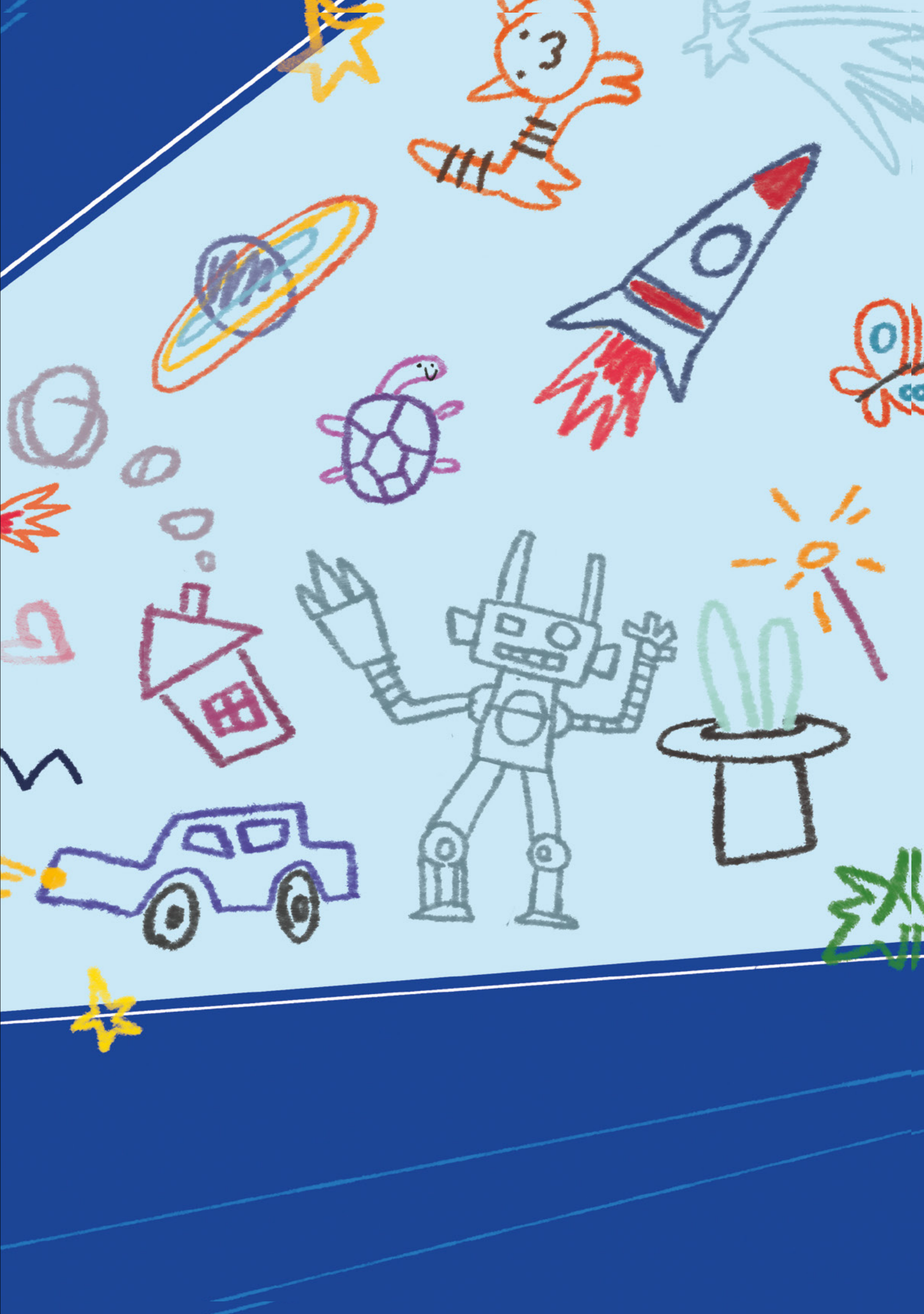
ALLIANCE
FOR THE PROTECTION OF
CHILDREN IN THE DIGITAL
ENVIRONMENT

Technologies for protecting children on the Internet

Rostelecom

MINDSMITH

TEQVISER



In addition to the obvious advantages, the new digital world is fraught with many dangers, especially for children and adolescents.

Studying the risks that minors face online, as well as technologies for their protection, is more relevant than ever now since the whole world has moved online. Due to their age and lack of experience, children are particularly vulnerable to various kinds of cybercriminals, so we must pay increased attention to their safety on the Internet.

It seems that the issue of children's safety on the Internet will never be fully studied, because every year and even every month we see new threats emerge. Today's risks are transformed, revealed and amplified under the influence of technological trends and global changes in society. How can we ensure the safety of children on the Internet and protect them from the risks that will come tomorrow?

This issue should be discussed at all levels ranging from each family to the entire state, along with the development of a space for joint responsibility for the safety of children. For example, IT developers need to focus on risks that cannot be countered efficiently. At the same time, businesses should make the safety of children a priority, taking it into account at the stage of product development. The role of educational institutions deserves a special mention. In my opinion, they should become the centers of expertise on this topic.

It is especially important to develop children's skills in digital hygiene and safe use of the Internet. However, a truly efficient protection of children from cyber risks and even prevention of these risks is only possible by combining the efforts of all stakeholders. Such work is already being carried out by the Alliance for the Protection of Children in the Digital Environment, founded by Rostelecom among others. The founding companies of the Alliance make every effort to create a safe and favorable digital environment, share best practices and the latest developments for the benefit of the youngest members of Russian society. I am convinced that together Russia's largest companies will be able to create a truly favorable environment for the development, education and safe communication of children in the virtual space.

Mikhail Oseevsky,
CEO of Rostelecom PJSC

Table of contents

Introduction

The Internet is becoming an integral part of our lives. The Internet penetration rate in Russia is 89%, which is 129.8 out of 145.9 million people, and children and minors make up 21.8% of the country's population. In 2021, the number of Internet users increased by 4.7%[1]. Children are literally "born with a smartphone in their hand" and actively use the Internet, while at the same time being the most vulnerable category of users. Their cognitive abilities, worldview and critical thinking skills are in the process of formation.

The number of crimes in cyberspace is growing. Every day there are new mechanics that pose a threat to children and teenagers on the Internet, and the old methods of protection stop working. In addition to the family, schools and law enforcement agencies, IT solutions embedded in the familiar digital environment, such as search engines, social networks, communication services, and games, are becoming important elements of child protection.

The development of technological methods of child protection aimed at ensuring their safety in the online environment is inextricably linked with the study of cyber risks facing minors.

The study "Child Protection Technologies on the Internet" was conducted from October 2021 to April 2022. As part of the study, an analysis of cyber risks for children and adolescents was carried out, technological measures to counteract cyber risks were studied, risks that minors may face in the future were identified, and recommendations for stakeholders were proposed.

23 risks

8 clusters

10 future risks

1 Digital 2022 Global Overview Report», We Are Social, Hootsuite, 2022

>> The research was based on artificial intelligence (machine learning). The presented information and conclusions were obtained using an intelligent analytical system for identifying new markets, promising technologies and methods of their use by TeqViser. The cluster analysis was carried out on the basis of a sample of more than 21 thousand scientific papers.

>> Based on the analysis of more than 500 literature sources, 23 risks threatening the safety of children and adolescents on the Internet were identified. In order to determine the degree of danger of risks and the effectiveness of technological solutions to counteract them, an expert assessment was given from experts invited to the study in the field of cybersecurity, child psychology and sociology.

>> As part of the study of technological measures to counter cyber risks for children and adolescents, more than 300 patents, companies and IT solutions in the field of cybersecurity of children and adolescents were analyzed. According to the results of the analysis, 8 clusters of technological solutions were formed.

>> Based on the existing risks and a number of trends dictated by technological, social and geopolitical changes, 10 areas were identified in which risks for minors will be formed in the near future.

>> Based on the results of the study, recommendations were proposed for stakeholders aimed at strengthening the safety of children and adolescents on the Internet.

Key findings

1

The most dangerous risks are associated with psychological abuse of a child

Risks that are the result of an aggressive collision between people have a high degree of danger. At the same time, technological solutions are sufficiently developed to resist primitive personal attacks and reduce their volume, but they are not able to prevent attacks from a large number of attackers or those who are well aware of the principles of the technology.

2

Solutions related to content filtering and protecting children from online fraud are better developed than others

The most effective methods of protection against risks are associated with filtering and blocking pornographic and violent content, as well as preventing cases of online fraud and the distribution of dangerous goods. Technological solutions aimed at countering these risks are embedded in the functionality of several clusters of technological control measures at once (parental control systems, Internet filters), and are also present directly on platforms providing digital content.

3 The risks associated with information and marketing pressure are underestimated

The risks associated with information and marketing pressure, the involvement of children in risky monetary relationships, as well as the spread of misinformation and content not intended for children and adolescents are largely underestimated. Although stakeholders are informed about their presence, it is necessary to increase digital literacy in the field of their prevention, as well as the consolidation of efforts on the part of all parties involved.

4 The future risks require special attention

In the medium term, the risks associated with the development of virtual reality and metaverses (the growing influence of digital influencers, new opportunities for interaction between adults and children), artificial intelligence as a tool of criminal activity and parenting technology, the growth of the digital divide, information wars and digital isolation, as well as new threats to privacy and personal data (digital footprint, biometrics) are expected to increase.

5 The fight against cyber threats requires the interaction of many stakeholders

The development of technologies both generating cyber risks and aimed at combating them is extremely dynamic. Many actors should be involved in the process of finding solutions in this area. At the same time, stakeholders should be free to take initiative and experiment. The process will be truly effective if a space of joint responsibility for the result is formed.

Cyber risks for children and teenagers

1

>>

In order to determine what risks children and adolescents may face on the Internet, a cluster analysis was used based on a sample of more than 21 thousand scientific papers.

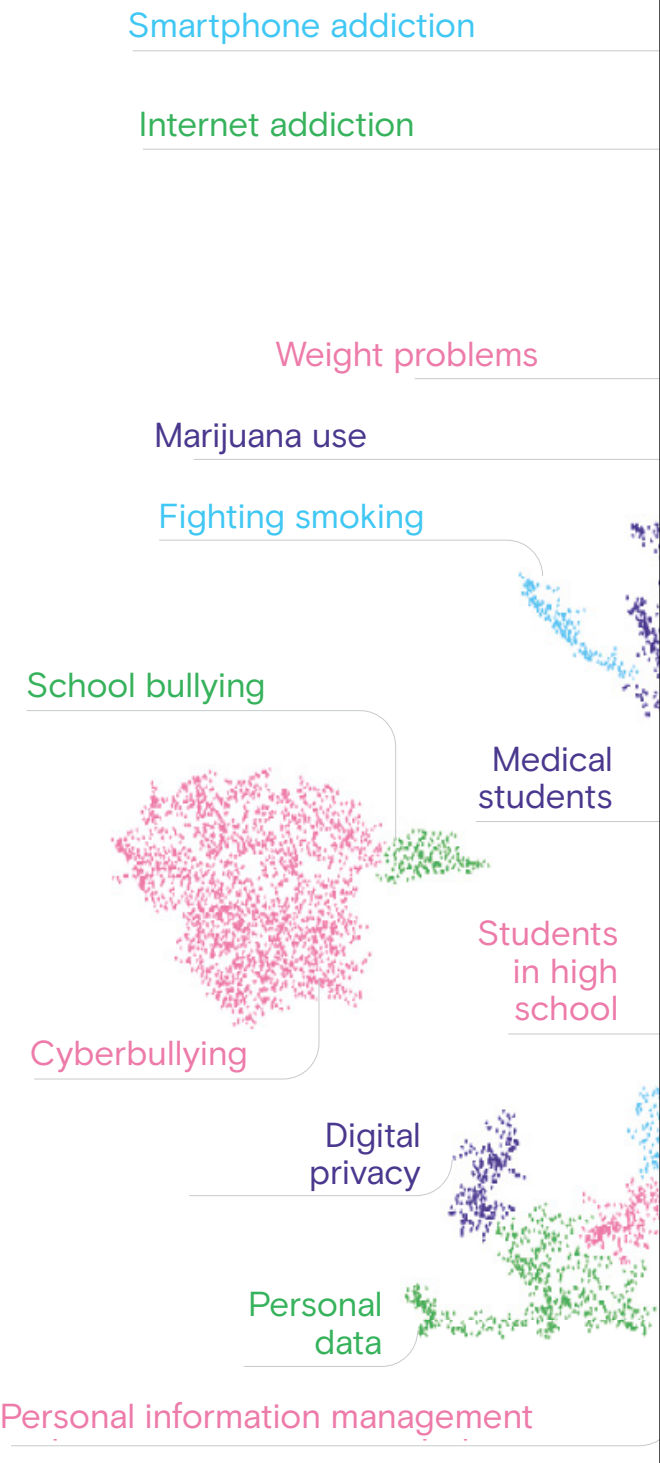
>> CLUSTERS OF RELEVANT SCIENTIFIC PAPERS

Clustering is the splitting of a sample of objects into subsets called clusters, so that each cluster consists of similar objects. Each point on the map represents one of the scientific articles that are grouped into clusters by belonging to a specific topic.

