

# Управление рисками

В нашей Компании внедрена и последовательно развивается система управления рисками, основанная на проактивном подходе и ориентированная на своевременное реагирование на внутренние и внешние вызовы.

## СОКБ 53

«Лаборатория Касперского» стремится не только минимизировать последствия реализации рисков, но и предотвращать их возникновение на ранних этапах.

Принципы управления рисками разработаны с учетом требований законодательства Российской Федерации, нормативных актов Центрального Банка Российской Федерации и международных практик в области риск-менеджмента. При развитии системы Компания ориентируется на современные подходы и лучшие отраслевые стандарты в области управления рисками.

## Развитие системы управления рисками

В 2024–2025 годах «Лаборатория Касперского» активно развивала систему управления рисками (СУР), сформированную на базе процесса Global Problem Management (GPM), изначально созданного для управления технологическими рисками. В процесс были вовлечены новые подразделения и дочерние компании, разработаны удобные дашборды для регулярного мониторинга рисков и инцидентов.

## Цели и задачи управления рисками

Целями управления операционными рисками являются своевременное выявление рисков и снижение их влияния, позволяющие обеспечивать устойчивое функционирование и развитие бизнеса Компании, поддержание высокого качества ее продуктов и сервисов в условиях высокой турбулентности внешней среды.

В рамках процесса GPM Компания управляет технологическими рисками — своевременно выявляет их и ведет непрерывную работу по их снижению. Такой подход позволяет предотвращать инциденты, связанные с качеством продуктов и сервисов, а также с функционированием внутренней и внешней IT-инфраструктуры.

Ключевые задачи управления рисками:

- 1. идентификация рисков, способных существенно повлиять на Компанию или пользователей ее продуктов и сервисов;
- 2. анализ и оценка выявленных рисков;
- 3. разработка и реализация планов по минимизации рисков;
- 4. мониторинг и контроль как новых, так и ранее идентифицированных рисков, включая случаи, когда их полное устранение невозможно.

## Принципы управления операционными рисками

**Формирование рискориентированной среды**

Управление рисками является неотъемлемой частью деятельности Компании и не ограничивается функциями отдельного подразделения. Процесс GPM обеспечивает работу с рисками как внутри отдельных департаментов, так и на пересечении зон ответственности нескольких подразделений. По мере развития СУР в процесс вовлекаются новые функции и команды.

**Непрерывность и обязательность процесса управления рисками**

Процесс управления рисками продолжается непрерывно. В подразделениях, вовлеченных в GPM, назначены сотрудники, для участия в выявлении, анализе, оценке рисков и разработке планов по их минимизации. Синхронизация по новым рискам и инцидентам проводится не реже одного раза в две недели, а актуализация статусов активных рисков — не реже одного раза в квартал.

**Информирование руководителей на каждом уровне принятия решений**

В Компании действует система коммуникаций и отчетности, позволяющая своевременно информировать руководителей всех уровней об актуальной карте рисков, связанных с принимаемыми ими решениями: активных, принятых и закрытых рисках. Это создает основу для рискориентированного принятия решений.

**Открытость и единые методы оценки**

Для анализа рисков в Компании применяются единые классификаторы и шкалы оценки, закрепленные в документации по GPM и используемые всеми вовлеченными подразделениями. В случае разногласий или выявления недостатков методологии проводятся сессии фасилитации, по итогам которых классификаторы и методы оценки дорабатываются.

# Процесс управления операционными рисками

## Отчетность и обмен информацией о рисках

Чтобы способствовать принятию объективных и действенных управленческих решений, Компания внедрила многоступенчатую систему отчетности по рискам. В отчетах и дашбордах отражается динамика работы над рисками, изменение их значимости, статистика по принятым и закрытым рискам, а также выделяются наиболее критичные риски текущего периода.

Генеральный директор «Лаборатории Касперского» ежегодно получает отчет о наиболее значимых рисках и инцидентах. Ежеквартальная отчетность о рисках представляется управляющему совету. Кроме того, статус рисков и инцидентов регулярно обсуждается с руководителями департаментов, структурных подразделений и их сотрудниками.



Идентификация рисков



Отчетность и обмен информацией по рискам



Оценка и анализ рисков



Мониторинг и контроль рисков

**Идентификация** (выявление) рисков представляет собой многоплановый процесс, распределенный между различными подразделениями Компании. Риски выявляются на основе анализа произошедших инцидентов, моделирования потенциальных инцидентов и анализа бизнес-процессов. Выявленные риски анализируются и оцениваются согласно разработанным шкалам классификации, согласованным и утвержденным между всеми вовлеченными департаментами.

Каждый выявленный риск проходит **анализ и оценку** по двум ключевым параметрам: вероятности реализации и масштабу фактического или потенциального ущерба для Компании и ее клиентов. Для каждого риска определяется владелец, причины возникновения, возможные последствия, а также формируется план мероприятий по снижению риска с назначением ответственных лиц.

