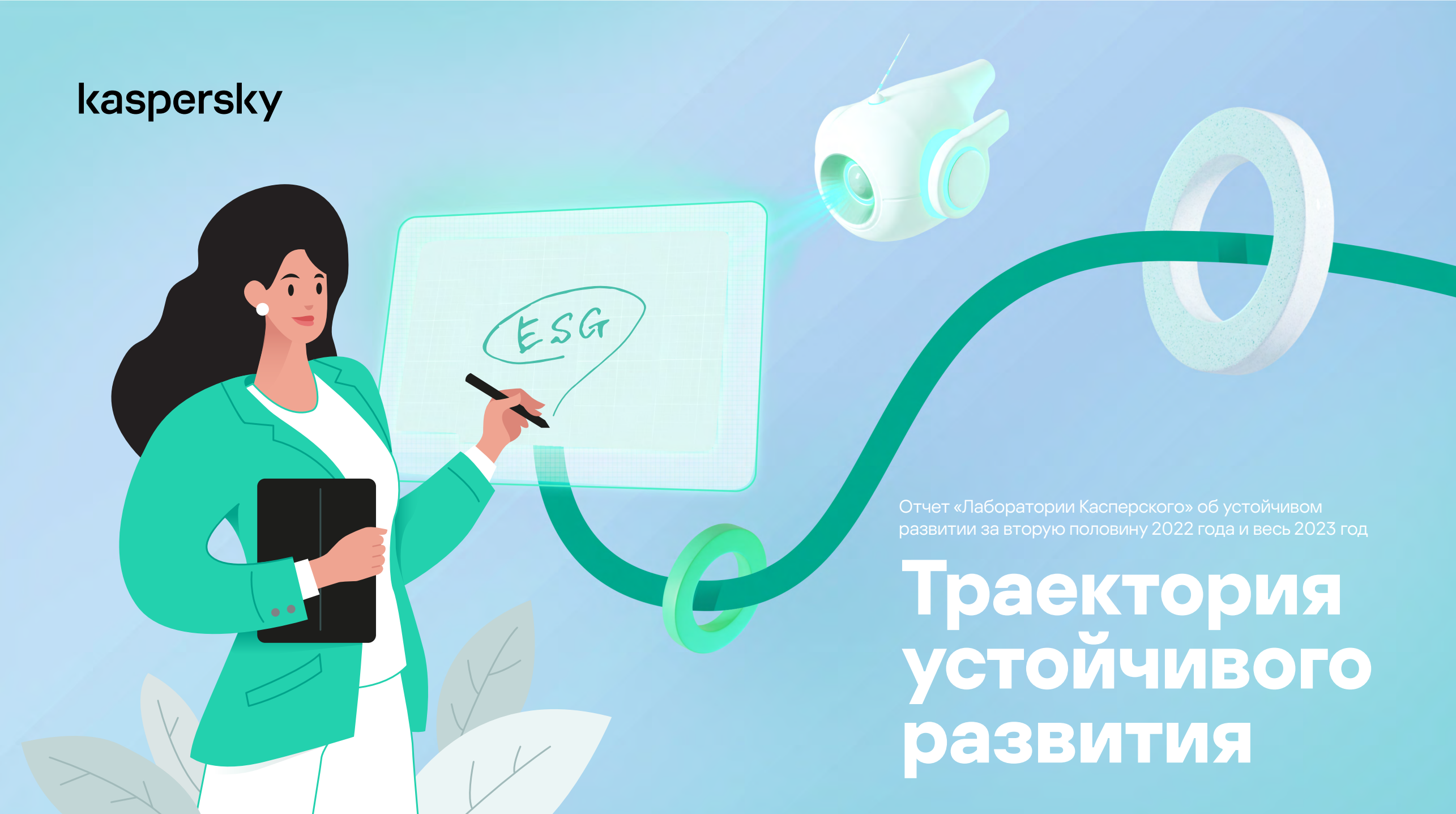
kaspersky




Отчет «Лаборатории Касперского» об устойчивом развитии за вторую половину 2022 года и весь 2023 год

# Траектория устойчивого развития

# Содержание

3 Обращение Евгения Касперского

**4 О Компании**
5 Миссия и ценности
6 География
7 Цепочка создания ценности
8 Продукты
9 Краткая история Компании
10 Ключевые достижения

**12 Устойчивое развитие**
13 ESG-стратегия
15 Управление устойчивым развитием
17 Вклад в достижение Целей устойчивого развития ООН
19 Существенные темы Отчета
21 Взаимодействие с заинтересованными сторонами
23 Устойчивая цепочка поставок
24 Соблюдение прав человека
27 Управление ESG-рисками

**28 Киберустойчивость**
29 Цифровая безопасность
47 Борьба с киберпреступностью

**55 Технологии будущего**
56 Защита промышленных предприятий и критической инфраструктуры
57 Что такое критическая инфраструктура
61 Экосистема промышленной безопасности

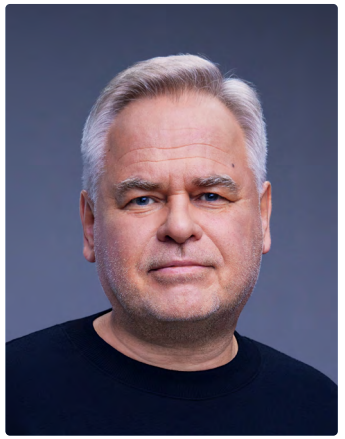
**73 Окружающая среда**
74 Управление экологическими воздействиями
75 Снижение углеродного следа
79 Использование воды
80 Управление отходами
84 Развитие экологической культуры персонала

**85 Возможности для людей**
86 Управление персоналом
90 Обучение и развитие
92 Социальная политика
93 Корпоративная культура и деловая этика
96 Безопасность труда и охрана здоровья
97 Взаимодействие с местными сообществами
103 Подготовка кадров для IT-отрасли. Наш опыт
114 Женщины в IT: сила равенства

**119 Этика и прозрачность**
120 Global Transparency Initiative
127 Защита данных
131 Охрана и защита интеллектуальной собственности
134 Корпоративное управление
137 Управление рисками

**140 Дополнительная информация**
141 Приложение 1. Об Отчете
142 Приложение 2. Участие в ассоциациях и объединениях
143 Приложение 3. К разделу «Возможности для людей»
151 Приложение 4. К разделу «Технологии будущего»
152 Приложение 5. Указатель соответствия Руководству GRI Standards
159 Приложение 6. Указатель соответствия Руководству SASB Standards
162 Приложение 7. Глоссарий
163 Приложение 8. Контактная информация

# «Каждый день мы делаем шаг к более безопасному и устойчивому цифровому миру»



**Евгений Касперский**
Генеральный директор
«Лаборатории Касперского»

Дорогие друзья!

**Перед вами второй Отчет об устойчивом развитии «Лаборатории Касперского», подготовленный по международным стандартам GRI и SASB**. Он рассказывает, что мы сделали для осуществления нашей ESG-стратегии за второе полугодие 2022 года и 2023 год. Каждый день мы сталкиваемся со все более и более разнообразными киберугрозами, и мы по-прежнему убеждены, что максимальную безопасность может обеспечить только кибериммунитет. Сегодня мы расскажем, как внедрение принципов устойчивого развития в наши бизнес-процессы помогает в этой непростой задаче.

**Уже почти 27 лет «Лаборатория Касперского» вносит значительный вклад в развитие технологий информационной безопасности**. Компания динамично развивается, успешно адаптируясь к внешним изменениям, совершенствуя свои технологии и продукты и расширяя свое присутствие на мировом рынке. На сегодняшний день наши решения используют на всех континентах и мы защищаем пользователей более чем в 200 странах и территориях. Мы предлагаем клиентам широкий спектр решений — 36 продуктов для дома и бизнеса. Региональные офисы работают более чем в 30 странах на пяти континентах. В нашей команде трудятся уже свыше 5 тысяч высококвалифицированных специалистов, а число наших корпоративных клиентов достигло 220 тысяч. Наши решения защищают как крупные индустриальные предприятия и критическую инфраструктуру, так и бизнесы любого масштаба — от крупного до малого.

**Мы привержены нашей миссии — шаг за шагом создавать безопасный и устойчивый мир**, в котором люди могут свободно пользоваться возможностями цифровых технологий для улучшения жизни. На протяжении отчетного периода «Лаборатория Касперского» активно развивала все пять ключевых направлений ESG: киберустойчивость, инновации и технологии будущего, охрану окружающей среды, заботу о сотрудниках и окружающих людях, этику и прозрачность.

**В области киберустойчивости мы продолжали разрабатывать передовые технологические решения**, способные эффективно защищать от новейших киберугроз, внедряли образовательные программы, проводили семинары и тренинги, помогали правоохранительным организациям в противодействии злоумышленникам. Наша команда обеспечивала клиентов надежными инструментами для защиты от киберпреступлений. В 2023 году наши решения помогли клиентам Компании отразить свыше 430 млн атак. 1 млрд устройств по всему миру находятся под охраной технологий «Лаборатории Касперского».

**Для защиты критической инфраструктуры «Лаборатория Касперского» разработала уникальную экосистему современных IT-технологий KOTCS**, которая позволяет защищать все уровни предприятия в одной консоли. Мы накопили многолетнюю экспертизу в области борьбы с кибератаками на промышленные объекты и успешно продолжали развивать решение KICS, продажи которого в 2023 году выросли на 54%.

**Большие усилия «Лаборатория Касперского» направила на внедрение инноваций**. Вместе с партнерами мы создали программно-аппаратную платформу нейроморфного машинного обучения, представили собственную облачную платформу кибербезопасности подключенных транспортных средств, разработали комплексный план по киберзащите АЭС на ранних стадиях создания.

**Помимо технологического прогресса, мы также нацелены на создание устойчивой и ответственной бизнес-практики**. В 2023 году «Лаборатория Касперского» отметила пятилетие глобальной инициативы по информационной открытости, которая обеспечивает прозрачность продуктов и бизнес-процессов Компании. За отчетный период мы увеличили число наших центров прозрачности до 11, открыв еще два центра — впервые на Ближнем Востоке и в Африке.

**Мы в «Лаборатории Касперского» не только добиваемся успехов в бизнесе, разрабатывая лучшие технологии, но и вносим свой вклад в защиту окружающей среды и благополучие общества в целом**. В Отчете мы рассказываем о нашей работе в области сокращения экологического следа, о том, что мы делаем для развития и благополучия наших сотрудников, а также о наших социальных и благотворительных программах.

**Новые вызовы всегда приносят новые возможности. В 2024 году мы продолжим двигаться вперед** и добиваться реализации всех наших планов. От имени Компании я хочу выразить благодарность всем сотрудникам, партнерам и клиентам за их доверие, поддержку и преданность нашим ценностям. Вместе мы сможем сделать больше и создать по-настоящему безопасное, кибериммунное будущее для всех.

# О Компании

В современном мире кибербезопасность является базовой потребностью людей, бизнеса и целых государств. С 1997 года «Лаборатория Касперского» работает для того, чтобы построить будущее, свободное от киберугроз.

GRI 2-6

«Лаборатория Касперского» — международная компания, разрабатывающая продукты и решения в области информационной безопасности и цифровой приватности. Мы стремимся сделать киберпространство защищенным и построить безопасный мир.

**1 млрд**

устройств защитила* «Лаборатория Касперского»

* Согласно данным из инфраструктуры облачных служб Kaspersky Security Network (KSN), содержащей информацию начиная с 2011 года, когда система была развернута.

**220 000**

корпоративных клиентов

**>5 000**

экспертов в команде

**36**

продуктов для дома и бизнеса

# Миссия и ценности

**Миссия «Лаборатории Касперского» —** строить безопасный и устойчивый цифровой мир, в котором люди могут использовать технологии для улучшения жизни на планете.

Реализацию своей миссии мы видим в повышении устойчивости цифрового пространства к угрозам за счет создания кибериммунитета и изначально защищенных систем. Одновременно с этим мы уделяем большое внимание социальным проектам и защите окружающей среды.

Подробнее о кибериммунитете — на с. 66

## Наши ценности

### Слушать и слышать

Наши клиенты, партнеры и команда всегда в фокусе нашего внимания. В своих решениях мы опираемся на их задачи и прислушиваемся к их потребностям. Мы обеспечиваем уровень безопасности, соответствующий самым высоким требованиям. Люди, для которых мы работаем, чувствуют нашу поддержку в любой ситуации и знают, что выбирают лучшую защиту, которая создана именно для них.

### Превосходить себя каждый день

Мы постоянно думаем, как сделать свои продукты еще лучше, и стремимся превзойти свои достижения, внедряя новые технологии и предугадывая новые угрозы.

Мы настойчиво испытываем на прочность собственные разработки и всегда находим способы еще на шаг приблизиться к совершенству. Мы никогда не стоим на месте и постоянно развиваемся, сохраняя свои ценности. Именно это раз за разом выводит эффективность наших решений на новый уровень.

### Быть сильнее трудностей

Как бы много и часто нам ни бросали вызов, мы становимся только сильнее. Мы делаем то, чего не могут другие, и решаемся на то, чего не делали раньше сами. Выделяемся, диктуем свои правила и гордимся тем, что отличает нас от остальных. Мы не ищем легких путей и простых задач, потому что умеем превращать трудности в возможности. Мы находим нестандартные решения даже в сложных ситуациях и делаем это по-своему.

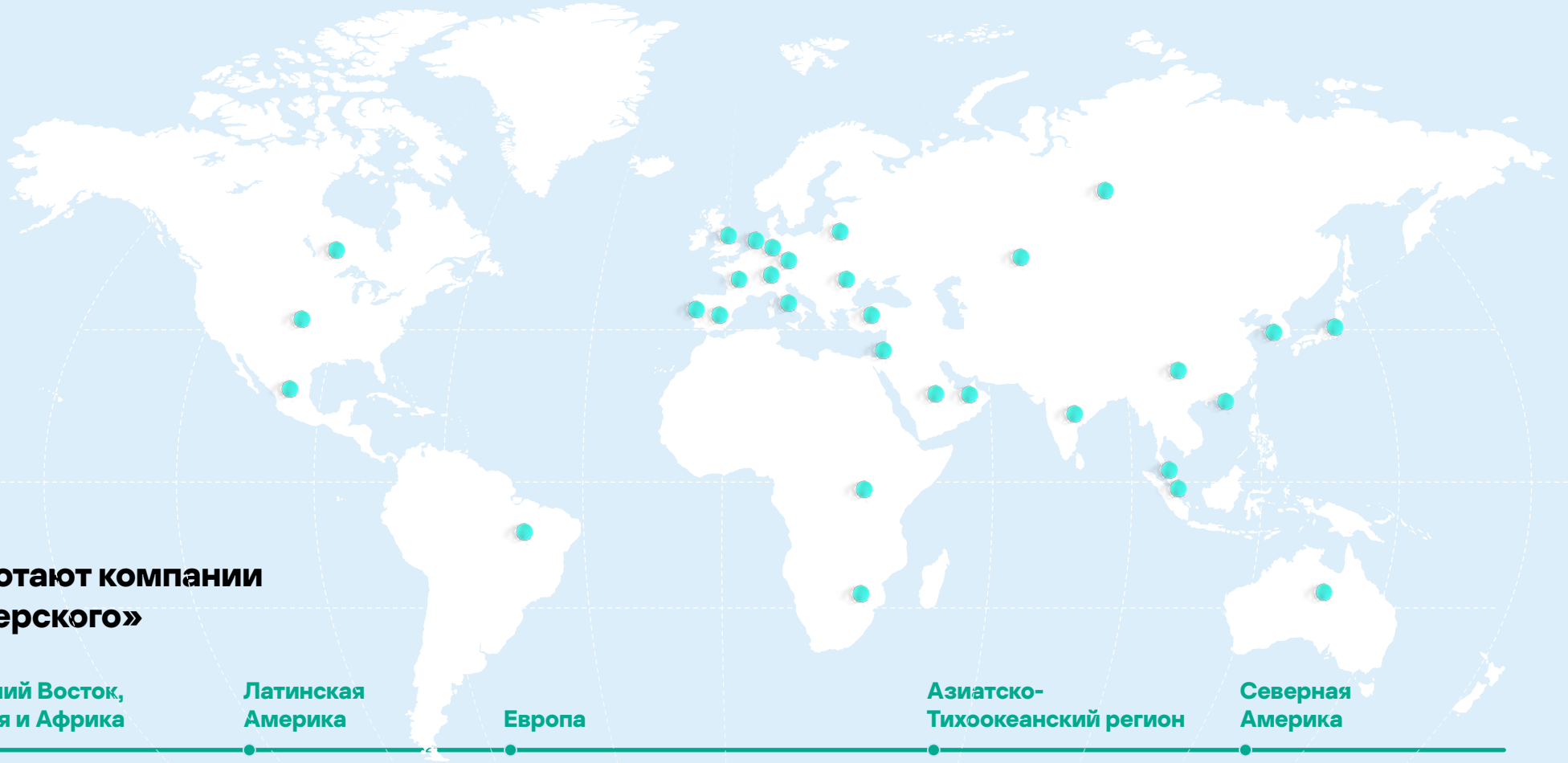
### Подтверждать лидерство

Мы ежедневно укрепляем свой лидерский статус, создавая передовые технологии, которые делают мир безопаснее. Мы никогда не перестаем работать над собой и развивать свою экспертизу. В области кибербезопасности нам нет равных: это подтверждают независимые эксперты индустрии. Клиенты, партнеры и пользователи доверяют нам. Мы, в свою очередь, считаем своим профессиональным долгом оправдывать это доверие и оставаться честными перед ними и перед самими собой.

# География

GRI 2-1

Продукты «Лаборатории Касперского» используются нашими клиентами по всему миру. Компании «Лаборатории Касперского» работают более чем в 30 странах на пяти континентах. Центр разработки программного обеспечения «Лаборатории Касперского» находится в Москве.



## В каких странах работают компании «Лаборатории Касперского»

### СНГ

- Россия
- Беларусь
- Казахстан

### Ближний Восток, Турция и Африка

- Руанда
- Саудовская Аравия
- ЮАР
- Турция
- ОАЭ

### Латинская Америка

- Бразилия
- Мексика

### Европа

- Чехия
- Германия
- Нидерланды
- Румыния
- Швейцария
- Великобритания
- Франция
- Израиль
- Италия
- Португалия
- Испания

### Азиатско-Тихоокеанский регион

- Австралия
- Япония
- Китай и Гонконг
- Индия
- Южная Корея
- Малайзия
- Сингапур

### Северная Америка

- Канада
- США

# Цепочка создания ценности

GRI 2-6

«Лаборатория Касперского» заботится о соблюдении принципов ведения социально ответственного бизнеса на всех этапах создания ценности в ходе операционной деятельности.

## Материалы и оборудование

## Операционные процессы и производство

## Дистрибуция и продажи

## Использование продукта

### Ключевые заинтересованные стороны

**Материалы и оборудование**
- Сервисные подрядчики
- Поставщики оборудования и ПО
- Партнеры
- Органы власти
- Регуляторы

**Операционные процессы и производство**
- Сотрудники
- IT-сообщество
- Органы судебной и законодательной власти
- Регуляторы
- НКО
- Пользователи

**Дистрибуция и продажи**
- Сотрудники
- Дистрибьюторы
- Реселлеры
- Предприятия
- Пользователи
- Органы власти
- IT-сообщество
- Отраслевые объединения

**Использование продукта**
- Сотрудники и их семьи
- НКО
- Школьники и студенты
- IT-сообщество
- Партнеры
- Подрядчики

- Поставщики
- Корпоративные клиенты
- Частные пользователи
- Органы власти
- Регуляторы
- Правоохранительные органы

### Воздействия

**Материалы и оборудование**
- Повышение прозрачности управления и устойчивости бизнеса.

**Операционные процессы и производство**
- Повышение прозрачности управления и устойчивости бизнеса.
- Забота о физическом и ментальном здоровье сотрудников в процессе их профессионального развития.
- Снижение воздействия на окружающую среду во всех аспектах деятельности «Лаборатории Касперского».

**Дистрибуция и продажи**
- Повышение прозрачности управления и устойчивости бизнеса.
- Снижение воздействия на окружающую среду во всех аспектах деятельности «Лаборатории Касперского».

**Использование продукта**
- Исключение утечек данных пользователей «Лаборатории Касперского».
- Повышение доверия пользователей, клиентов и других заинтересованных сторон к «Лаборатории Касперского».
- Защита пользователей от киберугроз с помощью продуктов и инициатив Компании.
- Защита критической инфраструктуры с помощью создания современных IT-технологий и сервисов.

- Содействие в расследованиях киберпреступлений международным и национальным правоохранительным организациям.
- Достижение гендерного равенства в IT.
- Подготовка кадров для кибербезопасности и повышение профессионального уровня IT-специалистов.

# Продукты

## Технологии «Лаборатории Касперского» защищают от киберугроз наших клиентов – частных лиц и компании – вне зависимости от масштабов их бизнеса.

GRI 2-6

В портфеле Компании – 36 продуктов информационной безопасности для дома и бизнеса[1]. В 2013–2023 годах продукты «Лаборатории Касперского» приняли участие в 927 независимых тестированиях и обзорах. В 680 случаях они заняли первое место, в 779 – вошли в тройку лучших.

Решение Kaspersky Endpoint Security Cloud продемонстрировало высокую эффективность в борьбе с программами-вымогателями и превзошло продукты десяти других вендоров в тестировании AV-TEST. Решение Kaspersky EDR Expert показало 100%-ную эффективность против таргетированных атак в исследованиях SE Labs Enterprise Advanced Security (EDR) 2022 и 2023 годов, а также дважды получило высокий рейтинг Strategic Leader по результатам тестов AV-Comparatives Endpoint Prevention and Response 2022 и 2023 годов. Решение Kaspersky Standard из новой линейки для защиты домашних пользователей получило награду «Продукт года» от AV-Comparatives за 2023 год.

[1] В перечень продуктов включены защитные решения, представленные на сайтах kaspersky.ru и kaspersky.com. Данные продукты предоставляются по большому количеству лицензий, удовлетворяющих потребностям различных клиентов (всего более 1500 позиций в прайс-листе Компании).

**36** продуктов
в портфеле Компании

**680** раз
наши продукты заняли первое место в независимых тестированиях в 2013–2023 годах

**779** раз
наши продукты вошли в тройку лучших в 2013–2023 годах

### Продукты для дома:

Kaspersky Standard
Kaspersky Plus
Kaspersky Premium

Подробнее о продуктах для дома

### Продукты для бизнеса:

Kaspersky Small Office Security
Kaspersky Endpoint Security
Kaspersky Container Security
Kaspersky EDR
Kaspersky XDR
Kaspersky Industrial CyberSecurity

Подробнее о продуктах для бизнеса

### Решения на KasperskyOS:

KasperskyOS SDK для IoT-контроллеров
Kaspersky Automotive Secure Gateway
Kaspersky IoT Secure Gateway
Kaspersky Thin Client

Подробнее о решениях

# Краткая история Компании

За более чем 25 лет работы «Лаборатория Касперского» внесла огромный вклад в развитие технологий информационной безопасности, которыми пользуются частные лица, компании и государственные органы в России и более чем в 200 странах по всему миру.

**1989** Евгений Касперский обнаруживает на рабочем компьютере Olivetti M24 вирус под названием Cascade.1704 и создает свой первый инструмент для удаления вирусов.

**26 июня 1997 года**

День основания «Лаборатории Касперского»

**1999** Открытие первого офиса Компании за рубежом – в Великобритании.

**2001** Разработанное Компанией антивирусное ПО для портативных устройств Kaspersky Anti-Virus поставляется в Россию с карманными компьютерами Palm, Handspring, Sony.

**2003** «Лаборатория Касперского» открывает офисы в Японии, Германии, Франции, Испании, Италии и Китае.

**2004** «Лаборатория Касперского» становится первым в мире разработчиком антивирусного программного обеспечения, который обновляет свои антивирусные базы каждый час.

Начинает работу офис Компании в США.

**2007** Компания представляет линейку продуктов для бизнеса Kaspersky Open Space Security.

**2008** Появляется глобальный центр исследования и анализа угроз (GReAT).

**2009** «Лаборатория Касперского» проводит Security Analyst Summit, первую конференцию для исследователей и аналитиков ИБ со всего мира.

**2009** Компания становится спонсором экспедиции в Антарктику. В дальнейшем «Лаборатория Касперского» выступает спонсором еще двух антарктических экспедиций и экспедиции «7 вулканов».

**2013** Компания начинает сотрудничество с Интерполом.

**2016** «Лаборатория Касперского» совместно с Европолом и Intel Security запускают инициативу No More Ransom, к которой вскоре присоединяются десятки государств и компаний — разработчиков ИБ.

**2017** Компания выпускает собственную безопасную операционную систему KasperskyOS, защищенную от любых, в том числе неизвестных, угроз.

**2018** «Лаборатория Касперского» запускает глобальную инициативу по информационной открытости (Global Transparency Initiative).

Открывается первый Центр прозрачности в Цюрихе (Швейцария).

**2019** Компания проходит ребрендинг и формулирует миссию: «Строим безопасный мир».

Центры прозрачности открываются в Испании, Малайзии и Бразилии.

**2020** Во время пандемии «Лаборатория Касперского» бесплатно передает лицензии на основные продукты медучреждениям по всему миру.

Центр прозрачности открывается в Канаде.

**2021** «Лаборатория Касперского» открывает доступ к Software Bill of Materials (SBOM), помогая клиентам и партнерам понять, что находится внутри ее продуктов и программного обеспечения.

Компания завершает сделку с Brain4Net и получает новый импульс для развития своей XDR-платформы.

«Лаборатория Касперского» продолжает стратегию по диверсификации бизнеса и инвестициям в перспективные IT-направления, увеличив долю в капитале «МойОфис» и купив акции разработчика решений для автоматизации HR-процессов ForPeople.

Компания также стала акционером компании «Мотив НТ» с долей участия 15%, с которой продолжила работу над созданием первого в России нейроморфного процессора.

**2022** Товарный знак Kaspersky Cyber Immunity® зарегистрирован в Евросоюзе.

**2023** Центры прозрачности открываются в Саудовской Аравии и Руанде.

# Ключевые достижения

**+51%**
продажи продуктов в России в 2022 году

**+8%**
продажи в сегменте[1] B2B по всему миру в 2022 году

**+23%**
мировые продажи в сегменте крупного бизнеса в 2022 году

**+54%**
мировые продажи Kaspersky Industrial CyberSecurity в 2022 году

## Важнейшие события отчетного периода

### Расширение бизнеса

- Компания продолжила открывать новые центры прозрачности. В 2022 году они появились в Италии и Нидерландах. В 2023 году были открыты первые центры прозрачности на Ближнем Востоке – в Королевстве Саудовская Аравия – и в Африке – в Руанде.
- «Лаборатория Касперского» приобрела 49% акций компании ForPeople, разработчика решений для автоматизации HR-процессов, и 49%-ную долю в ООО «Ксими ПРО», разработчике решений по контейнерной безопасности.

### Инновации

- «Лаборатория Касперского» совместно с «Мотив-НТ» представила программно-аппаратную платформу нейроморфного машинного обучения Kaspersky Neuromorphic Platform (KNP). Она предназначена для обучения нейронных сетей, исследований в области нейроморфного искусственного интеллекта (ИИ), создания и запуска решений на основе систем ИИ следующего поколения.
- «Лаборатория Касперского» и ГК «ТОНК» анонсировали коммерческий запуск первого кибериммунного тонкого клиента. С его помощью компании могут строить управляемую и функциональную инфраструктуру тонких клиентов на базе кибериммунной операционной системы KasperskyOS для защищенного подключения к инфраструктуре виртуальных рабочих столов (VDI). Для развития технологий тонкого клиента подписаны соглашения о сотрудничестве с ГК «ТОНК», Centerm, TSplus и ASWANT.
- «Лаборатория Касперского» совместно с ФГУП «НАМИ» и АО «ГЛОНАСС» представили первую в России облачную платформу кибербезопасности подключенных транспортных средств.
- «Атомэнергопроект» и «Лаборатория Касперского» разработали комплексный план по кибербезопасности, учитывающий самые строгие требования к безопасности объектов использования атомной энергии на самых ранних стадиях создания АЭС поколения 3+.
- «Лаборатория Касперского» заключила партнерство с компанией ASWANT для развития экосистемы кибериммунитета в Малайзии и Индонезии.
- «Лаборатория Касперского» и TSplus подписали соглашение о партнерстве. Компании будут поставлять кибериммунные решения для удаленных рабочих мест.

### Патенты и стандарты

- «Лаборатория Касперского» зарегистрировала в Евросоюзе товарный знак Kaspersky Cyber Immunity®. Действие знака распространяется на всю территорию Евросоюза.
- С апреля 2023 года введены в действие два национальных стандарта (ПНСТ) на системы с разделением доменов, разработанные «Лабораторией Касперского» и принятые ТК 194 «Киберфизические системы». Они определяют базовые понятия и основные архитектурные принципы, заложенные в системы с разделением доменов, в том числе в KasperskyOS.

### Международное сотрудничество

- «Лаборатория Касперского» оказала поддержку Интерполу, предоставив данные о киберугрозах в рамках операции Africa Cyber Surge II. Эта информация позволила выявить скомпрометированную инфраструктуру и задержать 14 подозреваемых в киберпреступлениях по всему Африканскому региону.
- Олимпийский комитет Катара использует продукты «Лаборатории Касперского» для обеспечения кибербезопасности.
- UAE Cyber Security Council и «Лаборатория Касперского» подписали меморандум о взаимопонимании, в рамках которого будет вестись обмен информацией о выявлении и расследовании киберинцидентов, а также своевременном реагировании на возникающие киберугрозы.

[1] Рост по сравнению с прошлым годом в цифровых сегментах МСП, крупного бизнеса и B2B. Все сегментные и региональные показатели отражают чистые продажи, а не выручку, и представлены в фиксированных ставках по состоянию на 2022 год. Рост в 2022 году представлен по сравнению с 2021 годом.

# Награды и признание

Наши разработки получают высокую оценку независимых экспертов и завоевывают награды в престижных международных конкурсах.

## 2022

В 2022 году продукты «Лаборатории Касперского» приняли участие в 86 независимых тестах и обзорах. Они 69 раз занимали первые места и 73 раза попадали в тройку лидеров. 85% этих продуктов Компании вошли в топ-3 в своей категории.

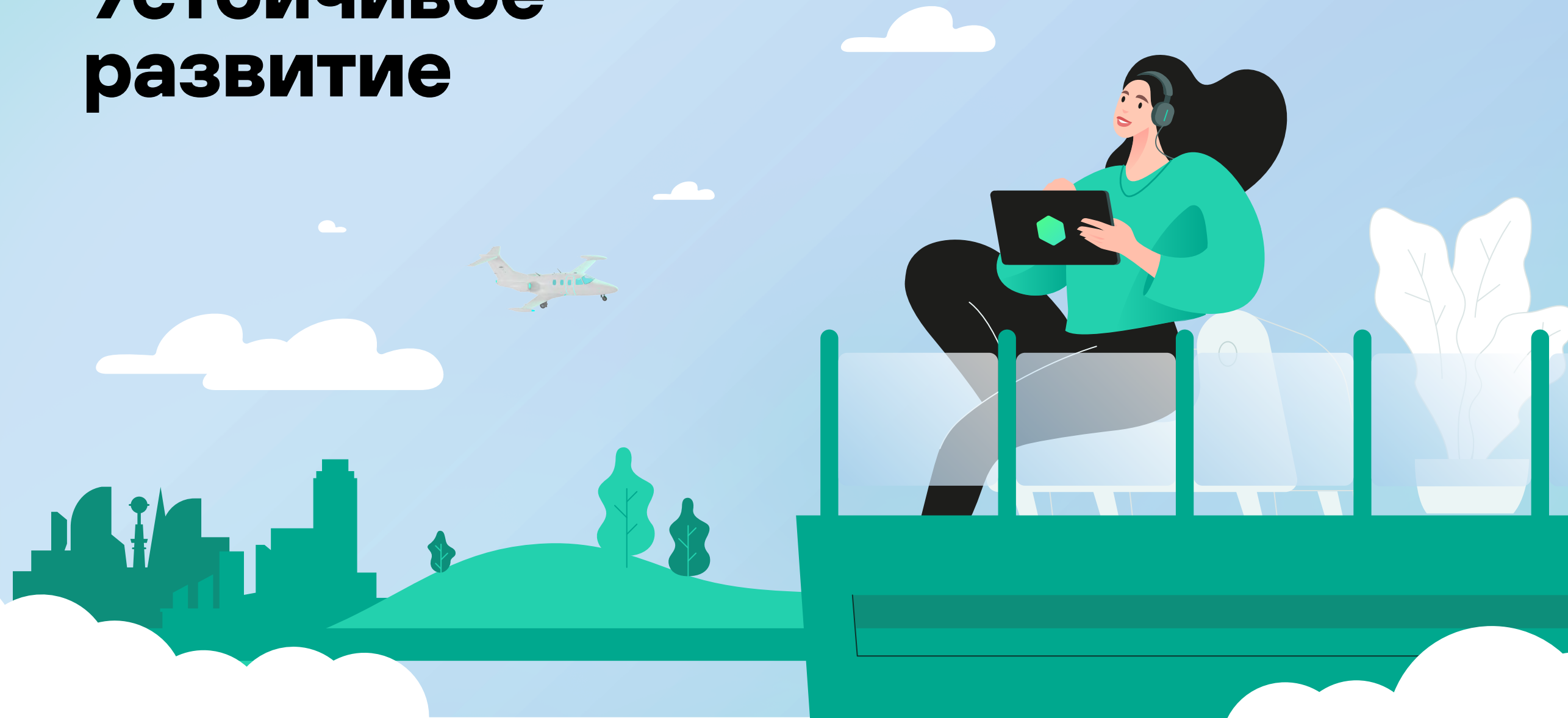
- «Лаборатория Касперского» признана лидером в области безопасности конечных точек по версии международной платформы G2 Crowd.
- Решение Kaspersky EDR Expert отразило 100% кибератак в ходе международного теста SE Labs.
- Решение Kaspersky Endpoint Detection and Response Expert получило статус стратегического лидера в результате всестороннего тестирования, проведенного австрийской компанией AV-Comparatives.
- «Лаборатория Касперского» стала лидером на глобальном рынке решений MDR по версии Quadrant Knowledge Solutions.
- Решение Kaspersky Secure Remote Workspace получило награду на World Internet Conference в Китае.

## 2023

В течение 2023 года решения «Лаборатории Касперского» 94 раза вошли в тройку лидеров по результатам 100 независимых тестирований защитных технологий, в том числе 93 раза заняли первые места.

- «Лаборатория Касперского» успешно прошла аудит Service and Organization Controls второго типа (SOC 2 Type 2) — всемирно признанного стандарта отчета для системы управления рисками кибербезопасности.
- Kaspersky Safe Kids в седьмой раз подряд получил сертификат качества от независимой лаборатории AV-TEST.
- «Лаборатория Касперского» стала лидером на глобальном рынке управляемых сервисов по версии консалтинговой компании Quadrant Knowledge Solutions.
- Решение Kaspersky Internet Security в 12-й раз подряд получило ежегодную награду от AV-Comparatives.
- Международная исследовательская компания IDC назвала «Лабораторию Касперского» вендором, определившим 2022 год в области защиты конечных устройств.
- Решения Kaspersky Security для бизнеса, Kaspersky Small Office Security и Kaspersky Internet Security продемонстрировали 100%-ную защиту от программ-вымогателей в ходе тестирования лабораторией AV-TEST.
- Решения «Лаборатории Касперского» отразили 100% атак в ходе международного теста SE Labs.
- Решение Kaspersky Security для бизнеса показало 100%-ную эффективность против попыток несанкционированного вмешательства в свою работу по итогам теста независимой лаборатории AV-Comparatives.
- Решение Kaspersky EDR Expert второй год подряд получило максимальную оценку по показателю Total Accuracy Rating по итогам тестирования SE Labs Enterprise Advanced Security решений класса EDR.
- Тренинги по цифровой грамотности Kaspersky Security Awareness названы лидером в отчете аналитической компании SoftwareReviews.
- Решение Kaspersky Automotive Secure Gateway получило награду на World Internet Conference в Китае.
- Независимая тестовая лаборатория AV-Comparatives назвала новый Kaspersky Standard «Продуктом года». Это наивысшая оценка, присуждаемая авторитетной независимой организацией, специализирующейся на тестировании защитных решений.

# Устойчивое развитие

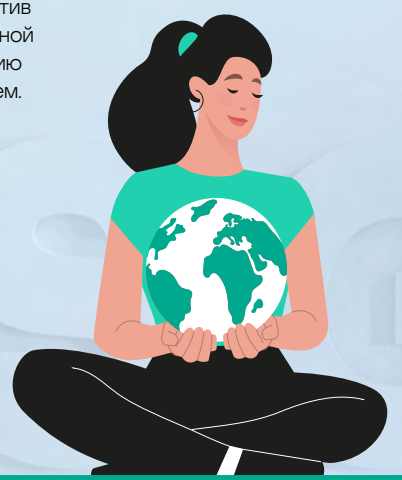


# ESG-стратегия[1]

Базовые принципы и задачи деятельности «Лаборатории Касперского» неразрывно связаны с ESG-целями: мы строим устойчивый цифровой мир, в котором могут безопасно жить и взаимодействовать частные лица, бизнес и общество.

GRI 2-22

«Лаборатория Касперского» выделила пять ключевых стратегических направлений деятельности, которые определяют наш подход к решению вопросов устойчивого развития. Они задают направление основных ESG-инициатив Компании по обеспечению безопасной цифровой среды, а также по решению экологических и социальных проблем.



## Стратегические приоритеты в области устойчивого развития

### Окружающая среда

- Уменьшение воздействия на окружающую среду: инфраструктура, бизнес-операции, продукты

### Технологии будущего

- Кибериммунитет для новых перспективных технологий

### Возможности для людей

- Забота о сотрудниках
- Женщины в STEM[2]
- Инклюзивность и доступность технологий
- Развитие кадров для IT

### Киберустойчивость

- Защита критической инфраструктуры в турбулентном мире
- Помощь в расследовании киберпреступлений по всему миру
- Защита пользователей от киберугроз

### Этика и прозрачность

- Прозрачность кода и процессов
- Защита данных и права на частную жизнь
- Прозрачность управления и устойчивость бизнеса


1 ESG-стратегия (environmental, social, governance) — экологическая, социальная и управленческая стратегия.

2 STEM (Science, technology, engineering, and mathematics) — это широкий термин, который используется для обозначения технических дисциплин (наука, технологии, инженерия и математика).

# # Цели

### Киберустойчивость

- Защищать пользователей от киберугроз с помощью продуктов и инициатив «Лаборатории Касперского».
- Защищать промышленность и критическую инфраструктуру с помощью экосистемы современных IT-технологий и сервисов.
- Содействовать в расследованиях киберпреступлений международным и национальным правоохранительным организациям для обеспечения безопасности пользователей.

### Технологии будущего

- Подключать новых партнеров к реализации стратегии кибериммунитета.

### Окружающая среда

- Снижать воздействие на окружающую среду во всех аспектах деятельности «Лаборатории Касперского».

### Возможности для людей

- Заботиться о физическом и ментальном здоровье сотрудников в процессе их профессионального развития.
- Способствовать достижению гендерного равенства в IT.
- Готовить кадры для кибербезопасности и повышать профессиональный уровень IT-специалистов.
- Повышать доступность продуктов, сервисов и возможностей информационной безопасности для людей с ограниченными возможностями здоровья.

### Этика и прозрачность

- Повысить прозрачность управления и устойчивость бизнеса.
- Выполнить требования нормативных актов по защите персональных данных и исключить утечки персональных данных пользователей «Лаборатории Касперского».
- Повысить доверие пользователей, клиентов и других заинтересованных сторон к «Лаборатории Касперского».

**GRI 2-23**

В реализации своих обязательств в области соблюдения прав человека Компания руководствуется принципами Глобального договора ООН и опирается на Резолюцию Генеральной Ассамблеи ООН о целях устойчивого развития, принятую в 2015 году, Парижское соглашение от 12 декабря 2015 года, Международный билль о правах человека, включающий Всеобщую декларацию прав человека, Конвенцию о защите прав человека и основных свобод, а также одобренные ООН «Руководящие принципы предпринимательской деятельности в аспекте прав человека». Компания строго соблюдает международное и локальное законодательства, опирается на «Руководство по социальной ответственности» ISO 26000–2010 и международный стандарт AA1000 (AccountAbility Principles, Stakeholder Engagement Standard).

«Лаборатория Касперского» также разделяет Принцип предосторожности (Принцип № 15), который закреплен в Рио-де-Жанейрской декларации по окружающей среде и развитию, принятой в 1992 году. Он является неотъемлемой частью системы управления рисками Компании. С учетом факторов потенциального воздействия на окружающую среду осуществляется работа дата-центров Компании и разработка ее продуктов и сервисов.

**GRI 2-28**

«Лаборатория Касперского» тесно сотрудничает с многочисленными международными ассоциациями и правоохранительными органами, участвуя в совместных операциях, расследованиях киберугроз, кибердипломатии и содействии открытому и безопасному интернету.

Полный список российских и международных ассоциаций, в которых участвует Компания, — в Приложении 2 на с. 142

# Управление устойчивым развитием

GRI 2-9 GRI 2-12 GRI 2-13 GRI 2-16 GRI 2-24

В «Лаборатории Касперского» функционирует система распределения ответственности между членами высшего руководства и руководителями профильных департаментов и подразделений. Мониторинг результатов координируется отделом проектов устойчивого развития, а также руководителями команд, реализующих проекты.

В начале 2024 года в Компании появился комитет устойчивого развития, подотчетный совету директоров. Основной целью комитета является выработка рекомендаций совету директоров по основным вопросам в сфере устойчивого развития (ESG), в числе которых:

- минимизация воздействия Компании на окружающую среду;
- создание условий для эффективного труда и развития человеческого потенциала в Компании;
- обеспечение соблюдения и защиты прав человека, инклюзивной среды и равного доступа к продуктам и услугам Компании;
- поддержка местных сообществ и НКО, содействие социальному развитию Компании;
- совершенствование практик корпоративного управления, обеспечения безопасности и управления ESG-рисками в Компании.

Заседания комитета будут проходить не менее двух раз в год. В ходе своей деятельности комитет активно взаимодействует с органами управления и подразделениями Компании, вовлеченными в реализацию проектов устойчивого развития.

# Подразделения, отвечающие за достижение целей устойчивого развития по ключевым направлениям

## Обеспечение киберустойчивости

- Управление по связям с государственными органами
- Департамент по развитию бизнеса решений на базе операционной системы KasperskyOS
- Отдел развития продуктов для промышленной кибербезопасности
- Управление исследования угроз
- Департамент продуктового маркетинга для потребительского рынка

## Этика и прозрачность

- Управление информационной безопасности
- Отдел экономической безопасности и противодействия коррупции
- Отдел исследований и анализа интеллектуальной собственности
- Управление внутреннего контроля
- Отдел закупок

## Возможности для людей

- Управление привлечения и развития сотрудников
- Управление образовательных программ
- Отдел проектов устойчивого развития

## Окружающая среда

- Управление по работе с партнерами департамента потребительского бизнеса
- Отдел финансовой аналитики потребительского бизнеса
- Отдел телекоммуникационной IT-инфраструктуры
- Административно-хозяйственное управление
- Управление финансовых сервисов
- Группа организации производства маркетинговых материалов
- Департамент онлайн-бизнеса
- Группа организации деловых поездок

## Технологии будущего

- Департамент по развитию бизнеса решений на базе операционной системы KasperskyOS
- Отдел развития продуктов для промышленной кибербезопасности

# Ключевые документы

Антикоррупционная политика[1]

Закупочная политика

Политика по контрактам

[1] Принята приказом от 18 мая 2012 года № 27.

# Вклад в достижение Целей устойчивого развития ООН

«Лаборатория Касперского» поддерживает все 17 Целей устойчивого развития ООН (ЦУР ООН) на период до 2030 года. Компания выделила шесть фокусных ЦУР ООН, достижению которых она в наибольшей мере способствует в ходе своей повседневной деятельности и реализации ключевых ESG-инициатив.

4 Качественное образование

7 Недорогостоящая и чистая энергия

5 Гендерное равенство

8 Достойная работа и экономический рост

Стратегические приоритеты Компании также соответствуют фокусным ЦУР ООН.

9 Индустриализация, инновации и инфраструктура

12 Ответственное потребление и производство

10 Уменьшение неравенства

13 Борьба с изменением климата

# Стратегические направления устойчивого развития Компании и их соотношение с ЦУР ООН

## Этика и прозрачность

- Прозрачность кода и процессов
- Защита данных и права на частную жизнь
- Прозрачность управления и устойчивость бизнеса


## Киберустойчивость

- Защита критической инфраструктуры в турбулентном мире
- Помощь в расследовании киберпреступлений по всему миру
- Защита пользователей от киберугроз


## Окружающая среда

- Уменьшение воздействия на окружающую среду: инфраструктура, бизнес-операции, продукты


## Возможности для людей

- Забота о сотрудниках
- Женщины в STEM
- Инклюзивность и доступность технологий
- Развитие кадров для IT


## Технологии будущего

- Кибериммунитет для новых перспективных технологий

# Существенные темы Отчета

GRI 3-1, 3-2

Для того чтобы содержание нашего Отчета в наибольшей мере отвечало интересам и ожиданиям представителей заинтересованных сторон, мы провели опрос стейкхолдеров с целью определения существенных тем Отчета в форме онлайн-анкетирования.

Первоначальный список тем для оценки стейкхолдерами был сформирован на основе перечня приоритетных аспектов устойчивого развития, выявленных в рамках процедуры определения существенности для предыдущего отчетного периода. Он включал 17 тем, которые отражают воздействия Компании на экономику, окружающую среду и общество.

Участники анкетирования могли оценить значимость каждой из предложенных тем по шкале от 1 до 5, где оценку «1» получали наименее важные, а «5» — исключительно важные темы. В анкете также была предусмотрена возможность оставлять замечания в свободной форме: стейкхолдеры могли как прокомментировать темы, предложенные для оценки, так и предложить новые темы. Для удобства участников анкета была составлена на двух языках — русском и английском.

В опросе приняли участие 35 представителей заинтересованных сторон: 14 внутренних и 21 внешний стейкхолдер. Полученные результаты были скорректированы с помощью весовых коэффициентов, чтобы придать равную значимость мнению каждой из групп стейкхолдеров. Затем на основе усредненных оценок, полученных от заинтересованных сторон, был сформирован итоговый список тем в порядке убывания их значимости.

Существенными для отражения в Отчете были признаны 15 тем, набравших общую оценку 3,4 балла и более. Это позволило в равной мере учесть мнения как внутренних, так и внешних стейкхолдеров, принимавших участие в опросе.

## Список существенных тем «Лаборатории Касперского» в Отчете об устойчивом развитии за вторую половину 2022–2023 год

| Тема | Оценка существенности | Страница отчета |
|---|---|---|
| Защита пользователей и пользовательских данных | 4,6 | 127 |
| Безопасная цифровая среда | 4,5 | 29 |
| Обеспечение программно-цифровой устойчивости в меняющемся мире | 4,2 | 29 |
| Просвещение в области информационной безопасности | 4,2 | 38 |
| Борьба с международной киберпреступностью | 4,1 | 47 |
| Вклад в развитие технологий | 4,1 | 56 |
| Подготовка профессионалов для отрасли | 4 | 103 |
| Ответственность перед сотрудниками | 4 | 92 |
| Инклюзивная цифровая среда | 3,9 | 99 |
| Деловая этика | 3,9 | 93, 136 |
| Прозрачность бизнеса и корпоративного управления | 3,7 | 134 |
| Социальные проекты, благотворительность и волонтерство | 3,6 | 97 |
| Женщины в STEM | 3,6 | 114 |
| Информационная и технологическая открытость | 3,4 | 120 |
| Снижение климатического и экологического следа | 3,4 | 75 |

# Матрица существенных тем с представлением оценок внутренних и внешних стейкхолдеров


| Номер темы | Название темы |
|---|---|
| 1 | Защита пользователей и пользовательских данных |
| 2 | Безопасная цифровая среда |
| 3 | Обеспечение программно-цифровой устойчивости в меняющемся мире |
| 4 | Просвещение в области информационной безопасности |
| 5 | Борьба с международной киберпреступностью |
| 6 | Вклад в развитие технологий |
| 7 | Подготовка профессионалов для отрасли |
| 8 | Ответственность перед сотрудниками |
| 9 | Инклюзивная цифровая среда |
| 10 | Деловая этика |
| 11 | Прозрачность бизнеса и корпоративного управления |
| 12 | Социальные проекты, благотворительность и волонтерство |
| 13 | Женщины в STEM |
| 14 | Информационная и технологическая открытость |
| 15 | Снижение климатического и экологического следа |
| 16 | Устойчивая цепочка поставок |
| 17 | Налогообложение |

# Взаимодействие с заинтересованными сторонами

Заинтересованные стороны «Лаборатории Касперского» — это сотрудники, пользователи, партнеры, поставщики, органы государственной власти, правоохранительные органы, местные сообщества и уязвимые с точки зрения информационной безопасности группы (пенсионеры, дети и их родители, а также пострадавшие от кибersталкинга). Мы стремимся к гармоничному взаимодействию с ними, выстраивая его на принципах взаимного уважения, прозрачности и ответственности.

GRI 2-29

| Группа заинтересованных сторон | Интересы группы | Каналы и способы взаимодействия | Результаты взаимодействия в отчетном периоде |
|---|---|---|---|
| Сотрудники | ■ Стабильное трудоустройство и карьерный рост<br>■ Справедливая заработная плата и социальное обеспечение<br>■ Комфортные и безопасные условия труда<br>■ Обучение и развитие<br>■ Отсутствие дискриминации | ■ Система внутрикорпоративных коммуникаций<br>■ Встречи с руководителями Компании<br>■ Совместные конференции, образовательные и спортивные мероприятия<br>■ Корпоративный веб-сайт | Подробнее о взаимодействии Компании с сотрудниками читайте в разделе «Возможности для людей», с. 86 |
| Пользователи | ■ Защита персональных данных<br>■ Высокое качество продукции<br>■ Высокий уровень сервиса<br>■ Приемлемые цены на продукцию | ■ Система обратной связи и сервисы<br>■ Пресс-релизы, рекламные и промоматериалы | Подробнее о взаимодействии Компании с пользователями читайте в разделе «Киберустойчивость», с. 29, и «Этика и прозрачность», с. 127 |
| Партнеры и поставщики | ■ Прозрачность и открытость конкурентных процедур<br>■ Контроль за качеством продукции<br>■ Соблюдение деловой этики<br>■ Противодействие коррупции<br>■ Своевременное и точное исполнение договорных обязательств | ■ Проведение открытых конкурентных закупочных процедур<br>■ Оперативное рассмотрение претензий<br>■ Деловые встречи, конференции и выставки<br>■ Раскрытие информации | Подробнее о взаимодействии Компании с партнерами читайте в подразделе «Устойчивая цепочка поставок», с. 23 |

| Группа заинтересованных сторон | Интересы группы | Каналы и способы взаимодействия | Результаты взаимодействия в отчетном периоде |
|---|---|---|---|
| Органы государственной власти и правоохранительные органы | ■ Соблюдение требований законодательства и стандартов<br>■ Своевременная уплата всех применимых налогов и сборов<br>■ Инвестиции в развитие регионов присутствия<br>■ Содействие в обеспечении занятости и поддержка предпринимательства<br>■ Обеспечение безопасности объектов КИ[1]<br>■ Содействие в борьбе с киберпреступлениями | ■ Консультации с сотрудниками правоохранительных органов<br>■ Разработка программного обеспечения и предоставление лицензий<br>■ Консультации по вопросам законотворчества | Подробнее о взаимодействии Компании с государственными и правоохранительными органами читайте в подразделе «Борьба с киберпреступностью», с. 47 |
| Местные сообщества | ■ Создание рабочих мест для местных жителей,- развитие человеческого капитала<br>■ Вклад в развитие социальной инфраструктуры<br>■ Развитие местных производств и поставщиков<br>■ Благотворительные проекты и социальные инвестиции<br>■ Минимизация негативного воздействия на окружающую среду территорий присутствия<br>■ Информационная открытость и прозрачность деятельности | ■ Наем персонала из представителей местных сообществ<br>■ Стажировки для студентов<br>■ Программы развития и повышения квалификации для персонала<br>■ Обучающие программы для широкого круга пользователей<br>■ Закупки у местных поставщиков | Подробнее о взаимодействии Компании с местными сообществами читайте в подразделе «Возможности для людей», с. 97 |
| Уязвимые с точки зрения информационной безопасности группы | ■ Обеспечение безопасности в интернете | ■ Проведение обучающих мероприятий для повышения-цифровой грамотности | Подробнее о взаимодействии Компании с уязвимыми группами читайте в подразделе «Возможности для людей», с. 97 |
| НКО | ■ Содействие в организации и реализации экологических и социальных программ | ■ Разработка, поддержка и проведение совместных-экологических и социальных проектов | Подробнее о взаимодействии Компании с НКО читайте в разделе «Киберустойчивость», с. 40 |

[1] Критическая инфраструктура.