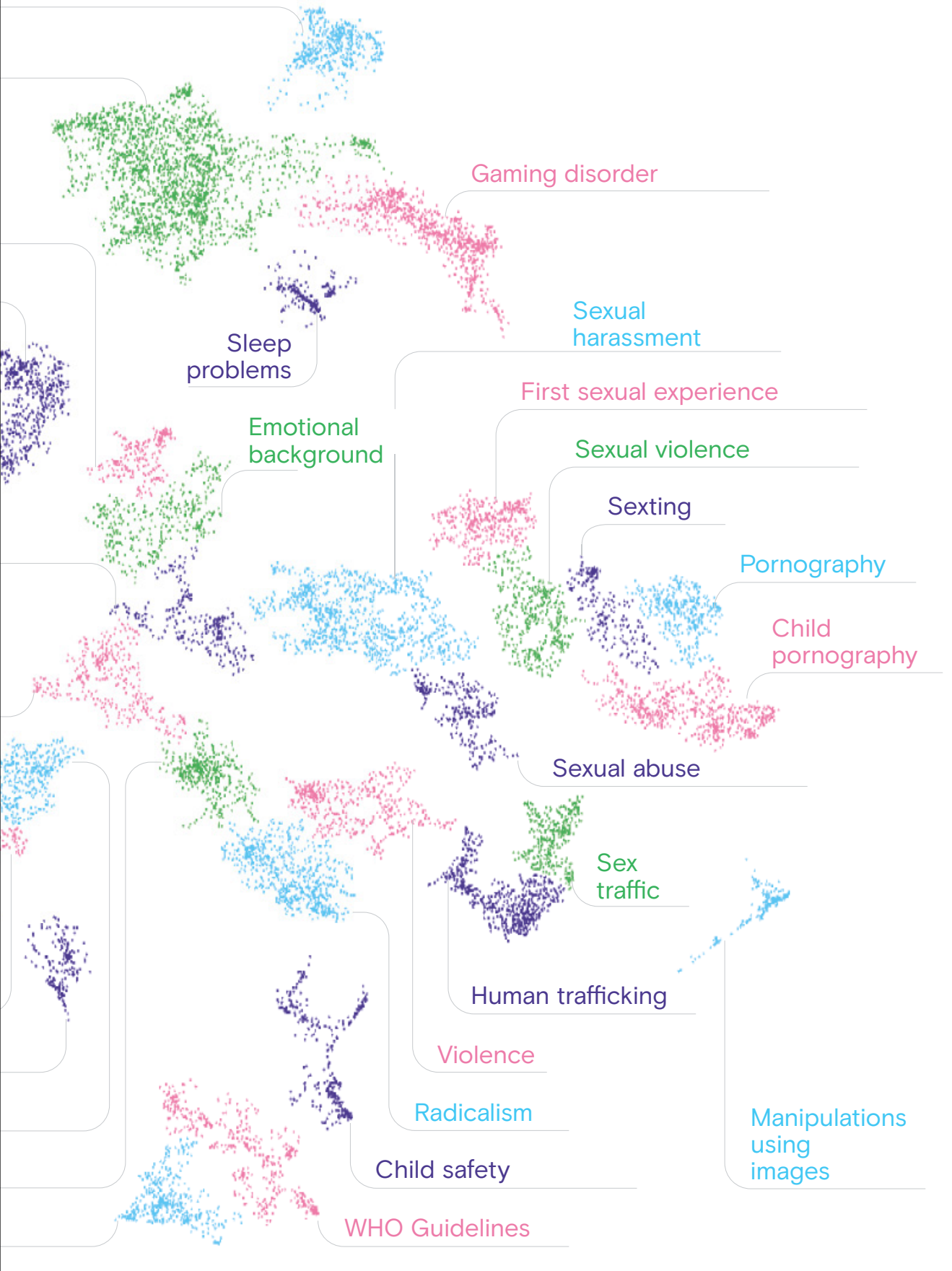
In total, 33 clusters of relevant scientific papers were identified. The largest clusters that attract the attention of researchers include cyberbullying, Internet addiction and risks of a sexual nature (harassment, pornographic content), trafficking, as well as risks related to the security of children's personal data.

33

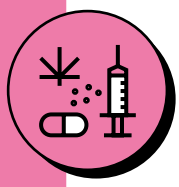
clusters of relevant scientific papers



Then we analyzed more than 500 domestic and foreign literature sources, as a result of which we identified 23 key cyber risks for minors and grouped them into 6 blocks.

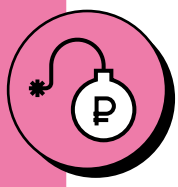

Gaming disorder
Sleep problems
Sexual harassment
First sexual experience
Emotional background
Sexual violence
Sexting
Pornography
Child pornography
Sexual abuse
Sex traffic
Human trafficking
Violence
Radicalism
Manipulations using images
Child safety
WHO Guidelines

>> CYBER RISKS FOR CHILDREN AND TEENAGERS



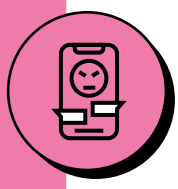
Criminalization, involvement in criminal practices

1. Involvement of children in criminal communities
2. Sale of prohibited goods and services
3. Radicalization and extremism
4. Trafficking



Marketing pressure, risky monetary relationships

5. Internet as a sales channel for goods dangerous to the life and health of children
6. Advanced marketing techniques
7. Dark patterns
8. Online fraud



Personal attack, psychological violence

9. Cyberbullying
10. Stalking
11. Grooming
12. Sexual harassment

Digital exploitation, using a child to create digital content

13 Doxing

14 Creation and distribution of child pornography materials

15 Theft, collection and exploitation of personal data

16 Sharenting

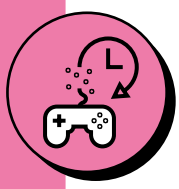
Information pressure, information not intended for children and adolescents

17 Content containing violent scenes

18 Pornographic content

19 Disinformation

20 Dangerous trends and challenges



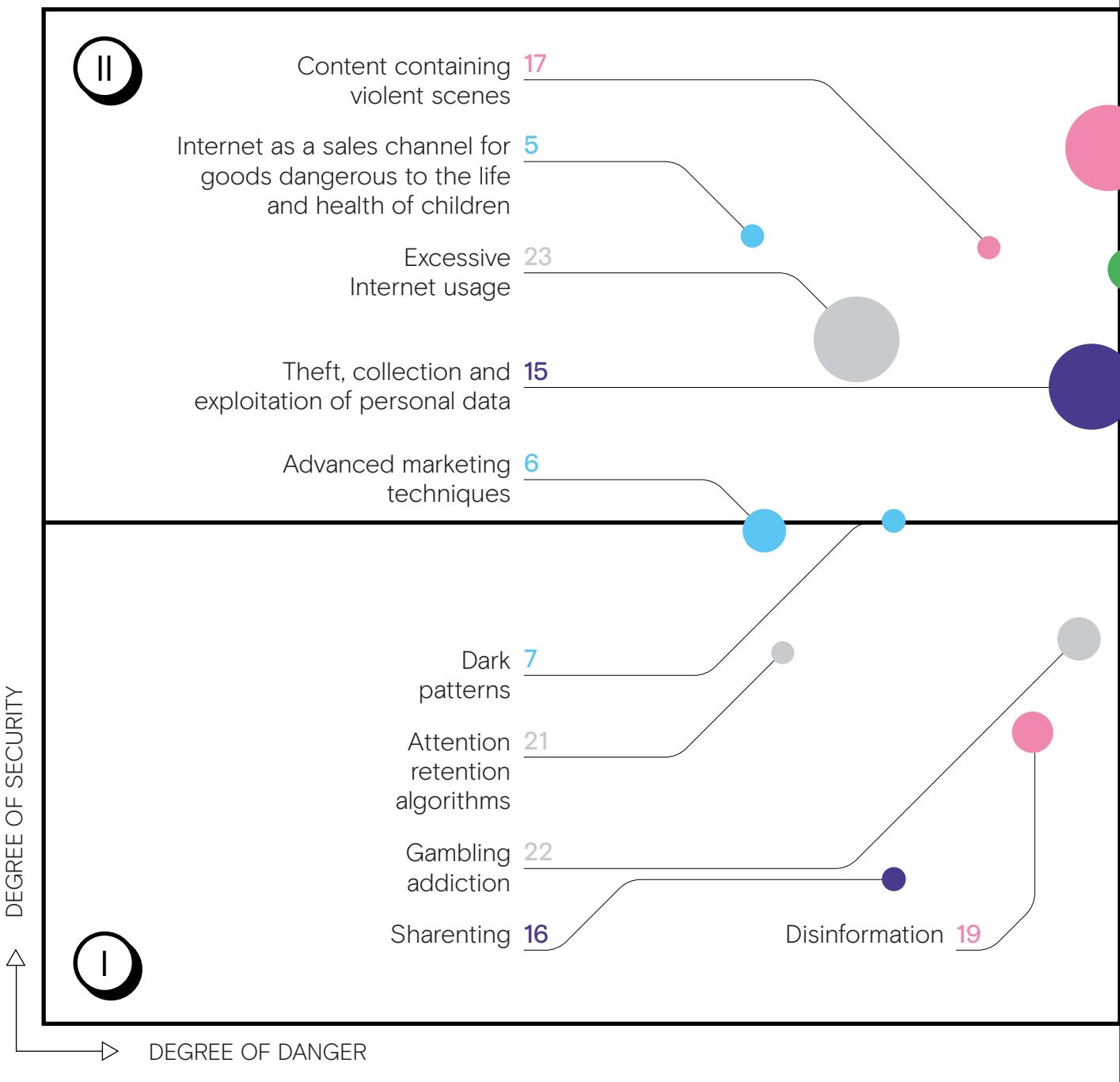
Addiction, formation of dependence on the Internet environment

21 Attention retention algorithms

22 Gambling addiction

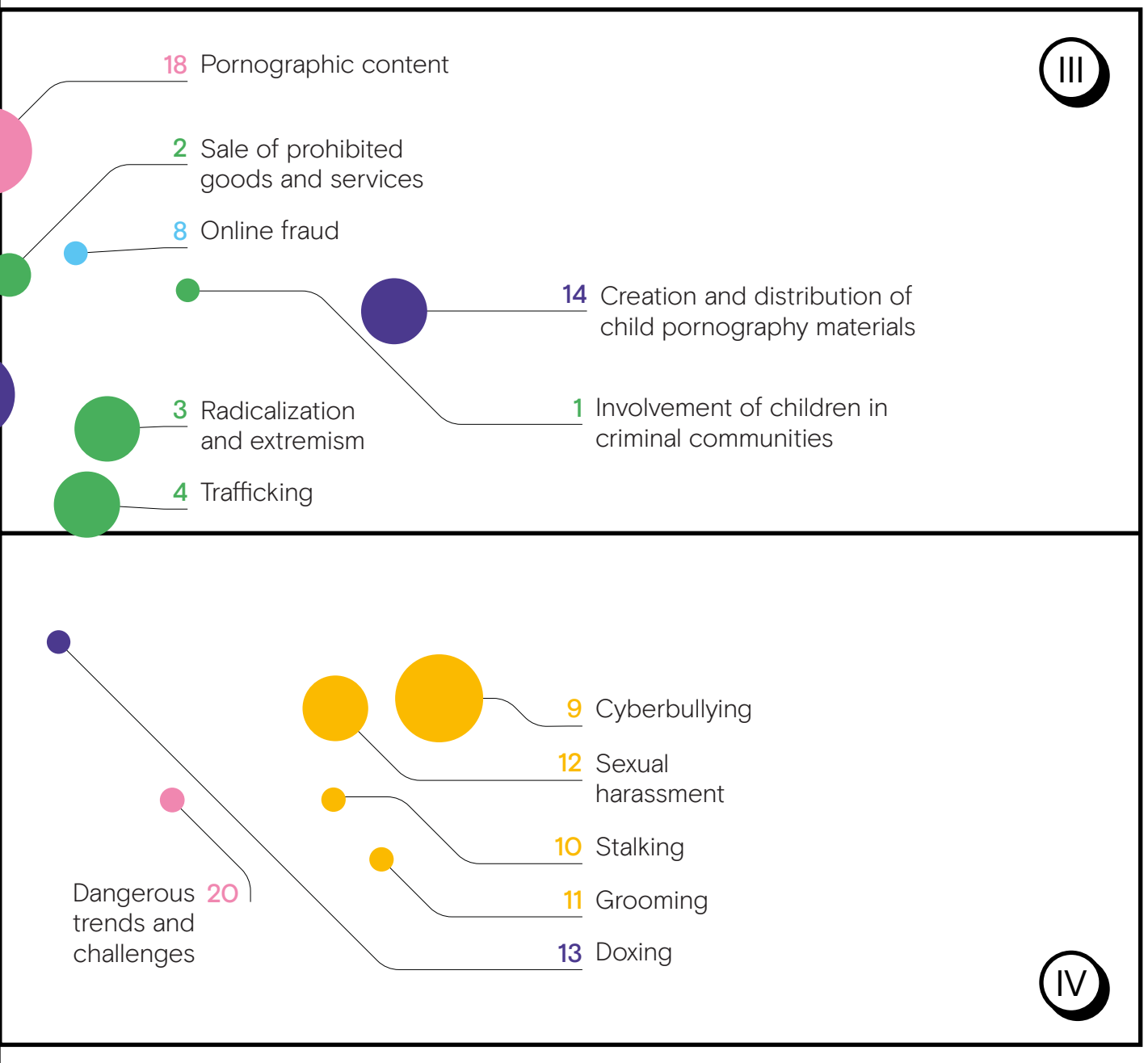
23 Excessive Internet usage

>> RISK MAP



- Criminalization, involvement in criminal practices
- Marketing pressure, risky monetary relationships
- Personal attack, psychological violence
- Digital exploitation, using a child to create digital content
- Information pressure, information not intended for children and adolescents
- Addiction, formation of dependence on the Internet environment

Number of mentions of a specific risk for children and adolescents in news and scientific papers (determined using TeqViser).



As part of the study, an expert survey was conducted, during which experts assessed the degree of danger and the degree of effectiveness of technological protection measures (the degree of protection) of each risk.
According to the survey results, we have placed all cyber risks on two axes, i.e. “degree of danger” (X axis) and “degree of security” (Y axis).

Thus, we have identified 4 risk groups:

I **UNDERESTIMATED** — risks with low degrees of danger and security

II **CONTROLLED** — risks with low risk and high security

III **CURRENT** — risks with high degrees of danger and security

IV **REQUIRING ATTENTION** — risks with high danger and low security

Criminalization, involvement in criminal practices

This group includes risks with the involvement of children in criminal practices prohibited by law, for example, the involvement of children in criminal communities, the sale of prohibited goods and services, radicalization and extremism, as well as trafficking.[2]

The consequences of such risks can have an extremely negative impact on the psycho-emotional and physical condition of the child, as well as pose a danger to society as a whole.

2 Trafficking – human trafficking

1 >> INVOLVEMENT OF CHILDREN IN CRIMINAL COMMUNITIES

Immoral values and attitudes are actively imposed on children who belong to groups and communities that promote destructive actions, for example, the devaluation of human life, or the manifestation of aggression and cruelty.

At the same time, such communities involve minors in drug addiction, topics of sociopathy, mass and ritual murders, Satanism, anarchy, Nazism, and extremism.

There are not isolated cases of recruitment of people to terrorist organizations via the Internet, which leads to the spread of terrorist ideology in the territories of individual countries, and also threatens the security and vital activity of society as a whole.

2 >> SALE OF PROHIBITED GOODS AND SERVICES

The Internet makes it possible to purchase goods and services, the free sale of which is prohibited or restricted by law. The most popular prohibited product that minors buy through the Internet is drugs.

In addition, teenagers can purchase illegal weapons on the Internet, order services for hacking computers, phones, accounts in social networks and applications. Usually, a darknet[3] ensuring the anonymity of the buyer and seller is used for this.

