kaspersky bring on the future

Building a safer world

Kaspersky's Sustainability Report for 2021 and the first half of 2022

Content

3 A message from Eugene Kaspersky

4 About the company

10 Sustainable development

21 Defining the main topics

26 **Global Transparency Initiative:** how and why we revealed our code and processes

34 **Users:** how we protect personal data and ensure privacy

42 **Ethical practices:** how we're increasing our management transparency and business resilience

50 **Critical infrastructure:** how we protect it in a changing world

61 **Fighting cybercrime:** how we work together with law enforcement

69 **Security in cyberspace:** how we protect our users against cyberworld threats

80 **Ecological footprint:** how we are reducing our impact on the environment

91 **Team:** how we take care of our employees

103 **Women in STEM:** how we attract them to IT and thereby attempt to reduce the gender gap

112 **Education:** how we educate specialists in information security

120 Annexes

152 Contacts and Feedback

“Increasing resilience against cyberthreats through the creation of Cyber Immunity”

GRI 2-22

Eugene Kaspersky
CEO of Kaspersky

This is our first sustainability report, prepared in accordance with the international GRI and SASB standards. In it, we go over our sustainable development strategy, our results for 2021 and the first six months of 2022, and the company’s key objectives for 2023. The report demonstrates how we implement sustainable development principles in our company’s business processes, and why this is particularly important now that the whole world is facing new challenges.

Our company’s mission is to build a safe and sustainable digital world so that people can use technological solutions to improve not only their day-to-day lives but also life on the planet as a whole. We go about fulfilling this mission by increasing the resilience of the digital space against threats through the creation of “Cyber Immunity”, while paying special attention to social projects and environmental awareness.

For some time now, the company has been a lot more than just a developer of antivirus software. In the 25 years since the company was founded, we have grown from a small group of like-minded individuals into a global firm with offices all over the world, protecting over 400 million users with our cybersecurity software and services. Besides the wide range of protective solutions we develop, we also organize educational initiatives – from those teaching the basics of cybersecurity, to training courses for highly-skilled developers. And we protect the Internet of Things and nurture the concept and development of smart cities, all the while working on building a Cyber Immune future based on our secure KasperskyOS operating system. In this report you will discover how we go about doing all this, and learn of some of the successes we have already had.

We have distinguished five key areas of the company’s sustainable development: Providing and maintaining **cyber-resilience** is our main objective, given that we have decades of expertise in protecting users against cyberthreats, protecting critical infrastructure, and assisting in cybercrime investigations. As to the other four sustainable development areas, we feel more of a connection to them on the level of the company’s values and culture. These include: **ethics and transparency, people empowerment,** and **future tech**. For instance, we focus a lot of attention on protecting and processing users’ personal data; hence, we feel it is our duty to share our expertise and take part in establishing uniform standards for the whole industry in these matters. An example of this is how we were the first in the cybersecurity industry to open up Transparency Centers all over the world (there are already nine of them). These centers store the source code of our products and allow it to be reviewed at any given time. Finally, **safer planet** is an area in which we plan to do a lot more in order to further reduce our ecological impact.

Our company collaborates with more than 10 non-profit organizations and charity funds worldwide. We provide financial aid, promote pro bono volunteering among our employees, and organize educational initiatives.

The company shows stable annual growth in sales, revenue and number of clients. For example, in 2021 our consolidated revenue under IFRS increased by 6.5% compared to 2020. This is a reassuring indication that more and more people trust our products and technologies.

The most important thing for us is to make the world around us a safer, better place. Both 2021 and 2022 were by far from easy years given the after-effects of the pandemic and the aggravated geopolitical situation, respectively. Yet despite such challenging circumstances, we still have ambitious plans for 2023. While working on these, we intend to remain a socially-responsible company and maintain the trust of our users, partners and employees. We believe that a Cyber-Immune future can and will become the Cyber-Immune present.

About the company

GRI 2-6

Kaspersky is an international company providing reliable information security based on advanced analytical data. Eugene Kaspersky founded the company in 1997 in Russia.

Kaspersky today:

400 million
users across
200 + countries

240 000
corporate
clients

>4 500
experts within
the company

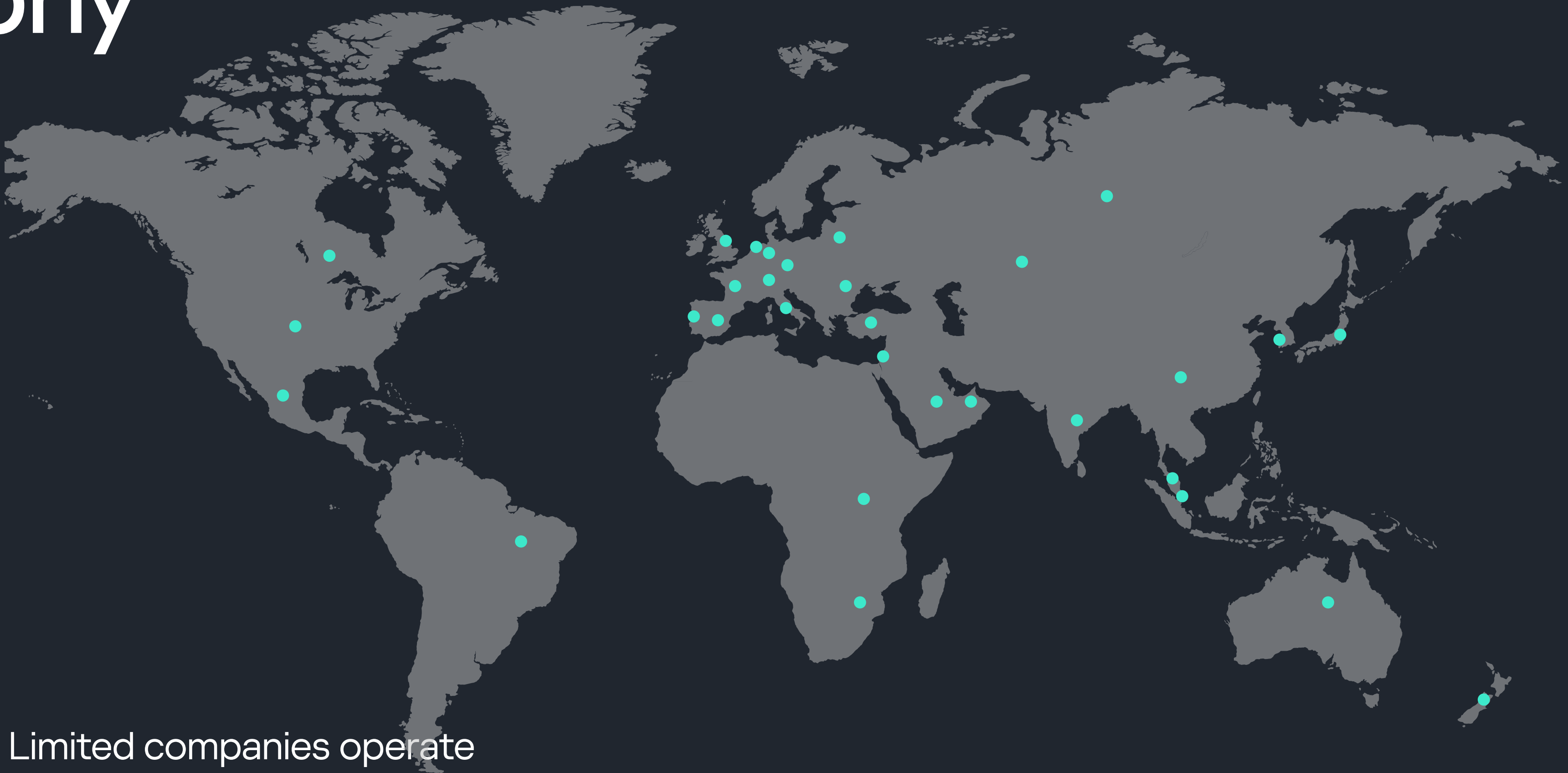
27
products for homes
and businesses

Our mission: to build a safer world.

Geography

GRI 2-6

Kaspersky's corporate group structure is made up of the holding company — Kaspersky Labs Limited — registered in the United Kingdom, and its subsidiary companies, registered all over the world. The group is comprised of private companies based in the UK, Russia, Switzerland, Germany, France, the U.S.A., and China, among other countries. We have more than 30 offices in six business regions across the globe.



Where Kaspersky Labs Limited companies operate

CIS countries
Russia
Belarus
Kazakhstan

META countries
Turkey
UAE
South Africa
Saudi Arabia
Rwanda

Latin America
Brazil
Mexico

Europe
UK
Switzerland
France
Germany
Netherlands
Israel
Czech Republic
Spain
Italy
Portugal
Romania

Asia-Pacific
China
Japan
Australia
New Zealand
Singapore
South Korea
India
Malaysia

North America
U.S.A.
Canada

Products

GRI 2-6

The company's portfolio includes 27 cybersecurity products that can be us in homes and businesses.* In 2021, Kaspersky products were reviewed in 741 independent tests and reviews. In 518, out of the 741 they came first place, and came second or third in a further 94 cases — 612 overall ranking in the top-three. In addition to top ranking, our products have also garnered a reputation for quality, for example, Kaspersky Endpoint Security Cloud proved 100% effective against ransomware — far more effective than all ten other vendors in the industry in a trial conducted by the independent antivirus and security software reviewer AV-TEST.

27

products in our portfolio

518

times — our products came first in independent tests conducted in 2021

94

times — our products ranked top-three in the same independent tests in 2021

Home products

Kaspersky Anti-Virus
Kaspersky Internet Security
See more: https://www.kaspersky.com/home-security

Small business products

Kaspersky Small Office Security
Kaspersky Endpoint Security Cloud
See more: https://www.kaspersky.com/small-business-security

Medium business products

Kaspersky Endpoint Security Cloud
Kaspersky Endpoint Security for Business Advanced
See more: https://www.kaspersky.com/small-to-medium-business-security

Enterprise products

Kaspersky Anti Targeted Attack Platform
Kaspersky Embedded Systems Security
See more: https://www.kaspersky.com/enterprise-security

* The list of products includes security solutions presented at kaspersky.ru and kaspersky.com. These products are provided under a large number of licenses that meet the needs of various customers (more than 1.500 items in total on the company's price list).

Business results

GRI 2-6

Financial results report for 2021. The financial results report for 2022 will be published in the next sustainability report.

$752 000 000

global unaudited revenue in 2021 under IFRS
an increase of 6.5% compared to 2020

↑

+19%

sales growth in B2B

↑

+29%

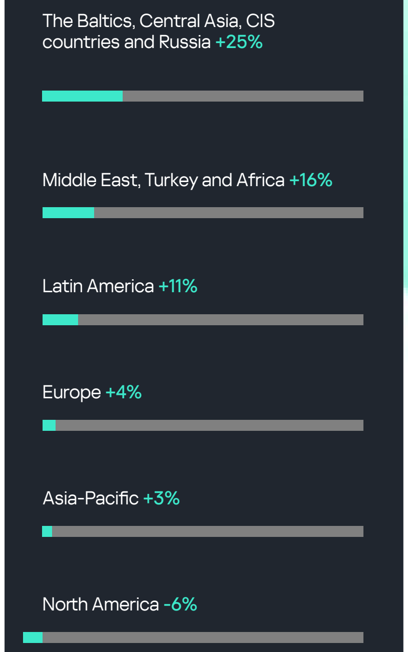
sales growth in the enterprise sector

↑

+50%

sales growth in non-endpoint – new innovative solutions and technologies to protect companies from complex cyberthreats

Sales across our business regions in 2021*, %



* All figures on sectors and regions refer to net sales rather than revenue, and are represented in fixed rates as of 2021.

Social investment

> $590 000

total amount of charitable donations during the reporting period

1 180

licenses for security products issued free of charge to private users with special needs or those undergoing hardship

2 407

licenses for our products granted free of charge to NPOs and charity funds

Notable moments

2021

1 We upgraded TinyCheck to detect geo-tracking apps. Initially developed as a stalkerware detection tool for organizations working with victims of domestic violence, TinyCheck now also helps uncover all types of geo-tracking apps.

2 We became one of the partners in the European DeStalk project. This EU-wide project aims to fight gender-based cyberviolence and stalkerware.

3 We marked five years of successfully fighting ransomware. In 2016, Kaspersky launched the international No More Ransom initiative in collaboration with Europol and other international law enforcement agencies. In the five years since its inception, we have prevented more than $900 million in illegal profits from being obtained from six million users who downloaded our free decryption tools.

4 We published our first transparency report. Kaspersky publicly shared information about the requests for information received from government and law enforcement agencies as well as private users.

5 We helped fundraise over $110,000 for prosthetic care for people who underwent amputation by joining the Climbing for Range of Motion initiative.

6 We made our software bill of materials (SBOM) available to both customers and partners. Kaspersky provides, upon request, a list of our software components, known as a software bill of materials, which helps clients and partners understand what is inside the company's products and software architecture.

7 Together with INTERPOL and other organizations we conducted two online training sessions to address the issue of digital stalking. More than 200 participants attended.

8 We acquired the company Brain4Net, allowing us to develop our XDR platform using SASE technologies to provide both Enterprise and SMB organizations with natively-integrated cross-product solutions.

9 We prepared our suggestion on how to protect supply chains as part of the Paris Peace Forum. The analytical report was drafted in cooperation with Cigref and GEODE. It represents concrete steps to be taken by, inter alia, governments, international organizations and market participants in order to increase security and effectiveness in regulating information and communication technology supply chains.

2022

1 We became a majority shareholder in the company MyOffice – increasing our share in the company's capital to 61.05%. MyOffice provides software solutions for enterprise, the public sector, academia, as well as individual users.

2 We successfully renewed our SOC 2 audit. The independent international assessment reaffirmed that the development and release process for Kaspersky's antivirus databases are protected against unauthorized changes.

3 We opened Transparency Centers in Japan, Singapore, and the United States. The centers provide the required information on software development documentation and the source code pertaining to the company's key product portfolio to corporate clients and state agencies responsible for cybersecurity.

4 We invested in the development of neuromorphic processors. Kaspersky became a 15% shareholder in Motive Neuromorphic Technologies, a company specializing in neuromorphic computing technologies. Together, the companies will develop machine learning solutions, and create self-learning systems and smart devices.

Sustainable development

GRI 2-22 GRI 2-23 GRI 2-24

Both the security and the resilience of cyberspace are essential for the sustainable development of modern day societies. And yet, cyberattacks and other threats undermine attempts at reaching all of the UN's 17 Sustainable Development Goals. How do we stay on track toward realizing our company's mission of building a safe and sustainable digital world during this especially disruptive period, while simultaneously attempting to reduce our ecological footprint and investing in a solution for social problems? This is the fundamental question underlying our Environmental, Social and Governance (ESG) sustainable development strategy.

kaspersky bring on the future

ESG strategy

The company’s **five key sustainable** development strategies are the following:

1

Ethics and transparency

- Source code transparency and process transparency
- Data protection and the right to privacy
- Management transparency and business resilience

2

Safer cyberworld

- Critical infrastructure protection
- Assistance in the investigation of cybercrimes on a global level
- Protection of users against cyberthreats

3

Safer planet

- Reducing the environmental impact of our infrastructure, business activities and products

4

People empowerment

- Employee care
- Women in STEM
- Inclusivity and availability of technologies
- Talent development in IT

5

Future Tech

- Cyber Immunity for new technologies

Where we are now: objectives and key results

Ethics and transparency

Objective 1

Increase management transparency and business resilience

Where we are now:

0
court rulings against the company, employees or partners regarding violations of anti-corruption laws

100%
of patent actions filed against our company in the U.S.A. successfully defended in court over the course of 17 years

141
patents for our products obtained by Kaspersky in 2021; 76 in the first six months of 2022

$10 million
The company was able to save $10 million in 2021 as a result of tenders and contract cost optimization

Learn more

Objective 2

Eliminate Kaspersky users' personal data leaks

Where we are now:

2 252
requests for personal data processing were handled by the company in 2021; 3285 in the first half of 2022

>800
More than 800 of the company's employees immediately involved in personal data processing operations completed an internal advanced course on personal data management

0
major violations of personal data legislation

Learn more

Objective 3

Build users, customers and other stakeholders' trust in Kaspersky

Where we are now:

$5.6 million
Kaspersky has invested $5.6 million in building its data infrastructure in Switzerland since 2018. User data from Europe, North and Latin America, the Middle East, and also several countries in Asia-Pacific

6
Since 2020, six government organizations have taken our special Cyber Capacity Building Program training course on assessing software's credibility

53
We have received 53 reports on minor vulnerabilities since March 2018, for which we have paid a total of $75,750 in bug bounties

in 2018
In 2018, our first Transparency Center was opened in Zurich, where stakeholders can review the company's source code. As of the end of 2022 we have Transparency Centers operating throughout the world, including three new ones opened during the reporting period

Learn more

A Safer (Cyber) World

Objective 1

Protect users against cyberthreats with Kaspersky's products and initiatives

Where we are now:

>1.5 million

More than 1.5 million users around the world were able to decrypt their data thanks to the No More Ransom anti-ransomware initiative co-founded by Kaspersky

+34%

2021 saw a revenue growth of 34% for ASAP, while in the small and medium business segment growth reached 66%. Meanwhile, demand for our cyber-education products continues to grow year on year

>750 000

Over 750.000 people from 24 Russian cities attended our webinars on internet safety for children

Learn more

Objective 2

Protect critical infrastructure by creating state-of-the-art IT technologies and services

Where we are now:

>100

More than 100 KasperskyOS-based pilot projects were launched by Kaspersky in Russia in 2021, and in 2022 we started releasing our first pilots in the Middle East. The projects mainly cater to the metallurgy, oil and gas, mechanical engineering, and metalworking industries, as well as government institutions and educational establishments

>150 000

More than 150.000 licenses and certificates for all products and services included in the Kaspersky Industrial Cybersecurity solution have been purchased by industrial companies from almost 50 countries worldwide since 2015

Learn more

Objective 3

Assist international and national law enforcement agencies in cybercrime investigations

Where we are now:

>114 million

More than 114 million unique malicious URLs were registered by our web-based antivirus from November 2020 to October 2021

>687 million

More than 687 million attacks launched from internet resources located in various countries worldwide were thwarted by Kaspersky's solutions from November 2020 to October 2021

>64.5 million

More than 64.5 million unique malicious objects were blocked by Kaspersky's web-based antivirus from November 2020 to October 2021

~30

During the reporting period, Kaspersky participated in around 30 joint cybersecurity events with stakeholders all over the world

Learn more

A cleaner planet

Objective

Reduce the environmental impact of all our activities

Where we are now:

81%

Kaspersky reduced its carbon emissions by 81% from 2019 to 2021 after cutting down on air travel from 5 085 flights in 2019 to 1 460 in 2021

50%

less physical media sales of Kaspersky products in favor of digital products from 2021–2022

8.14

out of 172.4 tons of Class IV waste was recycled in 2021 — 2.56 out of 218.2 tons in the first half of 2022

50%

We use up to 50% less water per month at our Moscow office since replacing the water supply system sensors

Learn more

People empowerment

Objective 1

Ensure our employees' physical and mental wellbeing in conjunction with their professional development

Where we are now:

52.3%

In 2022, our global "employee net promoter score" (eNPS), which measures employee satisfaction, increased by 6.7 percentage points compared to 2021, reaching 52.3%

6.7

training hours per company specialist were completed in addition to compulsory training

>40%

More than 1762 employees (40% of the total) spent a total of 28,508 hours taking optional training courses

>67.9 million

More than 67.9 million rubles were invested by Kaspersky in external courses and participation in conferences for employees during the reporting period

578 630

rubles raised by Kaspersky employees for the benefit of the charity funds Sindrom Lubvi, Vera, and Zhivi as part of our corporate fundraising from January 1, 2021 to June 30, 2022

Learn more

Objective 2

Contribute to achieving gender equality in the field of IT

Where we are now:

26%

of employees at Kaspersky are women, there is 17% of women in our development team

>17 000

The online community Women in CyberSecurity, created by Kaspersky, now has more than 17 000 members

>600

More than 600 downloads of three episodes of the Women in Tech podcast in France, featuring Kaspersky's female employees sharing their professional and personal experiences of working in the field and with the company

Learn more

Objective 3

Train cybersecurity personnel and raise the professional level of our IT specialists

Where we are now:

>4.8 million

Over 4.8 million Russian-speaking school students attended the Digital Lesson during the reporting period

25

students started work at Kaspersky's European and Singapore offices under the company's global internship program launched in 2021

>6 000

Over 6 000 students from all over the world have taken part in our Secur'IT Cup competition in four years, winners having received grants in the amount of $10.000

>100

More than a hundred new customers from 30 countries took training courses on cybersecurity via the Kaspersky Expert Training portal during the reporting period. The highest demand for the training came from Israel, Singapore and the U.S.A.

>100

Kaspersky.Academy is partnered with more than a hundred universities in 71 countries

Learn more

Objective 4

Increase the accessibility of information about our security products, services and capabilities to people with special needs

This objective is not covered as a main theme in this report. The topic is one of our strategic priorities, but we are still only in the initial phase; we will cover it in more depth in one of our future reports.

Future Tech

Objective

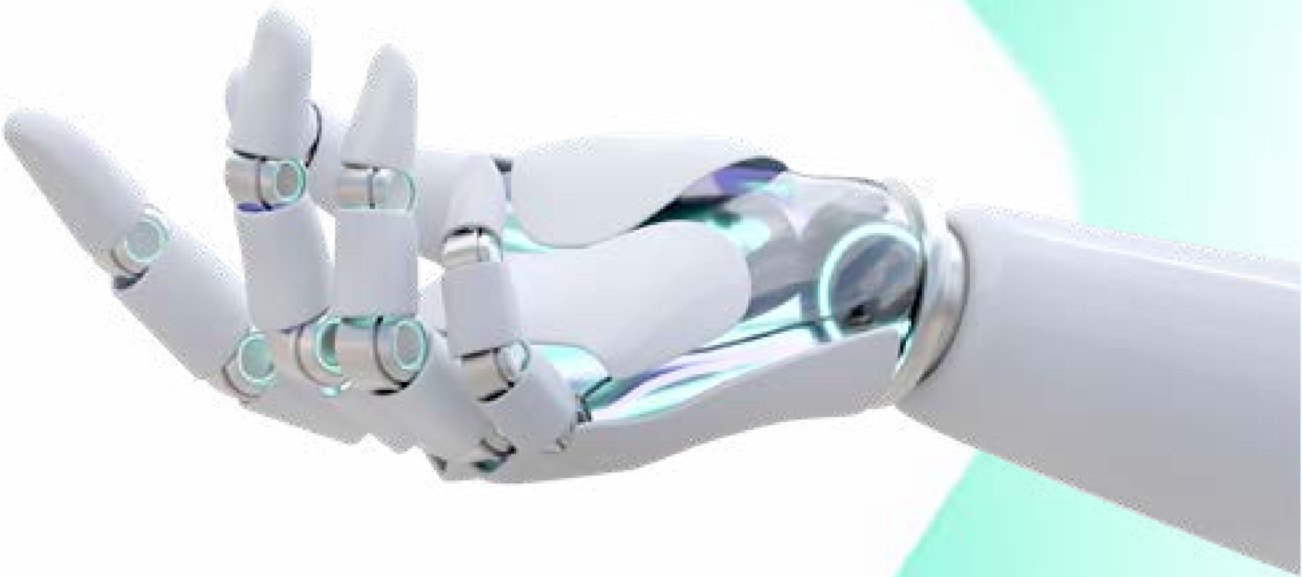
Onboard new partners to implement our Cyber Immunity strategy

Where we are now:

1 memorandum

During the reporting period, Kaspersky signed a memorandum on end-to-end cooperation involving Rosatom and the "Trusted Platform" Association. Its goal is to develop cyber immune products for Rosatom

Learn more



Our contribution to achieving the UN’s SDG

Our key sustainable development goal is to create a safe and stable digital space, without which the realization of the UN’s 17 Sustainable Development Goals (SDG) would be compromised. We simultaneously highlight several SDGs that some of our specific ESG initiatives are focused on in particular.

4	Quality education
5	Gender equality
7	Affordable and clean energy
8	Decent work and economic growth
9	Industry, innovation and infrastructure
10	Reduce inequality
12	Responsible consumption and production
13	Climate action

Read more about Kaspersky’s sustainable development goals, programs and initiatives and how they contribute to specific UN SDGs — here.

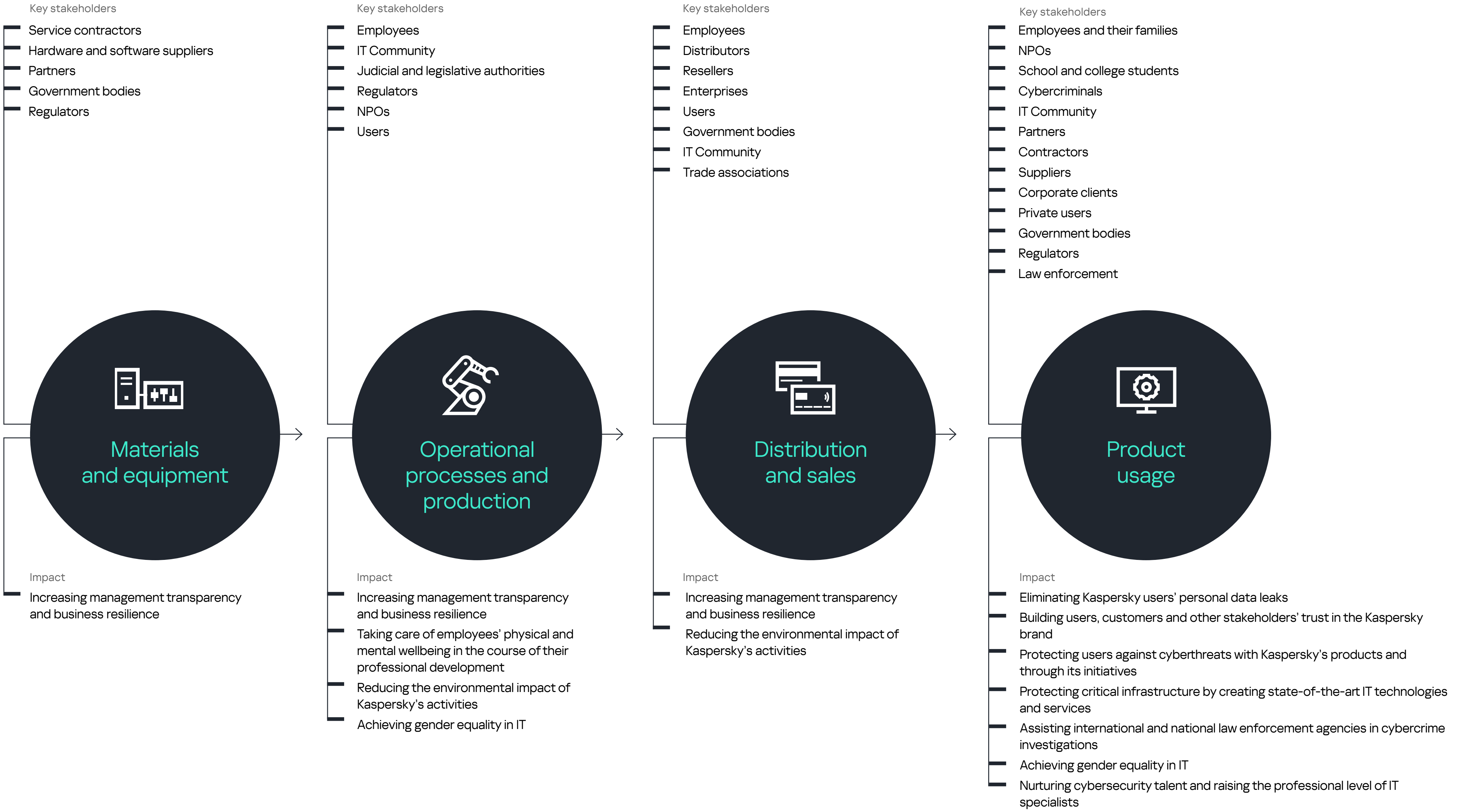
Stakeholder engagement

GRI 2-29

Kaspersky's stakeholders are employees, users, partners, suppliers, government bodies, law enforcement agencies, local communities, and the vulnerable in terms of information security (e.g., children and their parents, and people who may have suffered or are still suffering from cyberstalking). We organize our stakeholder relations taking into account the particular needs and opinions of each of the groups throughout the value creation chain.

Kaspersky’s value creation chain

GRI 2-6 GRI 2-29



Materials and equipment

Key stakeholders

- Service contractors
- Hardware and software suppliers
- Partners
- Government bodies
- Regulators

Impact

- Increasing management transparency and business resilience

Operational processes and production

Key stakeholders

- Employees
- IT Community
- Judicial and legislative authorities
- Regulators
- NPOs
- Users

Impact

- Increasing management transparency and business resilience
- Taking care of employees’ physical and mental wellbeing in the course of their professional development
- Reducing the environmental impact of Kaspersky’s activities
- Achieving gender equality in IT

Distribution and sales

Key stakeholders

- Employees
- Distributors
- Resellers
- Enterprises
- Users
- Government bodies
- IT Community
- Trade associations

Impact

- Increasing management transparency and business resilience
- Reducing the environmental impact of Kaspersky’s activities

Product usage

Key stakeholders

- Employees and their families
- NPOs
- School and college students
- Cybercriminals
- IT Community
- Partners
- Contractors
- Suppliers
- Corporate clients
- Private users
- Government bodies
- Regulators
- Law enforcement

Impact

- Eliminating Kaspersky users’ personal data leaks
- Building users, customers and other stakeholders’ trust in the Kaspersky brand
- Protecting users against cyberthreats with Kaspersky’s products and through its initiatives
- Protecting critical infrastructure by creating state-of-the-art IT technologies and services
- Assisting international and national law enforcement agencies in cybercrime investigations
- Achieving gender equality in IT
- Nurturing cybersecurity talent and raising the professional level of IT specialists

Managing sustainable development

GRI 2-12 GRI 2-13 GRI 2-24

Our sustainable development management system is only just taking shape: for the rest of 2023, our management structure is going to include a committee on sustainable development.

At the time of writing, the responsibility for managing the company's social, economic and environmental impact lies with the Head of Corporate Communications, Mr. Denis Zenkin. Impacts related to a specific topic are handled by the heads of the respective functions — interviews with whom are presented in each thematic block of this report. Kaspersky's board of directors, management board and its Chief Executive Officer are actively involved in pushing the sustainable development agenda via regular conferences, discussions and meetings. While a key indicator assessment system is yet to be developed, this is another objective we are working on for 2023.

Sustainable development risks

GRI 2-24

Managing sustainable development risks at Kaspersky is the duty of the company's senior executive officers and department managers. We try to minimize risks in all aspects of our company's activities. We have so far identified three key risks:

1. **Changes in the political and economic sphere in the regions of our presence, as well as legislative changes.** We monitor the introduction of new laws and the political situation of said regions to try and avert any setbacks that might affect the company's operations.

2. **Supply chain disruptions.** Due to the aggravated geopolitical situation at present, we have been forced to look for alternative logistics structures, as well as new partners and products to replace those that have withdrawn from the Russian market.

3. **Rise in cybercrime.** Under current conditions, international cooperation with law enforcement agencies has been put on hold. We nevertheless endeavor to maintain this cooperation to prevent a surge in cybercrime.

Defining the main topics

GRI 3-1

To be covered in the present ESG report for 2021 and the first half of 2022

The main topics to be covered in Kaspersky's first report on sustainable development were identified using a three-stage procedure.

In the **first stage**, a working group comprised of (i) sustainability work-stream leaders, (ii) representatives of various business functions, and (iii) external experts, identified 38 aspects to be included in the ESG agenda. These aspects reflect Kaspersky's chief influences on society, the economy, as well as the environment along the full length of the value creation chain.