# Устойчивая цепочка поставок

Закупочная деятельность «Лаборатории Касперского» строится на принципах прозрачности и честности. Всем компаниям, которые планируют стать контрагентами «Лаборатории Касперского», предоставляются равные условия участия в конкурсных процедурах.

**Закупочные процедуры Компании регламентируют внутренние документы:**
- **закупочная политика и процессы;**
- **политика по контрактам.**

«Лаборатория Касперского» внедряет IT-решение для управления закупками, разработанное российским вендором. Ранее для этой цели использовалась облачная платформа для управления закупками и поставками SAP Ariba.

Все закупки строятся на категорийной основе. Ключевыми критериями категоризации являются сходство технических и функциональных характеристик, а также области применения и бизнес-направления, например маркетинг, профессиональный сервис, IT, затраты на производство.

Для эффективного управления закупками определены следующие ключевые пороговые значения в зависимости от суммы кумулятивного закупочного объема в год по категории.
- Закупки до $25 тысяч идут по упрощенной процедуре: достаточно двух конкурентных предложений.
- Закупки от $25 тысяч до 100 тысяч требуют минимум трех предложений либо двух от доверенных поставщиков, которые были выбраны в тендерной процедуре и имеют успешный опыт работы с нашей Компанией.
- Закупки на сумму свыше $100 тысяч проводятся по тендерной процедуре, в которую вовлечены несколько подразделений Компании: отдел закупок, тендерный комитет, кросс-функциональные участники.

Тендерные закупки в зависимости от бюджета тоже имеют свои пороговые значения. Например, на тендерных процедурах по закупке на сумму около $1 млн присутствует бизнес-директор «Лаборатории Касперского».

Прежде чем пригласить партнера к участию в тендере, наша служба безопасности проводит его проверку. Мы не сотрудничаем с компаниями без опыта и репутации — 99% наших контрагентов работают на рынке не менее трех лет.

Мы планируем дополнить свод обязательных требований к поставщикам пунктом о наличии в компании антикоррупционной политики. В отчетном периоде мы уже начали включать антикоррупционную оговорку в договоры с нашими контрагентами.

Чтобы обеспечить конфиденциальность, которая требуется в связи со спецификой бизнеса и конкурентной средой, а также избежать сговора потенциальных поставщиков, мы не публикуем результаты тендеров в цифровом и качественном выражении, а также имена номинированных участников.

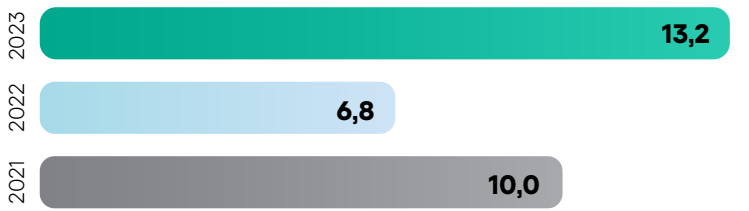
В 2023 году количество поставщиков осталось на том же уровне, что и в двух предыдущих годах. Экономия средств за счет конкурсных процедур и сокращения издержек при закупках в 2023 году выросла более чем вдвое по сравнению с показателем 2022 года и составила $13,2 млн.

**В 2023 году Компания сотрудничала**

**с 5,08 тысячи поставщиков**

Количество поставщиков Компании на конец отчетного периода, тысяч штук


Экономия Компании в результате тендеров и сокращения издержек при закупке товаров и услуг, $ млн[1]




[1] Без учета затрат по третьим лицам.

# Соблюдение прав человека

GRI 2-22 GRI 406-1

Соблюдение прав человека — основополагающий принцип деятельности «Лаборатории Касперского». Компания стремится предоставлять равные возможности сотрудникам по всему миру и поддерживать социокультурное разнообразие (diversity). Принципы уважения к правам и свободам человека будут закреплены в Этическом кодексе «Лаборатории Касперского», который находится в процессе разработки.

«Лаборатория Касперского» не приемлет использования любой формы детского, рабского или принудительного труда и ожидает аналогичных решений от своих контрагентов. Эта позиция Компании зафиксирована во внутренней политике, отражающей руководящие принципы ведения деятельности в странах ее присутствия.

**0** случаев дискриминации в Компании в отчетном периоде

## Соблюдение прав человека в деятельности Компании

| Основные права человека | Документы, которыми руководствуется Компания | Подходы Компании в области соблюдения прав человека | Заинтересованные стороны, которым Компания уделяет особое внимание в своем обязательстве | Результаты отчетного периода |
|---|---|---|---|---|
| Право на жизнь, свободу, неприкосновенность частной жизни, личную и семейную тайну | ■ Конституция Российской Федерации, статьи 20, 22, 23<br>■ Применимые законы в странах присутствия «Лаборатории Касперского», в том числе:<br>– EU General Data Protection Regulation (GDPR);<br>– Международный стандарт по информационной безопасности ISO/IEC 27001;<br>– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;<br>– China Personal information protection law (PIPL);<br>– California Consumer Privacy Act (CCPA);<br>– Lei Geral de Proteção de Dados (Общий закон о защите данных в Бразилии, LGPD);<br>– Vietnam's Personal Data Protection Decree (PDPD) | Один из приоритетов Компании — обеспечить защиту данных наших клиентов по всему миру при помощи внутренних систем и процедур по безопасности. Мы не используем данные в целях, отличающихся от целей сбора данных. | ■ Пользователи<br>■ Сотрудники<br>■ Уязвимые с точки зрения информационной безопасности группы<br>■ НКО[1] | 0 серьезных нарушений законодательства о персональных данных.<br>0 значительных утечек данных. |

[1] Некоммерческие организации.

| Основные права человека | Документы, которыми руководствуется Компания | Подходы Компании в области соблюдения прав человека | Заинтересованные стороны, которым Компания уделяет особое внимание в своем обязательстве | Результаты отчетного периода |
|---|---|---|---|---|
| Право на труд | ■ Конституция Российской Федерации, статья 37<br>■ Трудовой кодекс Российской Федерации<br>■ Правила внутреннего трудового распорядка<br>■ Положение об оплате труда<br>■ Политика в области охраны труда<br>■ Гайдлайн по благотворительным проектам<br>■ Положение о комитете по устойчивому развитию<br>■ Применимые законы в странах присутствия «Лаборатории Касперского» | Для «Лаборатории Касперского» сотрудники — самый ценный актив. Мы стремимся, чтобы людям в Компании было комфортно и интересно, чтобы они могли работать продуктивно, чувствовали себя защищенными, могли развиваться сами и развивать Компанию.<br><br>«Лаборатория Касперского» поддерживает деятельность некоммерческих организаций, помогающих людям с ограниченными возможностями здоровья в трудоустройстве и социализации, а также оказывающих им юридическую поддержку. | ■ Сотрудники<br>■ Уязвимые с точки зрения информационной безопасности группы<br>■ НКО | 5 152 человека — численность персонала на конец 2023 года (+4,4% к численности на конец 2022 года).<br><br>15% — текучесть персонала в 2023 году (–8 п. п. к текучести за 2022 год).<br><br>5 НКО, деятельность которых направлена на трудоустройство людей с инвалидностью, получили поддержку Компании за отчетный период.<br><br>Компания приняла участие в четырех мероприятиях по инклюзивному трудоустройству (бизнес-завтраки, ярмарки вакансий, менторская программа).<br><br>Один информационный проект про профессиональный и личный путь сотрудников с инвалидностью и тех, кто воспитывает детей с инвалидностью, опубликовала Компания: https://kasperskyspecial.ru/. |
| Право на благоприятную окружающую среду | ■ Конституция Российской Федерации, статья 42<br>■ Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды»<br>■ Положение о комитете по устойчивому развитию<br>■ Гайдлайн по благотворительным проектам<br>■ Применимые законы в странах присутствия «Лаборатории Касперского» | Ответственное отношение к окружающей среде — одна из важнейших ценностей «Лаборатории Касперского». Мы снижаем негативное воздействие на природу за счет экономного потребления ресурсов, хорошо организованных бизнес-процессов и ответственного отношения к источникам энергии для дата-центров и офиса. | ■ Сотрудники<br>■ Местные сообщества<br>■ Пользователи<br>■ НКО | 285 контрагентов подключили к ЭДО[1] с 2022 по 2023 год и подписали 7 126 документов.<br><br>1 407,9 кг вещей сдали на благотворительность, переработку и утилизацию сотрудники Компании.<br><br>370 кг электротехники передали на утилизацию в рамках эконедели. |

[1] Электронный документооборот.

| Основные права человека | Документы, которыми руководствуется Компания | Подходы Компании в области соблюдения прав человека | Заинтересованные стороны, которым Компания уделяет особое внимание в своем обязательстве | Результаты отчетного периода |
|---|---|---|---|---|
| Право на образование | ■ Конституция Российской Федерации, статья 43<br>■ Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 04.08.2023) «Об образовании в Российской Федерации»<br>■ Положение о комитете по устойчивому развитию<br>■ Гайдлайн по благотворительным проектам<br>■ Применимые законы в странах присутствия «Лаборатории Касперского» | Мы поощряем стремление сотрудников к новым знаниям, постоянно совершенствуем внутренние образовательные программы и добавляем новые.<br><br>Мы организовываем совместные образовательные проекты с некоммерческими организациями, которые помогают людям с ограниченными возможностями здоровья, пенсионерам, жертвам домашнего насилия и другим людям, оказавшимся в сложной жизненной ситуации.<br><br>«Лаборатория Касперского» создает собственные обучающие программы, нацеленные на взаимодействие с учебными заведениями и аудиторией, которой необходимо дополнительное образование. Мы вкладываем ресурсы в развитие как школьников и студентов, так и уже опытных специалистов кибербезопасности, нуждающихся в повышении квалификации. | ■ Сотрудники<br>■ Пользователи<br>■ Уязвимые с точки зрения информационной безопасности группы<br>■ НКО | 200+ университетов-партнеров в 42 странах мира насчитывает Kaspersky Academy.<br><br>13 549 заявок было получено Компанией за отчетный период на участие в программе стажировок SafeBoard.<br><br>134 студента прошли стажировку в «Лаборатории Касперского» в отчетном периоде.<br><br>>6 000 студентов со всего мира участвовали в конкурсе Secur'IT Cup с 2018 года.<br><br>Победители Secur'IT Cup получают гранты на $10 000.<br><br>>2 млн раз пройдены «Уроки цифры» от «Лаборатории Касперского» в 2023 году.<br><br>13,5 млн прохождений набрали «Уроки цифры» от «Лаборатории Касперского» с 2018 года.<br><br>2 000+ пользователей из более чем 50 стран – аудитория тренингов Компании для экспертов. |
| Право на охрану здоровья и медицинскую помощь | ■ Конституция Российской Федерации, статья 41<br>■ Положение о выплатах компенсационного и стимулирующего порядка<br>■ Применимые законы в странах присутствия «Лаборатории Касперского» | Забота о здоровье и благополучии сотрудников — важная составляющая социальной политики «Лаборатории Касперского». Социальный пакет, доступный всем сотрудникам[1] Компании, включает широкий спектр медицинских услуг. Мы также продвигаем идеи активного и здорового образа жизни среди сотрудников. | ■ Сотрудники | 0 случаев травматизма среди сотрудников в 2022 и 2023 годах.<br><br>0 случаев профессиональных заболеваний у сотрудников Компании выявлено в 2023 году.<br><br>100% сотрудников охвачены программой ДМС[2].<br><br>Одна лекция врача-онколога в формате вопросов-ответов об онкологических заболеваниях, необходимости своевременных чек-апов и сдачи анализов. |
| Право на защиту от дискриминации | ■ Конституция Российской Федерации, статьи 19, 29<br>■ Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН<br>■ Внутренняя политика «Лаборатории Касперского», отражающая руководящие принципы ведения деятельности в странах ее присутствия<br>■ Применимые законы в странах присутствия «Лаборатории Касперского» | Мы не приемлем и не поощряем дискриминацию любого рода в деятельности Компании. | ■ Сотрудники<br>■ Пользователи<br>■ Партнеры | 0 случаев дискриминации в Компании в отчетном периоде. |

[1] Для сотрудников с временными трудовыми договорами и работающих на условиях неполной занятости доступен сокращенный соцпакет. В Компании около 0,1% таких сотрудников.
[2] Добровольное медицинское страхование.

# Управление ESG-рисками

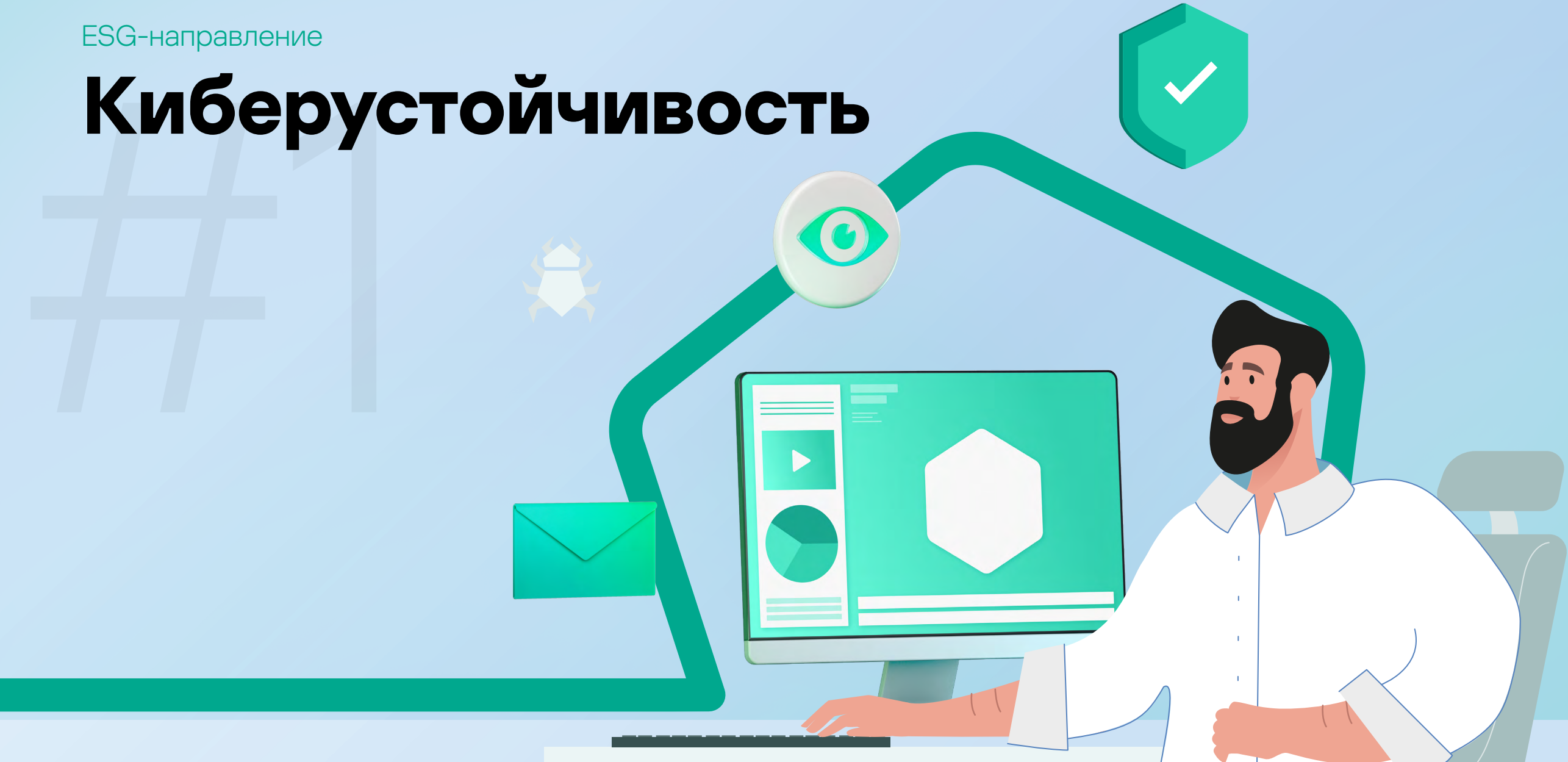
За управление рисками устойчивого развития в «Лаборатории Касперского» отвечают топ-менеджеры Компании и руководители направлений. В отчетном периоде Компания определила для себя три ключевых ESG-риска: риск изменений в политической и экономической обстановке в регионах присутствия Компании, изменения в законодательстве, риск роста киберпреступности и риск разрывов в цепочке поставок.

## Ключевые ESG-риски

| Риск | Почему риск важен | Меры по управлению рисками в 2022 и 2023 годах |
|---|---|---|
| Риск изменений в политической и экономической обстановке в регионах присутствия Компании, изменения в законодательстве | Возможны изменения в законодательстве, способные существенно ограничить способность Компании вести бизнес в стране/регионе присутствия | ■ Постоянный мониторинг изменений в законодательстве в странах/регионах присутствия с целью оперативного выявления потенциальных рисков<br>■ Членство Компании и отдельных сотрудников в различных отраслевых организациях для участия в коммуникации с регулирующими органами<br>■ 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<br>■ Дальнейшее развитие глобальной инициативы по информационной открытости (Global Transparency Initiative – GTI) с целью верификации надежности Компании и ее продуктов клиентами, партнерами, а также регуляторами |
| Риск роста киберпреступности | 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 | Компания продолжила активно сотрудничать с правоохранительными органами и международными организациями в отчетном периоде:<br>■ оказала содействие Интерполу в проведении операций Africa Cyber Surge в ноябре 2022 года и Africa Cyber Surge II в августе 2023 года, нацеленных на борьбу с киберперступностью на Африканском континенте;<br>■ под эгидой Интерпола организовала обучение более 100 представителей правоохранительных органов различных стран по направлениям «Реакция на инциденты» и «Анализ вредоносных программ»;<br>■ приняла участие в международной конференции Интерпола по кибербезопасности;<br>■ участвовала в формировании отзывов и предложений к проекту разрабатываемой в настоящее время под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях;<br>■ подписала меморандумы о взаимопонимании с рядом национальных регуляторов в области кибербезопасности |
| Риск разрывов в цепочке поставок | Геополитические изменения могут стать причиной прерывания логистических цепочек и оказывать негативное влияние на бизнес и результаты деятельности Компании. | Компания ранжировала свои сервисы по уровню критичности для непрерывности бизнеса и влиянию на его результаты. Несмотря на то что риски разрывов в цепочке поставок мы оцениваем как низкие, мы разработали меры по их снижению и переходу на новые продукты и платформы. В их числе:<br>■ импортозамещение ПО, систем, оборудования и сервисов:<br>– переход с CRM Sales Force на российскую платформу «Битрикс»,<br>– закупка российского сертифицированного оборудования «Русский Щит»;<br>■ изменение логистических моделей по закупке важных компонентов, замена пула поставщиков, отказавшихся от поставки или не имеющих возможности осуществлять поставку оборудования, ПО и услуг;<br>■ перевод услуг технической поддержки и инфраструктурных сервисов в другие регионы мира |

ESG-направление

# Киберустойчивость



# Цифровая безопасность

## Наша цель — защищать пользователей от киберугроз с помощью продуктов и инициатив «Лаборатории Касперского».

В современном цифровом обществе технологии все глубже проникают в повседневную жизнь людей, и вместе с этим постоянно растет количество киберугроз. В то время, когда вы обмениваетесь сообщениями, скачиваете фотографии или проводите онлайн-операции, вы можете подвергаться опасности. Злоумышленники совершенствуют методы кибератак, вторгаясь в личную жизнь людей. Мы стремимся защитить интересы пользователей в информационном пространстве и сделать его местом, где каждый человек чувствует себя в безопасности.

### Решения «Лаборатории Касперского»

**>411 тысяч**
новых вредоносных файлов обнаруживали ежедневно в 2023 году

**33 790 599**
атак с использованием вредоносного, рекламного или нежелательного мобильного ПО предотвратили в 2023 году

**~125 млн**
вредоносных файлов нашли с января по октябрь 2023 года

**135 980 457**
вредоносных почтовых вложений заблокировали в 2023 году

**>437 млн**
кибератак отразили с ноября 2022 года по октябрь 2023 года

**709 590 011**
попыток перехода по фишинговым ссылкам предотвратили в 2023 году

# Как мы защищаем пользователей от киберугроз

Чтобы противостоять киберугрозам, мы создаем качественные продукты и ведем просветительскую работу, обучая основам цифровой грамотности пользователей и основам кибербезопасности корпоративных клиентов.

**TC-SI-230a.2**

Наши решения защищают пользователей от широкого спектра киберугроз: онлайн-мошенничества, утечек данных, целевых кибератак. Чтобы получить контроль над компьютерными системами, злоумышленники используют различные виды программ.

- **Вирусы** — программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы** — программы, осуществляющие несанкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. Одно из ключевых отличий этого класса вредоносного ПО — неспособность к самовоспроизведению. Первые представители появились еще в конце 1980-х годов и полностью соответствовали своему названию, выдавая себя за легитимное ПО.
- **Шпионское ПО** — программы, втайне следящие за действиями пользователя и собирающие информацию, которую злоумышленники используют в своих целях.
- **Шифровальщики** — ПО, которое шифрует файлы и данные на компьютере пользователя, после чего злоумышленники требуют выкуп за восстановление доступа к информации, утверждая, что иначе пользователь потеряет данные. Злоумышленники могут также угрожать выложить скомпрометированные данные в открытый доступ.
- **Рекламное ПО** — программы рекламного характера, которые могут создавать проблемы на устройстве пользователя.
- **Ботнеты** — сети компьютеров, зараженных вредоносным ПО, которые злоумышленники используют в своих целях.

Пользователи и компании также могут стать жертвой фишинга, скама, телефонного мошенничества и DoS-атак.

Современный мир стал свидетелем значительного увеличения числа киберугроз по мере развития цифровых технологий и интернета. С каждым годом количество вредоносных файлов растет: если в 2020 году мы обнаруживали около 360 тысяч новых вредоносных файлов в день, то в 2023 году — уже 411 тысяч, что на 3% больше, чем годом ранее.

Количество вредоносных файлов, обнаруживаемых «Лабораторией Касперского» ежедневно, тысяч штук

# Боремся с кибersталкингом

# # Задача

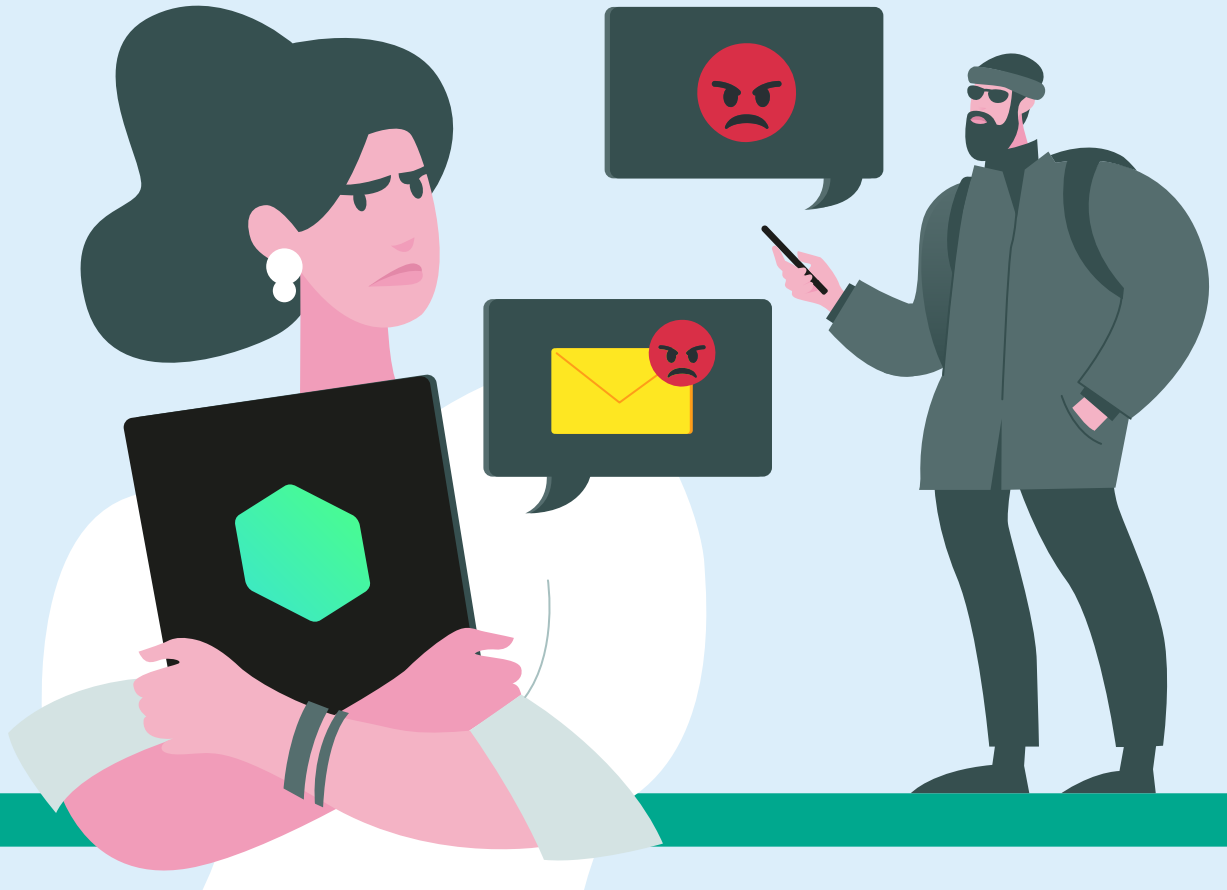
**Защита пользователей от цифрового преследования**

Результаты наших исследований свидетельствуют об устойчивом росте числа атак с использованием ПО для цифровой слежки, или, иначе, сталкерского ПО. Чаще всего их жертвами становятся жители России, Бразилии и Индии, но в целом это явление распространилось по всему миру.

Сталкерское ПО, или Stalkerware, — это программы, которые используются для скрытого наблюдения за другим человеком (это может быть, например, партнер или член семьи) через его устройство. Это не только техническая, но и социальная проблема, для решения которой необходим вклад всех участников цифрового пространства. Мы уведомляем пользователей об этой угрозе с помощью наших продуктов, в числе которых Kaspersky для Android. Это решение для защиты данных на смартфоне, предупреждающее пользователей в том числе об обнаружении сталкерских приложений на устройстве. Кроме того, мы работаем над решением проблемы кибersталкинга, сотрудничая с некоммерческими организациями, отраслевыми экспертами, исследовательскими компаниями и государственными учреждениями по всему миру и предлагая инструмент для борьбы с цифровой слежкой TinyCheck.

**>31 тысячи**

**пользователей во всем мире столкнулись с кибersталкингом в 2023 году (+5,9% к 2022 году)**



# # Решения

GRI 203-1

## Участвуем в проектах по защите от сталкерского ПО

В 2019 году «Лаборатория Касперского» стала сооснователем Коалиции по борьбе со сталкерским ПО (Coalition Against Stalkerware) — международной рабочей группы по борьбе со сталкерскими программами и домашним насилием. Коалиция объединяет усилия IT-компаний, НКО, исследовательских институтов и правоохранительных органов в области борьбы с кибersталкингом и помощи жертвам онлайн-насилия.

Сегодня в состав Коалиции входят более 40 организаций, которые делятся друг с другом опытом и вместе работают над решением проблемы цифрового сталкинга. Пользователи, которые подозревают, что за ними следят через мобильное устройство, могут обратиться за помощью на сайте Коалиции, доступном на семи языках.

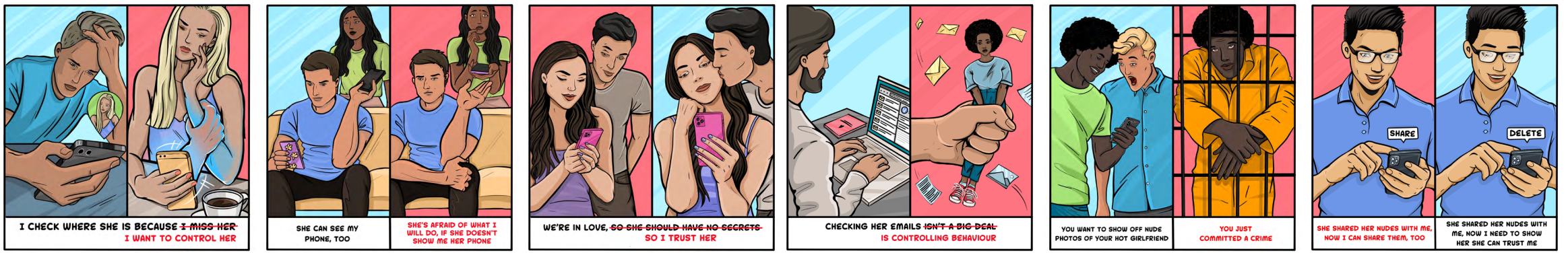
**>40**

**организаций вошли в международную Коалицию по борьбе со сталкерским ПО, сооснователем которой является «Лаборатория Касперского»**

«Лаборатория Касперского» сотрудничает также с Европейской сетью по работе с субъектами домашнего насилия[1]. В сентябре 2022 года мы провели глобальную кампанию #NoExcuse4Abuse, направленную на повышение осведомленности общественности о злоупотреблениях технологиями в отношениях. Мы считаем, что очень важно разрушить мифы вокруг этой темы и помочь жертвам распознать признаки возможного цифрового насилия. В рамках кампании были подготовлены комиксы, которые показывают примеры неподобающего поведения в отношениях, замаскированного под проявление «заботы». Главная цель проекта — оспорить аргументацию и оправдания абьюзеров, чтобы удержать их от проявления насилия в отношении своих партнеров.

**78,1 тысячи**

**пользователей были охвачены кампанией #NoExcuse4Abuse**




[1] European Network for the Work with Perpetrators of Domestic Violence (WWP EN).

## Организуем исследовательские и образовательные проекты против киберсталкинга

Совместно с разными международными компаниями, академическим сообществом и некоммерческими организациями «Лаборатория Касперского» участвует в проведении исследования «Как защитить жертв насилия со стороны партнера от рисков, связанных с цифровыми технологиями»[1]. Для участия в совместном исследовании мы создали партнерство с британским агентством исследований и инноваций UKRI.

Проект стартовал в 2023 году и продлится до 2026 года. «Лаборатория Касперского» поддерживает его своей экспертизой в сфере борьбы с кибернасилием и сталкингом, а также участием в дополнительных мероприятиях.

## Уведомляем об угрозе киберсталкинга

Наша Компания первой в отрасли стала предупреждать пользователей своих решений о наличии сталкерского ПО на их устройствах.

В июне 2022 года «Лаборатория Касперского» запустила портал о TinyCheck — бесплатном и безопасном инструменте с открытым исходным кодом для некоммерческих организаций и отделов полиции, которые работают с жертвами цифрового сталкинга. Это решение устанавливается не на смартфон, а на отдельное внешнее устройство — микрокомпьютер Raspberry Pi. TinyCheck может проверить исходящий интернет-трафик, проанализировать его в режиме реального времени и распознать подключения к центрам управления разработчиков сталкерского ПО. При этом решение не позволяет инициатору слежки узнать о такой проверке.

В 2022 году в рамках запуска новой линейки решений для защиты цифровой жизни пользователей мы расширили функции уведомления о нарушении конфиденциальности. Теперь пользователи TinyCheck получают предупреждение не только о наличии сталкерского ПО на устройстве, но и о том, что при его удалении установивший его человек узнает об этом, что может привести к обострению ситуации. Кроме того, жертва сталкинга должна знать, что, удалив приложение, она рискует удалить и важные данные или доказательства, которые могут быть использованы правоохранительными органами.

## DeStalk

С 2021 по 2023 год «Лаборатория Касперского» была партнером проекта DeStalk, запущенного в рамках программы EC Rights, Equality and Citizenship («Права, равенство и гражданственность»). Проект объединил пять организаций-партнеров, а также экспертов по кибербезопасности, представителей исследовательских, общественных организаций и органов власти.

На проекте DeStalk мы обучили более 350 профессионалов, которые помогают пострадавшим женщинам и занимаются вопросами насилия, и представителей органов власти. Они изучили действенные методы борьбы с киберсталкингом и научились противостоять другим формам цифрового гендерного насилия. Мы также прикладывали все силы, чтобы сделать доступной для широкой аудитории информацию о цифровом насилии и способах его преодоления.

## DeStalk e-learning

В рамках проекта DeStalk «Лаборатория Касперского» разработала электронный учебный курс The DeStalk e-learning по борьбе с кибернасилием и сталкерским ПО на пяти языках. Цель курса — обучить 80–100 профессионалов из 20–30 разных организаций:

- специалистов, работающих с жертвами насилия / пережившими насилие;
- специалистов, работающих с лицами, совершившими насилие в отношении партнера;
- государственных служащих, работающих в сфере борьбы с домашним насилием.

Курс состоял из четырех занятий, которые включали в себя теоретическую часть и тестирование. Первое занятие было посвящено теме цифрового гендерного насилия, второе — формам кибернасилия. На третьем занятии рассматривалась тема сталкинга, на четвертом — работа с жертвами насилия и с его инициаторами. Электронный курс доступен на сайте DeStalk.

DeStalk
detect and stop stalkerware and cyberviolence against women

**Более 350 профессионалов**
прошли обучение на проекте DeStalk, включая представителей органов власти

**130 человек**
обучились на курсах по борьбе с кибернасилием и сталкерским ПО

[1] How to protect victims / survivors of Intimate Partner Violence (IPV) from the risks created by digital technologies.

# Защищаем от шифровальщиков

# # Задача

**Борьба с программами-вымогателями**

По нашим данным, атаки программ-вымогателей становятся все более сложными и причиняют много вреда как компаниям, так и пользователям. Особую опасность вызывают таргетированные (целевые и более сложные) атаки на бизнес — как на крупные компании, так и на малые и средние. Организаторы целевых атак тщательно выбирают мишени — правительства, конкретные организации или отдельные группы людей внутри того или иного предприятия.

Шифровальщики в последние годы остаются одной из наиболее актуальных киберугроз, а их атаки становятся все сложнее. За период с ноября 2022 года по октябрь 2023 года троянцы-шифровальщики атаковали 193 662 уникальных пользователя, в том числе 52 999 пользователей из крупного бизнеса и 6 351 пользователя, связанного с малым и средним бизнесом.

В 2022 году «Лаборатория Касперского» обнаружила две новые кибергруппы вымогателей — RedAlert и Monster. В последнее время их основная цель — повредить как можно больше систем, адаптируя свой вредоносный код одновременно к нескольким ОС. Кроме того, с июля по сентябрь 2022 года Компания обнаружила две волны атак на правительственные организации Албании с использованием программ-вымогателей и вредоносных программ-вайперов. Злоумышленники использовали украденные сертификаты Nvidia и Kuwait Telecommunication для подписи своих вредоносных программ.

## Решения «Лаборатории Касперского»

выявили

**74,2 млн**

атак программ-вымогателей в 2022 году (+20% к 2021 году)

обнаружили

**23 364**

модификации шифровальщиков и 43 новых семейства программ-вымогателей с ноября 2022 года по октябрь 2023 года[1]

отразили атаки шифровальщиков на компьютерах

**193 662**

уникальных пользователей с ноября 2022 года по октябрь 2023 года

[1] Источник — https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf.

# # Решения

## Разрабатываем продукты для защиты от программ-вымогателей

«Лаборатория Касперского» разработала и опубликовала специальные правила для пользователей, которые хотят защитить себя и свой бизнес от атак программ-вымогателей. Пользователям могут помочь наши продукты, которые продемонстрировали высокую эффективность в защите от программ-вымогателей в результате тестирования[1]. В частности, три решения «Лаборатории Касперского» — Kaspersky Security для бизнеса, Kaspersky Small Office Security и Kaspersky Standard — успешно прошли все тесты, набрав максимальное количество баллов, и получили сертификаты Advanced Approved Endpoint Protection для бизнес-решений и Advanced Certified — для пользовательских.

## Предоставляем новейшие данные о киберугрозах

«Лаборатория Касперского» предлагает сервисы информирования о современных киберугрозах, которые помогут любой организации эффективно противостоять им. Сервис Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах, полученные нашими аналитиками и исследователями мирового класса. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT.

Запросить доступ к этому сервису можно здесь.

**158**
**глобальных пресс-релизов о киберугрозах выпущено Компанией за отчетный период**

Помимо этого, Компания постоянно проводит специальные исследования и опросы на разные темы. Это помогает информировать пользователей о киберугрозах, с которыми они могут столкнуться в реальной жизни, даже не подозревая об этом. Так, в отчетном периоде мы рассказали о:

- уязвимостях в популярных «умных» кормушках для домашних животных. Используя обнаруженные уязвимости, злоумышленники могут превратить кормушку в инструмент слежки, а также изменить расписание кормления, тем самым поставив под угрозу здоровье питомца;
- схеме онлайн-мошенничества, ориентированной на владельцев домашних животных, которые хотят купить импортные лекарства для своих питомцев. Через каналы в Telegram мошенники выманивают у них деньги и финансовую информацию;
- ловушках для туристов в период летних отпусков. Тревел-эксперты и специалисты по кибербезопасности предупредили о трех направлениях мошенничества, которые связаны с билетами, размещением туристов и опросами;
- рисках для желающих начать собственный бизнес. «Лаборатория Касперского» выяснила, что 80% россиян недооценивают важность навыков кибербезопасности для старта своего бизнеса, в то время как жертвой кибератаки может стать любая компания, не только крупная;
- новой схеме онлайн-мошенничества, нацеленной на русскоязычных школьников. В коротких видео на YouTube Shorts мошенники рассказывают, как легко зарабатывают много денег, и предлагают поделиться своими идеями со школьниками. Оказалось, что это всего лишь первый этап многоуровневой скам-схемы по выманиванию денег;
- новой кампании по краже криптовалюты через поддельный браузер Tor. Под видом браузера Tor на сторонних интернет-ресурсах злоумышленники распространяют троянца CryptoClipper. При попадании в систему пользователя он регистрируется в автозапуске, маскируясь иконкой какого-либо популярного приложения, например uTorrent. Как только зловред-клиппер обнаруживает в буфере обмена адрес, похожий на криптокошелек, он тут же меняет его на один из адресов, принадлежащих злоумышленнику. С вредоносной кампанией столкнулись более 15 тысяч пользователей в 52 странах, причем больше всего атак было зафиксировано в России;
- технологиях по созданию дипфейк-видео. Наши эксперты обнаружили, что в даркнете предлагают услуги по созданию таких роликов стоимостью до $20 тысяч за минуту. Дипфейки могут создавать для использования в скам-схемах, с целью политических манипуляций, мести и кибербуллинга;
- «Операции Триангуляции» — такое название получила APT-кампания на iOS-устройства с целью шпионажа;
- актуальных спам- и фишинговых атаках: статистика и тенденции, которым следовали злоумышленники в 2023 году, в новом отчете.

Кроме того, мы создали обучающие видео, где рассказываем о криптофишинге, провели вебинар о существующих угрозах в этой области, а также выпустили собственное исследование на эту тему.

[1] Тестирование AV-TEST проходило в августе 2023 года.

# Как мы раскрыли «Операцию Триангуляцию»

## Вместе против шпионажа

В начале июня 2023 года исследователи «Лаборатории Касперского» обнаружили ранее неизвестное вредоносное ПО, которое атакует устройства с операционной системой iOS. Это целевые атаки в рамках APT-кампании, которая получила название «Операция Триангуляция» (Operation Triangulation). Зловред проникает на устройства жертв с помощью эксплойта, доставляемого в скрытом сообщении iMessage, после этого он самостоятельно запускается и получает полный контроль над устройством и пользовательскими данными. Цель злоумышленников — шпионаж.

Специалисты установили, что внедренное шпионское ПО незаметно передает информацию с устройства жертвы на удаленные серверы. Злоумышленников интересовали записи с микрофонов, фотографии из мессенджеров, геолокация и данные о других действиях владельца.

«Сегодня у нас очень большая и важная новость. Экспертами нашей Компании была обнаружена крайне сложная, профессиональная целевая кибератака с использованием мобильных устройств производства Apple», — написал в своем блоге Евгений Касперский.

По его словам, косвенным признаком присутствия Triangulation на устройстве является блокировка возможности обновления iOS. Для более точного распознавания заражения потребуется снять резервную копию устройства и проверить ее специальной бесплатной утилитой.

Узнать больше об «Операции Триангуляция» и том, как проверить, заражено ли iOS-устройство, можно на портале Securelist.


## Что в результате?

«Лаборатория Касперского» разработала утилиту triangle_check для компьютеров на операционных системах Windows и Linux, с помощью которой пользователи могут проверить свой iPhone (бэкап системы) на факт заражения вредоносным ПО Operation Triangulation. Для проверки с помощью этой утилиты на Windows и Linux достаточно скачать бинарную сборку, а на macOS е можно установить ее как Python-пакет.

Специалисты компании Apple, в свою очередь, признали проблему и выпустили обновления, которые устраняют допущенные уязвимости.

GRI 203-1

NO MORE RANSOM

Чтобы противодействовать злоумышленникам, по инициативе «Лаборатории Касперского» в 2016 году был создан альянс No More Ransom, куда помимо нашей Компании вошли Европол, нидерландская полиция и вендоры из кибербезопасности. Участники альянса обмениваются опытом, знаниями и decryption tools — инструментами дешифровки, которые помогают восстанавливать данные, зашифрованные вымогателями.

# Наш вклад в инициативу No More Ransom

## Вместе против программ-вымогателей

**360 000**
раз были скачаны бесплатные инструменты для дешифровки

с их помощью можно расшифровать файлы, заблокированные
**39**
семействами программ-вымогателей

более **2 млн**
пользователей смогли восстановить данные

Международная инициатива No More Ransom, одним из основателей которой является «Лаборатория Касперского», создана с целью помочь жертвам троянцев-вымогателей снова получить доступ к своим зашифрованным данным, не выплачивая денег атакующим.

Этот проект представляет собой уникальное партнерство между правительственными организациями, правоохранительными структурами, антивирусными компаниями и образовательными учреждениями.

Участники инициативы разрабатывают бесплатные инструменты для дешифровки, рассказывают о рисках, связанных с атаками программ-вымогателей, а также о лучших практиках для противодействия им. В марте 2023 года «Лаборатория Касперского» выпустила новую версию инструмента для дешифровки в помощь жертвам модификации программы-вымогателя, основанной на утекшем ранее коде программы Conti.

Недавно No More Ransom отметила важную веху: более 2 млн пользователей получили возможность восстановить данные благодаря инициативе.

## Что в результате?

Совместными усилиями нам удалось сделать цифровую среду более безопасной: мы помогли сотням тысяч пользователей и снизили общий уровень угроз в онлайн-мире.

Бесплатные инструменты «Лаборатории Касперского» для дешифровки, доступные в рамках инициативы No More Ransom, были скачаны более 360 тысяч раз за пять лет. С их помощью можно расшифровать файлы, заблокированные 39 семействами программ-вымогателей. Эти инструменты предоставили жертвам средства для восстановления важных данных без необходимости выполнять требования преступников. Такой результат говорит об успехе инициативы.

# Обучаем пользователей основам кибербезопасности

## # Задача

**Предоставление пользователям инструментов самозащиты**

Умение обеспечить свою безопасность в цифровом пространстве становится важным навыком современного человека. Обучая наших пользователей основам кибербезопасности, мы не только помогаем им распознавать потенциальные угрозы, но и предоставляем инструменты для собственной защиты. Таким образом мы инвестируем в безопасное цифровое будущее для всех.

## # Решения

**Kaspersky Academy**

**>8 000**

**студентов обучились в Kaspersky Academy за 2022–2023 годы**

Еще в 2010 году мы запустили Kaspersky Academy, чтобы масштабировать образовательные инициативы и сделать их доступными для всех желающих. Мы планировали превратить ее в глобальный университет, где будут собраны все обучающие материалы, касающиеся информационной безопасности. И нам удалось реализовать этот проект.

Сейчас спикерами Kaspersky Academy выступают руководители команд Компании, директора направлений, ведущие специалисты и приглашенные эксперты в области информационной безопасности. За 2022–2023 годы в Kaspersky Academy прошли обучение более 8 000 студентов из России, Европы, Саудовской Аравии, Руанды и других стран.

## Преимущества Kaspersky Academy:

- один из механизмов получения доступа к контенту — платформа Education.kaspersky.com;
- адаптирована под два формата продуктов:
  1. видеоуроки + тестовые задания + сертификат;
  2. видеоуроки + прямые эфиры + тестовые задания + финальный тест + сертификат;
  3. формат онлайн рабочей тетради с автопроверкой + сертификат;
- позволяет отслеживать результаты студентов — промежуточные и финальные;
- оповещает студентов о предстоящем вебинаре;
- позволяет быстро кастомизировать формат тренинга и сбор аналитики под запрос заказчика и проект;
- дает возможность управлять длительностью доступа учащегося к платформе.

**В 2023 году были запущены курсы:**

- «Введение в кибербезопасность». Обновленный флагманский курс для русскоязычной аудитории, который рассматривает все основные аспекты информационной безопасности. Он ориентирован как на IT-специалистов или студентов, так и на частных пользователей;
- «Кибербезопасность для топ-менеджеров». Курс дает слушателям представление о кибербезопасности как системе и показывает, как киберриски влияют на бизнес и как можно ими управлять.

## Ключевые проекты Academic Affairs для школьников и студентов в 2023 году:

**SafeBoard** — 15+ направлений IT-стажировки (более 500 студентов присоединились к программе с 2016 года). За восемь лет существования этой программы более половины ее участников перешли в штат Компании и сейчас работают в том числе на ступенях Middle, Senior и Lead;

**Secure'IT Cup** — ежегодный международный конкурс студенческих проектов в сфере кибербезопасности (30+ стран-участниц, более 2 000 заявок от студентов каждый год);

**Долина технологий** — летняя практика для школьников и студентов колледжей (более 1 200 регистраций в 2023 году, 45 участников прошли практику в офисе);

**Cyber Generation** — тренинг-программа для студентов и недавних выпускников Саудовской Аравии (91 участник);

**Kaspersky Academy Alliance** — специальная программа для университетов, позволяющая интегрировать экспертизу в области кибербезопасности и новейшие технологии Kaspersky в процесс обучения студентов.

**«Лаборатория Касперского» делится практическими знаниями со студентами**

**почти 200 университетов**

**по всему миру в 42 странах.**

**Более 60 учебных заведений из этого числа находятся в России и СНГ.**

## Тренинги по кибербезопасности для НКО

GRI 203-1

Кибербезопасность важна для эффективной деятельности некоммерческих организаций (НКО), которые значительно зависят от цифровых технологий. «Лаборатория Касперского» регулярно проводит тренинги для некоммерческих организаций, чтобы повысить уровень их защиты от онлайн-угроз, которые постоянно эволюционируют. Такое партнерство способствует созданию более безопасного и устойчивого цифрового будущего для всех.

В 2022–2023 годах мы организовали тренинги на разные темы для российских и международных некоммерческих организаций:

- **Киберсталкинг**. Наши ведущие исследователи угроз информационной безопасности провели два тренинга по проблеме кибersталкинга для фонда «Благие дела» из Казани и Нижегородского женского кризисного центра, который оказывает бесплатную психологическую и юридическую поддержку людям, столкнувшимся с насилием и жестоким обращением. Также для этих организаций мы провели тренинг по использованию бесплатного open-source-инструмента TinyCheck, который способен обнаружить установленное на девайс ПО для слежки, не уведомляя об этом сталкера. Теперь в Нижегородском женском кризисном центре каждая женщина может проверить свое устройство на предмет обнаружения такого ПО.

- **Доксинг**[1]. Вместе с Сингапурским советом женских организаций[2] мы провели бесплатный семинар по борьбе с доксингом. Наши специалисты рассказали, как можно снизить риски неправомерного использования личной информации, защитить свои и чужие личные данные, познакомили слушателей с надежным защитным программным обеспечением и раскрыли возможные мотивы злоумышленников.

- **Кибергигиена**. В партнерстве с платформой социальных изменений todogood мы провели онлайн-интенсив на тему кибергигиены в рамках программы «Я могу» для уязвимых групп населения — женщин, попавших в сложную жизненную ситуацию, людей с ограниченными возможностями здоровья и людей старшего возраста. Цель программы — помочь участникам в профессиональной переподготовке, адаптации к обучению, работе в онлайн-среде, социально-культурным изменениям и новым технологиям. В записи и онлайн интенсив прошли 946 человек, которые сдали тест и получили сертификаты.

Мы также создали ряд проектов по кибербезопасности в партнерстве с международными организациями. В частности, был запущен Kids' Cyber Resilience Project, который активно развивался в странах Азиатско-Тихоокеанского региона с марта 2023 года. В рамках этого проекта мы провели ряд важных мероприятий, нацеленных на повышение грамотности местного населения в сфере кибербезопасности.

- Совместно с Centre For Cybersecurity и The HEAD Foundation «Лаборатория Касперского» запустила в Сингапуре свой глобальный проект «**Киберустойчивость для детей**» с панельной дискуссией о том, как совместный и проактивный подход к онлайн-безопасности может принести пользу детям в цифровой среде. В проекте участвуют родители, преподаватели, учащиеся, НКО и представители правительства.

- **Онлайн-семинары по киберустойчивости** для преподавателей в Азиатско-Тихоокеанском регионе (APAC) в партнерстве с Coalition Against Bullying for Children & Youth (CABCY). В рамках серии вебинаров мы более подробно рассмотрели тему буллинга и кибербуллинга. CABCY помогла участникам разобраться в этой сложной проблеме и понять роль взрослых в поддержке детей.