It is more difficult for children and adolescents than for adults to adhere to the rules of behavior and moral values on the Internet. They may purchase prohibited goods and services out of curiosity or for the sake of a sense of belonging to a certain group of people.

3 >> RADICALIZATION AND EXTREMISM

Teenagers aged 14 to 17 are most susceptible to radical nationalist, xenophobic and extremist ideas. Extremist and radical organizations are often recruited through social networks.

In addition, the algorithms of recommendation services are configured to display information depending on the user's interests. If a child is interested in radicalization of a certain form, the probability that algorithms will recommend counterarguments that can convince them is extremely small. The system can direct the user to radical communities, propaganda channels and materials that will only deepen their inclinations and strengthen extremist views.

3 Darknet (DarkNet) is a segment of the Internet that is hidden from public access

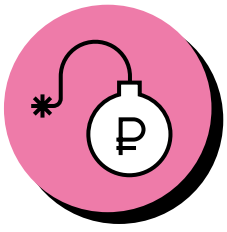
4 >> TRAFFICKING

Victims of trafficking or human trafficking, most of whom are women and teenagers, are forced into prostitution, forced to work, killed to sell organs for transplantation, and illegally adopted.

In addition, the Internet has opened up new forms of work and commercialization. For example, real-time video broadcasts in which a criminal receives money for inhumane actions towards a child.

Criminals can find potential victims in online chats, for this they are engaged in community development, victim profiling, and even use advertising. The Internet also makes it possible to find buyers, for example, advertise victims of trafficking, or attract customers and accomplices. At the same time, the real data of criminals and the history of their atrocities are hidden behind the barriers of closed communities and in the darknet.

Marketing pressure, risky monetary relationships



This group includes risks based on marketing tools, patterns of behavior and subtle psychological tricks created to manipulate children, for example, the sale of goods dangerous to the life and health of children, advanced marketing techniques, dark patterns, and online fraud.

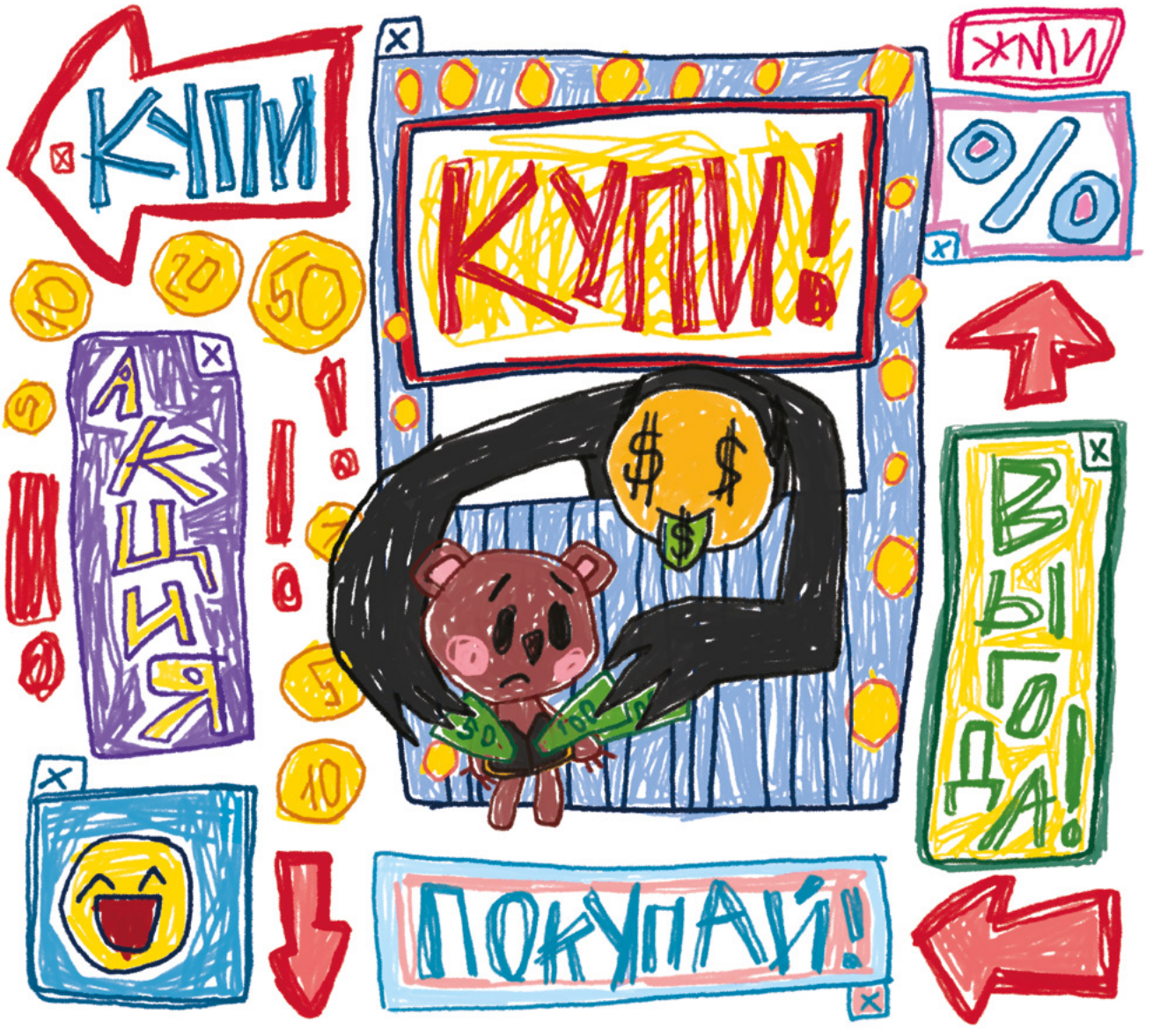
Marketing, psychological and design tools used both legally and illegally are most often aimed at extracting financial benefits, but in some cases they can lead to other serious consequences.

5 >> INTERNET AS A SALES CHANNEL FOR GOODS DANGEROUS TO THE LIFE AND HEALTH OF CHILDREN

Children form their own sales market and convince parents to purchase certain goods, for example, food, toys, clothes and shoes, cosmetics, electronics and stationery. At the same time, they are not able to analyze the quality of a potential purchase, and parents do not always carefully check the purchased goods.

Advertising and selling low-quality, dangerous goods to children can lead to a whole range of negative consequences. First of all, they concern the health of the child.

In some cases, children's products contain toxic substances in concentrations several times higher than permissible. They irritate the skin and mucous membrane, negatively affect human reproductive function, can cause allergies and even cancer.



6 >> ADVANCED MARKETING TECHNIQUES

Advanced marketing strategies help companies build relationships with customers, including children.

Children are a desirable target for marketers. Companies use sophisticated algorithms to target advertising to children on social networks and games, for example, data mining and profiling.

At the same time, personal data and profiles of children are available for purchase by the business.

Children tend to buy with pocket money what is advertised to them. At the same time, even if children cannot purchase goods on their own, they are able to convince their parents to make such purchases.

7 >> DARK PATTERNS

Dark patterns are subtle psychological tricks and design solutions that deliberately push users to perform certain actions and encourage constant shopping.

There are many manipulative design techniques that push users to do things they otherwise would not do. These methods have become widespread in recent years, and currently companies are widely applying them to children's audiences.

The impact of dark patterns is compounded by the fact that children cannot protect themselves from them, as they do not have the necessary cognitive and analytical abilities. They are vulnerable, prone to impulsive behavior, easily form relationships with characters, are influenced by rewards and statuses, all the while they have not yet formed a mature understanding of the value of money and a sufficiently high level of financial literacy.

8 >> ONLINE FRAUD

Online services or software with Internet access can be used to deceive victims. Types of online fraud include phishing, lotteries, gift promotions, spam with tempting offers, fake wallets of payment systems and all possible combinations of them.

Due to the fact that children and adolescents are most susceptible to suggestion, and their psycho-emotional characteristics are at the stage of maturation, they are one of the most vulnerable categories of victims for online scammers.

The consequences of online fraud have both financial and socio-psychological consequences, including feelings of frustration, injustice, and stress.

Personal attack, psychological violence

This group includes risks whose ultimate goal is to cause moral, physical or other damage to a particular child, for example, cyberbullying, stalking, grooming and sexual harassment.

In the event of these risks, a specific child becomes a victim, and the attacker shows purposeful aggression towards them or attempts to use the child for selfish and illegal purposes.

9 >> CYBERBULLYING

Cyberbullying involves repeated episodes of aggressive behavior aimed at scaring, humiliating or angering a person. This form of behavior is found in social networks, messengers, gaming platforms and other online platforms. Cyberbullying can be committed by both children and adults.

Cyberspace abusers are more violent because of anonymity. They are more difficult to identify and bring to justice. In addition, they do not see the victim, and therefore do not see the consequences and results of their actions, which only aggravates the situation.

Cyberbullying negatively affects the behavior, psycho-emotional and physical health of the victim. Changes in the emotional state are characterized by a sharp change in mood towards negative emotions, such as anger, irritability, despondency, fearfulness, and loneliness. The specific emotional effect and severity of the consequences depend on the child, but in extreme cases cyberbullying can even cause suicide.

10 >> STALKING

Stalking is a pattern of behavior that manifests itself in obsessive harassment, stalking and prolonged harassment of the victim. It is characterized by high duration and close attention to the actions of the victim.

Stalkers can use a wide range of tactics and approaches in their harassment and surveillance of the victim. For example, regular mails and e-mails, calls, messages and other actions in social networks, installation of monitoring software on the victim's devices.

Stalking causes a range of negative emotions in the victim, the main of which are fear and a sense of loss of control over life.

11 >> GROOMING

Grooming is the establishment of friendly and emotional contact with a child for their further sexual or criminal exploitation, fraud, blackmail, compromising or harassment.

Online groomers collect information about children and find the most vulnerable victims. They get acquainted with several children at once, and then choose their victim from those who responded to their messages, and analyze the child's social networks, for example, for loneliness, lack of attention and care. After that, groomers establish psychological contact with the child for the further realization of their goals.

12 >> SEXUAL HARASSMENT

Sexual harassment includes intimidation, bullying or coercion of a sexual nature, as well as unwanted or improper promise of remuneration in exchange for sexual services, other verbal or physical harassment of a sexual nature.

The peculiarities of sexual harassment on the Internet also include unwanted sexual behavior expressed in the use of digital content in private correspondence or on public platforms. For example, the exchange of images and videos of a sexual nature, coercion and threats, sexual bullying.

Children who become victims of sexual harassment on the Internet show serious deviations in physical and psychological health. For each victim who has been harassed, these consequences are unique, and recovery can last a lifetime. Harassment on the Internet can go offline and take the most critical form, i.e. rape.

Digital exploitation, using a child to create digital content

This group includes risks that are directly related to the exploitation of a child or information about them on the Internet, for example, doxing, creation and distribution of materials with child pornography, theft, collection and exploitation of personal data, as well as sharenting.

Thus, the child's personal data may be disclosed and/or used unlawfully, which will entail threats to their physical, psycho-emotional or financial well-being. At the same time, a child can be used to create digital content in a variety of ways, for example, from photos in the parents' blog to the illegal exploitation of children in the production of sexual materials.

13 >> DOXING

Doxing is the public disclosure of personal information about a person or group of people on the web. Such information may include, for example, real name, address of residence, place of employment, data of relatives, phone numbers, financial, medical and other identifying information.

Sometimes doxing means not only the publication of data, but also the preparation process, such as the collection of information about the victim and the victim's loved ones through the use of social networks, government reports, search engines and other sources of information.

The child's personal information is published and distributed without their consent. Doxing is usually done intentionally in order to take revenge, intimidate, blackmail or otherwise harm the victim.

14 >> CREATION AND DISTRIBUTION OF CHILD PORNOGRAPHY MATERIALS

With the development of technology, pornographic materials about children in large quantities are created and transferred by criminals around the world.

It is impossible to determine how many people consume child pornography, just as it is impossible to determine exactly how many children are victims of child pornography.

The consequences for child victims are extremely serious. Such crimes are directly related to child abuse. And the fact that the abuse was recorded and distributed makes the situation worse, since the trauma is amplified by the knowledge that the recorded and depicted violence spreads and gives pleasure to others.

15 >> THEFT, COLLECTION AND EXPLOITATION OF PERSONAL DATA

The exploitation of personal data implies obtaining access to children's personal data and collecting this information in an illegal way, as well as without the consent of the children themselves and their parents, including further misuse. In addition, this risk includes data obtained legally, but used for selfish purposes.

Most often, children themselves indicate personal information on the Internet and freely share it with other people. At the same time, they consider only contact information confidential and do not worry about the photo and video content that they publish.

Access to personal data opens up opportunities for other offenses and risks associated with danger to the mental and physical health of the victim.

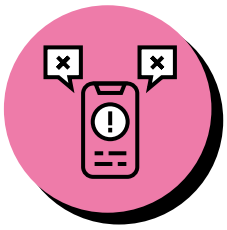
16 >> SHARENTING

Sharenting is the regular use of social networks by parents to share news, images and other information about children. The word is formed from the English words "share" and "parenting" meaning to educate, raise a child.

Children often feel awkward when their parents post their photos. They are also worried that they cannot influence the publication of photos by their parents in any way.

Sharenting can lead to a distortion of ideas about real life. Parents express their point of view, often without asking what the children themselves think about it. By publishing posts about their children, parents themselves create a digital portrait of the child on the Internet, thereby interfering with their digital identity. In addition to the fact that parents publish photos of their children and stories related to their upbringing, they also disclose confidential information about their children, which may include the children's full name, date of birth, weight, height, geolocation and other data.

Information pressure, information not intended for children and adolescents



This group includes risks based on information that can injure, misinform, push a child to incorrect conclusions or dangerous actions, for example, content containing violent scenes, pornographic content, misinformation, as well as dangerous trends and challenges.

The consequences of such risks can have an extremely negative impact on the psycho-emotional and physical condition of the child, as well as pose a danger to society as a whole.

17 >> CONTENT CONTAINING VIOLENT SCENES

This kind of content includes any perceptible form of presentation of information that reproduces situations or actions of a violent nature that cause or may cause harm to one or more persons.

Children learn by observing and trying behavioral scenarios, so they are particularly susceptible to the negative consequences that the consumption of violent content causes.

Short-term effects are associated with arousal processes and direct imitation of a certain behavior. The long-term effects are due to a longer study of such content, which is why the negative emotions of children towards violence gradually decrease, and new attitudes are formed.