In the **second stage**, the same working group conducted an internal expert assessment to establish the significance of the company's aforementioned chief influences. To this end, the highlighted aspects were considered with regard to: (a) Kaspersky's strategy, (b) the aspects' significance to stakeholders, (c) international standards GRI 2021 and SASB (Software and IT Services), and (d) global sustainability practices. As a result, 24 sustainable development aspects were determined as taking priority by degree of impact.

In the **third stage**, the work-stream leaders ranked the key sustainable development aspects, and, after grouping some of the 24 prioritized aspects together, formed 11 main topics to be covered in the report for 2021 and the first half of 2022.

Defining the report's main topics

Key aspects of Kaspersky's ESG agenda

LEGISLATION
CONTRACTING PARTIES
MARKETING
OHS
EDUCATION
DATA CENTERS
CARBON FOOTPRINT
DATA
FUTURE TECH
EMPLOYEES
DONORSHIP
CONTINUITY
GTI
EQUALITY
CYBERSECURITY
EMPLOYER
RESILIENCE
ETHICS
CYBERCRIME
CRITICAL INFRASTRUCTURE
VOLUNTEERING
INCLUSIVITY
EMISSIONS
MANAGEMENT
SD
WASTE
WOMEN IN STEM
ACCESSIBILITY
ANTI-CORRUPTION
CHILDREN
SUPPORTING WOMEN
NEW PROFESSIONS
TAXES
REMOTE WORK
EQUIPMENT RECYCLING
SCIENCE

Main topics 2021–2022

GRI 3-2

	Tag	Aspect explanation	Main topic	Report coverage
1	Employer	Responsible employer practices: guidelines for hiring, retention, development and support of employees	Responsibility toward employees	Team: How we take care of our employees
2	Cybercrime	Contribution to fighting international cybercrime	Fighting international cybercrime	Fighting cybercrime: how we help law enforcement agencies in preventing threats
3	Cybersecurity	A safer digital environment: anti-stalking, anti-ransom etc.	A safer digital environment Protecting users and user data	Security in cyberspace: how we protect users from cyberworld threats
4	Critical infrastructure	Protecting the critical infrastructure of society's vital systems and enterprises	Ensuring digital and software resilience in a rapidly changing world	Cyber-resilience: how we protect industrial objects in a changing world
5	GTI	Global Transparency Initiative: promoting programs on transparency (of both source code and processes) in global markets	Process transparency	Global Transparency Initiative: how we opened up our source code and processes
6	Equality	Equal opportunities and human rights: providing equal opportunities to employees around the world and supporting social and cultural diversity	Responsibility toward employees	Team: How we take care of our employees
7	Management	Increasing corporate management transparency	Ethics and transparency in business and corporate management	Ethical practices: how we are increasing management transparency and business resilience
8	Resilience	Software and digital resilience under sanctions	Ensuring digital and software resilience in a changing world	Cyber-resilience: how we protect industrial objects in a changing world

GRI 3-2

	Tag	Aspect explanation	Main topic	Report coverage
9	Continuity	Uninterrupted operation of the company's activities despite new geopolitical reality	Ensuring digital and software resilience in a changing world	Cyber-resilience: how we protect industrial objects in a changing world
10	Data	Protecting users' personal data	Protecting users and user data	How we protect personal data and ensure privacy Security in cyberspace: how we protect users from cyberworld threats
11	Waste	Responsible waste management; our aim for zero waste	Reducing our ecological footprint	Ecological footprint: how we are reducing our impact on the environment
12	Sustainable development	Sustainable development management within the company structure and all along the value creation chain	Ethics and transparency in business and corporate management	Ethical practices: how we are increasing management transparency and business resilience
13	Carbon footprint	The carbon l footprint from our business operations, and its reduction	Reducing our carbon footprint	Carbon footprint: how we are reducing our impact on the environment
14	Emissions	Combating climate change by reducing greenhouse gas emissions	Reducing our carbon footprint	Carbon footprint: how we are reducing our impact on the environment
15	Women in STEM	Self-development support and opportunities for women in technology-oriented professions — focusing on women in the software development field	Women in STEM	How we recruit women in STEM, and how we reduce the gender gap
16	Data centers	Using eco-friendly data centers and equipment	Reducing our ecological footprint	Ecological footprint: how we are reducing our impact on the environment
17	Volunteering	Developing volunteering practices	Responsibility toward employees	How we take care of our employees

GRI 3-2

Tag		Aspect explanation	Main topic	Report coverage
18	Children	Internet safety for kids	A safer digital environment	Security in cyberspace: how we protect users from cyberworld threats
19	Accessibility	Digital inclusion: increasing accessibility of information about security products, services and capabilities to individuals with special needs	Not included as a main topic in this report. This subject is one of our strategic priorities, but we are just starting on this path and will cover it more fully in one of our future reports	
20	Education	Educational activities in the cybersecurity field	Educational activities in the cybersecurity field	Security in cyberspace: how we protect users from cyberworld threats
21	Future Tech	Future tech: contributing to the development and security of groundbreaking technologies	Future tech	Future tech: how we are contributing to the world of the future
22	OHS	Occupational Health and Safety	Responsibility toward employees	How we take care of our employees
23	Anti-corruption	Zero tolerance policy on corruption	Ethics and transparency in business and corporate management	Ethical practices: how we are increasing management transparency and business resilience
24	Employees	Cultivating professionals for the information security field	Educational activities in the cybersecurity field	Education: how we educate specialists in information security

Aspects not included in the report

25	**New professions**	Developing new professions in the information security field
26	**Legislation**	Improving cybersecurity laws
27	**Supporting women**	Supporting women within the company (from maternity leave to female leadership opportunities)
28	**Ethics**	Ethical business practices and business conduct
29	**Marketing**	Responsible marketing
30	**Donorship**	Blood donorship
31	**Taxes**	Kaspersky as a high tax rate contributor
32	**Fostering talent**	Recruitment, development and support of talented specialists all over the world
33	**Inclusivity**	Developing an inclusive society in the digital environment
34	**Culture**	Initiatives supporting cultural projects
35	**Remote work**	Improving remote work security
36	**Equipment recycling**	How we recycle equipment in an effort to reduce our ecological footprint
37	**Science**	Supporting academic science
38	**Contracting parties**	Selecting contracting parties in consideration of social and environmental responsibility criteria

Global Transparency Initiative

How and why we revealed our source code and processes

kaspersky bring on the future

Proven. Transparent. Independent.

Our goal

To build users, customers and other stakeholders' trust in Kaspersky

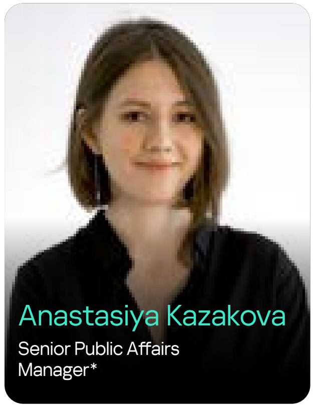
Key tasks

Develop more transparency of the company's processes in both data management and product development, and increase trust in its business processes through specific measures of the Global Transparency Initiative

Raise transparency and disclosure standards in the cybersecurity industry to enhance protection against cyberthreats

Three questions regarding the GTI

GRI 3-3


Anastasiya Kazakova
Senior Public Affairs Manager*

1

What problems can be solved using using the GTI?

Kaspersky's Global Transparency Initiative came about in response to enquiries from regulators in the company's key markets about how our products work, how data is processed, where data is stored, and so on. Since 2017, we have therefore been working on a package of measures to increase both our clients and partners' trust in our solutions. The package includes Transparency Centers, audits by independent experts, and a project to relocate part of the company's file processing infrastructure to data centers in Switzerland. Even at the very start of the project, we realized that the question of regulators' trust was starting to emerge across the cybersecurity industry in general — something that concerned other software developers too. That's why we started improving the GTI and, by extension, our approach to transparency and the disclosure of our internal and overall processes in both development and data handling, as well as our overall business processes. Since this time the company has developed a range of best practices in working with transparency, allowing us to raise the level of trust in our products with regulators, clients and customers, partners, and other organizations around the world.

2

How does the GTI work?

The Global Transparency Initiative represents a set of measures that help Kaspersky ensure the transparency of its products and both internal and business processes. This enables clients, external stakeholders, partners and regulators to be able to quickly have any of their questions answered regarding the source code of our flagship products or our data handling principles. At the same time, our employees are able to understand precisely what we need to improve on in terms of our processes being both open and mature, without compromising on security. Our goal is to ensure all our users and stakeholders feel they can trust Kaspersky's products.

3

How will the GTI grow?

Regulation of the cybersecurity field is gaining momentum, as is customers' maturity; more and more often they want to know how safe the solutions they use really are, and how the technologies are developed. So it was inevitable that programs like the Global Transparency Initiative have emerged. Rather than the price or design of any technology, buyers (ENT/B2B clients) prioritize their trust in it: where it is developed and by whom; what data will be collected and for what purposes, and how the customer can control this process. Ensuring a technology's transparency is now the developers' responsibility. We were among the first in the industry to launch such an initiative, which has allowed Kaspersky to be at the forefront of these changes. Our main aim now is to keep promoting the GTI, which requires a careful approach to both external and internal communications. To many people, the GTI is only associated with the Transparency Centers; however, it is important for us to illustrate that the GTI encompasses a whole set of measures.

* The position is specified for the period from 2021 to 2022.

Greater openness regarding internal processes through six key areas of the GTI

TC-SI-220-a.4

Our internal understanding of the GTI is continually evolving, meaning projects featured in this initiative have also emerged gradually. The first of such projects involved data relocation, then came the Transparency Centers, and after that we introduced independent security and reliability assessments of developmental processes. Next we added certification for our data management systems, then our program for handling vulnerabilities in our products and increasing the rewards for pointing out such vulnerabilities. Finally, we launched the educational Cyber Capacity Building Program and transparency reports.

$5.6 million

Kaspersky has invested $5.6 million in building its data infrastructure in Switzerland since 2018. User data from Europe, North and Latin America, the Middle East, and also several countries in Asia-Pacific

1 Data relocation

In 2018, the company started relocating its file processing and storage by transferring part of the data we receive from our users to two data centers in Switzerland, to better ensure its cybersecurity. This is a country with high-quality infrastructure in place, many technology companies with considerable capacity operate there, and its data protection legislation is one of the strictest in the world. Moreover, its historical reputation as a neutral state is especially critical in times of heightened geopolitical tensions.

2 Transparency Centers

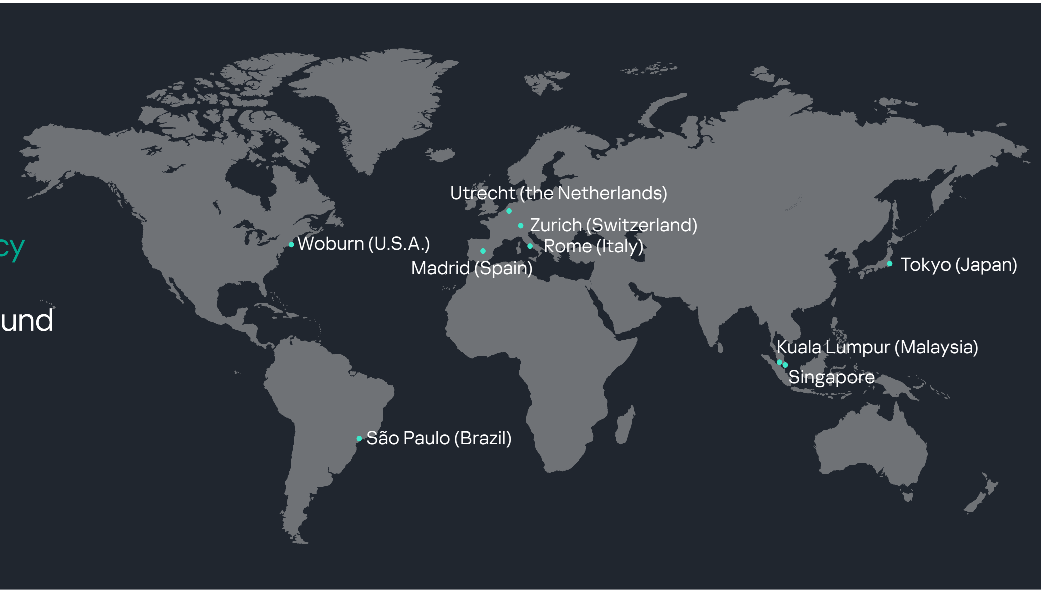
Our Transparency Centers house information about our data management and provide access to the source code of our solutions. In 2018, when our company first launched the GTI, we were the world's first information security vendor that made its source code available for review. At our Transparency Centers, customers can access all documentation concerning the development of our solutions. From 2018 through to September 2022, we opened nine Transparency Centers all over the world, including three during the reporting period.

We also provide access to the source code of our corporate products: consumer solutions, solutions for the enterprise segment, and a control console supporting all our enterprise products. At our Transparency Centers experts can moreover gain access to all software updates to analyze them for any backdoors* or hidden functionality.

Our Transparency Centers are also platforms for our company's experts to disclose our internal policies, how Kaspersky's internal processes work, and how we ensure cybersecurity. Our source code can be reviewed by enterprise customers and partners, as well as representatives of state agencies responsible for cybersecurity. We do not provide access to law enforcement or government entities that might use this information for purposes unrelated to ensuring cybersecurity.

When developing these centers, we expected the main stream of interested parties to come from regulators, but, as it turned out, regulators did not have as much interest as did other stakeholders. On the whole, regulators know how to inspect solutions for security, whereas enterprise clients and partners tend not to have the necessary expertise to review code, yet they wish to understand how our solutions work. Therefore since 2019 it has been enterprise clients and partners for whom we have arranged most visits to our Transparency Centers.

Nine Transparency Centers operate around the world



>35

More than 35 visits to our Transparency Centers, including remote ones, were organized from 2018 to December 2022

3

Three Transparency Centers — in Tokyo, Singapore, and Woburn — were unveiled during the reporting period

* A deliberately made code error that gives an attacker unauthorized access to a device with administrator privileges.

3 Independent assessment

To verify the security of Kaspersky's products, clients asked the company to provide them with relevant, internationally recognized certificates issued by an independent, accredited body. When developing the GTI measures, we worked on the following assumption: we must find an external organization to review the code, certify it, and deliver a verdict on whether the product is secure.

However, in the course of this process, we learned that no such organizations or general standards on certification appear to exist in the cybersecurity industry, mostly since this is a relatively new field, and one undergoing rapid development. So we decided we should arrange an audit ourselves, with a little help from independent auditors, and focus on data infrastructure and the process of developing and distributing virus databases. Following on from this, since 2019 our data management systems undergo regular certification for compliance with the international ISO/IEC 27001:2013 standard, and we also regularly take a SOC 2 audit with one of the Big Four accounting firms to review our process of developing and distributing virus databases.

In 2022

we successfully completed certification for data infrastructure (ISO 27001) and a SOC 2 audit in order to verify the security of our process for developing and distributing virus databases

4 Vulnerability handling program

In 2016 we launched a bug bounty program, rewarding anyone who might inform Kaspersky of any vulnerabilities identified within its systems. The reward for the most critical type of vulnerabilities is currently $100,000.

53

Since March 2018 we have received 53 reports on minor vulnerabilities, and to date have paid a total of $75.750 in rewards. This amount includes $15.800 paid for 13 reports identifying 43 bugs from January 2021 to July 2022

5 Educational Cyber Capacity Building Program

This program is aimed at government entities, universities and small companies that want to develop procedures and skills for assessing the IT products they use. Our experts talk about how to review the code*, how to build vulnerability handling processes, and how to fuzz test code . This is part of our commercial portfolio, which has already been utilized by several government bodies. Currently, most requests are coming from the APAC region, where the issue of developing competences is particularly pressing. The most recent training was held in August 2022 for an APAC government cybersecurity agency. Overall, our partners have praised the program's relevance and value.

6

Since 2020, six government bodies have taken our special Cyber Capacity Building Program to develop skills in assessing software's trustworthiness

6 Transparency reports

Our mission is to protect users from cyberthreats, which is why we support our partners, international organizations, and law enforcement agencies in fighting cybercrime. We regularly handle incoming requests, and have been publishing reports every six months since 2020 featuring in what jurisdictions such requests originate, how many of them have been complied with, and how many have been denied. Our company also has an internal process in place for handling such requests, including, in particular, clearly defined criteria for legal review.

Twice a year, Kaspersky discloses the number of requests from police to provide information on user data, expertise, and technical information for the investigation of threats. At the same time, we never grant access to our company's infrastructure, including data management infrastructure, to any third parties**. The same system applies for reports in which we disclose information on requests from our own users concerning their personal data; how we handle them, where they are stored, and so on.

* Fuzzing is a software testing technique that involves providing deliberately invalid data, analyzing the software's reaction, and thereby detecting errors.
** More detailed information on our request handling principles is available in our transparency reports.

Raising transparency and disclosure standards in the industry

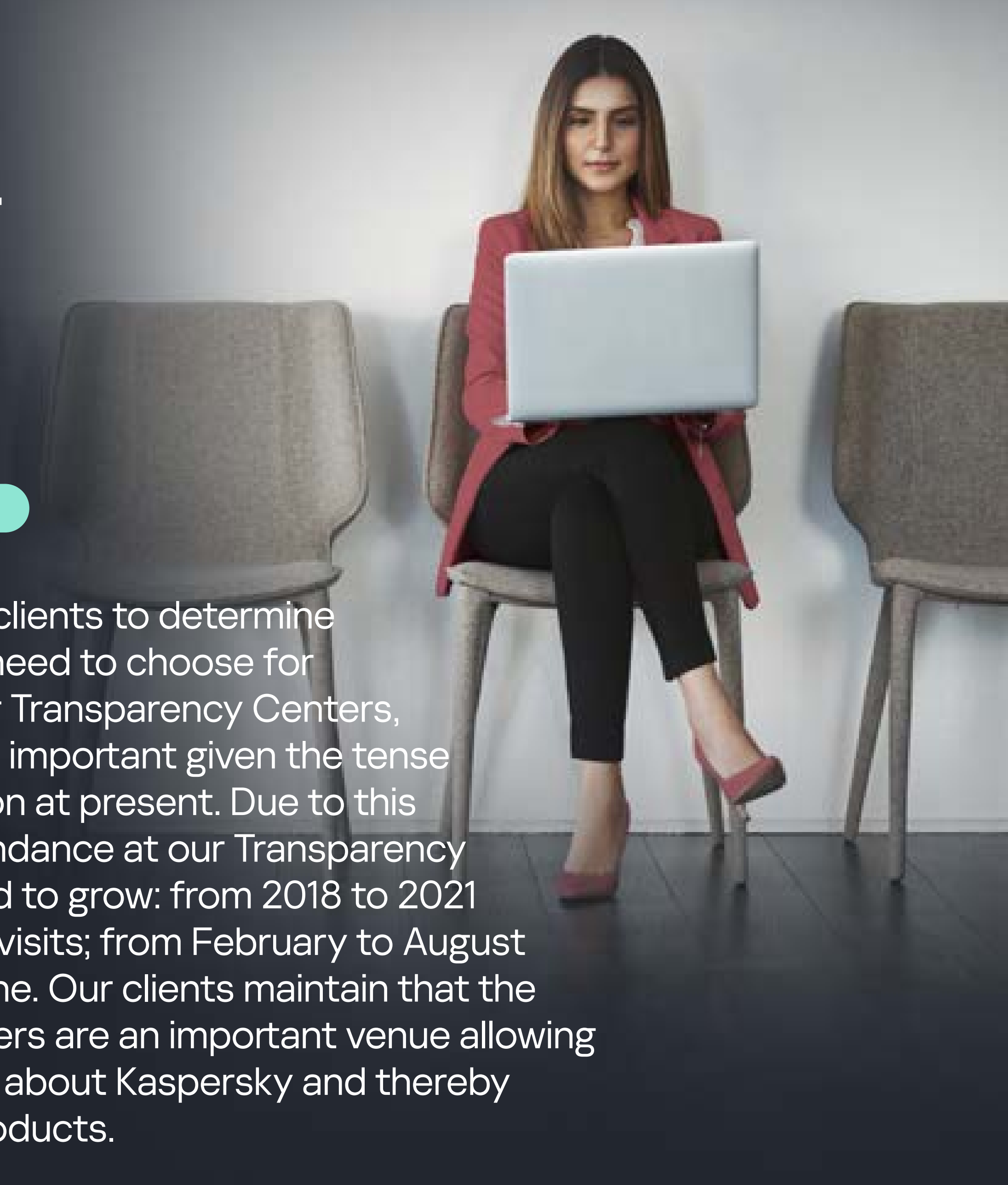
Due in no small part to the GTI, our company takes part in state-led and international initiatives on security in the digital environment on a regular basis.

These include, for example, the Geneva Dialogue initiated by the Swiss government, and the Paris Call, an initiative of the French government. Meanwhile, a report by the French National Assembly of June 2, 2021 mentions the GTI as a positive private-sector initiative for ensuring the security of digital products and services throughout their life cycle and supply chain.

Kaspersky's open data is widely used in academia, particularly by European scientists researching the openness of IT products.

Kaspersky's plans for 2023

- Open three new Transparency Centers; continue to regularly update our transparency reports; and again undergo audits and certifications to verify the safety and reliability of both our processes and systems.



Sustainable development in action

How we teach our clients to analyze solutions for trustworthiness through our Transparency Centers

Our goal

To build users, customers and other stakeholders' trust in Kaspersky

In 2018, when our company opened its first Transparency Center in Zurich, our first clients did not really understand how to make use of them. It became apparent that organizations tend to lack the competence and knowledge required for in-depth analysis of a software solution to assess the level of trustworthiness of such solutions. So to help clients determine which visit-option is most suitable and relevant to them, we put together a menu for our Transparency Centers consisting of three levels.

What was the outcome?

It is now easier for clients to determine which option they need to choose for a visit to one of our Transparency Centers, which is particularly important given the tense geopolitical situation at present. Due to this simplification, attendance at our Transparency Centers has started to grow: from 2018 to 2021 the centers saw 31 visits; from February to August 2022 there were nine. Our clients maintain that the Transparency Centers are an important venue allowing them to learn more about Kaspersky and thereby better trust our products.

Users

How we protect personal data and ensure privacy

kaspersky bring on the future

Our goal

To comply with all personal data protection regulations, and to ensure the highest level of data security processing

GRI 418-1

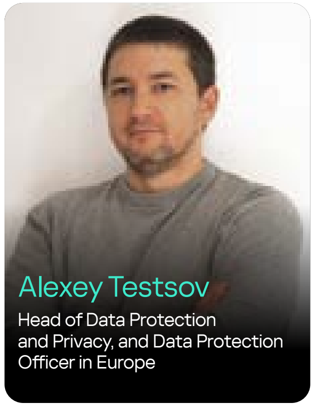
Key objectives

Provide the highest level of personal data protection for our users worldwide using robust internal security systems and procedures

Ensure our users are informed about the company’s approach to data security, and promptly provide information regarding the processing of their personal data

Reduce any possible risks to personal data processed by the company

Three questions regarding Kaspersky's personal data protection approach


Alexey Testsov
Head of Data Protection and Privacy, and Data Protection Officer in Europe

GRI 3-3

1

How does Kaspersky ensure personal data protection?

Protecting personal data is a key aspect of any company's corporate responsibility. For us, it means protecting processed personal data on a global level. As a software developer, we need to process data, in some cases including personal data, to be able to supply our products, but also in order to improve those products as well as services, and thereby live up to our clients' expectations. Personal data protection is a continuous process covering protection of personal information* against any potential unauthorized modification, compromise or loss. To this end, we take all necessary technical and organizational steps toward ensuring this, such as using pseudonymization** or data encryption. In all data transfers occurring via unsecured channels, we encrypt the data using strong encryption mechanisms and various protection tools to prevent unauthorized access to it.

2

What documents and other requirements does the company abide by to ensure the protection of personal data?

The main document is the EU's General Data Protection Regulation GDPR, which prescribes key technical and organizational measures for personal data protection. The GDPR is acknowledged as the reference in other jurisdictions also. The European requirements form the basis of our internal approach to the protection of personal data. In 2016 the company established its internal Privacy Team consisting of experts from different departments responsible for ensuring the company's compliance with privacy regulations, data security standards, and other relevant security requirements. For instance, one such security standard is the ISO/IEC 27001 international information security standard, whose requirements the company applies to its IT systems.

3

How effective is Kaspersky's approach in ensuring personal data protection?

We do everything in our power to ensure personal data protection. Thankfully, during the reporting period we experienced neither major personal data violations nor personal data leaks. This attests to the success of continual employee education. In 2021, we overhauled our internal training course for employees on personal data protection and privacy, and we also standardized our personal data protection approach worldwide to ensure that the company's requirements with regard to the processing and protection of personal data are uniform and also conform to the laws of each country where Kaspersky operates. In addition, we adhere to a policy of maximum transparency, and publish up-to-date information in response to requests from both government agencies and personal users in various countries. We provide the most up-to-date information, including the number of requests from subjects in our transparency report. This report is publicly available and is updated and published every six months.

* Personal data is any information related to a person, including their name, telephone number, home address, IP address, email address, etc.
** Pseudonymization is a means of processing personally identifiable information in such a way that the data cannot be attributed to a specific data subject without using further, separately stored information.

Ensuring personal data protection for our users worldwide

Over the last six years since the GDPR came into force in 2016, the company has developed an internal culture of responsible handling of personal data and its protection — based primarily on the EU's key principles regarding personal data protection and privacy.

Kaspersky's five key principles of privacy and protection of personal data

1. Personal data must be processed lawfully, and the need for its processing must be made clear in a transparent way for all data subjects.
2. Data must be collected for a specific, precise and legitimate purpose. Prior to processing, any personal data processing activities are subject to review from the legal, information security, and compliance standpoints, while technical and organizational data protection measures need to be implemented before commencing personal data collection. The Privacy Team monitors all personal data processing activities thoroughly and ensures that personal data is not used for any purposes other than collection, as stated.
3. Data needs to be limited — solely for the purpose of processing. Each set of personal data must be associated with a specific processing purpose. Any other personal data must not be collected or stored.
4. Data must be stored no longer than required for the express purpose of processing. Limited storage times are set for each personal data type and processing purpose, after which the data is anonymized (should there be a legal basis for anonymization) or securely deleted.
5. Data needs to be appropriately protected. Company employees are aware of notification procedures, and actively report potential incidents — being fully aware of the consequences and risks for the company that are likely to emerge in the case of improper data processing. We apply stringent limited access-rights controls regarding personal data processing — granting access only to those employees authorized to do so.

We don’t use data for purposes other than data collection. For example, our marketing systems keep records of marketing consents received. Incidental marketing emails sent without consent are identified, and corrective action is taken (training, user apology notifications, analysis of databases for errors).

We are currently working on creating uniform requirements worldwide for the processing of personal data so that they comply with all applicable privacy laws and regulations.

In 2019 (revised in 2021) Kaspersky elaborated a training program to raise awareness on how to properly manage users’ personal data. More than 800 people have taken the course — namely all employees globally in charge of personal data processing and ensuring the protection of personal data.

>800

employees involved in personal data processing and/or responsible for the protection of personal data have completed an internally-developed course on personal data protection and privacy

Risk assessment

Our company has implemented a risk-oriented approach to ensure protection of the personal data processed. Risk assessment is undertaken at all stages: when implementing new IT systems, when developing new products or services, and during any other stages or events involving the processing of personal data. At every stage we analyze the potential risks that may arise when processing personal data in order to minimize such risks.

Meeting the GDPR requirements and adhering to other relevant regulations and laws, as well as observing the ISO/IEC 27001 standard helps us ensure a high level of information security of the company’s systems, and thus to maintain the security of processed personal data.

Fulfilling data protection and privacy enquiries from users

Kaspersky regularly receives enquiries from its users regarding their personal data. Statistically, 90% of them are requests to delete their personal data so that they can exercise their right to “be forgotten”.

2 252

In 2021 we processed 2 252 requests, while in the first half of 2022 there were 3 285

Users sometimes also request that their data be exported, to provide information on where their personal data is stored, and/or what personal data Kaspersky processes. All such requests are approved and granted by default. To achieve maximum effectiveness and transparency, we monitor enquiries and publish the relevant statistics. In 2021 we processed 2 252 requests, while in the first half of 2022 there were 3 285 (see detailed information here). We see that the number of such requests is increasing worldwide, and we believe this is happening for two principal reasons: (i) users' increasing awareness of their rights, and (ii) tighter regulation relating to personal data protection and privacy.

Our goal is to ensure that our users are well-informed about both our personal data processing practices and our overall approach to personal data protection and privacy — so they feel they can trust us to process their personal data.

Like most companies, we also use some personal data in targeted advertising*. Such data processing activities are currently under scrutiny by legislative authorities around the world. According to the GDPR, data obtained through cookies** qualifies as **personal** data, meaning that respective norms need to be applied in the collection of that data. Tracking and collecting cookies as well as data transfers to third-party companies will decrease over time, leading to the diminished role of targeted ads. So far, this has affected how and how much we process personal data on our websites as well as how we use ad placement with third-party media. For both activities, our approach is cautious: for our various regional websites we have already implemented management systems for both cookies and trackers. These systems allow us to obtain consent from visitors to our websites prior to data processing or transfer, and they themselves can adjust the settings on what data they choose to submit to us while they are browsing.

To interact with consumers, customers and suppliers, Kaspersky has a feedback form on the company's official website:

www.kaspersky.ru/about/contact —
for Russian-speaking users
www.kaspersky.com/about/contact —
for international users

* Targeted advertising is a key marketing tool whereby users' personal data is collected via websites, apps and social networks to promote products and services.
** Cookies are small files stored on computers and devices enabling a website to store information on users'visits.

Preventing risks to personal data processing

GRI 418-1 | TC-SI-220-a.1 | TC-SI-220-a.2 | TC-SI-230-a.1 | TC-SI-230-a.2

The Kaspersky Privacy Team is responsible for the company's compliance with applicable laws and regulations to ensure personal data protection.

0

No major violations of personal data legislation or significant leaks during the reporting period

The team, initially set up in 2016, when the GDPR was adopted, now includes employees from the IT, research and development, information security, legal, and intellectual property departments. Our Privacy Team's main task is to ensure that the company's personal data protection approach adheres to all respective international standards and requirements. The team maintains constant contact with all departments of the company to provide any necessary advice and explanations, oversee policies, and manage controls.

Kaspersky's data systems are regularly certified (since 2019), for adherence to the international standard ISO/IEC 27001 to verify their high levels of protection. In 2022, the audit scope for this certification was significantly expanded so as to assess and certify more systems, and the most recent certification covers Kaspersky's data-processing services (KSN), including:

- The KSN system for secure file storage and access (KLDFS)
- The KSN system for statistical information processing (the KSNBuffer database).

The certification applies to data-processing services located in our data centers in Zurich, Frankfurt, Toronto, Moscow and Beijing.

Kaspersky's plans for 2023:

- Adjust uniform requirements and approaches to personal data protection across the company.
- Enhance integration of data protection requirements into all the company's working processes.
- Enhance the scope of the internal audits of information systems.
- Revise the training course on personal data processing taking into account changes to applicable laws.
- Organize specific campaigns to raise employees' awareness on managing users' personal data.

Sustainable development in action

How we faced a data leak and learned from our mistakes

Our goal

To reduce the number of personal data leaks

During the reporting period, our company suffered no major personal data leaks; however, it is important for us to rule out even minor incidents. In 2021 one such incident did occur, when one of our employees sent an email to 160 clients without using the blind-copy (Bcc) function. As far as GDPR is concerned, this is considered a personal data leak, as all recipients were able to see 159 email addresses of persons who may not have wished for their email addresses to be seen. As a consequence, we received around 30 responses from affected users expressing their disappointment with how Kaspersky violated their personal data privacy.

What was the outcome?