- **Face-to-Face** — семинар по киберустойчивости для преподавателей в Маниле, проведенный в сентябре 2023 года совместно с отделом школьного образования в Валенсуэле Департамента образования Филиппин в рамках глобального проекта «Лаборатории Касперского» Kids' Cyber Resilience. Цель семинара — помочь филиппинским преподавателям изучить основы кибергигиены, ознакомиться с бесплатными инструментами и ресурсами «Лаборатории Касперского» для обучения детей онлайн-безопасности в классе.

- **Cyber Resilience Day**. В сотрудничестве с городским советом Петалинг-Джая в Малайзии «Лаборатория Касперского» провела интерактивный тренинг по осведомленности о кибербезопасности и киберустойчивости для более чем 250 учащихся и учителей, представляющих десять государственных школ.

- **Семинар по кибербезопасности в Индии**. В партнерстве с Фондом ISAC «Лаборатория Касперского» провела семинар по кибербезопасности для 150 учителей, представляющих более 30 школ. Семинар был организован школой Air Force Bal Bharati в Дели.

[1] Doxing — практика публичного раскрытия личной информации о человеке в интернете без его согласия.
[2] The Singapore Council of Women's Organisations (SCWO).

# Наш вклад в формирование здорового цифрового поведения

## Учим защищаться от цифровых угроз, слушая подкаст

Подкаст «Смени пароль!» — документально-разговорное шоу про информационную безопасность, которое ведут журналист и писатель Алексей Андреев, главный эксперт «Лаборатории Касперского» Сергей Голованов и главный технологический эксперт «Лаборатории Касперского» Александр Гостев.

Подкаст выходит с 2021 года и насчитывает три сезона. Его можно найти на всех популярных подкаст-платформах, включая Apple Podcasts, «Яндекс Музыка», Google Podcasts, VK, Castbox, YouTube.

Ведущие подкаста «Смени пароль!» обсуждают насущные вопросы из мира цифровой безопасности и помогают слушателям разобраться в актуальных киберугрозах для пользователей и бизнеса.

- Куда утекают персональные данные?
- Чем опасен интернет вещей?
- Искусственный интеллект — защита или угроза?

Ответы на эти и многие другие вопросы дают ведущие проекта и приглашенные эксперты. В гостях у подкаста уже побывали представители Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) и крупнейших компаний, таких как «Ростелеком», «Яндекс», «Билайн», OZON, «Газпром-медиа», Райффайзен Банк и Хоум Банк.

Помимо дискуссий в формате аудио, в проекте есть практика очных встреч со слушателями. Так, осенью 2023 года открытая запись подкаста «Смени пароль!» стала первым мероприятием Дискуссионного клуба Музея криптографии. Эксперты обсудили, чем русские шифры отличаются от зарубежных, какая криптографическая защита нужна современному человеку и почему квантовые компьютеры напоминают «яблони на Марсе», а также ответили на многочисленные вопросы слушателей.

## Что в результате?

**>400 000 раз**

**прослушан подкаст за три сезона**

За три года подкаст стал источником актуальной информации об угрозах цифрового мира. Сегодня «Смени пароль!» помогает слушателям создавать более безопасное онлайн-пространство вокруг себя и своего бизнеса.

- Количество прослушиваний третьего сезона в конце 2023 года превысило 100 000, всего подкаст послушали более 400 000 раз.
- С 2022 года «Смени пароль!» регулярно попадает в топ подкастов про технологии на Apple Podcasts и «Яндекс Музыке», а также в тематические подборки от ведущих медиа.
- В 2023 году проект стал финалистом PROBA Awards и Премии Рунета.

## Обеспечиваем онлайн-безопасность детей

# # Задача

**Защита детей в цифровом мире**

«Лаборатория Касперского» несколько лет подряд регулярно проводит опрос по детской онлайн-безопасности. Компания делает это, чтобы понять, как интернет влияет на юных пользователей, чем они интересуются и с какими неприятностями могут столкнуться в Сети.

Согласно опросу 2022 года, проведенному по заказу «Лаборатории Касперского» в крупных городах России[1], 77% детей возраста от 7 до 10 лет познакомились с гаджетами еще до школы. По данным нового опроса, который Компания провела в 2023 году, у подавляющего числа школьников начальных классов (88%) сейчас есть собственный телефон или планшет. Практически каждый старшеклассник имеет собственный гаджет. Начиная со средней школы заметная часть детей проводит в гаджетах практически все свободное время. Родители беспокоятся о том, с кем общается в интернете их ребенок, не сталкивается ли он с агрессией в свой адрес, какие сайты посещает.

**88%**

**младших школьников имеют свой телефон или планшет**

**55%**

**детей за последний год сталкивались в интернете с жестокими видео или роликами со взрослым содержанием**

**29%**

**родителей не знают, какая информация об их детях есть в открытом доступе в интернете**

«Чтобы оградить детей от самых разных онлайн-угроз, необходимо сочетать технические и нетехнические меры защиты. К первым относятся специальные настройки, например семейные аккаунты, программы родительского контроля, антивирус и автоматические определители номеров. К нетехническим — постоянное повышение цифровой грамотности, в том числе в вопросах информационной безопасности. Обучать детей основам цифровой гигиены важно с самого раннего возраста. Со временем это станет эффективнее, чем одни только родительские запреты».

**Андрей Сиденко,**
руководитель направления «Лаборатории Касперского» по детской онлайн-безопасности

[1] Участниками опроса стали более 1 000 пар родитель — ребенок.

# # Решения

## Обучаем детей основам кибербезопасности

Создание безопасной онлайн-среды для детей — задача первостепенной важности, от которой зависит наше будущее. «Лаборатория Касперского» работает над этой задачей как своими силами, так и в партнерстве с министерствами, ведомствами и другими организациями по всему миру.

Чтобы понять, как интернет влияет на юных пользователей, чем они интересуются и с какими неприятностями могут столкнуться в Сети, «Лаборатория Касперского» несколько лет подряд проводит опросы и исследования по детской онлайн-безопасности. Вот некоторые из них, представленные в отчетном периоде.

- **«Взрослые и дети в интернете»** — серия опросов по детской онлайн-безопасности и одноименный отчет. В 2022 году опрос проводила компания Online Interviewer по заказу «Лаборатории Касперского» в мае — июне 2022 года. Всего было организовано 2 008 онлайн-интервью, в которых приняли участие 1 004 пары родитель — ребенок в возрасте от 3 до 18 лет, в крупных городах России. Темы для интервью были выбраны так, чтобы отразить ситуацию в самых разных сферах онлайн-жизни. Полученные результаты вместе с комментариями эксперта «Лаборатории Касперского» по детской онлайн-безопасности помогли взрослым лучше понять интересы юных пользователей и показали, как можно сделать цифровой мир более безопасным для них.

- **Новый опрос по детской онлайн-безопасности**. В мае — июне 2023 года специалисты Online Interviewer провели для нас новое исследование, чтобы выяснить, как обстоят дела с детской онлайн-безопасностью. Они организовали 2 032 онлайн-интервью (всего было опрошено 1 016 пар родитель — ребенок). В результате была получена такая статистика:

  - 29% родителей не знают, какая информация об их детях есть в открытом доступе в интернете;
  - больше половины (55%) детей, по их словам, за последний год сталкивались в интернете с жестокими видео или роликами со взрослым содержанием;
  - треть родителей хотят, чтобы их ребенок работал в сфере IT, когда вырастет. При этом среди детей доля тех, кто хотел бы в будущем работать в этой отрасли, еще выше — 41%;
  - 30% опрошенных родителей в России волнует проблема детской интернет-зависимости. Больше половины (54%) считают, что современные дети зависимы от гаджетов и интернета;
  - начиная с семи лет большинство детей проводят в интернете более часа в день;
  - больше половины родителей (53%) уверены, что через 10–15 лет сенсорные экраны и доски в школах заменят привычные инструменты проведения урока, 39% отметили, что вместо учебников будут планшеты, а 37% считают, что в будущем в обучении будут использоваться голосовые помощники.

- **Дети в интернете — 2022**. «Лаборатория Касперского» регулярно проводит глобальные исследования по теме детской онлайн-безопасности. В основу исследований ложится анонимизированная статистика, собранная решением Kaspersky Safe Kids.

Также в отчетном периоде мы организовали ряд образовательных мероприятий и проектов по кибербезопасности для школьников, учителей и родителей.

- **«Мама, я буду блогером!»**. В июне 2022 года «Лаборатория Касперского» запустила собственный интерактивный мини-сериал «Мама, я буду блогером!». Он состоит из десяти серий по 2–3 минуты, которые выходили до конца 2022 года. Благодаря сериалу вместе с главной героиней Милой дети узнали, как безопасно записывать вайны, избегать мошенников и хейтеров, как отличить фишинговый сайт от настоящего и почему важно следовать правилам этикета в Сети.

- **«Урок цифры»**. В 2022 и 2023 годах «Лаборатория Касперского» продолжила участие в акции «Урок цифры», которую проводит АНО «Цифровая экономика» при поддержке Министерства просвещения Российской Федерации (Минпросвещения России) и Минцифры России. На уроках Компании в 2022 году дети знакомились с темой «Исследование кибератак», а в 2023 году они обучались мобильной безопасности. За 2023 год школьники прошли урок более 2 млн раз. Они узнали, каким бывает вредоносное ПО для мобильных устройств, как обезопасить свои данные в интернете, а также познакомились с миром профессий в области кибербезопасности.

Подробнее о проекте читайте на с. 105

- **«Цифровой ликбез»**. «Лаборатория Касперского» и АНО «Цифровая экономика» при поддержке Минпросвещения России и Минцифры России создали серию коротких мультфильмов для детей про цифровую безопасность и приватность. В 2023 году они пополнили подборку полезных материалов всероссийского просветительского проекта «Цифровой ликбез».

- **Курс для школьников по кибербезопасности**. В октябре 2023 года «Лаборатория Касперского» открыла всем желающим доступ к первым материалам курса «Основы информационной безопасности» для учеников седьмого класса. Через некоторое время будет доступен курс для школьников 8–11-х классов. Это практико-ориентированный курс, его могут использовать учителя на уроках информатики и в рамках внеурочной деятельности, а также родители и сами учащиеся.

- **Образовательные мероприятия для учеников и учителей в России и странах СНГ**. В 2022–2023 годах было проведено более 150 онлайн- и офлайн-мероприятий для учащихся и учителей средних общеобразовательных школ, а также для родителей в 26 регионах России и в странах СНГ.

- **Kaspersky Safe Family Spain**. 35 спектаклей по книге «Kasper, Sky и зеленый медведь», обучающей основам кибербезопасности, были поставлены для 3 684 учеников испанских школ в рамках инициативы Safe Family.

- **#ShareAware Hub**. «Лаборатория Касперского» помогает родителям и детям повысить их безопасность в интернете с помощью советов и подсказок. На хабе представлено множество полезных материалов об использовании мультимедиа в интернете.

- **Kids on the Internet** — разработанный Компанией курс о безопасности детей в интернете. Он предназначен для детей и их родителей, а также для всех, кто использует интернет.

- **Hacker:HUNTER**. Компания приняла участие в производстве сериала о реальных киберинцидентах. В 2023 году вышел новый сезон, который посвящен тому, как злоумышленники вовлекают детей в свою деятельность и растят из них хакеров и как правоохранительные органы противостоят им.

- **«Киберазбука»**. Чтобы помочь детям и их родителям развивать цифровую грамотность, эксперты Компании подготовили познавательную книгу для детей и их родителей о популярных явлениях из мира технологий с советами о том, как защититься от распространенных цифровых угроз. В книге от А до Я читатели знакомятся с новыми технологиями, распространенными киберрисками и инструментами для защиты от них. «Киберазбука» доступна на английском языке для скачивания всеми желающими на сайте Компании. Позднее будут доступны также версии азбуки на русском, французском, итальянском и испанском языках.

В 2023 году проект «Взрослые и дети» — весь комплекс мероприятий «Лаборатории Касперского» по онлайн-безопасности детей и их родителей — стал финалистом премии Proba Awards.

## Сотрудничаем с IT-компаниями и регуляторами для защиты детей в интернете

Мы стремимся сделать онлайн-пространство, в котором живут современные дети, как можно более безопасным. «Лаборатория Касперского» — один из основателей Альянса по защите детей в цифровой среде, который был создан крупнейшими IT-компаниями России в сентябре 2021 года.

В 2022 году в рамках Альянса «Лаборатория Касперского», «Яндекс» и VK запустили пилотный проект по выявлению и блокировке контента, связанного с распространением детской порнографии, а также так называемого сексуализированного контента с участием несовершеннолетних.

В октябре 2023 года Альянс по защите детей в цифровой среде провел в Казани роуд-шоу «Маршрут построен: тропы безопасности в Сети», на котором были озвучены результаты исследования «Лаборатории Касперского»: большинство родителей в России (87%) предпринимают те или иные меры, чтобы оградить своего ребенка от опасностей в интернете. Однако выяснилось, что только 48% взрослых сами следуют всем установленным правилам, что снижает эффективность этих мер. Эксперты Компании напомнили родителям о необходимости быть хорошим примером для детей и составили чек-лист с рекомендациями, на что обратить внимание при выборе подходящего решения родительского контроля.

В декабре 2023 года Альянс по защите детей в цифровой среде организовал в Санкт-Петербурге двухдневный образовательный марафон «Безопасная цифра», посвященный правилам безопасного поведения в интернете. Гости марафона — в основном дети и подростки — могли поучаствовать в IT-квизе, тематических мастер-классах, круглых столах и семинарах. Родители и учителя обсудили вопросы цифровой безопасности. Также была организована деловая программа с участием IT-экспертов, представителей органов власти, бизнеса и общественных организаций. В марафоне участвовали основатели Альянса — «Лаборатория Касперского», «Яндекс», VK, «Ростелеком», «Билайн» и «МегаФон».

## Kaspersky Safe Kids

Мы стремимся защитить детей от онлайн-угроз и создать условия, в которых ребенок сможет максимально безопасно пользоваться интернетом. Для этого мы предлагаем наше решение Kaspersky Safe Kids — приложение родительского контроля, которое ограждает ребенка от контента, не соответствующего его возрасту, и помогает формировать полезные цифровые привычки. Решение представлено в том числе в бесплатной версии.

## Основные функции Kaspersky Safe Kids

### Безопасный поиск
Приложение взаимодействует с поисковыми системами и блокирует нежелательные запросы. Раз в неделю родители получают отчеты о том, что искал ребенок в интернете.

### Контроль использования приложений
Базовая функция — блокировка приложений, которые не подходят ребенку. Также предусмотрен контроль времени использования (можно настроить временные интервалы и назначить выходные дни).

### Контроль экранного времени
Приложение позволяет установить разрешенное количество часов экранного времени в день и заблокировать устройство, если лимит достигнут. Также можно отключать устройство в определенные промежутки времени.

### Установка безопасного периметра
Благодаря опции с GPS приложение отправляет уведомление родителям, если во время учебы ребенок покинул установленную локацию (например, школу).

### Мониторинг потенциально опасных контактов в соцсетях
Родители не могут читать сообщения ребенка, но приложение уведомляет их о самом факте переписки и дает возможность увидеть профиль собеседника.

В 2023 году мы дважды обновили решение Kaspersky Safe Kids. В новых версиях усовершенствованы дизайн и интерфейс приложения, появился новый функционал управления экранным временем, добавились видео с советами по воспитанию детей, легкой настройке функций и другой полезной для родителей информацией. Приложение можно установить на стационарные компьютеры и мобильные устройства со всеми популярными операционными системами. Дети теперь могут запрашивать у родителей дополнительное время на использование устройства, а родителям достаточно одобрить или отклонить запрос.

**7**
наград AV-TEST

**7**
наград AV-Comparatives

**>1 млн**
скачиваний по всему миру

**106 млн**
заблокированных сайтов

**Результаты тестирования Kaspersky Safe Kids**

По данным отчета независимой лаборатории AV-TEST, вышедшего в январе 2023 года, Kaspersky Safe Kids заблокировал:

- 92% потенциально неприемлемых ресурсов на Windows (по сравнению с 90% в 2021 году);
- 87% потенциально неприемлемых ресурсов на Android (в 2021 году — 85%);
- почти 100% нежелательного контента «для взрослых» на Windows.

## Наш вклад в защиту детей в киберпространстве

### Обучаем кибербезопасности со спектаклем «Kasper, Sky и зеленый медведь»

Число детей, использующих цифровые технологии, постоянно увеличивается. Вместе с этим в киберпространстве распространяются новые формы цифровых угроз, особенно опасные для детей из-за отсутствия у них опыта и знаний о таящихся там угрозах. Киберзапугивание, секс-вымогательство и другие виды притеснений стали проблемой, от которой дети и подростки страдают каждый день, поэтому «Лаборатория Касперского» сделала своей целью обеспечение их защиты в онлайн-мире.

В рамках инициативы Safe Family Компания запустила в Испании спектакль «Kasper, Sky и зеленый медведь» — адаптацию книги Марлис Слегерс для детей в возрасте от 6 до 9 лет, которая знакомит их с цифровым миром и учит использовать интернет безопасно. «Лаборатория Касперского» превратила эту книгу в кукольное представление, которое не только обучает детей, но и стремится донести до учителей и родителей, что киберугрозы сегодня выходят за рамки простого вируса.

Благодаря усилиям «Лаборатории Касперского» тысячи детей, педагогов и родителей обучились безопасному использованию интернета. А кампания «Kasper, Sky и зеленый медведь» была удостоена наград на церемонии Social Business Awards 2019:

- «Лучший ответственный проект в сфере защиты детей»;
- «Лучший проект социальной ответственности в сфере кибербезопасности»;
- «Лучший ответственный проект в борьбе с буллингом».

Кроме того, фонд Gala Acción Social наградил «Лабораторию Касперского» знаком отличия «Компания с лучшими действиями в борьбе за защиту детей».

### Что в результате?

**16 805** детей

в **106** школах

просмотрели спектакль с момента запуска проекта в 2018 году

В течение 2022/2023 учебного года в рамках инициативы состоялось

**35** представлений, которые посетили

**3 684** ученика.

[1] Ближний Восток, Турция и Африка.

## Наши достижения

«Лаборатория Касперского» в Испании получила награды Social Business Awards 2023 за свою деятельность в области борьбы с цифровым гендерным насилием. Компания была удостоена наград в следующих категориях: «Лучшая корпоративная социальная ответственность в секторе кибербезопасности», «Лучшая инициатива по предотвращению гендерного насилия в секторе кибербезопасности» и «Лучший проект по интернет-безопасности в секторе кибербезопасности». Кроме того, организатор премии Gala Acción Social присудил Компании специальную награду за лучшие инициативы в области кибербезопасности, а также назвал ее Платиновой компанией и Компанией года.

## Наши планы на 2024 год

- Развитие партнерства с международными правоохранительными организациями, коалициями и НКО, нацеленного на борьбу со сталкингом.
- Выпуск нового отчета о состоянии сталкерского ПО.
- Запуск курса по кибергигиене на двух языках.
- Начало продвижения проекта Kids Cyber Resilience в регионах СНГ и МЕТА[1].
- Выпуск аналитического отчета по детской онлайн-безопасности с данными опроса за 2023 год.
- Публикация «Киберазбуки» для самых юных пользователей на русском, испанском, итальянском и французском языках.

# Борьба с киберпреступностью

Наша цель — защищать мир от киберпреступлений. Эффективное противостояние киберпреступности требует объединения усилий всего общества, поэтому мы сотрудничаем с правоохранительными органами и вносим вклад в совершенствование законодательства в этой сфере.

## Ключевые документы

- Внутренняя политика «Лаборатории Касперского», определяющая работу с запросами правоохранительных органов[1] (утверждена в сентябре 2021 года топ-менеджерами Компании).
- Соглашение с Интерполом о совместной борьбе с киберпреступлениями.
- Меморандумы о сотрудничестве с различными агентствами по кибербезопасности и правоохранительными органами.

## Как мы сотрудничаем с правоохранительными организациями

Большинство кибератак совершаются злоумышленниками или хакерами с целью получения финансовой прибыли. Однако их мотивы могут быть также личными или политическими. Киберпреступления совершают частные лица и организации, которые используют продвинутые методики и хорошо подкованы технически.

Киберпреступления приводят к серьезным последствиям как для компаний, так и для частных лиц. В основном это финансовый ущерб, а также утрата доверия и репутационные потери. Киберпреступность не знает границ, и ни одна страна или организация не может справиться с ней в одиночку. Эта задача требует всестороннего подхода и объединения усилий.

Правоохранительные органы нередко обращаются за консультациями к IT-компаниям, которые обладают высоким уровнем экспертизы в области кибербезопасности. «Лаборатория Касперского» активно помогает в исследовании киберпреступлений. При этом мы очень серьезно подходим к вопросу прозрачности в совместной работе — у нас есть четкий порядок работы с запросами от правоохранительных органов, который регулируется внутренней политикой, и критерии для юридической проверки каждого запроса. Если запрос не соответствует нашим критериям, мы можем отклонить его или оспорить. Важно отметить, что мы не предоставляем доступ к нашей инфраструктуре или данным.

[1] Processing Law Enforcement and Government Requests for Disclosure of Data.

# # Задача

## Содействие в исследовании киберпреступлений

Киберпреступность не имеет границ, поэтому «Лаборатория Касперского» регулярно участвует в операциях и исследованиях, проводимых совместно с глобальным сообществом специалистов по IT-безопасности, международными организациями, такими как Интерпол, правоохранительными органами и центрами реагирования на компьютерные инциденты. Для исследования киберпреступлений мы предоставляем нашу экспертизу и необходимую техническую информацию, регулярно проводим тренинги.

# # Решения

## Защищаем киберпространство вместе с Интерполом

В 2014 году мы начали сотрудничество с Интерполом, подписав первое соглашение о совместной борьбе с киберпреступлениями. В 2019 году мы заключили новое соглашение на пять лет, которое предусматривает значительное расширение сферы нашего взаимодействия.

### Наша поддержка Интерпола

- Делимся экспертной информацией о новейших видах вредоносных программ и методах кибератак.
- Участвуем в совместных операциях по всему миру для выявления и пресечения киберпреступлений.
- Проводим обучающие программы в области кибербезопасности и консультируем сотрудников Интерпола и других правоохранительных органов.

Как мы помогали Интерполу в 2022–2023 годах:

- наши специалисты содействовали Интерполу в проведении операций Africa Cyber Surge и Africa Cyber Surge II, нацеленных на борьбу с киберпреступностью на Африканском континенте;
- под эгидой Интерпола мы организовали обучение более 100 представителей правоохранительных органов из разных стран по направлениям «Реакция на инциденты» и «Анализ вредоносных программ»;
- Виталий Камлюк, руководитель Глобального центра исследований и анализа угроз в Азиатско-Тихоокеанском регионе «Лаборатории Касперского», выступил с докладом на международной конференции по кибербезопасности INTERPOL Global Cybercrime Conference (IGCC) 2023. Он представил обзор крупнейших в мире эпидемий компьютерных червей и описал меры, которые были приняты для борьбы с ними.

## Поддерживаем международную кооперацию

«Лаборатория Касперского» тесно сотрудничает с многочисленными международными организациями и правоохранительными органами, участвуя в совместных операциях, исследованиях киберугроз, кибердипломатии, содействуя развитию открытого и безопасного интернета.

**33**
**международных и российских партнера по защите киберпространства**

**>10**
**меморандумов о взаимопонимании заключено с международными организациями и правительственными учреждениями**

**>60**
**организаций участвуют в обмене новыми вредоносными самплами**[1]

Например, в рамках альянса No More Ransom, который был создан совместно с Европолом и другими партнерами, мы помогаем жертвам вредоносных программ-вымогателей в 30 странах восстановить свои зашифрованные данные, не выплачивая выкуп. За семь лет работы этот альянс помог примерно 2 млн пользователей по всему миру восстановить свои данные.

**Наши партнеры в борьбе с киберпреступностью и содействии устойчивому развитию цифрового пространства**

- Интерпол
- Альянс No More Ransom
- Коалиция против сталкерского ПО (Coalition Against Stalkerware)
- Женевский диалог (Geneva Dialogue)
- Парижский призыв к доверию и безопасности в киберпространстве (Paris Call for Trust and Security in Cyberspace)
- Совет Европы
- Cybermalveillance.gouv.fr (GIP ACYMA) (Франция)
- Renaissance Numérique (Франция)
- World Internet Conference (член Экспертно-консультативного комитета высокого уровня)
- China Industrial Control System CERT (отраслевой партнер)
- Промышленный консорциум интернета вещей (Industry IoT Consortium, США)
- Международный союз электросвязи
- Международная организация по стандартизации (ISO)
- Альянс по защите детей в цифровой среде (Россия)
- АНО «Цифровая экономика» (Россия) и многие другие

Мы также охотно делимся нашей экспертизой в сфере кибербезопасности, выступая на крупных конференциях и мероприятиях, таких как RSA Conference и Virus Bulletin, публикуем информацию в собственных блогах и проводим бесплатные вебинары по кибербезопасности. Кроме того, в 2023 году мы расширили функционал бесплатных сервисов на портале Kaspersky Threat Intelligence, который позволяет найти информацию о киберугрозах в режиме реального времени.

В 2022–2023 годах в рамках борьбы с киберпреступностью «Лаборатория Касперского» расширяла сотрудничество с международными и национальными организациями, в частности подписала ряд важных соглашений, включая соглашения о сотрудничестве с национальными центрами по кибербезопасности, а также меморандумы о сотрудничестве с Университетом Корё, Советом по кибербезопасности ОАЭ и Министерством образования Италии.

В рамках Всемирной конференции в области интернета в Китае Компания получила награду World Leading Technology за разработку решения Kaspersky Automotive Secure Gateway, а глава Компании Евгений Касперский был удостоен звания Special Contributor за заслуги в продвижении глобального сотрудничества в области кибербезопасности.

В 2023 году «Лаборатория Касперского» получила награду Alliance of Public Private Cybercrime Stakeholders (основан под эгидой Сил полиции Сингапура) за вклад в формирование киберустойчивого мира.

Помимо этого, Компания занималась формированием отзывов и предложений к проекту всеобъемлющей международной конвенции о противодействии использованию информационных технологий в преступных целях, которая разрабатывается под эгидой ООН. Мы также направили свои предложения в рамках инициативы ООН «Глобальный цифровой общественный договор» с акцентом на вопросы повышения цифровой грамотности.

В 2022–2023 годах наши эксперты принимали участие в многочисленных форумах и конференциях по кибербезопасности, среди которых были:

- Рабочая группа открытого состава ООН по ИКТ (в ходе неформального диалога под эгидой председателя Рабочей группы);
- Пятые межсессионные консультации Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях;
- Африканский форум по управлению интернетом;
- Сессия по цифровой безопасности в рамках инициативы ООН «Глобальный цифровой общественный договор»;
- Рабочие группы «Женевского диалога»;
- Международная конференция Интерпола по кибербезопасности;
- Форум ООН по управлению интернетом;
- Формат B20 (Business 20) в рамках G20.

Кроме того, мы сотрудничаем с другими IT-компаниями по всему миру путем обмена образцами вредоносного ПО (более 60 компаний).

[1] Образец вредоносного ПО.

# # Задача

**Улучшение законодательной базы**

Современные технологические вызовы требуют более гибкого и адаптивного законодательства. Злоумышленники постоянно совершенствуют свои методы, поэтому законы должны позволять эффективно реагировать на новые угрозы. Кроме того, совершенствование законодательства помогает стандартизировать правовые механизмы на мировом уровне, обеспечивая более эффективный обмен информацией и экстрадицию преступников.

# # Решения

**Совершенствуем законодательство в сфере борьбы с киберпреступностью**

«Лаборатория Касперского» постоянно участвует в разработке законодательства, политик и других документов, направленных на обеспечение кибербезопасности в мире. Наши эксперты делятся своими знаниями и опытом в области защиты критической инфраструктуры, борьбы с киберпреступностью, а также защиты данных и других смежных тем. Поскольку регулирование в сфере кибербезопасности ужесточается во многих странах, мы все чаще получаем запросы от национальных, региональных и международных организаций на предоставление экспертной помощи. Некоторые из таких экспертных материалов доступны в нашем блоге о политике кибербезопасности.

Мы регулярно обмениваемся информацией с заинтересованными сторонами по вопросам кибербезопасности и киберпреступности на уровне ООН. В частности, начиная с 2020 года мы активно участвуем в неформальном диалоге ООН под эгидой председателя Рабочей группы открытого состава по кибернормам[1] (РГОС), где обсуждаются различные вопросы в сфере кибербезопасности, меры по повышению доверия в киберпространстве и развитие компетенций. В отчетном периоде Компания участвовала в двух встречах, на которых презентовала свои предложения в области использования ИИ с акцентом на кибербезопасность, а также комментарии к ежегодному отчету РГОС.

## Наш вклад в борьбу с международной киберпреступностью

### Участвуем в операции Africa Cyber Surge

Индустрия информационной безопасности в Африке не так хорошо развита, как в других регионах, поэтому ее страны более уязвимы для кибератак. Чтобы помочь Интерполу бороться с киберпреступностью в Африке, «Лаборатория Касперского» предоставила ему данные об угрозах в ходе операции Africa Cyber Surge.

Первая часть операции проходила с июля по ноябрь 2022 года и включала серию оперативно-разыскных мероприятий против злоумышленников. Вторая часть — Africa Cyber Surge II — началась в апреле 2023 года и продлилась четыре месяца, охватив 25 африканских стран.
Вместе с другими партнерами Интерпола «Лаборатория Касперского» передала международному агентству индикаторы компрометации (IoC), включая информацию о вредоносных серверах, фишинговые ссылки и домены, а также мошеннические IP-адреса.

### Что в результате?

Благодаря помощи «Лаборатории Касперского» следователям удалось обнаружить скомпрометированную инфраструктуру и задержать злоумышленников, подозреваемых в совершении киберпреступлений в Африке. В результате операции были арестованы 14 человек, а также выявлена сетевая инфраструктура, с которой связаны финансовые потери более чем на $40 млн.

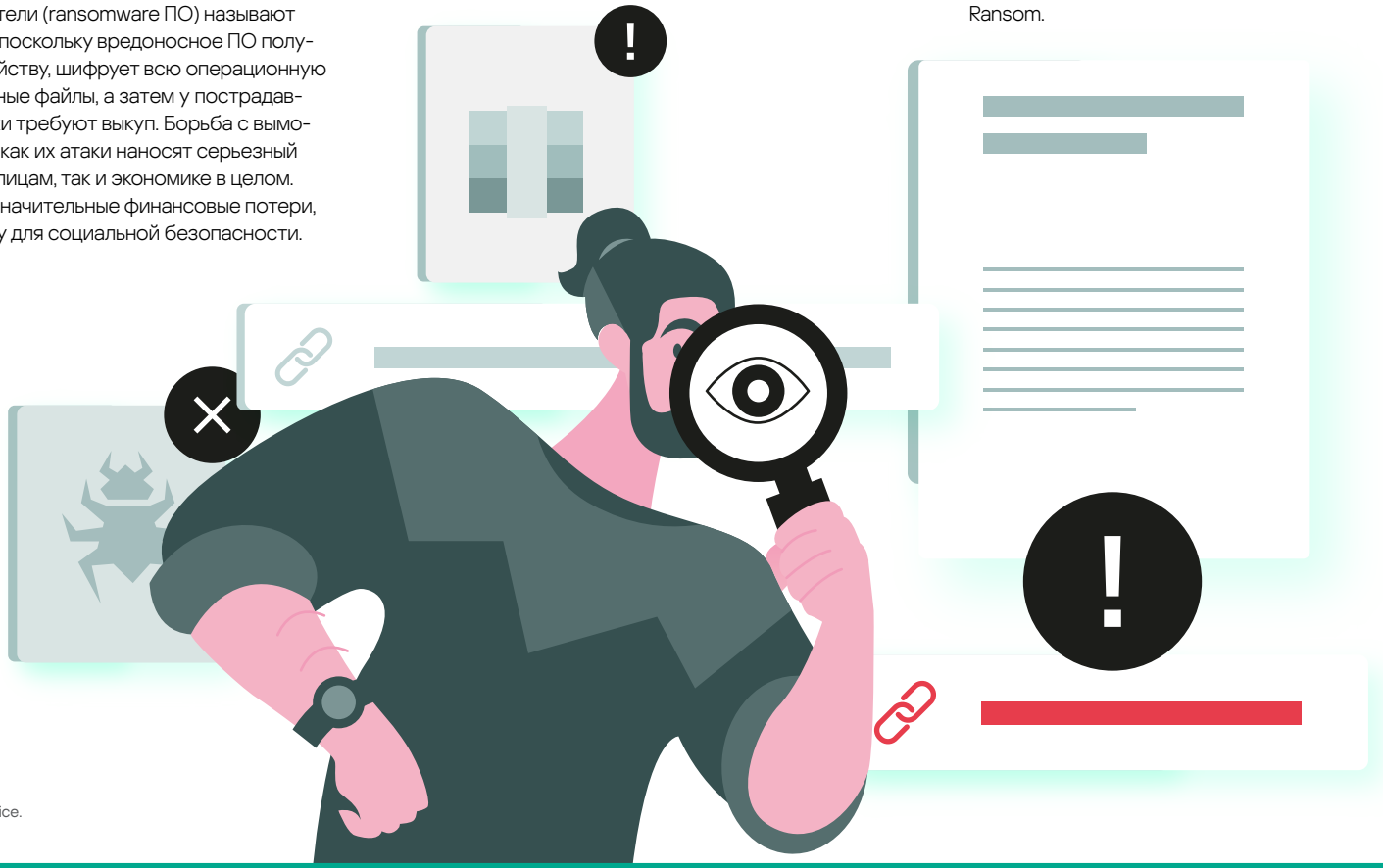
«Операция Africa Cyber Surge II помогла усилить борьбу с киберпреступностью в странах-участницах, а также укрепить партнерские отношения между ключевыми заинтересованными сторонами, такими как отделы по реагированию на компьютерные инциденты и интернет-провайдеры. В дальнейшем это будет способствовать снижению глобального влияния киберпреступности, а также защите сообществ в Африканском регионе».

**Юрген Шток,**
Генеральный секретарь Интерпола

# # Задача

**Защита пользователей от программ-вымогателей**

Программы-вымогатели (ransomware ПО) называют шифровальщиками, поскольку вредоносное ПО получает доступ к устройству, шифрует всю операционную систему или отдельные файлы, а затем у пострадавших злоумышленники требуют выкуп. Борьба с вымогателями важна, так как их атаки наносят серьезный ущерб как частным лицам, так и экономике в целом. Они могут вызвать значительные финансовые потери, а также несут угрозу для социальной безопасности.



[1] Ransomware-as-a-Service.

# # Решения

Раскрываем схемы атак, анализируем инструменты злоумышленников и обновляем собственные утилиты для дешифровки в рамках инициативы No More Ransom.

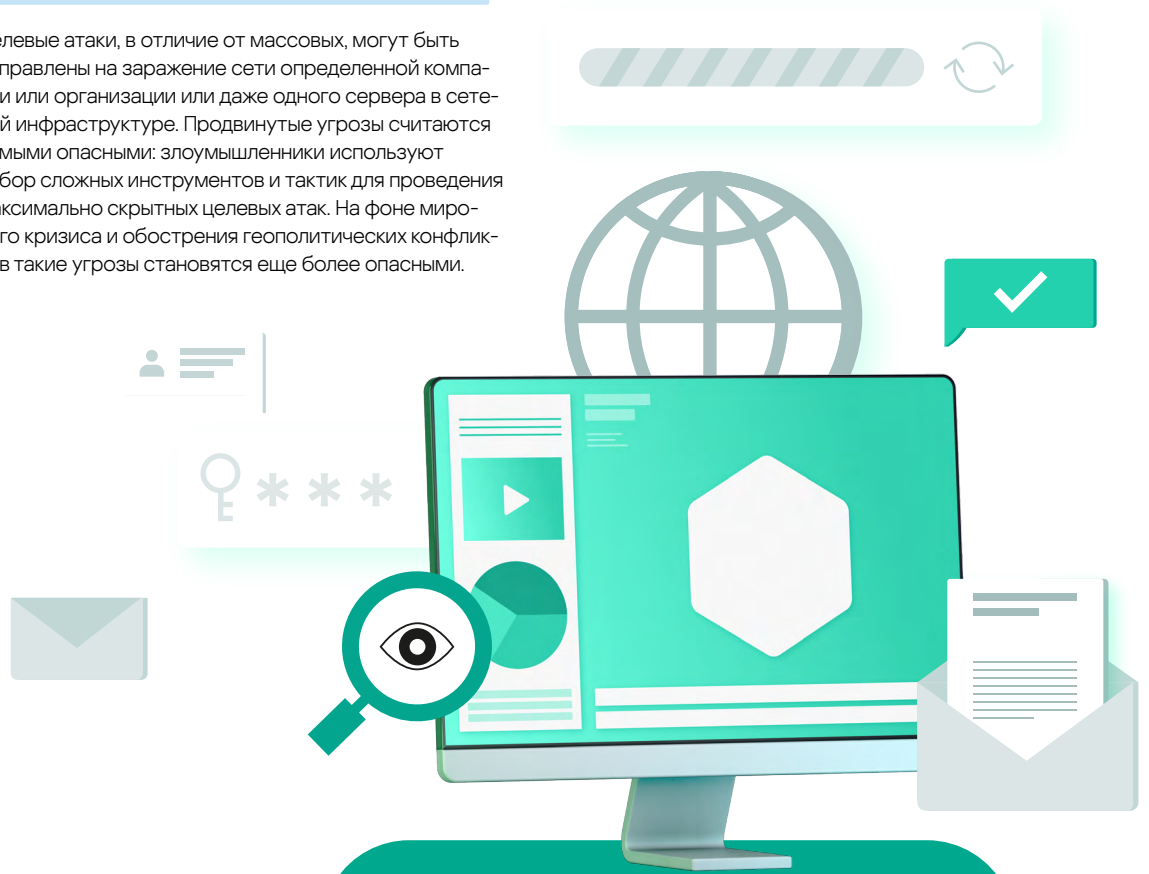
В отчетном периоде «Лаборатория Касперского»:

- обнаружила и помогла обезвредить атаки шифровальщиков с применением эксплойта нулевого дня (написанного для использования уязвимости, о которой еще не знает разработчик). В числе мишеней были предприятия малого и среднего бизнеса на Ближнем Востоке, в Северной Америке, а ранее и в азиатских регионах;
- обновила инструмент расшифровки для жертв программы-шифровальщика Conti. «Лаборатория Касперского» обновила общедоступный инструмент расшифровки на портале Noransom для версии, которая использовалась для атак на коммерческие компании и государственные учреждения;
- проанализировала билдер Lockbit 3. Lockbit — один из самых распространенных типов шифровальщиков. Он распространяется среди партнеров по модели RaaS[1], предлагая участникам до 80% от суммы выкупа. В сентябре 2022 года произошла утечка билдера Lockbit 3, позволяющего любому пользователю сконструировать свою собственную версию программы-шифровальщика. Глобальная команда реагирования на киберинциденты «Лаборатории Касперского» проанализировала билдер, чтобы разобраться в методологии конструирования шифровальщика и определить возможности для дополнительного анализа. Этот инструмент позволял любому создать свою собственную версию программы-вымогателя.

# # Задача

**Исследование целевых (таргетированных) атак и продвинутых угроз**

Целевые атаки, в отличие от массовых, могут быть направлены на заражение сети определенной компании или организации или даже одного сервера в сетевой инфраструктуре. Продвинутые угрозы считаются самыми опасными: злоумышленники используют набор сложных инструментов и тактик для проведения максимально скрытных целевых атак. На фоне мирового кризиса и обострения геополитических конфликтов такие угрозы становятся еще более опасными.



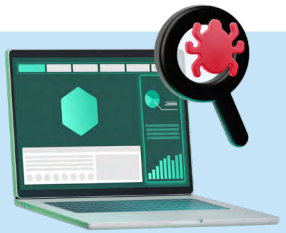
# # Решения

Эксперты глобального центра исследований и анализа угроз (GReAT) «Лаборатории Касперского» и команда Kaspersky Cyber Threat Intelligence пристально следят за множеством APT-групп, анализируют текущие тренды и прогнозируют развитие ландшафта киберугроз, чтобы оставаться на шаг впереди злоумышленников и обеспечивать безопасность клиентов «Лаборатории Касперского».

Примеры кибергруппировок, за которыми велось наблюдение, и их атак.

- **Разбор угроз группы Cuba Ransomware**. В 2023 году «Лаборатория Касперского» опубликовала результаты исследования нового киберинцидента с участием Cuba. Это группа вымогателей, которая атаковала многие компании по всему миру, в том числе торговые, логистические, финансовые, государственные учреждения и промышленные предприятия в Северной Америке, Европе, Океании и Азии. Наши эксперты разобрали историю, а также техники, тактики и процедуры известной кибергруппы.
- **Ошибки группы Andariel и новое семейство зловредов**. Эксперты «Лаборатории Касперского» обнаружили новый инструмент в арсенале кибергруппы Andariel, которая входит в состав Lazarus. Это троянец удаленного доступа, который получил название EarlyRat. Зловред может попадать на устройство через уязвимость, найденную с помощью эксплойта Log4j, либо через ссылки в фишинговых документах.
- **Новая группа GoldenJackal**. Данная группа ведет свою деятельность с 2019 года и обычно атакует правительственные и дипломатические организации на Ближнем Востоке и в Южной Азии. Эксперты «Лаборатории Касперского» начали следить за этой группой в середине 2020 года. Ее главная особенность — специфический набор зловредных имплантов, которые распространяются через съемные диски и используются для контроля целевых компьютеров, извлечения данных, кражи учетных записей, сбора информации о локальной системе и действиях жертвы в интернете, а также для создания и отправки снимков экрана.
- **Кибергруппа ToddyCat усложняет свои кампании кибершпионажа**. Эксперты «Лаборатории Касперского» рассказали о новом наборе вредоносных инструментов, о программах, используемых для кражи и эксфильтрации данных, а также о методах, применяемых этой активной группой для перемещения в инфраструктуре и проведения шпионских операций.

# Итоги работы по направлению борьбы с киберпреступностью



С ноября 2022 года по октябрь 2023 года[1] наш веб-антивирус заблокировал

**112 922 612**

**уникальных вредоносных объектов.**

В целом за этот период решения «Лаборатории Касперского»:

- отразили 437 414 681 вредоносную атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира;
- обнаружили 106 357 530 уникальных вредоносных URL, на которых происходило срабатывание веб-антивируса;
- отразили атаки шифровальщиков на компьютерах 193 662 уникальных пользователей;
- предотвратили атаки майнеров на 1 140 573 уникальных пользователя;
- заблокировали попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на устройствах 325 225 уникальных пользователей.

В этих результатах — вклад четырех наших подразделений: Лаборатории исследования киберугроз (AMR), Центра исследований безопасности промышленных систем и реагирования на инциденты информационной безопасности (ICS CERT), команды расследования компьютерных инцидентов и команды Глобального центра исследования и анализа угроз (GReAT).

## Наши планы на 2024 год

- Участие в формировании правового поля по борьбе с киберпреступностью.
- Обучение и повышение квалификации экспертов, проведение тренингов по актуальным темам в области кибербезопасности.
- Сотрудничество с внешними организациями и установление партнерских отношений с государственными учреждениями для обмена информацией о киберугрозах.
- Регулярное обновление ПО и технологий для надежной защиты от последних угроз.

[1] См. отчет «Лаборатории Касперского»: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf.

ESG-направление

# Технологии будущего

**18**

продуктов и сервисов включены в экосистему промышленной кибербезопасности Kaspersky OT CyberSecurity (KOTS)

**2**

российских ИБ-стандарта разработано Компанией

**>1 000**

крупных промышленных клиентов по всему миру защищены решениями Kaspersky Industrial CyberSecurity (KICS)

# Защита промышленных предприятий и критической инфраструктуры

Наша цель — обеспечить бесперебойное функционирование киберфизических систем на объектах критической инфраструктуры и в промышленности с помощью экосистемы современных технологий, знаний и экспертизы.

Защищены решениями «Лаборатории Касперского»

**12%**
ведущих производителей удобрений

**10%**
крупнейших международных нефтегазовых компаний

**15%**
ядерных реакторов по всему миру

# Что такое критическая инфраструктура

**Критическая инфраструктура (КИ)** — это системы управления технологическими процессами в отраслях, имеющих стратегическую важность для экономики, государственных институтов и общества.

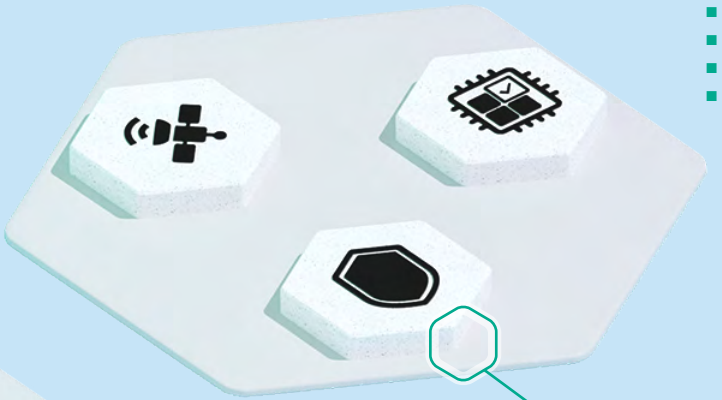
## Критическая инфраструктура в промышленности

### Тяжелая промышленность

- Добыча топлива
- Производство и поставка электроэнергии
- Горнорудная промышленность
- Металлургия
- Химическая промышленность
- Автомобильное производство
- Машиностроение
- Производство стройматериалов
- Целлюлозно-бумажная отрасль

### Легкая промышленность и социальная инфраструктура

- Логистика и транспорт
- Пищевая промышленность
- Фармацевтика
- Объекты ЖКХ



### Критически важное производство

- Оборонная промышленность
- Ракетно-космическая отрасль
- Производство микрочипов и электроники

# Как мы защищаем критическую инфраструктуру и промышленные предприятия

## Обеспечиваем промышленную кибербезопасность

# # Задача

### Исключение киберинцидентов на промышленных объектах наших клиентов

На сегодняшний день промышленная кибербезопасность — это активирующая технология для устойчивого развития предприятий. Наши решения могут использоваться для защиты предприятий из любой отрасли с любым уровнем цифровизации — с классическим или новейшим парком компьютерного оборудования.

Согласно нашему краткому обзору основных инцидентов промышленной кибербезопасности за второе полугодие 2023 года, подавляющее большинство атакованных организаций относятся к производственному сектору.

**Взломы критической инфраструктуры в 2022–2023 годах**

- Остановлено производство автомобильных запчастей компании ThyssenKrupp из-за кибератаки.
- Производитель элементов питания Varta приостановил производство на всех предприятиях компании из-за взлома IT-систем.
- Хакеры взяли под контроль IT-систему, связанную с одной из насосных станций компании Municipal Water Authority of Aliquippa, которая предоставляет услуги водоснабжения в американском штате Пенсильвания.
- Кибератака на международного оператора контейнерных терминалов DP World привела к серьезным сбоям в работе международных портов Австралии.
- Почти 2 млн жителей Техаса столкнулись с перебоями в подаче воды в результате кибератаки на их водопроводную компанию NTMWD.
- Группа хактивистов SiegedSec взломала Национальную ядерную лабораторию Айдахо, которая является центром ядерных исследований Министерства энергетики США, и похитила конфиденциальные данные.

## Отрасли, наиболее подверженные кибератакам во втором полугодии 2023 года


По данным Kaspersky ICS CERT[1], в 2023 году вредоносные объекты[2] были заблокированы на 38,5% компьютеров автоматизированных систем управления (АСУ).

### Наш вклад в минимизацию рисков и сокращение ущерба от кибератак на производственные предприятия

**Помогаем клиентам экономить деньги с помощью наших решений**

Кибератаки могут привести к перебоям в работе или полной остановке процессов и услуг, что может повлечь снижение экономических показателей. Внедрение наших продуктов для защиты критической инфраструктуры и промышленных предприятий позволяет избежать этого. В апреле 2021 года компания Forrester провела исследование того, как наше решение для промышленной безопасности KICS for Networks повлияло на экономические показатели крупного поставщика электроэнергии, сравнив сумму возможных убытков нашего клиента со стоимостью лицензии KICS.

### Что в результате?

**$2,5 млн**
сокращение риска нарушений безопасности

**$338 тысяч**
сокращение возможного ущерба для оборудования

**$1,6 млн NPV[3]**

**135% ROI**

Исследователи пришли к выводу, что решение окупилось всего за восемь месяцев, а показатель ROI составил 135% за три года. Кроме того, внедрение KICS помогло предприятию соотнести реальную и задокументированную сеть и внесло прозрачность в отношении сетевых активов и точек доступа.

1 Industrial Control Systems Cyber Emergency Response Team — группа реагирования на киберугрозы в промышленных системах управления.
2 Все виды угроз.
3 Чистая приведенная стоимость (Net Present Value) — финансовый показатель величины денежных средств, которые инвестор ожидает получить от проекта, после того как денежные притоки окупят его первоначальные инвестиционные затраты и периодические денежные оттоки, связанные с осуществлением проекта.

# # Решения

## Защищаем все уровни систем и сетей промышленного предприятия

## KOTCS

Мы стремимся предоставить каждому заказчику, независимо от его отрасли, уровня зрелости и сложности запроса, актуальную для него ценность от внедрения систем кибербезопасности.

Наша экосистема киберфизической безопасности промышленных предприятий Kaspersky OT CyberSecurity (KOTCS) снижает угрозы кибератак и исключает возможность возникновения недопустимых событий. Она содержит:

- **технологии**: полный спектр защитных решений, протестированных вендорами АСУ ТП;
- **знания**: достоверная аналитика угроз в АСУ ТП и специальные тренинги;
- **экспертизу**: набор экспертных сервисов для комплексной промышленной безопасности.

Экосистема KOTCS состоит из 18 продуктов и сервисов для промышленных предприятий, разработанных специалистами «Лаборатории Касперского» с высочайшим уровнем экспертизы — 15 лет опыта в защите промышленных объектов и 10 лет развития направления KICS. Это самая зрелая экосистема на рынке кибербезопасности, которая обеспечивает защиту всех уровней промышленного предприятия с управлением из единого центра. Она имеет расширенный функционал защиты от всех киберфизических угроз (например, собственную уникальную систему Antidrone) и способна обеспечить безопасность промышленных объектов, включая атомные электростанции, к надежности которых предъявляются самые строгие требования регулирующих органов.

## KOTCS — защита на каждом уровне

### Уровень 3. Корпоративные системы

- Конвергенция IT и OT, корреляция данных из всех доступных источников.
- Унифицированные процессы и подходы к обеспечению безопасности с помощью технологии расширенного обнаружения и реагирования на угрозы гибридного типа (Hybrid XDR).
- Программы обучения, консалтинг, расширенная аналитика угроз.

### Уровень 2. Мониторинг и управление

- IIoT[1], возможности подключения, охрана периметра и защита систем автоматизации верхнего уровня (SCADA).
- Контроль доступа и использования, аудит и видимость OT-систем.
- Экспертная поддержка на месте.