18 >> PORNOGRAPHIC CONTENT

The Internet is considered a key channel for the distribution of pornographic content. At the same time, children and adolescents may encounter pornography intentionally and unintentionally.

Deliberate search and consumption are possible due to the fact that the mechanisms of age verification in social networks and on websites with this kind of content are imperfect. Among the reasons for an unintentional encounter with pornography are the study of topics related to sex, for example, the relationship between a man and a woman.

When encountering pornographic materials, some children experience disgust, confusion and anxiety, but each time these feelings become weaker. This affects mental health and well-being, including encounters with pornography are a predictor of increased sexual aggression and a frivolous attitude to sexual contacts.

19 >> DISINFORMATION

Disinformation is an attempt to create a false impression and push the object of influence to the desired actions or inaction. This is the process of manipulating information, for example, misleading someone by providing incomplete or out of context information, distorting part of the information, spreading rumors, lies and loud statements not supported by facts.

The Internet is considered the main channel and tool for spreading disinformation. At the same time, children may be particularly vulnerable in matters of information perception, since their thinking and cognitive abilities are still developing.

Children cannot assess the reliability of the information they encounter on the Internet. This can lead to the formation of a false picture of the world in them, or committing incorrect actions towards themselves and others.

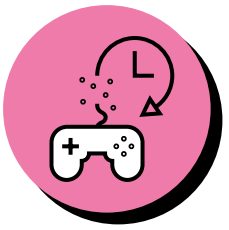
20 >> DANGEROUS TRENDS AND CHALLENGES

Trends and challenges involve children and teenagers in mass activities that can threaten the mental and physical health of participants or others through social networks and messaging in various messengers. Involvement occurs by inviting the audience to a game or competition with the performance of tasks, reports in photo and video format or online broadcast.

In most cases, participation in tasks or games leads to dangerous consequences due to a lack of understanding of the real risk and unformed critical thinking. If teenagers already have any psychological problems, including suicidal tendencies, they find dangerous trends that aggravate the condition, which together can lead to tragedy.

Among the consequences of dangerous trends can be poisoning, physical and psychological injuries inflicted on themselves and others, and even unintentional death or suicide. In addition, dangerous trends can contribute to the sexualization of children or involve them in criminal communities.

Addiction, formation of dependence on the Internet environment



This group includes risks, upon the onset of which a child develops dependence on the Internet in general or its specific elements, for example, attention retention algorithms, gaming addiction and excessive use of the Internet.

The consequences of such risks are the deterioration of the general well-being of the children, their social ties, and academic performance. Often, such dependence leads to behavioral deviations, lack of interest in the usual life and depression.

21 >> ATTENTION RETENTION ALGORITHMS

Algorithms analyze user reactions, read an instant response to information, and then select similar content. Thus, they limit the flow of information to publications interesting to the user, form recommendations, and show targeted advertising.

The main goal of algorithms is to keep the child's attention as long as possible. To do this, many marketing tools are used, for example, game loops that create the effect of incomplete action and cause the syndrome of missed opportunities (FOMO, English: fear of missing out).

Showing only what is interesting to the user, the algorithms are initially designed to polarize opinions on any topics that affect the formation of the worldview of children and adolescents.

The system selects people by interests and beliefs, combining them into groups. This effect is called an “echo chamber”, when the user is surrounded only by the information and those people who confirm one point of view, thus reinforcing his belief in being right. At the same time, the difference in views and attitudes between such groups increases, which provokes aggression and conflicts.

20 >> GAMBLING ADDICTION

Gambling addiction is characterized by a constant, recurring loss of control over the gameplay, an increase in the priority of games over other interests and daily activities of the child, as well as the continuation or escalation of this behavior pattern, despite the occurrence of negative consequences.

Among the reasons for gambling addiction, there is an increase in social status. Thus, the status of the character and achievements in the game directly depend on the time spent. At the same time, many games have paid in-game items that give the user an advantage, which puts a lot of pressure on the fragile psyche of children and adolescents and pushes them to buy.

Addiction to games causes various problems with social, psychological and even physical condition. It leads to a violation of the classic social interaction of the child with family and friends, changes the way of life, and interferes with academic performance.

23 >> EXCESSIVE INTERNET USAGE

Excessive use of the Internet leads to a violation of a person’s psychological, social, personal, academic or professional well-being. In some cases, this translates into dependence on the Internet, when a person has an unjustified anxiety and a desire to connect to the network as soon as possible.

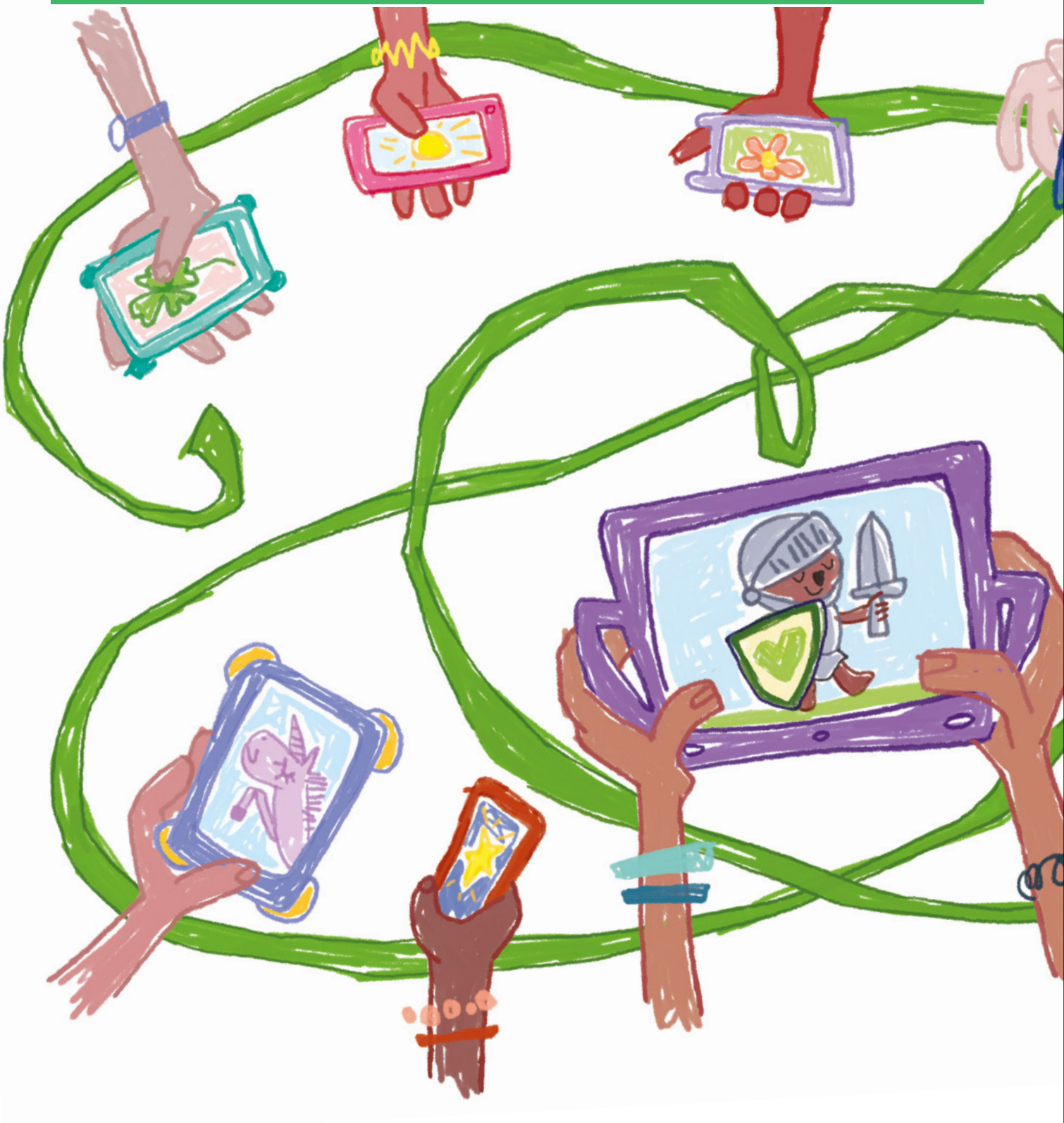
The main symptoms of Internet addiction include not only an increase in the amount of time spent on the Internet, but also mood swings, feelings of loneliness, anxiety and irritability. In addition, Internet addicts tend to refuse responsibility and deny problems.

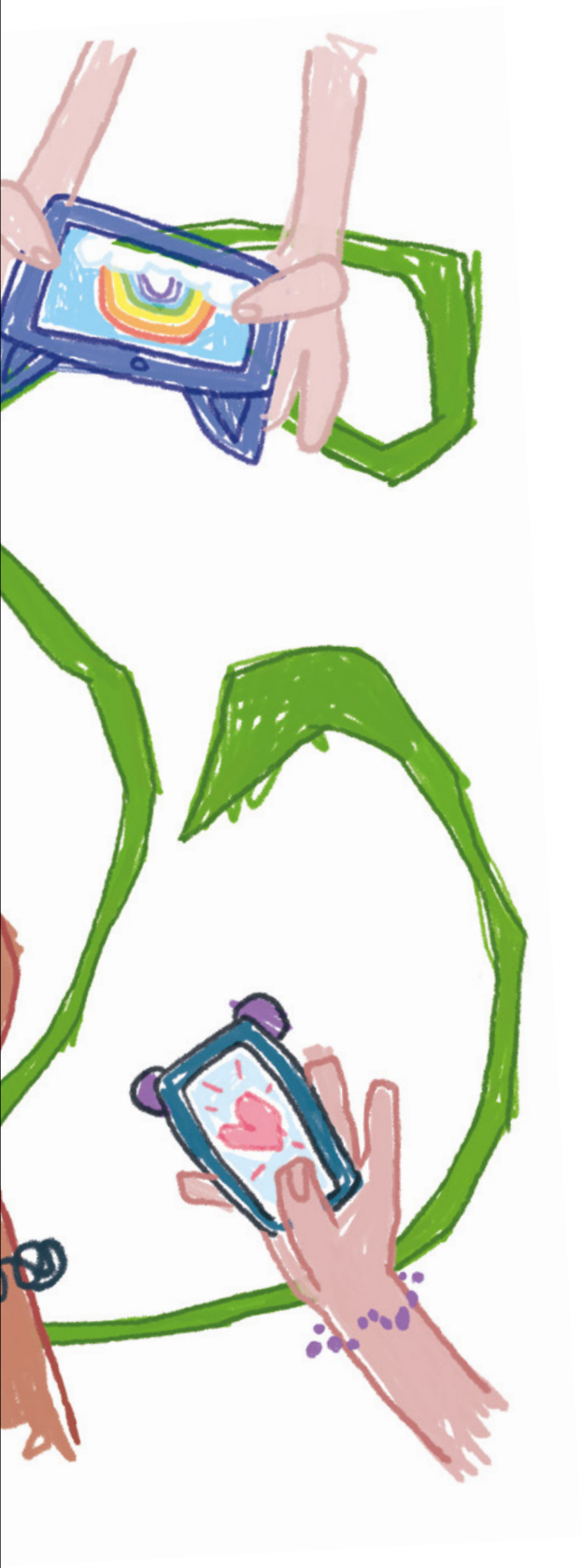
Such teenagers most often cannot control the time spent online, and are also unable to reduce it on their own.

Teenagers addicted to the Internet and social networks also have dysmorphic phobia, a mental disorder in which a person is overly concerned about a minor defect or feature of their body. Filters, tools for retouching and photo processing form misconceptions about appearance in children and adolescents, which leads to complexes in real life.


GAME OVER

Technological solutions for the protection of children on the Internet



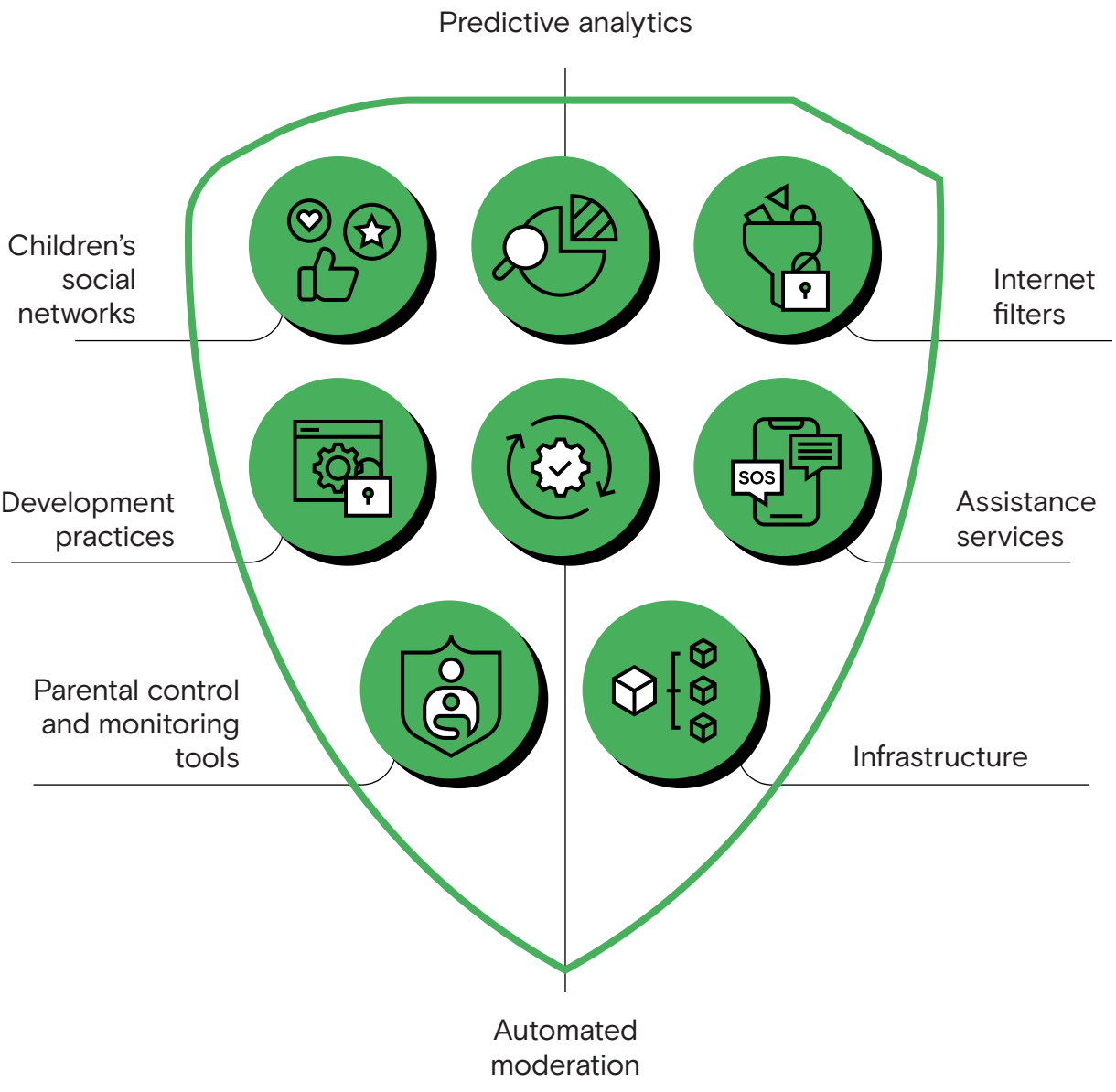


2

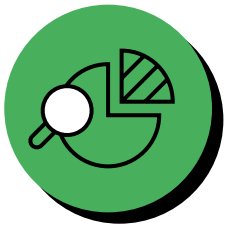
>>

In order to determine the range of existing technological solutions aimed at ensuring the safety of children on the Internet, we analyzed more than 300 patents, companies and IT solutions in this area. According to the results of the analysis, 8 clusters of technological solutions were formed.