We investigated the incident and concluded that no significant harm was done to the users. Nevertheless, we notified everyone affected by the incident and offered our sincere apologies. Even such minor violations should never happen again, so the employee responsible for the leak completed an additional course on the management of customers’ personal data, and we sent an emailed memo to all employees highlighting the importance of information protection in daily operations, illustrating it with examples of potential incidents.

Ethical practices

How we’re increasing our management transparency and business resilience

kaspersky bring on the future

Our goal

To increase management transparency and business resilience

Key tasks

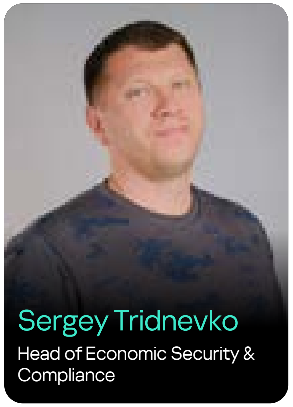
Ensure the transparency of our corporate management

Comply with the company's anti-corruption policy by preventing any violations

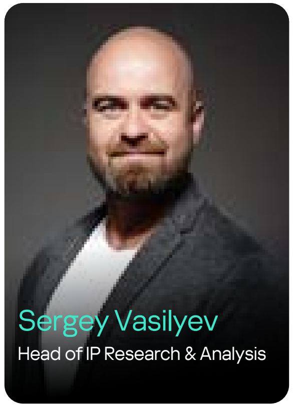
Provide a high level of legal support related to the protection of intellectual property

Mitigate risks throughout the supply chain

Three questions regarding the ethical conduct of our business


Sergey Tridnevko
Head of Economic Security & Compliance

Elena Volodenkova
Head of Procurement


Sergey Vasilyev
Head of IP Research & Analysis

GRI 3-3

1

What does the ethical conduct of business mean to Kaspersky?

— Our business is based on the principle of being open and fair to our clients, partners and competitors. We value the company's reputation and endeavor to increase management transparency in all aspects of our business activities. We intend to formalize the basic rules of business and corporate ethics in the company's code of conduct, which is currently in its initial phase.

2

What are you primarily focused on?

— Our company takes a zero-tolerance approach to corruption, and we strive to prevent any violations of the company's anti-corruption policy. To this end, all our employees take compulsory training courses on the policy, during which we highlight how each and every one of us bears responsibility for complying with it.

We apply our anti-corruption principles to our relations with suppliers, ensuring that the principles are binding by articulating them in our contracts, and we intend to supplement our tender questionnaires with an item that stipulates the counterparty must have an anti-corruption policy in place.

For the purposes of business resilience and strengthening our position as a leader in the technology industry, we ensure that our company offers a high level of legal support in the realm of intellectual property. On this note, we have not lost a single lawsuit brought against us by patent trolls in the U.S.A.

3

What challenges did you face during the reporting period?

— 2022 was not an easy year for many, nor for the company, chiefly regarding the supply chain. Many Europe-based suppliers stopped working with us since we are a company of Russian origin. Therefore, to prevent our logistics chains worldwide from collapsing, we had to look for alternatives: new suppliers, new logistical structures, and import substitution for products and components we were no longer able to acquire in Russia. Given the circumstances, we had difficulty guaranteeing previously established delivery timeframes, though we strove to reduce any risks and ensure the continued operation of the company despite the disruption.

Maintaining corporate management transparency

GRI 2-9 GRI 2-10 GRI 2-11 GRI 2-12 GRI 2-19

The company's highest governing body is its board of directors — responsible for making key decisions and adopting global policies and strategies that are implemented in all the companies within the Kaspersky group.

Candidates to the board of directors are nominated by existing board members. Our company does not have a permanent president on the board of directors. The president is elected for each board meeting, and he or she does not have any special powers and cannot simultaneously be the CEO. The board does not have any independent members — only executive directors.

Responsibility for the economic, social, and environmental impacts of sustainable development is delegated to three representatives of Denis Zenkin, Head of Corporate Communications.

The governing board of the LLC Kaspersky Group defines specific strategic and tactical steps for the purposes of the company's operating development, confirms appointments of senior managers, and defines the management structure of the corporate group.

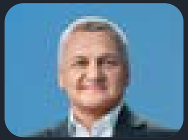
The CEO, Eugene Kaspersky, has a defining role in the company's management, since he is at once the major shareholder of the holding company, a member of the board of directors, and a member of the governing board.

The total compensation for members of the highest management body and the top managers is governed by the company's general compensation policies, and comprises three elements: fixed (salary), bonus (based on work performance), and long-term remuneration payment. The bonus is paid according to individual goal attainment in any position for the respective financial year. Long-term remuneration payments are also annual, but linked to the three-year reporting cycle, and depend on the company's overall financial results. The main calculation metrics are the EBITDA measure and the overall sales growth year-on-year. The three elements of the compensation system add up, roughly equally, to the total compensation package for top managers, which encourages both attainment of individual results and provides motivation for reaching overall corporate objectives.

Currently, the board is comprised of four persons, all of whom have had a permanent contract of employment of more than five years.

Eugene Kaspersky

sole executive of both JSC "Kaspersky Lab" and LLC "Kaspersky Group", member of the board of directors of the holding company, and member of the governing board

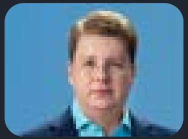


Andrey Tikhonov

member of the board of directors of the holding company, member of the governing board, and sole executive of JSC «Vodny Stadion Sport Invest»

Svetlana Ivanova

member of the board of directors of the holding company



Daniil Borschev

member of the board of directors of the holding company, member of the governing board, and member of the board of directors of LLC «Novye Oblachnye Tekhnologii»

Complying with anti-corruption policy

GRI 2-23 GRI 205-2

As an international company, Kaspersky complies with laws and regulatory requirements across the globe. The basic principles are formalized in the company's anti-corruption policy, adopted in 2012.

The policy is available on our official website and translated into the 30 languages of the regions we are present in. Some of our main principles are that we do not tolerate any form of bribery of private persons or public officials, and we never participate in any forms of unethical rewards or payments.

Compliance with the anti-corruption policy is the responsibility of a designated team consisting of a compliance officer and their regional representatives. They investigate any and all potential violations, which any employee can report to their superior, a compliance officer or their representatives, as well as through the hotline number 8-800-700-88-11 or via email at infosec@kaspersky.com. The message or call can be anonymous.

0

court orders against the company, employees or partners regarding violation of anti-corruption laws

Safeguarding and protecting intellectual property

TC-SI-520-a.1

Business resilience, openness and leadership in the hi-tech sphere are not possible without safeguarding and protecting intellectual property. That is why Kaspersky always protects its exclusive rights in the course of its intellectual activities and its means of individualization, such as with inventions, codes or trademarks. In the event of any infringement of these rights, we defend them in court.

141

patents were obtained by Kaspersky in 2021, and 76 in the first six months of 2022

The company's department for intellectual property protection was set up in 2005, and not once have we lost a patent lawsuit. In these 17 years we have established a transparent legal protection process for all kinds of intellectual activity. We not only protect our own intellectual products, we moreover neutralize risks concerning the unauthorized use of someone else's intellectual property within our own company, such as through third-party code, by checking the licenses. An important aspect of this work involves the proper training of Kaspersky's employees. All new employees are informed about intellectual property on a basic level as part of their introductory training. And within a year we intend to launch a patent-related training course for employees of Kaspersky's technical departments. Here they will learn what to watch out for when developing new products, how technologies are checked for patent purity, how patent applications are filed, and how patent rights are protected.

We are prepared for any litigation. Traditionally, most lawsuits take place in the U.S.A., and mostly at the initiative of patent trolls*. In Russia we have faced litigation with regard to antitrust laws, but have also won these cases. Our core principle is to be ready to defend our interests by all means necessary — and we never opt for out-of-court settlements.

100%

of patent actions filed against our company in the U.S.A. over the course of 17 years were successfully defended in court

In March 2022, we faced a novel challenge when the antivirus company Webroot brought a patent action against Kaspersky in the U.S.A. This was our first ever proceeding involving a direct competitor. In June, we filed a counterclaim for infringement of our patents. We estimate that the legal procedures may extend to 2025.

* A natural or legal person specializing in filing patent suits.

Reducing risks in the supply chain

GRI 2-6

Kaspersky works with more than 1300 partners all over the world. To enhance transparency when interacting with suppliers, we rely on our company's procurement policy as well as our contract policy*.

All procurement is based on categories such as marketing or IT, and is grouped according to three amount thresholds. Procurement amounts of up to $25.000 are subject to a simplified procedure where two competitive bids suffice. $25.000 to $100.000 acquisitions require at least three offers or two offers from trusted suppliers that have already been validated in the course of working with our company. Everything above the $100.000 threshold requires a tender, and involves several of the company's departments, including procurement, the tender committee, and cross-functional participants. Tender acquisitions also have their own thresholds depending on the budget. For instance, tender procedures for procurement in the amount of around a million dollars are handled by Kaspersky's business director.

Before we invite a participant to a tender, they must be vetted by our security service. We do not work with companies that have neither experience nor reputation, and 99% of our contract partners have been in the market for at least three years. In the near future we are going to add a requirement that the supplying company must have an anti-corruption policy in place too. Currently, all issues concerning compliance with anti-corruption laws are incorporated into contracts between Kaspersky and our counterparties.

Since February 2022, we have faced new challenges and risks in our interactions with suppliers:

- Mass refusals from European suppliers to cooperate with our company. To prevent our logistics chains from collapsing, we had to quickly find alternative logistical structures, new partners and procure new products.
- Our main procurement tool — the SAP Ariba platform — is not supported in Russia anymore. Within 1.5 to two years we plan to switch to a new platform, and our IT department is currently working on its implementation.

With the help of our IT team we have already set up a tender archive, which we plan to connect to our contract portal. This way we can make all tender documentation transparent and available to everyone involved in our tenders.

$10 million**

Our company was able to save $10 million in 2021 as a result of tenders, audits, and contract cost optimization

Kaspersky's plans for 2023

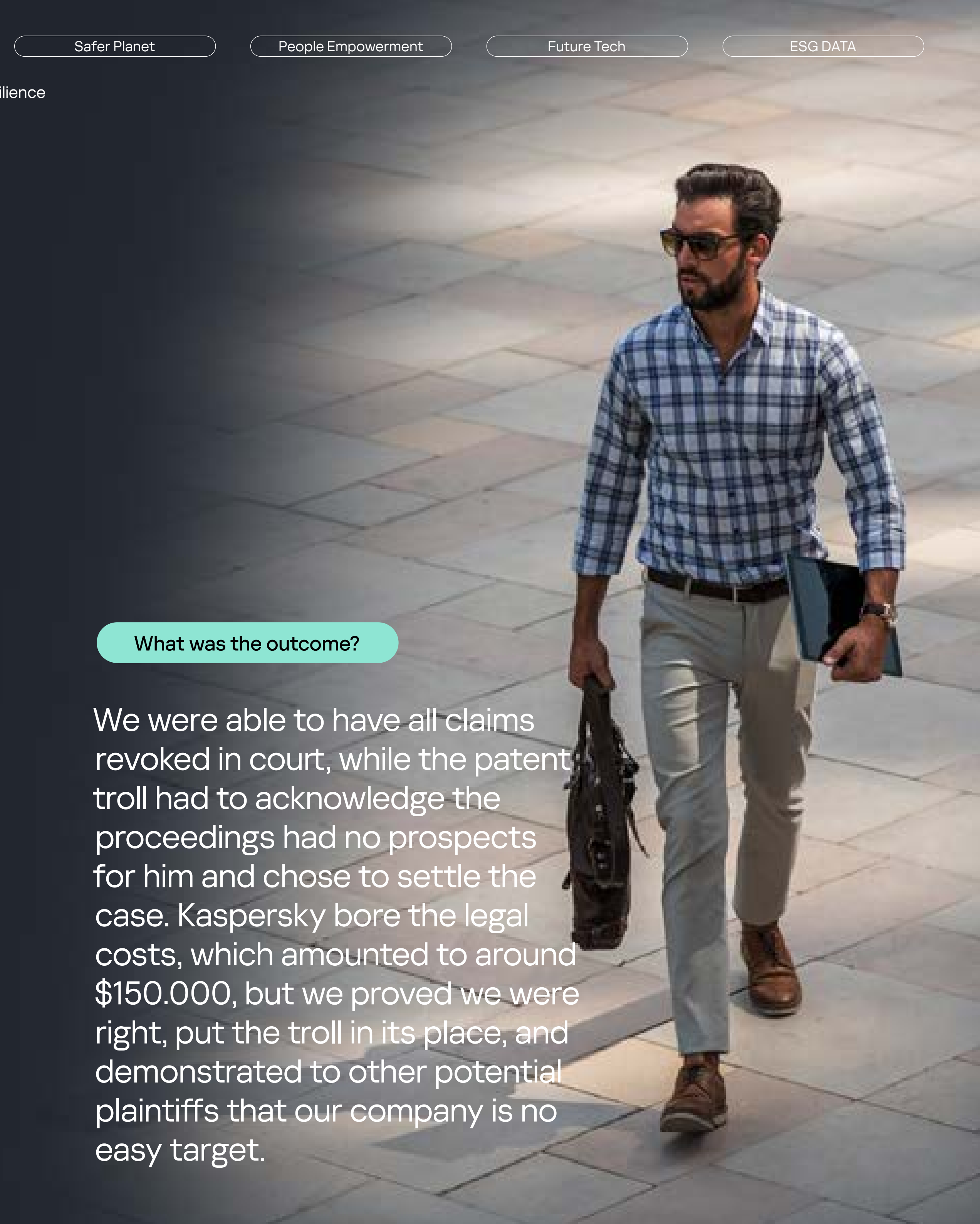
- Conduct our annual anti-corruption online training for our employees.
- Launch a patent-related training course for employees of Kaspersky's technical departments.
- Switch from SAP Ariba to a new procurement platform to ensure the stable operation of the supply chain.

* We do not publish links to policies, since these documents are classified commercial information.
** Excluding third-party costs.

Sustainable development in action

How we defeated a patent troll

TC-SI-520-a.1



Our goal

To increase management transparency and business resilience

Kaspersky frequently has to defend its rights in relation to patent lawsuits initiated by patent trolls. In April 2021, Kaspersky received a summons on a suit from the patent troll called Cybersoft IP, LLC. We estimated that in the worst-case scenario, the potential damages could amount to $500.000. The plaintiff insisted that our product – Kaspersky Secure Mail Gateway – was in violation of a network security patent that allows for checking communicated data on a user device. The patent pertains to a personal firewall-type solution implemented on a user device where network data is intercepted and scanned. Similar network-traffic filtering solutions are well-known and have been in use for a long time. The lawsuit seemed like a risky one for us at first sight. Cybersoft IP, LLC offered to close the case for $90.000 and intimidated us with litigation concerning further patents, but this is not the kind of deal our company makes. After analyzing the patent we saw that not all the elements of the patent claim were disclosed in the description, nor were they understandable to specialists, which is grounds to revoke a patent.

What was the outcome?

We were able to have all claims revoked in court, while the patent troll had to acknowledge the proceedings had no prospects for him and chose to settle the case. Kaspersky bore the legal costs, which amounted to around $150.000, but we proved we were right, put the troll in its place, and demonstrated to other potential plaintiffs that our company is no easy target.

Critical infrastructure

How we protect it in a changing world

kaspersky bring on the future

Our goal

To protect industry and critical infrastructure using an ecosystem of state-of-the-art IT technologies and services

Key tasks

Connect new partners to our Cyber Immunity strategy

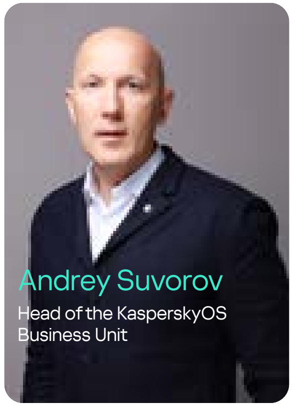
Support the digitalization of industrial sectors such as energy, metals, oil and gas, etc. through our cyber immune approach to reducing cyberattack risks

Reduce the number of incidents at our clients' industrial facilities

Reduce our company's systemic risks so as to minimize process failures

Three questions regarding critical infrastructure protection

TC-SI-230-a.2 GRI 3-3



Andrey Suvorov

Head of the KasperskyOS Business Unit

Andrew Strelkov

Head of Industrial Cybersecurity Product Line

Sergey Abramov

Director Quality Audit & Risk Assessment

1

What is critical infrastructure and why is it important to protect it?

Critical infrastructure (CI) comprises process control systems in industrial sectors of strategic importance for the economy, state institutions and society. CI is to be found in the following industries: public health, science, transportation, telecommunications, banking, fuel and energy (including atomic), defense, rocket and space, mining, metallurgy, and chemicals. A system malfunction in critical infrastructure not only halts operations, it can also cause environmental disasters or even fatal incidents.

Cyberattacks on critical infrastructure cause estimated damages of eight to ten trillion dollars annually. 2021 alone saw more than 200 incidents involving attackers halting business processes, and in the first half of 2022, malicious objects were detected and blocked on 31.8% of computers in automated control systems among our users worldwide. The tense geopolitical situation throughout most of 2022 also took its toll. For instance, in the spring, we observed increased activity among hacktivists* who attacked not only government bodies and the mass media, but also several industrial companies.

2

What is Kaspersky's contribution to infrastructure protection?

If we look at the long-term development strategies of global leaders in industry, we see two main trends: digitalization and incident prevention. We therefore endeavor to offer practical help to our clients in both these digital strategies.

Thanks to digitalization, businesses aim to get the most out of industrial data that is collected and analyzed, while at the same time it is of crucial importance to ensure that the data transfers involved for this work both correctly and securely. Kaspersky IoT Secure Gateway for the Industrial Internet of Things (IIoT) delivers on both these fronts.

We have developed a Cyber Immune methodology for the creation of IT systems, as well as our own operating system — KasperskyOS — which is a platform designed to create digital products with built-in immunity against most kinds of cyberattacks. Unlike the conventional cybersecurity model based on the "vulnerability vs. antidote" principle, the architecture of Cyber Immune solutions prevents a perpetrator from developing an attack on the system, even if a non-immune component is compromised. By default, this ensures the security of industrial systems when the device only performs needed functions but is otherwise immune to current and future threats.

To minimize information security incidents, our company is developing Kaspersky Industrial CyberSecurity. This is a platform of integrated technologies, expertise and services that can help protect all kinds of industrial systems to maintain the stability and continuity of technological processes.

Despite the maturity of many technologies in critical infrastructure, most incidents today are still the result of human error. For example, an employee might connect their personal smartphone to a SCADA machine (a system that controls technological processes) to charge it, and thereby infect the entire system. That is why Kaspersky offers a set of training courses that we have especially adapted for industrial companies and critical infrastructure facilities. One of the most recent additions to the courses is the one on Critical Information

* Hacktivism is the use of cyberattacks to raise public awareness of social, political and other issues.

Infrastructure Security in 2021: Recent Changes in the Law and Practical Realization.

We are currently working on developing an expert community on critical infrastructure protection. Meanwhile, we held the tenth Kaspersky Industrial Cyber Security Conference in Sochi, Russia, in the fall of 2022. This is an annual event bringing together national regulators, industry experts and critical infrastructure operators. This year's conference was attended by guests from the oil and gas industry of the META region, Africa's metallurgy sector, as well as representatives from the energy sector of Eastern Europe and Indian governmental authorities.

3

What results are worth noting?

Products of the KICS line protect more than 350 industrial clients and hundreds of industrial networks with more than two thousand projects. Altogether, more than 100.000 licenses were sold..

Meanwhile, Cyber Immune products based on KasperskyOS have started to prove their effectiveness in projects of the Industrial Internet of Things. The first public companies running their end-to-end digital services using Cyber Immune solutions include the Chelyabinsk Tube Rolling Plant (a member of the TMK Group), Moskabelmet Group, and Lenpoligraphmash among others.

As part of our Cyber Immunity strategy, in August 2021 we signed an end-to-end memorandum of cooperation with Rosatom and the Trusted Platform Association to co-develop industrial products with built-in protection against most kinds of threats. We also invested in the development of Russia's first neuromorphic chip. The launch and learning of neural networks consume a lot of processing power, which is why their worldwide development and application has so far stalled. Neuromorphic chips circumvent this problem, for this reason we are predicting their success.

In terms of systemic risks, our company was able to promptly address issues that arose in spring 2022, when Western companies withdrew from the Russian market. We transferred all our domains to a Russian registrar company, diversified our cloud providers in favor of Russian solutions, and purchased 49% of the shares in a Russian company that develops a digitalization solution for management control and HR processes.

Onboarding new partners for implementation of the Cyber Immunity strategy

During the reporting period, our company signed a pioneering memorandum on end-to-end cooperation involving Rosatom and the Trusted Platform Association. This document was signed as part of the Cyber Immunity approach, which our company is developing and actively promoting in the field of Future Tech.

The core of this approach is to ensure the highest level of protection of a company's infrastructure, so that an attack on that company would cost more than the amount of possible damage or financial gain to the attackers. To this end, security requirements must be designed as early as possible in the product development stage. However, this approach is not yet popular, and most companies prefer using superimposed security products*, because cyber immunity requires more investment and highly-skilled developers.

Cyber immunity is most effective when used throughout the entire technology stack**: microchip development, designing devices based on those microchips, and an operating system for the devices and apps that will work on this system. In this scenario, the final product will have the highest reliability in terms of information security — and consequently the lowest price. But this approach requires cooperation between companies from different industries. That is why the above-mentioned memorandum is so important, since it involves (i) the end user — Rosatom; (ii) the Trusted Platform, which focuses on the implementation of end-to-end trust and security technologies; and (iii) Kaspersky — as the developer of information security products. In the future we intend to implement the end-to-end security principle across Rosatom products and projects.

This is not the first joint project between Kaspersky and Rosatom. In 2021, our employees developed some of the design documentation for the Hanhikivi Nuclear Power Plant to be built by Rosatom in Finland. The department involved in this work was our ICS CERT. Its experts analyze the most urgent cyberthreats in industrial process networks and inform the community. The nuclear power plant project is currently on hold due to geopolitical tensions, but the information systems were designed in accordance with cyber immunity requirements at the earliest stages.

Kaspersky also invested in the development of Russia's first neuromorphic chip. The company concluded a cooperation agreement with Motiv NT as early as 2019 and thereafter collaborated on the development of the Altai neuromorphic processor designed to accelerate the hardware of AI systems. Testing results show that conventional graphic accelerators widely used today consume a thousand-fold more energy than Altai, making it one of the world's most power-efficient processors. This experimental success motivated Kaspersky to become, in June 2022, a shareholder of Motiv NT with a 15% share.

* Features that complement the built-in security mechanisms of operating systems, such as antivirus software.
** A stack is a set of tools used in IT projects.

Making industrial digitalization secure

The Fourth Industrial Revolution* is underway and focused on integration between production and enterprise applications. This approach has eroded the conventional information security architecture of the last 25 years, as it would normally have taken several weeks for information to make its way from production to a senior manager's desk. These days companies are shortening this process to make sure that data from industrial machinery goes straight to analytical systems and from there to the management in a matter of seconds.

However, this new approach comes with new risks. Conventional cybersecurity architecture implies that the industry uses superimposed security features**; if any vulnerability is detected within the system, the manufacturer releases a patch***, which is then either distributed to users by way of updates or sold individually. For example, when viruses emerge, antiviruses follow next. Mail phishing is counteracted with anti-phishing software. This kind of whack-a-mole is endless. With the new architecture, the conventional approach leads to high overhead costs and is hard to handle. Superimposed features put strong limitations on the rate of information transfer, which is why we believe it is the suppliers of secure-by-design solutions who have a winning hand here.

According to this secure-by-design principle, as mentioned above, we developed the Cyber Immune approach to creating IT solutions, as well as our own operating system — KasperskyOS — a platform dedicated to the development of cyber immune digital infrastructure products. To make sure that a KasperskyOS-based solution is Cyber Immune, we need to follow a specific methodology when creating it; we must clearly define the security objectives and the future operating conditions of the system. To this aim, we have to split the solutions into isolated security domains, taking into consideration the functionality of and the degree of trust in each of them, and we need to ensure the control of data flows between these domains, allowing only the prescribed types of interaction to occur.

>100

More than a hundred KasperskyOS-based pilot projects were launched by Kaspersky in Russia in 2021, and in 2022 we started releasing our first pilots in the Middle East in the metallurgy, oil and gas, mechanical engineering, and metalworking industries, as well as among government institutions and educational establishments

* A new approach to production based on the mass adoption of information technologies in industry, large-scale automation of business processes and wide-spread expansion of artificial intelligence.
** Utilities that are installed on top of operating systems and supplement built-in security mechanisms.
*** A modification to an application or software program to fix any errors and weaknesses so as to eliminate any vulnerabilities.

Kaspersky's Cyber Immune products have built-in protection: they are practically impossible to compromise in nominal operation modes, and the number of possible vulnerabilities is fundamentally minimized. And while there is no such thing as 100% security, a cyber immune IT system is practically impossible to hack into, as, effectively, nothing endangers the performance of critical functions prescribed in the design stage.

In November 2021, Kaspersky provided access to KasperskyOS Community Edition 1.0 — a consumer version of it. Its main areas of application are the Internet of Things and process control in sectors with high cybersecurity standards such as in industry, energy, state institutions and transportation.

Alongside the Internet of Things Gateway, in 2022 a Cyber Immune thin client* was added to the portfolio of KasperskyOS-based products to protect remote workplaces and build secure infrastructure. With an annual sales potential of around 100.000 thin clients over the next two to three years, we hope to secure a good market share in its market among the banking and industrial sectors, government and healthcare institutions, as well as in education. One of our first clients in this field was the Ministry for Digital Development and Communications of Orenburg Region in Russia.

Our approach to critical infrastructure protection

Estimating the production component. When dealing with CI, its most critical parts are technological installations and elements of automated industrial control systems**. These are very expensive; for instance, a blast furnace is worth over $2 million, so any downtime would cost the company much more than a hacked laptop or server. So, before proceeding with the protection, we need to define the most important production elements.

The new solution must have no impact on critical technological processes. In industry, one of the most important factors is the availability of services; for example, any delay in catalyst injection in high-octane gasoline production would gravely affect the quality of a vast amount of product. Therefore, when implementing our solutions, our client companies must be convinced that this will not lead to a halt in production.

We are committed to the principle of passive influence. Information systems can have false positives that might affect the availability of services. That's why our solutions may not override a command in production, but rather register an anomaly and inform the specialists who must make the final decision.

* In networks with a client/server or terminal architecture, this is a client program that transfers all or the main information processing tasks to the server.
** The multitude of computer devices and combined systems which are used to control various processes in industrial production.

Reducing the number of incidents at our clients' production facilities to zero

Kaspersky Industrial CyberSecurity (KICS) is a platform combining a multifunctional system to monitor and detect threats and anomalies in both the network and the technological process, as well as a specialized solution to protect workstations and servers in the technological segment.

>150 000

More than 150 000 licenses and certificates for all products and services included in the Kaspersky Industrial Cybersecurity solution have been purchased by industrial companies in almost 50 countries worldwide since 2015

This product first appeared in 2012 and was called KICS for Networks. It was a joint project of Kaspersky's Future Tech department and a state-owned company. The basic idea was to create a second trusted monitoring circuit for the technological process. Later it evolved into the concept of passive monitoring, which would allow for the detection of threats without affecting the technological process. In 2015 KICS was released for the general commercial market.

The KICS platform represents the core of an ecosystem of technologies and solutions for industrial corporations based on Kaspersky's expertise and many years of hands-on experience in protecting industrial environments. The platform helps manufacturing companies understand what happens at the interface of the corporate and industrial environment and ward off attacks of any scale or complexity.

Since 2015, industrial companies from almost 50 countries have purchased more than 150 000 licenses and certificates for all products and services included in the Kaspersky Industrial Cybersecurity solution. This has been made possible with the support of Kaspersky's global distribution network; distributors from 40 countries were engaged in the KICS deals. Statistics from recent years show that KICS is in high demand, involving double-digit year-on-year growth — in some countries as high as 300%. These figures are attributed to the increasing number of attacks on critical infrastructure and the cumulative damage inflicted.

The main industries include the electric power industry (generation and distribution), the oil and gas sector, extraction of mineral resources, metallurgy, the chemical industry, transportation, and utilities. Products of the KICS ecosystem are used in nuclear power plants — in Russia (the Leningrad Nuclear Power Plant) and Brazil (Angra I, the country's only nuclear power plant, yielding up to 5% of the country's total power generation). We also have a joint project with Russia's largest automobile corporation KAMAZ. This manufacturer of diesel trucks and diesel engines employs Kaspersky Industrial CyberSecurity to protect its own digital production. We are also engaged in electricity power grid projects with Rosseti Severo-Zapad and AO Setevaya Kompaniya. KICS also protects the two largest hydroelectric power plants in Kazakhstan: in Ust-Kamenogorsk and Shulbinsk.

— Enterprises are often told by industrial automation vendors which software they can or cannot install.

Andrey Strelkov
Head of Industrial Cybersecurity Product Line

The industrial sector also has some other peculiarities; for example, many companies use outdated operating systems with limited system resources, no regular patches and so on. That is why it is very important for a product like KICS to maintain technical interaction and cooperation with leading manufacturers of automation and network security systems. We set up a team of industrial experts that works on the certification of our product to comply with vendor requirements. Kaspersky has joint solutions with Bosch Security and Safety Systems (integration of KICS with its CCTV control system and various building security subsystems), Siemens Energy (integration with its power plant control system), and Waterfall Security (integration with its network hardware for industrial networks), among many others.

Reducing systemic technological failure risks

Our systemic risk management emerged in 2007. An incident prevention group was assembled in the R&D department, which eventually became the separate Global Problem Management Team. This team currently comprises specialists from the following departments: finance, IT, R&D, marketing, legal, security, and sales.

The Global Problem Management Team covers six key areas:

- legal issues;
- findings from both internal and external audits;
- mass user requests (more than 10,000 requests concerning the same problem);
- business problems (whenever the company bears losses of more than $10.000 due to a specific problem);
- business continuity risks;
- reputational challenges — including negative PR on social media or in the media due to internal company problems.

Employees of all levels are involved in this work. The expert team meets every two weeks. Incident elimination is controlled monthly by the CTO and CIO, and on a quarterly basis by the board of directors.

Besides our own products, our employees also pursue quality management of the company's internal IT infrastructure and business continuity risks. As a result, in the spring of 2022 the company was poised for the withdrawal of Western providers. For example, when SAP* left the Russian market, its functions were promptly substituted with analogous systems. In September 2022, Kaspersky purchased a 49% share of the LLC ForPeople, developer of GP OrgManager — a system similar to SAP. In the long term, we plan to use this solution not only for our own needs, but also to sell it in the markets of Eastern Europe, the Middle East and Africa, as well as China, India and Brazil.

Another case involves domain names. Until February 2022, most domains of Kaspersky's websites were registered via a UK company. In a few months' time the domains were transferred to a Russian registrar company.

Concurrently our company diversified cloud providers and transferred part of its virtual capacities from international providers (Microsoft Azure and AWS) to Russian solutions (Yandex Cloud).