### Уровень 1. Контроллеры и защита

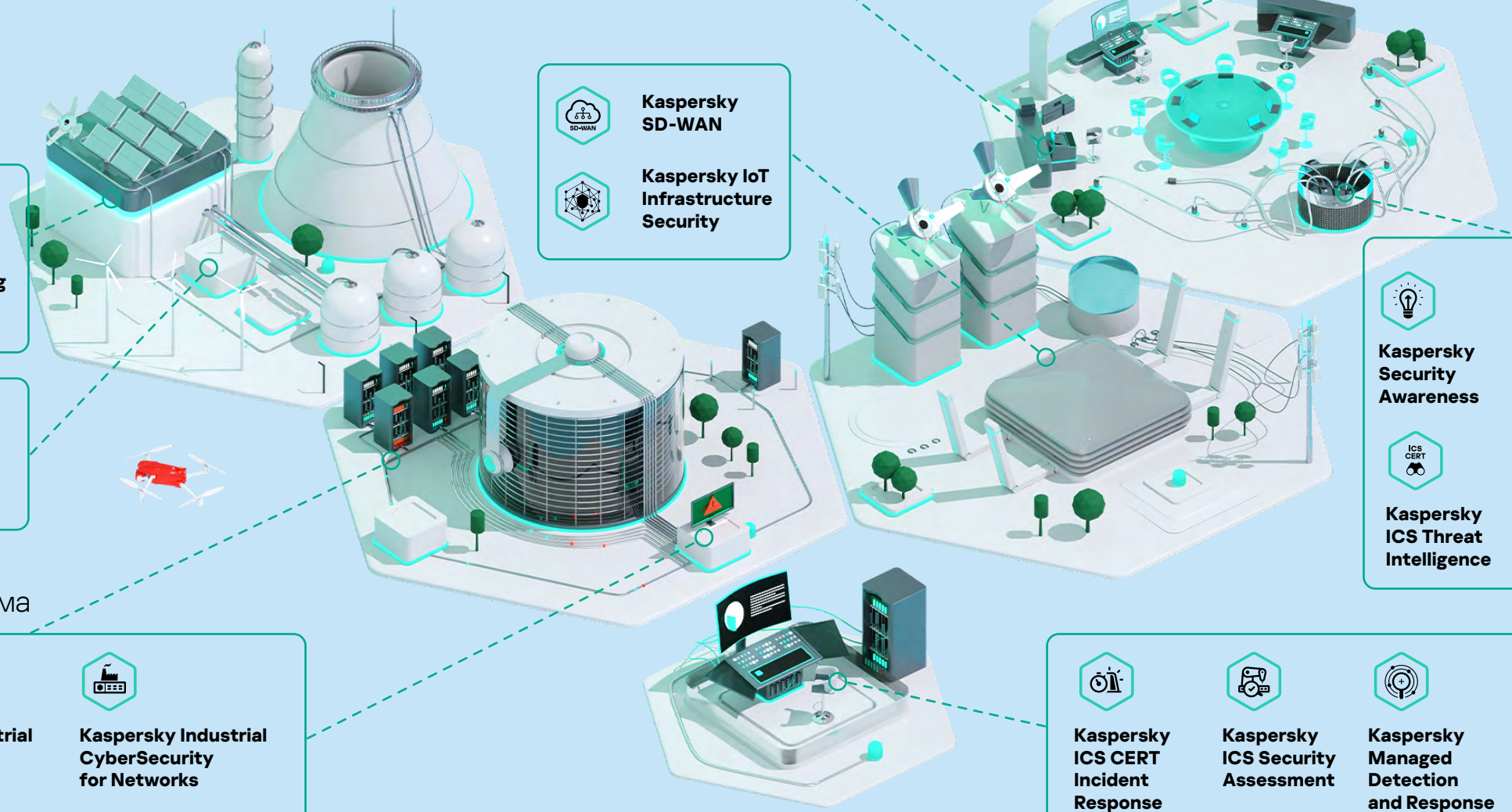
- Обнаружение вторжений, попыток взлома и компрометации, а также уязвимостей микропроцессорного технологического оборудования нижнего уровня автоматизации: контроллеров, терминалов защиты, измерительных центров.
- Глубокая инспекция протоколов (DPI); защита встроенных операционных систем в промышленном оборудовании от сетевых угроз и попыток вредоносного воздействия на уставки (параметры) технологического процесса.
- Обнаружение аномалий в технологическом процессе с помощью машинного обучения по выборке из баз данных или получаемых в реальном времени.

### Уровень 0. Технологический процесс

Мониторинг воздушного пространства для защиты основного оборудования от киберфизических угроз и обеспечения безопасности подключенных транспортных средств.

[1] Industrial Internet of Things, или промышленный интернет вещей, — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

# Экосистема промышленной безопасности



**Kaspersky Unified Monitoring and Analysis Platform**

**Kaspersky Secure Remote Workspace**

**Kaspersky SD-WAN**

**Kaspersky IoT Infrastructure Security**

**Kaspersky Machine Learning for Anomaly Detection**

**Kaspersky Antidrone**

**Kaspersky Security Awareness**

**Kaspersky Ask the Analyst**

**Kaspersky ICS Threat Intelligence**

**Kaspersky ICS CERT Training**

XDR-платформа

**Kaspersky Industrial CyberSecurity for Nodes**

**Kaspersky Industrial CyberSecurity for Networks**

**Kaspersky ICS CERT Incident Response**

**Kaspersky ICS Security Assessment**

**Kaspersky Managed Detection and Response**

**Kaspersky Industrial Emergency Kit**

# Kaspersky Industrial CyberSecurity

## Ключевые отрасли применения экосистемы

- Нефтегазовая и химическая отрасли
- Энергетика, в том числе атомная
- Металлургия и добыча полезных ископаемых
- Промышленное производство

## Перспективные направления применения KOTCS

- Фармацевтика и медтехника
- Транспорт и логистика
- Телекоммуникации

Ключевым элементом экосистемы KOTCS является платформа Kaspersky Industrial CyberSecurity (KICS), предназначенная для защиты промышленных предприятий и объектов КИ и не оказывающая негативного влияния на непрерывность технологических процессов.



# KICS

Нативная XDR-платформа KICS работает в самой глубине АСУ ТП[1], проводит глубокий анализ трафика и телеметрии узлов, активно реагирует на угрозы или просто информирует о них. Она помогает защищать от атак любой сложности современные цифровые и подключенные системы промышленной автоматизации, а также контролировать безопасность эксплуатации программно-технических комплексов прошлых поколений.

KICS обеспечивает полную видимость происходящего на всех уровнях технологического процесса: на уровне физических устройств, контроллеров, серверов SCADA[2] и системы управления производством. Платформа протестирована на совместимость с продуктами ведущих вендоров систем промышленной автоматизации, включая Siemens, Honeywell, B&R (ABB Group), Yokogawa, Emerson, Schneider Electric, Baker Hughes, GE и других.

**Платформа KICS совместима со множеством АСУ ТП от 50+ вендоров**

В составе платформы два тесно взаимосвязанных и дополняющих друг друга компонента: KICS for Nodes для защиты промышленных панелей оператора, рабочих станций и серверов и KICS for Networks — для мониторинга безопасности промышленнй сети.

## KICS сегодня

**~230 000**
проданных лицензий KICS for Nodes

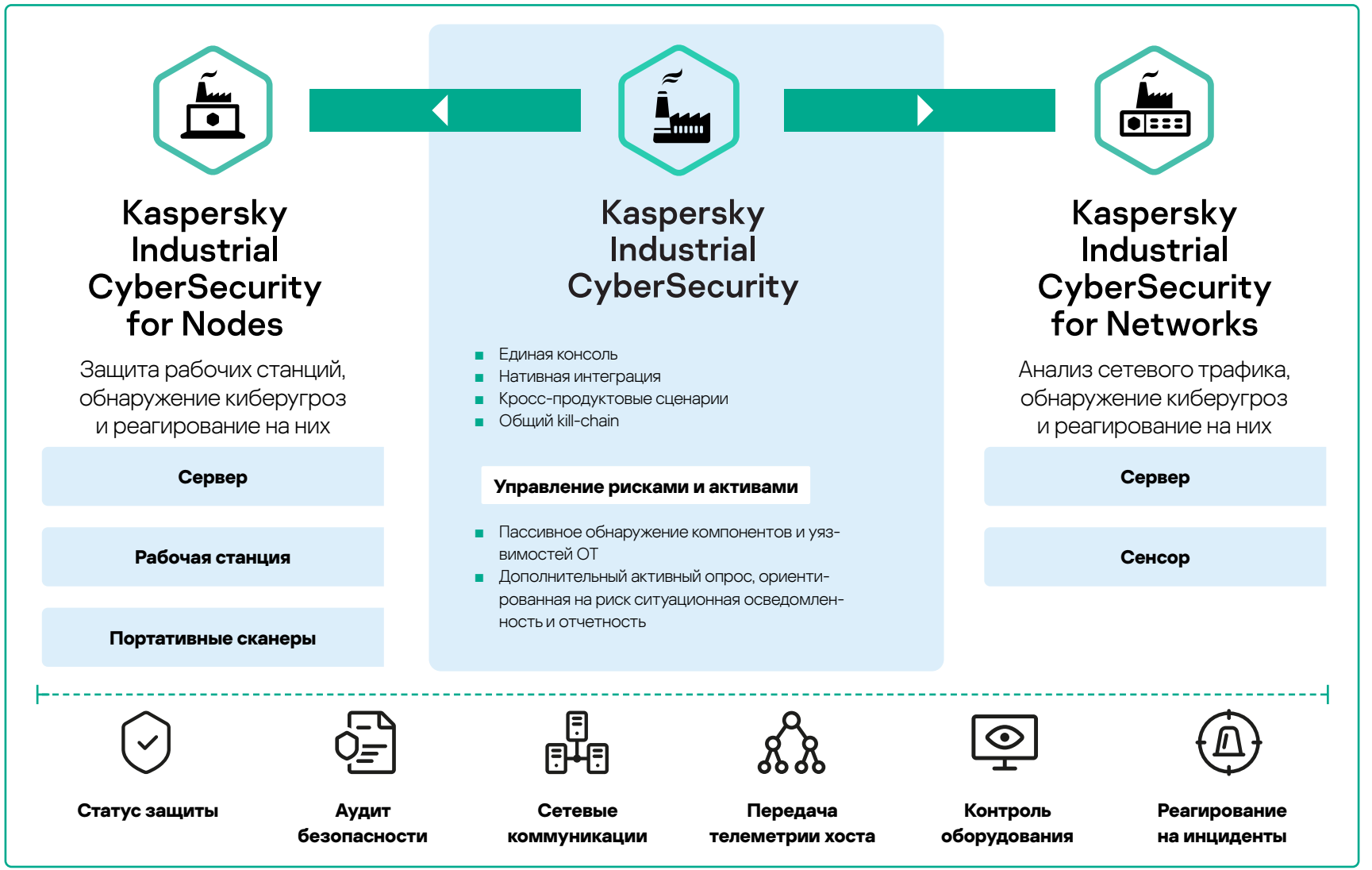
**>1 000**
промышленных клиентов используют решения KICS

**430**
промышленных сетей крупных клиентов защищено по всему миру

**+20%**
средний доход на одного клиента

[1] Автоматизированная система управления технологическим процессом.
[2] Диспетчерское управление и сбор данных (Supervisory Control and Data Acquisition).

# Платформа XDR для промышленности




KICS защищает все ныне эксплуатируемые системы АСУ ТП:

- brown field (более 90%) — это системы, создававшиеся с 2005 по 2020 год. Как правило, распределенные системы управления (РСУ), состоящие из микропроцессорных контроллеров разных типов (ПЛК[1], ИЭУ[2], РЗА[3] и др.), компьютерных человеко-машинных интерфейсов (ЧМИ) на старых ОС Windows и промышленных Ethernet-based сетей;

- перспективные проекты, популярные направления (5–10%) — различные виды цифровизации, подключенные площадки, облачные технологии, IIoT, цифровые двойники, виртуализация промышленных систем, ИИ / машинное зрение, СППР[4], аддитивные технологии и т. п.

В процессе работы платформа KICS обеспечивает полную наблюдаемость и контроль над тем, что происходит в системах управления ключевым технологическим процессом промышленного предприятия. Она обнаруживает и блокирует сетевые угрозы, аномалии трафика и технологического процесса, предотвращает заражения компьютерного оборудования вредоносным ПО и обнаруживает нарушение политики безопасной эксплуатации установок персоналом. В дополнение к этому платформа помогает производить инвентаризацию промышленных активов, аудит безопасности, а также позволяет обнаруживать уязвимости и управлять рисками.

1 Программируемые логические контроллеры.
2 Интеллектуальные электронные устройства.
3 Релейная защита и автоматика.
4 Системы поддержки принятия решений.

## Наш вклад в безопасное производство чистой энергии

**Защищаем энергообъекты с помощью современных информационных и операционных технологий и сервисов**

Усть-Каменогорская и Шульбинская ГЭС — крупные стратегические объекты, поставляющие чистую энергию из возобновляемых источников жителям и предприятиям Восточного Казахстана. Руководители электростанций искали наилучшее решение для обеспечения их безопасной и бесперебойной работы.

Сложность проекта по защите инфраструктуры ГЭС была в том, что при выборе подходящего решения нужно было учитывать следующие важные критерии:

- требования в архитектуре;
- требования по совместимости с другими решениями;
- требования к системам АСУ ТП.

В итоге наиболее подходящей для защиты производственных процессов станций оказалась платформа KICS. Это решение было внедрено в технологические системы ГЭС, расположенные в разных городах и связанные только VPN-каналом.

## Что в результате?

Наше решение KICS обеспечивает безопасность промышленной инфраструктуры двух ГЭС на всех уровнях — от серверов АСУ ТП и автоматизированных рабочих мест до программируемых логических контроллеров и сетевого оборудования, — не нарушая взаимодействия информационных систем и промышленного оборудования. KICS позволяет выявлять разные типы угроз на ГЭС: человеческие ошибки, нарушение коммуникаций между устройствами, появление сотрудника, выполняющего работы без согласования, атаки и вредоносное ПО.

## Формируем кибериммунитет

# # Задача

### Обеспечение надежной и прогнозируемой работы промышленных систем, снижение рисков инцидентов и связанных с ними аварий

Число подключенных к интернету устройств с каждым днем увеличивается, а вместе с этим повышается и уровень киберпреступности. Киберугрозы могут стать причиной значительного физического ущерба, если речь идет, например, о промышленных предприятиях, объектах энергетики, автомобилях или системах «Умного города». Индустрия информационной безопасности создает все новые технологии и продукты, но часто оказывается, что они лишь догоняют злоумышленников. Необходимо найти способ опередить их и защититься от киберугроз.

# # Решения

### Предотвращаем кибератаки с помощью собственной операционной системы KasperskyOS

Кибериммунитет — это подход, позволяющий создавать программно-аппаратные IT-системы со встроенной защитой от кибератак. Это один из определяющих факторов развития в области промышленной автоматизации, носимых промышленных устройств, интернета вещей, удаленного доступа к критически важным объектам. Например, уже сейчас нам доступны такие кибериммунные устройства, как шлюзы промышленного интернета вещей, тонкие клиенты, контроллеры для «Умного города», шлюзы для автомобилей.

В рамках кибериммунного подхода мы разработали собственную операционную систему KasperskyOS — платформу для создания продуктов и решений, защищенных на уровне архитектуры.

Кибериммунитет обеспечивается благодаря разделению системы на изолированные части и контролю взаимодействий между ними. При таком подходе большинство возможных атак на систему будут бесполезны — она продолжает выполнять критически важные функции даже в условиях агрессивной среды и не позволяет злоумышленнику развить атаку.

Важными особенностями KasperskyOS являются собственное микроядро и монитор безопасности — подсистема Kaspersky Security System. Это обеспечивает более высокий уровень безопасности и удовлетворяет требованиям кибериммунности «из коробки». Эти решения практически невозможно скомпрометировать, а число возможных уязвимостей в них сведено к минимуму.

# Помогаем промышленным компаниям реализовывать ESG-стратегию

## # Задача

### Мониторинг и анализ показателей устойчивого развития

Крупные промышленные компании ведут деятельность, руководствуясь принципами устойчивого развития, и разрабатывают собственные ESG-стратегии. Они устанавливают целевые показатели в области изменения климата и планируют постепенно снижать углеродный след до минимума. Чтобы отслеживать свой прогресс в этой сфере, компании в реальном времени и ретроспективно отслеживают и анализируют значения показателей выбросов парниковых газов и загрязняющих веществ. В подобной системе учета особенно заинтересованы предприятия, деятельность которых сопровождается существенными выбросами парниковых газов, в том числе транспортные и добывающие компании.

Еще одним из важных аспектов устойчивого развития являются производственная безопасность и охрана труда. Промышленные предприятия включают цели по сокращению травматизма в свои ESG-стратегии. Чтобы отслеживать свой прогресс в достижении целей, определять уязвимые места и принимать меры для предотвращения несчастных случаев на производстве, они собирают и анализируют данные об условиях труда и травматизме. Для этого используются IT-решения, позволяющие автоматически контролировать соблюдение техники безопасности, фиксировать нарушения и передавать эти данные в систему учета.

## # Решения

### Создаем продукты, позволяющие отслеживать целевые ESG-показатели

Чтобы помочь нашим клиентам не только защитить автомобили от взлома, но и контролировать потребление топлива, строить оптимальные логистические маршруты и учитывать выбросы от автомобильного транспорта, мы создали решение Kaspersky Automotive Secure Gateway. Оно работает на базе операционной системы KasperskyOS и собирает все необходимые цифровые данные о работе транспортного средства, делает их видимыми, прозрачными и понятными, отправляет на серверы для анализа и оценки возможности улучшения показателей, предлагает новые пути для этого. Наше решение позволяет клиентам достигать своих целей в области устойчивого развития в реальности, а не только на бумаге. Кроме того, оно проводит безопасное обновление шлюза и помогает в обновлении других электронных блоков автомобиля, собирает события внутренней сети автомобиля и отправляет их в центр мониторинга безопасности, обеспечивая единое место управления и реагирования и минимизируя расходы на обслуживание.

# Помогаем соблюдать требования в области защиты КИ

## # Задача

### Обеспечение соблюдения законов разных стран пользователями наших решений

Промышленные предприятия и операторы КИ обязаны соблюдать местные законодательные и отраслевые требования по управлению рисками и отчетности об инцидентах. «Лаборатория Касперского» гарантирует соответствие своих продуктов стандартам и законодательным требованиям к промышленной кибербезопасности в разных странах мира.

Подробнее о законодательных и отраслевых требованиях, которые мы учитываем при разработке наших продуктов и решений, читайте в Приложении 4 на стр. 151

# # Решения

## Учитываем требования и стандарты при разработке продуктов для промышленных предприятий

**KICS — первая в мире XDR-платформа, сертифицированная по промышленному стандарту IEC 62443–4-1**

Оба продукта, входящие в платформу KICS, — KICS for Nodes и KICS for Network — прошли сертификацию по основным международным стандартам в области кибербезопасности, а также учитывают или помогают выполнять требования других международных законов и отраслевых стандартов:

- ISO/IEC 27 001 IEC 27 002 (DIN 2008 в Германии) — стандарт, устанавливающий требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы управления информационной безопасностью в контексте организации;
- ISO/IEC 27 019 (DIN 2011 в Германии) — стандарт, использующийся для обеспечения информационной безопасности в энергетике;
- ISO/IEC 27 032 — стандарт, который касается вопросов обеспечения безопасности в интернете и содержит рекомендации по устранению наиболее распространенных угроз в этой сфере (социальная инженерия, атаки нулевого дня, шпионское ПО и т. д.);
- ISO/IEC 15 408 — стандарт, который имеет исторически сложившееся название «Общие критерии» и представляет собой обобщенный опыт различных государств по разработке и практическому использованию критериев оценки безопасности информационных технологий;
- IEC 62 443 (ANSI/ISA99) — серия этих стандартов содержит требования к проектированию систем управления кибербезопасностью АСУ ТП и SCADA;
- IEC 62 351 — стандарт, который охватывает вопросы информационной безопасности энергетических систем;
- NIST CSF — рекомендации по обеспечению безопасности промышленных систем управления, разработанные Национальным институтом стандартов и технологий США (NIST);
- NERC CIP — свод стандартов кибербезопасности для критической инфраструктуры и защиты энергосистемы США, на которые также ориентируются некоторые страны Латинской Америки;
- NIS 2 Directive (EU) 2022/2555) — новая директива ЕС о кибербезопасности[1];
- IMO MSC.428(98) — резолюция Комитета по безопасности на море, которая регулирует управление киберрисками в морской отрасли в рамках систем управления безопасностью;
- ICAO — стратегия кибербезопасности в авиации[2];
- IAEA Nuclear Security Series No. 17-T (Rev. 1) — методы обеспечения компьютерной безопасности для ядерных установок.

С 8 февраля 2022 года область сертификации распространяется на сервисы обработки данных «Лаборатории Касперского» (KSN). Многие клиенты KICS активируют KSN при установке. Для них крайне важно, что Компания использует лучшие мировые практики в своих дата-центрах в Цюрихе, Франкфурте-на-Майне, Торонто, Москве и Пекине. Подробнее об этом читайте здесь.

Наша платформа KICS полностью сертифицирована европейской сертификационной TUV Austria на соответствие международному стандарту в части жизненного цикла разработки ПО для обеспечения кибербезопасности промышленных предприятий. Уровень доверия — 3 из 4.

«Лаборатория Касперского» проходит аудиты Service Organization Controls (SOC 2). В рамках сертификации Type 2 проверялась эффективность средств контроля, используемых с целью обезопасить процесс разработки и выпуска антивирусных баз от несанкционированного вмешательства. Работоспособность механизмов контроля, принятых в Компании, оценивалась не на определенную дату, как при аудите первого типа, а за шесть месяцев.

Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks имеют также сертификаты государственных органов Российской Федерации (ФСТЭК и ФСБ). В декабре 2023 года успешно прошли сертификационные испытания версии 3.2.0.273 (для Windows) и 1.3.0.1 206 (для Linux). Помимо этого, решения «Лаборатории Касперского» включены в Единый реестр российских программ для электронных вычислительных машин и баз данных, который был создан в начале 2023 года Минцифры России.

В октябре 2023 года «Лаборатория Касперского» запустила регуляторный хаб знаний в области информационной безопасности, который включает все нормативные правовые акты в области ИБ, действующие в России. Центр знаний призван помочь пользователям ориентироваться в законодательстве в сфере ИБ, понимать текущие требования и рекомендации для конкретной отрасли.

[1] Государства — члены Евросоюза должны принять и опубликовать меры по кибербезопасности, необходимые для соблюдения новой директивы, до 17 октября 2024 года.

[2] FAA Advisory Circular 119-1 — Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).

**Наш вклад в создание стандартизированного подхода к кибербезопасности**

# Разрабатываем российские ИБ-стандарты в области кибербезопасности

При разработке операционной системы KasperskyOS мы обнаружили, что в российских документах и учебниках по информационной безопасности не хватает терминов, определений и понятий, с помощью которых можно описать проектные архитектурные решения. Чтобы решить эту проблему, мы начали разработку двух национальных стандартов. Они определяют базовые понятия и основные архитектурные принципы, заложенные в системы с разделением доменов, в том числе в KasperskyOS.

## Что в результате?

В апреле 2023 года оба стандарта были приняты Техническим комитетом «Киберфизические системы» (ТК 194) и вступили в действие.

- Информационные технологии. Интернет вещей. Системы с разделением доменов. Термины и определения
- Информационные технологии. Интернет вещей. Системы с разделением доменов. Базовые компоненты

# Наши результаты

## KICS

Продажи платформы KICS существенно увеличились на всех основных рынках решений для промышленной кибербезопасности. Российский рынок, оставаясь ключевым для Компании, генерирует около 80% бизнеса и показывает рост более 50%. Это объясняется стремительным импортозамещением решений иностранных вендоров, а также возросшим спросом на защиту из-за роста количества атак на российскую инфраструктуру.

В 2023 году направление промышленной кибербезопасности показало следующие результаты.

- Платформа KICS уверенно вошла в пятерку лучших по выручке среди всех B2B-продуктов Компании.
- Направление Industrial Cybersecurity в очередной раз показало трехзначный рост выручки в процентном соотношении относительно прошлого года.
- Перевыполнение плана продаж составило 128%.
- Показатели Gross EBITDA margin; Operating EBITDA margin и EBITDA margin лежат в диапазоне от 20 до 40%.

### Основные драйверы развития платформы Kaspersky Industrial CyberSecurity

- Возрастающие угрозы и возникающие инциденты информационной безопасности, с которыми промышленные компании, к сожалению, все чаще сталкиваются на практике.
- Потребность в решении, способном защищать гетерогенную инфраструктуру, состоящую одновременно из технологических процессов, управляемых как устаревшими системами автоматизации, так и современными решениями на основе сетей с продвинутой архитектурой, актуальных операционных систем и версий промышленного ПО.
- Активное внедрение подключенных интеллектуальных устройств и устройств промышленного интернета вещей в рамках процесса цифровизации, а также широкого использования IT-, программного, аппаратного и сетевого технологического стека на промышленных объектах.

В ближайшие 4 года мы ожидаем двукратный рост в этом бизнес-сегменте. Для этого мы продолжим инвестировать в развитие технологических возможностей KICS и ее продвижение в ключевых регионах.

## KasperskyOS

В отчетном периоде мы начали развивать региональный бизнес по защите виртуальных рабочих мест. Это направление стало особенно актуальным в постпандемийный период, когда многие компании перешли на гибридную модель работы сотрудников.

В частности, в августе 2023 года мы подписали соглашение с корпорацией Centerm, согласно которому специализированные рабочие места (тонкий клиент на KasperskyOS) могут поставляться по заказам из любых стран. Мы уже получили первые заказы из Швейцарии и Малайзии.

В 2023 году наши специалисты детально изучили вопрос расширения аппаратных платформ уникальными решениями, построенными на принципах кибериммунитета, и начали экспертную работу для получения необходимых заключений и разрешений регуляторов.

# Наши планы на 2024 год

## Промышленная кибербезопасность

### Предложение глубокой и всесторонней защиты

во всех сегментах инфраструктуры наших клиентов с помощью технологий, знаний и экспертизы, входящих в нашу OT-экосистему. Развитие кросс-продуктовых сценариев использования наших нативно интегрированных технологий в ответ на новые запросы заказчиков, а также включение в нашу открытую экосистему решений наших партнеров.

- Инвестиции в Linux-функционал и в развитие технологических возможностей платформы KICS.
- Расширение поддерживаемых аппаратных платформ, протоколов промышленной передачи данных и развитие экспертной базы данных промышленных устройств.
- Отработка сценариев использования носимых устройств, безопасного обмена данными, а также создание инструментария аудита информационной безопасности и плановой проверки даже изолированных систем и сетей.

### Расширение

на новые вертикальные рынки, участникам которых необходимо четко отслеживать ESG-показатели.

- Сотрудничество с клиентами из таких отраслей, как транспорт, логистика, полупроводники, автомобильная промышленность и производство комплектующих.
- Партнерство с лидерами в OT-интеграции, а также создание технологических альянсов с региональными чемпионами среди вендоров систем промышленной автоматизации[1].

### Геоэкспансия

в регионы с меньшим присутствием Компании. Для этого мы адаптируем экосистему под особенности каждого региона.

- Сохранение инвестиций в исторические рынки — Россия, СНГ, Европа.
- Расширение сотрудничества с региональными партнерами в области защиты КИ: Бразилия, Китай, Индия, Индонезия, Саудовская Аравия, ОАЭ, Алжир, ЮАР.

## KasperskyOS

### Развитие

бизнес-сообщества партнеров, участники которого используют киберриммунные продукты в вертикальных отраслевых решениях.

### Запуск

пилотных проектов с ключевыми заказчиками в различных отраслях для разработки сценария с эффективным применением кибериммунных решений.

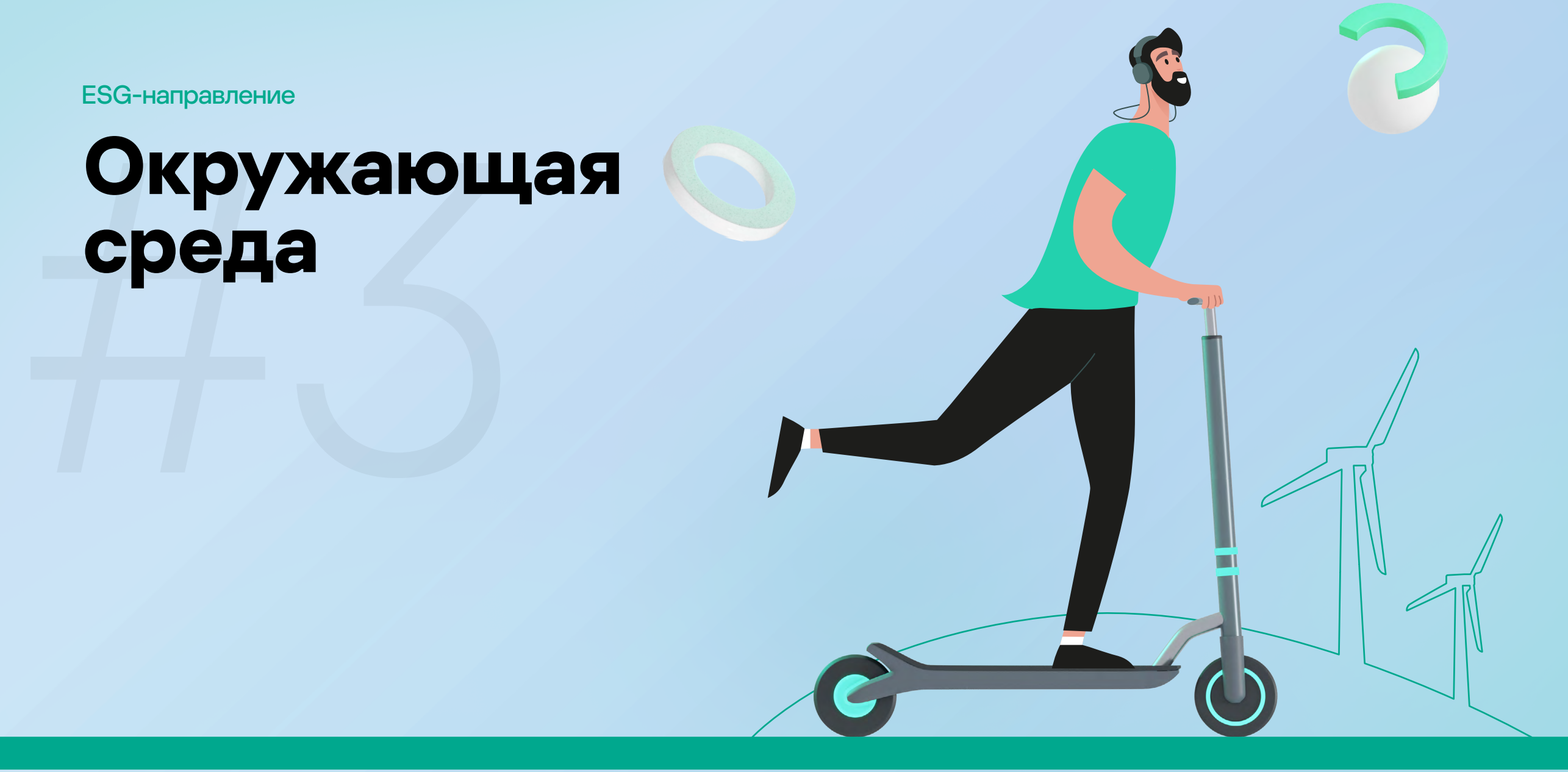
### Проработка

требований регуляторов для создания описания нового класса устройств со встроенной (кибериммунной) защитой.

[1] Региональные лидеры, производители промышленного оборудования и систем автоматизации.

ESG-направление

# Окружающая среда



# Управление экологическими воздействиями

Мы отслеживаем и стремимся свести к минимуму любые прямые и непрямые воздействия, которые наша деятельность оказывает на окружающую среду и климат. Для этого мы оптимизируем бизнес-процессы, сокращаем потребление ресурсов, снижаем объемы образования отходов и повышаем энергоэффективность нашего офиса и дата-центров.

## Ключевые документы

В 2023 году Компания продолжила разработку Единой экологической политики — ключевого документа, который будет определять деятельность Компании по охране окружающей среды. Мы планируем завершить работу над этим документом к 2025 году.

## Подход к управлению охраной окружающей среды

GRI 307-1

Ответственное отношение к окружающей среде — одна из ключевых ценностей Компании.

«Лаборатория Касперского» потребляет воду и производит отходы, которые образуются в основном в результате деятельности офиса и представляют собой упаковку от физических продуктов.

Углеродный след Компании формируют непрямые источники: авиаперелеты, работа серверов, энергопотребление офисов, корпоративный транспорт, а также услуги для создания и распространения продуктов.

Вопросы охраны окружающей среды находятся в зоне ответственности руководителей направлений «Лаборатории Касперского». Наши коллеги внедряют современные решения, с помощью которых Компания сокращает объем потребления ресурсов и образования отходов.

# Снижение углеродного следа

## Мы сознаем важность проблемы изменения климата и стремимся снизить углеродный след от работы дата-центров и бизнес-операций Компании.

Мы стремимся внести свой вклад в достижение ЦУР 13 «Борьба с изменением климата» и работаем над сокращением углеродного следа нашей Компании, используя энергоэффективное оборудование и технологии, а также минимизируя углродный след от авиаперелетов и поездок автотранспортом.

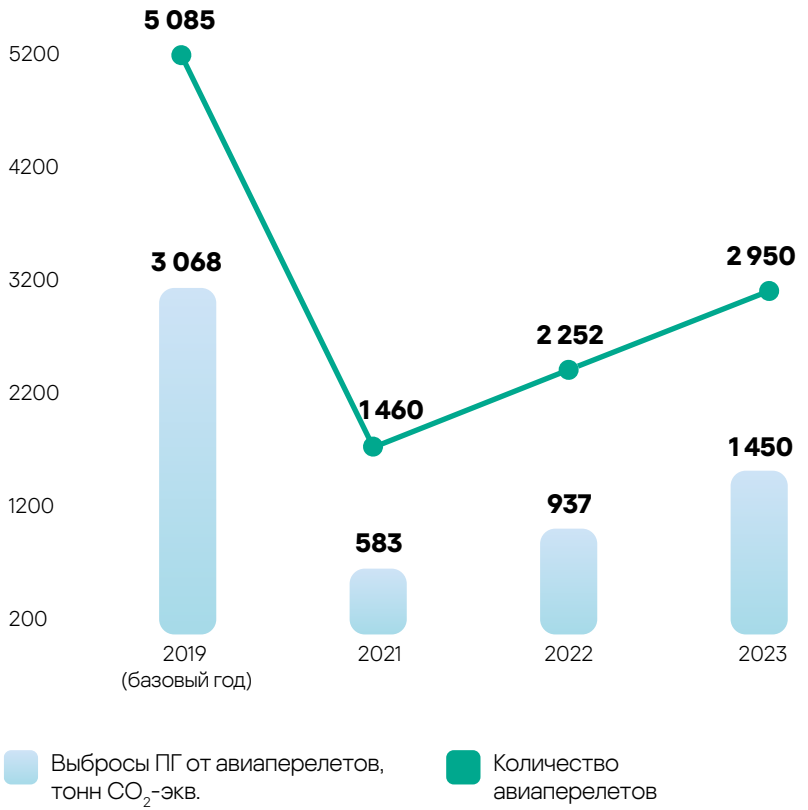
# Как мы управляем выбросами от транспорта

GRI 305-5

Мы понимаем, что использование авиа- и автотранспорта приводит к росту экологической и климатической нагрузки, поэтому стремимся снизить объем выбросов от сжигания топлива транспортом. Мы сократили наш автопарк до трех автомобилей и используем их только для срочных поездок.

Мы делаем все, чтобы минимизировать наш углеродный след от авиаперелетов. Однако в 2022 и 2023 годах мы расширяли наш бизнес в Латинской Америке, Африке, на Ближнем Востоке и в Турции, в связи с чем число авиаперелетов сотрудников выросло в сравнении с 2021 годом. Тем не менее в 2023 году нам удалось сохранить объем выбросов на уровне вдвое ниже, чем в базовом 2019 году (3,1 тысячи тонн $CO_2$-экв.).

## Выбросы парниковых газов от авиаперелетов сотрудников Компании[1]




[1] Данные об авиаперелетах за 2020 год не приводятся в связи с приостановкой авиасообщения в 2020 году из-за пандемии.

[2] https://www.cell.com/joule/fulltext/S2542-4351(19)30255-7?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435119302557%3Fshowall%3Dtrue.

[3] Данные на основе анонимизированной статистики срабатывания решений «Лаборатории Касперского» в 2022 году по всему миру.

### Наш вклад в сокращение выбросов $CO_2$ от майнинга

**Блокировка вредоносного ПО, направленного на потребление чужих энергоресурсов**

Многие пользователи становятся жертвами скрытого майнинга — их ресурсы используются без их ведома путем запуска специального ПО на компьютерах или смартфонах. Это может привести к снижению производительности и скорости работы устройства, выводу его из строя, а также повлечь за собой проникновение сторонних вирусов. Более того, майнинг расходует огромный объем электроэнергии. Ежегодный углеродный след криптовалютной отрасли сравним с объемом выбросов крупного города[2].

Защищая людей от скрытого майнинга, мы способствуем снижению выбросов парниковых газов. В 2022 году мы разработали и внедрили специальную методику для расчета потенциального объема энергии, сэкономленной благодаря блокировке вредоносных майнеров с помощью решений «Лаборатории Касперского».

## Что в результате?

В 2022 году наши решения предотвратили более 200 млн попыток использовать чужие устройства для майнинга криптовалют[3] и, как следствие, до 3 тысяч тонн выбросов углекислого газа в атмосферу. Это сопоставимо с ежегодным объемом выбросов 652 автомобилей.

# Как мы управляем энергопотреблением в офисе

GRI 302-1 GRI 302-4 GRI 305-5 TC-SI-130-a.1

**7 881 208 кВт • ч**

общее потребление электроэнергии в 2023 году

Штаб-квартира «Лаборатории Касперского» расположена в московском бизнес-центре «Олимпия Парк», которому присвоен класс энергоэффективности A. Здание сертифицировано по международному экологическому стандарту BREEAM, при его строительстве использовались энергоэффективные технологии и материалы.

В нашем главном офисе мы применяем современные решения, такие как светодиодные осветительные приборы, датчики движения, позволяющие отключать свет при ненадобности, и автоматические регуляторы освещения при изменении количества дневного света. С 2020 года светодиодными приборами полностью освещается и парковка бизнес-центра. Это позволило сократить расходы на освещение на 30–45% в сравнении с 2019 годом.

Потребление электроэнергии в Компании в 2022 и 2023 годах несколько выросло в сравнении с 2021 годом. Причиной послужило то, что ряд сотрудников перешли с удаленного и гибридного форматов работы, преобладавших в 2021 году, на работу в офисе, а в конце 2023 года часть сотрудников Компании переехали в московскую штаб-квартиру из другого офиса, соответственно, потребление энергии компьютерным оборудованием и осветительными приборами увеличилось. Кроме того, после простоя, связанного с коронавирусными ограничениями, вновь открылись спортзал, столовая и ресторан на территории офиса, что также способствовало росту потребления электроэнергии в этих пространствах.

## Общее энергопотребление в Компании[1], кВт • ч


[1] Границы раскрытия — московский офис акционерного общества «Лаборатория Касперского», включающий в себя и дата-центр Компании. По остальным офисам информация в отчетном периоде не собиралась.

# Как мы управляем энергопотреблением в ЦОД

TC-SI-130-a.3

**PUE 2**

**показатель энергоэффективности дата-центра «Лаборатории Касперского»**

Один из главных факторов, формирующих углеродный след IT-компаний, — работа дата-центров, или центров обработки данных (ЦОД). Они объединяют тысячи серверов и работают круглосуточно, потребляя большое количество энергии. Кроме того, энергию потребляют промышленные кондиционеры, обеспечивающие необходимое охлаждение ЦОД. Компания использует собственный ЦОД, включающий 33 стойки с серверами, которые поддерживают работу пользовательской инфраструктуры и бэк-офиса, а также арендованные дата-центры для нужд разработки.

ЦОД «Лаборатории Касперского» получает электроэнергию от двух независимых подстанций, на случай аварийной ситуации в готовности находится дизельный генератор, а UPS-батареи позволяют серверам продолжать работу около 30 минут после отключения всех прочих источников питания. В серверной установлена система газового пожаротушения, не наносящая вреда окружающей среде.

Все электрооборудование регулярно проходит техосмотр. Раз в две недели проводятся тестовые запуски генератора на холостом ходу, раз в квартал — запуски под нагрузкой, а топливо в генераторе заменяется ежегодно. Обслуживание системы UPS-снабжения проводится ежеквартально.

При строительстве ЦОД мы использовали энергоэффективные технологии и материалы, в том числе интеллектуальные регуляторы температуры и датчики присутствия для освещения.

Новейшее вычислительное оборудование помогает нам экономить мощность и сокращать энергопотребление. Мы заменяем устаревшее оборудование новым, которое в пересчете на единицу мощности выдает больше производительности, уменьшаем количество используемых кабелей и стоек, серверов, используя среды виртуализации и SSD-диски. Мы перерабатываем старое компьютерное оборудование и передаем на благотворительность клавиатуры, ноутбуки, мониторы и телефоны. В 2023 году мы передали 237 единиц оборудования семи различным некоммерческим организациям.

Мы предъявляем высокие требования к инфраструктуре ЦОД и стремимся эффективно использовать все имеющиеся возможности. Например, зимой мы переходим на систему фрикулинга — обеспечиваем охлаждение дата-центра за счет температуры внешнего воздуха. Мы используем такие энергоэффективные методы охлаждения в дата-центре, как расширение температурного диапазона эксплуатации серверов до 22–24 °C, а также организацию холодных и горячих воздушных коридоров.

Чтобы предотвратить утечку газов, использующихся для охлаждения серверов, наши сотрудники два раза в день проверяют работу охлаждающего оборудования. В случае выявления утечки оборудование отключается, перекрывается подача хладагента и газ эвакуируется в специальный баллон.

Для оценки энергоэффективности дата-центров во всем мире используется показатель PUE (Power Usage Effectiveness), который рассчитывается как отношение общего энергопотребления дата-центра к энергопотреблению IT-оборудования. В 2023 году значение PUE наших дата-центров составило 2 (для сравнения: среднее значение по миру в 2022 году составляло 1,55, по оценке Uptime Institute).

# Использование воды

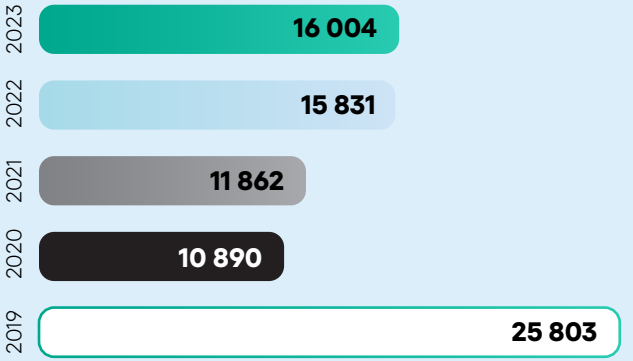
## Чтобы снизить потребление воды, мы совершенствуем систему водоснабжения в наших офисах.

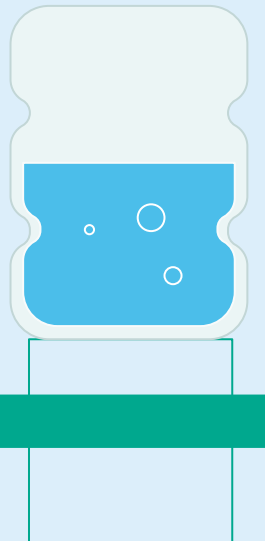
GRI 303-1 GRI 303-2 GRI 303-3 GRI 303-4 GRI 303-5 TC-SI-130-a.2

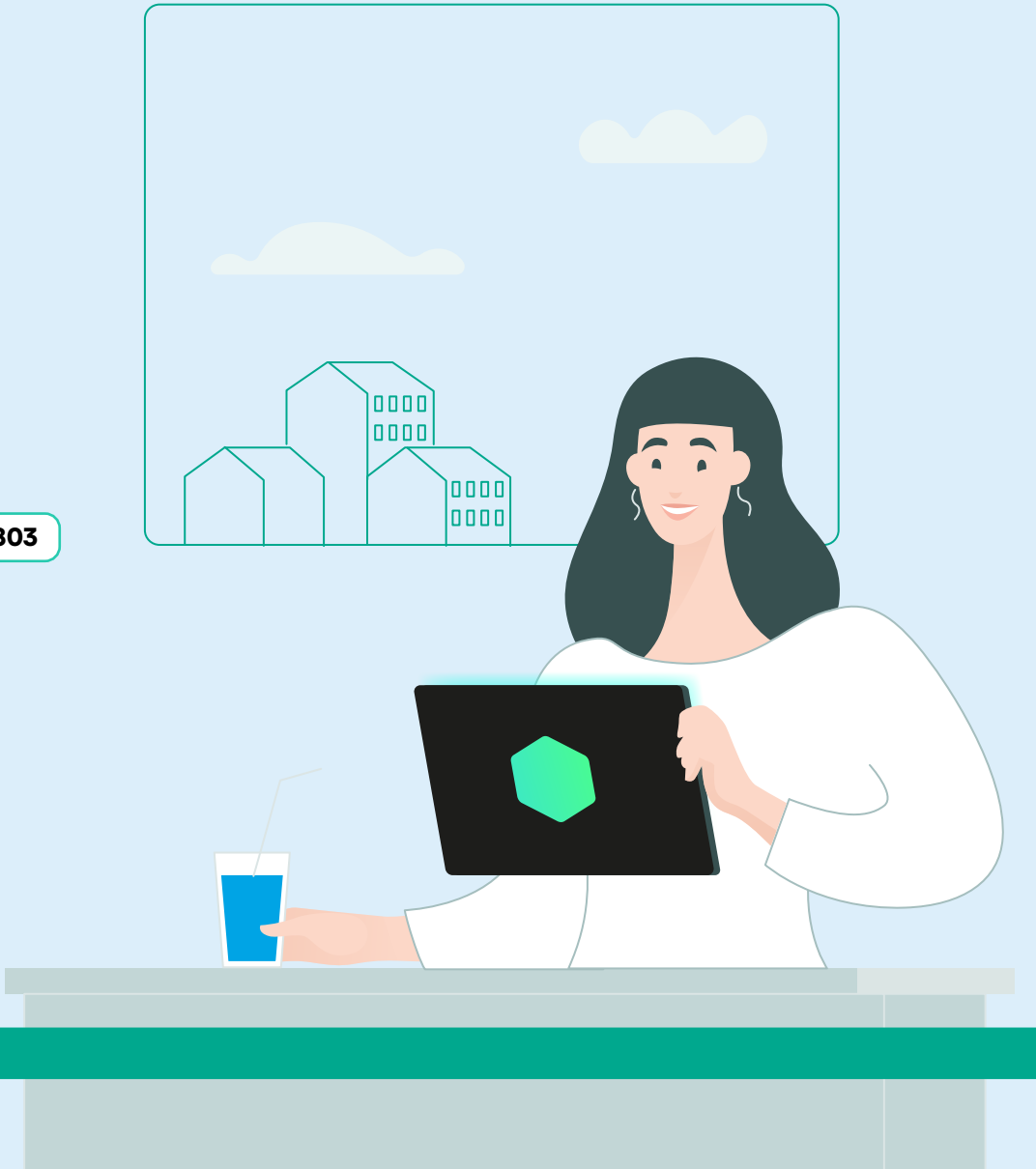
«Лаборатория Касперского» потребляет воду исключительно для целей жизнеобеспечения офиса и дата-центра и только из муниципальных источников. Забор воды из природных источников и открытых водных объектов и сброс воды в природные водоемы не осуществляются.

В 2022 и 2023 годах объем потребления воды в Компании увеличился по сравнению с двумя предыдущими годами. Такая динамика объясняется тем, что в 2020 и 2021 годах сотрудники «Лаборатории Касперского» в основном работали удаленно, а в последующие два года начали постепенно возвращаться в офис, кроме того, вновь были открыты столовая, спортзал и ресторан на территории офиса. Все это повлияло на рост объема потребления воды. Тем не менее уровень водопотребления в 2022 и 2023 годах оказался существенно ниже уровня базового 2019 года благодаря установке новых датчиков системы водоснабжения.

### Объем потребления воды[1], куб. м



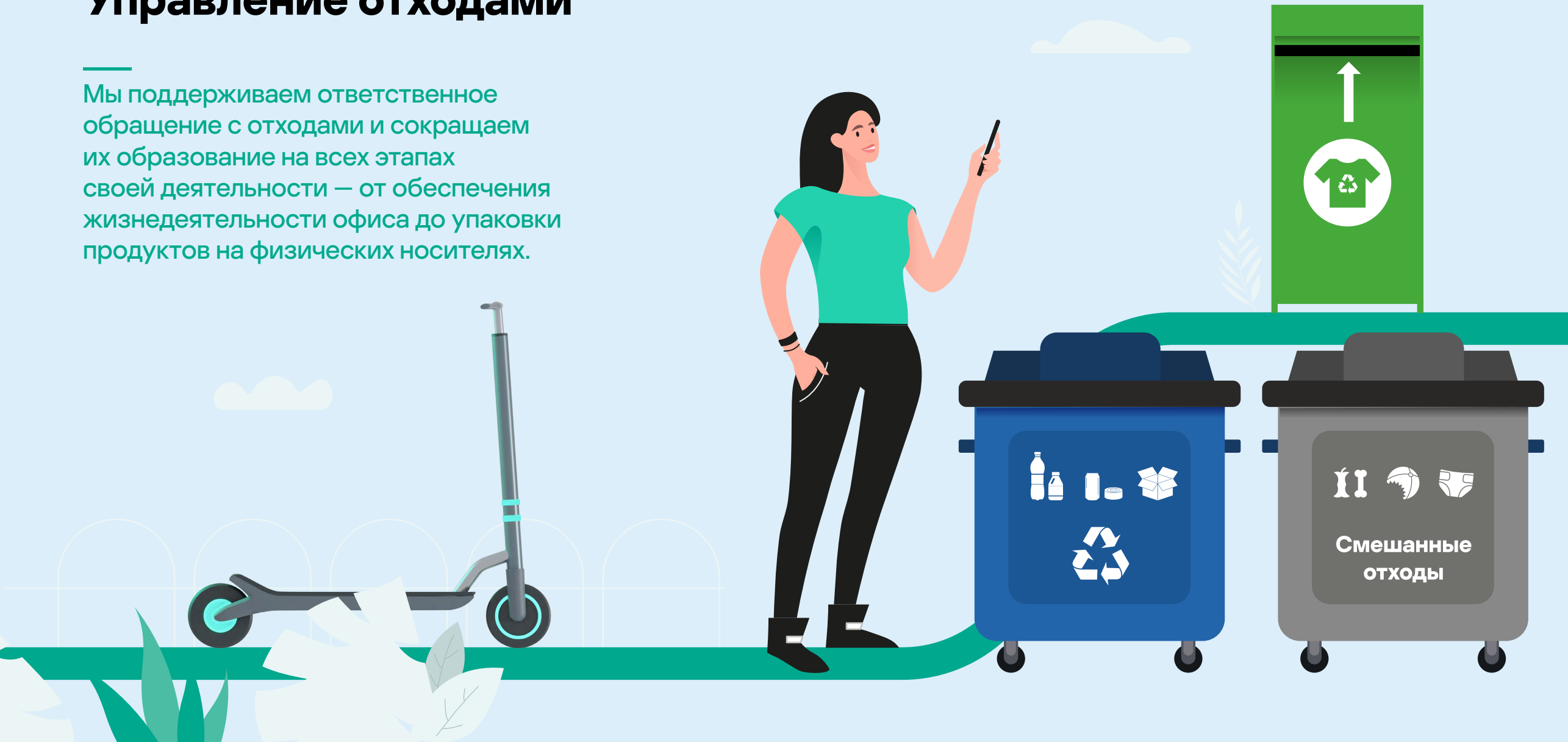





[1] Границы раскрытия — московский офис акционерного общества «Лаборатория Касперского», включающий в себя и дата-центр Компании (основной источник водопотребления в организации). По остальным офисам информация в отчетном периоде не собиралась. Вода в бизнес-операциях используется для хозяйственно-бытовых целей в офисах Компании, поэтому учет водопотребления общий. Территории расположения офисов Компании не относятся к регионам водного стресса.