>> CLUSTERS



Predictive analytics



Predictive analytics can be used to protect children online by identifying individuals at risk of committing a crime or becoming a victim of a crime. It allows for predicting and identifying risks of various types at an early stage, studying and classifying risk sources, and ranking them according to the age groups of children.

Predictive systems use big data, statistical methods, as well as artificial intelligence and machine learning. Predictive analytics involves the study of the online environment, including algorithms, devices and user habits of children, as well as profiling and analysis of the graph of connections. However, this raises a number of ethical questions about the use of children's personal data.

During the analysis of information, predictors are identified. These are certain signs in the pattern of behavior that are a signal of possible risk. The limitation in this case is the complexity of collecting relevant data, as well as long-term training of algorithms for building predictive systems and possible errors in the results.

#

PrevBOT

A chatbot based on algorithms. It helps the police in identifying intruders in chat rooms, messengers and social networks. The bot reads other people's correspondence and records them, and can also simulate the communication of a child, which allows for detecting intruders. The linguistic model of the robot allows for determining the gender, age and author's handwriting of a person and correlating it with the database of cyber-profiled accounts of other potential criminals. In addition, since the robot is able to recognize criminals and determine which digital spaces they occupy, it can be used as a tool to identify communities that are dangerous for children.

Children's social networks

Children's social networks are analogous to conventional social networks. They are able to provide additional security and protection from threats that a child may encounter on the Internet.

Social networks for children are protected by various systems of moderation and filtering, which allows for blocking the publication of rude, cruel, undesirable content for viewing. However, automatic content filtering systems even in children's social networks are imperfect, and moderators do not always have time to track such incidents.

Children's social networks are also aimed at limiting children's contacts with intruders and adults. In addition, some children's social networks provide for communication of the child only with those users who have been previously approved by parents or guardians. At the same time, there remains a fairly high probability of registering an adult attacker in a children's social network under the guise of a child.

#

GromSocial

A children's social network that teaches children to build confidence and not take angry comments to heart. Parents are required to register in GromSocial, which minimizes the presence of adult intruders in it. As soon as the social network is activated, 17 cartoon characters get to the child's friends, behind which there are moderators who are ready to help with any questions.

Development practices

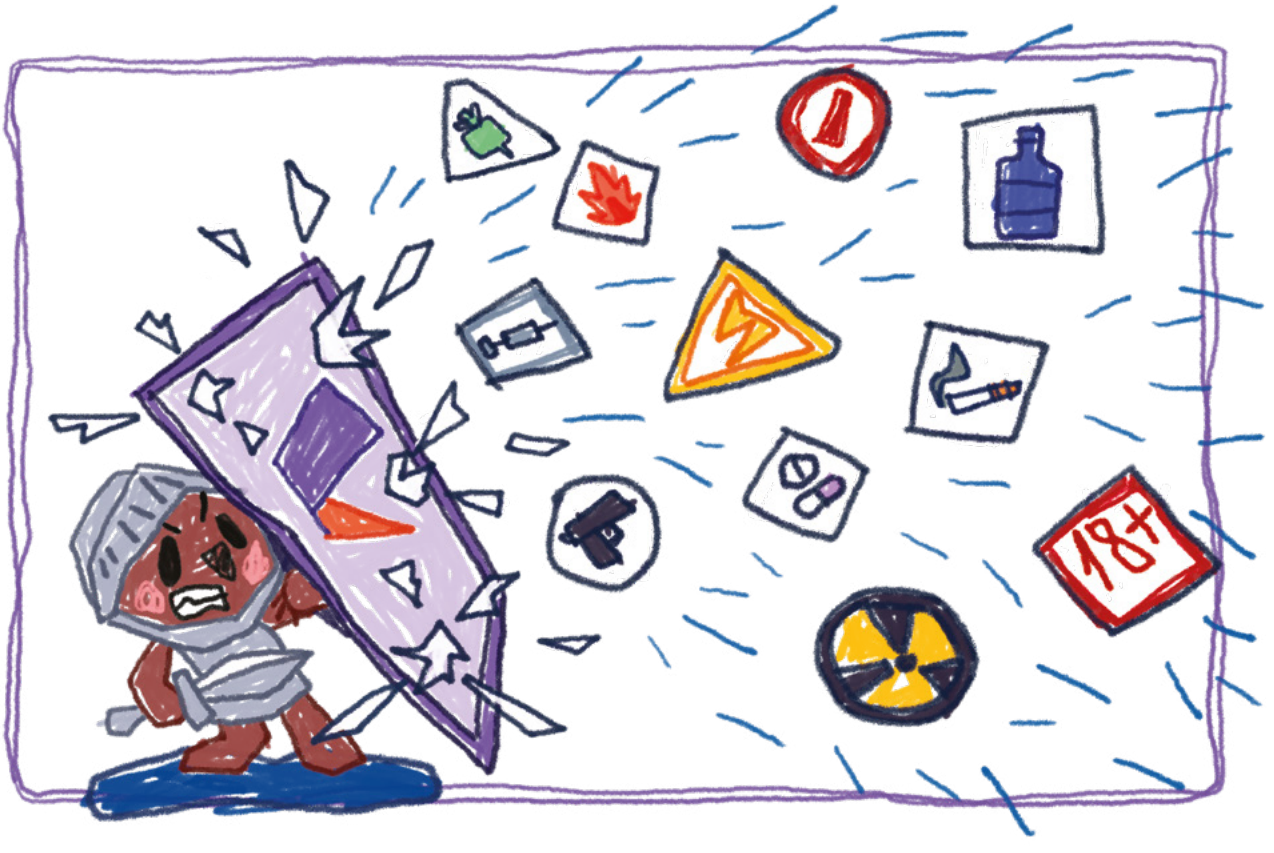
Development practices include the creation and improvement of functionality related to child safety in apps and on Internet websites.

The user interface should provide the ability to block certain functions in order to avoid launching unwanted actions and protect children from viewing unacceptable information. As an example, we can cite solutions that ensure compliance with age restrictions, notify about potentially traumatic content of a publication or the insecurity of certain websites.

Often, existing solutions do not block, but are only limited to notifying users about age restrictions and the content of the content, including its potential danger. At the same time, users themselves are responsible for subsequent actions on the platform, website or in the app.

Deutsche Bank API Program (DBAPI)

A solution that helps online sellers of adult products to prevent minors from entering their websites. The DBAPI Age Certificate offers verification based on Deutsche Bank customer data. Verified information about the user's age is sent to the website in real time, which allows for increasing the reliability of data about the age of visitors.



Parental control and monitoring tools

Parental control tools provide parents with an increased degree of control over the actions of children in the online and offline environment by installing special software on smartphones, computers and other devices of the child.

The basic functionality of parental control tools includes blocking access to the Internet, apps and games, limiting screen time, protecting against inappropriate content by filtering it, tracking online activity, contacts and the location of the child.

These functions consist in proactive regulation and monitoring of the child's actions on the Internet, and therefore, such software allows for identifying and minimizing cyber risks for children in advance. Despite the wide range of functions of such programs, the complete isolation of a child from cyber risks will not contribute to the development of the necessary cybersecurity competencies that they will need in the future.

Scientific research also shows that parental control tools that allow for constant monitoring of the child destroy trust in parents, and in some cases can even lead to psychological trauma and depression. In the case when a child or teenager experiences rejection and rejection of parental control tools, they can find ways to circumvent the established rules.

#

Kaspersky Safe Kids

Parental control solution. Compatible with Windows, macOS, Android and iOS. Functionality: blocking unwanted content, restricting access to devices according to a schedule, restricting access to applications, compiling a list of applications that are accessed with parental permission, GPS location tracking, safe search and activity history on YouTube, battery level monitoring.

Internet filters

One of the ways to protect children on the Internet is the use of Internet filters that block access to unwanted websites and download files of certain subjects, restrict the launch of apps and games.

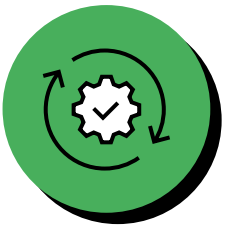
There are also special programs that provide filtering of Internet resources by keywords encountered without the need for parents to manually blacklist individual websites with unacceptable content for children.

Such filters are not tied to the response time of the moderator team or the neural network, but protect the child constantly.

Lidrekon

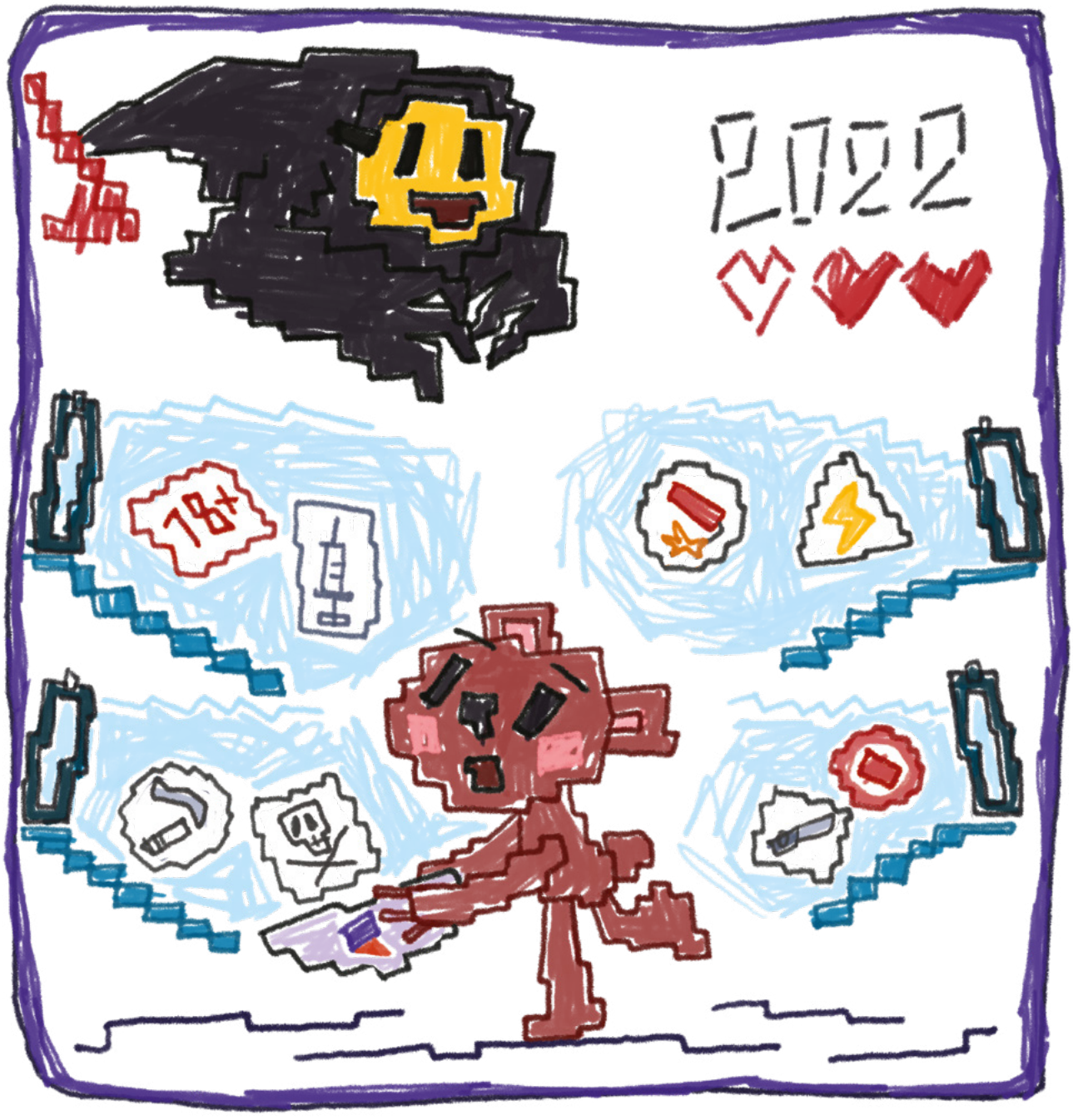
A browser extension that allows for filtering content. The content is checked on the basis of the Russian filter library, which is constantly updated. Filters content by topics: self-mutilation, suicide, surfactants, drugs, tobacco, alcohol, gambling, prostitution, vagrancy, justification of violence against people and animals, denial of family values, non-traditional orientations, disrespect for children and parents, crime, weapons, obscene language, pornography, extremism.

Automated moderation



Content moderation involves deleting information, filtering or blocking it, recommending content through news feeds, thematic lists and personalized offers, as well as monitoring content.

Automated content moderation can be used at the appropriate stages of preventive detection of potentially problematic content, as well as for automated evaluation and execution of decisions on removal, labeling or demarcation, demonetization or prioritization of content. Automation of moderation allows for significantly speeding up the process, and also has a wider scope, for example, the ability to check content in closed communities. However, in order to bypass self-moderation systems, data modification options are widely used, including, for example, the introduction of additional spaces or their complete absence, the use of transliteration, and other methods.



At the same time, the advantage of manual moderation lies in the relative accuracy, verifiability of the results of the removal of materials, as well as the possibility of improving the criteria for blocking.

Automatic filtering mechanisms are more effective, but they are more likely to make mistakes when blocking or deleting content.