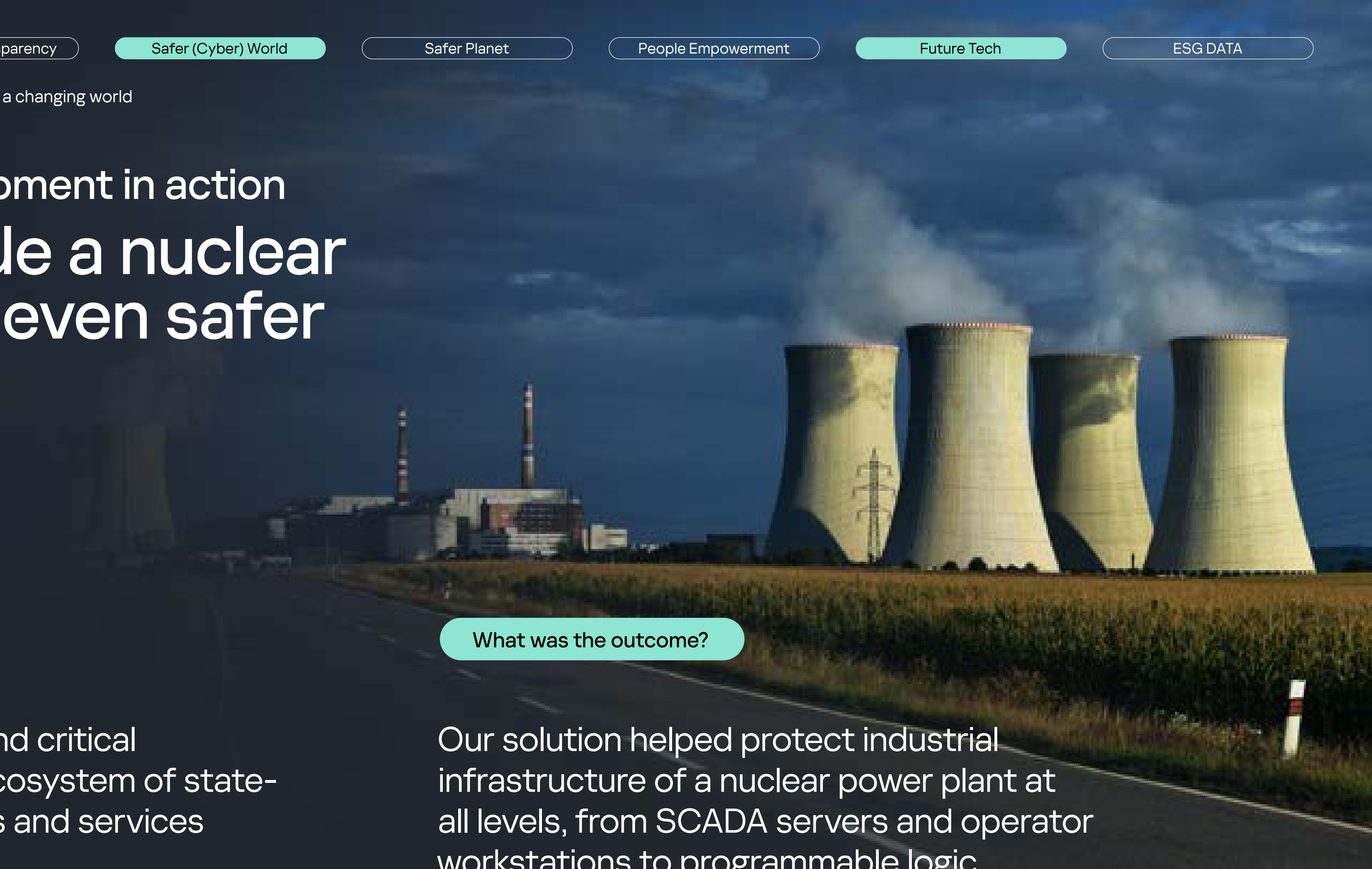
Kaspersky's plans for 2023

- Release a joint solution with the Russian software developer 1C, ensuring data transfer from equipment to new digital services at the level of the 1C:Enterprise development platform, offer the first set of KasperskyOS-based products to international markets (Middle East, Asia, Latin America); and release at least two new training courses covering KasperskyOS for developers.
- For the integrated promotion of our KICS platform, offer our partners among industrial infrastructure companies the chance to specialize in the protection of automated process control systems and industrial infrastructure.
- Continue to reduce any of our own systemic technological failure risks.

* SAP (System Analysis and Program Development) is an automated software system that aids setting up the information space for an enterprise and its effective resource and workflow planning .

Sustainable development in action

How we made a nuclear power plant even safer



Our goal

To protect the industry and critical infrastructure using an ecosystem of state-of-the-art IT technologies and services

The management of the Russia-based Leningrad Nuclear Power Plant was looking for a specialized solution to protect its industrial facilities. A solution was required to ensure the highest level of protection for its power unit control systems, which would simultaneously eliminate any risks of shutting technological processes down without which no stable production operation would be possible. The power plant began operating in 1973, and it currently provides electricity for more than seven million people, generating more than 55% of the total electricity of Saint Petersburg and the surrounding Leningrad Region.

After a thorough market analysis, representatives of the power plant settled on Kaspersky Industrial CyberSecurity. In 2020, this product was implemented at two power generation units in order to test its overall effectiveness, to assess any risks, and to understand what additional settings needed to be configured for full-scale operation. The pilot project was acknowledged as successful, and in 2021 KICS was implemented on the remaining four generation units.

What was the outcome?

Our solution helped protect industrial infrastructure of a nuclear power plant at all levels, from SCADA servers and operator workstations to programmable logic controllers and network equipment. This demonstrated how Kaspersky Industrial CyberSecurity allows for the detection and prevention of both accidental malware infections and targeted attacks, thus ensuring the continuity of technological processes.

Fighting cybercrime

How we work together with law enforcement

kaspersky bring on the future

Our goal

To assist international, regional and national law enforcement agencies with their cybercrime investigations to ensure the security of our users

Key objectives

Contributing to fighting cybercrime by cooperating with international, regional and national law enforcement agencies in the investigation of cybercrime and cyberthreats by providing expertise and required technical information, as well as organizing capacity building such as through the provision of training courses to law enforcement officials in partnership with INTERPOL

Developing successful international cooperation to ensure effective investigation of cybercrime and cyber-incidents in the context of current geopolitical tensions on the global stage

Improving cybercrime-related legislation by sharing expertise reports and other analytical studies

Three questions on fighting cybercrime

GRI 3-3

Yuliya Shlychkova
Head of Global Public Affairs

1

What is cybercrime and why fight it?

There is no single, universally accepted definition of cybercrime; all countries work out their own approach on how to define it. At Kaspersky, by cybercrime we mean illegal actions when people use modern technologies, computers and computer networks for criminal purposes. Today's cybercriminals can shut down a factory or even disrupt the operation of a country's central bank. For instance, the Carbanak group managed to steal a combined total of around a billion dollars from dozens of banks in 2015. With each passing year, the number of cyberattacks keeps growing: in 2021 we uncovered around 380.000 new malicious files per day, which is 5.7% more than in 2020, while in 2022 we detected around 400.000 such files every day — 5% more than in 2021.

Our aim is to protect the world against cybercrime. And we achieve this goal with the help of technology, educational activities, and cooperating in cybercrime investigations led by international, regional and national law enforcement agencies — because this is a problem that can only be tackled holistically. Moreover, cybercrime is international, so cooperation is required on an international level, because no organization or state is able to cope with it single-handedly. The same applies to private vendors — like any other company working in cybersecurity, we alone cannot eliminate a botnet* that is spread across various countries. Only law enforcement agencies have the power to do this, but they often lack the expertise that we have, and the private sector commonly possesses more of the required information on current cyberthreats. That is why Kaspersky is active in fighting cybercrime in cooperation with law enforcement and other international partners.

2

How does this cooperation work?

To ensure the transparency of collaborative cybercrime investigations we rely on our internal policy that regulates handling requests from law enforcement agencies. We have developed a process and formulated the main criteria to run a legal review of all such requests. If the request fails to meet these criteria, we can decline or dispute it. That said, our company neither accepts requests for, nor provides, access to its infrastructure — including data processing infrastructure. The statistics on how many requests have been approved or not is provided within the company's law enforcement and government requests reports**.

The company's participation in cybercrime investigations is often established under existing joint agreements with international partners. For instance, our current cooperation agreement with INTERPOL was signed in Singapore in 2019. Thereunder, we share with INTERPOL information that we have on cyberthreats as well as required data for the investigation of any incidents. Kaspersky's employees also help analyze cyber-incidents and organize capacity building, including training courses for law enforcement officials in INTERPOL member countries.

* Botnet (a portmanteau of the words «robot» and «network») is a network of infected computers used by attackers to perform mass spam-messaging campaigns.
** www.kaspersky.com/transparency-center

3

How do you rate the effectiveness of the company's assistance in fighting cybercrime?

From November 2020 to October 2021, our web-based antivirus blocked 64,559,357 unique malicious objects. Altogether, Kaspersky's solutions thwarted 687,861,449 attacks launched from internet resources all over the world. These results are thanks to the combined effort of four of our departments: (i) the threat research team, (ii) Kaspersky ICS CERT (industrial control systems cyber emergency response team), (iii) the computer incident investigation team, and (iv) the Global Research & Analysis Team (GReAT).

The tense geopolitical situation at present has lowered the level of international cooperation among companies, and also between companies and governments. Various administrative and political barriers are growing, which have a negative effect on information exchange on threats across sectors and national borders. We see this in the dwindling number of assistance requests our experts receive from law enforcement agencies — though of course the number of threats is not going down.

Nevertheless, as cybersecurity professionals we endeavor to maintain cooperation and provide our expertise to the international community to help investigate cyberthreats and cybercrime, and alert the respective authorities on current risks and threats. Since cybercrime has no national borders, a lack of cooperation between states and the private sector only puts cybercriminals at an advantage.

Our cooperation with INTERPOL for the protection of our users in cyberspace

Cooperation with international, regional and national law enforcement agencies is one of the company's key priorities. In 2014, INTERPOL became our partner when we signed our first agreement to fight cybercrime together. Five years later, a new agreement was signed for another five years, which significantly expanded the scope of our cooperation.

What Kaspersky's experts currently do:

1. Assist INTERPOL in international cybercrime investigations by sharing, where and when needed, necessary technical information and threat intelligence. In particular, this includes sharing information through the company's Threat Intelligence Portal, which searches for data on all current cyberthreats;
2. Provide capacity building, including training sessions for enhancing cybersecurity awareness and preparedness.

Our company is also an active participant of Project Gateway, where private-sector companies share data on cyberthreats with INTERPOL.

What we jointly achieved with INTERPOL in 2021-2022

7

high-profile arrests of cybercriminals were made in four countries thanks to active cyber-expertise exchanges between Kaspersky and INTERPOL also prevented a cyber-heist from taking place in a central bank in Latin America in 2021

6

Kaspersky held six training sessions (on reverse engineering, incident response, the ransomware landscape, and stalkerware) for INTERPOL officers in 2021

In 2021

Also in 2021 INTERPOL expressed support with the Coalition Against Stalkerware, founded in 2019 by Kaspersky and other partners, to combine partners' expertise in domestic violence survivor support, digital rights advocacy, and cybersecurity in general — all to address the criminal behavior perpetrated by stalkerware

Maintaining international cooperation in the context of growing geopolitical tensions

Cybercrime, as a rule, does not confine itself to the borders of just one state, and is thereby transnational in nature. To fight it successfully, international cooperation is vital, including between states and the private sector.

≈30

During the reporting period, Kaspersky participated in around 30 joint cybersecurity events with stakeholders all over the world

International cooperation is important as cybercriminals become more sophisticated and their attacks more destructive and costly.

Despite the current difficult geopolitical situation, our company continues to assist international organizations in fighting cybercrime. For instance, with the No More Ransom initiative – jointly launched by Kaspersky, Europol, the Dutch Police and McAfee in 2016 — the company has joined forces with partners to help victims of ransomware retrieve their encrypted data without having to pay the criminals. We share our expertise on handling ransomware with the victims and assist with the required data.

We also continue to share our know-how with diverse stakeholder communities at major cybersecurity expert conferences (e.g., SAS, RSA, Virus Bulletin, and DEF CON 30 — BTV5), publish data on our blogs, and hold webinars on cybersecurity.

In 2022, Kaspersky expanded the free service functionality of the Kaspersky Threat Intelligence Portal, which enables real-time search for data on threats.

687 861 449

Kaspersky's solutions thwarted 687,861,449 cyberattacks worldwide launched from internet resources from November 2020 to October 2021

64 559 357

Kaspersky's web-based antivirus blocked 64,559,357 unique malicious objects from November 2020 to October 2021

114 525 734

Our web-based antivirus registered 114,525,734 unique malicious URLs from November 2020 to October 2021

Our aim is to help improve policies and laws to effectively fight cybercrime

Kaspersky is continuously involved in public processes to develop and improve policies, laws, procedures, and documents that support worldwide cybersecurity.

Our experts share their know-how on critical infrastructure protection, cybercrime and data protection, among others areas. Meanwhile, due to continually evolving regulation on cybersecurity in most countries worldwide, Kaspersky experts continuously share their expertise on relevant initiatives with the respective national, regional and international organizations. Some examples of our submissions and positions can be found on the company's Policy Blog.

Kaspersky is actively involved in international conversations with various stakeholders and states on cybersecurity and cybercrime, including with regional organizations and at the UN level. For instance, since 2020, the company has actively contributed to the UN's "cyber-dialogue" – its Open-Ended Working Group (OEWG), as a non-state industry actor. In particular, we have proposed eight practical suggestions on strengthening security and stability in cyberspace, including the implementation of some agreed cyber norms. Overall, since the launch of the first OEWG, we have publicly shared five company positions featuring specific proposals.

Since 2021, our company has also become an accredited organization of the UN Ad Hoc Committee to "Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes". We continually monitor the intergovernmental process and hope that new and effective forms of international cooperation will be elaborated to prevent and investigate cybercrime.

Kaspersky's plans for 2023

- Continuing to boost cooperation with international, regional and national law enforcement agencies to effectively investigate and prevent cybercrime; continuing to publish data on investigations and threats; and openly disclosing data requests from government and law enforcement agencies every six months in our Transparency reports.
- Continuing to organize cooperative activities (such as training sessions, capacity building initiatives and expert discussions) with representatives of the respective national authorities, regional and international organizations to improve cybersecurity, including within the scope of annual cybersecurity awareness months in different countries and regions. In 2022 we organized the company's EU Cyberpolicy forum as part of the European Cybersecurity Month and held four training courses for law enforcement officials in INTERPOL member countries.
- Continuing to share our views and opinions with national, regional and international authorities to improve existing, and develop new policies and laws on cybersecurity, data protection and related subjects.

Sustainable development in action

How we prevented a central bank heist

Key goal

Preventing cybercrime across the globe

In 2021, Kaspersky's experts discovered stolen data showing that a group of criminals had gained access to and infiltrated the infrastructure of a Latin American country's central bank. The group were looking for partners to follow up on the attack. This type of cooperation has been quite common over the last two years: one group would hack into an organization, another would encrypt and steal the data, while a third group would demand a ransom and handle the financial aspect.

Our experts analyzed the data and discovered that the perpetrators had access to the entire infrastructure of the central bank — including the international financial transfer system. Kaspersky notified INTERPOL and the respective international payment system about what happened.

What was the outcome?

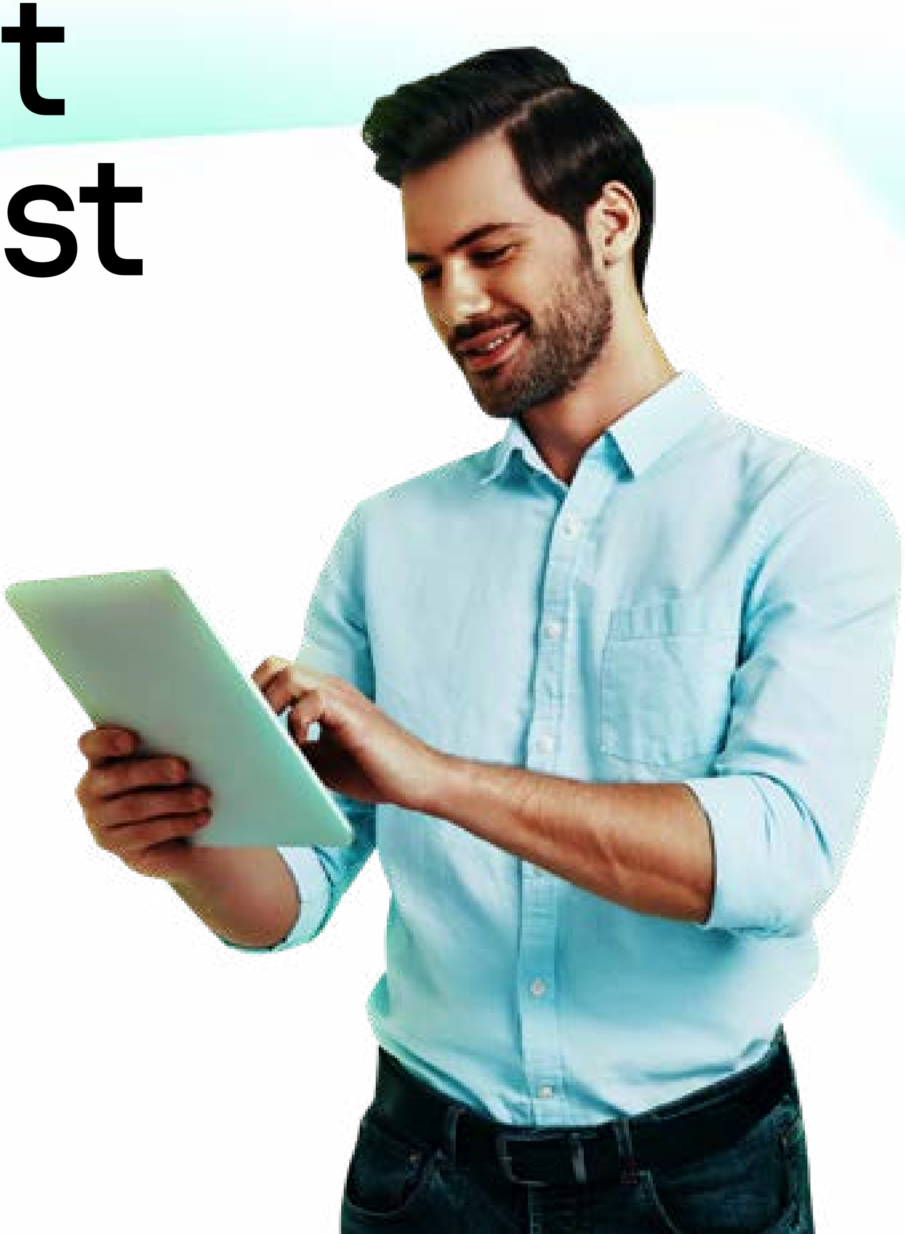
After a joint investigation, all vulnerabilities within the corporate network were eliminated and the possibilities for the planned attack were blocked. Our seamless cooperation was instrumental in stopping the perpetrators before the organization suffered real losses.

Stephen Kavanagh
Executive Director of INTERPOL Police Services

— We are happy that, together with our partner Kaspersky, we were able to prevent an attack that could have affected the entire country's economy. It is only through effective cooperation on the international level and striving to be ahead of the curve that we will be able to effectively protect the entire community.

Security in cyberspace

How we protect our users against cyberworld threats



Our goal

To protect users from cyberthreats using Kaspersky's products and initiatives

Key tasks

Create tools and services to protect users from online stalking and help them recover lost data

Organize educational programs on cybersecurity to improve users' digital literacy and overall security

Develop products and host events to raise both parents' and children's awareness of online privacy and security

Three questions on security in cyberspace

TC-SI-230-a.2 GRI 3-3

Anton Ivanov
Chief Technology Officer

1

What cyberthreats do you consider to be critical?

Over the last few years, one of the most serious cyberthreats worldwide has been **ransomware**, or cryptoware. Our research shows that attacks using this type of malware affecting both businesses and individual users are increasingly common, and the consequences of such attacks can range from heavy financial losses to a company's complete ruin.

Annually, over the last few years, up to a million people worldwide are victims of **cyberstalking**, that is, persistent online tracking. Digital stalking invades users' privacy, removes the barriers between online and offline crime, and can lead to more serious offenses such as harassment or domestic violence, among other examples.

The **online safety of children** is another serious challenge. Our research shows that 70% of children spend at least three hours a day on digital gadgets.

2

What does the company do to counter cyberthreats?

First and foremost, we create high quality products. For example, in October 2021 researchers from AV-Test published the results of their study on how 11 of our advanced security solutions counteract modern cryptoware. According to this independent testing laboratory, Kaspersky Endpoint Security Cloud was the only solution that demonstrated 100% protection against all threats.

To fight attackers who create cryptoware, six years ago we initiated the creation of the No More Ransom alliance, one which involves cybersecurity software manufacturers sharing their experience and exchanging decrypting tools, helping users recover data encrypted by ransomware attackers.

Infection with this kind of malware mostly occurs through human error, such as by clicking on a suspicious link or by opening infected files. Technology alone can never completely protect you against cyberthreats, and that is why — besides developing protection products — Kaspersky is also involved in educational activities, such as by teaching cybersecurity to both individual users and corporate clients.

Our company was among the first to start dealing with digital stalking: since 2019 we have had a designated team working on this issue alone. We believe that the more specialists from diverse fields confront a cyberstalking threat, the more effectively they can handle it. This is why we work with more than 40 partners in the Coalition Against Stalkerware, and we are always attracting new partners, including IT companies, law enforcement agencies, NPOs and schools.

Meanwhile, for children and parents, we developed Kaspersky Safe Kids, a service that helps inexperienced users explore the internet as safely as possible. We also regularly hold webinars and take part in events aimed at kid's online safety.

3

How significant is Kaspersky's contribution to global cybersecurity?

Since 2016, more than 1.5 million users all over the world have been able to recover their data with the help of the No More Ransom initiative, while the number of partners and the decryption tools it offers keeps growing.

Our training courses aimed at improving digital literacy are available in 22 languages; we created a virtual-reality version of the business game Kaspersky Interactive Protection Simulation; and we also released a mobile game called **[Dis]connected**, which helps reinforce previously learned knowledge. The market has noted our efforts in cybereducation; for example, in 2021 our online tool designed to coach employees in IT security — the Automated Security Awareness Platform — helped revenue grow by 34%. In 2022, the company also made two educational products available free of charge. The first one, aimed at Russian audiences, is a training course on phishing, as it is considered to be one of the most pressing threat, while the second, aimed worldwide, is a course on social engineering in social media.

As part of our fight against cyberstalking, we have undertaken a series of joint projects in partnership with NPOs, international organizations and law enforcement agencies. For example, for the Secur'IT competition for students in 2021, we suggested a special nomination for projects aimed at fighting cyberbullying; and as part of the international, interdisciplinary DeStalk project group, we launched an initiative to train and support professionals assisting victims of cyberstalking. During the reporting period we updated, modified, and simplified our user notification language concerning digital tracking in Kaspersky's Android-based products, and we launched the official website for TinyCheck, our free and open-source stalkerware detection tool.

The effectiveness of Kaspersky Safe Kids is confirmed by user feedback and international awards. In 2022 it was named the best parental control app by the online portal Make Use Of, and received a Best of MWC 2022 award at the Mobile World Congress in Barcelona.

Creating tools and services to protect users from online stalking

Stalking entails the persistent tracking of or spying on a person and represents, overall, an invasion of someone's privacy. Digital stalkers use spying software or apps that can be installed on a victim's personal device such as a smartphone.

Stalkerware allows the stalker to view the victim's videos and photographs, read messages, listen to conversations and audio messages, turn on their camera, and access their contacts. Such programs are often used in abusive relationships; in most cases the victims are women. Cyberstalking is also a risk for employees whose employers might use stalkerware without their consent. To protect potential victims, Kaspersky creates malware detection tools, notifies users of any detected stalking, cooperates with law enforcement agencies and international organizations, and helps restore data lost as a result of an attack.

>32 000

unique users worldwide were victims of cyberstalking in 2021. This was revealed in a study on stalkerware based on anonymized usage data from Kaspersky products. The Coalition Against Stalkerware, founded in 2019 at our company's initiative, estimates that every year up to a million individuals across the globe are victims of digital stalking

Supporting NPOs and law enforcement

We organize anti-cyberstalking projects in partnership with NPOs, international organizations and law enforcement agencies. In October 2021, Kaspersky, with the participation of the National Network to End Domestic Violence (NNEDV) based in the USA, and Australia's Wesnet, developed training courses for police officers on the subject of stalkerware. Officially supported by INTERPOL, more than 210 participants completed the training program aimed at building the required capacities to detect and handle stalkerware.

In 2021, we joined the above-mentioned DeStalk for a two-year research project (with financing from the European Commission), addressing the development of a strategy to train and support professionals who assist victims of cyberstalking. Our partners were NPOs and law enforcement agencies that used the tools and products co-developed by Kaspersky. We also delivered a series of training sessions for NPO employees on how to handle stalkerware.

Raising awareness of the problem

In November 2021, we published our report on Digital Stalking in Relationships featuring the results of a survey (coinciding with the second anniversary of the Coalition Against Stalkerware) which involved 21,000 participants from 21 countries. According to the research data, 30% of respondents stated that they may track their partner "under certain circumstances". We also collected data from users who experienced digital abuse, and identified which devices tended to be used. We then shared this data with our partners who work with victims of cyberstalking. Kaspersky employees in the LATAM region presented their report findings during a webinar to 50 journalists from Argentina, Chile, Colombia, Mexico and Peru, and announced that the Mexican NPO Luchadoras would join the Coalition Against Stalkerware.

In April 2022, we published the third edition of the Kaspersky Stalkerware Report — for the year 2021 — featuring a detailed description of the scale of the Stalkerware problem, as well as methods to fight it.

Notifying users about digital stalking

- Kaspersky was the first vendor in the cybersecurity field to employ comprehensive alerts reporting stalkerware installed on devices instead of standard threat warnings;
- During the reporting period, we simplified our user notification language concerning digital tracking in our Android-based products;
- If a Kaspersky program detects stalkerware on a smartphone, it notifies the user and provides them with two options: to keep the stalkerware or to delete it. Having the option to keep it is important, as the stalker might become aware of the victim deleting it, which might provoke the aggressor and in turn, potentially put the victim in danger.

In June 2022, we launched the TinyCheck website. This free, open-source tool for detecting stalkerware on any personal device is capable of detecting malware without alerting the stalker. The website brings together all available information about TinyCheck as well as supporting materials.

>1.5 million

users worldwide have been able to decrypt their data with the help of the No More Ransom initiative since 2016

Cryptoware protection

Ransomware programs are also called cryptoware, because this type of malicious software obtains access to a device and encrypts the entire operating system or individual files, after which the perpetrators demand a ransom from the victims. Over the last few years cryptoware has become a large-scale problem. For example, in 2021 the number of companies affected by such programs increased by 30% compared to 2020. In the first three months of 2022, more than 74,000 users encountered cryptoware attacks.

To thwart such attacks, Kaspersky initiated the No More Ransom alliance in 2016 together with Europol, the Dutch National Police and other cybersecurity vendors. The alliance enables members to exchange experience, knowledge and decryption tools that help restore data encrypted by attackers.

To date, the program has evolved from four to 188 partners and made 136 file decryption tools available on its website. Kaspersky has contributed to the development of nine decryption tools that help restore data encrypted by 38 ransomware families. From 2021 to July 2022, these tools were downloaded more than 50,000 times all over the world.

As a general rule, cryptoware infections occur when inexperienced employees of a company click on links and unknowingly grant privileged rights to a virus. In cryptoware protection, individuals are still the weakest link. This is why it is important not only to create the technology, but to also promote awareness of how to properly utilize it.

Organizing cybersecurity educational programs for users

85% of cyberattacks are attributed to human error: users follow suspicious links or click open infected files. That's why we educate users by holding webinars on cybersecurity, while we also regularly develop and update training courses to help increase companies' security. Our training programs are based on our own expertise in the cybersecurity field. We focus on practical skills and their deployment rather than theoretical knowledge.

For general use

Kaspersky has acted as partner for several training courses under the sponsorship of the European Commission aimed at teaching cybersecurity to the most vulnerable population groups, including Trapeze for senior citizens, CitySCAPE for public transport users, and DeStalk for women who have experienced online violence and/or stalking.

At a time when attacks on ordinary people are on the rise, we have developed free of charge courses for anyone interested in taking them. For example, during the pandemic we launched a course in cooperation with Area9 Lyceum on remote-working security; in the summer of 2022 we ran a course on email security and phishing for Russia-based users; and just recently, a course on social media security worldwide users.

We developed our training resource Kaspersky Education, which features courses on cybersecurity in the form of video tutorials for the general public, as well as specialized content for students. The courses are available in both Russian and English.

One more educational project based on the experience and expertise of our specialists is Kaspersky.Academy, which we plan to transform into a global university within the next two years. We will bring together all educational content relating to information security in order to benefit both cybersecurity experts and ordinary people alike. We plan to include both paid and free content.

For corporate clients

We use our self-engineered online Automated Security Awareness Platform (ASAP) to help rank-and-file employees of customer companies improve their IT security skills. Available in 22 languages, it hones practical cyber-hygiene skills and reinforces them through tests and simulated attacks. Participants' progress is evaluated in reports. We are currently working on developing an on-premises* version of ASAP, as for many clients from Russia and the Middle East it is important that the solution works from their own private server.

For company executives, corporate cybersecurity experts, and employees of IT departments, we have developed the business-oriented game Kaspersky Interactive Protection Simulation. Using the VR format, KIPS puts the players into a business environment where, faced with serious cyberthreats, they have to choose a defense strategy, all the while maximizing company profit. Both KIPS and ASAP are also used as tools to deepen knowledge.

Another tool to reinforce previously gained knowledge in real life is our mobile game [Dis]connected, an interactive cybersecurity quest –which we released in 2022. The aim of the game is to strike the right work-life balance.

For finding out what the market demands concerning the creation of new courses, we primarily rely on win-loss analysis — a study of client relations where we analyze effective sales and missed opportunities. Starting in 2020, we also introduced the customer success procedure, one in which we ask our users how effective they consider our products to be after they have been using them for six to 12 months. Our customers can also use the feedback portal to submit their comments and requests, which our product managers attend to.

— Professional education in general changed drastically due to the pandemic...

Elena Molchanova

Head of Security Awareness Marketing**

Though the changes did not affect us so much since we were focused on online courses from the outset, adapting them to different sectors and regions. Still, after 2020 both our customers and society in general began to better appreciate the online interaction format. Even Kaspersky Interactive Protection Simulation, which we traditionally held offline, now takes place 90% online.

In 2022, the world changed once again; one result was that social engineering expanded, and in Russia phishing incidents became increasingly more frequent. We therefore made the relevant courses available free of charge to protect people under the changing circumstances. The company regularly makes certain courses available free of charge, based on the character of prevailing attacks at a given time. For example, in 2020 we promptly developed a course on ensuring security in remote work settings — available for the general public.

+34%

ASAP saw a total revenue growth of 34%, while in the small and medium-sized enterprises segment growth reached 66%

* Installed on the client's equipment.
** The position is specified for the period from 2021 to 2022.

Developing products and hosting events about the online security of kids

We conducted a survey involving more than 11,000 parents from 19 countries, and the results evidenced that 61% of those parents' children were given their first digital device aged between eight and 12 years old — with 11% starting to use gadgets earlier than five years old. The parents surveyed were concerned about who their children interact with online, what websites they browse, and whether or not they encounter aggressive behavior online. To help parents, from 2014 to 2015 we developed and released Safe Kids, a parental control app that protects children from content that is not age-appropriate – allowing them to explore the internet as safely as possible.

Key features of Safe Kids

1. **Safe search.** The application interacts with search engines and blocks search requests. Once a week, parents receive reports on what their child searched for on the internet. This helps them to better understand their child's interests and to remind them what is suitable for them to search on the internet and what is not.
2. **App usage control.** The basic function is inappropriate app blocking based on the child's age. Usage time can also be controlled (you can set allowed time intervals and schedule days off).
3. **Screen time control.** You can set a maximum amount of allowed screen time in hours and have the device blocked when the limit is up. The device can also be switched off at a given time when the child needs to do their homework or otherwise be engaged screen-free.
4. **Setting up a secure perimeter.** This service is GPS-based and sends an alert to parents if the child has left a defined perimeter (e.g., school premises) during a prescribed time.
5. **Monitoring social media messaging.** Parents cannot view the messages, but will know about the communication happening and can view the other person's profile. If an adult stranger starts messaging the child this might be a red flag.