# Управление отходами

Мы поддерживаем ответственное обращение с отходами и сокращаем их образование на всех этапах своей деятельности — от обеспечения жизнедеятельности офиса до упаковки продуктов на физических носителях.



# Как мы минимизируем вред от выпуска продуктов на физических носителях

GRI 306-1 GRI 306-2 GRI 306-3 GRI 306-6

Значительную часть отходов в мире составляет упаковка реальных товаров. Чтобы сократить ее объем, мы снижаем выпуск продуктов на физических носителях и переходим к продаже онлайн-лицензий. В отчетном периоде доля коробочных продуктов в B2C-продажах «Лаборатории Касперского» снизилась с 11 до 7%. Доля электронных лицензий и POSA[1]-карт в глобальных продажах приближается к 40% и будет увеличиваться в будущем. Наилучшие результаты в области продаж электронных продуктов показывают такие регионы, как Латинская Америка и Россия.

**Форматы продуктов «Лаборатории Касперского» на физических носителях**

- **Боксы** (коробки с компакт-диском, содержащим продукт)
- **Лифлеты и чек-карты** (информационные материалы, предназначенные для использования прямо в магазине)
- **POSA-карты** (карты из тонкого картона для доставки электронного продукта)

К нашему сожалению, полный отказ от выпуска продукции на физических носителях сейчас невозможен: некоторые покупатели предпочитают приобретать CD или DVD в силу традиции, а в ряде регионов, например в странах Африки, — из-за отсутствия стабильного доступа к интернету. Для таких товаров мы ввели компактную упаковку с минимально возможным содержанием пластика. На нее наносятся международные коды переработки, чтобы покупатели могли экологично утилизировать ее в своих странах. Во всех регионах продаж «Лаборатория Касперского» соблюдает законодательные требования, связанные со ввозом и утилизацией упаковки: уплачивает экологические сборы, собирает и передает регуляторам необходимые данные и проч.

Кроме того, мы сокращаем количество пластика в производстве сувенирной продукции и переходим к использованию перерабатываемых или экологичных материалов. Вместо пластиковых пакетов мы используем пакеты из беленой крафтовой бумаги и холщовые шоперы.

Сокращение продаж физических товаров и рост цифровой дистрибуции — глобальный процесс, темпы которого различаются в зависимости от региона.

30% выручки B2C-продаж приходится на реактивацию, когда спустя год после покупки новой лицензии пользователи снова возвращаются в ретейл за покупкой следующей лицензии. 7% этой выручки ежегодно переходит в цифровой сегмент — после того как пользователь совершает первую покупку в розничном магазине, на следующий год он уже осуществляет покупку онлайн.

Нашим партнерам мы предлагаем переходить к покупке онлайн-лицензий, а дистрибьюторам — распространять лицензии через собственные сайты, что также упрощает доступ к зарубежным рынкам.

**56%**

**доля продаж в коробочных решениях**

**44%**

**доля продаж в электронных форматах**

## Наш вклад в сокращение продаж физических товаров

**Мотивируем клиентов покупать цифровые продукты**

В отчетном периоде мы запустили проект «Подписка для ретейл-клиентов». Она стимулирует тех, кто привык приобретать наши товары в розничных магазинах, переходить на покупку электронных лицензий онлайн. Такой подход позволит нам уменьшить объемы производства пластиковой упаковки и печатной продукции, сократить расходы и минимизировать негативное воздействие на окружающую среду.

## Что в результате?

Наши клиенты могут зарегистрироваться на портале My Kaspersky и оформить электронную подписку на новую линейку продуктов через наш сайт. Чтобы повысить интерес клиентов к цифровым подпискам, мы предлагаем им новые методы онлайн-оплаты и привлекательные цены.

[1] Point-of-Sales Activation — продукт, который активируется в точке продаж.

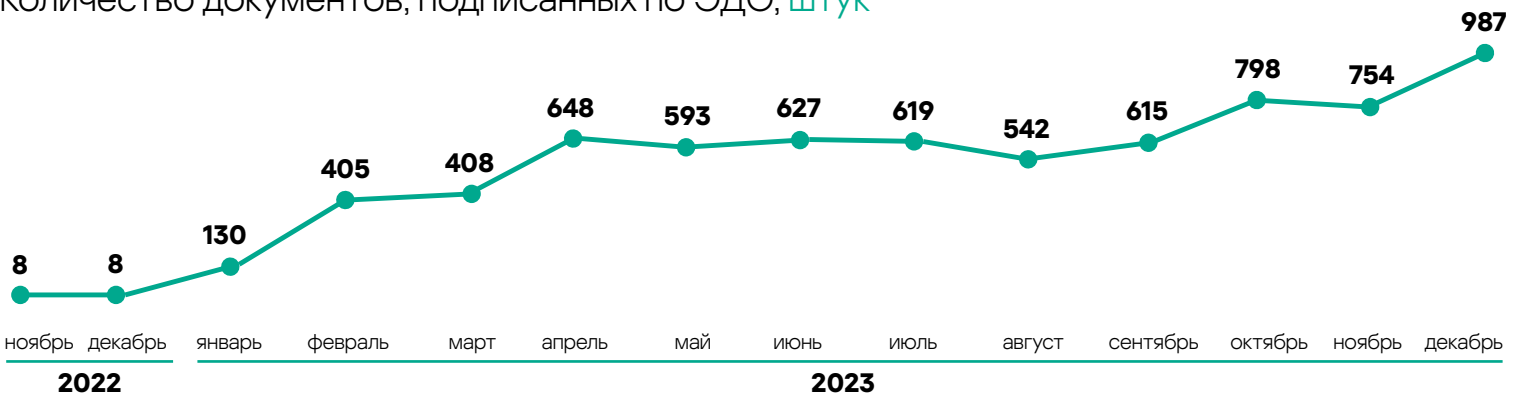
# Как мы экономим бумагу

Мы стремимся сократить количество печатных информационных и рекламных материалов, а также передаем на утилизацию устаревшие плакаты, таблички, баннеры и фотопанели, которые были изготовлены для наших внутренних мероприятий.

В ноябре 2022 года мы запустили электронный документооборот (ЭДО) в работе с внешними контрагентами, что позволяет нам и нашим партнерам значительно снизить расход бумаги. На 31 декабря 2023 года количество контрагентов, использующих систему обмена электронными документами с нашей Компанией, достигло 498 (против 2 в 2021 году).

В 2023 году мы провели аудит инфраструктуры совместно с вендором для повышения ее стабильности и скорости работы, внесли изменения в интерфейс ЭДО-платформы для удобства ее использования, перешли к взаимодействию со сторонними операторами и интеграции платформы с внутренним контрактным порталом. Это позволит нам и дальше расширять электронный документооборот и увеличивать число партнеров, использующих его в нашей совместной работе.

## Количество документов, подписанных по ЭДО, штук




## Динамика подключения новых контрагентов к ЭДО

# Как мы утилизируем отходы

Значимая часть отходов Компании производится в результате жизнедеятельности офиса. Чтобы сократить их количество, мы отдаем предпочтение качественным материалам с долгим сроком службы — например, используем многоразовую посуду вместо одноразовой.

В нашем московском офисе размещены плакаты с инфографикой на тему раздельного сбора мусора, установлены контейнеры для раздельного сбора бумаги, пластика, стекла, металла и смешанных отходов. В 2023 году в принтерных комнатах были установлены новые контейнеры с отделениями для макулатуры, пластиковых крышек, батареек, аккумуляторов и электронных сигарет.

Ежедневный вывоз мусора, его транспортировку и передачу на переработку и утилизацию Компания поручает специализированным предприятиям. Все контрагенты, включая операторов по утилизации отходов, проходят проверку на соблюдение требований законодательства.

Отходы I и III классов опасности перед отправкой на захоронение или утилизацию частично обезвреживаются.

## Образование отходов[1], тонн

| | Образовано всего | | | Отправлено на переработку, вторичное использование и иное восстановление | | | Отправлено на захоронение и утилизацию | | |
|---|---|---|---|---|---|---|---|---|---|
| **Класс отходов** | **2021** | **2022** | **2023** | **2021** | **2022** | **2023** | **2021** | **2022** | **2023** |
| **I класс** | | | | | | | | | |
| чрезвычайно опасные, неразлагаемые: пестициды, асбест, приборы, содержащие ртуть | 0,068 | 0,072 | 0,098 | 0 | 0 | 0 | 0,068 | 0,072 | 0,098 |
| **II класс** | | | | | | | | | |
| высокоопасные, разлагаются более 10 лет: инсектициды, фунгициды, свинец, мышьяк, аккумуляторы, пиротехника | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **III класс** | | | | | | | | | |
| умеренно опасные, разлагаются от трех до десяти лет: гербициды, лакокрасочные материалы, моющие средства, шампуни, дезодоранты, мобильные телефоны | 0,926 | 0 | 0,728 | 0 | 0 | 0 | 0,926 | 0 | 0,728 |
| **IV класс** | | | | | | | | | |
| малоопасные, разлагаются до трех лет: азотные удобрения, ДВП, ДСП, полиэтиленовая пленка, зеркала, резиновые перчатки и обувь, одноразовая посуда, бытовая техника | 172,4 | 224,7 | 219,4 | 8,14 | 0 | 0 | 164,26 | 224,7 | 219,4 |
| **V класс** | | | | | | | | | |
| практически неопасные, разлагаются до трех лет: продукты питания, натуральные ткани и изделия из них, бумажные и картонные изделия | 3,1 | 4,8 | 5,4 | 0 | 0 | 0 | 3,1 | 4,8 | 5,4 |

[1] Учитываются отходы московского офиса, включая ЦОД, а также отходы в результате бизнес-операций.

# Развитие экологической культуры персонала

## «Лаборатория Касперского» стремится прививать сотрудникам экологическую культуру и информирует о принципах разумного потребления.

Наши работники активно участвуют в экологических инициативах. Для желающих вести экологичный образ жизни создано сообщество Green like Midori, в которое приглашают всех новичков Компании. Кроме того, мы организуем лекции и экскурсии по теме защиты окружающей среды, а для тех, кто не смог на них присутствовать, публикуем во внутренней сети видеорепортажи с мероприятий.

В 2022 году мы запустили для сотрудников московского офиса игру Trash Ninja. Она знакомит игроков с типами отходов, образующихся в офисе и дома, и позволяет соревноваться с коллегами в сортировке мусора. Большинство сотрудников Компании уже прошли Trash Ninja и научились сортировать мусор.

### Наш вклад в продвижение идеи осознанного потребления

**Дарим вещам вторую жизнь**

В 2022 году «Лаборатория Касперского» начала сотрудничать с фондом «Второе дыхание», который занимается сбором, сортировкой, перераспределением и переработкой одежды на любой стадии ее жизни. Мы организовали экскурсию на московский склад фонда, в ходе которой сотрудники узнали, как развивается инфраструктура сбора ненужной одежды, как осуществляются ее сортировка, переработка и утилизация, как устроена передача одежды на благотворительные цели. Теперь в нашем московском офисе установлен контейнер для сбора одежды, которую приносят наши сотрудники. Вещи передают фонду, и он распределяет их в пользу малоимущих и многодетных семей, бездомных людей, людей с ограниченными возможностями здоровья, беженцев и многих других, продает в своих благотворительных магазинах или перерабатывает.

### Что в результате?

С октября 2022 года по декабрь 2023 года наши сотрудники собрали 1 408 кг вещей.

65% вещей фонд отправил на переработку.

34% вещей было передано в качестве гуманитарной помощи людям из социально незащищенных групп и отправлено на реализацию в благотворительные магазины фонда Charity Shop и другие секонд-хенды.

1% вещей отправили на утилизацию.

В офисе Компании регулярно проводятся акции по сбору неработающей электроники и бытовой техники для передачи на экологичную утилизацию нашему партнеру «Петромакс». Наши сотрудники также могут сдать использованные литиевые батарейки в офисе. Мы собираем их и передаем на переработку нашим партнерам по утилизации отходов. Кроме того, с 2023 года мы сотрудничаем с социальным экопроектом Re:Books — собираем ненужные книги и передаем их в сельские библиотеки.

**370 кг**

**техники сдано на экологическую переработку в 2022–2023 годах**

**350 кг**

**батареек было передано на утилизацию в 2023 году**

ESG-направление

# Возможности для людей

# Управление персоналом


Сотрудники — самый ценный актив нашей Компании. Мы делаем все, чтобы людям у нас было комфортно и интересно, чтобы они могли работать продуктивно, чувствовали себя защищенными, могли развиваться сами и развивать Компанию.

**~ 5,1 тысячи**
сотрудников работают в «Лаборатории Касперского»

**+2,5 тысячи**
новых рабочих мест в 2022–2023 годах

## Ключевые документы

- Трудовой Кодекс Российской Федерации
- Правила внутреннего трудового распорядка
- Положение о выплатах компенсационного порядка
- Положение об оплате труда

## Подход к управлению персоналом

Мы выстраиваем отношения, основанные на доверии и взаимоуважении. Чтобы рабочая обстановка была комфортной для каждого сотрудника, мы ежедневно анализируем все, с чем он сталкивается по ходу деятельности: от условий в офисе до процессов оценки результатов. Мы слышим потребности каждого и делаем все, чтобы сотрудники «Лаборатории Касперского» чувствовали поддержку и заботу в любой ситуации. Мы создаем необходимые условия для развития и роста отдельных сотрудников, команд и всего бизнеса в целом.

**Наши ключевые задачи:**

- обеспечение достойных условий труда и развития, включая конкурентное вознаграждение и объемный соцпакет;
- инвестиции в обучение и развитие сотрудников, внедрение новых образовательных программ, рост количества учебных часов на каждого сотрудника;
- развитие программы корпоративного волонтерства за счет роста количества участников и расширения сотрудничества с благотворительными фондами.

# Система управления персоналом

**Департамент по работе с персоналом**

| Управление HR-партнерства | Управление инвестициями в персонал | Управление привлечения и развития сотрудников | Kaspersky Academy | Отдел операционной поддержки персонала | Управление развития HR-систем |
|---|---|---|---|---|---|
| Отдел управления персоналом международной региональной сети | Отдел вознаграждения | Отдел подбора персонала | Отдел бизнес-обучения | Группа по работе с обращениями сотрудников | Группа информационных систем управления персоналом |
| Отдел глобальных HR бизнес-партнеров | Группа организационного развития | Отдел международного подбора персонала и руководителей высшего звена | Отдел обучения в сфере информационной безопасности | Группа кадрового администрирования и Направление администрирования социальных льгот | |
| | Группа HR-аналитики | Отдел маркетинга в сфере управления персоналом | Отдел разработки обучающих онлайн-курсов | | |

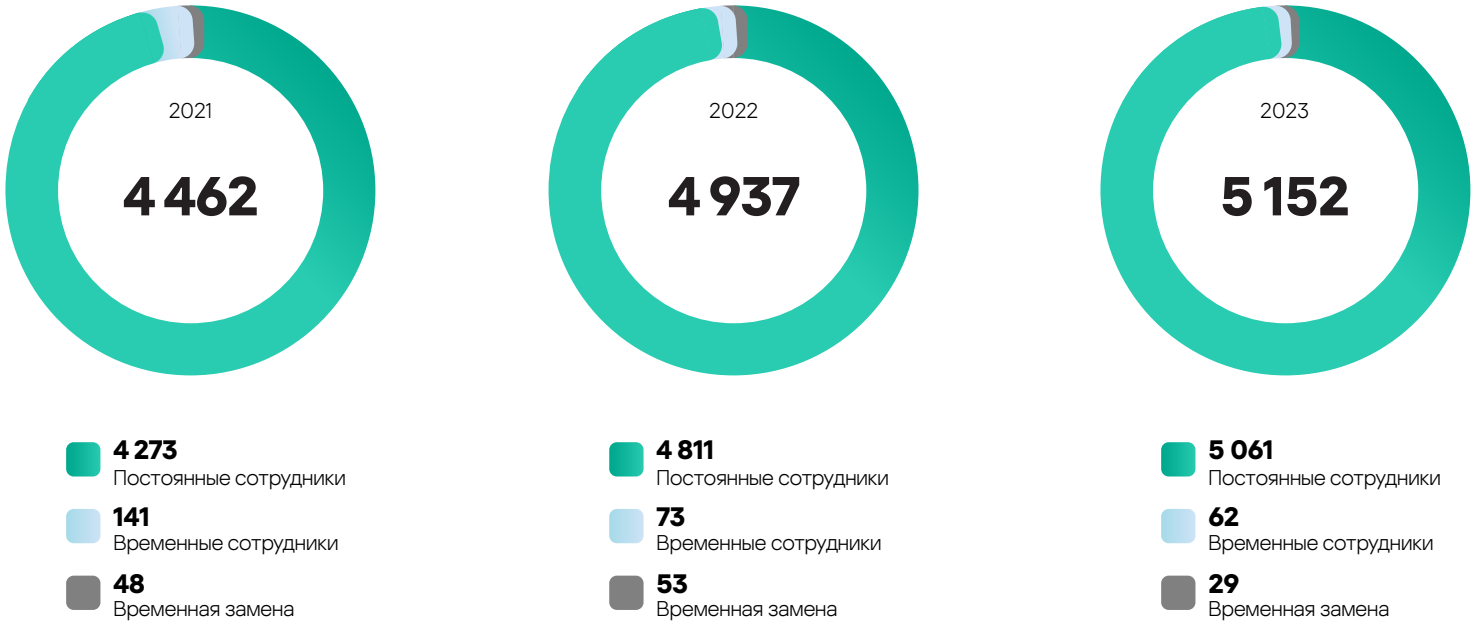
# Численность и структура персонала

GRI 2-7 GRI 401-1

В отчетном году численность персонала «Лаборатории Касперского» выросла на 4,4% и на 31 декабря 2023 года составила 5 152 человека. Несущественное увеличение фактической численности связано со снижением количества увольнений по собственному желанию и развитием бизнес-направлений в Латинской Америке, государствах Африки, Ближнего Востока и в Турции.

**+4,4%**
**рост общей численности сотрудников в 2023 году в сравнении с 2022 годом**

## Общая численность сотрудников Компании, человек




| 2021 | 2022 | 2023 |
|---|---|---|
| **4 273** Постоянные сотрудники | **4 811** Постоянные сотрудники | **5 061** Постоянные сотрудники |
| **141** Временные сотрудники | **73** Временные сотрудники | **62** Временные сотрудники |
| **48** Временная замена | **53** Временная замена | **29** Временная замена |

# Текучесть персонала

Команда «Лаборатории Касперского» объединяет лучших специалистов и формирует среду, в которой каждый сотрудник может проявить и развить свои лучшие качества. Это позволяет нам быстро и эффективно решать сложнейшие задачи.

При подборе персонала мы оцениваем сотрудников независимо от их возраста, гендерной принадлежности и иных признаков, не имеющих отношения к профессиональным компетенциям. Для сотрудников с ограниченными возможностями здоровья мы создаем все необходимые условия, позволяющие им реализовать свой потенциал.

В 2023 году текучесть сократилась во всех регионах присутствия Компании и во всех возрастных группах персонала в связи с изменением тенденций на рынке труда и экономической ситуацией в мире.

**в 1,5 раза**
**сократилась текучесть персонала в сравнении с 2022 годом**

# Программы карьерного роста

Компания заинтересована в создании условий для карьерного роста, расширении профессионального опыта или изменении карьерного пути для сотрудников — в частности, в вертикальных и горизонтальных перемещениях сотрудников с должности на должность и (или) переходе в другую команду. Это отличная возможность повысить мотивацию, улучшить кросс-функциональное взаимодействие между подразделениями внутри департамента.

Сотрудники Компании могут совершенствовать свои профессиональные навыки и личные компетенции, изучать иностранные языки и участвовать во внешних тренингах и мероприятиях.

С 2016 года мы вкладываемся в молодые таланты и помогаем им строить карьеру. Есть у нас и полноценная программа оплачиваемых стажировок для студентов — Kaspersky SafeBoard. За восемь лет существования нашей программы SafeBoard более половины ее участников перешли в штат и сейчас работают на middle- и senior-позициях, стали руководителями разных уровней

Подробнее о программе SafeBoard читайте в подразделе «Подготовка кадров для IT», с. 112

# Материальная мотивация

Мы убеждены, что вклад квалифицированных специалистов в развитие Компании должен вознаграждаться. Поэтому мы поддерживаем заработную плату на конкурентном уровне и поощряем достижения сотрудников.

Для удержания своих экспертов и сохранения их заработной платы на конкурентном уровне в конце 2021 года мы расширили экспертную команду направления Compensations & Benefits. Это помогает нам быстрее и глубже анализировать изменения на рынке, тренды и финансовую оценку выплат сотрудникам. В результате в 2022 году Компания инвестировала в зарплаты и бонусы в два раза больше средств по сравнению с 2021 годом.

В 2022 году заработная плата сотрудников «Лаборатории Касперского» в России выросла в среднем на 20%, а по всему миру — на 18%. В 2023 году повышение вознаграждения сотрудникам «Лаборатории Касперского» в России составило порядка 19% (17% по всему миру), а рост заработной платы стажеров — до 50% в зависимости от направления стажировки.

**Среднее повышение заработной платы сотрудников Компании по всему миру:**

**18%**
в 2022 году

**17%**
в 2023 году

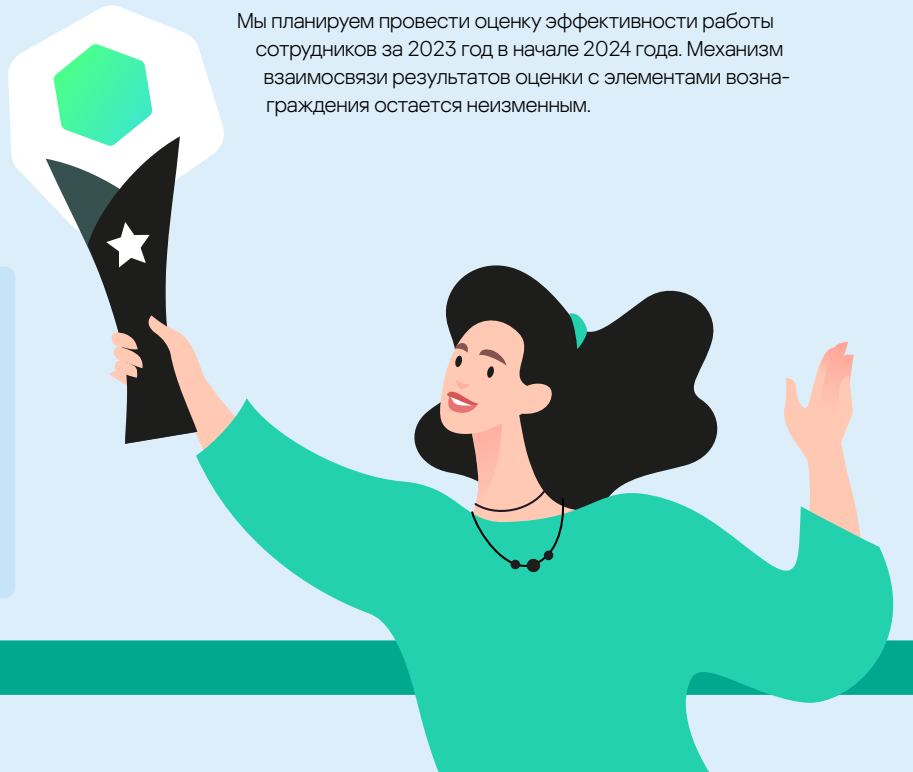
# Оценка персонала

GRI 404-3

Мы регулярно оцениваем качество работы персонала Компании. По итогам 2022 года через процесс оценки эффективности прошли более 90% сотрудников, подпадающих под данный комплекс мероприятий в отчетном периоде.

Один из ключевых компенсационных принципов Компании — «Вознаграждение за результаты». Результаты оценки эффективности оказали непосредственное влияние на выплату бонусов, пересмотр заработной платы и продвижение в должности наших сотрудников.

Мы планируем провести оценку эффективности работы сотрудников за 2023 год в начале 2024 года. Механизм взаимосвязи результатов оценки с элементами вознаграждения остается неизменным.



# Обучение и развитие

GRI 404-2

Компания предоставляет возможности для внутреннего и внешнего обучения всем сотрудникам: они могут пройти онлайн-курсы о продуктах Компании, записаться на курсы по развитию бизнес-навыков, навыков продаж или персональных компетенций, выбрать удобный способ изучения иностранного языка, а также оформить заявку на участие во внешних тренингах и мероприятиях. У нас есть как обязательные, так и необязательные корпоративные образовательные программы.

## Обязательные курсы

### Информационная безопасность

Какие бы меры безопасности мы ни внедрили, в конечном счете главный участник системы — это человек. Человеческий фактор является самым уязвимым аспектом с точки зрения информационной безопасности. Обучение основам кибербезопасности проходят все сотрудники «Лаборатории Касперского», даже если они напрямую не связаны с разработкой или продвижением наших решений.

Из серии курсов по информационной безопасности наши сотрудники узнают о правилах работы с конфиденциальной информацией, учатся безопасно хранить пароли и данные аккаунтов, а также выявлять фишинговые письма и сайты.

### Правила поведения при возникновении чрезвычайной ситуации

Возгорание, задымление, искрение электропроводки и аппаратуры, аварии и другие происшествия приводят к серьезному материальному ущербу и, что более важно, наносят вред здоровью и уносят жизни людей. Изучение правил безопасности обязательно для всех сотрудников «Лаборатории Касперского» и проводится для подготовки сотрудников к адекватным и слаженным действиям во время потенциальной чрезвычайной ситуации.

### Антикоррупционное поведение

Сотрудникам любой современной компании необходимо понимать и соблюдать антикоррупционное законодательство. Следуя изученным в курсе правилам, наши сотрудники могут поддержать репутацию и целостность «Лаборатории Касперского», а также избежать возможных штрафов для Компании и личной ответственности.

### Обучение по продуктам Компании

Этот вид обучения предполагает прохождение обязательных тренингов по продуктам «Лаборатории Касперского» сотрудниками команд Sales и Presales. В течение 90–180 дней в зависимости от занимаемой должности сотруднику необходимо пройти курс и сдать экзамен, подтвердив свой уровень знаний о продуктах Компании.

# Необязательные курсы и внешнее обучение

- Курсы на MOOC-платформах
- Очные тренинги и вебинары на внутреннем портале Kaspersky Academy
- Обучающие программы в рамках проекта Colab Tech
- Внешние курсы для поддержания и развития профессиональной экспертизы
- Обучение иностранным языкам

GRI 404-1

## Показатели в области реализации обучающих программ

| Показатель | 2021 | 2022 | 2023 | Изменение 2023/2022, % |
|---|---|---|---|---|
| **Среднее количество часов обучения (все виды) на одного работника Компании, час** | | | | |
| **Всего** | **5,5** | **6,2** | **8,5** | **+37** |
| **Общее количество часов обучения работников Компании, час** | | | | |
| Женщины | 7 903 | 8 909 | **11 419** | +28 |
| Мужчины | 15 555 | 21 002 | **31 450** | +50 |
| Технические специалисты и руководители | 13 805 | 15 003 | **21 806** | +45 |
| Прочие специалисты и руководители | 9 653 | 14 908 | **21 063** | +41 |
| **Всего** | **23 458** | **29 911** | **42 869** | **+43** |

В 2023 году среднее количество часов обучения на одного работника увеличилось на 37% благодаря тому, что сотрудники все чаще выбирают комплексные долгосрочные программы внешнего обучения, а не точечные короткие курсы, а также по причине существенного роста портфеля внутренних тренингов Kaspersky Academy и онлайн-курсов, доступных сотрудникам на портале.

Мы продолжаем совершенствовать наши программы обучения и увеличиваем инвестиции в образование наших сотрудников. В 2023 году наши расходы на обучение и развитие выросли на 13,5% относительно предыдущего года.

## Инвестиции Компании в развитие и обучение персонала, млн рублей


В 2023 году произошел переход на новую платформу обучения (LMS), ключевыми преимуществами которой стали удобство интерфейса и разнообразие форматов обучения. В ближайших планах — дальнейшее развитие платформы, расширение каталога онлайн-курсов Академии, включая тренинги на иностранных языках и формирование образовательных траекторий для комплексного развития как по определенным темам (enterprise-продажи, навыки коммуникации и т. п.), так и в привязке к ролям и должностям.

# Социальная политика

GRI 401-2

Мы поддерживаем сотрудников на протяжении всего времени работы в Компании: мотивируем их вести здоровый образ жизни, предоставляем доступ к квалифицированной медицинской помощи, обеспечиваем материальную поддержку в сложных жизненных ситуациях.

## Забота о людях

Мы поддерживаем стремление наших сотрудников к здоровому образу жизни, обеспечиваем им объемный соцпакет, медицинское обслуживание в рамках программы страхования и предоставляем материальную помощь тем, кто столкнулся с непредвиденными сложностями. Составляющие социального пакета могут отличаться в местах присутствия Компании в мире.

В России соцпакет доступен всем сотрудникам[1] и включает, помимо прочего:

- ДМС со стоматологией (в том числе для детей сотрудников до 16 лет включительно);
- доплату до 100% оклада к листку нетрудоспособности до 15 рабочих дней в год;
- участие в программе лечения онкологии в России;
- материальную помощь в случае смерти близкого родственника и в других сложных жизненных ситуациях;
- страхование от несчастного случая;
- страхование выезжающих за рубеж;
- вакцинацию взрослых и детей;
- релокационную выплату при переезде в Москву;
- премии юбилярам (по достижении 50, 60, 70 лет) и сотрудникам, стаж которых в Компании достиг 10 и 25 лет;
- компенсацию стоимости занятий спортом;
- изучение иностранных языков.

Это один из самых широких социальных пакетов на российском рынке. У сотрудников есть возможность не выходя из офиса посещать врача-терапевта, врачей-массажистов и психологов, а также спортивные залы с сауной. Кроме того, мы запускаем корпоративные спортивные инициативы и компенсируем сотрудникам стоимость занятий фитнесом.

Для Компании важно знать мнение сотрудников по поводу различных аспектов работы и делиться новостями. Несколько раз в год мы проводим AMA-сессии[2] и Kick-off-встречи[3] с руководством Компании для обсуждения ее результатов, планов и стратегии.

Ежегодно проходит церемония Annual Kaspersky Awards. Ее ключевая задача — признать в равной степени достижения всех департаментов Компании за год. В рамках Kaspersky Awards награждают самых продуктивных сотрудников — тех, кто внес наибольший вклад в успех Компании в уходящем году.

## Поддержка родительства

GRI 401-3

Мы поддерживаем всех наших сотрудников, в семьях которых появляются дети, — в равной мере родителей, усыновителей или опекунов. Им предоставляется отпуск по уходу за ребенком, а к государственному пособию по беременности и родам добавляется корпоративная доплата до полного оклада на протяжении всего отпуска по беременности и родам (как правило, 140 календарных дней)[4].

Корпоративная программа ДМС включает ведение беременности и родов, а после рождения ребенка выплачивается материальная помощь: 150 тысяч рублей за первого ребенка и 200 тысяч рублей — за второго и последующих детей.

[1] Для сотрудников с временными трудовыми договорами и работающих на условиях неполной занятости доступен сокращенный соцпакет. Таких сотрудников в Компании около 0,1%.
[2] От англ. Ask Me Anything («спроси меня о чем угодно»). Онлайн-мероприятие, на котором руководство Компании отвечает на вопросы сотрудников.
[3] Установочная встреча.
[4] Для сотрудниц, проработавших в Компании не менее года.

# Корпоративная культура и деловая этика

Мы стремимся следовать лучшим корпоративным практикам, обеспечивать высокое качество управления и следование принципам деловой этики.

## Ключевые документы

- Трудовой кодекс Российской Федерации
- Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН

**25%**
сотрудников Компании составляют женщины

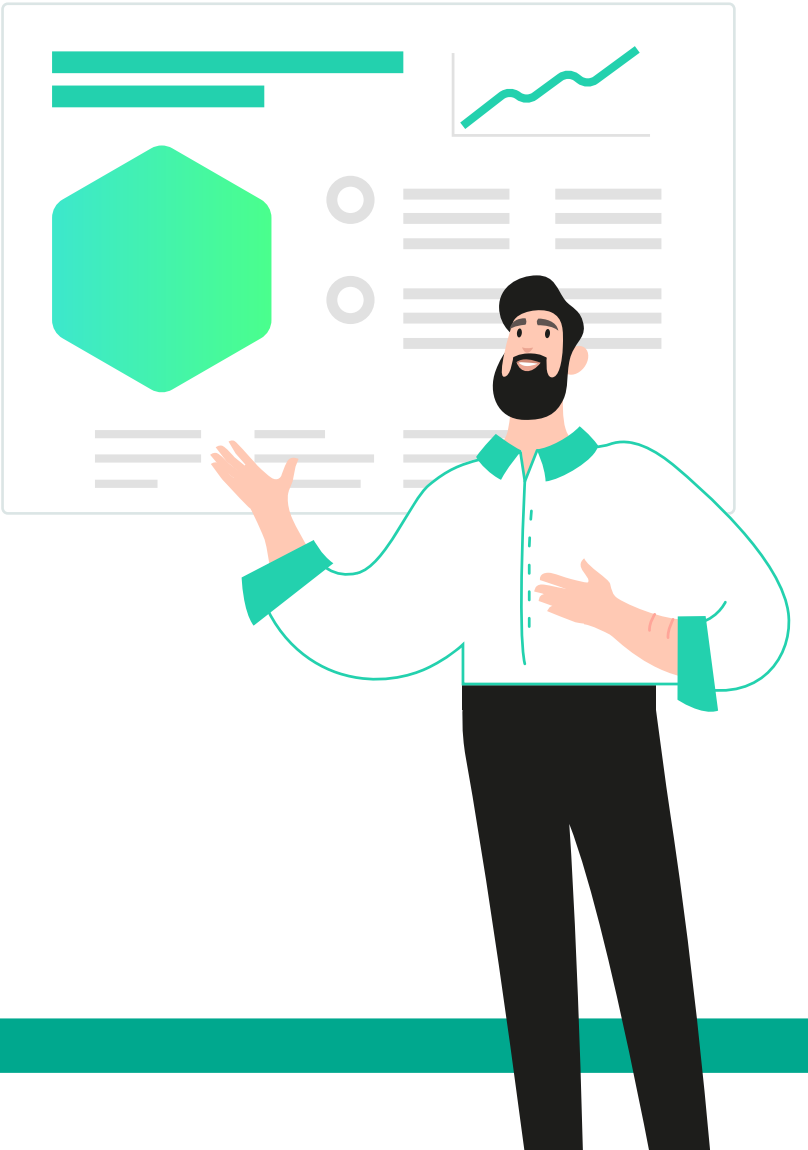
**95%**
соотношение вознаграждения мужчин и женщин

## Равные возможности

«Лаборатория Касперского» не приемлет дискриминацию ни в каких проявлениях. Это один из ключевых принципов Компании, который согласуется с одобренными ООН Руководящими принципами предпринимательской деятельности в аспекте прав человека, а также Целями устойчивого развития ООН (ЦУР ООН), включая задачи ЦУР ООН 4.5, 5.1 и 8.5.

Подробнее о вкладе Компании в достижение ЦУР ООН читайте в разделе «Устойчивое развитие» на с. 17–18

Мы строго соблюдаем законодательство и не ограничиваем наем людей по возрасту, гендеру и иным признакам, а также обеспечиваем право на труд сотрудникам с ограниченными возможностями здоровья. «Лаборатория Касперского» поддерживает уважительные отношения в коллективе и работает над преодолением стереотипов, связанных с работой в IT.



**Наш вклад в разрушение стереотипов об IT-отрасли**

## Делимся вдохновляющими историями о работе в нашей сфере

Вокруг IT-отрасли сложилось множество домыслов, которые могут отпугнуть кандидатов с высоким потенциалом, а также помешать Компании вовремя распознать самых ценных из них. Мы решили развенчать распространенные мифы на примере своих сотрудников, которым стереотипы не помешали построить карьеру в IT.

Быстро вырасти в корпорации и стать руководителем в 23 года? Мечта...

Невозможно воспитывать троих детей и преуспеть в карьере...

Быть ценным гуманитарием в команде программистов? Это утопия...

Экстраверту в IT-среде не прижиться...

Разве можно создать инновационные и прорывные продукты и решения в России?..

Мы провели исследование в нашей компании и профессиональном сообществе и собрали топ-20 стереотипов о российском IT. Затем мы предложили своим сотрудникам опровергнуть их собственным примером. Так родился проект **People in Tech**, запущенный в конце 2022 года, где 20 сотрудников «Лаборатории Касперского» из разных департаментов на позициях от junior до VP рассказывают свои ценные профессиональные истории, развенчивая мифы.

Чтобы проект был действительно вдохновляющим, мы внедрили элемент интерактива: пользователи делятся своим мнением о каком-либо стереотипе. Полученная статистика обнадеживает: до 90% респондентов не разделяют отдельные стереотипы, несмотря на то что по некоторым вопросам мнения все еще делятся почти поровну.

## Что в результате?

**7+ млн**
человек охват проекта

**20 тысяч**
голосов за или против того или иного стереотипа

People in Tech на уровне бизнеса и рекрутмента позволил укрепить имидж «Лаборатории Касперского» как открытого работодателя, способного найти нестандартный способ представить кандидатам свои команды и продукты. Проект также внес свой вклад в борьбу с устаревшими представлениями о российской IT-индустрии и мотивировал людей изменить свое отношение к ней.

Подробнее на сайте проекта careers.kaspersky.ru/peopleintech

GRI 405-2

«Лаборатория Касперского» оплачивает труд каждого специалиста в соответствии с его должностью и квалификацией, независимо от гендерной принадлежности. Для каждой должности проводится оценка рыночного уровня заработной платы — для этого Компания усилила подразделение HR-департамента, специализирующееся на компенсациях и льготах.

Мы стремимся привлекать в IT-индустрию больше женщин и для этого, помимо прочего, сотрудничаем с учебными заведениями по всему миру. Компания проводит для школьников и студентов образовательные мероприятия и мастер-классы, организует стажировки.

Компания запустила несколько онлайн-проектов, в рамках которых женщины могут делиться знаниями и опытом работы в IT. Это комьюнити в социальных сетях Women in CyberSecurity, в котором состоят более 17 тысяч участниц, и сайт Empower Women, где сотрудницы Компании рассказывают о своем образовании, карьерном пути, дают советы и участвуют в подкастах.

Подробнее о вкладе Компании в решение проблемы гендерного дисбаланса в IT-отрасли читайте в подразделе «Женщины в IT: сила равенства»

GRI 405-1, TC-SI-330-a.3

«Лаборатория Касперского» поддерживает соискателей и сотрудников с ограниченными возможностями здоровья. Главное для нас — это человек и его потенциал, а не ограничения.

При отборе мы оцениваем исключительно профессиональные навыки, опыт и экспертность кандидатов. Ряд наших вакансий предусматривает возможность удаленной работы, что может быть важно для сотрудников с ограничениями по здоровью.

Всем сотрудникам, имеющим инвалидность, предоставляются предусмотренные российским законодательством льготы: увеличенный ежегодный отпуск (для всех групп инвалидности) и сокращенный рабочий день (для определенной группы людей с инвалидностью).

# Вовлеченность сотрудников

TC-SI-330-a.2

Мы ежегодно оцениваем уровень удовлетворенности сотрудников в рамках анонимного опроса YourVoice. Опрос позволяет узнать их отношение к изменениям в Компании, корректировке стратегии, оценить уровень влияния на них различных драйверов, таких как оплата, социальный пакет, баланс работы и личной жизни, перспективы профессионального роста, атмосфера в команде и т. д.

Ключевой показатель, на который мы ориентируемся, — это глобальный индекс удовлетворенности работой (eNPS), который отражает долю сотрудников, готовых рекомендовать Компанию как работодателя.

В 2022 году eNPS вырос на 6,7 п. п., до 52,3, а в 2023 году — на 4,5 п. п., до рекордных 56,8, что выше уровня российского рынка[1]. В 2023 году был также побит рекорд по количеству участников опроса — почти 90% сотрудников.

**Результаты опроса в различных представлениях (по командам, департаментам, дивизионам, регионам, возрастным группам, уровням позиций и т. д.) доступны для анализа всем руководителям «Лаборатории Касперского», включая топ-менеджеров. Это позволяет объективно оценить ситуацию как в Компании в целом, так и в отдельных подразделениях, увидеть сильные стороны и определить зоны развития.**

[1] По данным Happy Inc — российской компании в области HR Tech, лидера рынка решений для опросов вовлеченности.

# Безопасность труда и охрана здоровья

Мы следим за тем, чтобы каждое рабочее место в «Лаборатории Касперского» было комфортным и безопасным, а все работники имели доступ к квалифицированной медицинской помощи.

**0**

**несчастных случаев, связанных с реализацией профессиональных рисков в 2022 и 2023 годах**

## Ключевые документы

- Трудовой кодекс Российский Федерации
- Положение по идентификации опасностей и определению уровня профессиональных рисков
- Инструкция о мерах пожарной безопасности
- Правила внутреннего трудового распорядка
- Политика в области охраны труда

## Управление охраной труда и здоровья

GRI 403-2 GRI 403-4 GRI 403-5 GRI 403-6

Безопасность труда в «Лаборатории Касперского» обеспечивает департамент по работе с персоналом с привлечением внешних консультантов. В состав департамента входит Группа кадрового администрирования, отвечающая за охрану труда в Компании и здоровье сотрудников.

Кроме того, в Компании действует комиссия по охране труда, в состав которой входят представители различных департаментов. Весной 2023 года мы создали серию видеороликов «Безопасная среда», в которых напомнили сотрудникам о важных вещах, связанных с комфортным и безопасным нахождением в офисе, включая порядок проведения праздников, оформления пропусков, правила парковки и т. д.

GRI 403-9

Большинство сотрудников «Лаборатории Касперского» работают в офисе. За отчетный период не было зафиксировано ни одного случая травматизма среди сотрудников.

GRI 403-6

Весь российский персонал «Лаборатории Касперского» и их дети в возрасте до 16 лет включительно охвачены корпоративной программой ДМС, в которую также входит страхование от несчастных случаев (для сотрудников Компании). Если с сотрудником происходит несчастный случай, об этом можно сообщить в страховую компанию через департамент по работе с персоналом.

В рамках программы ДМС можно пройти лечение от онкологических заболеваний, воспользоваться услугами стационара, получить психологическую помощь онлайн и офлайн, пройти ежегодный медосмотр для получения санаторно-курортной карты, вакцинироваться от сезонных заболеваний. В штаб-квартире Компании работают спортивный зал и сауна, есть возможность посетить терапевта, психолога и массажиста в офисе. Мы также компенсируем сотрудникам часть трат, направленных на оздоровление, — например, оплату фитнеса или детских оздоровительных лагерей. Кроме того, сотрудники «Лаборатории Касперского» получают корпоративную скидку в сети аптек «Ригла».

Чтобы оценить эффективность системы управления охраной труда и здоровья, мы систематически проводим опросы сотрудников.

Во всех подразделениях регулярно проводится специальная оценка условий труда. По результатам такой оценки в отчетном периоде рабочим местам был присвоен второй итоговый класс условий труда.

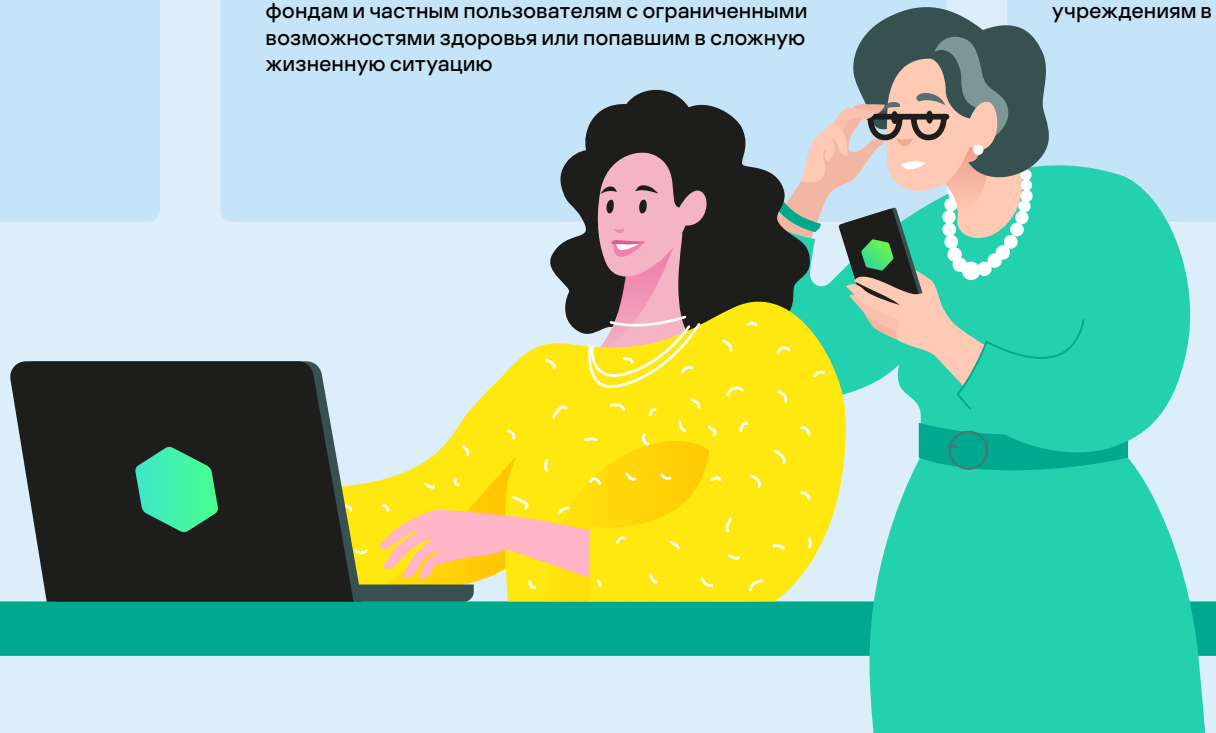
# Взаимодействие с местными сообществами

Мы учитываем интересы тех, кто нуждается в нашей поддержке. «Лаборатория Касперского» сотрудничает с федеральными и региональными благотворительными фондами, помогает людям с тяжелыми заболеваниями и социально незащищенным гражданам, стремится вовлечь в эту деятельность своих сотрудников.

**55,8 млн рублей**
прямые затраты на благотворительность за 2022–2023 годы

**4,8 тысячи**
лицензий безвозмездно передано благотворительным фондам и частным пользователям с ограниченными возможностями здоровья или попавшим в сложную жизненную ситуацию

**>300**
единиц техники передано НКО и образовательным учреждениям в отчетном периоде



Команда проектов устойчивого развития в соответствии с внутренней политикой благотворительности определяет:

- основные направления благотворительной деятельности Компании;
- критерии и порядок взаимодействия со сторонними организациями при разработке, выборе и реализации благотворительных проектов и акций;
- процедуры благотворительной передачи лицензий на защитные решения и IT-оборудование.

Летом 2023 года мы создали на внутреннем портале специальную страницу, где собрана вся актуальная информация о деятельности Компании в области устойчивого развития. Там приведен полный список наших партнеров — фондов, некоммерческих организаций (НКО) и образовательных учреждений, объем оказанной каждому партнеру помощи и перечень волонтерских проектов, к которым сотрудники Компании могут присоединиться самостоятельно.

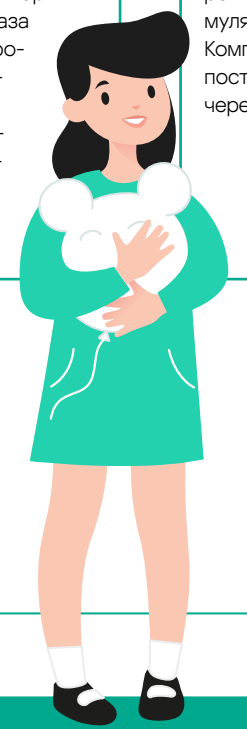
В частности, Компания поддерживает детский дом и интернат, образовательные учреждения и НКО, которые организуют альтернативную опеку над сиротами, помогают жертвам насилия (в том числе цифрового), людям с ограниченными возможностями здоровья и тяжелыми заболеваниями, а также НКО, которые занимаются защитой природы и просветительской деятельностью в области донорства, экологии и других тем, связанных с направлением устойчивого развития.

«Лаборатория Касперского» поддерживает более десяти фондов и НКО — как федеральные («Подари жизнь», «Вера», «Синдром любви»), так и специализированные или региональные («Игра», Нижегородский женский кризисный центр, «Живи»). Компания стремится строить с фондами и НКО длительные партнерские отношения, поддерживая их мероприятия, организовывая волонтерские проекты, в том числе делясь профессиональной экспертизой pro bono.

Мы оказываем административно-хозяйственную поддержку Удомельскому детскому дому (УДД) и Тверской школе № 4 — специализированному интернату для детей с задержкой психического развития, расстройствами аутистического спектра и нарушениями в работе опорно-двигательного аппарата. Компания помогает учреждениям проводить ремонт, закупать оборудование, бытовую химию, одежду, обувь и школьные принадлежности для воспитанников, а также организовывать поездки на летний отдых. Мы помогаем УДД с 2014 года. Именно тогда группа волонтеров из Компании, их друзья и близкие начали ездить в Удомлю. С тех пор наши визиты стали традицией: четыре раза в год мы приезжаем к воспитанникам, проводим мастер-классы, игры, гуляем вместе. Каждое лето сотрудники Компании и администрация детского дома устраивают для детей двухдневный туристический поход.

Кроме того, Компания оказывает поддержку жертвам катастроф и стихийных бедствий, пожилым людям и тем, кто оказался в сложной жизненной ситуации.

Так, в феврале 2023 года «Лаборатория Касперского» выделила бюджет в размере 390 тысяч турецких лир для организаций, помогающих жертвам землетрясения: Управлению по чрезвычайным ситуациям и стихийным бедствиям Турции (AFAD), НКО Ahbap и сообществу TBD (Türkiye Bilişim Derneği). Коллеги из офиса в Турции закупили и отправили в пострадавший регион фургон питьевой воды и внешние аккумуляторы (пауэрбанки). А в сентябре 2023 года Компания выделила $10 тысяч на помощь пострадавшим от землетрясения в Марокко через наш офис в этой стране.



