел.:
+7 (985) 761-84-63

ymarinichev@ptsecurity.com

Марина Кан
Корпоративный секретарь

corporatesecretary@ptsecurity.com

Мы открыты к прямому и постоянному взаимодействию с нашими акционерами, участниками рынка, профессиональными и начинающими инвесторами.

Как молодому эмитенту нам особенно важно получать обратную связь и развивать систему коммуникаций с акционерами и инвесторами.

Следите за нашими успехами и новостями
group.ptsecurity.com

ПОЗИТИВ

ПЕРВОЕ ХАЙТЕК-РАЗМЕЩЕНИЕ

ПЕРВОЕ ПРЯМОЕ РАЗМЕЩЕНИЕ

ПЕРВАЯ КИБЕРБЕЗ-КОМПАНИЯ

НА МОСКОВСКОЙ БИРЖЕ

pt

POSI