Andrey Sidenko
Head of Child Safety at Kaspersky Network

— In 2021, we added the option of monitoring YouTube watch history and expanded the iOS functionality. Now parents can filter unsuitable content more thoroughly, class it by specific categories, and learn more about their children's interests based on the YouTube videos viewed.

The application can be installed on both desktop computers and mobile devices on all popular operating systems.

Awards

Kaspersky Safe Kids reaps regular awards. In 2021 the app was certified as Approved Parental Control Software based on testing results of the independent AV-TEST lab. It also won a Best of MWC 2022 award as the best parental control solution at the Mobile World Congress in Barcelona.

What else have we done for children during the reporting period?

1. We launched two free-of-charge courses: an online course dedicated to kids' online safety on the micro-learning platform Skill Cup, and the training course Cyberfox 2021: anti-hacking protection created in cooperation with the Foxford online school.

2. We participated in the nationwide Russian education project The Digital Lesson for which we provided online games for three school age groups: junior, middle and high school. With a geographical coverage reaching Russian-speaking pupils all over the world, in February 2021 our online lesson was on Privacy in the Digital World, attended by a total of 2.3 million children across the country; and in February 2022 our lesson was on the Study of cyberattacks, attended by 2.5 million.

3. We published a children's fiction book — **Midori Kuma and a Very Special Race** — which informs children about online safety at a level suitable to them. It was written by the Italian children's book author Alessia Cruciani, and illustrated by Disney-Pixar cartoonist Gianfranco Florio. The book was published in six languages: Arabic, English, German, Portuguese, Russian and Spanish. The book's promotional partner in Italy was EducazioneDigitale.it, an educational platform with more than 55,000 registered Italian teachers. In Serbia, a similar partner role was assumed by the country's most renowned schoolchildren's magazine, Mali Politikin Zabavnik.

4. We published a textbook titled **Information Security: How to Behave on the Web. Grades 2-4**, authored by Andrey Sidenko – Head of Child Safety at Kaspersky Network, Lead Web Content Analyst, and winner of the Russian nationwide Teacher of the Year Award in 2013.

5. We held 113 webinars on kids online safety in 24 Russian cities and regions, reaching an audience of more than 750,000.

6. We launched an interactive mini-series titled **Mom, I'm Going to Be a Blogger!** on our kids.kaspersky.ru portal. With 10 episodes, each running two to three minutes long, this is a series about online safety for pupils of elementary and middle-school age. At the end of each episode, there is a small interactive assignment that helps reinforce the episode's central message.

7. We announced the establishment of the Alliance for the Protection of Children in the Digital Environment together with Russia's largest digital companies: VimpelCom, Gazprom-Media Holding, MegaFon, MTS, VK, National Media Group, Rostelecom, and Yandex. The main goal of the Alliance is to create a child-friendly online environment based on creative and safe technologies and digital solutions. One of the first initiatives of the Alliance was the development of the Digital Childhood Ethics Charter. It lays out key principles and practical recommendations on how to create a safe and friendly online space.

8. We conducted a new survey on children's online safety titled "Adults and Children on the Internet", in which 2008 individuals – both adults and children — took part.

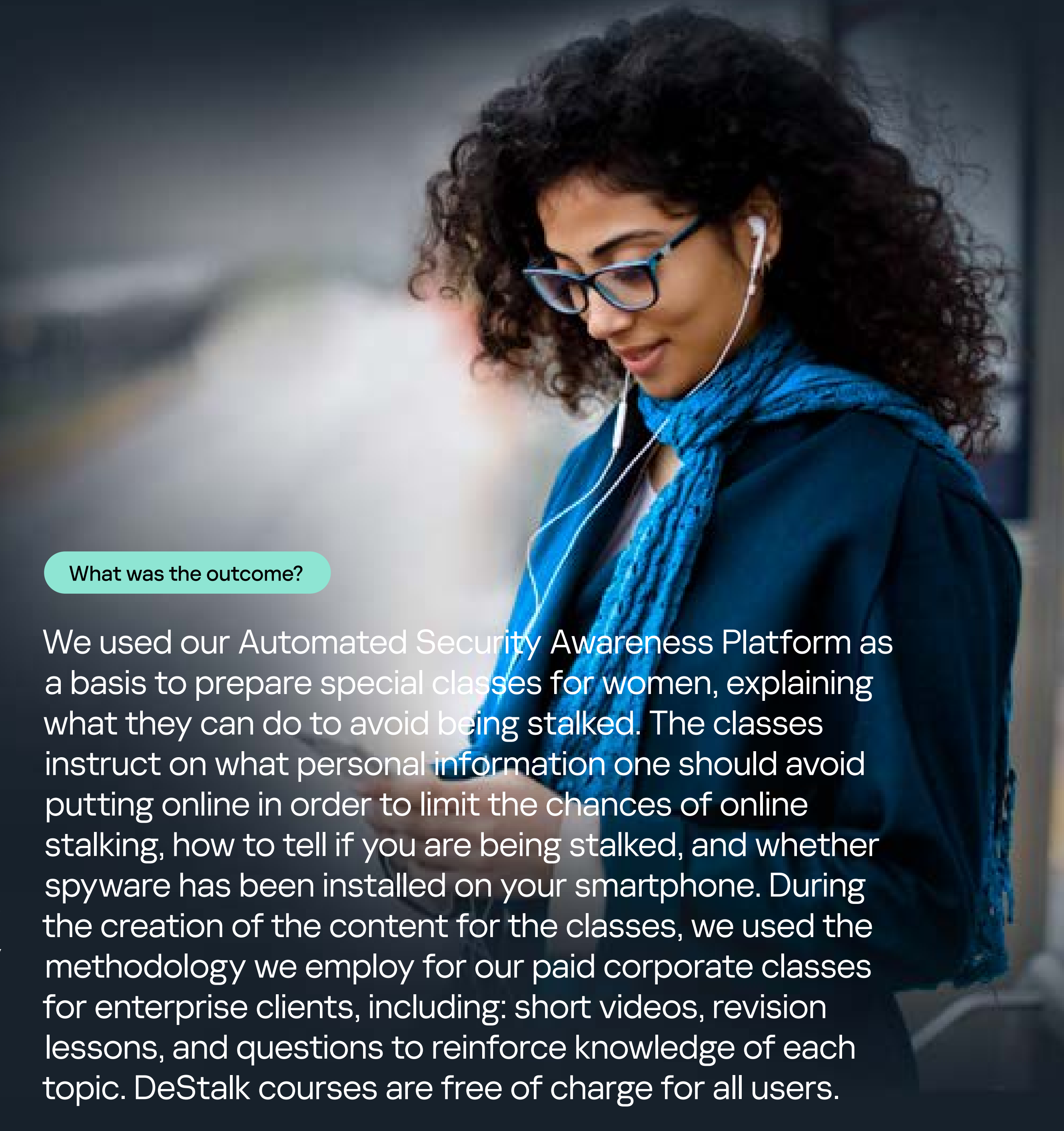
9. We participated in an event organized by Telefono Azzurro, an Italian non-profit organization protecting children's rights. Kaspersky's representative Cesare D'Angelo spoke on the topic of the "Ethics and Responsibility of Society, Institutions, and Companies in the Digital Ecosystem".

10. In Germany, we held a four-hour seminar and training-session on cybermobbing* and deanonymization**, during which we talked to both parents and children about online safety.

Kaspersky's plans for 2023

- We will modify the TinyCheck tool so that it can be installed on any hardware and thus make it more accessible to a wider circle of NPOs and law enforcement agencies.
- We will continue to hold educational events in all regions of our presence, in cooperation with various NPOs. In November 2022, together with the Singapore NPO SCWO, we will organize a joint webinar on doxing and data protection in the digital environment.
- We will continue to cooperate with the European Commission and release a learning course for teenagers.
- We will release an on-premises version of ASAP and update KIPS so that the game comes equipped with a Threat Design Wizard. This will allow every company to independently construct a customized training simulator for its own needs, instead of using the universal version.
- We will continue to release products and host events for the protection of children by offering updated surveys on the subject of kid's online safety, publish new episodes of "Mom, I'm Going to Be a Blogger", and, in partnership with the publishing house **Detskaya Literatura** ("Children's Literature"), publish the book **Parents' ABC of Information Security.**

* Cyberbullying includes insults and threats, and the transferring of data compromising a specific person over an extended period of time, among other examples.
** Violating anonymity, publishing an individual's personal data.



Sustainable development in action

How we helped protect women from online stalking

Our goal

To reduce the risk of cyberthreats through Kaspersky's products and initiatives

Within the context of reducing cyberthreat risks to our users, we protect potential victims from online stalking. Online stalking is a major concern, in particular for women in Europe: one in ten women have experienced online violence from the age of 15, and 20% of young women regularly experience sexual harassment online. At the same time, 70% of women who have been victims of cyberstalking are also subjected to physical and/or sexual violence by their partners.

In 2020, together with several partners, we applied for a European Commission grant to protect women from this threat. This was the start of the DeStalk initiative, which aims to counteract the online stalking of women by offering psychological studies as well as the technical means to protect them. It also features instructional functions, the educational aspect for which Kaspersky was in charge of developing.

What was the outcome?

We used our Automated Security Awareness Platform as a basis to prepare special classes for women, explaining what they can do to avoid being stalked. The classes instruct on what personal information one should avoid putting online in order to limit the chances of online stalking, how to tell if you are being stalked, and whether spyware has been installed on your smartphone. During the creation of the content for the classes, we used the methodology we employ for our paid corporate classes for enterprise clients, including: short videos, revision lessons, and questions to reinforce knowledge of each topic. DeStalk courses are free of charge for all users.

Ecological footprint

How we are reducing our impact on the environment

kaspersky bring on the future

Our goal

To reduce the impact of all our activities on the environment

Key tasks

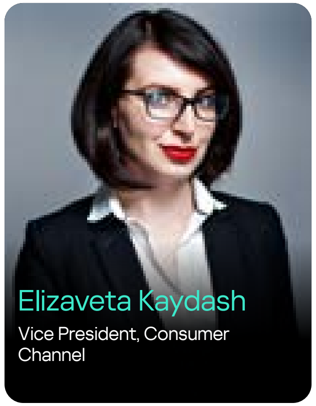
Reduce our environmental footprint by improving energy efficiency at our data centers

Reduce the impact of our operations by being more selective about business trips, transitioning from physical media sales to online licenses, using environmentally-friendly and recyclable packaging materials, and by switching to an electronic document flow

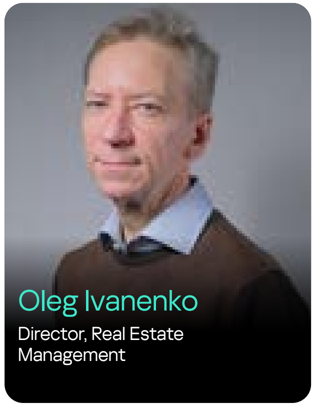
Reduce our environmental footprint by increasing the amount of recyclable materials we use, and by utilizing ecologically sustainable and energy-efficient solutions in our offices

Three questions regarding how we reduce our ecological footprint

GRI 3-3


Elizaveta Kaydash

Vice President, Consumer Channel


Oleg Ivanenko

Director, Real Estate Management

1

What is the company's impact on the environment?

– Our business goals overlap to a great extent with the UN's Sustainable Development Goals. We create hi-tech products that improve life in modern societies, while recognizing that such improvement is not possible without the simultaneous reduction of one's environmental impact.

This comprises both our carbon footprint (waste originating from the company's activities) and water consumption, principally originating from the company's infrastructure, office buildings, and business operations.

Kaspersky's carbon footprint largely results from indirect sources, such as air travel, server operation, energy used at the office, corporate transport, and services used to create and distribute our products. Waste generated in the course of production primarily includes packaging waste from physical products and operational office waste.

2

What is your approach to managing your environmental impact?

– A single universal environmental policy has yet to be developed, but environmental responsibility is one of the company's core values. We try to minimize our negative impact by economizing on our use of resources, by having well-organized business processes in place, and by carefully considering the energy sources for our data centers and offices. Moreover, the company's department heads are responsible for implementing modern solutions to minimize the use of resources.

3

What is the company doing to reduce its environmental impact?

– We continually strive to increase the energy efficiency of our infrastructure: our data processing center as well as rented rack servers in data centers in Moscow and other locations. Through regular equipment upgrades we minimize our electricity consumption used for the operation and cooling of the servers.

We are also trying to reduce our carbon footprint by minimizing business trips. Cutting down on our air travel reduces the emissions the company is responsible for.

To reduce the amount of packaging we use, for example, we are switching from physical products to selling licenses online, and we use less plastic in our promotional gifts and marketing materials. We also sort our office waste, adhering to responsible waste handling criteria. Simultaneously, in order to save water at the office we use contactless taps with short water discharge periods. And to save electricity on lighting we have motion sensors installed throughout the office.

Another way we save resources and energy — particularly electricity — in our daily activities is by having transitioned to a largely remote and hybrid work mode for our employees. We also use much less paper since implementing an electronic document flow.

Reducing our ecological footprint in relation to infrastructure usage

GRI 302-1 | GRI 302-3 | GRI 302-4 | GRI 302-5 | TC-SI-130-a.1 | TC-SI-130-a.3

Carbon footprint

IT companies add to the world's carbon footprint through CO_2 emissions generated from their energy consumption and transportation usage. In particular, most of their electricity consumption is for powering infrastructural objects such as data centers and offices. The carbon footprint is measured in tons of carbon dioxide (CO_2).

Data processing centers house thousands of servers operating around the clock, which consume a considerable amount of electricity to feed the infrastructure and also cool it down with industrial air conditioners. Kaspersky imposes high requirements on its infrastructure, and also has to ensure that the capacities of the servers cover the needs of its IT and R&D teams. This is why we only use state-of-the-art technologies that help limit electricity and other energy consumption, allowing us to save on energy resources. Our own data processing center consists of 33 server racks that ensure the vital operation of user infrastructure and the back office. For development needs we use servers in rented data processing centers: around 400 server racks are located in Moscow alone.

An important criterion for the energy efficiency evaluation of our data centers is the PUE value (power usage effectiveness), meaning the ratio between a data center's total energy consumption and the energy consumption of IT equipment. Research data of the Uptime Institute shows that the average PUE value of data centers worldwide was 1.58 in 2020. We are currently working to systematize the calculation process of the PUE value for Kaspersky's data centers and we plan to share our data in future reports.

To ensure the uninterrupted operation of our data processing center, two energy sources from autonomous substations are used. There is also a diesel generator, and in the event of its failure, UPS batteries support the electric power supply to enable server room operation for about 30 minutes until the problem in the power network is resolved. All electricity supply networks undergo regular inspection, as does the diesel generator — including a yearly fuel replacement. We give the generator a no-load test run every two weeks, and hot runs every three months, as well as conduct quarterly maintenance works on the data center's UPS system.

In winter we utilize the natural atmosphere's cold air in a free cooling system for the data center. The room is also equipped with a modern gaseous fire suppression system, which uses 3M's Novec gas — harmless to the environment.

Waste and water

Kaspersky's data center is located in the same building as its office, meaning waste generation and water consumption are measured on a joint meter. For now, we do not take into account the servers in the rented data centers.

Total energy consumption (percentage of grid electricity)

7 576 858 kW·h

2021

3 347 291 kW·h

2022 (January 1 to June 30)

27 276.7 GJ

2021

12 050.2 GJ

2022

Reducing the environmental impact of our operations

GRI 305-1 GRI 305-2

Carbon footprint

Air travel and road transport

The pandemic made us completely rethink our approach to business processes, which resulted in cutting down our carbon footprint. In 2021, our employees' flights contributed to the CO2 equivalent* of 583 tons of greenhouse gas, which is 81% less than in 2019. Beginning in 2020, we reduced our air travel expenses in the digital sales department by 75–80% due to the pandemic. Gradually, what started as a forced response became the new normal. Now we carefully consider the necessity of any business trips before embarking on them.

Carbon footprint sources also include fuel emissions from corporate transportation. To minimize these we keep a fleet of just three vehicles, which are used for urgent needs only.

81%

Kaspersky reduced its emissions by 81% from 2019 to 2021 after cutting down on air travel from 5,085 flights in 2019 to 1,460 in 2021

840

The company's employees made 840 flights in the first half of 2022, which contributed to the CO_2 equivalent of 225 tons of greenhouse gas

* Calculated on the basis of distance, flight type and service class.

Tangible sales

Tangible sales entail selling our consumer products on physical media. These can be ordered online via kaspersky.com, on online marketplaces, or offline at major retail chains (FNAC, MediaMarkt, Euronics, Exper), DIY stores and through mini-resellers.

As of today, 9% of our products are sold offline, and we are continuing to switch our sales to the digital track. This is paired with a global decrease in demand for tangible goods and a move to the electronic distribution of software and digital content (Electronic Software Distribution — ESD). The physical media market keeps decreasing by 15–20% in favor of ESD products.

Consumption levels of tangible and online products vary from region to region. Nevertheless, we endeavor to speed up clients' transition to the digital track and make it as seamless as possible for users, while still maintaining the sales channel. To this end, as of 2022, when selling offline items we require users to create an account at my.kaspersky.com to make sure that all further communication is maintained digitally — including extension of licenses and all additional sales and cross-sales. In Latin America, where the ESD transition is among the fastest worldwide, we rely on our distributors' assistance to integrate digital code delivery systems and implement new digital tools for user-friendliness.

50%

less physical media sales of Kaspersky products in favor of digital products in 2021–2022

Why we still use CDs and DVDs

To reduce our carbon and waste footprint, we have been reducing the volume of products sold on CD and DVD by 2% over the last five years. However, it is not yet possible to do away with them completely, since this format is still in demand in various regions, including Africa and some European countries. While Europeans traditionally prefer CDs, in African countries DVDs are more in demand due to the unreliable performance of internet providers.

We invite our distributors and partners to make the move to license-purchase mode or to distribute licenses via their own websites. This requires improved technological capabilities on both sides, but allows for the transition of users to digital products while maintaining the channel as well as reaching out to new marketplaces (Latin America, Asia-Pacific).

We support the current trend in the industry of eliminating the use of plastics, producing and utilizing packaging made from more environmentally-friendly materials instead. For this reason, minimizing the amount of plastics in our box packaging has been one of our top objectives for the last five years. We have modified and improved the materials used, made the box formats smaller, and reduced the number of DVD deliveries. With PoSA cards, we stopped using large boxes and opted for more compact formats. For packaging materials, we use plastic boxes (DVD) and plastic cards to a lesser extent, as well as overprinted cardboard packaging of varying densities (boxes, flyers, PoSA cards). Products in this kind of packaging currently account for around 30% of all our products sold across Europe.

Kaspersky's products on physical media come in a variety of formats

Boxes. Cases with a compact disc containing the product

Leaflets and check cards. Informational materials intended to be used directly at the store

PoSA (point-of-sales activation) cards. Thin cardboard cards used to deliver electronic products

* Calculated on the basis of distance, flight type and service class.

Digital sales at Kaspersky

48%	52%	72%
B2B	B2C	B2C sales consist of fully digital products

Digital sales and document flow

Digital sales, meaning sales of electronic IT products and services, are another aspect of our carbon footprint. When creating these, we rely on the services of hundreds of partners, technologies and systems. These include Google servers, Facebook's data resources, third-party developers and so on. All this uses a lot of energy and therefore also increases our carbon emissions.

Since digital sales involve third parties, we have not yet measured the carbon footprint from this angle.

To speed up our business processes and to reduce paper consumption, in 2021 we started our transition to an **electronic document flow**. The need for this transition manifested itself during the pandemic, and we are currently active in implementing this format in transactions with Russian contractual parties: sending documents from our company to the counterparties via an electronic transmission system that was especially developed for Kaspersky. Early in 2022, we launched an internal electronic document flow system for some company-based clients.

Waste

GRI 306-1 GRI 306-2

A significant proportion of waste from our business operations originates from the packaging and marketing of our products.

Since 2019, we have been receiving more and more requests for promotional gifts made out of recyclable or environmentally-friendly materials. We stopped using plastic bags and introduced bleached kraft paper bags and canvas shopper bags instead. We have reduced the amount of plastic blister wrap we use, and seek out manufacturers who make use of recycled materials (for example, Xindao backpacks).

We recycle outdated marketing materials, informational posters and signs used in our offices (posted on every floor in the elevator areas and kitchen/dining areas), as well as decorative materials for internal events (banners, photo panels and so on).

We are gradually using less and less printed products and leaflets. Printed materials are included in the quarterly catalog of promotional and marketing items under “Information materials”. The number of these items went down from 24 to 7 in 2022 — a 70% decrease.

Water

Water is used for utility purposes in the company's offices, so water level figures are recorded on a single meter.

How we recycle packaging

Many countries in Europe and the META region have a procedure in place whereby manufacturers (including Kaspersky) put international recycling codes on the packaging of their products, while the buyers recycle the packaging themselves.

The regulations for this process vary from country to country:

1. In Germany, the manufacturer (Kaspersky) has to pay an annual recycling fee and license its packaging volumes on the regulator's platform. Failure to comply can result in a sales ban in Germany and a fine of up to €200,000. Compliance is controlled at the level of retailers, which periodically request LUCID ID*. Our company is registered with the LUCID platform, our packaging volumes are fully licensed, and Kaspersky GmbH is listed in the public register alongside brands such as Microsoft, NortonLifeLock and others. The licensing budget is €5000 per year.

2. In other countries we receive occasional requests from regulators (for example, once or twice a year from the UK; once a year from Spain) for data on the volume of cardboard and plastics we bring into the country, and we in turn provide all the required information.

* LUCID is a **packaging register** in Germany and it applies to everyone who is the first to fill packaging with goods and commercially place it on the German market.

Using environmentally-friendly materials and energy-efficient solutions in our offices

GRI 306-3 GRI 306-4 GRI 306-5 GRI 306-1 GRI 306-2

Carbon footprint

To reduce the carbon footprint generated at the company's office, we recycle our waste and use LED lamps and motion sensor lights to use less electricity.

Kaspersky's headquarters in Moscow are located in the Olympia Park business center, a class A office building, meaning that energy-efficient technologies and materials were used in the construction of the office space. The building is certified according to the international environmental BREEAM standard, and we continue to operate it using cutting-edge technological solutions. For example, we only use LED bulbs for our lighting because they use far less energy and yet still provide a high level of illumination. Indoor motion sensors as well as brightness sensors (that regulate the artificial light according to the changing levels of natural daylight) also help save energy. In 2020, we completely replaced fluorescent lamps in the business center parking lot with LED lamps, cutting our total lighting expenses by 30–45%.

Waste

Office waste is another factor contributing to our carbon footprint. In our drive toward more responsible waste-handling we focus on three main areas:

1. waste sorting
2. using high-quality materials
3. increasing the percentage of waste that goes into recycling

To reduce our waste footprint, we endeavor to use high-quality, long-lasting materials — for example, non-disposable tableware rather than plastics. Since the end of 2019, we have been sorting our office-generated waste into recyclable materials and miscellaneous waste. Key locations throughout the office, such as the kitchen and dining areas, cafeteria and others, are equipped with designated bins for paper, plastics, glass and metal, as well as unsorted/miscellaneous waste. The bins are taken out daily for recycling, while the miscellaneous waste is disposed of.

Some of the waste collection and handling is outsourced to companies that organize waste collection, transportation and disposal, as well as being responsible for environmental services and compliance with environmental laws. Every month we collect and analyze data to draft reports on waste generation across different categories. Class I and III hazard level waste is partially neutralized prior to being transported for burial or other disposal.

8.14

out of 172.4 tons of Class IV waste was recycled in 2021; 2.56 out of 218.2 tons recycled for the first half of 2022

Waste composition, in tons*

Waste class	Total generation		Sent for recycling, reuse or other recovery		Sent for burial and disposal	
	2021	2022**	2021	2022	2021	2022
Class I (hazardous waste, non biodegradable): pesticides, asbestos, mercury-containing devices, etc.	0.068				0.068	
Class III (moderately hazardous waste, degradable within three to ten years): herbicides, paints and other coatings, detergents, shampoos, deodorants, mobile phones, etc.	0.926	0.564			0.926	0.564
Class IV (low-hazardous waste, degradable within three years or less): nitrogen fertilizers, MDF, LDF, plastic wrap, mirrors, rubber gloves and shoes, disposable tableware, home appliances, etc.	172.4	218.2	8.14	2.56	164.26	215.64
Class V (virtually non-hazardous waste, degradable within three years or less): food, natural fabrics and objects made from fabrics, paper and cardboard-based goods	3.1	11.3			3.1	11.3

The increase in Class IV and V waste in 2022 is due to changes in the company's mode of operation. During the pandemic most employees worked remotely, but as of 2021 and 2022 they began returning to the office.

* The calculation was based on the Order of the Ministry of Natural Resources of the Russian Federation № 1028 of 08.12.2020 "On approval of the accounting procedure in the field of waste management".
** Hereinafter: from January 1 to June 30, 2022.

Water

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

Kaspersky's water consumption is insignificant and mostly accounted for by the office. Since 2019, it has dropped by around 50% due to our transition to a hybrid work mode. At our Moscow office we also replaced the water supply with sensors, so that water is now turned on and off with a motion of the hand, which helps reduce water consumption by approximately 50%.

Water consumption at Kaspersky's data center and office, m^3

2019	25 803
2020	10 890
2021	11 862
2022*	7 359

We use municipal-source water of AO Mosvodokanal.

Kaspersky's plans for 2023

- We will reduce power consumption in our data processing centers.
- We will increase digital sales by reducing physical media sales to minimize the environmental impact from business operations; we will complete the transition to an electronic document flow; old equipment will go to charity in order to reduce the need for disposal.
- We will increase the amount of recyclable waste in our office by offering information materials, training sessions, and an informative online game on the topic, as well as by equipping new, easy-to-use waste bins.

* From January 1 to June 30, 2022.

Sustainable development in action

How we used an online game to teach our employees about waste sorting

Our goal

To reduce our impact on the environment across all our business activities

In 2021–2022, we started implementing a sorted waste collection system in the office. The first important step was to teach our employees how to properly sort waste. We started off with a video tutorial for everyone explaining what the main waste categories in the office are, and we placed informational posters above the containers at every kitchen/dining area. We developed a FAQ list containing answers to the most frequent and trickiest questions about waste: why sort it, what is produced from recycled waste, and so on. And we also provided training for the cleaning personnel on how to collect and sort the waste bags.

So that all the information provided about sorted waste collection sank in all the better, we decided to reinforce it with an unusual game. On Earth Day, April 22, 2022, we launched an online game called Trash Ninja for all our employees. The premise is to help your colleagues better navigate office waste. The game has fairly simple rules, so it can be used to challenge coworkers and compete for the title of waste-sorting guru — or Trash Ninja.

What was the outcome?

969 employees in our Moscow office have already completed the Trash Ninja game and learned how to properly sort their waste — not only in the office but also at home.

Team

How we take care of our employees

Our goal

To take care of our employees' physical and mental wellbeing in conjunction with their professional development

Key tasks

Ensure favorable working conditions and development opportunities through competitive remuneration and fair employee benefits

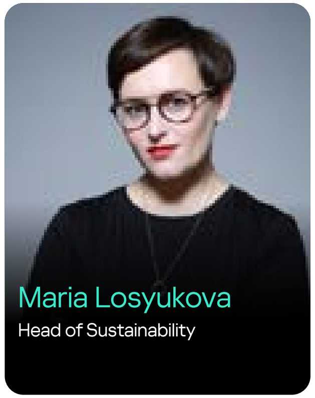
Invest in employee education and advancement through individual development plans, the implementation of newly available educational programs, and by increasing the number of training hours per employee

Develop corporate volunteering by increasing the number of both participants and partner charity funds

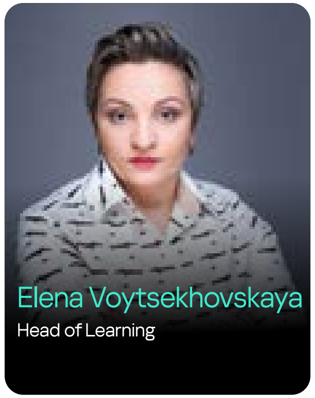
Three questions regarding employee care

GRI 3-3

Kirill Shiryaev
Head of HR Center of Expertise



Maria Losyukova
Head of Sustainability



Elena Voytsekhovskaya
Head of Learning

1

What does employee care mean to Kaspersky?

— Employees are our most valuable asset. It is therefore important for us to make sure that our team feels comfortable, taken care of, and engaged in what they are doing in order to be productive and be able to develop both themselves and the company further. This is why we ensure both the physical and emotional wellbeing of our employees, while at the same time encourage them in their pursuit of further education and development.

2

What does the company focus on in this regard?

— Employee care covers a whole range of measures. Our colleagues enjoy one of the broadest social benefits packages in Russia. Our office has a general practitioner and massage therapists, and is also equipped with two gyms and saunas. We support corporate sports initiatives and reimburse our employees for any fitness-related classes. From the very first day of employment at Kaspersky, employees can benefit from remote psychological and legal support, remote financial consulting, and can schedule an appointment with the company's therapist.

Our company also offers three possible working options: remote, hybrid, or in-office. To ensure that employees have a pleasant experience working in the office, every building is equipped with games and music rooms, stationary and merchandise lockerstations, as well as different types of vending machines — including one with free hot drinks. A relocation-to-Moscow program is also available to employees from other regions of Russia.

We continually add to and improve our educational programs. At present there are more than 100 internal courses available to our employees, including language programs, development of soft and management skills, and the option to attend any external technical courses or conferences. Every year we invest more than 80 million rubles in employee education.

We revise our salary rates on a regular basis and have a bonus system in place. In April 2022, our company invested twice as much in salaries and bonuses than it did in 2021, with an average pay rise across Russia of 20%.

We count on and nurture young specialists because we see a lot of potential in them. We believe that in this modern digital age, higher education institutions and employers need to work closely together to train IT specialists. For this reason, our experts give regular lectures on information security at leading technical universities. We also offer SafeBoard — a fully-fledged paid internship program for students.

3

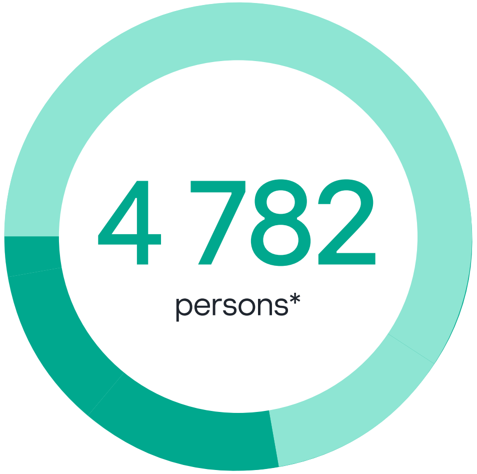
How effective do you consider these measures?

— As mentioned, people are the company's main asset, so we want to keep track of what our employees think about various aspects of their work at Kaspersky — such as salary and benefits, work-life balance, career opportunities, etc. We also conduct annual surveys called YourVoice in order to better understand overall job satisfaction (employee net promoter score (eNPS). In 2022, our eNPS increased by 6.7 percentage points compared to 2021, reaching 52.3%.

In addition, we regularly receive outside recognition. In 2021 the company won three awards in Russia's best employer ranking by Forbes: Bronze in the Ecology nomination, Silver in Corporate Management, and Gold in Employees and Society. In 2022 we were also ranked first in the employer rating by RBC.

Ensuring favorable work and development conditions for our employees while increasing engagement

GRI 2-7 GRI 401-1



74%
3 520 men

26%
1262 women

Across our business regions:

Asia-Pacific **219**
Latin America **104**
Middle East, Turkey and Africa **106**
Europe **368**
North America **86**
CIS **3 899** (including 3 874 in Russia)

Total number of full-time staff, classified by contract type, gender, and region (persons)**.