# Социальные и благотворительные проекты

**GRI 203-1**

Ежегодно мы проводим фандрайзинговые акции среди сотрудников: поддерживаем сборы партнеров-НКО и организуем собственные, приуроченные к важным датам и праздникам. С 1 января 2022 года по 31 декабря 2023 года наши сотрудники собрали более

**2,6 млн рублей**

для фондов «Живи», «Игра», «Подари жизнь», «Синдром любви», «Вера», «Подарок ангелу».

В начале 2022 года «Лаборатория Касперского» вошла в созданный Региональной общественной организацией инвалидов (РООИ) «Перспектива» Совет бизнеса по вопросам инвалидности, а летом впервые приняла участие в ярмарке вакансий для соискателей с инвалидностью. Компания продолжила поддерживать это мероприятие и в 2023 году.

Осенью 2022 года Компания запустила проект по обсуждению и дестигматизации темы инклюзивного трудоустройства. К Международному дню человека с инвалидностью стартовал внутрикорпоративный специальный проект «Границы, которые мы раздвигаем», посвященный профессиональному и личному пути сотрудников Компании, имеющих инвалидность. В 2023 году мы продолжили развитие проекта, создав сайт, где рассказали про профессиональный и личный путь наших коллег с инвалидностью и тех, кто воспитывает детей с инвалидностью. Таким образом, проект впервые стал публичным — мы считаем, что важно открыто говорить о сложном и трудном, чтобы напомнить о ценности взаимной поддержки.

Той же осенью мы начали ежеквартально рассказывать о своих благотворительных инициативах, социальных и волонтерских проектах. В телеграм-канале Kaspersky Daily появилась рубрика CSR digest, посвященная благотворительной деятельности Компании. Кроме того, «Лаборатория Касперского» поддержала проведение международного кинофестиваля о жизни людей с инвалидностью «Кино без барьеров», организованного РООИ «Перспектива». Зимой 2022/2023 года совместно с фондом «Подари жизнь» Компания помогла открыть игровую комнату в отделении лучевой терапии Морозовской больницы для маленьких пациентов, проходящих там лечение.

В мае и декабре 2023 года мы помогли организовать бизнес-завтраки для Совета бизнеса по вопросам инвалидности. Первое мероприятие было посвящено теме «Первые шаги при найме сотрудника с инвалидностью: создание условий внутри компании». А в декабре участники бизнес-завтрака обсудили тему «Трудоустройство соискателей с инвалидностью: коммуникационное продвижение, обучение, подготовка руководства и ответственных сотрудников». Во всех мероприятиях приняли участие 30 представителей компаний, поддерживающих инклюзию.

С ноября 2023 года мы стали участниками проекта «Технологии добра». Это федеральный проект ПАО «Совкомбанк» и Skolkovo Fintech Hub для организации инфраструктурной поддержки и цифрового развития некоммерческих организаций и благотворительных фондов в Российской Федерации. Здесь социально ориентированные организации могут найти для себя нужные продукты и сервисы бесплатно либо на льготных условиях. В рамках программы мы безвозмездно передаем лицензии на продукты «Лаборатории Касперского», в частности в 2023 году бесплатные лицензии получили 11 НКО.

В 2024 году мы планируем создать карточки по основам компьютерной грамотности совместно с фондом «Синдром любви». Они будут написаны простым и доступным языком, чтобы облегчить восприятие материала людьми с ментальными особенностями.

Мы стремимся повышать доступность продуктов, сервисов и возможностей информационной безопасности для людей с инвалидностью.

В 2023 году мы провели ряд усовершенствований наших продуктов. Kaspersky for Windows теперь поддерживает режим высокой контрастности. Обновление улучшает читаемость, яркость элементов и навигацию, что делает взаимодействие с приложением более эффективным и комфортным для наших пользователей с цветовой слепотой.

Kaspersky for Mac полностью совместим с macOS Dark Mode и Display Settings, которые позволяют настроить интерфейс с учетом индивидуальных предпочтений, обеспечивая удобство использования для всех наших пользователей. Кроме того, в Kaspersky for Mac теперь имеется функция VoiceOver, которая обеспечивает доступность для пользователей с ограниченными возможностями зрения.

**Наш вклад в профессиональное развитие молодых специалистов с инвалидностью**

## Помогаем молодежи реализовать свой потенциал

- Участники из 22 городов России
- 8 менторов
- 6 недель практики

В ноябре 2023 года совместно с другими компаниями «Лаборатория Касперского» приняла участие в программе «Попробуй профессию в деле», организованной РООИ «Перспектива», нашей дружественной НКО. Цель проекта — помочь студентам и выпускникам с инвалидностью в реализации своего потенциала путем погружения в будущую профессию.

К участию в программе приглашались недавние выпускники и студенты последних курсов, обучающиеся по направлениям:

- IT;
- экономика/финансы;
- юриспруденция;
- маркетинг;
- HR.

Наша Компания принимала участие в этой программе впервые, и менторами для участников с инвалидностью стали восемь сотрудников из самых разных подразделений.

## Что в результате?

В программе приняли участие ребята из 22 городов России. В течение шести недель они вместе с менторами выбрали и проработали бизнес-кейсы, а по завершении программы представили свои проекты перед онлайн-аудиторией. К примеру, одна пара участников разработала браузерное решение, вторая — приложение для редактирования alt-текстов, а третья подготовила набор маркетинговых ассетов для выдуманной видеоигры.

Таким образом, студенты и выпускники получили возможность попробовать свои силы в разных сферах, применить навыки для решения реальных технических задач, а также приобрели опыт работы в команде.

# Волонтерские программы

Более 200 сотрудников «Лаборатории Касперского» участвуют в программе корпоративного волонтерства, которая включает несколько направлений: донорство крови, благотворительные спортивные мероприятия, патронаж детского дома и оказание бесплатной профессиональной помощи.

## Спортивное волонтерство

В 2022–2023 годах сотрудники Компании приняли участие в ряде благотворительных спортивных мероприятий в пользу фондов «Синдром любви» и «Вера» и РООИ «Перспектива»: забеги, сайклинг-марафоны, онлайн-триатлоны, соревнования по биатлону и мини-футболу. Мы продолжаем поддерживать этот формат по нескольким причинам. Во-первых, спорт пользуется большой популярностью среди сотрудников. За последние пять лет внутри Компании образовалось полноценное сообщество единомышленников-спортсменов. Во-вторых, спортивные мероприятия помогают фондам продвигать тему инклюзии и участия в добрых делах, которая очень важна и для Компании. В-третьих, это отличная форма тимбилдинга, которая помогает сблизиться коллегам из разных департаментов.

## Патронаж Удомельского детского дома

Наши сотрудники ежеквартально посещают УДД и каждый раз тщательно продумывают программу для подопечных, включая образовательные лекции, спортивные мероприятия и летний поход с палатками и песнями у костра. Перед каждой поездкой сотрудники помогают закупить лекарства, средства гигиены, одежду, обувь и школьные товары для воспитанников.

## Субботники

Дважды в год наши сотрудники участвуют в субботниках в московских хосписах и центрах паллиативной помощи, находящихся под патронажем фонда «Вера». Волонтеры проводят генеральную уборку в главных холлах, убирают территорию, сажают цветы и помогают решить хозяйственные вопросы: закупают продукты, хозтовары, воду и прочее.

## Донорство

Около 150 сотрудников Компании дважды в год сдают кровь для подопечных фонда «Подари жизнь». Акция проводится в московском офисе «Лаборатории Касперского» совместно с Центром крови Федерального медико-биологического агентства (ФМБА) России. В 2023 году мы предложили сотрудникам вступить в ряды потенциальных доноров костного мозга и стволовых клеток. Мы провели лекцию-ликбез с представителем ФМБА, которая рассказала нашим донорам подробнее о процедуре первичного HLA-типирования, противопоказаниях и подготовке к ней. Осенью на очередной акции 32 сотрудника Компании сдали кровь для вступления в регистр доноров.

## Волонтерство pro bono

С 2022 года мы развиваем новое направление волонтерства — pro bono, или оказание безвозмездной профессиональной помощи.

Наши специалисты помогли провести онлайн-голосование для ежегодной премии «Благотворительность против рака» фонда «Подари жизнь», два тренинга по основам кибергигиены для сотрудников «Детских деревень SOS» из разных регионов России и еще два — для образовательного проекта «Я могу» совместно с платформой социальных изменений todogood.

Летом 2022 года наши специалисты провели профориентационную лекцию для детей с инвалидностью в рамках летнего выездного лагеря РООИ «Перспектива» и выступили менторами для людей с инвалидностью в рамках образовательного проекта «Межрегиональные карьерные перспективы».

В 2023 году наша дизайн-команда помогла фонду «Синдром любви» обновить страницу онлайн-акции «Апельсины», посвященной Международному дню людей с синдромом Дауна. Задачей было оценить и обновить страницу акции визуально, сделать ее более привлекательной с точки зрения картинок, цветовых сочетаний, логики (уменьшить число кликов) и упрощения клиентского (донорского) пути. Проведя анализ аналогичных акций и проконсультировавшись с командой продуктового дизайна, наши дизайнеры предложили минималистичный дизайн с понятными и простыми визуалами, которые помогли бы сделать акцент на ключевом сообщении и сместить фокус на более взрослую аудиторию. Мы рады, что внесли свой вклад в продвижение акции и помогли фонду собрать рекордное количество пожертвований — более 1 000 000 рублей, что вдвое больше, чем в 2022 году.

**Наш вклад в повышение мотивации сотрудников**

# Вдохновляем коллег на достижения

В 2023 году мы добавили новые уникальные и полезные функции в личный кабинет сотрудников. В нем появились разделы, которые каждый из них может заполнить сам. К примеру, можно указать свой размер футболки, чтобы, заказывая мерч к ежегодному корпоративу, команда внутренних коммуникаций и продакшен точно знали, сколько и каких футболок необходимо. Точность в расчетах позволила сэкономить в этом году до 0,5 млн рублей.

Кроме того, сотруднику предлагается отметить проекты, которыми он занимается, область экспертизы, а также указать, чем он может быть полезен коллегам. Все эти данные в виде тегов подгружаются в личный кабинет, облегчая коллегам поиск не только ответственных за тот или иной проект, но и друга по интересам.

Одной из самых обсуждаемых новинок на интранете в 2023 году стало появление ачивок[1] в личном профиле сотрудника. Так команда внутренних коммуникаций называет виртуальные награды (бейджи), которые присваиваются за заслуги перед Компанией. Ачивки присваиваются сотрудникам за длительный срок работы в «Лаборатории Касперского», победителям корпоративных премий и конкурсов, спортсменам, волонтерам, публичным спикерам, авторам запатентованных технологий и т. д. С помощью этого инструмента мы даем возможность сотрудникам понять, какое поведение в Компании поощряется, а состязательность и игровая стилистика наград делают их особо привлекательными. В Компании очень насыщенная внерабочая или околорабочая жизнь, поэтому есть масса поводов наградить ачивками за разные активности: музыканты, артисты, флудеры, специальные ачивки за мемы и т. д.


## Что в результате?

За год с небольшим существования награды команда внутренних коммуникаций придумала

**43 ачивки**.

Их уже получили

**более 1,7 тысячи** человек

(всего **2 523 бейджа**).

# Подготовка кадров для IT-отрасли. Наш опыт

## Как мы готовим специалистов

- Мотивируем школьников, обучаем студентов
- Прокачиваем квалификацию специалистов в информационной безопасности

В условиях бурного развития технологий важно поддерживать профессиональный уровень IT-специалистов и постоянно пополнять команду новыми кадрами. Мы считаем, что самый надежный способ обучить будущие кадры — взращивать их собственными силами. Уже сейчас мы реализуем комплекс образовательных и партнерских проектов, охватывающих аудиторию от школьников до IT-специалистов.

## Наш подход к образованию

В сфере информационных технологий важно мыслить на перспективу: кто будет работать в нашей компании завтра? Через год? Через пять-десять лет? Представляем ли мы, чем сейчас занимаются эти люди, будь то специалисты или школьники, только вставшие на путь изучения информационных технологий? Какими будут их знания и умения в тот момент, когда они придут в нашу команду? Будет ли уровень их знаний соответствовать уровню развития технологий?

Согласно результатам нашего исследования, проведенного в 2022 году, кадровый вопрос стоит остро не только для IT-отрасли, но и для многих других российских компаний. Нехватка собственных специалистов по кибербезопасности — одна из главных причин, по которой компании обращаются к поставщикам IT- и ИБ-услуг, наряду с более высокой эффективностью аутсорсинга и необходимостью соблюдать регуляторные требования.

**42%**

**российских компаний испытывают дефицит специалистов по информационной безопасности**[1]

Мы осознаем, что заниматься подготовкой кадров нужно заблаговременно и непрерывно. Именно поэтому мы разработали и постоянно расширяем комплекс образовательных проектов. Мы работаем со школьниками, студентами и преподавателями, записываем мультфильмы и видеолекции для подрастающего поколения, проводим хакатоны[2], летнюю практику и оплачиваемые стажировки, а также реализуем множество образовательных проектов в партнерстве с профильными ведомствами и вузами. Отдельное направление — обучение специалистов, которым также необходимо постоянно актуализировать свои знания и практические навыки.

«Образование — один из главных драйверов безопасного будущего, которое мы стремимся построить, уделяя особое внимание социальным проектам».

**Кирилл Ширяев,**
руководитель Kaspersky Academy

[1] По данным опроса, проведенного «Лабораторией Касперского» в 2022 году среди 3,2 тысячи специалистов компаний со штатом более 50 человек в 26 странах, включая Россию.
[2] Хакатон — событие, где IT-специалисты совместно разрабатывают решение поставленной задачи.

# Просвещаем школьников

Мы считаем, что детей необходимо знакомить с отраслью, в которой им предстоит работать. По данным нашего опроса[1], 41% детей в России хотят работать в сфере IT. «Лаборатория Касперского» постоянно находит новые форматы просвещения и обучения школьников, чтобы сделать тему кибербезопасности знакомой и понятной для них.

## Математическая вертикаль Касперского

Один из наших ключевых образовательных проектов — «Математическая вертикаль», в рамках которой мы разработали собственную программу с акцентом на информационной безопасности. Мы подходим к вопросу комплексно: наша программа подразумевает работу не только со школьниками, но и с учителями.

«Лаборатория Касперского» участвует в московской программе «Математическая вертикаль» под эгидой Департамента образования Москвы с момента ее запуска в 2018 году. По условиям программы школьники углубленно изучают математику и направления естественно-научного цикла. При поддержке Компании создан отдельный курс «Математическая вертикаль Касперского» с акцентом на программировании и информационной безопасности, который уже три года проводится в наших подшефных московских школах для учеников 7–11-х классов.

На сегодняшний день «Лаборатория Касперского» присутствует уже в 15 школах Москвы. Наши эксперты преподают ученикам спецкурсы и проводят семинары. По окончании 10-го класса ребята приходят к нам на стажировку, которая не только упрощает им путь в вуз на IT-специальность, но и дает шанс остаться и развиваться в самой Компании.

В 2023 году первые участники программы «Математическая вертикаль» окончили школу, некоторые из них — в статусе победителей Национальной технологической олимпиады по информационной безопасности.

Школьники участвуют во многих онлайн-мероприятиях, которые проводит «Лаборатория Касперского». В частности, в московских школах мы организовали IT-марафон Касперского. В 2023 году в нем принимали участие 34 школы, в каждой из которых обучается несколько тысяч учеников.

Более 400 московских учителей математики и информатики прошли курсы повышения квалификации от «Лаборатории Касперского» в 2022/2023 учебном году.

Мы плотно работаем со школьными преподавателями. Третий год подряд наши специалисты ведут курсы повышения квалификации для московских учителей математики и информатики совместно с Департаментом образования и науки Москвы. Обучение проходит в онлайн-режиме, а по его окончании слушатели проверяют свои знания с помощью тестирования. Некоторые учителя проходят наш курс ежегодно, так как понимают, что IT-отрасль быстро развивается и знания необходимо обновлять.

Учителя, окончившие наши курсы, получают соответствующий документ государственного образца, который выдается городским методическим центром. В первом полугодии 2023/2024 учебного года на этих курсах успешно обучились 250 преподавателей, примерно столько же закончат их во втором полугодии. Мы готовы распространять свои обучающие программы и на слушателей в регионах.

**В 15 подшефных школах создана «Математическая вертикаль Касперского»**

**34 школы участвуют в IT-марафоне Касперского**

«Несколько лет назад мы заключили историческое соглашение с министерством образования Москвы. Условия были такими: мы начинаем с одной базовой школы, постепенно расширяем охват, размещаем в интернете материалы, которые могут быть полезны всему городу, а в дальнейшем — и всей стране. Эти условия мы выполняем безоговорочно».

**Вениамин Гинодман,**
советник генерального директора «Лаборатории Касперского» по образовательным проектам

[1] Опрос проведен по заказу «Лаборатории Касперского» весной 2023 года в России среди 2 тысяч родителей и их детей школьного и дошкольного возраста.

# «Урок цифры»

С 2018 года «Лаборатория Касперского» выступает партнером всероссийского образовательного проекта «Урок цифры», который является частью федерального проекта «Кадры для цифровой экономики». Каждый год мы разрабатываем и выпускаем один тематический урок с интерактивным тренажером для школьников, их родителей и учителей, который изучают в российских школах в течение трех недель.

НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ ЦИФРОВАЯ ЭКОНОМИКА

**Федеральный проект «Кадры для цифровой экономики»**

**Всероссийский образовательный проект «Урок цифры»**

Реализуют Министерство просвещения, Минцифры России и АНО «Цифровая экономика» в партнерстве с ведущими российскими технологическими компаниями

С 2018 года мы разработали шесть тематических уроков о кибербезопасности, способах защитить себя и свои данные, а также о работе IT-специалистов и разработчиков. Мы прилагаем большие усилия, чтобы не перегружать школьников сложной информацией, а, наоборот, подать только самые важные идеи легко и доступно, а также заинтересовать их качественной анимацией и интерактивом.

В частности, темой одного из уроков 2022/2023 учебного года стала защита личных данных и мобильных устройств: «Что прячется в смартфоне: исследуем мобильные угрозы». Все уроки начиная с 2018 года доступны на сайте проекта в любое время, а пройти их можно в школе или дома всей семьей.

В начале 2024 года школьники отправились вместе с нами в 2050 год и смогли попробовать себя в построении кибербезопасного будущего. Даже в фантастическом мире ребята решают вполне реальную проблему: как защищать умный дом и отражать кибератаки с применением новейших технологий. Кроме того, у детей снова появился повод задуматься о будущей профессии — в 2024 году на наших уроках они узнали, кто такие пентестеры[1] и специалисты по безопасной разработке.

Подробнее на сайте проекта «Урок цифры»

Ученик проходит несколько этапов:

- изучает видеолекцию с участием талисмана компании — Мидори Кума;
- практикуется на тренажере, разделенном на три уровня сложности в зависимости от того, в каком классе он учится. Тренажер — это анимированный и интерактивный комикс о приключениях двух ребят, которым Мидори вместе с обучающимися помогает разобраться в IT-проблеме;
- получает сертификат за прохождение урока и коллекционирует достижения.

Записывая для детей уроки о кибербезопасности, мы достигаем следующих целей:

- рассказываем детям и взрослым о виртуальном мире и его угрозах;
- обучаем методам защиты личности и персональных данных;
- знакомим школьников с новыми профессиями: разработчик защитных решений для смартфонов, эксперт по информационной безопасности, а также контент- и спам-аналитик;
- раскрываем нюансы разработки защиты мобильных устройств.

**13,5 млн**

прохождений набрали «Уроки цифры» от «Лаборатории Касперского» с 2018 года

**11–15%**

детей сталкивались хотя бы с одной из угроз: телефонным или онлайн-мошенничеством, взломом аккаунтов или заражением устройств вредоносным ПО[2]

**>2 млн**

раз пройдены «Уроки цифры» в 2023 году

[1] Пентестер — специалист, который тестирует программу на умышленное проникновение (хакерскую атаку).
[2] По данным опроса, проведенного по заказу «Лаборатории Касперского» в России в 2022 году среди 2008 человек — детей и их родителей.

# Онлайн-курс для школьников

В октябре 2023 года мы опубликовали первые материалы онлайн-курса «Основы информационной безопасности», рассчитанного на учеников 7-го класса и доступного в системе «Московская электронная школа» (МЭШ).

Курс состоит из трех модулей для поэтапного погружения в тему. Он основан на материалах, накопленных за время сотрудничества с московскими школами по совместным проектам с Департаментом образования и науки Москвы с учетом последних тенденций в индустрии. Школьники изучают тему в игровой форме, помогая положительным персонажам бороться со злом.

Чему мы обучаем учеников средних и старших классов:
- программированию на скриптовых языках[1];
- настройкам безопасных информационных систем;
- шифрованию и дешифрованию данных;
- созданию защищенных приложений.

Летом 2024 года мы планируем обновить наш онлайн-курс по информационной безопасности, а к 1 октября подготовим точно такой же для учеников 8-х классов. Он будет адресован не только москвичам, но и жителям всей России. Каждый заинтересованный школьник и нуждающийся в помощи учитель или ответственный родитель из любого уголка страны может зайти на сайт https://kids.kaspersky.ru и воспользоваться материалами нашего курса.

[1] Языки программирования.

# Цифровой ликбез

Еще один формат, который мы используем, чтобы познакомить подрастающее поколение с техникой безопасности в интернете, — короткие мультфильмы. В 2022 году мы присоединились к просветительскому проекту «Цифровой ликбез», направленному на повышение цифровой грамотности и кибербезопасности. Проект основан на видеороликах для детей и взрослых, созданных ведущими цифровыми компаниями.

В 2022–2023 годах вместе с АНО «Цифровая экономика» при поддержке Министерства просвещения и Минцифры России мы выпустили три мультфильма для детей старше шести лет. Мы рекомендуем взрослым просматривать их вместе с детьми, чтобы разъяснить ребенку непонятные слова и помочь усвоить информацию.

Всего за две минуты мы рассказываем детям об основных киберугрозах. Сюжет повествует о приключениях обитателей морского городка Оушенсити. Главная героиня Лина — начинающая журналистка, которая проходит стажировку в самой крупной IT-компании «Карасевский», где ведет блог о том, как жители городка попадаются на крючок кибермошенников.

Сложные понятия и детали вынесены за пределы ролика в текстовое описание, чтобы взрослый смог не только объяснить ребенку непонятные моменты, но и рассказать чуть больше, а также расширить собственные знания. Все ролики доступны для скачивания, так что их можно использовать для обучения даже там, где нет доступа к интернету, в любой подходящий момент.

Мы уверены, что подобные форматы не только повышают общий уровень цифровой грамотности, но и помогают нам популяризировать IT-профессию, а также постоянно поддерживать интерес к ней со стороны будущих специалистов.

# «Долина технологий»

**1 200**
**участников зарегистрировались в «Долине технологий»**

**44**
**победителя приехали на финальный тренинг**

Разрабатывая образовательные проекты для школьников, мы задумались о том, чтобы организовать для них настоящую практику, как для студентов вузов, чтобы дать возможность ближе познакомиться с разными IT-профессиями и окунуться в мир кибербезопасности. В 2023 году мы впервые провели открытую летнюю практику для школьников 8–10-х классов и студентов колледжей первого и второго курсов. Трехнедельная программа «Долина технологий» состоит из вебинаров и офлайн-занятий в штаб-квартире Компании. На очную часть практики мы пригласили тех, кто наиболее успешно проявил себя в ходе онлайн-обучения.

Всего в проекте зарегистрировались 1 200 участников, которых специалисты «Лаборатории Касперского» знакомили с IT-профессиями в онлайн-режиме. Затем участники «Долины технологий» выполняли домашние задания, а по их результатам мы отобрали 44 человека (32 из Москвы и 12 из регионов), которые приехали в наш московский офис. Мы проводили для них экскурсии, а наши разработчики, тестировщики и другие эксперты три дня рассказывали ребятам о профессиях в IT и помогли им сформировать представление о работе в Компании. Также для них были организованы командообразующие мероприятия и квиз.

В 2024 году Компания планирует повторить программу и масштабировать ее, так как мы отметили большой интерес целевой аудитории к «Долине технологий».

## Развитие детско-юношеского киберспорта

Россия стала первой страной, где спортивное программирование официально признано видом спорта. В июне 2023 года мы заключили соглашение о стратегическом сотрудничестве с Федерацией спортивного программирования. Помогая спортсменам в подготовке к соревнованиям, мы надеемся внести свой вклад в наращивание кадрового потенциала в IT-сфере. Школьники и студенты смогут повысить уровень своих знаний и умений в IT и всегда оставаться в курсе главных событий в нашей отрасли.

## Новые проекты для школьников

Мы получаем множество запросов от школ и колледжей, которые заинтересованы в наших новых курсах. Чтобы удовлетворить их потребности, «Лаборатория Касперского» в 2024 году планирует запустить два новых курса. Один из них — Enter_IT, посвященный реальным профессиям в IT-компании. Этот курс расскажет слушателям, что представляет собой отрасль информационной безопасности, какие есть профессии в этой сфере и как можно в них попасть. Новый курс будет доступен школьникам из любого уголка России и других русскоязычных стран, так как он будет выпущен в видеоформате.

Также мы готовим курс по кибергигиене, посвященный правилам поведения в интернете. Это также будет видеокурс, который мы планируем выпустить в 2024 году на русском и английском языках и распространять как в России, так и в других странах.

# Kaspersky Academy

Стремясь укрепить кадровый потенциал в IT-сфере, мы постоянно расширяем взаимодействие с вузами. Наша задача — дать необходимые знания и практический опыт студентам по всему миру. Кроме того, мы помогаем талантливой молодежи узнать друг о друге, общаться, делиться знаниями и познакомиться с экспертами отрасли, чтобы лучше подготовиться к реальной работе.

Для этого мы уже более десяти лет сотрудничаем с вузами по нескольким направлениям: организуем хакатоны и конкурсы, в том числе международные, предлагаем студентам возможность стажировок, создаем совместные лаборатории и научные центры на базе университетов и оснащаем их самым современным оборудованием для отработки навыков.

## Academy Alliance

**~20 вузов**

**из разных стран присоединились к программе Academy Alliance с осени 2023 года**

В 2023 году мы расширили перечень форматов сотрудничества с вузами и студенчеством, разработав специальную партнерскую программу Kaspersky Academy Alliance, которую запустили в сентябре. Она позволит использовать в образовательном процессе наши технологии и опыт в сфере кибербезопасности. Мы считаем, что это поможет усилить существующие программы и поставлять отрасли специалистов, максимально подготовленных к реальной работе. Участникам программы открыт доступ к онлайн-курсам и мировой экспертизе, проводятся лекции и тренинги, а также предоставляется доступ к продуктам «Лаборатории Касперского».

В программе предусмотрены два типа участия для вузов:

- Associate Membership — для вузов, выпускающих ежегодно от 400 бакалавров и 50 магистров по таким профилям, как информатика, прикладная информатика и компьютерные науки.
- Advanced Membership — для вузов, в дополнение к вышеперечисленному также выпускающих не менее 50 студентов по профилю «информационная безопасность».

Программой Kaspersky Academy Alliance заинтересовались многие учебные заведения, причем их география довольно широка. В настоящее время мы сотрудничаем примерно с 20 вузами и находимся в процессе подписания договоров с целым рядом образовательных учреждений. Среди них не только крупнейшие российские, но и, например, вузы Казахстана, Узбекистана, Перу, Индии, Испании — фактически это уже межконтинентальное партнерство. Мы ожидаем, что со временем к числу желающих участвовать в программе присоединятся ряд европейских вузов, учебные заведения из африканских стран, Азии и Латинской Америки.

В долгосрочной перспективе «Лаборатория Касперского» планирует перевести на рельсы Kaspersky Academy Alliance сотрудничество со всеми вузами, с которыми ранее она взаимодействовала на уровне меморандумов. Kaspersky Academy Alliance — это логическое продолжение привычного взаимодействия, это партнерство, которое предусматривает более системную и осознанную работу как со стороны вузов, так и со стороны Компании. В наших планах на будущее — дальнейшее расширение регионального сотрудничества в рамках Kaspersky Academy Alliance.

# Сотрудничество с вузами

Сотрудничество с вузами — это важный элемент стратегии «Лаборатории Касперского» в области развития человеческого капитала и научно-технического потенциала Компании. Мы работаем с вузами по всему миру и в России, в том числе с Московским государственным университетом (МГУ) им. М. В. Ломоносова, Национальным исследовательским университетом «Высшая школа экономики» (НИУ ВШЭ), Московским государственным техническим университетом (МГТУ) им. Н. Э. Баумана, Санкт-Петербургским политехническим университетом Петра Великого (СПбПУ), Дальневосточным федеральным университетом (ДВФУ), Казанским (Приволжским) федеральным университетом (КФУ), Иннополисом, Новосибирским государственным техническим университетом (НГТУ) и многими другими.

## Московский авиационный институт

Одно из направлений нашей работы с Московским авиационным институтом (МАИ) — кафедра и лаборатория кибериммунных решений, где студенты учатся разрабатывать решения на базе KasperskyOS. В июле 2023 года состоялся первый выпуск — шестеро учащихся бакалавриата МАИ участвовали в работе лаборатории кибериммунных решений и защитили дипломные работы по разработке решений на базе нашей операционной системы.

**Курсы, созданные при нашем участии в МАИ**

- Архитектура информационных систем
- Программирование для UNIX[1]
- Информационная безопасность
- Программная инженерия

**200+** университетов

**42** страны

**150** студентов

прошли обучение разработке на базе KasperskyOS с момента открытия лаборатории

Подробнее о кибериммунитете и KasperskyOS — в разделе «Киберустойчивость»

### Роботы-тягачи и их кибериммунитет

Мы следим за тенденциями в коммерции, в частности за тем, как растет популярность автоматизированных логистических систем. Повышение киберустойчивости — одна из ключевых задач в их разработке. В ноябре 2022 года совместно с МАИ мы провели хакатон по созданию системы управления логистическими роботами на базе Alphabot/RaspberryPi под управлением операционной системы «Лаборатории Касперского» KasperskyOS. Система должна быть неуязвима под натиском хакерских атак и успешно доставить груз, следуя заданному маршруту.

[1] Семейство операционных систем 1970-х годов.

## Санкт-Петербургский политехнический университет Петра Великого (СПбПУ)

В 2023 году «Лаборатория Касперского» договорилась о сотрудничестве с СПбПУ для усиления подготовки кадров. Совместно с представителями вуза мы планируем взаимодействовать во всех ключевых форматах — от встреч со студентами и выпускниками до реализации НИОКР в области кибербезопасности.

## Пермский университет

Еще один регион, где мы наращиваем кадровый потенциал, — Пермский край. В 2023 году мы заключили соглашение о совместной разработке и реализации научных и образовательных инициатив с Институтом компьютерных наук и технологий Пермского университета. Наша цель — добиться того, чтобы студенты выпускались из университета квалифицированными специалистами и помогали нам развивать отрасль. Наши усилия также будут направлены на повышение квалификации преподавательского состава.

## Вузы Оренбурга

Осенью 2022 года мы подписали соглашение с Министерством цифрового развития и связи Оренбургской области о передаче своих курсов по информационной безопасности и KasperskyOS в учебные заведения Оренбурга. Так мы поможем подготовить грамотных специалистов для безопасности и цифровизации региона, испытывающего дефицит экспертов в этой области, и повысить квалификацию уже действующих сотрудников. Мы создадим инфраструктуру удаленных рабочих мест в вузах на основе нашего решения Kaspersky Secure Remote Workspace. Одним из первых учебных заведений, где вместо обычных компьютеров будут установлены «тонкие клиенты»[1], станет Оренбургский колледж экономики и информатики. После этого мы оснастим аналогичными устройствами остальные классы колледжа, а также другие учебные заведения.

Кроме того, мы приняли решение открыть кафедру кибербезопасности в Оренбургском государственном университете (ОГУ) и повысить качество подготовки специалистов. Для этого учебные программы подготовки в области кибербезопасности будут обновлены, а студенты научатся программировать на базе KasperskyOS. В частности, в университете появится модуль «Кибериммунный подход к разработке» для бакалавров и магистров.

В 2023 году совместно с ОГУ мы открыли научно-образовательный центр «Информационная безопасность в АСУ ТП» (НОЦ), где обучающиеся смогут получить практические навыки программирования и работы с системами сбора данных и оперативного контроля (SCADA).

## РГУ нефти и газа (НИУ) им. И. М. Губкина

Защита предприятий топливно-энергетического комплекса (ТЭК) — один из национальных приоритетов. Мы вносим в него свой вклад, повышая уровень подготовки кадров в этом секторе. В конце 2022 года мы заключили трехстороннее соглашение о сотрудничестве с Министерством энергетики Российской Федерации (Минэнерго России) и Российским государственным университетом нефти и газа (национальным исследовательским университетом) им. И. М. Губкина. В числе ключевых направлений сотрудничества — формирование кадрового резерва и повышение квалификации специалистов отрасли.

Мы оборудовали в университете учебный класс комплексной безопасности критической информационной инфраструктуры ТЭК, оснастив его новейшими программно-аппаратными комплексами. Эта лаборатория станет ключевым звеном в работе над импортозамещением и обеспечением кибербезопасности. Ее будут использовать для обучения студентов защите систем промышленной автоматизации и переподготовки представителей нефтегазовой отрасли.

[1] Компактные устройства, защищенные от киберугроз за счет установленной на них безопасной по умолчанию (Secure-by-Design) операционной системы Kaspersky Thin Client.

# Secur'IT Cup: распространяем знания о кибербезопасности по всему миру

Мы считаем правильным давать шанс на успешное продвижение идей и развитие карьеры как можно большему числу молодых людей в разных странах мира. Среди них не только студенты, но и недавние выпускники вузов.

С 2018 года мы предлагаем талантливой молодежи проявить себя в разработке инновационных идей для решения актуальных проблем информационной безопасности, участвуя в нашем международном конкурсе Secur'IT Cup. По правилам конкурса мы предлагаем участникам — индивидуально или в команде — разработать проекты в определенных областях и побороться за денежные призы и возможность пройти наши онлайн-курсы Kaspersky Expert Training. В жюри входят эксперты Глобального центра исследований и анализа угроз «Лаборатории Касперского» (GReAT), а также представители зарубежных университетов и победители конкурсов прошлых лет.

В 2023 году мы уделили внимание развитию игровой вселенной, обеспечению безопасности данных и финансов, а также защите старшего поколения и домашних животных. Важное нововведение конкурса в этом году — возможность вживую пообщаться с экспертами «Лаборатории Касперского» в ходе менторских сессий, чтобы получить грамотный совет и довести проект до совершенства. В финал Secur'IT Cup 2023 вышли разработчики из Кении, Маврикия, Нигерии, России, Саудовской Аравии и Сингапура.

**Более 6 тысяч**
человек участвовали в конкурсе с 2018 года

**$10 тысяч** –
главный приз Secur'IT Cup 2023

# KIPS-чемпионат: тренируем навыки в информационной безопасности

Осенью 2022 года «Лаборатория Касперского провела международный чемпионат среди студентов Kaspersky Interactive Protection Simulation (KIPS). Это игровой тренинг, который дает реалистичное представление о том, что происходит во время кибератаки, и позволяет участникам получить игровой и учебный опыт. Благодаря KIPS-чемпионату молодые специалисты учатся эффективно реагировать на киберинциденты в таких сферах, как банковское дело и государственное управление.

На конкурс зарегистрировались 77 команд, представляющих 17 стран. По итогам финального мероприятия, прошедшего онлайн 1 декабря 2022 года, победителем была признана команда SPAM из Национального исследовательского ядерного университета «МИФИ». Последний раунд соревнований был посвящен технической атрибуции с использованием специально разработанной вымышленной среды, имитирующей кибератаки на ООН. Игрокам пришлось собирать кусочки головоломки с техническими доказательствами и принимать решения с помощью карточек действий, чтобы выполнить наиболее точный технический анализ атаки.


**77 команд из 17 стран**
зарегистрировались на KIPS-чемпионат в 2022 году

# Стажировки

Мы уверены, что востребованность выпускников зависит от того, имеют ли они практический опыт работы в отрасли.

В «Лаборатории Касперского» студенты могут пройти оплачиваемую стажировку SafeBoard, чтобы поработать бок о бок с экспертами индустрии. SafeBoard — это целое сообщество, где стажеру гарантированы поддержка и помощь, а также шанс получить работу в компании — лидере отрасли сразу после окончания вуза. Стажировки проводятся дважды в год — осенью и весной. Чтобы пройти стажировку, студентам, проживающим в Москве и Московской области, нужно подать заявку и пройти трехэтапный отбор. Он состоит из тестирования технических знаний, практического задания или видеоинтервью.

Как социально ответственная компания, мы следим за уровнем зарплаты стажеров программы SafeBoard. В 2023 году мы повысили ее на 15%.

Мы заботимся о том, чтобы стажировка не мешала образовательному процессу: студенты могут самостоятельно определить количество рабочих часов в неделю (от 20 до 35 часов во время учебы и до 40 часов — летом) и формат работы (полностью офисный или гибридный).

В 2023 году мы обновили процедуру онбординга[1] и теперь обучаем стажеров техническим и бизнес-навыкам. Кроме того, у них есть доступ к курсам и митапам[2], а также нашей онлайн-библиотеке. В ходе осеннего отбора к нашей команде присоединились 40 стажеров.

Важная особенность нашей программы стажировки — в ней могут участвовать студенты любых направлений обучения, даже не технических. Главное условие — интерес к миру IT и желание в нем разобраться.

**>15**

направлений стажировки, включая разработку на C/C++, C#, Python, Go, JavaScript[3], а также тестирование, анализ угроз и DevOps[4]

**13,5 тысячи**

заявок на стажировку SafeBoard получено в отчетном периоде

**>50%**

стажеров перешли в штат Компании за 8 лет работы программы SafeBoard

# Kaspersky Academy Expert Community

Обучая школьников и студентов, «Лаборатория Касперского» не забывает и сообщество преподавателей. Kaspersky Academy Expert Community — это серия специализированных мероприятий, которые мы регулярно проводим для преподавателей, исследователей, деканов и заведующих кафедрами в области информационной безопасности и смежных областей знания. А еще это сообщество единомышленников.

Мероприятия проводятся в нескольких форматах, в том числе в виде офлайн-собраний нашего комьюнити. Это и регулярные встречи сообщества, которые проходят каждые два месяца на базе нашего офиса, где специалисты Компании делятся своим опытом по актуальным темам. А еще это Training Lab — полноценные бесплатные двух- или трехдневные тренинги для преподавательского состава вузов с участием наших экспертов. Темы тренингов самые разнообразные — начиная с общих направлений информационной безопасности и заканчивая непосредственно продуктами «Лаборатории Касперского».

География Kaspersky Academy Expert Community очень широкая, она охватывает практически всю Россию и страны СНГ. К нам приезжают коллеги из Челябинска, Владивостока, Алма-Аты, Минска и других городов. В 2023 году мы проводили мероприятия для преподавателей в Дубае, Каире, Бомбее и Дели, а в 2024 году намерены повторить их в других городах и странах Ближневосточного и Тихоокеанского регионов. Мы всегда рады видеть в Kaspersky Academy Expert Community новых людей — всех, кто преподает информационную безопасность в вузах, заинтересован в развитии своих знаний и общении с единомышленниками.

[1] Процедура знакомства нового сотрудника/стажера с компанией и его адаптации в команде.
[2] Встреча представителей индустрии для обсуждения общих тем и вопросов.
[3] Языки программирования.
[4] Development and operations — методология взаимодействия разработчиков и интеграции процессов при создании продукта.

# Обучение IT-специалистов

Основные драйверы появления новых профессий и компетенций — это развитие технологий и законодательства. Поэтому постоянное обучение становится одним из главных требований для специалистов по кибербезопасности. Чтобы помочь им прокачивать свои навыки, мы разработали комплекс образовательных тренингов на собственном портале онлайн-обучения Kaspersky Expert Training.

Авторы курсов — ведущие специалисты Компании — знакомы более чем с 400 тысячами образцов вредоносного ПО и умеют им противостоять. Мы дополнили теоретическую базу кейсами на основе реальных угроз. Это не фундаментальное образование, а практическое обучение, позволяющее специалистам освоить техники и инструменты, которые смогут сразу же использовать в работе.

Круг пользователей курсов широк и охватывает всех, кто связан с нашей отраслью, — от специалистов по кибербезопасности и SOC-команд до исследовательских институтов, центров реагирования на инциденты и правительственных организаций.

**Навыки, которые можно прокачать в Kaspersky Expert Training**

- Обратная разработка
- Поиск и обнаружение угроз
- Реагирование на инциденты
- Анализ защищенности продукта

Для обучения доступны как базовые курсы, рассчитанные на любой уровень подготовки, так и продвинутые — для экспертов и профессионалов с опытом.

В числе инструментов, использованию которых мы обучаем для обеспечения защиты, — Ghidra, Yara, Suricata, Frida.

Портфолио онлайн-тренингов для экспертов Kaspersky Expert Training включает 11 курсов. В 2023 году мы пополнили его тремя онлайн-курсами:

- **продвинутый реверс-инжиниринг вредоносного ПО с помощью Ghidra**, посвященный процессу анализа вредоносных программ с использованием фреймворка Ghidra на основе реального опыта его авторов — экспертов команды расследования компьютерных инцидентов и команды Глобального центра исследования и анализа угроз (GReAT);
- **Suricata для реагирования на инциденты и поиска угроз**, направленный на обучение использованию Suricata для работы с разными потоками данных для обнаружения и блокировки даже самых сложных угроз;
- **онлайн-тренинг по кибербезопасности для руководителей**, созданный командой Kaspersky Academy для топ-менеджеров. Он объясняет сложные термины простым языком и призван помочь разобраться в основных концепциях информационной безопасности, а также научиться управлять компанией в условиях киберугроз.

**2 000+ пользователей**
**из более чем 50 стран — аудитория тренингов для экспертов**

**~10 часов**
**в среднем изучали каждую программу студенты Kaspersky Expert Training**

**20 часов**
**в среднем провели студенты Kaspersky Expert Training в нашей виртуальной лаборатории для отработки практических навыков**

**Самые увлекательные темы 2023 года — передовые методы анализа вредоносных программ с помощью Yara. На них студенты потратили суммарно 4 тысячи минут.**

**Самые «практические» курсы — анализ вредоносных программ и реверс-инжиниринг.**

В 2025 году мы планируем дополнить портфолио тренингами, посвященными цифровой криминалистике и безопасной разработке. Компания также занимается переводом существующих тренингов на русский язык и уже выбрала для них отдельную обучающую платформу. В 2024 году планируется начать продажи русскоязычных тренингов в России.

В 2023 году мы продолжили проводить бесплатные тренинги для сотрудников Интерпола из России, стран Европы, Латинской Америки, Азии, Африки, Ближнего Востока и т. д.

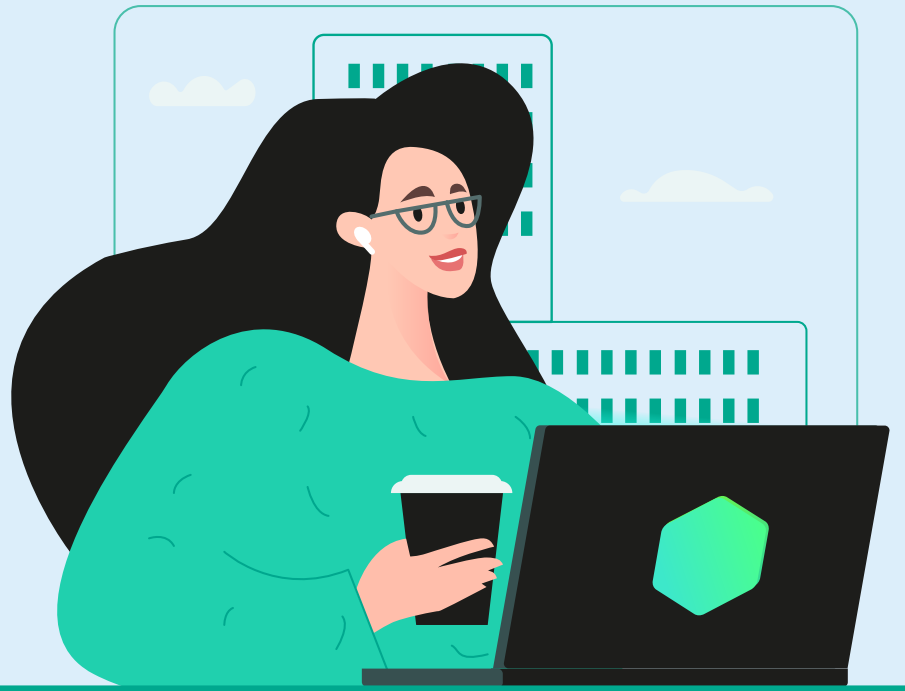
71 сотрудник Интерпола прошел бесплатные тренинги Kaspersky Expert Training в 2023 году.

Кроме того, мы предоставили десяти стажерам — участникам программы Suricata Outreach бесплатный доступ к курсу по использованию Suricata для реагирования на инциденты и поиска угроз. Список участников инициативы определило Suricata-комьюнити. Также наши тренинги использовались в качестве призов для победителей международного студенческого конкурса Secur'IT Cup.

**158 сотрудников**
**«Лаборатории Касперского» бесплатно прошли курсы Kaspersky Expert Training**

# Женщины в IT: сила равенства

Долгое время IT-сфера считалась исключительно мужским полем деятельности, но сегодня женщины успешно применяют в ней свои способности, преодолевая стереотипы и препятствия. Привлечение женщин в IT-индустрию и их поддержка — часть нашей корпоративной культуры.



## Гендерный дисбаланс в IT-индустрии: причины и вызовы

В IT-индустрии наблюдается значительный гендерный дисбаланс, при котором специалистов-мужчин значительно больше, чем женщин. Этот феномен вызван рядом факторов — от культурных предубеждений до социальных стереотипов. Изначально компьютерные технологии ассоциировались с мужскими интересами и хобби, что создало своеобразную культуру, исключающую женщин. Со временем этот стереотип укрепился и стал частью профессиональной идентичности IT-сферы. Кроме того, дисбаланс усиливается в связи с проблемой неравенства, с которой сталкиваются женщины во всех отраслях, включая IT. Не все компании обеспечивают одинаковые условия для своих сотрудников, и это препятствует привлечению и удержанию талантливых женщин. По данным Министерства труда и социальной защиты Российской Федерации, разница между зарплатами мужчин и женщин в России на начало 2023 года составляла 28% не в пользу последних, хотя этот разрыв с каждым годом сокращается. И наконец, карьерный рост женщин продвигается медленнее, чем у коллег мужского пола. Одна из причин этого — отпуск по уходу за ребенком, который обычно предпочитают брать матери, хотя в «Лаборатории Касперского» такой отпуск по желанию предоставляется и отцам.

Тем не менее количество женщин в IT-отрасли постепенно растет. Так, на начало 2023 года доля женщин, работающих в сфере высоких технологий во всем мире, составляла 25%, увеличившись на 6,9 п. п. за последние четыре года. При этом в «Лаборатории Касперского»[1] женщины составляют 25%, среди которых 16% — руководители направлений и крупные менеджеры, а 34% — технические специалисты.

**25%**

**доля IT-специалистов-женщин в мире в 2022 году**

**25%**

**доля сотрудников-женщин в «Лаборатории Касперского» в 2023 году**

[1] По данным на 31 декабря 2023 года.

# Наш подход к поддержке женщин

В последние годы женщины продолжают активно развиваться в Компании — они занимаются разработкой ПО, управляют проектами, трудятся в других областях IT. Смешанные команды, в которых присутствуют как мужчины, так и женщины, демонстрируют хорошие результаты благодаря разнообразию опыта и точек зрения.

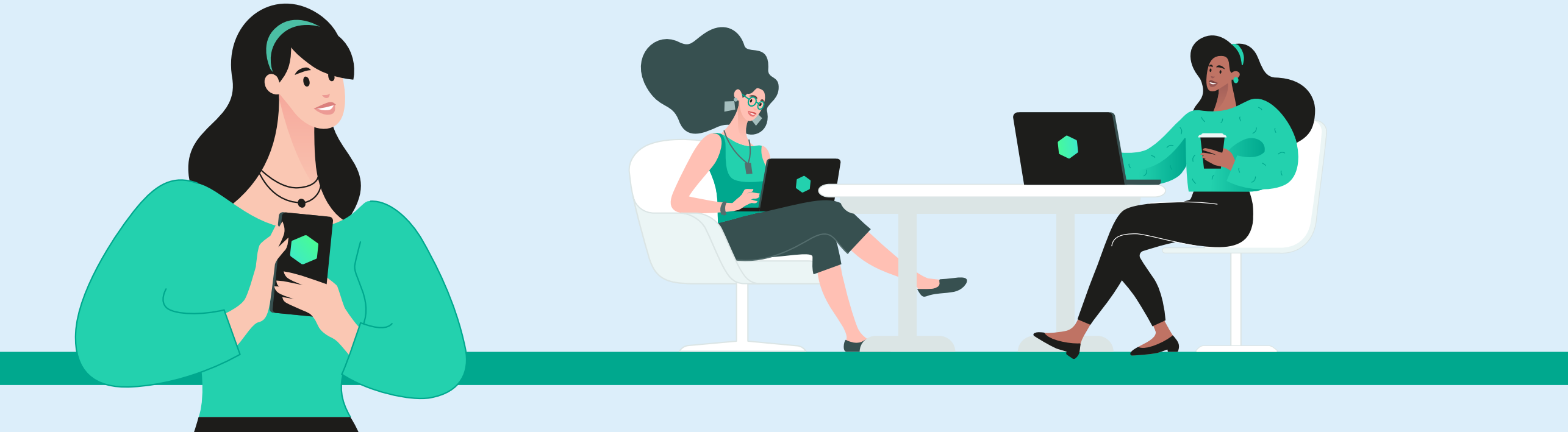
Решать проблему гендерного дисбаланса «Лаборатория Касперского» начинает еще на уровне школ и вузов. Мы заботимся о том, чтобы с ранних лет опровергать гендерные стереотипы и делать IT-образование доступным и открытым для всех. Мы сотрудничаем со школами и университетами, чтобы предоставить всем школьникам и студентам вне зависимости от их пола информацию об обучении в области IT и возможность обнаружить свой потенциал в технологической сфере.

Мы также стремимся обеспечить равную оплату труда всем сотрудникам Компании. В нашем подходе к оплате труда учитываются должность и квалификация каждого сотрудника независимо от пола. Для этого мы применяем оценку рыночного уровня компенсации по каждой должности. По итогам оценки было принято решение в 2022 году увеличить заработную плату сотрудников «Лаборатории Касперского» в среднем на 20% в России. Компания смогла инвестировать в зарплаты и бонусы в два раза больше средств по сравнению с 2021 годом. А в 2023 году повышение вознаграждения сотрудникам «Лаборатории Касперского» в России составило порядка 19%.

Кроме того, мы предоставляем нашим сотрудницам дополнительную поддержку и выплаты во время декретного отпуска, возможности для образования в их сфере деятельности и помогаем продвигаться по карьерной лестнице с помощью индивидуальных планов развития.