Meta[5]

It uses self-moderation to identify spam, fake pages, pornography, extremist materials, videos with scenes of cruelty. However, to date, algorithms are not able to accurately recognize calls for extremist activity, and moderators are engaged in this. Instagram5 has implemented an AI-based DeepText program to filter bullying and bullying. Initially, it was only looking for spam, then it learned to detect offensive comments, and then the tool began to be trained to analyze not only comments, but also posts.

Assistance services

Assistance services include a range of organizations and services that allow a child, parent or other interested persons to request the help of psychologists, volunteers, human rights defenders and other specialists.

They can serve to provide psychological assistance, communication between children and the state, NGOs, and volunteers. Such organizations actively use technology and are being implemented in the infrastructure that concerns child support. One of the tasks of the response platforms is also to educate the public about helping children.

5 Recognized as extremist organizations whose activities are prohibited on the territory of the Russian Federation

At the same time, the main limitations of such services are the competence of specialists and the quality of assistance provided. Volunteers often work in such organizations, who are not always able to properly help a child faced with difficulties and risks.

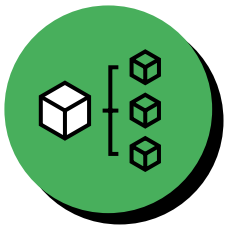
Many response platforms involve several channels for communication with children, for example, a helpline, websites, messengers or chatbots. Depending on the size and technical capabilities of the organization, the number and bandwidth of such channels vary.

#

It's hard for teenagers

A chatbot that allows children affected by bullying to seek help. The bot is able to redirect requests for help to organizations and individual specialists. It identifies the child's problem and then sends reference materials, contacts of specialists and specialized services.

Infrastructure



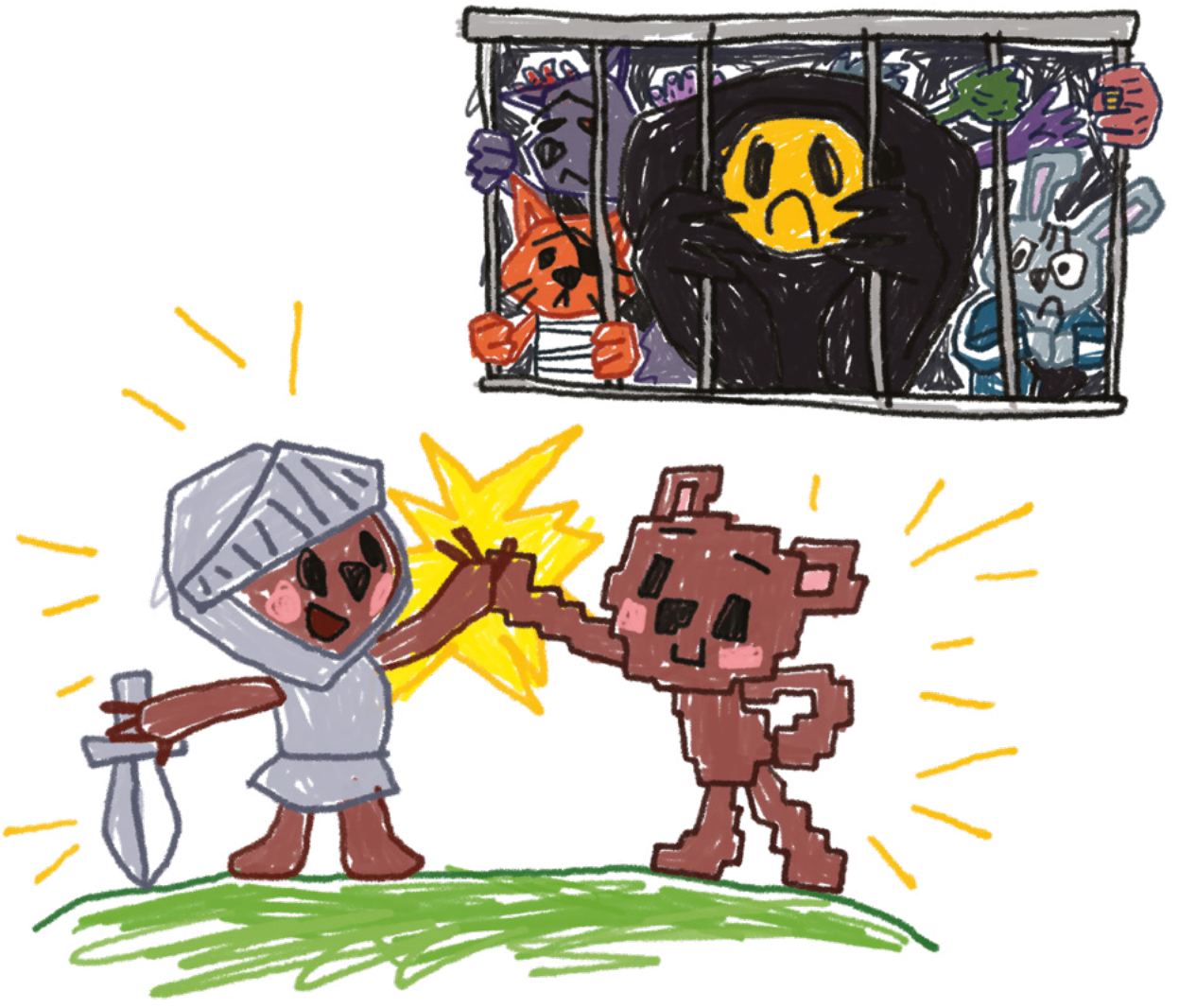
Infrastructure means a set of interconnected objects, structures, and security solutions integrated into a single system.

The basic principle of security is the continuity of protection in space and time.

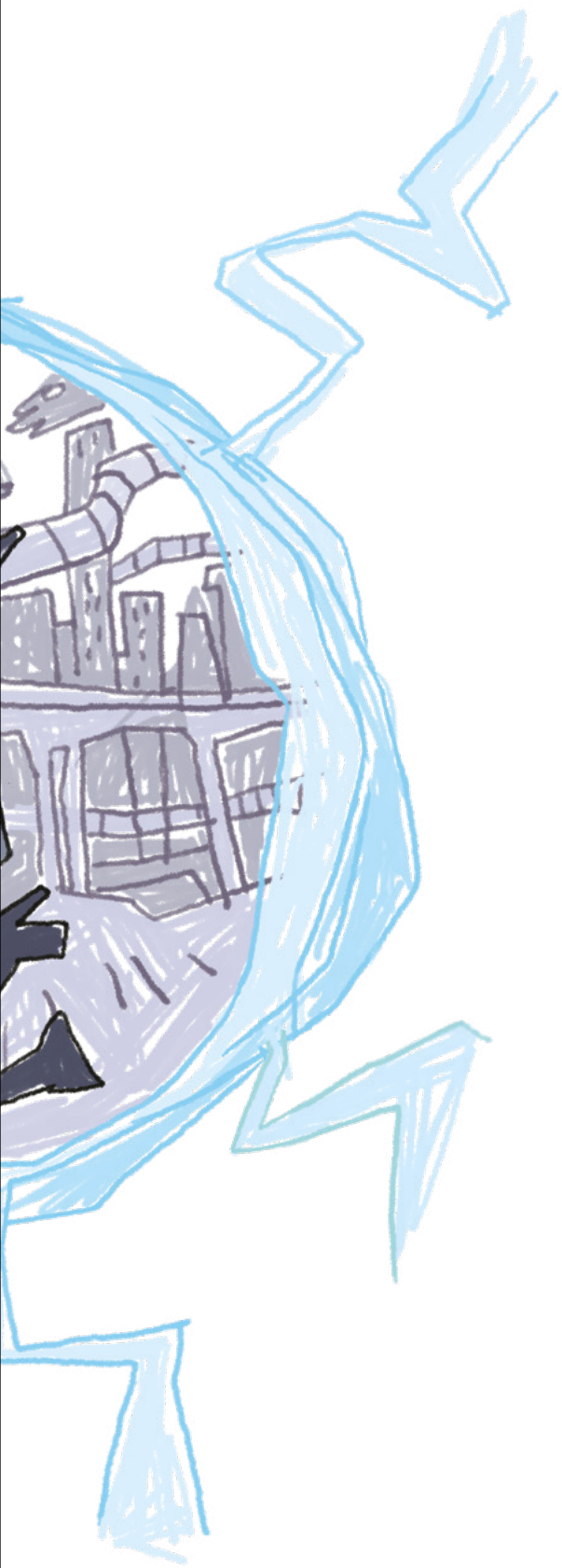
Through system integration, infrastructure unites resources and spaces. Resources are understood as various technical and hardware tools, software and databases, channels and means of communication. Spaces, in turn, include various physical objects, starting from the child's place of residence, and ending with public places, transport, educational institutions and the city as a whole.

AviaTor

Infrastructure project of INHOPE (International Association of Internet Hotlines). INHOPE unites 50 hotlines in 46 countries to combat materials containing sexual abuse of children. The organization processes thousands of requests annually. AviaTor is a system in which moderators process images, placing markers and hashes, as well as fixing them in the database. This allows for automatically detecting similar criminal materials on the Internet. INHOPE transmits data to law enforcement agencies, which facilitates the search and capture of criminals distributing such materials.



Future risks



3

>>

The digital world is changing rapidly, and therefore, in the next 5-10 years, it is possible to predict the emergence of new cyber risks for children and adolescents associated with the development of technology, geopolitical changes and new trends. We have identified 10 areas where risks for minors will be formed in the near future.