	Permanent employment contract			Fixed-term contract			Temporary replacement			
	F	M	Total	F	M	Total	F	M	Total	Grand total
Asia-Pacific	75	126	201	4	9	13	3	-	3	217
Latin America	34	69	103	-	1	1	-	-	-	104
Middle East, Turkey and Africa	18	82	100	1	3	4	1	1	2	106
Europe	84	267	351	5	4	9	2	0	2	362
North America	26	60	86	-	-	-	-	-	-	86
CIS	927	2 798	3 725	26	60	86	32	9	41	3 852
Grand total	**1164**	**3 402**	**4 566**	**36**	**77**	**113**	**38**	**10**	**48**	**4 727**

* As of June 30, 2022.
** Hereinafter: headcount.

GRI 2-7

Total number of part-time staff, classified by contract type, gender, and region (persons)

	Permanent employment contract			Temporary replacement			
	F	M	Total	F	M	Total	Grand total
Asia-Pacific	2	-	2	-	-	-	2
Europe	5	-	5	-	1	1	6
CIS	14	20	34	3	10	13	47
Total	**21**	**20**	**41**	**3**	**11**	**14**	**55**

Most of our team (4 813 persons) are employed on a full-time basis. During the reporting period we had no significant headcount variations. As to the gender gap, here we explain the possible reasons for this and how we endeavor to reduce it.

Our team grows every year. In 2022, Kaspersky created around a thousand new jobs. Most of them are in research and development in Russia, including the department in charge of developing the cyber immune operating system KasperskyOS. As of June 30, 2022, the company has 4 782 employees, almost 50% of them in R&D. From 2021, as already stated above, the company offers three working options: remote, office and hybrid. Our employees are motivated both financially and with non-financial incentives: we revise salaries on a regular basis, expand the social package, and invest in training. Kaspersky also has various financial aid programs in place for employees and their families who may be experiencing difficult life situations.

GRI 401-1

The total number and share of new employees hired during the reporting period, and the employee turnover rate classified by age group, gender and region

	Total number and share of new hires				Total number of employees and turnover rate			
	2021		as of 30.06.2022		2021		as of 30.06.2022	
	1039		**769**		**826**		**528**	
	Total	%	Total	%	Total	%	Total	%
by gender								
M	762	73%	558	73%	521	17%	345	15%
F	277	27%	211	27%	305	27%	183	15%
by age								
up to 30	351	34%	275	36%	275	28%	135	11%
30–50	638	61%	465	60%	506	17%	346	11%
>50	50	5%	29	4%	45	12%	47	20%
by region								
Asia-Pacific	47	5%	17	2%		22%		18%
Latin America	22	2%	12	2%		9%		11%
Middle East, Turkey and Africa	19	2%	14	2%		13%		8%
Europe	53	5%	26	3%		35%		41%
North America	14	1%	3	0%		31%		28%
CIS	884	85%	697	91%		55%		28%

* As of June 30, 2022.
** Hereinafter: headcount.

Financial incentives

We revise our remuneration rates on a regular basis, and the company has a bonus system in place. We want to retain our experts, therefore, we try to keep their salaries at a competitive level. We have expanded our expert Compensations & Benefits team in order to enable a faster, deeper analysis of market changes, trends, and the financial assessment of remuneration for our employees.

100% of our employees undergo a quarterly or annual (depending on employment specifics) performance review. The results may be used when considering an employee for a bonus, raise, or promotion. By April 2022 the company had invested twice as much in salaries and bonuses than in the previous year, while the average salary increase across Russia was 20%.

Separately, we assist our employees in obtaining patents for their inventions and provide financial encouragement in this endeavor. Our company also has a bonus payment program in place for recommending potential new employees for a vacancy.

Non-financial incentives

GRI 401-2

The benefits package for Kaspersky employees varies region to region. In Russia, the benefits package is available to all employees*, regardless of their type of employment, and includes, among other things:

- Health insurance and dental care (including for children under the age of 16)
- Up to 100% paid maternity leave
- Up to 100% paid sick leave for up to 15 business days per year
- Paid prenatal and pregnancy care
- Benefits amounting to 150,000 rubles following the birth of the first child and 200 000 rubles for the second and any subsequent children
- Paid oncology treatment across Russia
- Financial aid in the event of the death of a close relative or during other difficult circumstances
- Accident and travel insurance**
- Vaccinations for adults and children
- Relocation package for employees moving to Moscow
- Jubilee birthday bonuses (50, 60 and 70 years old)
- Bonuses for employees who have dedicated 10 years to the company
- Reimbursement for any fitness memberships outside the workplace
- Reimbursement for language courses offered inside the workplace
- Educational programs for employees

It is important for the company to know our employees' opinions on their various work aspects and to share these views. To this end, several times a year we hold AMA sessions and kick-off meetings with the company management. These are "Ask Me Anything" meetings during which the company's top management executives answer any questions our employees have. As a general rule, the company's plans and strategies for the year ahead are discussed and results are shared during these meetings.

Meanwhile, the key goal of the annual Kaspersky Awards ceremony is to acknowledge, in equal measure, the achievements of all the different departments within the company over the past year. Kaspersky Awards are given to the most productive employees — those who made a major contribution to the company's success in the outgoing year.

* A reduced social package is available for employees with temporary and part-time employment contracts. The company has about 0.3% of such employees.
** Employees can take out an electronic policy for themselves and their children to travel abroad for both business and private, trips outside the Russian Federation.

Engagement assessment

TC-SI-330-a.2

Every year we make use of our survey, YourVoice, to perform an overall satisfaction assessment (eNPS). All managers, including senior management, study the survey's results. This helps each leader have an objective feel of the company's "pulse" in general, and of their team in particular: to gauge the strengths and to spotlight any areas in need of change. As mentioned, in 2022, eNPS increased by 6.7 percentage points compared to 2021, reaching 52.3%.

Equal opportunities

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

Kaspersky does not impose any limitations on hiring people based on their gender, age, disability or otherwise. 26% of staff at Kaspersky are women, and almost half of them are heads of various departments or senior managers. Our company has support programs in place for women, and we guarantee the right to work to employees with disabilities in accordance with the law.

According to the findings from a study conducted across 600 Russian companies in 18 different business sectors, the median eNPS value was +26.1. The lowest values were registered among manufacturing and natural resources companies, while the IT and banking field displayed the highest levels in this index. According to HappyJob, a company specializing in engagement surveys across Russia, the benchmark for the IT industry is 39.8–51.6.

GRI 405-1

Employees in senior management classified by gender and age

	In senior management				**Total at the company**			
	as of 31.12.2021		as of 30.06.2022		2021		as of 30.06.2022	
Total	**14**		**14**		**4 462**		**4 782**	
	Total	%	Total	%	Total	%	Total	%
by gender								
M	11	79%	13	93%	3 308	74%	3 519	74%
F	3	21%	1	7%	1154	26%	1263	26%
by age								
up to 30	-	-	-	-	879	20%	1095	23%
30–50	10	71%	10	71%	3 256	73%	3 379	71%
>50	4	29%	4	29%	327	7%	308	6%

Investing in education and development

GRI 404-1 GRI 404-2 GRI 404-3

Our company offers opportunities for both in-house and external education for all its employees. We have both compulsory and optional corporate educational programs. Our employees show a high level of interest in education; for example, in 2021 1762 completed additional training, which is more than 40% of the total number of staff.

When designing training courses for our employees, we rely on the "learning journey" approach. This entails the training is put together based on each specialist's role, their expertise, as well as regional aspects. This way, employees acquire the relevant knowledge step by step, which can then be integrated into their work process right away.

Compulsory courses

Compulsory courses consist of several subject matters.

1. **Information security courses.** These cover the basics of cybersecurity that all Kaspersky employees must know — even if they are not directly involved in developing or promoting our solutions. Employees learn what kinds of links should not be clicked on, and how to properly process confidential information.
2. **Certification.** Certification is provided as a set of compulsory courses for the sales and pre-sales teams, and is related to the product line's roadmap. Within 90 to 180 days, depending on the position they hold, the employee needs to pass an exam confirming their acquired knowledge.
3. **Training on the rules of conduct in the event of an emergency at the workplace.** Compulsory for all the company's employees.
4. **On-boarding.** Training for all new employees of the company.

How Kaspersky employees studied in 2021

GRI 404-1

6.7

training hours* per company specialist in addition to compulsory training. Women took more intensive training — amounting to 6.4 hours, with men completing 5.1 hours

9.8

training hours per technical specialist. Other specialists studied less — 3.2 hours

28 508

hours in optional courses completed by all employees

>40%

More than 40% of all employees (1762 people) completed training on optional courses

* Clock hours (60 minutes).

Optional courses

We do not limit our employees to any specific catalog: they can complete a training course on our internal portal Kaspersky. Academy, select a course on any MOOC platform, or choose any other external training that they regard as helpful for the development of their professional expertise. Kaspersky.Academy has a portfolio of training programs for both technical specialists and managers of various levels, as well as workshops on the most in-demand skills at the company. Beyond that, the company has been running the CoLab Tech project for several years, which offers both regular lectures on technical subjects and support webinars on how to deal with stress, anxiety and one's emotional wellbeing in general.

Both vertical and horizontal development is available at the company. Each year, Kaspersky's employees complete professional retraining courses of their own choosing. For example, an R&D engineer can retrain as an IT architect*, or a specialist in information security can become a recruiter. Those who are interested can seek guidance from the HR department to develop themselves beyond their current professional experience and skills and design a step-by-step training schedule required to master a new profession. If the employee is unsure what new professional direction would suit them, they can take an interactive test on our corporate portal and have concrete potential development options offered to them.

External training

We encourage any pursuit of knowledge by our employees, including through external training. Upon request we help our specialists find suitable courses to learn a new programming language, or attend specialized conferences, for example. The year 2021 saw an average of 5.85 hours of external training completed per employee. All training costs are reimbursed.

>$920 000

invested in employee training
on external courses and participation in conferences
during the reporting period

* A specialist who decides what an organization's information system will look like both on the whole and in detail.

Ensuring health and safety in the workplace

GRI 403-1 GRI 403-3 GRI 403-5 GRI 403-6

Kaspersky has an occupational safety management system in place for which the HR department is responsible. The main indicators of the system's effectiveness are zero on-the-job injuries, successful completion of oversight inspections, and regular audits of documents.

100%

All employees take a compulsory course on the rules of conduct in the event of an emergency at the workplace

In accordance with the law, the company conducts regular health and safety assessments of the workplace as well as safety briefings. All employees take a compulsory course on the rules of conduct in the event of an emergency at the workplace (e.g., a fire).

Our corporate medical insurance covers workplace accidents — employees can report an insurance claim by contacting the HR department.

As part of our employee care plan we offer annual flu vaccinations and "health days", involving medical consultations in clinics covered by our private medical insurance. At Kaspersky's headquarters in Moscow, employees always have access to an on-premises general practitioner, massage therapist, gyms and saunas. We support corporate sports initiatives and reimburse any fitness classes taken.

Early on in the pandemic, our company promptly expanded the corporate private medical insurance plan by offering free COVID-19 testing. Since 2021, all Moscow-based employees now have the opportunity to be vaccinated at the office. Of late, our employees' private medical insurance plan now also covers private hospital stays if diagnosed with COVID-19.

We also think of our employees' mental health. In 2022 we organized a series of online meetings with therapists for employees of our Russian and foreign offices. The HR department arranged more than 15 seminars with experts in the field of communication, stress management and modulation of emotions, which helped our employees worldwide feel both connected and supported. In some regions, employees were able to book individual consultations with therapists.

In 2021 we developed the digital relax platform Kaspersky Cyber Spa. This package of online procedures, including meditation and technosound therapy, helps deal with stress and negative emotions.

Developing corporate volunteering

Kaspersky's employees are regularly involved in our corporate volunteering program. It runs in many regions where the company is present, and includes several areas: donorship, charitable sports events, patronage of orphanages, and, since 2022, pro bono volunteering.

>$7 800

for the benefit of charity funds such as Sindrom Lubvi, Vera, and Zhivi were raised by Kaspersky's employees as part of our corporate fundraising initiative from January 1, 2021 to June 30, 2022

How our volunteers make the world a better place

In Russia

- Taking part in sports events run by partner funds: running, cycling, triathlons.
- Being patrons of the Udomlya orphanage;
- Organizing volunteer workdays at Moscow's Rostokino hospice together with the hospice charity **Vera**;
- In-office employee blood-donating days twice a year for the benefit of the Podari Zhizn (Gift of Life) charity;
- Holding free-of-charge consultations and training sessions for partner charities as part of pro bono volunteering. During the reporting period we volunteered for organizations such as SOS Children's Villages, ROOI Perspektiva, and Podari Zhizn;
- Participating in corporate fundraising.

In the Asia-Pacific region

- Our employees from Singapore hold free-of-charge consultations and training sessions for partner funds as part of pro bono volunteering.

In North America

- In the U.S.A., our employees participate in the Boston Children's Hospital Corporate Cup annual field day competition.
- In August 2021, US-based employees visited Cradles to Crayons in Newtonville, Massachusetts, to help sort and pack 700 sets of school supplies for children in need.

Kaspersky's plans for 2023

- Expand our portfolio of training courses and programs for both inside and outside audiences, and put together a separate portfolio for the company's partners.
- Continue to hold seminars and webcasts concerning emotional self-regulation, empathy and emotion control in an age of increasing worldwide challenges.
- Continue to actively hire and create new jobs, provide competitive remuneration to attract, retain and motivate talents.
- Continue to develop volunteer projects featuring pro bono activities and sports volunteering.
- Expand our pool of partner charities and NPOs.

Sustainable development in action

How Kaspersky’s employees help hundreds of people through pro bono volunteering

Our goal

To ensure our employees’ physical and mental wellbeing in conjunction with their professional development

In 2022, we started pro bono as a new kind of corporate volunteering. Many of our colleagues wish to help, but not everyone is ready to visit an orphanage or take part in sports events, for example. So we decided they can share their knowledge and skills instead. Pro bono implies offering professional help to NPOs, people or organizations who cannot afford to pay for the services they need. For example, Kaspersky is approached by partner funds seeking assistance in the field of IT, communications, marketing, audits or research. We pass on such requests through internal newsletters and on our corporate social media.

What was the outcome?

As part of the pro bono initiative, in 2022 the Polys project team helped the Podari Zhizn charity in organizing the voting process for their annual Charity Against Cancer awards. Kaspersky’s head of technical training and certification helped IT specialists of SOS Children’s Villages understand the functionality of Kaspersky Endpoint Security. Meanwhile, our methodological support manager conducted two events for NPOs: information security training for employees of SOS Children’s Villages from six regions of Russia was attended by around a hundred participants, while a career guidance lecture for children with disabilities was attended by 24 participants of a summer camp organized by ROOI Perspektiva.

Women in STEM*

How we attract women to IT and thereby attempt to reduce the gender gap

kaspersky bring on the future

* STEM (Science, Technology, Engineering, and Mathematics) is a term used to encompass these technical disciplines.

Our goal

Contribute to achieving gender equality in IT

Key tasks

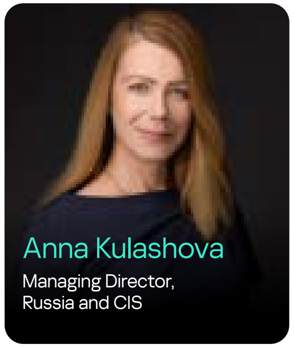
Increase the number of women in software development teams through further cooperation with schools and universities and by providing equal opportunities during the hiring process and for career growth

Develop internal programs to provide additional support to women and new parents

Attract more female members to Kaspersky-founded women in IT online communities

Three questions regarding women in IT

GRI 3-3



Anna Kulashova
Managing Director,
Russia and CIS

Noushin Shabab
Senior Security Researcher
(GReAT)

1

What is the reason behind the gender gap in the IT industry?

— Many hi-tech companies today are striving to ensure equal opportunities to employees and to recruit more women. 26% of IT specialists worldwide are women, which is quite a step forward compared to the figure in 2018, when it was just 15%. The gender gap in the software development field is even more noticeable: according to a study by Stack Overflow, the number of male developers, on average, is 15 times greater than that of women. Among other factors, the disparity appears to stem from the fact that, due to gender stereotypes, girls are less likely than boys to take technical disciplines at school, have less access to technical specializations and, as a result, are less likely to consider a job in IT when choosing their career path.

2

What challenges do women face in IT today?

— No matter how hard a company tries to provide equal opportunities for its employees, a disparity is still inevitable. One of the key problems is the gender pay gap. According to Moscow's Higher School of Economics, in Russia, the pay gap between men and women is on average 30-35% but can reach as high as 70%.

At Kaspersky, women make up 26% of our staff, while in our software development teams women make up around 17%. This disparity should be solved not at the hiring stage, but much earlier — at the school and college stage, by dispelling gender stereotypes and providing more information on educational opportunities available in the field of IT to all students.

Many women rightly believe that their career in IT is not always advancing as fast as some of their male counterparts'. One of the main reasons for this is that women are still more frequently the ones who interrupt their career growth to start a family and go on maternity leave, even though men at Kaspersky can be granted paternity leave too.

3

What does Kaspersky do to support women?

We endeavor to eliminate the gender pay gap. At Kaspersky, every specialist's work is remunerated based on their qualifications and the position in question. We use a market level assessment for the evaluation of every role. This is a detailed kind of analysis that requires additional investment into our compensation and benefits team.

We offer our female employees additional support and benefits when on maternity leave, further education opportunities in their chosen field, and career promotion through the use of individual development plans.

Separate to our internal projects we also run external ones. To recruit more women into the IT industry, we cooperate with schools all over the world. We hold educational events for students, master classes, and have an internship program in place. We also have a specially designated community called Women in Cybersecurity on one of the social media networks, consisting of 17,000 members who share their knowledge and experience to help encourage each other in their professional trajectory.

Our goal is to motivate as many women as possible to pursue a career in IT and the cybersecurity field. Another major online project of ours — Empower Women — attempts to do just this. Its website features personal career growth stories, podcasts and general advice from our female employees in the field of cybersecurity and IT, who share their personal experience, talk about their education and how they built their careers.

Increasing the number of women in software development teams

Recruiting women into the IT industry and supporting them is at the heart of our corporate culture — developed by the board of directors and top management, and conveyed through all the company's departments. Women who achieved particular success within the company participate in support programs, communicating their experience and setting an example to their colleagues, subordinates and aspiring IT specialists.

TC-SI-330-a.3

The total number of full-time staff, classified by gender and function, in the context of gender balance (persons)*

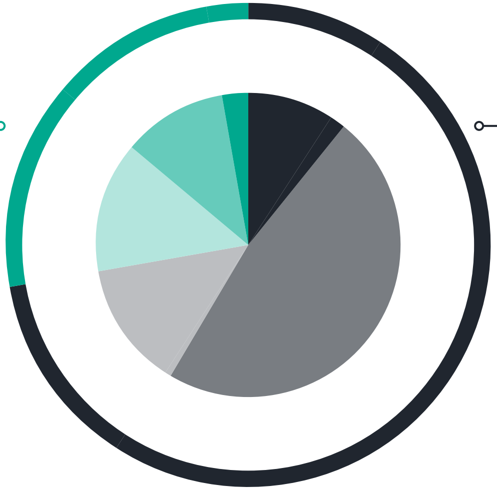
26%

1262 persons

Managers**
4% — 187 persons ●

Technical specialists
9% — 448 persons ●

Other specialists
13% — 627 persons ●



74%

3 520 persons

● Managers
14% — 641 persons

● Technical specialists
42% — 2 005 persons

● Other specialists
18% — 874 persons

* As of June 30, 2022.
** Managers who have one person or more under their command.

Women in IT in the aftermath of the COVID-19 pandemic: signs of progress in the industry

In 2020-21, we carried out research among women working in IT and technology, across Europe, North America, APAC and Latin America. We sought to find out how women in the industry have been affected by the COVID-19 pandemic and the changes in the work culture that it caused.

Some of the findings, presented fully in the Kaspersky Women in Tech Report, are encouraging. Many of the women surveyed either felt a shift in the mindset or attitudes among their employers concerning women in the sphere, or saw tangible progress regarding more female IT or technology leaders entering the sector. In general, just over half (53%) agreed that the number of women in senior IT or technology roles in their organization had increased over the past two years. Interestingly enough, working from home helped some women feel more autonomous in their positions, improving both their confidence and career prospects.

Our research found that companies were also making strides to provide more equal opportunities for women in IT roles. In fact, more than half (56%) of female respondents agreed that gender equality improved in their collective from 2020-2021. Seven-in-ten women believe their skills and experience were considered to be more important than their gender during the interview process for their first IT or tech role. This has translated into the workspace dynamic too: 69% of women working in IT agreed they were now more confident that their opinion would be respected from day one, regardless of their gender.

However, the outlook is not entirely positive. Only 10% of women working in a technology role work in a female-majority team, compared to 48% working in a male-majority team. This is where remote working may play a significant role, with many female respondents stating that a good work-life balance is a key factor that would encourage women toward more technology-related careers moving forward.

GRI 405-2

Ratio of basic salary (wage) to remuneration* among women and men**,%

	Women's salary to men	Women's remuneration to men
Managers***	90	93
Technical specialists	99	98
Other specialists	97	97

* Salary and remunerations depending on the category, length of service, etc.
** Data as per Moscow office of AO Kaspersky Lab.
*** Managers who have one person or more under their command.

Cooperation with schools and colleges

We believe that boys and girls at universities, schools and even in pre-school education should have equal opportunities to develop their talents, including in STEM disciplines. At Kaspersky, we hold events for high-school students to popularize the IT field, where our specialists talk about cybersecurity, working in the IT sector and other professional subjects. We are convinced that motivating young people to choose a certain career trajectory at the college and university level is one of the most effective ways of simultaneously attracting young women into IT specializations. This is why we cooperate with colleges and universities and hold seminars and master classes for students. This brings more specialists into the field, removes barriers for beginners, and promotes development of the IT industry.

For seven years now we have been successfully running a paid internship program for students at Kaspersky called SafeBoard. Participants are given the opportunity to gain practical skills and to work on real cybersecurity projects. The best trainees are thereafter offered a permanent job within the company.

In 2021 Kaspersky launched a pilot internship program at our offices in London, Milan, Paris, Prague, Rome, Singapore and Utrecht. The program is aimed at both undergraduate and graduate students eligible for a position in sales, marketing, IT, technical support, corporate communications, or operations.

Providing equal opportunities at the hiring stage and for future career growth

One of the challenges women face in IT is employment discrimination. According to the Equality in Tech Report conducted by the career marketplace Dice, 38% of female respondents experienced discrimination during the hiring process. And even though in 2021 more than half of the women surveyed by Kaspersky noted that the situation had improved over the last two years and 70% agreed that employers in IT had primarily considered their professional skills, true equality is still a long way off.

To rule out the possibility of gender discrimination, the hiring process at Kaspersky is as transparent as possible and exclusively based on the applicants' technical talents and skills, as well as any other competences they are able to bring to the team. This is a key factor in our decision-making process when appointing personnel or when considering an employee for promotion.

According to the global study conducted by Kaspersky in 2021,44% of women maintain that men progress faster than they do in the tech sphere. By the same token, 41% of women agree that a more equal gender split in the industry would improve their career advancement. We are therefore working to provide more equal growth opportunities for all our employees.

Providing support to women and parents

GRI 401-3

Kaspersky offers support programs for women in all the regions of our presence, though the specifics may vary depending on the laws of a given country.

The coronavirus pandemic increased the overall burden on women, as shown by Kaspersky's 2021 study Women in Tech. According to the report remote working only increased the number of tasks and household chores women had to take on; many experienced the need for additional emotional-psychological support as a result. Following this testing period, all our employees now have access to a 24/7 support hotline.

48%

of the women we surveyed admitted they found juggling work and family life since March 2020 (the start of the pandemic) increasingly stressful

6 out of 10

women did the bulk of household chores and oversaw children's homeschooling and/or homework during the pandemic

The number of employees who took parental leave and those who returned to work afterward (persons).

Employees who took parental leave during the reporting period from 01.01.2021 to 30.06.2022

Total No. of employees 59

👩	👨
57	2

Employees who returned to work after parental leave during the reporting period from 01.01.2021 to 30.06.2022

Total No. of employees 48

👩	👨
46	2

Employees who returned to work and continue working at the company 12 months after parental leave (total during the period from February 2007 to October 2021)

Total No. of employees 88

👩	👨
83	5

Bringing women together in online communities on the topic of cybersecurity

Our company runs two major online projects for women in IT. Our goal is to help women in the industry overcome barriers and achieve success. To this aim, we spread the word about any existing opportunities for professional growth within our industry among accomplished women in the sphere.

Sociologists from Moscow's Higher School of Economics agree that information campaigns to dispel gender myths might be helpful in increasing women's employment rate in hi-tech industries.

In 2021, we launched Empower Women, a project dedicated to women in cybersecurity. The project features studies on women in the IT industry across various regions, news, and also our Women in IT podcast, featuring Kaspersky's female employees sharing their professional and personal experiences of working in the sphere. We also actively promote the Women in Tech podcast in France. Just three episodes in, it has already had over 600 downloads.

Five years ago we developed an initiative envisioned by one of our female employees — Women in Cybersecurity — an online community for women in IT on one of the social media networks. With around 17,000 members, it is one of the largest such online communities today. This is an active, growing and supportive community with professionals in cybersecurity and other IT fields, one in which members ask questions, share their experiences, and exchange advice on career advancement.

Following requests by members of the community, we plan to create new content (interviews, podcasts, etc.) on the Empower Women website. We will also develop mentoring programs involving Kaspersky's experts who will offer consultations to the community members.

Kaspersky is in active cooperation with various NPOs around the world, including Girls in Tech, Advisory, Ada's list, Singapore Council of Women's Organizations and Division Zero (Div0) to produce joint educational events and discussions focused on female target groups.

In March 2021, ahead of the International Women's Day, we held a webinar together with Ada's List, an organization that supports women in STEM. The discussion featured members of that organization, Kaspersky's employees, plus independent experts, and the central talking point was dedicated to tech business assistance in supporting and promoting women in IT. There were also conversations on progress made in support for women in the workplace, the work-life balance, role models, the COVID-pandemic, and remote work influencing women's free time and work time in IT. The event was attended by 60 people.

Kaspersky is also a partner with the French organization CEFCYS, which seeks to empower women to realize themselves in cybersecurity — 10 of our specialists are CEFCYS members. In the context of this cooperation we offer discounts for our training courses, have organized a master class in reverse engineering, participated in CEFCYS summit, carried out a PR campaign on women in cybersecurity and invited speakers from the organization on our podcast.

>600

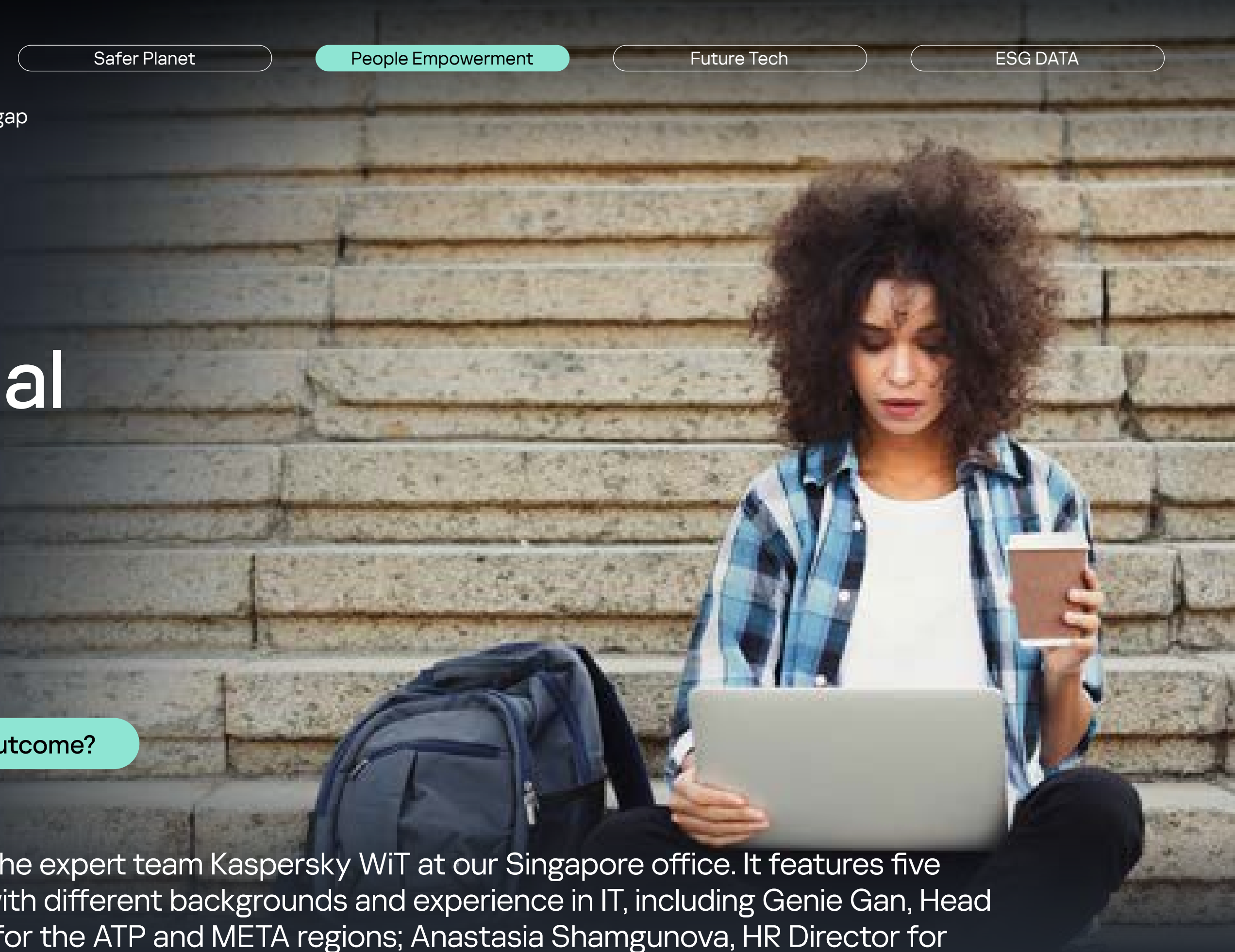
Over 600 downloads of the first three episodes of the Women in Tech podcast in France

17 000

members have joined the Women in Cybersecurity community

Kaspersky's plans for 2023

- Continue to promote the recruitment of more women in the IT industry and attempt to achieve gender equality on software development teams — including through the SafeBoard internship program across Russia.
- Participate in specialized events like the European Cyberwomanday Awards and support the development of discussions about women in cybersecurity. We will offer professional training courses on basic cybersecurity to victims of domestic violence co-authored with NPOs, so that women can use the knowledge they gained to look for employment.
- Continue to develop the Empower Women portal to raise awareness about career possibilities in IT for women. We plan to introduce new sections and post more interviews that will meet the community members' professional demands.



Sustainable development in action

How we help students choose their professional path and support women in IT

Our goal

To contribute to achieving gender equality in IT

On March 8, 2021, the government of Singapore invited Kaspersky to join the initiative Singapore Women in Tech Corporate Pledge. As part of that initiative, we were one of more than 50 companies to commit to creating a positive environment for attracting more women into the IT field, as well as for the professional development of female technical specialists. We made three commitments:

1. To encourage and enable female undergraduates to pursue cybersecurity careers through activities such as career talks, and book prizes
2. To promote cyber literacy and better the understanding of cybersecurity career pathways
3. To build a Kaspersky WiT resource team to heighten confidence of female professionals in cybersecurity through mentorship and coaching

What was the outcome?