Помимо работы внутри Компании, мы реализуем различные проекты вовне, чтобы привлечь больше женщин в IT-индустрию. В частности, мы сотрудничаем с учебными заведениями по всему миру, организуем образовательные мероприятия, мастер-классы и программы стажировок. В социальных сетях мы создали комьюнити Women in CyberSecurity — пространство, где каждая женщина чувствует свою важность и поддержку на пути к успеху в сфере кибербезопасности. В этом сообществе уже более 29 тысяч участниц.

Чтобы вдохновить как можно больше девушек на карьеру в области IT и кибербезопасности, «Лаборатория Касперского» запустила еще один собственный онлайн-проект — сайт Empower Women. На этом сайте сотрудницы нашей компании делятся личным опытом в кибербезопасности и IT: они рассказывают, как получили образование и построили карьеру, участвуют в подкастах и дают полезные советы.



# Увеличиваем число женщин в разработке

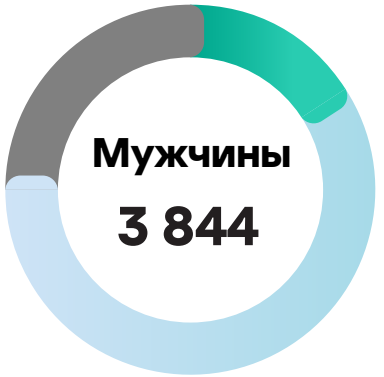
Вовлечение женщин в IT-индустрию и их поддержка — это неотъемлемая часть корпоративной культуры «Лаборатории Касперского», которая формируется на уровне Совета директоров и высшего менеджмента. Мы стремимся создать во всех подразделениях атмосферу взаимопонимания, в которой каждая женщина может раскрыть свой потенциал и стать успешной в IT-сфере. При этом женщины, которые уже достигли успеха на различных уровнях, активно участвуют в программах поддержки, общаются с коллегами и подчиненными, делятся опытом и своим примером вдохновляют начинающих IT-специалистов.

«Лаборатория Касперского» стремится быть максимально честной и открытой, чтобы не допустить проявлений гендерной дискриминации. Когда мы подбираем новых сотрудников для нашей команды, нас волнуют только их способности и навыки независимо от того, женщина это или мужчина. Главное — наличие необходимых компетенций и то, какой вклад они могут внести в нашу Компанию.

TC-SI-330-a.3

## Общая численность сотрудников в разбивке по полу и категориям в контексте гендерного баланса, человек[1]


## Сотрудники Компании в разбивке по гендеру и категориям




**16%** Руководители[2]
**59%** Технические специалисты
**25%** Прочие специалисты


**16%** Руководители[2]
**34%** Технические специалисты
**50%** Прочие специалисты

## Соотношение базовой заработной платы (оклада) и вознаграждения[3] женщин и мужчин[4], %


[1] Данные указаны на 31 декабря 2023 года.
[2] Менеджеры, у которых в подчинении от одного человека.
[3] Оклад и выплаты в зависимости от категории, выслуги лет и др.
[4] Данные указаны на 31 декабря 2023 года.

# Обеспечиваем социальную поддержку женщин и родительства

Во всех странах нашего присутствия мы стараемся вдохновлять сотрудниц на их карьерном пути и поддерживать в самые важные моменты жизни. Вот, например, что мы предлагаем нашим сотрудницам в России, у которых в семье просходит пополнение:

- отпуск по уходу за ребенком, который может взять любой из родителей, независимо от того, родной это ребенок, усыновленный или находящийся под опекой;
- 100%-ную доплату к государственному пособию по беременности и родам, чтобы общая сумма выплат достигала полного размера оклада, — ее получают сотрудницы, имеющие стаж работы в Компании не менее одного года;
- программу ведения беременности и родов по ДМС.

# Объединяем женщин в онлайн-сообщества по кибербезопасности

Компания реализует два крупных онлайн-проекта для женщин в IT. Мы стремимся поддерживать женщин в IT-индустрии, помогая им преодолевать барьеры и достигать своих целей. Наша задача — делиться информацией о возможностях профессионального роста в этой отрасли и вдохновлять наших участниц рассказами об успешных женщинах-профессионалах, чтобы укрепить новые ролевые модели.

В 2021 году мы запустили проект Empower Women, посвященный деятельности женщин в сфере кибербезопасности. Проект включает исследования о женщинах в IT-индустрии по различным регионам, интересные новости, а также вдохновляющий подкаст Women in IT, где сотрудницы из «Лаборатории Касперского» делятся профессиональным и личным опытом. За отчетный период на сайте появилось 11 новых рассказов о наших коллегах из разных регионов мира, где они делятся историями своего профессионального и личного развития. Мы стремимся показать широкий спектр возможностей построения карьеры в IT-индустрии — многие наши героини не имеют технического образования, но смогли добиться высоких результатов в своих профессиональных областях внутри IT-компании, будь то продажи, образовательные проекты или коммуникации.

Другой проект «Лаборатории Касперского», затрагивающий тему женского лидерства в IT, — подкаст Fast Forward. В нем принимают участие гости со всего мира, работающие на переднем крае наших новейших технологий. Первый сезон Fast Forward, в который вошли эпизоды, посвященные супермаркетам будущего и новой космической гонке, в 2022 году был удостоен престижной награды Webby Honoree за лучший фирменный подкаст и серебряной награды за фирменный подкаст от Ассоциации контент-маркетинга. Во втором сезоне Fast Forward рассказывает о метавселенной, виртуальной моде, технологиях в семейной жизни, цифровом здравоохранении и так называемых «дополненных людях». В этом сезоне много внимания уделяется тому, как женщины меняют свое восприятие сферы технологий и начинают лидировать в ней. В двух эпизодах речь идет о женщинах и девушках в гейминге, а также о карьерных возможностях женщин в STEM[1].

Также успешно развивается наше сообщество для женщин в IT Women in CyberSecurity, созданное в социальных сетях пять лет назад по инициативе одной из наших сотрудниц. Сегодня это активное и динамично развивающееся комьюнити, объединяющее профессионалов по кибербезопасности и других сфер IT-индустрии. Здесь женщины каждый день обсуждают актуальные вопросы, делятся опытом и обмениваются советами по карьерному росту, обучению, выбору специализации в сфере кибербезопасности. В настоящее время в Women in CyberSecurity насчитывает уже более 30 тысяч участниц, что делает его одним из самых крупных и востребованных онлайн-сообществ данной тематики. Каждый месяц в сообществе публикуется больше 20 постов.

**29 тысяч**

**участниц состоят в сообществе Women in CyberSecurity**

В ноябре 2023 года «Лаборатория Касперского» выступила спонсором ежегодного конгресса Female in IT (FIT) IT-академии Vogel в Германии. Этот конгресс объединяет женщин в сфере IT, чтобы они могли поддерживать друг друга в бизнесе, обмениваться опытом и продвигать молодые таланты. Девизом 2023 года был призыв «Женщины, готовьтесь к бизнесу нового поколения!». Конгресс впечатлил участниц первоклассной программой интересных докладов, панельных дискуссий и предоставил им возможности для налаживания полезных связей.

## Наши планы на 2024 год

Мы продолжим работать над текущими проектами и разрабатывать новые программы в области привлечения женщин в IT-отрасль, участвовать в профильных конференциях и форумах, публиковать истории успеха наших коллег и рассказывать о возможностях профессионального развития, которые открываются для женщин в индустрии кибербезопасности.

[1] STEM (Science, technology, engineering, and mathematics) — это широкий термин, который используется для обозначения технических дисциплин (наука, технологии, инжиниринг и математика).

## Как наши сотрудницы достигают вершин в IT и помогают другим женщинам

**Представляем Джини Суджин Ган, которая получила награду «Выдающейся женщине за лидерство в сфере ИКТ».**

Джини отвечает за развитие доверительных отношений «Лаборатории Касперского» с представителями государственных органов в Азиатско-Тихоокеанском регионе, на Ближнем Востоке, в Турции и Африке. Она часто выступает на международных конференциях и является лидером мнений по темам, связанным с государственной политикой в области кибербезопасности, а также с пересечением технологий и политики.

Джини — настоящий амбассадор женского лидерства в мире информационных технологий. Она отдает много сил, чтобы поддержать других женщин в IT-сфере. Джини помогает им получать знания, наставляет и консультирует. Она создает специальные сообщества, где женщины могут делиться опытом, знаниями и поддержкой. Такой подход помогает им расти и развиваться, преодолевая стереотипы и препятствия на пути к успеху.

В 2023 году Джини получила несколько наград и знаков признания за свою деятельность, в числе которых следующие.

- Excellent Woman ICT Leadership award: «Выдающейся женщине за лидерство в сфере ИКТ» — эту награду Джини получила в Дели в рамках Международного дня «Девушки в ИКТ» 2023 года. Он отмечается, чтобы привлечь внимание к необходимости увеличения числа девушек и женщин в секторе информационно-коммуникационных технологий. Мероприятие было организовано совместно Международным союзом электросвязи ООН (ITU), базирующимся в Женеве, и Индийской ассоциацией производителей телекоммуникационного оборудования Индии (TEMA). Джини стала единственным лауреатом в секторе кибербезопасности.

«Это признание является не только моим личным достижением, но и достижением «Лаборатории Касперского», которая поддерживает меня в персональном развитии, а также стремится создать для женщин более разнообразную и безопасную рабочую среду в области кибербезопасности»,

— отметила Джини, комментируя полученную награду.

- International Women Empowerment Forum (IWEF, Международный форум по расширению прав и возможностей женщин)

Джини была назначена заместителем председателя IWEF. Эта организация делает упор на многоплановое развитие женщин: социальное, экономическое, финансовое и политическое расширение их прав и возможностей. Джини — единственная представительница неиндийского происхождения, вошедшая в состав совета директоров IWEF.

- Singapore's The Cybersecurity Awards

Джини стала финалистом Сингапурской премии в области кибербезопасности (профессиональная категория). Она получила эту награду, организованную Ассоциацией специалистов по информационной безопасности (AiSP) при поддержке Агентства кибербезопасности Сингапура в знак признания выдающегося вклада отдельных лиц и организаций в местную и региональные экосистемы кибербезопасности.

- Top 25 Cybersecurity Star of the Year 2023

Вошла в 25 лучших звезд кибербезопасности 2023 года — это награда, присуждаемая DIGITALCONFEX за вклад в интеллектуальное лидерство по темам, находящимся на стыке государственной политики, технологий и права.

- Top 30 Women in Security ASEAN Region Awards 2023

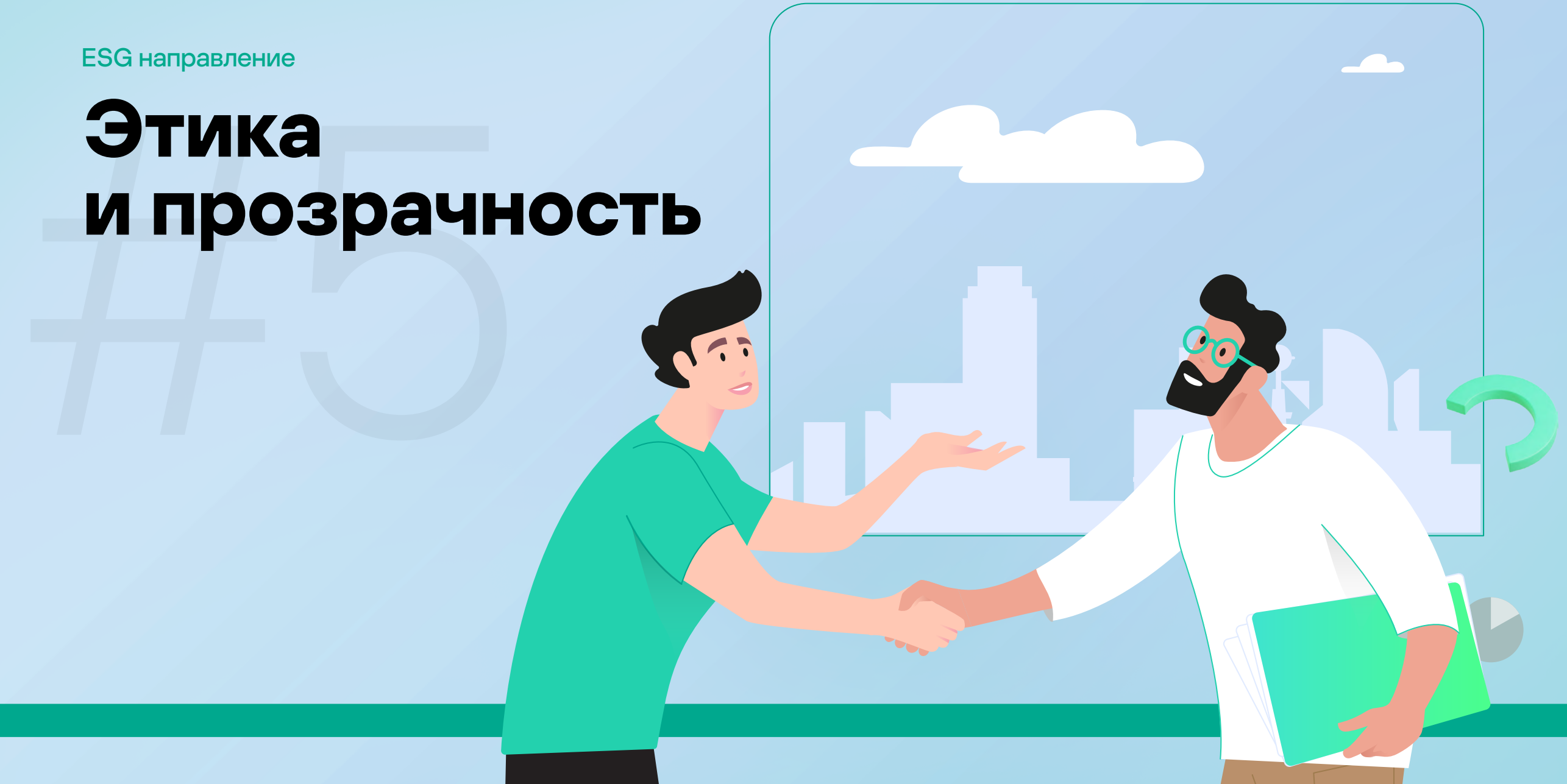
Получила премию «30 лучших женщин в сфере безопасности региона АСЕАН — 2023», которая организована Ассоциацией государств Юго-Восточной Азии (АСЕАН) и является частью глобальной кампании Альянса «Женщины в сфере безопасности и устойчивости» (WISECRA).

### Что в результате?

Активно продвигаясь в IT и поддерживая других женщин на этом пути, Джини стала для них вдохновляющим примером, показав, что успех в технологической сфере доступен всем людям независимо от пола. Ее история показывает, что упорный труд, образование и поддержка могут привести женщин к заметным результатам даже в тех отраслях, где традиционно преобладают мужчины.

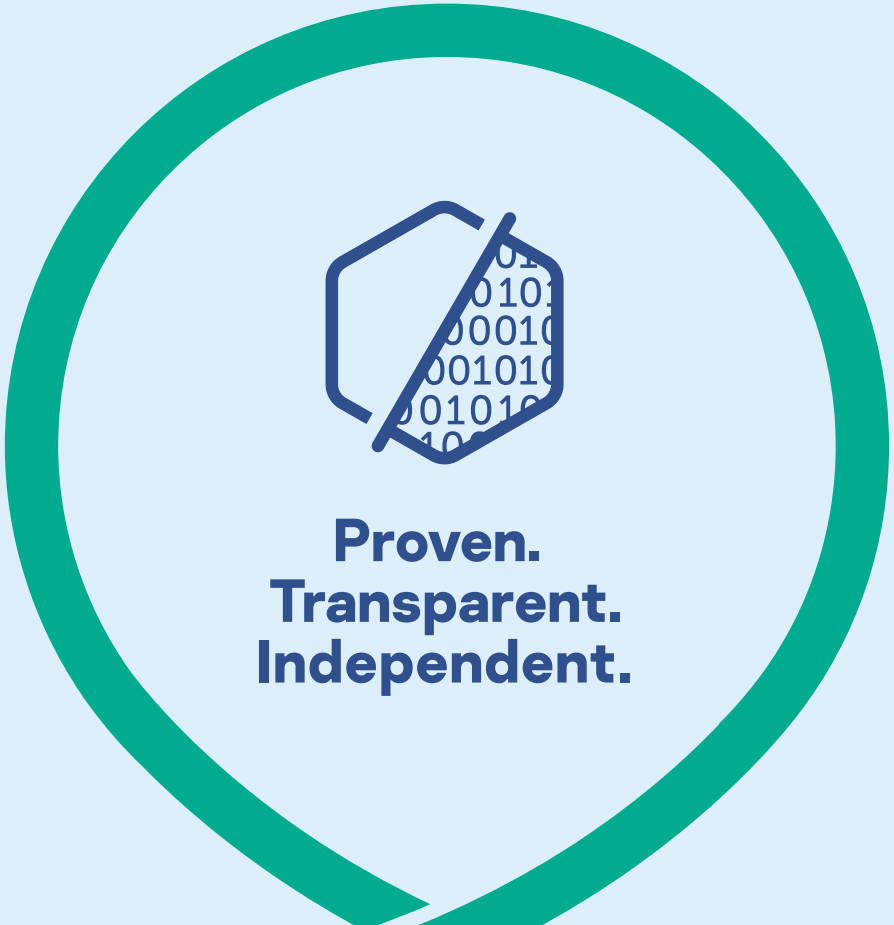
ESG направление

# Этика и прозрачность



# Global Transparency Initiative

Наша цель — предоставить инструменты и условия для валидации целостности и надежности продуктов нашим корпоративным клиентам, партнерам и регуляторам.




## Что такое Global Transparency Initiative

Global Transparency Initiative (GTI, Глобальная инициатива по информационной открытости) — комплекс мер, с помощью которых мы обеспечиваем прозрачность и надежность своих продуктов, а также процессов разработки и бизнес-процессов. Благодаря GTI корпоративные клиенты, партнеры и регуляторы могут посетить наши специализированные центры, чтобы ознакомиться с исходным кодом продуктов Компании, получить разъяснения о наших принципах работы с данными. А сотрудники, получая обратную связь от экспертного сообщества, понимают, что именно нам нужно совершенствовать в вопросах открытости, зрелости процессов и как обеспечивать при этом безопасность продуктов.

# Как возникла и развивалась GTI

Изначально «Лаборатория Касперского» запустила глобальную инициативу по информационной открытости (GTI) в ответ на запросы регулирующих органов, которые интересовались деталями работы наших продуктов: процессом обработки данных, местом их хранения и другими аспектами. С 2017 года мы работаем над пакетом инициатив, направленных на укрепление доверия со стороны наших клиентов и партнеров. Этот пакет включает в себя создание центров прозрачности, проведение независимых аудитов по безопасности и надежности процессов разработки, а также инициативу по переносу части нашей инфраструктуры для обработки вредоносных и подозрительных файлов в дата-центры в Швейцарии.

В дальнейшем в рамках GTI был принят еще ряд мер:

- внедрен независимый анализ исходного кода, программных обновлений и правил обнаружения угроз;
- внедрена независимая оценка процесса безопасной разработки и стратегии по минимизации рисков в цепочке поставщиков и в программном обеспечении;
- открыты центры прозрачности (Transparency Centers) по всему миру;
- усовершенствована программа bug bounty[1] за обнаружение наиболее серьезных уязвимостей в программном обеспечении «Лаборатории Касперского»;
- проведены обучающие семинары по безопасности цепочек поставок и методикам оценки надежности продуктов ИКТ[2];
- создана дополнительная инфраструктура в Швейцарии для хранения и обработки вредоносных и подозрительных файлов, поступающих от пользователей в нашу облачную систему Kaspersky Security Network;
- продолжалась публикация отчетов с информацией о том, сколько запросов на получение данных поступает в Компанию от правоохранительных органов и государственных структур;
- продолжалось развитие образовательных программ, таких как Cyber Capacity Building Program, направленных на повышение квалификации специалистов в области безопасности ИКТ-продуктов.

В 2023 году «Лаборатория Касперского» отметила пятилетие Глобальной инициативы по информационной открытости. Сегодня GTI продолжает эволюционировать, адаптируясь к меняющимся условиям и требованиям рынка кибербезопасности.

## Результаты работы GTI за пять лет

**> $8,4 млн**
инвестиции в развитие GTI с 2018 года

**2 дата-центра**
в Цюрихе

**11**
центров прозрачности по всему миру

**60 ревью**
продуктов Компании в центрах прозрачности

**2**
независимых аудита SOC 2 и на соответствие ISO 27001 ежегодно

**> $81 тысячи**
выплачено за 59 репортов об ошибках в рамках bug bounty

[1] Программа поощрения поиска ошибок и уязвимостей в программном обеспечении, которую, как правило, объявляют разработчики приложений и сетевых платформ, чтобы обнаружить проблемы в безопасности своих продуктов. Обычно в рамках программы энтузиасты получают денежное вознаграждение за сообщение об ошибках, которые могут быть использованы злоумышленниками; иногда в качестве поощрения может выступать доступ к платному онлайн-сервису или признание в профессиональном сообществе.

[2] ИКТ — информационные и коммуникационные технологии.

# Как работает GTI

GRI 3-3

Global Transparency Initiative — это не просто набор мероприятий. Это стратегическое направление, целью которого является создание надежного, безопасного и прозрачного цифрового пространства для всех участников.

## Основные элементы GTI

1

### Обзор исходного кода для клиентов и регуляторов

- Одним из ключевых элементов GTI является независимая верификация кода продуктов «Лаборатории Касперского». Кроме того, заинтересованные лица могут получить информацию об исходном коде основных продуктов Компании и наших принципах работы с данными.

2

### Сотрудничество с экспертами

- Другая важная часть GTI — активное сотрудничество с независимыми экспертами и организациями. Мы приглашаем специалистов из разных стран мира для проверки наших систем и продуктов, что добавляет еще больше уверенности в их надежности.

3

### Обучение и просвещение

- Global Transparency Initiative способствует просвещению в области кибербезопасности. «Лаборатория Касперского» активно участвует в различных инициативах, направленных на повышение осведомленности пользователей и партнеров о важности безопасности в цифровом мире.

# Как мы обеспечиваем прозрачность наших продуктов и бизнес-процессов

## # Задача

### Укрепление доверия общества к продуктам и деятельности Компании

Чтобы убедить наших корпоративных клиентов, пользователей, партнеров и регуляторов рынка в безопасности и высоком качестве наших продуктов и технологий, мы постоянно совершенствуем GTI, открываем все больше данных о наших процессах, проходим аудиты и сертификации. Благодаря обратной связи от наших стейкхолдеров мы понимаем, какие аспекты требуют особого внимания в вопросах открытости, зрелости процессов и каким образом мы можем обеспечивать при этом безопасность наших продуктов.

TC-SI-220-a.4

## # Решения

### Переносим данные в защищенные дата-центры

Одним из первых шагов Глобальной инициативы по информационной открытости был запуск процесса релокации обработки и хранения файлов. Для этого в 2018 году мы создали два дата-центра в Швейцарии, в которых действуют строгие правила защиты данных. За пять лет в оборудование этих центров, куда Компания перенесла данные своих пользователей, было инвестировано $8,4 млн. Благодаря этому сегодня в Цюрихе успешно действуют два центра обработки вредоносных и подозрительных файлов, поступающих от пользователей на добровольной основе в облачную систему Kaspersky Security Network. Здесь мы обрабатываем и храним данные, связанные с киберугрозами, от пользователей из Европы, Северной и Латинской Америки, Ближнего Востока, а также ряда стран Азиатско-Тихоокеанского региона.

# Открываем новые центры прозрачности

Чтобы дать нашим корпоративным клиентам, партнерам и государственным регуляторам, отвечающим за кибербезопасность, возможность проверить надежность решений Компании, изучив их исходный код, а также узнать больше о наших внутренних процессах, мы создаем центры прозрачности.

Первый такой центр был открыт в Цюрихе в ноябре 2018 года. За пять лет действия GTI Компания создала 11 таких центров — в Бразилии, Италии, Японии, Малайзии, Нидерландах, Руанде, Саудовской Аравии, Сингапуре, Испании, Швейцарии и США. Четыре из них были открыты с июля 2022 года до конца 2023 года.

Мы постоянно расширяем спектр возможностей, предлагаемых в центрах прозрачности. Ранее для ознакомления предлагался только исходный код флагманских продуктов для домашних пользователей и бизнеса. В июле 2023 года стал доступным обзор исходного кода всех решений on-premise для корпоративных клиентов. Вскоре в центрах можно будет увидеть результаты самосертификации продуктов Компании, включая такие элементы, как проектная документация и модели угроз. Это соответствует рекомендациям проекта европейского Закона о киберустойчивости.

**11 центров прозрачности** работают по всему миру

## Итоги 2022–2023 годов

**4 новых центра прозрачности** открыты — в Руанде, Саудовской Аравии, Италии и Нидерландах

Центр прозрачности в Саудовской Аравии стал **первым на Ближнем Востоке**, а центр в Руанде — **первым в Африке**

**34 визита** в центры проведено по всему миру

Расширен перечень продуктов, доступных для аудита в центрах

| США | Бразилия | Испания | Нидерланды | Швейцария | Италия | Саудовская Аравия | Сингапур | Малайзия | Япония | Руанда |
|---|---|---|---|---|---|---|---|---|---|---|
| Вуберн | Сан-Паулу | Мадрид | Утрехт | Цюрих | Рим | Эр-Рияд | Сингапур | Куала-Лумпур | Токио | Кигали |

## Проходим независимую оценку

В 2023 году мы успешно прошли

**аудит SOC 2**

второго типа

В рамках Глобальной инициативы по информационной открытости «Лаборатория Касперского» регулярно получает независимую оценку своих внутренних процессов. Так, с 2019 года системы управления данными Компании проходят ежегодную сертификацию в соответствии со стандартом ISO/IEC 27001:2013. Аудит подтверждает безопасность решений Компании. Также с 2019 года «Лаборатория Касперского» регулярно проходит аудит Service Organization Control for Service Organizations (SOC 2).

В 2023 году Компания успешно прошла аудит SOC 2 Type 2. Аудит показал, что внутренние средства контроля «Лаборатории Касперского», которые обеспечивают регулярное автоматическое обновление антивирусных баз, работают эффективно, а процесс разработки и выпуска антивирусных баз защищен от несанкционированного вмешательства.

## Собираем данные об уязвимостях через программу bug bounty

**59 репортов**

о незначительных уязвимостях получено за пять лет

**$81 750**

выплачено за репорты

С марта 2018 года «Лаборатория Касперского» получила 59 сообщений о незначительных уязвимостях в рамках программы bug bounty, устранила их и на сегодняшний день выплатила независимым исследователям в качестве вознаграждения в общей сложности $81 750.

Максимальный размер вознаграждения в программе bug bounty установлен на уровне до $100 тысяч за обнаружение наиболее серьезных уязвимостей в ПО «Лаборатории Касперского». С 2022 года Компания проводит свою публичную программу вознаграждения за ошибки на платформе Yogosha. Также мы поддерживаем проект Disclose.io, который представляет собой безопасную площадку для исследователей уязвимостей, обеспокоенных возможными негативными юридическими последствиями своих раскрытий.

## Учим, как оценивать уровень кибербезопасности

**2 организации**

(государственное учреждение и частная компания) прошли тренинги Cyber Capacity Building Program в отчетном периоде

Наша образовательная программа Cyber Capacity Building предназначена для сотрудников частных и государственных компаний, а также университетов, которые хотят получить практические навыки в области оценки уровня безопасности IT-инфраструктуры.

В рамках программы наши специалисты предоставляют рекомендации по аудиту кода, созданию процедур для обработки уязвимостей и методике фаззинга кода[1]. Этим предложением интересуются представители государственного и частного сектора. За отчетный период две организации прошли тренинги: представители регулирующего органа связи Намибии и частной организации.

## Публикуем отчеты о прозрачности

Наша миссия — защищать пользователей от киберугроз, поэтому мы оказываем поддержку партнерам, международным организациям и правоохранительным органам в борьбе с киберпреступностью. Мы регулярно обрабатываем запросы и с 2020 года каждые шесть месяцев публикуем отчетность: в каких юрисдикциях получаем такие запросы, сколько из них удовлетворены и сколько отклонены. Для этого внутри Компании существует процесс по обработке таких запросов и, в частности, четкие критерии для их юридической проверки.

Теперь «Лаборатория Касперского» один раз в полгода раскрывает количество запросов от полиции на предоставление информации о пользовательских данных, экспертизы и технической информации для расследования угроз. При этом мы не предоставляем доступ к инфраструктуре Компании, включая инфраструктуру по работе с данными, никаким третьим сторонам[2]. С такой же периодичностью мы рассказываем о запросах от наших собственных пользователей об их персональных данных и о том, как мы с ними работаем, где они хранятся и т. д.

[1] Метод тестирования программного обеспечения, когда программе отправляют заведомо неверные данные, анализируют реакцию и за счет этого обнаруживают ошибки.

[2] Подробнее о принципах работы с запросами можно прочитать в наших отчетах о прозрачности.

# Планы по развитию GTI на 2024 год

К середине 2024 года Компания планирует расширить сеть центров прозрачности, открыв еще как минимум один центр, организовать не менее пяти визитов в центры прозрачности, а также продолжить прохождение международных независимых сертификаций и выпуск отчетов по взаимодействию с правоохранительными органами.

**Наш вклад в разработку этических принципов цифрового развития**

## Представили принципы этичного использования искусственного интеллекта (ИИ) в кибербезопасности

Искусственный интеллект дает большие преимущества для индустрии кибербезопасности, но также несет риски в области приватности и свободы пользователей. В октябре 2023 года на Форуме по управлению интернетом, прошедшем под эгидой Организации Объединенных Наций (ООН), «Лаборатория Касперского» представила свои этические принципы разработки и использования систем на основе машинного обучения, созданные в рамках GTI:

**Прозрачность**

Компания информирует клиентов об использовании технологий машинного обучения в своих продуктах и услугах.

**Безопасность**

Следует использовать широкий спектр мер безопасности для обеспечения качества систем машинного обучения.

**Человеческий контроль**

Он нужен для проверки работы AI/ML-систем при анализе сложных угроз.

**Право на цифровую приватность**

Компания применяет ряд технических и организационных мер для защиты данных и систем, чтобы обеспечить цифровую приватность пользователей.

**Приверженность целям кибербезопасности**

Инструменты машинного обучения должны использоваться исключительно в целях кибербезопасности.

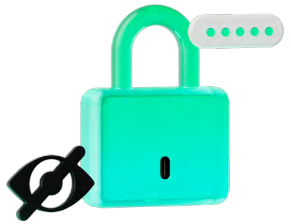
**Открытость к диалогу**

Мы готовы обмениваться передовым опытом в области этичного использования алгоритмов машинного обучения со всеми заинтересованными сторонами.

### Что в результате?

Мы рассказали нашим партнерам, пользователям, профессиональному сообществу, как мы обеспечиваем надежность работы систем машинного обучения, и призвали других участников отрасли присоединиться к диалогу и выработать общие этические принципы.

# Защита данных



Мы уважаем право наших клиентов на конфиденциальность и защищаем их данные. Наша цель — исключить их утечки у пользователей «Лаборатории Касперского».

**~4 тысячи** сотрудников прошли курс по работе с данными клиентов

**>3 тысяч** запросов на обработку данных пользователей в 2023 году

GRI 418-1

## Ключевые задачи

- Обеспечение защиты данных клиентов по всему миру с использованием лучших практик в области информационной безопасности и учетом локальных нормативных актов.
- Оперативное реагирование на запросы клиентов по вопросам обработки и защиты их данных.
- Предотвращение несанкционированного доступа и утечек данных пользователей.

GRI 3-3

## Наш подход к защите данных

Мы делаем все, чтобы обеспечить защиту данных наших клиентов по всему миру. Такая информация — ценный актив для современных компаний. Мы защищаем персональную информацию[1] наших клиентов от возможных несанкционированных изменений, компрометации или потери. Для этого мы используем лучшие в своем классе технологии и принимаем следующие меры безопасности.

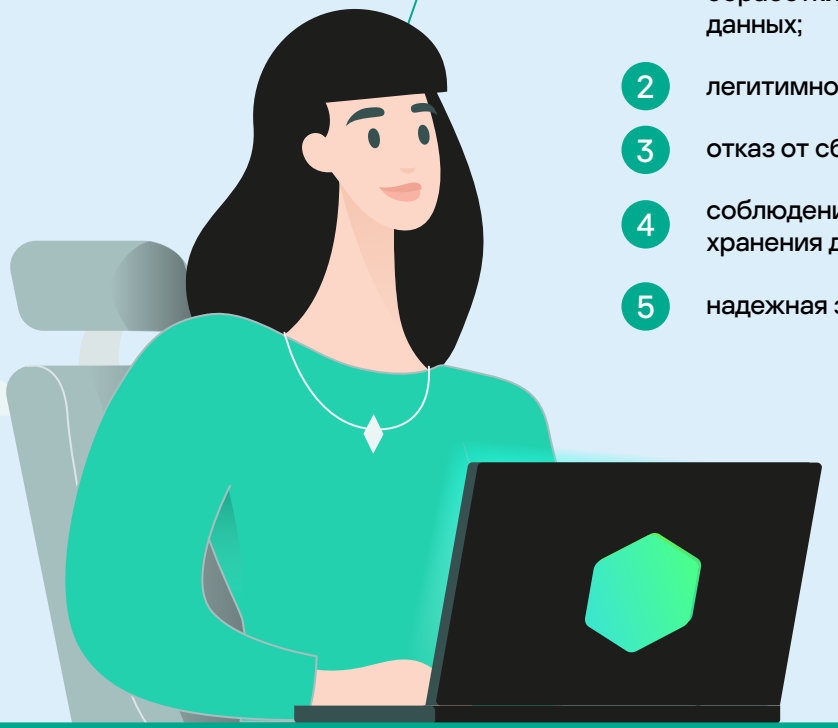
- Жизненный цикл безопасной разработки ПО обеспечивает создание защищенных продуктов и оперативное исправление уязвимостей.
- Надежное шифрование гарантирует безопасный обмен данными между устройством пользователя и облаком.
- Цифровые сертификаты позволяют выполнять легитимную и безопасную аутентификацию серверов и обновление приложений.
- Данные хранятся раздельно на множестве серверов с ограниченными правами и строгими политиками доступа.
- Данные анонимизируются различными методами, среди которых удаление данных учетных записей из переданных URL-адресов, получение хеш-сумм вредоносных файлов вместо самих файлов, сокрытие IP-адресов пользователей и т. д.

[1] Персональная информация — любая информация, относящаяся к физическому лицу, включая Ф.И.О., номера телефонов, адрес, IP-адрес, адрес электронной почты и т. д.

# Как мы защищаем данные по всему миру и предотвращаем их утечки

TC-SI-220-a.1 TC-SI-230-a.2

Мы руководствуемся ключевыми принципами работы с данными согласно европейскому регламенту по защите данных (EU General Data Protection Regulation GDPR), принятому в 2016 году. Именно этот законодательный акт предписывает фундаментальные технические и организационные меры, которые также признаются эталонными в других юрисдикциях. Кроме того, мы выполняем требования международного стандарта по информационной безопасности ISO/IEC 27001 и учитываем требования законов о защите персональных данных разных стран, в числе которых PIPL[1], CCPA[2], LGPD[3], PDPD[4], 152-ФЗ[5] и др.



## Пять ключевых принципов работы с данными клиентов:

1. **законность и прозрачность обработки данных для субъектов данных;**
2. **легитимность целей обработки;**
3. **отказ от сбора избыточных данных;**
4. **соблюдение предельных сроков хранения данных;**
5. **надежная защита данных.**

Мы стремимся свести число инцидентов к нулю. За отчетный период у нас не было нарушений законодательства о персональных данных или утечек данных. Это стало возможным благодаря постоянному обучению сотрудников, внедренным технологиям защиты информации и стандартизации работы с данными. В отчетном периоде мы обновили наши требования к обработке данных, а также провели адаптацию этих требований под законодательство разных стран.

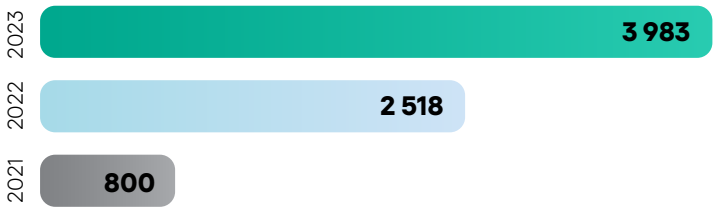
Самую актуальную информацию, включая количество удовлетворенных запросов от наших пользователей, мы собираем в отчете прозрачности. Документ находится в открытом доступе, обновляется и публикуется каждые шесть месяцев.

[1] Закон КНР о защите персональных данных (Personal Information Protection Law of the People's Republic of China).
[2] Закон штата Калифорния о защите персональных данных потребителей (California Consumer Privacy Act).
[3] Общий закон о защите данных Бразилии (Lei Geral de Proteção de Dados).
[4] Закон Вьетнама о защите персональных данных (Personal Data Protection Decree).
[5] Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

# Обучаем правилам работы с данными

В «Лаборатории Касперского» действует курс повышения осведомленности для сотрудников, непосредственно вовлеченных в процессы обработки данных клиентов. В 2023 году этот курс прошли 3 983 человека — все европейские работники Компании и сотрудники по всему миру, вовлеченные в процессы обработки и защиты данных клиентов. Это на 58% больше, чем годом ранее.

## Количество сотрудников, прошедших курс по работе с данными клиентов




## Оценка рисков

Мы используем риск-ориентированный подход, направленный на защиту данных наших пользователей. Оценка рисков выполняется на всех этапах: при внедрении новых систем, разработке новых решений, расследовании инцидентов. В каждом случае мы заранее анализируем, какие риски могут возникнуть при обработке данных клиентов, и сводим эти риски к минимуму.

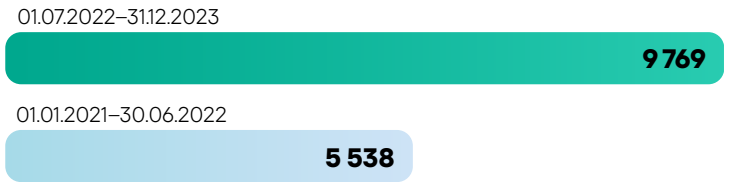
Требования GDPR и региональные законодательства учитывают риски, которым могут подвергнуться пользователи. Нивелировать репутационные и финансовые риски для Компании нам помогает стандарт ISO/IEC 27001.

# Оперативно реагируем на запросы пользователей

TC-SI-220-a.1

**Количество ежемесячных запросов на обработку данных, которые «Лаборатория Касперского» получает от пользователей, иногда доходит до тысячи. 90% этих запросов — требования об удалении их данных из баз Компании.**

## Количество обработанных Компанией запросов пользователей на обработку их данных[1], штук




Пользователи также просят предоставить выгрузку своих данных и сведения о том, какая информация о них хранится и где. В отчетном периоде (с 1 июля 2022 года по конец 2023 года) мы успешно обработали 9 769 обращений, а в период 1 января 2021 года по 30 июня 2022 года — 5 538. Мы наблюдаем тенденцию к увеличению количества таких запросов как в Европе, так и по всему миру. Это происходит по двум причинам: повышение осведомленности пользователей о своих правах и принятие новых законов о персональных данных.

Наша цель — предоставлять всю необходимую информацию о данных пользователям, чтобы они могли доверять нашей Компании и продуктам. В рамках налаженного процесса получения и обработки запросов мы создаем отчеты прозрачности, в которых фиксируем количество и типы запросов, поступающих к нам от клиентов. Мы обновляем и публикуем такие отчеты каждые шесть месяцев.

Как и большинство компаний, мы работаем с данными пользователей и в таргетированной рекламе[2]. Согласно GDPR, данные, полученные через cookies[3], считаются персональными, а значит, при их сборе нужно соблюдать соответствующие правила. Единые строгие политики по получению согласий для сбора информации на сайтах применены в Бразилии, Великобритании и во всей Европе. В остальных странах мы собираем минимальные данные для предоставления релевантной информации для наших потенциальных клиентов.

Для взаимодействия с потребителями, клиентами и поставщиками в «Лаборатории Касперского» работает форма обратной связи на официальном сайте:
www.kaspersky.ru/about/contact — для русскоязычных пользователей;
www.kaspersky.com/about/contact — для международных пользователей.

[1] Согласно отчетам прозрачности.
[2] Таргетированная реклама — один из ключевых инструментов маркетинга, когда для продвижения товаров и услуг используют персональные данные пользователей, собранные с помощью различных веб-сайтов, приложений и соцсетей.
[3] Cookies — небольшие файлы, хранящиеся на компьютерах и гаджетах, с помощью которых сайт запоминает информацию о посещениях пользователя.

# Предотвращаем утечки данных

GRI-418-1 TC-SI-220-a.1 TC-SI-230-a.1 TC-SI-220-a.2 TC-SI-220-a.3

**За соблюдение принципов и процедур в области безопасности данных в Компании отвечает Privacy Team.**

Команда, в которую вошли сотрудники подразделений IT, R&D, ИБ и интеллектуальной собственности, сформировалась в 2016 году, когда внедрялись требования GDPR. Privacy Team приводила в соответствие европейскому регламенту все процессы в Компании. Сейчас команда обеспечивает выполнение функций обработки данных в таких направлениях, как консультирование, организационные вопросы и контроль.

Начиная с 2019 года «Лаборатория Касперского» ежегодно проходит сертификацию своих систем по работе с данными на соответствие требованиям международного стандарта ISO/IEC 27001, подтверждая их высокий уровень защиты. В отчетном периоде область аудита информационных систем была значительно расширена. Мы наняли новых сотрудников и сформировали новое подразделение, с помощью которого в 2023 году было проведено 388 внутренних аудитов.

Область сертификации распространяется на область обработки данных «Лаборатории Касперского» «Доставка вредоносных и подозрительных файлов и статических данных об активности с помощью инфраструктуры Kaspersky Security Network (KSN), их безопасное хранение и доступ в Kaspersky Lab Distributed File System (KLDFS) и к базе данных KSNBuffer».

Сертификация действительна для сервисов обработки данных, расположенных в дата-центрах в Цюрихе, Франкфурте-на-Майне, Глаттбурге, Торонто, Москве и Пекине.

## Запуск новой системы учета

В отчетном периоде мы завершили масштабный проект — запустили новую систему учета процессов и сервисов обработки данных, созданную силами команды разработчиков «Лаборатории Касперского». В ней учитывается, какие сервисы обрабатывают данные клиентов, в каких бизнес-процессах они используются, кто контроллер (оператор) и процессор (обработчик) данных, какие данные в системе хранятся, как долго, на каком основании, в каком объеме, в каких странах и т. д. Новая система готова к работе, и в нее уже перенесено 80% данных.

**0**
серьезных нарушений законодательства о персональных данных и значительных утечек

**0**
убытков в результате судебных разбирательств из-за нарушения конфиденциальности за отчетный период

**388**
**внутренних аудитов**
на сертификацию соответствия ISO/IEC 27001 в 2023 году

## Наши планы на 2024 год

- Выставление обновленных требований по обработке и защите данных ко всем сервисам, в которых обрабатываются данные клиентов.
- Проведение консультаций команд по обновленным требованиям.
- Проведение аудитов эффективности сервисов в области обработки и защиты данных пользователей.

# Охрана и защита интеллектуальной собственности

Мы постоянно работаем над созданием и внедрением перспективных решений в области кибербезопасности и регулярно патентуем наши изобретения и инновационные технологии.

**231 патент**
на свои продукты получила «Лаборатория Касперского» за 2022–2023 годы

## Как мы охраняем и защищаем интеллектуальную собственность

Один из важнейших компонентов развития и стабильности нашего бизнеса — права на интеллектуальную собственность. Мы охраняем свои разработки, а также уважаем права других компаний на их технологии и решения.

## # Задача

**Охрана и защита прав на продукты, решения и технологии**

# # Решения

## Получаем патенты в разных юрисдикциях

TC-SI-520-a.1

«Лаборатория Касперского» всегда стремится закрепить за собой охраняемые государством исключительные права на результаты своей интеллектуальной деятельности, а в случае их нарушения защищает эти права через суд. Это помогает нам поддерживать справедливость и законность в бизнес-среде.

За отчетный период Компания получила 231 патент на свои технологии в разных юрисдикциях.

Отметим, что направленность патентов на ключевые технологии в последние годы сместилась в сторону B2B-продуктов и KasperskyOS. Это SIEM[1], Research Sandbox[2], технологии машинного обучения, которые выявляют не только новые вредоносные объекты, но и аномалии (MLAD[3]), а также технологии по защите от шифровальщиков.

Охрана и защита интеллектуальной собственности стали неотъемлемой частью деятельности «Лаборатории Касперского» с 2005 года. За это время мы смогли выстроить и оптимизировать процессы получения правовой охраны для любых результатов интеллектуальной деятельности. Также за эти годы наша Компания достигла впечатляющего результата: не было ни одного случая, когда бы мы проиграли инициированные против нас судебные процессы, связанные с патентами.

Накопленный опыт и экспертиза помогают нам не только успешно охранять и защищать свои инновации, но и содействовать развитию сферы интеллектуальной собственности в целом.

Одновременно с совершенствованием наших продуктов мы активно участвуем в развитии open-source-движения. Только за 2022–2023 годы Компания сделала 20 публикаций open-source-проектов, предоставляющих доступ к нашим технологиям всему сообществу разработчиков. Мы верим в важность таких публикаций и их ценность для сотрудничества, обмена опытом и знаниями.

В дополнение к этому мы придаем большое значение образованию и поддержке сотрудников, обучающихся в высших учебных заведениях и желающих использовать интеллектуальную собственность Компании в своих научных исследованиях. Для реализации их стремлений и защиты критически важной информации мы разработаем процедуру, предоставляющую им такую возможность. Для этого создаются регламенты и инструкции по вопросам, связанным с использованием интеллектуальной собственности.

### Патенты, полученные на продукты «Лаборатории Касперского», штук


**20**
**open-source-публикаций за 2022–2023 годы**

[1] Security Information and Event Management — класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.
[2] «Песочница» для исследования сложных угроз, которую можно развернуть внутри корпоративной инфраструктуры.
[3] Machine Learning for Anomaly Detection.

# Неукоснительно соблюдаем закон в сфере интеллектуальной собственности

Помимо охраны собственных достижений для нас важно своевременно реагировать и устранять риски, связанные с неправомерным использованием интеллектуальной собственности других компаний внутри нашей организации, включая использование стороннего кода, и реагировать на них соответствующим образом. Это достигается путем внедрения соответствующих политик, тщательной проверки лицензий и контроля за соблюдением всех необходимых правил и норм.

Еще одна важная часть работы в этом направлении — обучение и информирование наших сотрудников. В частности, каждый новый сотрудник проходит специальный ознакомительный тренинг, который позволяет ему получить базовое представление об интеллектуальной собственности.

Кроме того, в II квартале 2024 года мы планируем запустить специализированный курс по патентам для сотрудников технических подразделений «Лаборатории Касперского». В рамках курса наши коллеги, вовлеченные в разработку новых продуктов, получат информацию о внутренних процедурах, связанных с вопросами охраны интеллектуальной собственности.

При необходимости мы всегда готовы отстаивать свои права в суде — это одна из наших ключевых стратегических позиций. В большинстве случаев судебные споры возникают в США, в основном в результате действий патентных троллей[1]. В России мы имели опыт разрешения споров, связанных с нарушением антимонопольного законодательства, и также успешно отстояли свои интересы.

Таким образом, мы всегда стремимся защищать свои права с использованием всех доступных законных средств, но при этом не готовы идти на необоснованные схемы урегулирований. Наша цель — обеспечить справедливое и законное разрешение споров, которое учитывает позиции всех сторон.

В отчетном периоде мы завершили патентный спор с троллем Cybersoft, который утверждал, что наш продукт Kaspersky Secure Mail Gateway нарушает патент на технологию в области сетевой безопасности, позволяющую выполнять проверку передаваемых по сети данных на устройстве пользователя. По нашим оценкам, сумма возможного ущерба в самом негативном для нас сценарии спора могла составить около $500 тысяч. Однако в 2022 году дело завершилось в нашу пользу. Патентный тролль осознал бесперспективность разбирательства для него и выступил за урегулирование кейса.

**100%**

**патентных исков, предъявленных Компании в течение 18 лет в США, мы успешно отстояли в суде**

В марте 2022 года «Лаборатория Касперского» столкнулась с новым вызовом в виде патентного спора, инициированного антивирусной компанией Webroot в США. Этот случай можно считать историческим, так как мы впервые вступили в разбирательство с нашим прямым конкурентом. В июне того же года мы подали встречный иск к Webroot в ответ на нарушение наших патентных прав. Ожидается, что непосредственные судебные слушания по этому делу состоятся только в ноябре 2024 года. Мы намерены защитить наши права и минимизировать возможное негативное влияние этого спора на бизнес и репутацию нашей Компании.

## Наши планы на 2024 год

- Начать получать правовую охрану изобретениям в дополнительных юрисдикциях.
- Начать патентовать объекты интеллектуальной собственности, которые относятся к дизайну наших продуктов (в том числе интерфейс).
- Подготовить и запустить патентный курс для сотрудников.
- Пересмотреть некоторые локальные нормативные акты в области ИС, чтобы соответствовать меняющемуся правовому ландшафту.
- Формировать ресурсы и инструкции сотрудникам, учащимся в институтах, по вопросам, связанным с интеллектуальной собственностью, чтобы обеспечить соблюдение правил и политик Компании.

[1] Физическое или юридическое лицо, чей бизнес состоит исключительно в получении лицензионных платежей за использование принадлежащих ему патентов, без попыток реализовать запатентованные изобретения на практике.

# Корпоративное управление

GRI 2-9 GRI 2-10 GRI 2-11 GRI 2-13

Наш бизнес основан на принципах открытости и честности по отношению к клиентам, партнерам, конкурентам. Мы постоянно работаем над повышением прозрачности и открытости нашей Компании.

## Подход к корпоративному управлению

Мы дорожим репутацией нашей Компании и стремимся повышать прозрачность управления во всех аспектах своей деятельности. Ключевые правила деловой и корпоративной этики будут зафиксированы. Они будут закреплены в Этическом кодексе «Лаборатории Касперского», который находится в процессе разработки.

### Ключевые принципы

- Обеспечение прозрачности корпоративного управления.
- Соблюдение антикоррупционной политики за счет недопущения случаев ее нарушений.
- Высокий уровень правовой поддержки, связанной с охраной и защитой интеллектуальной собственности.
- Снижение рисков по цепочке поставок.

### Как работает наша система корпоративного управления

Высший орган управления в «Лаборатории Касперского» — совет директоров. Он отвечает за ключевые решения, принимает глобальные политики и стратегии, которые имплементируются во все компании внутри группы. В текущем составе совета директоров четыре человека. Все они находятся на постоянном контракте более пяти лет. Независимых членов в совете директоров нет, только исполнительные.

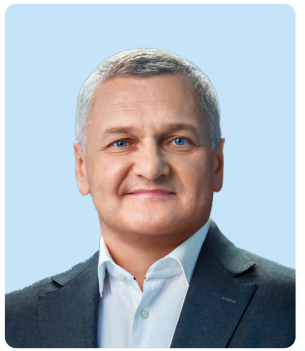
Кандидатов в совет директоров назначают действующие члены совета.