**Мониторинг** фактически понесенных и потенциальных потерь ведется Компанией на регулярной основе. Все инциденты фиксируются, проводится обязательная оценка ущерба, а также детальный анализ источников и причин рисков.

**Контроль** рисков в Компании носит непрерывный характер и направлен:

- на использование информации о рисках при принятии управленческих решений;
- регулярный контроль статусов активных рисков в соответствии с утвержденным процессом;
- своевременную реализацию эффективных мер по снижению рисков, способных повлиять на деятельность Компании.

# Управление ESG-рисками

За управление рисками устойчивого развития в «Лаборатории Касперского» отвечают топ-менеджеры Компании и руководители направлений. В отчетном периоде Компания выделила два существенных<sup>1</sup> ESG-риска: риск изменений в политической и экономической обстановке в регионах присутствия, изменений в законодательстве и риск роста киберпреступности.

## Ключевые ESG-риски

SASB TC-SI-550a.2

### Риск изменений в политической и экономической обстановке в регионах присутствия Компании, изменения в законодательстве

#### Почему риск важен

Возможны изменения в законодательстве, способные существенно ограничить способность Компании вести бизнес в стране/регионе присутствия

#### Меры по управлению рисками в 2024 и 2025 годах

- Постоянный мониторинг изменений в законодательстве в странах/регионах присутствия с целью оперативного выявления потенциальных рисков
- Членство Компании и отдельных сотрудников в различных отраслевых организациях для участия в коммуникации с регулируемыми органами
- Участие в публичных консультациях, проводимых органами государственной власти в странах/регионах присутствия, по проектам внесения изменений в действующее регулирование или введения нового с целью продвижения позиции Компании
- Дальнейшее развитие GTI с целью верификации надежности Компании и ее продуктов клиентами, партнерами, а также регуляторами

<sup>1</sup> Существенные риски — это риски, которые, по мнению руководства Компании, могут оказать существенное влияние на результаты деятельности.

<sup>2</sup> Аналитика и мониторинг киберугроз — сбор, анализ и интерпретация данных о существующих и потенциальных кибератаках.

### Риск роста киберпреступности

#### Почему риск важен

В нынешних условиях наблюдается снижение уровня сотрудничества между правоохранительными органами и частными компаниями в разных странах. Чтобы не допустить всплеска киберпреступности, важно сохранить сотрудничество и обмен экспертизой с частным сектором

#### Меры по управлению рисками в 2024 и 2025 годах

Компания продолжила активно сотрудничать с правоохранительными органами и международными организациями в отчетном периоде:

- внесла свой вклад в проведение ряда операций под эгидой Интерпола, в том числе [Synergia](#) и [Synergia II](#), [Serengeti](#) и [Serengeti 2.0](#), [Red Card](#) и [Secure](#);
- помогла обеспечить безопасность крупных международных спортивных мероприятий, таких как [летние Олимпийские игры 2024 года в Париже](#) и [Гран-при Сингапура в рамках чемпионата мира «Формулы-1» 2025 года](#);
- поделилась данными для двух изданий Interpol Africa Cyberthreat Assessment Report ([2024](#), [2025](#)), в которых представлен ландшафт киберугроз и атак на Африканском континенте;
- приняла участие в трех встречах экспертных рабочих групп под эгидой Интерпола, проходивших в Бангкоке, Ханое и Дохе, где поделились экспертизой в исследовании киберугроз с представителями правоохранительных органов, агентств по кибербезопасности, других государственных структур и частных компаний;
- участвовала в формировании отзывов и предложений к нескольким документам, разрабатываемым под эгидой ООН, включая Конвенцию против киберпреступности и Глобальный цифровой договор;
- подписала меморандумы о взаимопонимании с Африполем и рядом национальных регуляторов в области кибербезопасности.

## Реализовавшиеся риски

SASB TC-SI-220a.5

В отчетном периоде были зафиксированы следующие риски, реализовавшиеся в условиях геополитической нестабильности:

- прекращение сотрудничества отдельных контрагентов с «Лабораторией Касперского»;
- сложности с оплатой товаров и услуг за рубежом.

В частности, 20 июня 2024 года министерство торговли США ввело запрет на продажу и использование в стране программного обеспечения «Лаборатории Касперского». В связи с этим Компания прекратила продажи ПО и начала сворачивать операционную деятельность в стране. «Лаборатория Касперского» считает, что такое решение было принято на фоне геополитической ситуации и не основано на технической оценке продуктов. При этом Компания сохраняет возможность продавать и продвигать на территории США сервисы информирования об угрозах Threat Intelligence<sup>2</sup>, обучения по информационной безопасности (Kaspersky Threat Intelligence и Kaspersky Cybersecurity Training) и консалтинговые услуги (SOC Consulting, Security Consulting, Ask the Analyst и Incident Response).

### Планы на 2026 год

В 2026 году «Лаборатория Касперского» планирует сосредоточиться на систематизации и агрегации накопленной базы рисков, а также на дальнейшей оптимизации форматов отчетности и аналитических инструментов.