We established the expert team Kaspersky WiT at our Singapore office. It features five female experts with different backgrounds and experience in IT, including Genie Gan, Head of Public Affairs for the ATP and META regions; Anastasia Shamgunova, HR Director for the Eastern Region (ATP, the Middle East, Turkey and Africa); and Noushin Shabab, Senior Security Researcher with the Global Research & Analysis Team (GReAT). Together with Singapore-based women support foundations, government agencies and NPOs, the team has implemented a series of activities for both college graduates and technical specialists. For example, in August 2021 our experts hosted, together with the youth-led NPO Advisory, an event called Ladies' Night:Women in Tech for 175 students . The participants talked about what challenges they face in IT and how they are overcoming those challenges, and what skills are required to work in the hi-tech field. The Kaspersky WiT team participated in Wave 2 of the Advisory Mentorship Programme for students. More than 1250 professionals from the IT industry became mentors to more than 1500 Singaporean college students. Meanwhile, together with the Singapore Cybersecurity Community Div0 in January 2022 we hosted a three-day workshop for female security specialists on how to write simple and sound YARA rules that can be used to identify malware families from a collection of files and to classify malware to assist the malware analysis process.

Education

How we educate specialists in information security

kaspersky bring on the future

Our goal

To train students in cybersecurity and level-up IT specialists

Key objectives

Attract schools, universities and colleges worldwide to participate in our educational programs

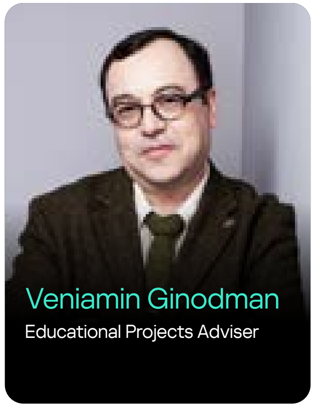
Increase the availability of in-demand classes for industry professionals on the latest aspects of information security

Popularize information security in accessible and understandable terms, such as through hi-tech art, in order to increase our media outreach

Three questions regarding the company's activities in personnel training

Evgeniya Russkikh

Academic Affairs Group Manager



Veniamin Ginodman

Educational Projects Adviser

GRI 3-3

1

Why does Kaspersky pursue educational projects?

Education worldwide is struggling to keep up with technological advancements. There is currently a shortage of skilled specialists in the industry, and if businesses fail to train more personnel to fill the gap, the situation will become critical over the next few years. That is why we at Kaspersky, being a socially responsible company, create our own learning programs aimed at interaction with educational institutions and with audiences in need of such additional training. We invest in educating both school and college students, as well as already experienced cybersecurity specialists in need of advanced training. All education focuses on the company's main area of expertise: information technology and information security.

2

Which key projects can you single out?

We work with students from all over the world, offering both training sessions in specialized professions and involvement projects for first-year university students, such as through our Kaspersky. Academy Secur'IT Cup student project competitions, for example. In our Moscow-based Kaspersky Math Vertical program, as well as in the federal Digital Lesson project, we teach schoolchildren all about cybersecurity — helping them to protect themselves against possible cyberthreats while simultaneously attracting them to our industry.

We seek not just to inform the public about cyberthreats and new trends in information security using conventional press releases and presentations of new products, but to also communicate our technologies through the language of art, more commonly understood by the general public. That is why we support the high-tech art field and also lay the groundwork for collaborations among our experts, scientists and modern artists; we share our expertise and technologies and in turn produce joint artworks and exhibitions.

3

What are some of the successes of the company's educational programs?

Our project Kaspersky.Academy is currently supported by over a hundred partner universities in 71 countries across the world. And over 6000 students have already participated in the Secur'IT Cup competition.

In the four years since its inception, students in the Kaspersky Math Vertical program have won numerous awards. To mention a few examples, three students received diplomas in the InnoCTF Junior 2021 computer security tournament for school students, and in May 2022, a team from Moscow School No. 1409 (the same school involving 10th-graders in our Math Vertical study) won the city-wide Victory-Museum Hackathon. Moreover, two graduates of the Math Vertical are already employed in Kaspersky's R&D department. We frequently get requests from other Russian regions, asking for the establishment of Math Vertical classes at their schools, and we therefore endeavor to make this program available for all school students across the country.

Engaging schools, universities and colleges in our educational programs

Kaspersky's involvement with educational institutions began 10 years ago when our experts began holding lectures on cybersecurity at both Moscow State University and the Bauman Moscow State Technical University. We quickly understood that we wanted to do more, so we developed the Kaspersky.Academy project to scale up our learning initiatives and make them accessible to anyone interested. Today we have the company's team leaders, heads of departments, top specialists and guest experts in information security on the Academy's speaker roster. This project has also greatly helped us develop our international brand.

In 2022, the fifth annual Secur'IT Cup competition for information security projects took place. Participants were invited to design projects aimed at solving cybersecurity problems in areas such as mobile device security, care for the elderly, protection of smart homes, and combating cheating in online chess. Every year the competition gathers around 1500–2000 students from all over the world, and the winner is awarded a $10,000 grant.

In 2021, we launched a new project — the international KIPS Championship for students. KIPS, which stands for Kaspersky Interactive Protection Simulation, is game-based training, raising awareness of information-security threats for both management and employees. 53 student teams from all over the world took part in the championship.

Meanwhile, 25 students are now employed in our company's European and Singapore offices as a result of the global internship program launched in 2021. We held a series of live streamed sessions for them as well as for students from partner universities, during which the company's experts talked about their jobs in an effort to inform and encourage students about their potential future work sphere and also help them better navigate cybersecurity in general.

As part of an ongoing collaboration with schools, for the last six years Kaspersky has regularly been on the board of the above-mentioned Digital Lesson, the federal IT project for school students jointly curated by Russia's Ministry of Education and the Ministry of Digital Development, Communications and Mass Media. The project focuses on education and career counseling for school students in the field of IT. Over 4.8 million Russian-speaking school students attended Digital Lesson during the reporting period.

Kaspersky's employees teach a special course on the Basics of Information Security at Moscow's School No. 1409, providing students with an introduction to the basics of programming and advanced tech, along with information on how to protect oneself against cyberthreats. Since September 2021 moreover, our company's experts have held an online advancement course on Protecting the Information Space of Young Children and Teenagers for 210 teachers in Moscow. All the teachers have received a course completion certificate from Moscow's Department of Education and Science.

>100

Kaspersky.Academy has over a hundred partner universities across 71 countries

>6 000

Over 6000 students from all over the world have taken part in the Secur'IT Cup competition in the four years since its inception — winners receiving grants of up to $10,000

25

students are now employed in Kaspersky's European and Singapore offices thanks to our global internship program launched in 2021

4.8 million

Over 4.8 million Russian-speaking school students attended the Digital Lesson during the reporting period

Increasing the availability of classes on current cyberthreats for industry professionals

Both emerging technologies and legislation are the main drivers of new professions and competences. This is why continuous training in cybersecurity is one key requirement for specialists already working in the industry.

>100

Over a hundred new clients from 30 countries took training courses on cybersecurity via the Kaspersky Expert Training portal during the reporting period. The highest demand for training came from Singapore, the U.S.A. and Israel

We assist with such further training with our own online education portal called Kaspersky Expert Training. This is a tool allowing cybersecurity specialists to broaden their knowledge, study new threat detection strategies, and work with the impacts of those threats. We do not provide fundamental education like universities, colleges or specialized institutions, but rather take current knowledge and apply it to work in the here and now.

In 2021, we transferred all our expert training courses on security to the Kaspersky Expert Training portal. That same year the courses were also made available to the general public for purchase, and as a result we acquired over a hundred new customers from 30 countries. Previously, the training courses could only be taken by corporate clients, government agencies, and — on a free-of-charge basis — INTERPOL officers.

We are continually developing new training courses. For instance, in April 2022 we launched a reverse engineering class held by researchers of our GReAT (Global Research & Analysis Team) — cybersecurity experts Denis Legezo and Ivan Kwiatkowski. There's also a Windows Digital Forensics course in the pipeline, which will teach users how to search for signs of intrusion in components of the Windows operating system.

Popularizing information security through art

To get the subject of technology and information security across to the general public effectively, we employ somewhat non-traditional methods. In 2018, Kaspersky launched a project on ‘science art’. Through interaction of our experts with artists, and the collaborative search for new mediums of expression, we communicate and inform people on technology and cybersecurity.

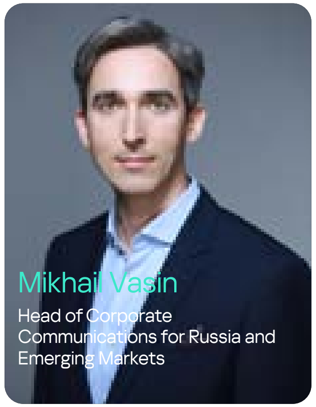
~100 000

Around 100,000 visitors attended the exhibitions May the Other Live in Me and New Elements — the events were covered by 239 media-outlets

The idea came about thanks to Thomas Feuerstein, an Austrian modern artist, who took an interest in the company’s research and development and suggested visualizing our cyberthreat map. That led to his work, DAIMON — which materializes cyberattacks related to the Internet of Things — being exhibited at the Moscow Museum of Modern Art that same year (2018).

From 2021–2022, the company acted as a strategic partner for two international hi-tech art exhibitions – May the Other Live in Me and New Elements — in the New Tretyakov Gallery in Moscow, which were attended by almost 100,000 visitors. The shows featured works by well-known artists in collaboration with Kaspersky experts. As part of the New Elements project, the company also supported the idea of holding an international symposium at the intersection between art, technology and nature. These partnerships were realized in cooperation with the Laboratoria Art&Science Foundation, which has spearheaded the promotion of the science-art movement in Russia.

— Our collaboration with the Laboratoria Art&Science Foundation was more than just financial and media support for hi-tech art.


Mikhail Vasin

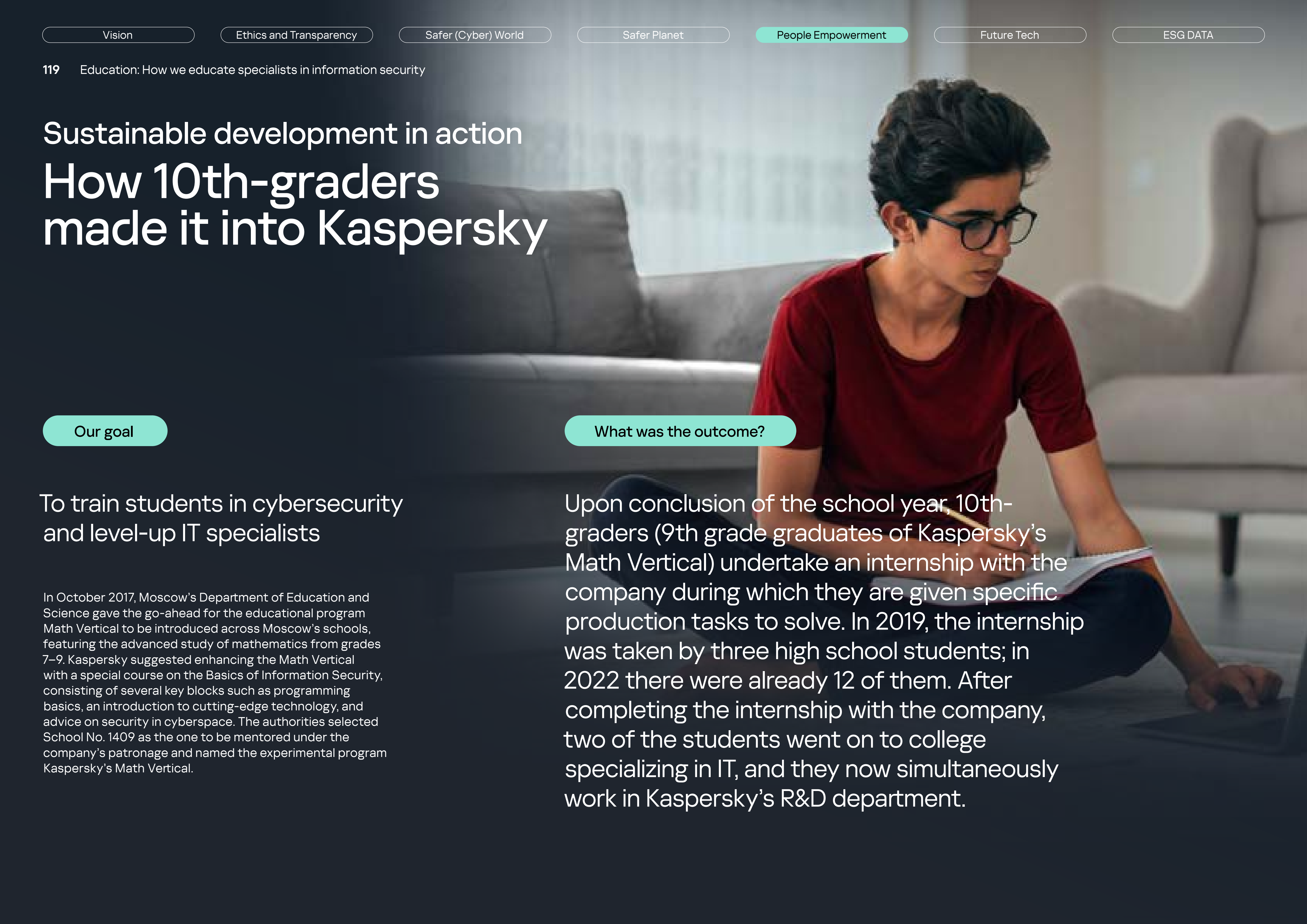
Head of Corporate Communications for Russia and Emerging Markets

As part of this collaboration, the artists received new tools and expert consultations from Kaspersky specialists, while our specialists, in turn, discovered new ideas for their work and had the opportunity to engage in open dialogue with the general public through art. But it was the visitors who gained the most from this collaboration: they came away with new impressions, a valuable sensory and intellectual experience, and a reminder that they need to increase their digital literacy and think seriously about their own cybersecurity.

Moving forward, we would like to support the creation of an incubator for science art, where creators can generate art objects together with scientists and tech companies. Such an incubator would be a scientific, technological and cultural space, helping to popularize information security among the general public.

Kaspersky's plans for 2023

- Hold the international Secur'IT Cup competition in CIS, Asia-Pacific and META countries, as well as the international KIPS championship in November; help set up classes for the IT Vertical in 300 schools across Moscow; instruct 300 teachers in our advanced qualification courses on Protecting the Information Space of Young Children and Teenagers for the 2022-2023 school year.
- Elaborate and offer a general course on cybersecurity for aspiring specialists in the field. Our company will offer this course free of charge to people with disabilities in order to facilitate their entry into the profession. We will also offer two free basic training courses on the Kaspersky.Academy portal, and four supplementary courses on the Online Cyber Security Training portal.
- Continue to collaborate with the Laboratoria Art&Science Foundation in support of high-tech art.



Sustainable development in action

How 10th-graders made it into Kaspersky

Our goal

To train students in cybersecurity and level-up IT specialists

In October 2017, Moscow's Department of Education and Science gave the go-ahead for the educational program Math Vertical to be introduced across Moscow's schools, featuring the advanced study of mathematics from grades 7–9. Kaspersky suggested enhancing the Math Vertical with a special course on the Basics of Information Security, consisting of several key blocks such as programming basics, an introduction to cutting-edge technology, and advice on security in cyberspace. The authorities selected School No. 1409 as the one to be mentored under the company's patronage and named the experimental program Kaspersky's Math Vertical.

What was the outcome?

Upon conclusion of the school year, 10th-graders (9th grade graduates of Kaspersky's Math Vertical) undertake an internship with the company during which they are given specific production tasks to solve. In 2019, the internship was taken by three high school students; in 2022 there were already 12 of them. After completing the internship with the company, two of the students went on to college specializing in IT, and they now simultaneously work in Kaspersky's R&D department.

Annexes

121 About the report

122 Associations, unions, initiatives

123 Compliance of the company’s initiatives with the UN SDG

131 GRI Standards

146 SASB Standards

About the report

GRI 2-1 GRI 2-2-a GRI 2-3 GRI 2-14

— In the present report (hereinafter referred to as the report), Kaspersky discloses information in accordance with the requirements of the international sustainable development standards, such as the Global Reporting Initiative Guideline (GRI 2021) and the industry-specific Sustainability Accounting Standards BoardGuideline (SASB) for Software & IT-Services. The compliance of disclosed information with the requirements of these standards is presented in the sections GRI Standards Compliance Guide and SASB Standards Compliance Guide. The company's sustainable development initiatives are brought into line with the objectives of the UN SDG.

— The report is drafted in accordance with the reporting principles of the international GRI standard: accuracy, balance, clarity, comparability, completeness, sustainability context, timeliness and verifiability. The report content is defined by the significance assessment of Kaspersky's impact on sustainable development aspects (economy, environment and society), the company's strategic ESG priorities and goals, as well the requirements of the international GRI and SASB Standards concerning disclosure of information. In the preparation of this report, the company defined the material topics using the procedure in accordance with the universal GRI (3-1) standards. Since the GRI Standards Guideline 2021 does not include an industry-specific standard for IT companies, the SASB Standard for Software & IT-Services was used as an industry-specific reference in the procedure to define material topics. In disclosing the information to each of the material topics, the relevant disclosures from the corresponding thematic standards of the GRI Standards Guideline (200, 300, 400) were used. To disclose all material topics that have no applicable matching thematic GRI standard, the requirements of GRI 3-3 for the disclosure of management approach were used.

— The process of gathering information for the report included stakeholder opinion research, a series of interviews with top managers, heads of departments and functions, participants involved in the company's sustainable development initiatives, programs and projects, as well as analysis of the external context, internal documents and media publications.

— The information published in this report covers, unless expressly stated otherwise*, the activities of AO Kaspersky Lab, including the company's headquarters, AO Kaspersky Lab (HQ), and its affiliated companies in the countries of presence (regional offices): JSC Kaspersky Lab, JSC VSSI (real estate company), Kaspersky Lab UK Limited, Kaspersky Lab Inc., Kaspersky Labs GmbH, Kaspersky Lab France EURL, Kaspersky Labs Asia Ltd, KK Kaspersky Labs Japan, KL Anti-Virus Solutions, JSC Kaspersky Group, Kaspersky Lab ME FZ-LLC, Kaspersky Info Systems SRL, Kaspersky Lab Czech Republic S.R.O., Kaspersky Lab South Africa (Pty) Limited, Kaspersky Bilisim Hizmetleri San. Ve Tic Ltd, Kaspersky Lab KZ, Kaspersky Lab Israel Ltd, Kaspersky Lab Denmark Aps, Kaspersky Lab S.L.U., Kaspersky Lab Italia S.r.l., Kaspersky Lab B.V., Kaspersky Lab Unipessoal LDA, Kaspersky Lab Switzerland GmbH, Kaspersky Security Solutions Ireland Limited, Threatpost, Inc., Kaspersky Lab Soluções Seguras Brasil LTDA, Kaspersky Technology Development (Beijing) Co Ltd, Kaspersky Lab Australia and New Zealand Pty Ltd, Kaspersky Lab India Private Limited, Kaspersky Lab SEA SDN. BHD., Kaspersky Lab Korea Ltd, Kaspersky Lab Singapore Pte Ltd, Kaspersky Lab Canada Limited, Kaspersky Lab BLR LLC, Kaspersky Lab Rwanda Ltd., BPI Bureau de Promotion Immobilière SA (holding company), Nexway Group AG (holding company), Nexway LLC, B4N Group Limited (holding company), Programmiruemie seti LLC, NPO AproTech LLC and Shield Mode LLC.

— This report covers the period from January 1, 2021 to June 30, 2022 года. Further sustainable development reports will be published annually.

— This is the company's first sustainable development report. Previous publications include corporate social responsibility reports for 2015–2016, 2017–2018, and 2019–2020.

— Kaspersky's forward-looking statements and plans in this report are of a preliminary nature and may vary depending on external and internal circumstances uncertain at the time of planning. Thus, the results of the activities in the field of sustainable development in the succeeding reporting period may vary from those declared in the present report.

— This report was reviewed and approved by CEO of Kaspersky. This report is published on the company's website in Russian and English language.

* Information concerning the ecological impacts only covers Kaspersky's headquarters (Russian office).

Associations, unions, initiatives

GRI 2-28

Kaspersky cooperates closely with numerous international organizations and law enforcement agencies, being involved in joint operations, cyberthreat investigations, cyberdiplomacy and contributing to an open and safe internet.

INTERPOL. As part of long-term relations with INTERPOL, Kaspersky provides support in human resources, training, digital forensic tools and recent data on the activities of cybercriminals. Cybercrime knows no national borders, so our cooperation with INTERPOL is of vital importance for worldwide attack prevention.

No More Ransom. This initiative was launched in 2016 by Kaspersky together with Europol, the Dutch national police and McAfee to help ransomware victims in decrypting their data. The initiative involves 188 partners and has already helped more than 1.5 million people worldwide.

European Union Agency for Cybersecurity (ENISA). Kaspersky takes part in several of the agency's research and publications, while also being a member of ENISA's special working group on the cyberthreat landscape.

The Paris Call for trust and security in cyberspace. Kaspersky was one of the first to support the French government's initiative, and in 2021, together with Cigref, the digital association of companies and public administrations, co-chaired Working Group 6 (WG6) to improve the level of security in cyberspace. The working group presented an analytical report suggesting practical tools for protection of supply chains and improving their cybersecurity.

Kaspersky's Global Transparency Initiative (GTI) was also distinguished as the best implementation practice of the Paris Call's principle 6 on lifecycle security.

The Geneva dialogue on responsible conduct in cyberspace. Kaspersky is a partner of the international process to discuss and elaborate solutions for the security of digital products and cybersecurity.

Coalition Against Stalkerware. This initiative, which Kaspersky helped launch in cooperation with a wide circle of international partners, is aimed against commercial spyware. The coalition keeps growing and is supported by non-governmental organizations and partners involved in helping victims of domestic violence, protecting digital rights, IT security and academic research worldwide.

Beyond that, Kaspersky is involved in the following industry associations:

- Australia Cyber Security Centre
- CERT-In, India
- Data Security Council of India
- Indonesia's National Cyber and Encryption Agency, BSSN
- Communication and Information System Security Research Center (CISSReC)
- Singapore's Cybersecurity Agency's Cyber Security Awareness Alliance
- Singapore's Infocomm Media Development Authority's Women in Technology movement
- Singapore Police Force's APPACT (Alliance of Public PrivAte Cybercrime sTakeholders)
- SGTech's Cybersecurity Chapter
- Singapore Computer Society
- Vietnam's Authority of Information Security & National Cyber Security Center
- Council of Europe
- Deutschland sicher im Netz e.V.
- IT-Sicherheitscluster e.V.
- BVMW e.V. Der Mittelstand
- Actor of the Plattform Industrie 4.0
- Cybermalveillance
- Paris Call
- Renaissance Numérique
- CEPEL (Center of Research in Electric Energy)
- MASP (Museum of Art of São Paulo)
- Ronald McDonalds Institute
- American Chamber of Commerce
- Luchadoras: Mexican women organization working on a free of violence internet
- Industry IoT Consortium (IIC)
- Global Platform
- International Telecommunication Union (ITU-T)
- Institute of Electrical and Electronics Engineers (IEEE)
- Forum of Incident Response and Security Teams (FIRST)
- European Union Agency for Cybersecurity (ENISA)
- ISO/IEC SC41 (ISO - International Organization for Standardization. Active members of SC41 WG3 (Reference Architecture and Trustworthiness) and WG5 (Compatibility in IoT))
- RF CCI (Chamber of Commerce and Industry of the Russian Federation)
- Russoft
- ARPP (Software Developers' Association "Domestic Soft")
- RSPP (Russian Union of Industrialists and Entrepreneurs)
- APKIT (Information & Computer Technologies Industry Association)
- TK-MTK-22 "Information Technologies"
- SRPO TEC (The Union of Software Developers and Information Technologies in the Fuel and Energy Complex)
- The Alliance for Protection of Children in the Digital Environment
- Autonomous Non-Commercial Organization "Digital Economy"

Compliance of the company's initiatives with the UN SDG

GRI 2-23

5 areas of the ESG strategy	Agenda for Sustainable Development	Sustainable Development Goals (SDG)
Ethics and transparency	• Transparency of source code and processes • Data and privacy protection • Transparency in management and business resilience	8 DECENT WORK AND ECONOMIC GROWTH 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
Safer cyberworld	• Protection of critical infrastructure in a changing world • Assistance with the investigation of cybercrimes on a global level • Protection of users against cyberthreats	8 DECENT WORK AND ECONOMIC GROWTH 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
Safer planet	• Reducing the environmental impact of our infrastructure, business activities and products	7 AFFORDABLE AND CLEAN ENERGY 12 RESPONSIBLE CONSUMPTION AND PRODUCTION 13 CLIMATE ACTION
People empowerment	• How we take care of our employees • Women in STEM • Inclusivity and availability of technologies • Employee development in IT	4 QUALITY EDUCATION 5 GENDER EQUALITY 8 DECENT WORK AND ECONOMIC GROWTH 10 REDUCED INEQUALITIES
Future Tech	• Cyber-immunity for new emerging technologies	9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Correlating the UN SDG objectives with Kaspersky's initiatives under its ESG strategy

Goal No. 4

Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all

Kaspersky's strategic area:

People Empowerment / Employee Development in IT and Women in STEM

SDG No. 4*	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
4.1 By 2030, ensure that all girls and boys complete free, equitable and quality primary and secondary education leading to relevant and Goal-4 effective learning outcomes 4.3 By 2030, ensure equal access for all women and men to affordable and quality technical, vocational and tertiary education, including university 4.4 By 2030, substantially increase the number of youth and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship 4.5 By 2030, eliminate gender disparities in education and ensure equal access to all levels of education and vocational training for the vulnerable, including persons with disabilities, indigenous peoples and children in vulnerable situations	• Women in STEM: facilitating the elimination of barriers for more women to have the possibility of growth and development in technical professions • Employee development in IT: educational programs in information security for colleges, schools and the general public	Women in STEM: how we attract women to IT and thereby attempt to reduce the gender gap Education: how we educate specialists in information security

* Hereinafter — the objectives corresponding to the specified SDG as formulated in the UN Sustainable Development Goals, contributed to by Kaspersky's specific sustainable development goals, programs and initiatives.

Goal No. 5

Achieve gender equality and empower all women and girls

Kaspersky's strategic area:
People Empowerment / Women in STEM

SDG No. 5	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
5.1. End all forms of discrimination against all women and girls everywhere 5.5. Ensure women's full and effective participation and equal opportunities for leadership at all levels of decision making in political, economic and public life	• Women in STEM: facilitating the elimination of barriers for more women to have the possibility of growth and development in technical professions	Women in STEM: how we attract women to IT and thereby attempt to reduce the gender gap
5.8. Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women	• Employee care with respect to women support within the company: developing leadership, increasing the number of women in management positions, childcare leave and possibilities to continue career	Team: how we take care of our employees

Goal No. 7

Affordable and clean energy. Ensure access to affordable, reliable, sustainable and modern energy for all

Kaspersky's strategic area:
Safer Planet / Energy efficiency and energy saving

SDG No. 7	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
7.3 By 2030, double the global rate of improvement in energy efficiency	• Reducing our environmental impact. Energy efficiency and energy saving. . Increasing the energy efficiency of our data centers, offices and business activities by using advanced energy-saving technologies	Ecological footprint: how we are reducing our impact on the environment

Goal No. 8

Decent work and economic growth. Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all

Kaspersky’s strategic areas:

Ethics and transparency / Transparency in management and business resilience

Safer cyber world / Protection of critical infrastructure and Protection of users against cyberthreats

People Empowerment / Employee care. Employee development in IT and Women in STEM

SDG No. 8	Specific sustainable development areas within Kaspersky’s ESG strategy	See more in the report
8.2. Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors	• Protection of critical infrastructure in a changing world. Ensuring software and digital resilience of industry and critical infrastructure by using an ecosystem of state-of-the-art IT technologies and services.	Critical infrastructure: how we protect it in a changing world
8.3. Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services	• Protection of users against cyberthreats. Creating services and products for small and medium businesses that ensure preventing loss of productivity resulting from hacker activities.	Users: how we protect personal data and ensure privacy
	• Transparency in management and business resilience. Providing business opportunities and creation of jobs for 1,300 partners worldwide.	Ethical practices: how weare increasing our management transparency and business resilience

Goal No. 8

Decent work and economic growth. Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all

8.5. By 2030, achieve full and productive employment and decent work for all women and men, including for young people and persons with disabilities, and equal pay for work of equal value	• Employee care. Provision of decent working conditions and equal opportunities, taking care of employees' physical and mental well-being in the course of their professional development	Team: how we take care of our employees
	• Employee development in IT: educational programs in information security for colleges, schools and the general public	Education: how we educate specialists in information security
	• Women in STEM: facilitating the elimination of barriers for more women to have the possibility of growth and development in technical professions	Women in STEM: how we attract women to IT and thereby attempt to reduce the gender gap
8.6. By 2020, substantially reduce the proportion of youth not in employment, education or training	• Employee development in IT: educational programs in information security for colleges, schools and the general public	Education: how we educate specialists in information security
8.8. Protect labour rights and promote safe and secure working environments for all workers, including migrant workers, in particular women migrants, and those in precarious employment	• Employee care. Provision of decent working conditions and equal opportunities, taking care of employees' physical and mental well-being in the course of their professional development	Team: how we take care of our employees

Goal No. 9

Industry, innovation and infrastructure. Build resilient infrastructure, promote sustainable industrialization and foster innovation

Kaspersky's strategic areas:

Ethics and transparency / Transparency of source code and processes

Safer cyber world / Protection of critical infrastructure

Future Tech / Creating cyber-immunity for new emerging technologies

SDG No. 9	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
9.1 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all	• Transparency of code and processes. Investing in building our own data infrastructure to ensure transparency and safety of user data.	Global Transparency Initiative: how and why we revealed our code and processes
	• Protection of users against cyberthreats. Creating services and products for small and medium businesses that ensure preventing loss of productivity resulting from hacker activities	Global Transparency Initiative: how and why we revealed our code and processes
	• Protection of critical infrastructure in a changing world. Ensuring software and digital resilience of industry and critical infrastructure by using an ecosystem of state-of-the-art IT technologies and services	Global Transparency Initiative: how and why we revealed our code and processes
	• Creating cyber-immunity for new emerging technologies. Connecting new partners to the development of the safe internet of tomorrow.	Global Transparency Initiative: how and why we revealed our code and processes

Goal No. 10

Reduce inequality. Reduce inequality within and among countries

Kaspersky's strategic area:

People Empowerment / Employee care. Digital inclusion

SDG No. 10	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
10.1. By 2030, progressively achieve and sustain income growth of the bottom 40 per cent of the population at a rate higher than the national average 10.2. By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status	• Employee care. Provision of decent working conditions and equal opportunities, taking care of employees' physical and mental well-being in the course of their professional development • Digital Inclusion: increasing accessibility of information security products, services and capabilities to individuals with special needs	Team: how we take care of our employees

Goal No. 12

Responsible consumption and production. Ensure sustainable consumption and production patterns

Kaspersky's strategic area:

Safer Planet / Responsible waste management

SDG No. 12	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
12.5. By 2030, substantially reduce waste generation through prevention, reduction, recycling and reuse	• Reducing the environmental impact. Responsible waste management in all of the company's activities and increasing the proportion of ecologically-friendly and recyclable materials	Ecological footprint: how we are reducing our impact on the environment

Goal No. 13

Climate action. Take urgent action to combat climate change and its impacts

Kaspersky's strategic area:
Safer Planet / Reducing greenhouse gas emissions

SDG No. 13	Specific sustainable development areas within Kaspersky's ESG strategy	See more in the report
13.2. Integrate climate change measures into national policies, strategies and planning 13.3. Improve education, awareness-raising and human and institutional capacity on climate change mitigation, adaptation, impact reduction and early warning	• Reducing the environmental impact. Responsible waste management in all of the company's activities and increasing the proportion of ecologically-friendly and recyclable materials • Publicly communicating the sustainable development practices, including those related to increasing the energy efficiency and reducing the carbon footprint	Ecological footprint: how we are reducing our impact on the environment

GRI Content Index

This section contains a GRI Standards reporting compliance guide (as of 2021), as well as additional information according to the requirements of the GRI Standards, not reflected in the main report (see Remarks).