В нашей Компании нет постоянного председателя совета директоров. Он избирается на каждое заседание совета, у него нет специальных полномочий, он не является одновременно и CEO.

Ответственность за экономические, социальные и экологические воздействия устойчивого развития делегирована руководителю департамента корпоративных коммуникаций Денису Зенкину.

# Совет директоров

**Евгений Касперский,**
единоличный исполнительный орган акционерного общества «Лаборатория Касперского» и ООО «Группа компаний Касперского», член совета директоров холдинговой компании и управляющего совета.



**Андрей Тихонов,**
член совета директоров холдинговой компании и управляющего совета, единоличный исполнительный орган АО «Водный Стадион Спорт Инвест».

**Даниил Борщев,**
член совета директоров холдинговой компании и управляющего совета, член совета директоров ООО «Новые Облачные Технологии».

**Светлана Иванова,**
член совета директоров холдинговой компании.

# Управляющий совет

Управляющий совет ООО «Группа компаний Касперского» определяет конкретные стратегические и тактические шаги для операционного развития компании и структуру управления группой компаний, а также утверждает назначения топ-менеджеров.

Роль генерального директора Евгения Касперского в управлении Компанией определяющая, поскольку он одновременно крупнейший акционер холдинговой компании, член совета директоров и управляющего совета.

# Вознаграждение

GRI 2-20

Совокупное вознаграждение членов высшего органа управления и высших руководителей регулируется общими компенсационными политиками Компании и включает в себя следующие элементы:

- **фиксированная часть** (оклад);
- **премиальная часть** (бонус по результатам работы) — выплачивается по итогам достижения индивидуальных целей, определенных для каждой должности на финансовый год;
- **выплаты в рамках программы долгосрочного вознаграждения** — производятся ежегодно, но привязаны к трехлетнему отчетному циклу и зависят от финансовых результатов Компании в целом (основой для расчетов таких выплат являются EBITDA и общий рост объема продаж год к году).

Все три элемента системы вознаграждения приблизительно в равных долях составляют совокупный компенсационный пакет высших руководителей. Такая система вознаграждения позволяет поощрять руководителей Компании за индивидуальные успехи и мотивировать их к достижению общих корпоративных целей.

# Как мы соблюдаем антикоррупционную политику

GRI 2-23 GRI 205-2

## «Лаборатория Касперского» — международная компания, которая соблюдает законодательство и требования регуляторов по всему миру.

**0 судебных решений**

**по вопросам нарушений антикоррупционного законодательства в отношении Компании, сотрудников и партнеров**

При этом в штаб-квартире приоритет отдается законодательству Российской Федерации, а в зарубежных офисах — местному антикоррупционному законодательству.

Базовые принципы противодействия коррупции закреплены в антикоррупционной политике Компании, принятой в 2012 году. Она размещена на нашем официальном сайте и переведена на 30 языков регионов присутствия «Лаборатории Касперского». Главный принцип антикоррупционной политики — наша Компания не приемлет никаких форм подкупа или коррупции частных лиц или госслужащих и не участвует ни в каких формах неэтичных поощрений или платежей.

За соблюдение антикоррупционной политики отвечают комплаенс-офицер и его представители в регионах. Они расследуют все факты возможных нарушений, о которых любой сотрудник может сообщить своему руководителю, комплаенс-офицеру или его представителям, а также по телефону горячей линии 8–800–700–88–11 или на почтовый ящик infosec@kaspersky.com. При желании отправить сообщение или позвонить можно анонимно.

GRI 205-1

## Антикоррупционные практики

В «Лаборатории Касперского» регулярно проводится оценка рисков, связанных с коррупцией. В отчетном периоде мы провели такую оценку дважды.

GRI 205-3

Кроме того, мы ежегодно информируем сотрудников об антикоррупционной политике и соответствующих процедурах. При заключении договоров с контрагентами мы разработали и интегрируем в договоры антикоррупционную политику.

В отчетном периоде мы провели обучение сотрудников антикоррупционным политикам и процедурам на специальном онлайн-курсе, посвященном борьбе со взяточничеством и коррупцией. Этот курс включает знакомство с базовыми принципами и основными направлениями антикоррупционной политики Компании, в числе которых:

- цели антикоррупционного законодательства;
- важность соблюдения норм российских и зарубежных законов о взяточничестве и противодействии коррупции;
- модели поведения, которые приводят к нарушению законов по борьбе с коррупцией;
- необходимость проявления осмотрительности в деловых отношениях с третьими лицами;
- механизмы внутреннего контроля, определяющие деятельность сотрудников в соответствии с антикоррупционной политикой.

Антикоррупционный курс рассчитан на 30–40 минут обучения. Результаты тестирования по итогам курса заносятся во внутреннюю систему «Лаборатории Касперского».

В отчетном периоде обучение прошли все сотрудники Компании — от высшего менеджмента до младших специалистов.

**100%**

**сотрудников и партнеров проинформированы об антикоррупционной политике**

**0**

**подтвержденных случаев коррупции в Компании**

## Планы по совершенствованию антикоррупционных практик на 2024 год

В 2024 году мы планируем обновить материалы обучающего антикоррупционного курса, а также продолжить внедрение лучших антикоррупционных практик в деятельность Компании.

# Управление рисками

TC-SI-550-a.2

В течение 2022–2023 годов на основе ранее внедренного Global Problem Management процесса по управлению технологическими рисками в Компании сформирована и активно развивается система управления рисками (СУР). Она обеспечивает управление операционными и технологическими рисками как на уровне департаментов и подразделений Компании, так и на пересечении зон ответственности функциональных областей.

Основные принципы управления рисками Компании разработаны в соответствии с законодательством Российской Федерации, нормативными актами Центрального банка Российской Федерации, международной практикой управления рисками.

## Цели и задачи управления рисками

Целями управления операционными рисками являются выявление, оценка, агрегирование и контроль объема операционных рисков «Лаборатории Касперского» во всех ее подразделениях. Кроме того, Компания стремится поддерживать операционные риски на приемлемом уровне, обеспечивающем устойчивое функционирование и развитие бизнеса в рамках реализации стратегии, сохранения активов и поддержания высокого качества продуктов и услуг.

Компания управляет технологическими рисками, своевременно и проактивно выявляя их и предотвращая инциденты, связанные с качеством продуктов и сервисов Компании, ее внутренней IT-инфраструктуры, а также с рисками непрерывности бизнеса.

Задачи системы управления рисками:

- обеспечение осведомленности руководства Компании о ключевых операционных и технологических рисках, в том числе о характере и возможных последствиях, а также об уровне контроля этих рисков;
- своевременная идентификация и оценка операционных и технологических рисков Компании во всех ее подразделениях, включая все новые направления деятельности, процессы, системы, активы, и снижение вероятности возникновения потерь, величины потерь в процессе осуществления деятельности Компании;
- обеспечение бесперебойной деятельности Компании.

## Принципы управления операционными рисками

- **Создание рискориентированной среды в Компании**

Управление операционными рисками не является изолированным процессом в рамках отдельного подразделения. Это неотъемлемая часть трудового процесса каждого сотрудника «Лаборатории Касперского».

- **Непрерывность и обязательность процесса управления операционными рисками**

Процедуры управления операционными рисками применяются к бизнес-процессам и операциям, обеспечивающим достижение целей деятельности и выполнение функций Компании.

- **Информированность и осведомленность об операционных рисках для каждого уровня принятия решений в Компании**

Компания создает систему отчетности об уровне операционных рисков и приоритизирует риски таким образом, чтобы лицам, принимающим решения, была доступна наиболее актуальная информация о рисках, связанных с принимаемыми решениями. Для показателей операционных рисков устанавливаются пороговые значения, о превышении которых информируют менеджеров более высокого уровня.

- **Открытость и прозрачность процедур и методов анализа операционных рисков**

Подразделение Компании, ответственное за анализ рисков, максимально полно отражает во внутренних нормативных документах подходы к оценке рисков и документирует процедуру анализа операционных рисков. В будущем это позволит провести оценку эффективности системы управления операционными рисками.

# Процесс управления операционными рисками


**Идентификация** (выявление) рисков представляет собой определение и классификацию выявленных рисков. Для идентификации рисков используется комбинация различных методик и инструментов. Для каждого выявленного риска определяются его владелец, причина возникновения события операционного риска, а также ответственный за меры по снижению рисков.

Оценка значимости рисков и анализ проводятся по двум параметрам: оценка фактически понесенных или потенциальных потерь для Компании в случае реализации риска (влияние) и вероятность реализации события операционного риска.

**Мониторинг** фактически понесенных и потенциальных потерь осуществляется Компанией на регулярной основе. В процессе выявляются источники реализации риска, а также критические уязвимости в текущих бизнес-процессах, соответствие установленному уровню риска, выявление нарушений допустимого уровня риска.

**Контроль** рисков в Компании осуществляется непрерывно и в первую очередь направлен:

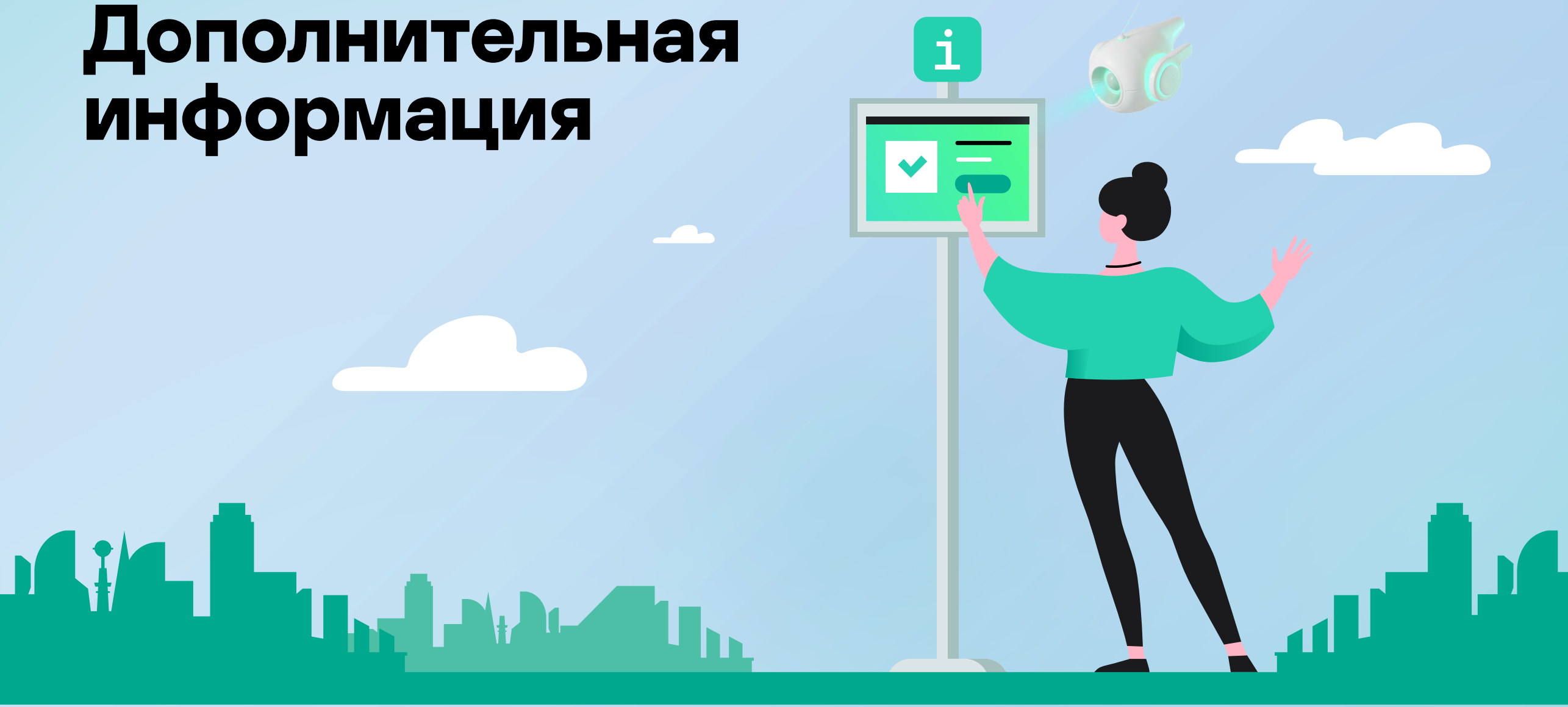
- на соблюдение установленных процедур и полномочий при принятии и реализации управленческих решений, затрагивающих интересы Компании и клиентов;
- управление операционными рисками, возникающими при осуществлении деятельности Компании;
- принятие своевременных и эффективных мер, способствующих устранению выявленных недостатков и нарушений в деятельности Компании.

# Отчетность по операционным рискам и обмен информацией о рисках

Чтобы способствовать принятию объективных и действенных управленческих решений, Компания внедрила многоступенчатую систему отчетности по рискам. Отчетность содержит сведения о фактических или потенциальных потерях, понесенных Компанией в связи с реализацией операционных рисков, о рисках в разрезе категорий операционных рисков, об источниках операционных рисков, а также количественный анализ событий, карту операционных рисков и информацию о превентивных и последующих мерах по минимизации потерь Компании.

Генеральный директор «Лаборатории Касперского» получает ежегодный отчет с указанием наиболее значимых рисков и событий операционного риска. Ежеквартальный отчет об операционных рисках представляется управляющему совету. Кроме того, в Компании проводится регулярное обсуждение статуса инцидентов и рисков с руководителями департаментов, руководителями и сотрудниками структурных подразделений.

# Дополнительная информация



# Приложение 1. Об Отчете

GRI 2-2 GRI 2-3 GRI 2-14

В настоящем Отчете «Лаборатория Касперского» раскрывает информацию в соответствии с требованиями следующих международных стандартов в области устойчивого развития:

- Руководство Глобальной инициативы по отчетности (GRI 2021);
- отраслевое Руководство Sustainability Accounting Standards Board (SASB) для сектора Software & IT Services.

Информация о соответствии раскрываемой информации требованиям этих стандартов представлена в разделах «Указатель соответствия Руководству GRI Standards» и «Указатель соответствия Руководству SASB Standards».

Информация, опубликованная в Отчете, если специально не указано иное[1], охватывает деятельность акционерного общества «Лаборатория Касперского», включая штаб-квартиру компании АО Kaspersky Lab и дочерние компании в странах присутствия (региональные офисы), список которых приведен в консолидированной отчетности компании Kaspersky Lab Limited за 2021 год[2].

Отчет охватывает период с 1 июля 2022 года по 31 декабря 2023 года. В дальнейшем Компания намерена выпускать отчеты об устойчивом развитии на ежегодной основе.

Прогнозные заявления и планы «Лаборатории Касперского», отраженные в настоящем Отчете, носят предварительный характер. Они могут меняться в зависимости от внешних и внутренних обстоятельств, неизвестных на момент планирования, поэтому результаты деятельности в области устойчивого развития в последующих отчетных периодах могут отличаться от заявленных в настоящем Отчете.

Отчет опубликован на сайте Компании на русском и английском языках.

[1] Информация по экологическим воздействиям охватывает только штаб-квартиру «Лаборатории Касперского» (российский офис).
[2] Кроме того, в периметр отчетности добавился офис Компании в столице Саудовской Аравии Эр-Рияде, открытый в сентябре 2023 года.

# Приложение 2. Участие в ассоциациях и объединениях

GRI 2-28

**«Лаборатория Касперского» сотрудничает со следующими организациями:**

- Интерпол;
- Международный союз электросвязи;
- Международная организация по стандартизации (МОС/МЭК SC41 (МОС — Международная организация по стандартизации. Активные члены SC41 WG3 (Эталонная архитектура и надежность) и WG5 (Совместимость в интернет вещей));
- Альянс No More Ransom;
- Коалиция против сталкерского ПО (Coalition Against Stalkerware);
- Женевский диалог (Geneva Dialogue);
- Парижский призыв к доверию и безопасности в киберпространстве (Paris Call for Trust and Security in Cyberspace);
- Совет Европы (Council of Europe);
- IT-Sicherheitscluster e.V. (Германия);
- BVMW e.V. Der Mittelstand (Германия);
- Plattform Industrie 4.0 (Германия);
- Cybermalveillance.gouv.fr (GIP ACYMA) (Франция);
- Renaissance Numérique (Франция);
- Всемирная интернет-конференция World Internet Conference (участник High-Level Expert Advisory Committee);
- China Industrial Control System CERT (отраслевой партнер);
- Operational Technology Information Sharing and Analysis Center (OT-ISAC, Singapore);
- Сингапурская ассоциация технологической отрасли (SGTech);
- Singapore Computer Society;
- Malaysian Internet-of-Things Association (MyIoTA);
- Движение Women in Technology;
- Data Security Council of India;
- Communication and Information System Security Research Center (Индонезия);
- Промышленный консорциум интернета вещей (Industry IoT Consortium (США));
- Интернет Ассоциация Казахстана;
- Ассоциация разработчиков программных продуктов «Отечественный софт» (АРПП);
- Российский союз промышленников и предпринимателей (РСПП);
- Ассоциация предприятий компьютерных и информационных технологий (АПКИТ);
- ТК-МТК-22 «Информационные технологии»;
- Альянс по защите детей в цифровой среде;
- АНО «Цифровая экономика».

# Приложение 3. К разделу «Возможности для людей»

GRI 2-7 GRI 401-1 GRI 401-3 GRI 405-1 GRI 405-2

## Общая численность с разбивкой по типу трудового договора и по полу, человек

| 2021 | | | | | | 2022 | | | | | | 2023 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Постоянный | | Временный | | Временная замена | | Постоянный | | Временный | | Временная замена | | Постоянный | | Временный | | Временная замена | |
| Ж | М | Ж | М | Ж | М | Ж | М | Ж | М | Ж | М | Ж | М | Ж | М | Ж | М |
| 1 083 | 3 190 | 37 | 104 | 34 | 14 | 1 227 | 3 584 | 25 | 48 | 42 | 11 | **1 263** | **3 798** | **23** | **39** | **22** | **7** |

## Общая численность работников с разбивкой по типу занятости и по полу, человек

| 2021 | | | | 2022 | | | | 2023 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Полная | | Частичная | | Полная | | Частичная | | Полная | | Частичная | |
| Ж | М | Ж | М | Ж | М | Ж | М | Ж | М | Ж | М |
| 1 122 | 3 282 | 32 | 26 | 1 269 | 3 619 | 25 | 24 | **1 271** | **3 823** | **37** | **21** |

## Процент от общего количества сотрудников на неполной занятости, %

| 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|
| **Ж** | **М** | **Всего** | **Ж** | **М** | **Всего** | **Ж** | **М** | **Всего** |
| 3 | 1 | 1 | 2 | 1 | 1 | **3** | **1** | **1** |

## Общая численность в разбивке по регионам, человек

| **Регион** | **2021** | **2022** | **2023** | **Изменение 2023/2022, %** |
|---|---|---|---|---|
| АТР | 242 | 222 | **227** | 2 |
| Латинская Америка | 102 | 107 | **134** | 25 |
| Ближний Восток, Турция и Африка | 97 | 103 | **136** | 32 |
| Европа | 424 | 343 | **340** | –1 |
| Северная Америка | 114 | 71 | **65** | –8 |
| СНГ | 3 483 | 4 091 | **4 250** | 4 |
| в том числе Россия | 3 463 | 4 064 | **4 221** | 4 |

# Структура персонала по категориям сотрудников

| | На 31.12.2021 | | На 31.12.2022 | | На 31.12.2023 | | Изменение доли 2023/2022, п. п. |
|---|---|---|---|---|---|---|---|
| **Категория** | **человек** | **%** | **человек** | **%** | **человек** | **%** | |
| **Руководители**[1] | **763** | **17** | **817** | **17** | **835** | **16** | **0** |
| в том числе: | | | | | | | |
| мужчины | 577 | 76 | 621 | 76 | **622** | **74** | –2 |
| женщины | 186 | 24 | 196 | 24 | **213** | **26** | 2 |
| в том числе: | | | | | | | |
| до 30 лет | 47 | 6 | 66 | 8 | **65** | **8** | 0 |
| от 30 до 50 лет | 624 | 82 | 667 | 82 | **685** | **82** | 0 |
| свыше 50 лет | 92 | 12 | 84 | 10 | **85** | **10** | 0 |
| **Технические специалисты** | **2 213** | **50** | **2 564** | **52** | **2 698** | **52** | **0** |
| в том числе: | | | | | | | |
| мужчины | 1 822 | 82 | 2 107 | 82 | **2 250** | **83** | 1 |
| женщины | 391 | 18 | 457 | 18 | **448** | **17** | –1 |
| в том числе: | | | | | | | |
| до 30 лет | 710 | 32 | 922 | 36 | **940** | **35** | –1 |
| от 30 до 50 лет | 1 448 | 65 | 1 575 | 61 | **1 680** | **62** | 1 |
| свыше 50 лет | 55 | 2 | 67 | 3 | **78** | **3** | 0 |
| **Прочие специалисты** | **1 486** | **33** | **1 556** | **32** | **1 619** | **31** | **0** |
| в том числе: | | | | | | | |
| мужчины | 909 | 61 | 915 | 59 | **972** | **60** | 1 |
| женщины | 577 | 39 | 641 | 41 | **647** | **40** | –1 |
| в том числе: | | | | | | | |
| до 30 лет | 122 | 8 | 382 | 25 | **356** | **22** | –3 |
| от 30 до 50 лет | 1 184 | 80 | 1 079 | 69 | **1 139** | **70** | 1 |
| свыше 50 лет | 180 | 12 | 95 | 6 | **124** | **8** | 2 |

[1] Менеджеры, у которых в подчинении от одного человека.

## Численность принятых работников, человек

| Показатель | 2021 | 2022 | 2023 | Изменение 2023/2022, % |
|---|---|---|---|---|
| Принятые работники | 1 039 | 1 445 | **944** | –35 |

Численность принятых в 2023 году работников сократилась более чем на треть в сравнении с 2022 годом.
Это обусловлено сокращением текучести и соответствующим снижением числа вакансий для заполнения.

## Численность принятых работников с разбивкой по возрастным группам

| | 2021 | | 2022 | | 2023 | | Изменение численности 2023/2022, % |
|---|---|---|---|---|---|---|---|
| Возраст работников | человек | % | человек | % | человек | % | |
| До 30 лет | 351 | 34 | 557 | 39 | **371** | **39** | –33 |
| От 30 до 40 лет | 496 | 48 | 648 | 45 | **407** | **43** | –37 |
| От 40 до 50 лет | 142 | 14 | 200 | 14 | **131** | **14** | –36 |
| 50 лет и старше | 50 | 5 | 40 | 3 | **35** | **4** | –13 |

## Численность принятых работников с разбивкой по полу

| | 2021 | | 2022 | | 2023 | | Изменение численности 2023/2022, % |
|---|---|---|---|---|---|---|---|
| Пол работников | человек | % | человек | % | человек | % | |
| Мужчины | 762 | 73 | 1 075 | 74 | **721** | **76** | –33 |
| Женщины | 277 | 27 | 370 | 26 | **223** | **24** | –40 |

## Численность принятых работников по региону, человек

| Регион | 2021 | 2022 | 2023 | Изменение 2023/2022, % |
|---|---|---|---|---|
| АТР | 47 | 37 | **33** | –11 |
| Латинская Америка | 22 | 25 | **39** | 56 |
| Ближний Восток, Турция и Африка | 19 | 24 | **50** | 108 |
| Европа | 53 | 45 | **41** | –9 |
| Северная Америка | 14 | 7 | **3** | –57 |
| СНГ | 884 | 1 307 | **778** | –40 |
| в том числе Россия | 875 | 1 291 | **769** | –40 |

## Численность выбывших работников, человек

| Показатель | 2021 | 2022 | 2023 | Изменение 2023/2022, % |
|---|---|---|---|---|
| Выбывшие работники | 826 | 1 101 | **770** | –30 |

## Численность выбывших работников с разбивкой по возрастным группам

| | 2021 | | 2022 | | 2023 | | Изменение 2023/2022, % |
|---|---|---|---|---|---|---|---|
| **Возраст работников** | **человек** | **%** | **человек** | **%** | **человек** | **%** | |
| До 30 лет | 275 | 33 | 356 | 32 | **265** | **34** | –26 |
| От 30 до 40 лет | 361 | 44 | 477 | 43 | **320** | **42** | –33 |
| От 40 до 50 лет | 145 | 18 | 204 | 19 | **142** | **18** | –30 |
| 50 лет и старше | 45 | 5 | 64 | 6 | **43** | **6** | –33 |

Численность выбывших сотрудников в 2023 году снижалась благодаря общему тренду на снижение текучести.

## Численность выбывших работников с разбивкой по полу

| | 2021 | | 2022 | | 2023 | | Изменение 2023/2022, % |
|---|---|---|---|---|---|---|---|
| **Пол работников** | **человек** | **%** | **человек** | **%** | **человек** | **%** | |
| Мужчины | 521 | 63 | 812 | 74 | **521** | **68** | –36 |
| Женщины | 305 | 37 | 289 | 26 | **249** | **32** | –14 |

## Численность выбывших работников и текучесть кадров по региону

| | Всего выбыло, человек | | | Текучесть кадров, % | | | |
|---|---|---|---|---|---|---|---|
| **Регион** | **2021** | **2022** | **2023** | **2021** | **2022** | **2023** | **Изменение 2023/2022, п. п.** |
| АТР | 54 | 59 | **29** | 22 | 26 | **13** | –13 |
| Латинская Америка | 9 | 21 | **13** | 9 | 20 | **10** | –10 |
| Ближний Восток, Турция и Африка | 12 | 20 | **19** | 13 | 19 | **15** | –4 |
| Европа | 77 | 127 | **52** | 18 | 34 | **15** | –19 |
| Северная Америка | 39 | 44 | **7** | 31 | 49 | **10** | –39 |
| СНГ | 635 | 830 | **650** | 20 | 22 | **16** | –6 |
| в том числе Россия | 629 | 821 | **644** | 19 | 22 | **16** | –6 |
| **Всего** | **826** | **1 101** | **770** | **19** | **23** | **15** | **–8** |

## Работники, оставшиеся в Компании после отпуска по уходу за ребенком

| | 2021 | | 2022 | | 2023 | | |
|---|---|---|---|---|---|---|---|
| **Пол работников** | **человек** | **%** | **человек** | **%** | **человек** | **%** | **Изменение 2023/2022, %** |
| Женщины | 28 | 72 | 38 | 76 | **42** | **68** | 11 |
| Мужчины | 2 | 100 | 4 | 67 | **2** | **67** | –50 |

## Коэффициент возвращения к работе после отпуска по уходу за ребенком, %

| Пол работников | 2021 | 2022 | 2023 |
|---|---|---|---|
| Женщины | 98 | 96 | **98** |
| Мужчины | 100 | 100 | **100** |

## Коэффициент удержания сотрудников, %

| Пол работников | 2021 | 2022 | 2023 |
|---|---|---|---|
| Женщины | 90 | 67 | **71** |
| Мужчины | 50 | 38 | **50** |

## Соотношение вознаграждения[1] женщин и мужчин[2], %

| Показатель | 2021 | 2022 | 2023 |
|---|---|---|---|
| **Руководители** | | | |
| Оклад женщин в процентах от оклада мужчин | 96 | 95 | **95** |
| Вознаграждение женщин в процентах от вознаграждения мужчин | 98 | 95 | **95** |
| **Технические специалисты** | | | |
| Оклад женщин в процентах от оклада мужчин | 97 | 98 | **96** |
| Вознаграждение женщин в процентах от вознаграждения мужчин | 97 | 98 | **95** |
| **Прочие специалисты** | | | |
| Оклад женщин в процентах от оклада мужчин | 95 | 100 | **96** |
| Вознаграждение женщин в процентах от вознаграждения мужчин | 95 | 100 | **96** |

[1] Оклад и выплаты в зависимости от категории, выслуги лет и др.
[2] Данные указаны для московского офиса Компании.

# Приложение 4. К разделу «Технологии будущего»

Список законов, подзаконных актов, приказов или рекомендаций, которые Компания учитывает при разработке продуктов и решений

| Страна | Регуляторы | Законы, подзаконные акты, приказы или рекомендации |
|---|---|---|
| Россия | Минцифры.<br>Роскомнадзор.<br>Банк России.<br>ФСТЭК России.<br>ФСБ России | Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».<br>Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» |
| Германия | UP KRITIS: BSI, BBK BMI; BDEW; BNetzA | IT Security ACT UP KRITIS; Namur 153; VDMA 66418; DIN2008; DIN2011 |
| Франция | ANSSI | Critical Information Infrastructure Protection (CIIP) framework. CIIP law; Sécurité des activités d'importance vitale (SAIV); Décret 350, 351 |
| Великобритания | National Cyber Security Centre.<br>National Protective Security Authority | OG86 — Cyber Security for Industrial Automation and Control Systems (IACS) |
| Испания | El Centro Nacional de Protección de Infraestructuras Críticas | El Plan Nacional de Protección de Infraestructuras Críticas |
| ОАЭ | UAE Cybersecurity Council | NESA IAS |
| Саудовская Аравия | National Cybersecurity Authority | OTCC Operational Technology Cybersecurity Controls |
| Турция | Ministry of Transport Maritime affairs and communications | National Cybersecurity Strategy |
| Индия | NCIIP | Guidelines for the Protection of National Critical Information Infrastructure |
| Сингапур | OTCCF.<br>CII Cybersecurity ACT | Cybersecurity code of practice for Critical information infrastructure |

# Приложение 5. Указатель соответствия Руководству GRI Standards

«Лаборатория Касперского» представляет Отчет с указанием стандартов GRI за период с 1 июля 2022 года по 31 декабря 2023 года.

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| **Общее раскрытие** | | | | |
| GRI 2-1 | Информация об организации | Наименование головной компании — холдинговая компания Kaspersky Lab Limited (зарегистрирована в Великобритании). Основное юридическое лицо в Российской Федерации — акционерное общество «Лаборатория Касперского». Штаб-квартира организации расположена по адресу: 125212, Россия, г. Москва, Ленинградское шоссе, д. 39а, стр. 2. Юридическая информация: https://www.kaspersky.ru/legal | | 6 |
| GRI 2-2 | Юридические лица, включенные в отчетность организации в области устойчивого развития | | Приложение 1 | 141 |
| GRI 2-3 | Отчетный период, периодичность и контактное лицо | Отчет об устойчивом развитии «Лаборатории Касперского» охватывает период с 1 июля 2022 года по 31 декабря 2023 года. В дальнейшем планируется публиковать отчет об устойчивом развитии ежегодно и приблизить сроки его выхода к публикации финансовой отчетности. | Приложение 8 | 163 |
| GRI 2-4 | Пересмотр данных | Пересмотра данных не проводилось. | | |
| GRI 2-5 | Внешнее заверение отчета | Внешнего заверения Отчета не проводилось. | | |
| GRI 2-6 | Деятельность, цепочка создания стоимости и другие деловые отношения | | О Компании | 4, 7, 8 |
| GRI 2-7 | Сотрудники | | Возможности для людей<br>Приложение 3 | 88<br>143 |
| GRI 2-8 | Сотрудники, которые не являются наемными работниками | Все работники являются сотрудниками «Лаборатории Касперского». | | |
| GRI 2-9 | Структура и состав управления | | Устойчивое развитие<br>Этика и прозрачность | 15<br>134–135 |
| GRI 2-10 | Выдвижение и избрание высшего органа управления | | Этика и прозрачность | 134 |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| GRI 2-11 | Председатель высшего органа управления | | Этика и прозрачность | 134 |
| GRI 2-12 | Роль высшего органа управления в обеспечении контроля над управлением воздействиями | | Устойчивое развитие | 15 |
| GRI 2-13 | Делегирование ответственности по управлению воздействиями | | Устойчивое развитие<br>Этика и прозрачность | 15–16<br>134 |
| GRI 2-15 | Конфликт интересов | В «Лаборатории Касперского» принята политика декларирования участия в иных компаниях в качестве учредителей, участников, акционеров или членов правления. Совмещение участия без согласия совета директоров или управляющего совета запрещено. Члены совета директоров и управляющего совета состоят в правлении только тех компаний, которые принадлежат Kaspersky Lab Ltd либо аффилированы с этой организацией.<br><br>В отчетном периоде случаев совмещения участия членов высших органов управления Компании в других организациях без согласия совета директоров или управляющего совета не выявлено. | | |
| GRI 2-16 | Сообщение о важнейших проблемах | | Устойчивое развитие | 15 |
| GRI 2-17 | Коллективные знания высшего руководящего органа | Для повышения информированности и компетенций высшего органа управления в вопросах устойчивого развития представители совета директоров и управляющего совета регулярно участвуют в обучающих мероприятиях с приглашением внешних экспертов. | | |
| GRI 2-18 | Оценка деятельности высшего органа управления | Регулярная оценка деятельности совета директоров и управляющего совета осуществляется собранием акционеров компании ежегодно. На основе оценки проводятся реструктуризации, улучшающие операционное управление компанией. Критерии оценки деятельности управляющих органов по вопросам надзора за управлением воздействиями организации на экономику, окружающую среду и социальную сферу в отчетном периоде не внедрялись. | | |
| GRI 2-19 | Политика вознаграждения | На момент подготовки Отчета политика вознаграждения Компании не учитывала результативность управления воздействиями Компании на экономику, социальную сферу и окружающую среду. | | |
| GRI 2-20 | Процесс определения вознаграждения | | Этика и прозрачность | 135 |
| GRI 2-21 | Годовой общий коэффициент компенсации | Информация не раскрывается в связи с ограничениями внутренней политики конфиденциальности Компании. | | |
| GRI 2-22 | Заявление о стратегии устойчивого развития | | Устойчивое развитие | 13 |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| GRI 2-23 | Стратегические обязательства | | Устойчивое развитие | 14 |
| GRI 2-24 | Внедрение стратегических обязательств | | Устойчивое развитие<br>Этика и прозрачность | 14<br>136 |
| GRI 2-25 | Процессы устранения негативных воздействий | | Этика и прозрачность | 129, 136 |
| GRI 2-26 | Механизмы для получения консультаций и выражения озабоченности | | Этика и прозрачность | 129, 136 |
| GRI 2-27 | Соблюдение законов и нормативных актов | В отчетном периоде в «Лаборатории Касперского» не было зафиксировано случаев несоблюдения законодательства и нормативных требований; на Компанию не налагались штрафы или иные виды ответственности за нарушение законодательства. | | |
| GRI 2-28 | Членство в ассоциациях | | Устойчивое развитие<br>Приложение 2 | 14<br>142 |
| GRI 2-29 | Подход к взаимодействию с заинтересованными сторонами | | Устойчивое развитие | 21 |
| GRI 2-30 | Коллективные договоры | В «Лаборатории Касперского» нет практики коллективного договора по причине отсутствия запроса от сотрудников. | | |
| **Существенные темы** | | | | |
| GRI 3-1 | Процесс определения существенных тем | | Устойчивое развитие | 19 |
| GRI 3-2 | Список существенных тем | | Устойчивое развитие | 20 |
| **Непрямые экономические воздействия** | | | | |
| GRI 203-1 | Инвестиции в инфраструктуру и безвозмездные услуги | | Киберустойчивость<br>Возможности для людей | 32–34, 37, 40<br>99–101 |
| **Противодействие коррупции** | | | | |
| GRI 205-1 | Деятельность организации, прошедшая оценку рисков, связанных с коррупцией | | Этика и прозрачность | 136 |
| GRI 205-2 | Информирование о политике и методах противодействия коррупции и обучение им | | Этика и прозрачность | |
| GRI 205-3 | Подтвержденные случаи коррупции и предпринятые меры | | Этика и прозрачность | |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| **Энергия** | | | | |
| GRI 302-1 | Потребление энергии внутри организации | | Окружающая среда | 77 |
| GRI 302-4 | Сокращение энергопотребления | | Окружающая среда | |
| **Водные ресурсы** | | | | |
| GRI 303-1 | Ответственное управление водными ресурсами как ресурсами общего пользования | Территории расположения офисов Компании не относятся к регионам водного стресса. | Окружающая среда | 79 |
| GRI 303-2 | Управление воздействиями, связанными со сбросами воды | | Окружающая среда | |
| GRI 303-3 | Водозабор | | Окружающая среда | |
| GRI 303-4 | Водоотведение | | Окружающая среда | |
| GRI 303-5 | Потребление воды | | Окружающая среда | |
| **Выбросы** | | | | |
| GRI 305-1 | Прямые выбросы парниковых газов (область охвата 1) | Методика сбора данных и расчета общего количества прямых выбросов парниковых газов по всем объектам Компании (область охвата 1) в процессе разработки, данные будут представлены в последующих отчетах. | | |
| GRI 305-2 | Непрямые энергетические выбросы парниковых газов (область охвата 2) | Методика сбора данных и расчета общего количества косвенных выбросов парниковых газов от энергопотребления (область охвата 2) в процессе разработки, данные будут представлены в последующих отчетах. | | |
| GRI 305-5 | Сокращение выбросов парниковых газов | | Окружающая среда | 76 |
| GRI 305-6 | Выбросы озоноразрушающих веществ (ОРВ) | Неприменимо. Выбросы ОРВ Компания не производит. | | |
| GRI 305-7 | Выбросы в атмосферу NOx, SOx и других значимых загрязняющих веществ | Неприменимо. Выбросы указанных загрязняющих веществ в атмосферу Компания не производит. | | |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| **Отходы** | | | | |
| GRI 306-1 | Образование отходов и связанные с ними существенные воздействия | | Окружающая среда | 81–84 |
| GRI 306-2 | Управление существенными воздействиями, связанными с отходами | | Окружающая среда | |
| GRI 306-3 | Образование отходов | | Окружающая среда | |
| GRI 306-5 | Удаление и захоронение отходов | | Окружающая среда | |
| **Занятость** | | | | |
| GRI 401-1 | Число новых работников и текучесть кадров | | Возможности для людей<br>Приложение 3 | 88<br>143 |
| GRI 401-2 | Льготы, предоставляемые сотрудникам, работающим на условиях полной занятости, которые не предоставляются сотрудникам, работающим на условиях временной или неполной занятости | | Возможности для людей | 92 |
| GRI 401-3 | Отпуск по уходу за ребенком | | Возможности для людей<br>Приложение 3 | 92<br>149–150 |
| **Здоровье и безопасность на рабочем месте** | | | | |
| GRI 403-1 | Система управления вопросами охраны труда и промышленной безопасностью | Система менеджмента охраны труда и здоровья во всех офисах «Лаборатории Касперского» в границах раскрытия в Отчете соответствует требованиям действующего трудового законодательства на территориях присутствия Компании. Она включает в себя регулярные инструктажи сотрудников и проведение регулярной специальной оценки рабочих мест во всех подразделениях, систему управления рисками и расследования несчастных случаев, а также организацию мероприятий по улучшению условий труда. Ключевым показателем эффективности является отсутствие травм на рабочем месте. | | |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| GRI 403-2 | Выявление опасностей, оценка рисков и расследование происшествий | За отчетный период в Компании не зафиксировано несчастных случаев, связанных с реализацией профессиональных рисков. | Возможности для людей | 96 |
| GRI 403-4 | Вовлечение работников, консультации и коммуникации по вопросам охраны труда и промышленной безопасности | | Возможности для людей | |
| GRI 403-5 | Обучение работников, связанное с вопросами охраны труда и безопасности на рабочем месте | | Возможности для людей | |
| GRI 403-6 | Профилактика и охрана здоровья работников | | Возможности для людей | |
| GRI 403-8 | Работники, охваченные системой управления вопросами охраны труда и промышленной безопасностью | | Возможности для людей | |
| GRI 403-9 | Производственный травматизм | | Возможности для людей | |
| GRI 403-10 | Профессиональные заболевания | В отчетном периоде в «Лаборатории Касперского» не зафиксировано случаев профессиональных заболеваний. | | |
| **Обучение и образование** | | | | |
| GRI 404-1 | Среднегодовое количество часов обучения на одного работника | | Возможности для людей | 91 |
| GRI 404-2 | Программы повышения квалификации работников и поддержки карьерных изменений | | Возможности для людей | 90–91 |
| GRI 404-3 | Доля сотрудников, для которых проводятся периодические оценки результативности и развития карьеры | | Возможности для людей | 89 |
| **Разнообразие и равные возможности** | | | | |
| GRI 405-1 | Разнообразие состава органов управления и структуры персонала | | Возможности для людей<br>Приложение 3 | 95<br>143–150 |
| GRI 405-2 | Соотношение базовой заработной платы и вознаграждений у мужчин и женщин | | Приложение 3 | 150 |
| **Недопущение дискриминации** | | | | |
| GRI 406-1 | Случаи дискриминации и принятые меры | В отчетном периоде случаев дискриминации не выявлено. | | |

| Индикатор | Название раскрытия | Комментарий | Раздел Отчета | Стр. |
|---|---|---|---|---|
| **Детский труд** | | | | |
| GRI 408-1 | Операции и поставщики, подверженные значительному риску случаев детского труда | Компания не использует детский труд и не принимает на работу сотрудников младше 18 лет. | | |
| **Принудительный или рабский труд** | | | | |
| GRI 409-1 | Операции и поставщики, подверженные значительному риску случаев принудительного или рабского труда | Компания не использует принудительный и рабский труд. | | |
| **Местные сообщества** | | | | |
| GRI 413-1 | Подразделения с реализованными программами взаимодействия с местными сообществами, программами оценки воздействия деятельности на местные сообщества и программами развития местных сообществ | | Возможности для людей | 97–101 |
| **Защита данных клиентов** | | | | |
| GRI 418-1 | Обоснованные жалобы и выявленные утечки персональных данных клиентов | | Этика и прозрачность | 127 |

# Приложение 6. Указатель соответствия Руководству SASB Standards

Соответствие элементов отчетности отраслевому Руководству SASB Software and IT Services, версия 2018-10 (TC-SI)

| Индикатор | Информация к раскрытию | Раздел Отчета | Примечания | Стр. |
|---|---|---|---|---|
| **Экологический след инфраструктуры** | | | | |
| TC-SI-130-a.1 | 1. Общее потребление энергии.<br>2. Процент сетевой электроэнергии.<br>3. Процент возобновляемой энергии | Окружающая среда | | 77 |
| TC-SI-130-a.2 | 1. Общий водозабор.<br>2. Общее потребление воды и процент каждого показателя в регионах водного стресса или с резким дефицитом воды | Окружающая среда | | 79 |
| TC-SI-130-a.3 | Учет экологических аспектов при стратегическом планировании потребностей дата-центров | Окружающая среда | | 78 |
| **Конфиденциальность персональных данных и свобода самовыражения** | | | | |
| TC-SI-220-a.1 | Описание политик и практик, касающихся таргетированной рекламы и конфиденциальности персональных данных пользователей | Окружающая среда | | 128–130 |
| TC-SI-220-a.2 | Количество пользователей, информация о которых используется во вторичных целях | | Таких пользователей — 0 (ноль). | |
| TC-SI-220-a.3 | Общая сумма денежных убытков, возникших в результате судебных разбирательств, связанных с нарушением конфиденциальности пользователей/клиентов | | В отчетном периоде таких случаев не было, сумма убытков — 0 (ноль). | |

| Индикатор | Информация к раскрытию | Раздел Отчета | Примечания | Стр. |
|---|---|---|---|---|
| TC-SI-220-a.4 | 1. Число запросов государственных органов на получение информации о пользователях.<br>2. Число пользователей, информация о которых была запрошена.<br>3. Процент пользователей, информация о которых была раскрыта | Этика и прозрачность | 1. Политика описана в соответствующем разделе Отчета. Число запросов государственных органов можно найти в регулярном отчете «Лаборатории Касперского» Law Enforcement & Government Requests Report. Последний отчет был опубликован за второе полугодие 2023 года.<br>2. Такую статистику Компания не ведет, мы учитываем только количество запросов на предоставление данных пользователей и неперсональной технической информации.<br>3. 0% — «Лаборатория Касперского» пока не предоставляла такие данные государственным органам. | 123–126 |
| TC-SI-220-a.5 | Список стран, в которых основные продукты или услуги подлежат государственному мониторингу, блокировке, фильтрации контента или цензуре | | Таких стран нет. | |
| **Безопасность данных** | | | | |
| TC-SI-230-a.1 | 1. Число утечек данных.<br>2. Процент утечек, касающихся персональных данных пользователей.<br>3. Число пострадавших пользователей | Этика и прозрачность | | 130 |
| TC-SI-230-a.2 | Описание подхода к выявлению и устранению рисков безопасности данных, включая использование сторонних стандартов кибербезопасности | Этика и прозрачность | | 128–130 |
| **Наем и управление квалифицированными кадрами со всего мира и их социокультурное разнообразие** | | | | |
| TC-SI-330-a.1 | Доля сотрудников, которые:<br>1. Являются иностранными гражданами.<br>2. Работают из-за границы | | 1. В «Лаборатории Касперского» на 31 декабря 2023 года работали 64 иностранных гражданина, что составляет 1,5% от общего количества сотрудников. По другим региональным офисам информация в отчетном периоде не собиралась.<br>2. К «Лаборатории Касперского» неприменимо, так как российское трудовое законодательство не подразумевает работу за пределами Российской Федерации. По офисам вне России информация в отчетном периоде не собиралась. | |
| TC-SI-330-a.2 | Вовлеченность сотрудников | Возможности для людей | | 95 |
| TC-SI-330-a.3 | Процент представленности обоих полов и расовых/этнических групп:<br>1. Среди руководства.<br>2. Среди технического персонала.<br>3. Среди всех остальных сотрудников | Возможности для людей | Компания не ведет статистику по этническим группам сотрудников. | 95, 116 |

| Индикатор | Информация к раскрытию | Раздел Отчета | Примечания | Стр. |
|---|---|---|---|---|
| **Защита интеллектуальной собственности и конкурентное поведение** | | | | |
| TC-SI-520-a.1 | Общая сумма денежных убытков, возникших в результате судебных разбирательств, связанных с защитой интеллектуальной собственности и недобросовестной конкуренцией | Этика и прозрачность | | 132 |
| **Управление системными рисками технологических сбоев** | | | | |
| TC-SI-550-a.1 | Количество:<br>1. Проблем с производительностью.<br>2. Перебоев в обслуживании.<br>3. Общего времени простоя для клиентов | | Информация не раскрывается в связи с ограничениями внутренней политики конфиденциальности Компании. | |
| TC-SI-550-a.2 | Описание рисков, связанных с обеспечением бесперебойной работы систем | Этика и прозрачность | | 137–139 |
| **Показатели деятельности организации** | | | | |
| TC-SI-000.A | 1. Количество лицензий или подписок.<br>2. Процент облачных технологий | | 1. 851.<br>2. 33% облачных. | |
| TC-SI-000.B | 1. Возможности обработки данных.<br>2. Доля аутсорсинга | | 1. 240 узлов в локальной сети и 7 372 узла на аутсорсинге.<br>2. 97% аутсорсинга (коллокация). | |
| TC-SI-000.C | 1. Объем хранилища данных.<br>2. Доля аутсорсинга | | 1. Не менее 100 ПБ.<br>2. Более 91% аутсорсинга (коллокация). | |

# Приложение 7. Глоссарий

| | |
|---|---|
| **Alt-текст** | Краткое описание изображения для помощи при поиске |
| **APT** | Целевая кибератака (англ. Advanced Persistent Threat) |
| **HR** | Человеческие ресурсы (англ. Human Resources) |
| **IoT** | Интернет вещей (англ. Internet of Things), коллективная сеть подключенных устройств и технологии, которая облегчает связь между устройствами и облаком, а также между самими устройствами |
| **Kill Chain** | В кибербезопасности термин Kill Chain («цепь уничтожения») описывает последовательность этапов, которые киберпреступники проходят при попытке осуществить успешную кибератаку |
| **LMS** | Система управления обучением (англ. Learning Management System) |
| **MOOC** | Массовые открытые онлайн-курсы (англ. Massive Open Online Courses), одна из современных форм дистанционного образования |
| **ROI** | Коэффициент рентабельности инвестиций, который помогает рассчитать окупаемость вложений в проект (англ. Return on Investment) |
| **XDR** | Класс систем информационной безопасности, предназначенных для расширенного обнаружения и реагирования на сложные угрозы и целевые атаки (англ. Extended Detection and Response) |
| **Аддитивные технологии** | Метод создания трехмерных объектов, деталей или вещей путем послойного добавления материала |
| **АСУ ТП** | Автоматизированная система управления технологическим процессом |
| **Билдер** | Инструмент, который позволяет настраивать параметры вредоносного программного обеспечения перед его использованием в кибератаке (англ. Builder) |
| **Вендор** | Поставщик, который продает и продвигает товары и услуги под собственным брендом или торговой маркой (англ. Vendor) |
| **Конечные точки, конечные устройства** | Физические устройства, которые подключаются к компьютерной сети и обмениваются с ней данными (мобильные устройства, настольные компьютеры, виртуальные машины, встроенная аппаратура или серверы) |
| **Нейроморфный процессор** | Процессор, принцип работы и архитектура которого имеют сходство с нейронными сетями живых организмов |
| **ПГ** | Парниковые газы, газообразные вещества природного или антропогенного происхождения, которые поглощают и переизлучают инфракрасное излучение |
| **Реверс-инжиниринг** | Обратная разработка кода — это процесс анализа машинного кода программы, который ставит своей целью понять принцип работы, восстановить алгоритм, обнаружить недокументированные возможности программы и т. п. (англ. Reverse Engineering) |
| **Решения MDR** | Решения для автоматического обнаружения и анализа инцидентов безопасности в инфраструктуре с помощью телеметрии и передовых технологий машинного обучения (англ. Managed Detection and Response) |
| **Стейкхолдеры** | Заинтересованные стороны, лица, которые имеют интересы относительно проекта или организации либо влияют на проект или организацию (англ. Stakeholders) |
| **Техническая атрибуция** | Процесс определения или выявления идентификационных данных, позволяющих идентифицировать или связать конкретного злоумышленника, группу злоумышленников или страну-источник с определенной кибератакой или киберинцидентом |
| **Уникальный пользователь** | Пользователь, который за определенный промежуток времени (как правило, в течение суток) посетил интернет-ресурс |
| **Фреймворк** | Набор правил, шаблонов и инструментов, использующихся для построения продуктов или процессов (англ. Framework) |
| **Эксплойт** | Вредоносный код, который использует ошибки или недостатки системы безопасности для распространения киберугроз (англ. Exploit) |
| **Эксфильтрация данных** | Процесс, во время которого злоумышленник извлекает конфиденциальные данные из системы другого компьютера и использует их для личных целей |

# Приложение 8. Контактная информация

GRI 2-3

По всем вопросам, связанным с Отчетом об устойчивом развитии, обращайтесь к **Марии Лосюковой, руководителю проектов устойчивого развития**:

Maria.Losyukova@kaspersky.com

**Почтовый адрес центрального офиса:**

125212, Россия, г. Москва,
Ленинградское шоссе, д. 39а, стр. 3,
БЦ «Олимпия Парк»,

+7 (495) 797-87-00,
+7 (495) 737-34-12

**Сайт Компании:**
www.kaspersky.com

**Для общих вопросов:**
info@kaspersky.com

**Контактная информация:**
https://www.kaspersky.ru/about/contact

**Контакты для прессы:**
empr@kaspersky.com