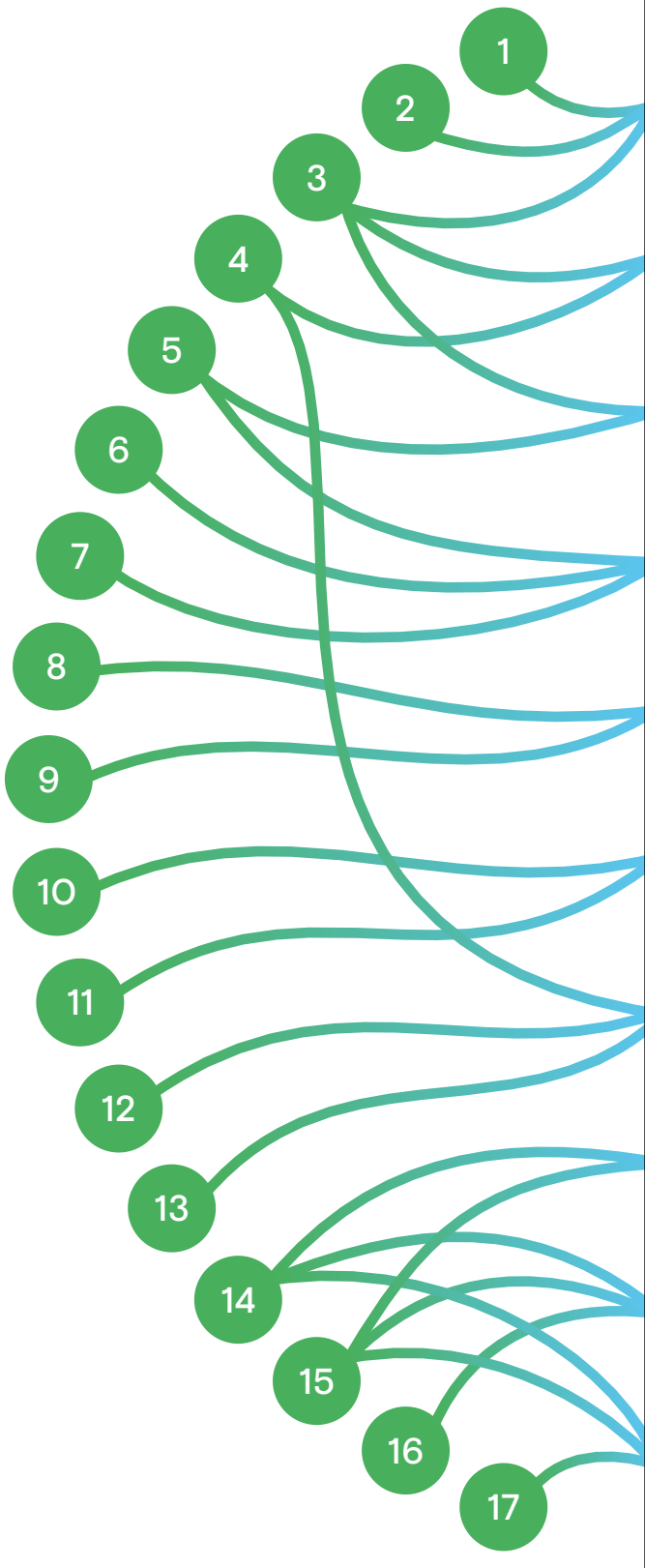
>> FUTURE RISKS

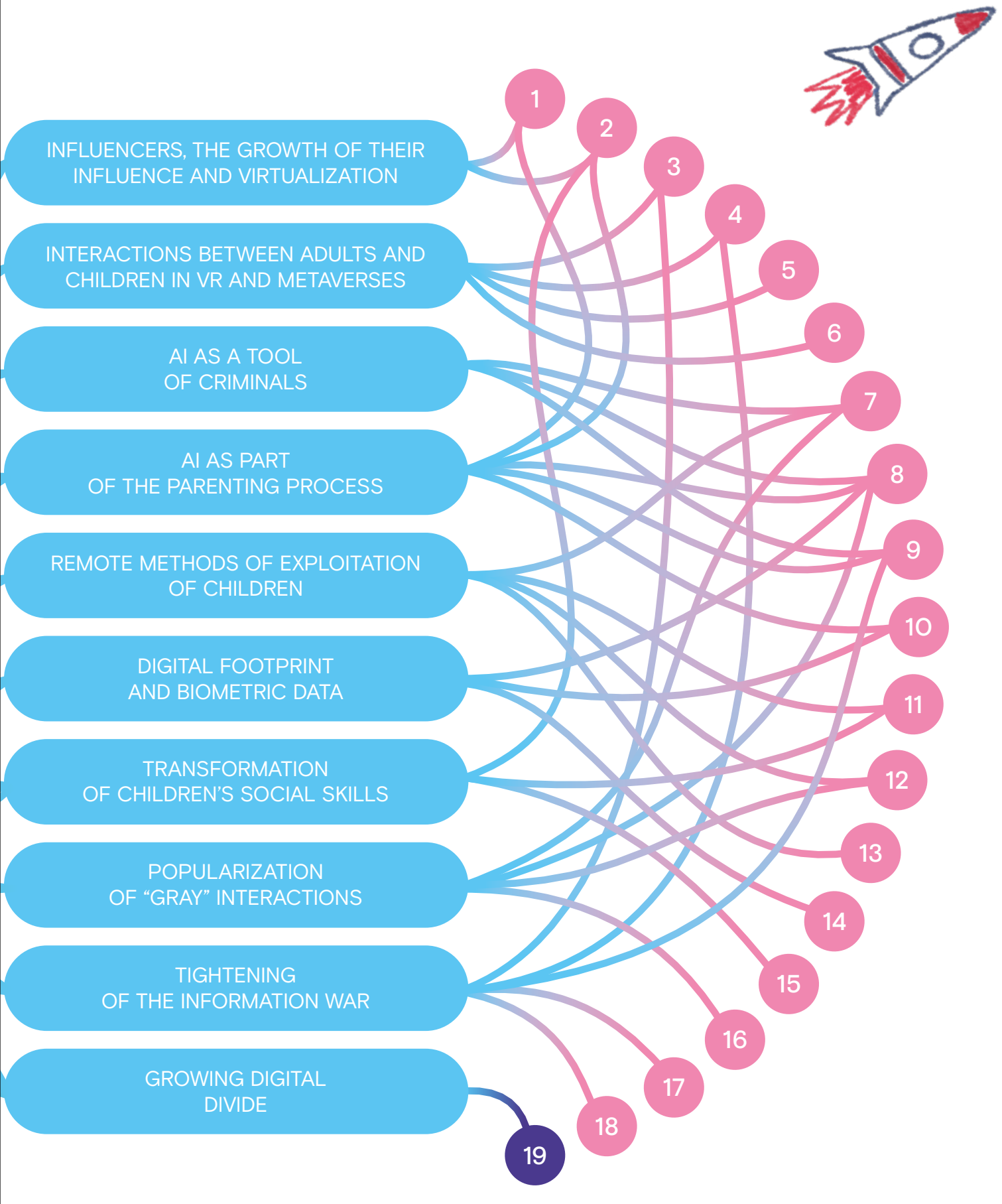
Trends and technologies

1 Influencers
2 Neural networks
3 VR
4 Metaverses
5 Artificial intelligence
6 Smart systems and gadgets
7 Strengthening the influence of corporations
8 Models of earnings in games
9 Monetization of user content
10 Biometrics
11 Big Data
12 COVID-19 / social isolation
13 Digitalization of society
14 Geopolitical changes
15 Blocking and incorrect regulation of Internet resources
16 Post-truth
17 Socio-economic changes

Existing risks

1 Dangerous trends and challenges
2 Attention retention algorithms
3 Cyberbullying
4 Stalking
5 Grooming
6 Sexual harassment
7 Online fraud
8 Theft, collection and exploitation of personal data
9 Disinformation
10 Advanced marketing techniques
11 Gambling addiction
12 Sale of prohibited goods and services
13 Dark patterns
14 Sharenting
15 Excessive Internet usage
16 Involvement of children in criminal communities
17 Doxing
18 Radicalization and extremism
19 Includes all 23 risks




INFLUENCERS, THE GROWTH OF THEIR INFLUENCE AND VIRTUALIZATION
INTERACTIONS BETWEEN ADULTS AND CHILDREN IN VR AND METAVERSES
AI AS A TOOL OF CRIMINALS
AI AS PART OF THE PARENTING PROCESS
REMOTE METHODS OF EXPLOITATION OF CHILDREN
DIGITAL FOOTPRINT AND BIOMETRIC DATA
TRANSFORMATION OF CHILDREN'S SOCIAL SKILLS
POPULARIZATION OF "GRAY" INTERACTIONS
TIGHTENING OF THE INFORMATION WAR
GROWING DIGITAL DIVIDE
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

1 >> INFLUENCERS, THEIR GROWING INFLUENCE AND VIRTUALIZATION

Influencers influence the opinions and choices of children and adolescents, broadcast their values and enjoy the trust of the audience, but they are not always aware of the responsibility for this. At the same time, semi-virtual and virtual influencers appear, whose avatars are unknown people or organizations capable of broadcasting their values and manipulating the audience's trust for various purposes.

2 >> INTERACTIONS BETWEEN ADULTS AND CHILDREN IN VIRTUAL REALITY AND METAVERSES

In modern VR applications, the degree of control over the interaction of children and adults is low, since adults can use avatars of children, and children can use avatars of adults. With the penetration of virtual reality and metaverses into our lives, more and more people of different ages will go to the same platforms. There have already been precedents in VR of cyberbullying, sexual harassment and other actions that can spread the associated risks to children and adolescents.

3 >> ARTIFICIAL INTELLIGENCE AS A TOOL OF CRIMINALS

The commodification of artificial intelligence, the simplification of the creation of neural networks and the entry of such technologies into the consumer market will allow attackers to use them as a tool. There are already examples of systems capable of copying a face, voice and facial expressions. This can be used by fraudsters to bypass systems based on biometric verification. Such technologies allow

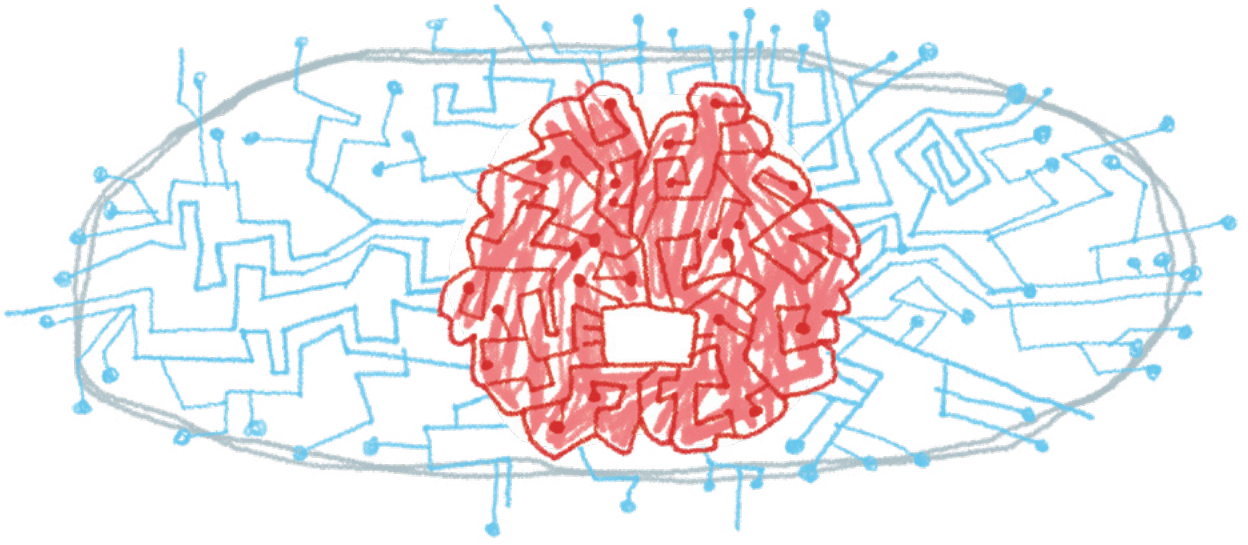
an aggressively minded child to create a photo or video in which a peer is in a compromising situation.

4 >> ARTIFICIAL INTELLIGENCE AS PART OF THE EDUCATION PROCESS

Home voice assistants open up a new vector for corporate intrusion into the family. There is a possibility that children using AI assistants as toys will become victims of the creators of such devices. Creators can broadcast ideas through them, manipulate content selection algorithms, and collect data. There is also the question of parents' awareness of the unprecedented role that corporations are beginning to play in the upbringing of their children.

5 >> REMOTE METHODS OF EXPLOITATION OF CHILDREN

One of the mechanics of Web 2.0 is the creation of content by users. Minors are already producing content on the platforms of commercial companies absolutely free of charge. For example, hundreds of hours of group work are spent on projects in the Roblox video game, for which the company receives profit, and not the actual content creators. The topic of child labor exploitation on the Internet has been little studied, and adults rarely understand the rules by which the complex ecosystem of virtual child labor functions.

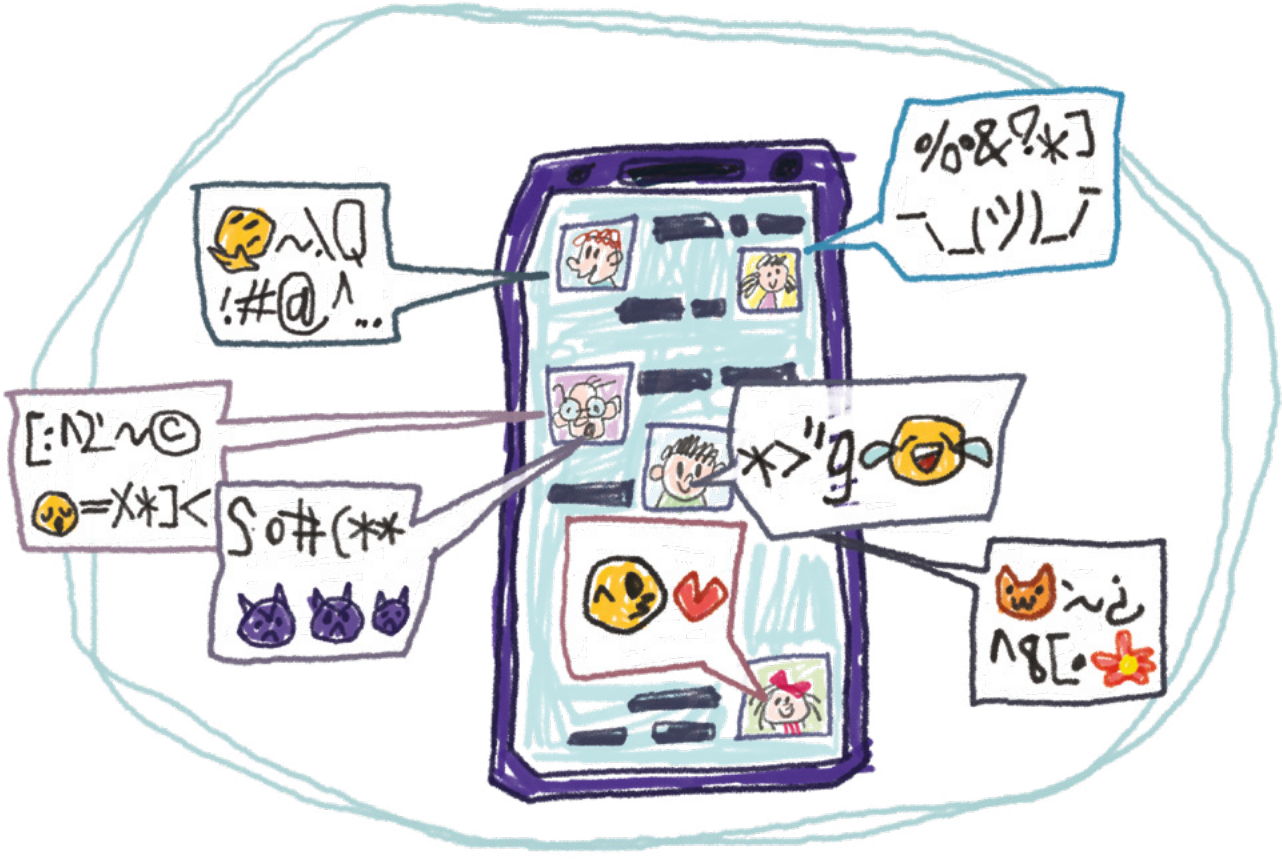


6 >> DIGITAL FOOTPRINT AND BIOMETRIC DATA

The digital footprint begins to accumulate by the child from an early age. This can be a vector for a variety of attacks, for example, a careless statement on the Internet can become a reason for dismissal, and an extensive digital footprint, biometric and personal data is a target for scammers, stalkers and other intruders.

7 >> TRANSFORMATION OF CHILDREN'S SOCIAL SKILLS

Children began to communicate more online, use home devices with artificial intelligence and form parasocial relationships with bloggers and influencers. The process of mastering the social field has changed, and children may have problems with the traditional form of socialization. At the same time, the risks associated with



dependence on the Internet, social networks and computer games will become increasingly widespread.

8 >> POPULARIZATION OF “GRAY” INTERACTIONS

Massive restrictions on access to resources on the Internet and the possible regionalization of the Internet have already led to the spread of various services and approaches to overcome the imposed prohibitions. Such software are popular with both adults and children, have a user-friendly interface and are often posted on the Internet with setup guides. Popularization of “gray” interactions can lead a child not only to study information technology, but also to join a hacker cell as a so-called “script kiddie”, a young apprentice of more experienced hackers.

9 >> TIGHTENING OF THE INFORMATION WAR

Various actors are increasingly using cyberspace for information wars. Children do not have developed critical thinking, and therefore they are the most vulnerable, since they unwittingly turn out to be the main victims of information wars, the consequences of which will multiply and become less predictable.

10 >> GROWING DIGITAL DIVIDE

Digital inequality and actual deprivation of children in certain countries of their civil rights may limit their ability to receive timely assistance and protection, since service providers will not be able to use the full range of measures to counter cyber risks, and law enforcement agencies will be limited in investigating crimes.

Recommendations to stakeholders

4

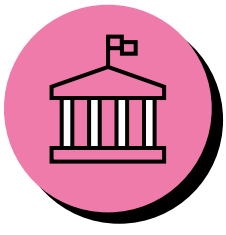
>>

The analysis of threats and risks faced by children and adolescents in the process of using the Internet allows for formulating a number of recommendations to stakeholders who are more or less responsible for the implementation of security technologies in the online environment.

Among such stakeholders we include the state, educational institutions, commercial enterprises, parents, non-profit organizations (NGOs) and social entrepreneurs, as well as IT developers.

It is important to take into account, on the one hand, that effective protection can be achieved with coordinated and reasonable efforts on the part of all stakeholders. On the other hand, we are convinced that the key role in ensuring Internet security is to facilitate the process of forming a child as a conscious and experienced subject who actively uses digital resources for their development.

State



The state should take a leading role in organizing and coordinating the joint activities of various stakeholders. It is necessary to expand support for existing and create new communication platforms designed to discuss cybersecurity issues and find joint ways to solve them.

There is a need for state programs to codify and monitor the problems of cybersecurity of children and adolescents, as well as programs to support interdisciplinary theoretical and applied research in this area.

The legislative regulation of personal data needs to be improved in terms of openness and security of practices related to the data of children and adolescents. The digital rights of children of both private and platform users should be reviewed and reviewed on a regular basis.