Kaspersky has submitted the sustainable development report for the period from January 1, 2021 to June 30, 2022 in accordance with the requirements of GRI Standards Guide.

GRI Standards Index

Compliance of reporting elements with the GRI Standards Guide 2021

Material Topics	Description	Section of the report	Remarks
GRI 2	**General Disclosures**		
	The organization and its reporting practices		
2-1	Name of the organization	About the company Annexes. About the Report Annexes. GRI Standards Index	Parent company name: Holding Company Kaspersky Labs Limited (registered in the UK). Main legal entity in the Russian Federation is AO Kaspersky Lab. The organization is headquartered at 39A/2 Leningradskoe Shosse, Moscow, 125212, Russian Federation. Legal information: https://www.kaspersky.ru/legal.ru
2-2	Entities included in the organization's sustainability reporting	Annexes. About the Report (2-2-a) Annexes. GRI Standards Index (2-2-b, c)	2-2-b, c. The consolidated financial statement of Kaspersky Labs Limited is published here: https://find-and-update.company-information.service.gov.uk/company/04249748/filing-history. At the time of publication of this report, the consolidated financial statement for 2021 is available. The list of subsidiary companies to be included in the disclosure limits of this report differs from the list of entities in the consolidated financial statement for 2020; these variations are attributable to the fact that new regional offices were opened and some were closed in the period from 2021–2022. These changes will be reflected in the consolidated financial statement for 2021 and 2022. The companies included in the present report are listed under Annexes. About this report. The limits of disclosure concerning non-financial values cover the companies in this list, unless otherwise specified in disclosure notes. Thus, the results concerning the environmental aspects of sustainable development in this report only include the Moscow office (aka AO Kaspersky Lab) that represents the most significant environmental impact, while no data has been collected concerning other offices in the reporting period.
2-3	Reporting period, frequency and contact point	Annexes. About the Report Contacts and Feedback	This is Kaspersky's first sustainable development report. The publication date of the first report is March 2023. Further sustainable development reports will be published annually, at the same time as the financial statement.
2-4	Restatements of information	Annexes. GRI Standards Index	This is Kaspersky's first sustainable development report, there has been no data revision or reformulation.
2-5	External assurance	Annexes. GRI Standards Index	This report has not been externally certified.

	Activities and workers		
2-6	Activities, value chain and other business relationships	About the company Sustainable development. Stakeholder engagement Ethical practices: how weare increasing our management transparency and business resilience. Reducing risks in the supply chain Annexes. GRI Standards Index	2-6-c. Description of essential partnerships is given in the material topics disclosure. 2-6-d. This is Kaspersky's first sustainable development report.
2-7	Employees	Team: how we take care of our employees. Ensuring favorable work and development conditions for our employees while increasing engagement	2-7-e. No significant headcount variations were recorded during the reporting period.
2-8	Workers who are not employees	Annexes. GRI Standards Index	All workers are Kaspersky's employees.
	Governance		
2-9	Governance structure and composition	Ethical practices: how weare increasing our management transparency and business resilience. Maintaining corporate management transparency	
2-10	Nomination and selection of the highest governance body	Ethical practices: how weare increasing our management transparency and business resilience. Maintaining corporate management transparency Annexes. GRI Standards Index	2-10-b. The nomination criteria include recommendations from shareholders and members of the board of directors of the holding company, as well as from members of the governing board, based on the competence of the candidates.
2-11	Chair of the highest governance body	Ethical practices: how weare increasing our management transparency and business resilience. Maintaining corporate management transparency	

2-12	Role of the highest governance body in overseeing the management of impacts	Sustainable development. Managing sustainable development Ethical practices: how weare increasing our management transparency and business resilience. Maintaining corporate management transparency Annexes. GRI Standards Index	As of 2023, the management structure is going to include a committee on sustainable development.
2-13	Delegation of responsibility for managing impacts	Sustainable development. Managing sustainable development	
2-14	Role of the highest governance body in sustainability reporting	Annexes. About the Report Annexes. GRI Standards Index	The involvement procedure for the highest management body in the approval of material topics and sustainable development reports is yet to be developed: the plans for 2023 include the establishment of a committee on sustainable development in the management structure. The information regarding the approval of this report is given under **Annexes. About this report.**
2-15	Conflicts of interest	Annexes. GRI Standards Index	Avoiding conflict of interests between members of Kaspersky's highest management bodies is enshrined in the company's anti-corruption policy. The company implements a declaration policy concerning any participation in other companies in the capacity of founding members, shareholders, or board members. Concurrent participation is not allowed without the consent of Kaspersky's board of directors or governing board. Members of the board of directors and the governing board only occupy governing positions in companies owned by or affiliated with Kaspersky Labs Ltd.
2-16	Communication of critical concerns	Annexes. GRI Standards Index	2-16-a. The procedure to inform the board of directors and the governing board includes regular meetings and conferences, where the management bodies get the latest updates on critical topics directly from the department heads. 2-16-b. During the reporting period, the company did not maintain records on the amount of critical issues reported to the management bodies.
2-17	Collective knowledge of the highest governance body	Annexes. GRI Standards Index	To raise the awareness and competences of the highest management body in matters of sustainable development, the representatives of the board of directors and the governing board are regularly involved in training events with external experts.

2-18	Evaluation of the performance of the highest governance body	Annexes. GRI Standards Index	The annual shareholder meeting makes a regular performance assessment of the board of directors and the governing board. This evaluation forms the basis for restructuring to improve the operational management of the company. Assessment criteria to evaluate the management bodies' activities regarding supervision of the company's impact management on the economy, environment and social sphere were not implemented during the reporting period.
2-19	Remuneration policies	Ethical practices: how weare increasing our management transparency and business resilience. Maintaining corporate management transparency Annexes. GRI Standards Index	At the time of this report, the company's remuneration policy did not specifically consider the effectiveness of management of the company's impact on the economy, social sphere and environment.
2-20	Process to determine remuneration	Annexes. GRI Standards Index	The remuneration procedure for members of the highest management body is developed by the HR department and approved by the general director on the basis of the compensation policies described under Ethical practices: how weare increasing our management transparency and business resilience, sub-clause Maintaining corporate management transparency. The amount and structure of the target incentive for the executive positions are subject to annual revision based on the data provided by an independent consulting company.
2-21	The ratio of the annual total compensation for the organization's highest-paid individual to the median annual total compensation for all employees	Annexes. GRI Standards Index	This information is not disclosed due to the limitations imposed by the company's internal confidentiality policy.
	Strategy, policies and practices		
2-22	Statement on sustainable development strategy	"Increasing resilience against cyberthreats through the creation of Cyber Immunity". A message from Eugene Kaspersky, CEO of Kaspersky Sustainable development. ESG strategy	

2-23	Policy commitments	Sustainable development. ESG strategy Ethical practices: how weare increasing our management transparency and business resilience. Three questions regarding the ethical conduct of our business Ethical practices: how weare increasing our management transparency and business resilience. Complying with anti-corruption policy Team: how we take care of our employees Annexes. GRI Standards Index	The company's policies reflecting its commitments on sustainable development and human rights (Anti-corruption policy, Ethics code* etc.) are stated in the corresponding sections concerning disclosure of information on material topics. In realizing its commitments on sustainable development and human rights observance, the company relies on the principles of the UN Global Compact and the 2015 Resolution of the UN General Assembly on the sustainable development goals, as well as the Paris Agreement of December 12, 2015, the International Bill of Human Rights, including the Universal Declaration of Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms, and the United Nations Guiding Principles on Business and Human Rights. The company strictly observes both the international and local legislations and relies on the Guidance on social responsibility (ISO 26000:2010) and the international AA1000 standard (AccountAbility Principles, Stakeholder Engagement Standard). Kaspersky also adopts the precautionary principle (Principle No. 15) of the 1992 Rio Declaration on Environment and Development. This principle is an integral part of the company's risk management system. The potential environmental impact factors are taken into account in the operation of the company's data centers and the development of its products and services.
2-24	Embedding policy commitments	Sustainable development. ESG strategy Sustainable development. Where we are now: objectives and key results Sustainable development. Managing sustainable development Annexes. GRI Standards Index	The company's sustainability management system has yet to be developed. As of 2023, the management structure is going to include a committee on sustainable development that will integrate the implementation of the relevant practices.

* It is in the process of being finalized.

2-25	Processes to remediate negative impacts	Annexes. GRI Standards Index	Generic procedures within the risk management system apply. In the near future the company intends to establish a sustainable development committee that can elaborate specific procedures and measures with regard to potential negative impacts on society and environment. The company's current procedure to identify negative impacts and address complaints includes interaction with consumers, customers and suppliers through the use of feedback forms on the company's official website: • https://www.kaspersky.ru/about/contact — for Russian-speaking users; • https://www.kaspersky.com/about/contact — for international users. The company also has a procedure in place to analyze complaints and requests from users who contact the technical support desk https://support.kaspersky.com/. As of the publication date of this report, 99% of all incoming requests concern the technical aspects of the products. The anti-corruption hotline number is given under Ethical practices: how weare increasing our management transparency and business resilience, Sub-Clause **Complying with the anti-corruption policy**. To identify further potential impacts as well as to improve procedures for their detection and elimination, the company maintains active interaction with stakeholders and regularly monitors the mass-media.
2-26	Mechanisms for seeking advice and raising concerns	Annexes. GRI Standards Index	Any employee or member of the public can address the company and ask any question at info@kaspersky.com. Incoming messages are handled by the administration division and forwarded to the respective employees in charge of specific matters. The response time is 48 hours. Requests regarding matters of sustainable development and the company's impacts on environment and society can be addressed to the sustainable development division at csr@kaspersky.com. The messages are dealt with in two to three working days.
2-27	Compliance with laws and regulations	Annexes. GRI Standards Index	During the reporting period, no incidents of non-compliance with the legislation or any regulatory requirements were recorded at Kaspersky; no fines or any other liabilities for any law violations were imposed upon the company.
2-28	Membership associations	Annexes. Associations, unions, initiatives	
	Stakeholder engagement		
2-29	Approach to stakeholder engagement	Sustainable development. Stakeholder engagement	
2-30	Collective bargaining agreements	Annexes. GRI Standards Index	Kaspersky has no practice of collective agreements due to a lack of demand therefor from employees.

GRI 3	**Material Topics**		
3-1	Process to determine material topics	Defining the main topics	
3-2	List of material topics	Defining the main topics	3-2-b. This is Kaspersky's first sustainable development report, so the material topics have been defined for the first time.
3-3	Management of material topics	Defining the main topics Annexes. GRI Standards Index	Each disclosure unit in this report begins with the management approach, specifying the goals, objectives and focus in management of each material topic as a brief interview with the respective head of department.
GRI	**Topical disclosures**		
GRI 204	**Procurement Practices**		
204-1	Proportion of spending on local suppliers	Annexes. GRI Standards Index	Due to the specific nature of the company's activities, the proportion of purchases from local suppliers is not a key indicator of sustainable development for Kaspersky, so no separate records with this information are maintained.
GRI 205	**Anti-corruption**		
205-1	Operations assessed for risks related to corruption	Annexes. GRI Standards Index	During the reporting period, no special assessment of corruption-related risks was carried out. Corruption risks are considered within the general process of the company's anti-corruption compliance management.
205-2	Communication and training about anti-corruption policies and procedures	Ethical practices: how weare increasing our management transparency and business resilience. Complying with anti-corruption policy Annexes. GRI Standards Index	100% of employees and partners are aware of the company's anti-corruption policy. Employees are informed about the anti-corruption policy on an annual basis, while partners are informed when concluding contracts.
205-3	Confirmed incidents of corruption and actions taken	Annexes. GRI Standards Index	During the reporting period, no confirmed incidents of corruption or violation of the anti-corruption policy were detected.

GRI 302	Energy		
302-1	Energy consumption within the organization	Ecological footprint: how we are reducing our impact on the environment. Annexes. GRI Standards Index	The report section **Ecological footprint: how we are reducing our impact on the environment** describes in detail the company's approach to reducing power consumption and increasing energy efficiency. The same section also discloses data on the essential impact, which is the consumption of electricity and diesel fuel in the company's data management center (Kaspersky's Moscow office). During the reporting period, no records were maintained of data concerning the consumption of other kinds of energy as well as energy usage in other offices of the company.
302-2	Energy consumption outside of the organization	Annexes. GRI Standards Index	During the reporting period, no data was collected
302-3	Energy intensity	Ecological footprint: how we are reducing our impact on the environment. Reducing our ecological footprint in relation to infrastructure usage Annexes. GRI Standards Index	The methodology for systematization of information and calculation has yet to be developed, see remark in the report.
302-4	Reduction of energy consumption	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	The report section **Ecological footprint: how we are reducing our impact on the environment** describes in detail the company's approach to reducing power consumption and increasing energy efficiency. During the reporting period, no quantitative data was collected, since this is the company's first sustainable development report.
302-5	Reductions in energy requirements of products and services	Ecological footprint: how we are reducing our impact on the environment. Reducing the environmental impact of our operations Annexes. GRI Standards Index	The report section **Ecological footprint: how we are reducing our impact on the environment** describes the company's efforts to reduce the energy demand in products and services. During the reporting period, no quantitative data was collected.
GRI 303	**Water and Effluents**		
303-1	Interactions with water as a shared resource	Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices. Water Annexes. GRI Standards Index	The locations of the company's offices are not qualified as water stress regions. Kaspersky's water consumption is insignificant.
303-2	Management of water discharge-related impacts	Annexes. GRI Standards Index	The company does not discharge water into natural water bodies.

303-3	Water withdrawal	Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices. Water Annexes. GRI Standards Index	The company does not withdraw water directly from natural sources or open water bodies. 100% of water withdrawal comes from public sources.
303-4	Water discharge	Annexes. GRI Standards Index	The company does not discharge water into natural water bodies.
303-5	Water consumption	Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices. Water Annexes. GRI Standards Index	Disclosure limits cover the Moscow office of AO Kaspersky Lab, also including the company's data center (being the company's main water consumer). During the reporting period. no data concerning other offices was collected.
GRI 304	**Biodiversity**		
304-1	Operational sites owned, leased, managed in, or adjacent to, protected areas and areas of high biodiversity value outside protected areas	Annexes. GRI Standards Index	Kaspersky does not operate in protected natural areas or areas of high biodiversity value.
304-2	Significant impacts of activities, products, and services on biodiversity	Annexes. GRI Standards Index	The company's activity as a whole and its products and services have no significant impact on biodiversity.
GRI 305	**Emissions**		
305-1	Direct (Scope 1) GHG emissions	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	The report section **Ecological footprint: how we are reducing our impact on the environment** describes in detail how the company's carbon footprint is generated and what approach to reducing it the company takes. We have presented quantitative data on the data center's power consumption and the greenhouse gas emissions from air travel. The methodology of data collection and calculation of the total amount of direct greenhouse gas emissions across all of the company's objects (Scope 1), as well as indirect emissions from energy consumption (Scope 2) has yet to be developed, the data will be presented in the subsequent reports.
305-2	Energy indirect (Scope 2) GHG emissions	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	

305-3	Other indirect (Scope 3) GHG emissions	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	As yet, no data on greenhouse gas emissions across the company's supply chain is being collected.
305-4	GHG emissions intensity	Annexes. GRI Standards Index	Data is not yet being collected.
305-5	Reduction of GHG emissions	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	The report section **Ecological footprint: how we are reducing our impact on the environment** describes in detail the company's approach to reducing its carbon footprint. Quantitative data will be presented in the subsequent reports, after the data collection to Scope 1 and 2 has been systematized.
305-6	Emissions of ozone-depleting substances (ODS)	Annexes. GRI Standards Index	Not applicable. The company produces no ODS emissions.
305-7	Nitrogen oxides (NOx), sulfur oxides (SOx), and other significant air emissions	Annexes. GRI Standards Index	Not applicable. The company produces no emissions of specified pollutants into the atmosphere.
GRI 306	**Waste**		
306-1	Waste generation and significant waste-related impacts	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	Information on waste generation is given with regard to essential impacts: waste generated by the Moscow office (headquarters), including the data center, and waste generated as a result of the business activities.
306-2	Management of significant waste-related impacts	Ecological footprint: how we are reducing our impact on the environment Annexes. GRI Standards Index	Kaspersky vets all contractors to check that they comply with the legal requirements, this procedure also applies to operators in charge of waste management.
306-3	Waste generated	Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices Annexes. GRI Standards Index	

306-4	Waste diverted from disposal	Ecological footprint: how we are reducing our impact on the environment. Reducing the environmental impact of our operations Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices	The report section **Ecological footprint: how we are reducing our impact on the environment** describes in detail the company's approach to the transition towards environmentally-friendly materials and increasing the share of recycled waste. During the reporting period, no quantitative data on material recycling was collected.
306-5	Waste directed to disposal	Ecological footprint: how we are reducing our impact on the environment. Using environmentally-friendly materials and energy-efficient solutions in our offices	
GRI 307	**Environmental Compliance**		
307-1	Non-compliance with environmental laws and regulations	Annexes. GRI Standards Index	Kaspersky operates in strict observance of all applicable laws governing the negative environmental impact. During the reporting period, there were no fines, non-financial sanctions or complaints against the company in connection with any violation of or failure to comply with the requirements of the environmental legislation.
GRI 401	**Employment**		
401-1	New employee hires and employee turnover	Team: how we take care of our employees	
401-2	Benefits provided to full-time employees that are not provided to temporary or part-time employees	Team: how we take care of our employees. Non-financial incentives Annexes. GRI Standards Index	
401-3	Parental leave	Women in STEM: how we attract them to IT and thereby attempt to reduce the gender gap. Providing support to women and parents Annexes. GRI Standards Index	All the required information is disclosed, except return to work rate and retention rate, during the reporting period, no data was collected in this regard.

GRI 403	Occupational Health and Safety		
403-1	Occupational health and safety management system	Team: how we take care of our employees. Ensuring health and safety in the workplace Annexes. GRI Standards Index	The occupational health and safety management system in all of Kaspersky's offices within the scope of disclosure in this report complies with the requirements of applicable employment legislations in the company's territories of presence. The system includes regular employee training and regular special workplace assessment in all divisions, as well as the risk management and accident investigation system and measures to improve working conditions. The main criterion for the system's effectiveness is zero on-the-job injuries.
403-2	Hazard identification, risk assessment, and incident investigation.	Annexes. GRI Standards Index	During the reporting period, no accidents related to occupational risks were recorded in the company.
403-3	Occupational health services	Team: how we take care of our employees. Ensuring health and safety in the workplace Annexes. GRI Standards Index	All employees are offered an opportunity to be vaccinated against seasonal diseases. The employees in the headquarters (the most numerous group of workers) have access to a general practitioner, a massage therapist, and an in-house psychologist right at the office. The corporate medical insurance in Russia also includes accident insurance. The system's effectiveness is measured by a regular employee satisfaction survey.
403-4	Worker participation, consultation, and communication on occupational health and safety	Annexes. GRI Standards Index	The company has a health and safety commission in place, comprising representatives of various departments.
403-5	Worker training on occupational health and safety	Team: how we take care of our employees. Ensuring health and safety in the workplace	Training effectiveness is evaluated by a special commission in charge of health and safety knowledge assessment.
403-6	Promotion of worker health	Team: how we take care of our employees. Ensuring health and safety in the workplace	
403-7	Prevention and mitigation of occupational health and safety impacts directly linked by business relationships	Annexes. GRI Standards Index	Not applicable.
403-8	Workers covered by an occupational health and safety management system	Annexes. GRI Standards Index	The occupational health and safety management system covers 100% of the company's employees, regardless of form of employment and type of contract.

403-9	Work-related injuries	Annexes. GRI Standards Index	Most of Kaspersky's employees are involved in office work. Prevention of injuries in the workplace or during job performance is the company's key performance indicator for the occupational health and safety management system. During the reporting period, no such injuries and accidents were recorded.
403-10	Work-related ill health	Annexes. GRI Standards Index	During the recording period, no incidents of work-related ill health were recorded at AO Kaspersky Lab. The measures for promotion of employees' physical and mental health, as described in the report section **Our team: how we take care of our employees**, Sub-Clause **Ensuring health and safety in the workplace**, as well as in the comments to Disclosure GRI 403-3, are designed with typical work-related conditions in IT specialists and other office workers in mind (such as visual impairment, hypodynamia, carpal tunnel syndrome, diseases of the musculoskeletal system, etc.). The company makes regular special assessments of working conditions in all departments, the employees also can have a medical examination as part of the private medical insurance or corresponding programs in their country.
GRI 404	**Training and Education**		
404-1	Average hours of training per year per employee	Team: how we take care of our employees. Investing in education and development	
404-2	Programs for upgrading employee skills and transition assistance programs	Team: how we take care of our employees. Investing in education and development Annexes. GRI Standards Index	404-2-b. The company does not have special transition assistance programs (changing to another company, retirement), since there has been no need for such programs yet. Kaspersky does have an internal program to transition to available open vacancies. The company also provides the funds for additional one-off payments to employees who have reached the age of 50, 60 and 70 years. The corresponding report section gives detailed information about the company's employee development programs and opportunities for advanced training and retraining.
404-3	Percentage of employees receiving regular performance and career development reviews	Team: how we take care of our employees. Investing in education and development	100%, on an annual or quarterly basis. Based on assessment results, the company may make a decision regarding bonus payments, raises or promotion.
GRI 405	**Diversity and Equal Opportunity**		
405-1	Diversity of governance bodies and employees	Team: how we take care of our employees. Equal opportunities (405-1-a) Team: how we take care of our employees. How many of us are there? (405-1-b)	
405-2	Ratio of basic salary and remuneration of women to men	Women in STEM: how we attract them to IT and thereby attempt to reduce the gender gap	

GRI 406	**Non-discrimination**		
406-1	Incidents of discrimination and corrective actions taken	Annexes. GRI Standards Index	During the reporting period, no incidents of discrimination were detected. Any discrimination is unacceptable. This position is enshrined in the company's main principles and will be reflected in the Ethics Code (currently under review). The principles of unacceptability of any discrimination draw on the United Nations Guiding Principles on Business and Human Rights.
GRI 418	**Customer Privacy**		
418-1	Substantiated complaints concerning breaches of customer privacy and losses of customer data	How we protect personal data and ensure privacy. Ensuring personal data protection for our users worldwide	

SASB Content Index

This section contains a SASB Software and IT-services reporting compliance guide (as of October 2018), as well as additional information according to the requirements of this SASB version, not reflected in the main report (see Remarks).

SASB Standards

Compliance of reporting elements with the industry guide SASB Software and IT-services, version of 2018-10 (TC-SI)

Disclosure	Description	Section of the report	Remarks
	Environmental Footprint of Hardware Infrastructure		
TC-SI-130-a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Ecological footprint: how we are reducing our impact on the environment. Reducing our ecological footprint in relation to infrastructure usage Annexes. SASB Standards	This information is disclosed in the limits of the Moscow office of AO Kaspersky Lab (headquarters), including the data management enter. This is the most significant part of the organization's entire power consumption.
TC-SI-130-a.2	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Ecological footprint: how we are reducing our impact on the environment. Reducing our ecological footprint in relation to infrastructure usage Annexes. SASB Standards	See also the Index GRI Standards 303-1 and 303-3: Remarks.
TC-SI-130-a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	Ecological footprint: how we are reducing our impact on the environment. Reducing our ecological footprint in relation to infrastructure usage	
	Data Privacy & Freedom of Expression		
TC-SI-220-a.1	Description of policies and practices relating to behavioral advertising and user privacy	How we protect personal data and ensure privacy	

TC-SI-220-a.2	Number of users whose information is used for secondary purposes	How we protect personal data and ensure privacy	0 (zero).
TC-SI-220-a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	How we protect personal data and ensure privacy Annexes. SASB Standards	No such incidents during the reporting period; the amount of monetary losses is 0 (zero).
TC-SI-220-a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Global Transparency Initiative: how and why we revealed our code and processes. Greater openness regarding internal processes through six key areas of the GTI Annexes. SASB Standards	(1) The policy is described in the corresponding section of the report. The number of requests from government authorities can be found in Kaspersky's regular Law Enforcement & Government Requests Report. The most recent report covers the second half of 2021. (2) The company does not keep track of this statistic; we only take into account the number of requests to provide user data and non-personal technical information. (3) 0% — Kaspersky has not yet disclosed such data to government authorities.
TC-SI-220-a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Annexes. SASB Standards	No such countries.
	Data Security		
TC-SI-230-a.1	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	How we protect personal data and ensure privacy	
TC-SI-230-a.2	Description of approach to identifying and addressing data security risks	How we protect personal data and ensure privacy Critical infrastructure: how we protect it in a changing world Critical infrastructure: how we protect it in a changing world	

	Recruiting & Managing a Global, Diverse & Skilled Workforce		
TC-SI-330-a.1	Percentage of employees that are (1) foreign nationals, and (2) located offshore	Annexes. SASB Standards	(1) As of June 2022, AO Kaspersky Lab had 40 foreign citizens employed, <1% of the total headcount. No information concerning other regional offices was collected during the reporting period. (2) Not applicable to AO Kaspersky Lab, since Russian labor legislation does not imply working outside of the Russian Federation. No information concerning offices outside of Russia was collected during the reporting period.
TC-SI-330-a.2	Employee engagement as a percentage	Team: how we take care of our employees. Engagement assessment	
TC-SI-330-a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	Team: how we take care of our employees. How many of us are there? Annexes. SASB Standards	The breakdown by gender and categories of employees is presented in the corresponding section of the report. The company does not keep track of employee statistics by ethnic groups.
	Intellectual Property Protection & Competitive Behavior		
TC-SI-520-a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Ethical practices: how weare increasing our management transparency and business resilience Ethical practices: how weare increasing our management transparency and business resilience. Sustainable development in action. How we defeated a patent troll	
	Managing Systemic Risks from Technology Disruptions		
TC-SI-550-a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Annexes. SASB Standards	This information is not disclosed due to the limitations imposed by the company's internal confidentiality policy.

TC-SI-550-a.2	Description of business continuity risks related to disruptions of operations	Critical infrastructure: how we protect it in a changing world. Reducing systemic technological failure risks	
	Activity Metrics		
TC-SI-000.A	(1) Number of licenses or subscriptions, (2) percentage cloud-based	Annexes. SASB Standards	(1) 714 (2) 35% cloud-based
TC-SI-000.B	(1) Data processing capacity, (2) percentage outsourced	Annexes. SASB Standards	(1) 266 units in the local network and 6 921 outsourced (2) 96% outsourced (collocation)
TC-SI-000.C	(1) Amount of data storage, (2) percentage outsourced	Annexes. SASB Standards	(1) Upwards of 100 petabytes (2) More than 90% outsourced (collocation)

We would like to thank the following Kaspersky employees for their help in preparing this report:

A message from Eugene Kaspersky, CEO of Kaspersky About the company Ethical practices: how weare increasing our management transparency and business resilience	Oxana Sotnikova	Senior Corporate Communications Manager
	Marina Tyupkina	Head of Internal Communications & Corporate Events
	Ekaterina Burdova	Head of Corporate PR and Strategic Projects
	Nikita Krapukhin	Deputy Chief Legal Officer, Head of Corporate Law
	Anastasiya Vizerskaya	Senior Legal Counsel
Users: how we protect personal data and ensure privacy	Alexey Vovk	Head of Information Security
	Yury Shelikhov	Head of Cybersecurity and Data Protection
	Anastasia Kazakova	Senior Public Affairs Manager*
Critical infrastructure: how we protect it in a changing world	Natalya Axelbant	Senior Marketing Communications Manager
	Ekaterina Ulyashova	Product Marketing Manager
	Kirill Naboyshchikov	Senior Product Marketing Manager
	Mikhail Chekalin	Business Development Manager, Industrial CyberSecurity
Fighting cybercrime: how we work together with law enforcement	Anastasia Kazakova	Senior Public Affairs Manager*
	Igor Kumagin	Senior Project Manager
	Elizaveta Shulyndina	Head of Threat Research and Security Intelligence PR
	Victoria Ilina	Corporate Communications Manager

* The position is specified for the period from 2021 to 2022.

Security in cyberspace: how we protect our users against the cyberworld threats	Ivan Shadrin	Deputy Head of PR
	Elizaveta Shulyndina	Head of Threat Research and Security Intelligence PR
	Elena Molchanova	Head of Security Awareness Marketing*
	Tatyana Shumaylova	Senior Product Marketing Manager
	Svetlana A. Kalashnikova	Product Manager
	Oleg M. Ignatov	Senior Product Manager
	Victor Chebyshev	Lead Security Researcher*
	Andrey Sidenko	Head of Child Safety at Kaspersky Network
	Elena Chekhievskaya	Marketing Lead
	Ekaterina Chingaeva	Senior Corporate Communications Manager
Security in cyberspace: how we protect our users against the cyberworld threats	Sergey Pakhomov	Property Manager
	Mikhail Kuznetsov	Head of Office Administration
	Denis Kuznetsov	Telecom Group Manager
	Denis Yablonsky	Power Engineer
	Sergey Lapshin	Head of Business Travel
	Margarita Khrapova	Head of Internal Communications
	Tatyana Agapova	Marketing Production Group Manager
	Ivan Imhoff	VP, Digital Business*
	Irina M. Smirnova	Head of Finance Shared Service Center
	Anastasia Pereprosova	Business Process Manager
How we take care of our employees	Ellina Kozlovskaya	Head of Employer Branding
	Kristina Bratanova	Employer Branding Manager
	Darya Shchekochikhina	Employer Branding Manager
	Petr Pokrovsky	Employer Branding Manager
	Elizaveta Kozlova	Training & Development Manager
	Elizaveta Myltseva	Sustainability Manager

* The position is specified for the period from 2021 to 2022.

Women in STEM: how we attract women to IT and thereby attempt to reduce the gender gap	Ekaterina Burdova	Head of Corporate PR and Strategic Projects
	Ellina Kozlovskaya	Head of Employer Branding
	Evgeniya Russkikh	Head of Academic Affairs
	Genie Gan	Head of Public Affairs, APAC & META
	Anastasia Shamgunova	HR Director, Eastern
	Dana Serova	Corporate Communications Specialist*
GRI & SASB Standards Compliance Guides	Nikita Krapukhin	Deputy Chief Legal Officer, Head of Corporate Law
	Anastasiya Vizerskaya	Senior Legal Counsel
	Sergey Tridnevko	Head of Economic Security & Compliance
	Sergey Vasilyev	Head of IP Research & Analysis
	Ellina Kozlovskaya	Head of Employer Branding
	Sergey Pakhomov	Property manager
	Elena Volodenkova	Head of Procurement
	Alexey Testsov	Head of Data Protection and Privacy, Data Protection Officer
	Sergey Klochkov	Director IT Infrastructure
	Sergey Verkhovykh	IT Service Manager
Photography	Darya Khilobok	Community Specialist
	Vasily Kamaldinov	Head of Corporate Social Media
Editing and proof-reading	Nicholas Hodgkins	Senior Editor-Writer

* The position is specified for the period from 2021 to 2022.

Contacts and Feedback

GRI 2-3

For all questions related to this Sustainable Development Report, please contact Maria Losyukova, Head of Sustainability:

Maria.Losyukova@kaspersky.com

Company website:
www.kaspersky.com

For general enquiries:
info@kaspersky.com

Contact information:
https://www.kaspersky.com/about/contact

Press contacts:
prhq@kaspersky.com

Headquarters mail address:
39A/2 Leningradskoe Shosse, Moscow, 125212, Russian Federation, Olympia Park Business Center
+7 495 797-87-00, +7 495 737-34-12