Educational institutions

Educational institutions face a complex task related simultaneously to the safe inclusion of online technologies in the educational process, the implementation of curricula and disciplines dedicated to Internet security, as well as the digital socialization of children and adolescents. It is necessary to conduct a comprehensive analysis of cyber risks and standardization of processes related to the use of computer and Internet technologies in education.

Educational modules on cybersecurity and digital literacy should become a cross-cutting direction in the education of children and adolescents at all stages of education. In addition, professional development programs should be developed for specialists related to the cyber defense of children and adolescents (teachers, lawyers, law enforcement officers, psychologists, etc.).

Teachers should become moderators of the household culture of Internet and digital technology security. The institute of a class teacher and a school psychologist needs to be rethought taking into account the digitalization of the environment surrounding children and adolescents. Through the joint efforts of teachers and parents, it is necessary to find a balance between control and privacy, while the main task should be the realization of the Internet needs and interests of the student on the basis of mutual respect, support and development of independence.

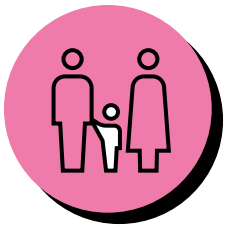
Commercial enterprises

In general, the task of business in the field of ensuring the Internet security of children and adolescents is to take a socially responsible position in relation to the risks and threats that arise in relation to this category of the population when developing and selling digital goods and services designed for various target audiences.

Commercial enterprises should conduct an ethical examination of distributed digital content, design elements, user interfaces, implemented UX/UI solutions, etc. The corresponding functionality should be the responsibility of special employees dealing with compliance with the requirements in the field of cybersecurity of children and adolescents (“Chief Kids Compliance Officer”).

Special attention should be paid to the development of initiatives aimed at supporting and developing cooperation between business and other key stakeholders in the development and implementation of new effective mechanisms to ensure the privacy of children and adolescents in an online environment.

Parents

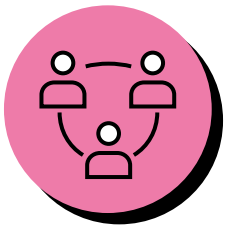


Parents play a key role in the primary socialization of children, and the organization of their daily practices.

Firstly, parents need to be involved in the virtual life of their children, showing respect and interest in this part of the socialization of the individual. Secondly, it is necessary to use all opportunities to improve their own competencies in the field of digital literacy and cybersecurity.

Thirdly, it is necessary to share the best practices of organizing children’s Internet activity, taking into account the balance between their privacy and control over their actions. And finally, do not ignore the available technological tools for information security of children and adolescents.

NGOs

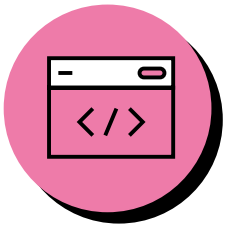


The task of public organizations, one way or another related to the problems of Internet safety of childhood, is to spread initiatives aimed at the development of this area, as well as to coordinate the actions of various factors.

The NGO's function is to create and support interdisciplinary discussion platforms on cybersecurity of children and adolescents. NGOs are able to act as centers of knowledge and competence for various stakeholders who need appropriate expertise.

They should also take on targeted support for children and adolescents who have faced the consequences of various types of cyber attacks, and those who need rehabilitation and resocialization. It should be noted separately the prospects for the development of social entrepreneurship in the field of Internet security of children and adolescents.

IT developers



IT developers are a source of professional competencies in the field of cybersecurity, as well as creators of products aimed at information protection of various categories of the population, including children and adolescents.

Effective work on the development of IT solutions that support cybersecurity and reduce the risks of Internet users is impossible without the exchange of experience, discussions at professional and industrial events, including of international level, the study and use of foreign experience, as well as mastering best practices.

One of the most promising areas in this area is the development of a set of preventive protection measures based on big data, profiling, predictive analytics and continuous monitoring through cooperation with specialists in the field of psychology, criminology, etc.

Attention should also be paid to the importance of ensuring environmentally friendly development of software products, taking into account the principles and goals in the field of sustainable development of the United Nations.

Methodology

5

>>

The study was conducted in two stages:

1. Analysis of primary sources
2. Survey of experts

First stage

1 >> A cluster analysis was carried out based on a sample of more than 21 thousand scientific articles.

>21 000
scientific articles

2 >> More than 500 literature sources devoted to the topic of the safety of minors on the Internet were analyzed.

>500
sources of literature

3 >> After the initial systematization, 23 cyber risks were identified. Combining risks into categories was based on independent expert coding. 4 experts participated in the work, each of whom created their own set of categories. After that, the results of each expert's work were compared with others, and a decision was made on the formation of a category and its name. Discrepancies were discussed, and experts agreed on each of them.

23
cyber risks

4 >> For each category, we have created a description containing a definition, a story about the essence and specifics of the threat, available statistics and research, as well as cases and examples.

5 >> We have analyzed more than 300 IT solutions, patents, commercial companies, platforms and services in terms of their real or potential ability to counter cyber risks. As a result, 8 categories of IT solutions were formed according to the same analytical procedure.

8
categories of IT solutions

Second stage

The second stage was also based on the methodology of aggregated expert assessments. The purpose of the stage is to sort 23 cyber risks according to their degree of danger and the effectiveness of technological measures to protect children from a specific risk.

24 experts specializing in the field of Internet research (sociologists, psychologists and educators), cybersecurity and IT were selected to participate in the work. Each expert was offered materials, i.e. “data sheet cards” of cyber risks and protective IT solutions. In addition, an online seminar was held with a presentation of the results of the first stage of the study, analysis of cyber risks and tasks for expert work.

>> EACH EXPERT WAS ASKED TO EVALUATE ON A 10-POINT SCALE THE FOLLOWING COMPONENTS:

the “degree of danger” of each risk, i.e. the severity of the consequences for the psychological and physical health of the child, the impact on social well-being, and the complexity of rehabilitation.

the risk is not dangerous

the risk has a critical level of danger

“Technology effectiveness” of protection, i.e. how well the available technologies protect the child from a specific cyber risk.

there is no protection / technologies are not effective / technologies are absent

existing technologies completely protect against risk

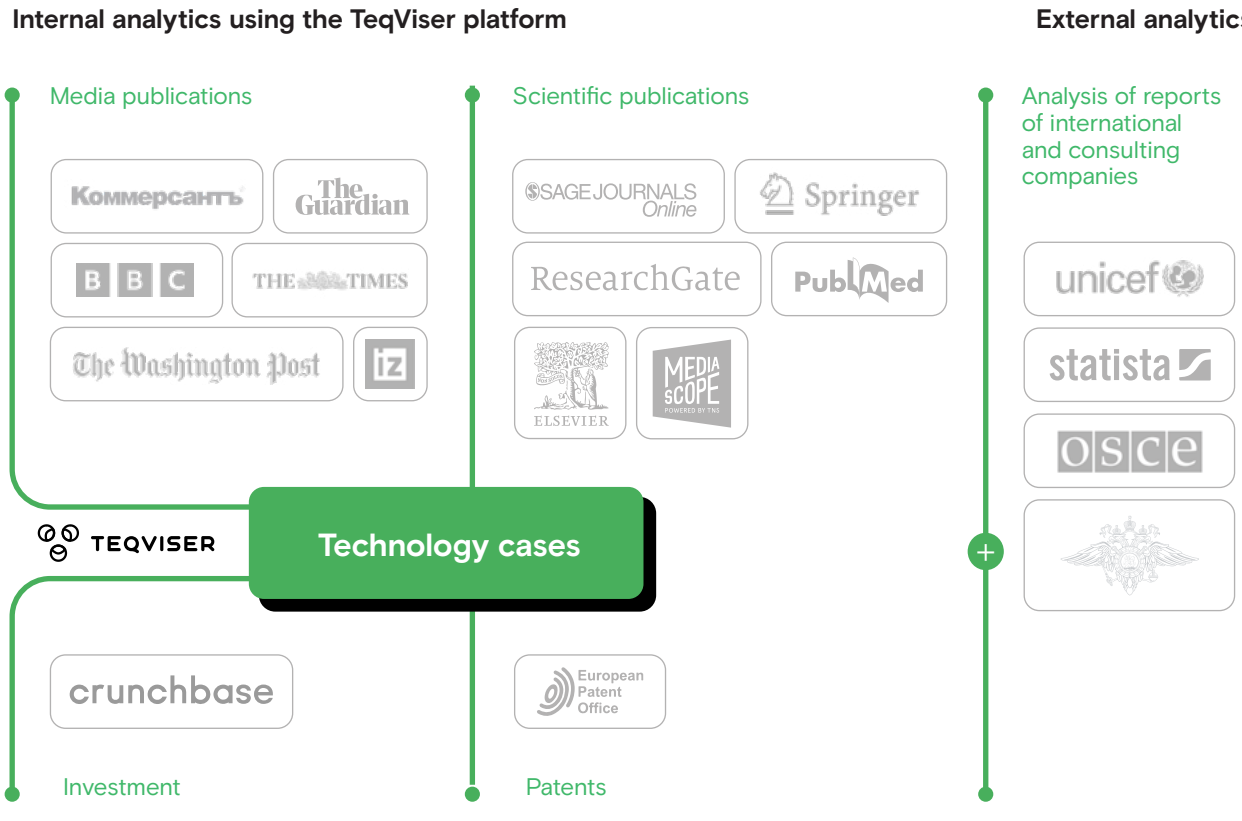
The estimates obtained for each of the risks and for each technology were analyzed for convergence. Various variants of average estimates (arithmetic mean, median), as well as statistical variation were evaluated.

As a result, cases of bimodal distribution were identified. This mainly concerned the evaluation of the effectiveness of information technology. The bimodal distribution indicates a significant difference of opinion, for example, some experts attributed a certain technology with a high ability to protect against risks, and some, on the contrary, attributed lower ratings.

After completing the procedure, we asked some experts to comment on their grading logic. The arguments and comments are systematized in the report on the results of the study.

The peculiarity of this study is the use of artificial intelligence (machine learning) in its basis, as well as the prevalence of methods of automatic quantitative analysis in order to ensure the reliability of the results. The presented information and conclusions were obtained using an intelligent analytical system for identifying new markets, promising technologies and methods of their use by TeqViser.

TeqViser is a tool for objective and timely decision-making, which can significantly complement the traditional methods of assessing the economic prospects of innovative developments and technological startups. Digital technologies have not only significantly expanded the sample under study, but also significantly reduced the processing time of the initial data, presenting results and recommendations for managerial decision-making. The study is based on the analysis of primary sources, mainly textual English-speaking. Structured data are obtained from the obtained arrays using machine linguistic analysis, as well as analysis of the frequency of mentions of a particular direction of technological development and its scope of application.



The data sources for the research are databases accumulated over several years that allow for analyzing trends at different stages of the life cycle, from solving fundamental scientific problems to the practical application of technologies in market products and solutions. Primary evidence of technology development not interpreted by experts was selected as the initial data.

Common base TeqViser

1.2 million
media publications

608 000
investments

32 million
patents

64 million
scientific publications

Risks on the Internet

53 000
media publications

2 200
investments

32 000
patents

109 000
scientific publications

Risks for children on the Internet

13 000
media publications

120
investments

1 000
patents

22 000
scientific publications

Manual analysis

500+
of scientific articles

200
patents and solutions

100
IT companies

About the authors

>> **BORIS GLAZKOV**

Vice President for Strategic Initiatives, Rostelecom PJSC

>> **PAVEL KRASOVSKY**

Deputy Director of the Center for Strategic Innovations, Rostelecom PJSC

>> **RUSLAN YUSUFOV**

Managing Partner, MINDSMITH

>> **MAXIM KONDRATIEV**

Analyst, MINDSMITH

>> **ANASTASIA TETERKINA**

Analyst, MINDSMITH

>> **NATALIA KUROVSKAYA**

Analyst, MINDSMITH

>> **DARIA VORONINA**

Senior Analyst, MINDSMITH

>> **IVAN KLIMOV**

MINDSMITH expert, Associate Professor at the Faculty of Social Sciences, Senior Researcher at the HSE International Laboratory of Applied Network Analysis

>> **SERGEY DAVYDOV**

MINDSMITH expert, Associate Professor of the HSE Department of Sociology

>> **DANIIL SHCHERBAKOV**

Junior Analyst, MINDSMITH

>> **OUR ACKNOWLEDGEMENTS**

Alexey Gusev
Anastasia Starkova
Artem Kalashnikov
Victor Ivanovsky
Denis Batrankov
Dmitry Manannikov
Ekaterina Legostaeva
Elizabeth Parshina
Kristina Raguzova
Maria Zelenova
Natalia Feldman
Natalia Lezina
Natalia Khilimonchik
Oksana Demyanenko
Oksana Razumova
Olga Zhuravskaya
Olga Ignatchenko
Roman Shapiro
Rustem Khayretdinov
Semyon Rozhkov
Sergey Bashuk
Yuliana Chepurnaya

ALLIANCE
FOR THE PROTECTION
OF CHILDREN IN THE
DIGITAL ENVIRONMENT

The Alliance for the Protection of Children in the Digital Environment is the first industrial association in Russia aimed at creating a friendly, comfortable and safe digital environment for children, which is capable of fully unlocking the creative potential of a new generation. The Alliance was founded on September 1, 2021 by nine of Russia's largest IT and communications companies, namely, VimpelCom, Gazprom-Media Holding, Kaspersky Lab, MegaFon, MTS, VK (formerly Mail.ru Group), National Media Group, Rostelecom, and Yandex.

The members of the Alliance have made voluntary commitments designed to improve the digital literacy of children, parents and teachers, develop children's skills of responsible and safe behavior on the Internet, demonstrate to them the possibilities of creative use of digital technologies, form and promote positive and educational content, develop new approaches to protect children on the Internet, create the necessary information and technological solutions to protect personal data, as well as proactively identify and remove content that may harm the health and development of children.

An important area of the Alliance's work is a constant dialogue with the state and international organizations to unite efforts to protect children in the digital world. The Alliance intends to become the leader of global cooperation in the field of child protection in the online environment and promote Russian initiatives and approaches of civil society institutions, technology and media companies on international platforms.

Detailed information about the Alliance and its activities is available on the website: https://internetforkids.ru

“Technologies for protecting children on the Internet”

Rostelecom PJSC, address:
30, Goncharnaya str., bld. 1,
115172, Moscow

E-mail: rostelecom@rt.ru
Media address: pr@rt.ru

Tel.: +7(499) 999-82-83
Fax: +7(499) 999-82-22