MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA: KEY INFORMATION

2024

AI-generated cover page

OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA: KEY INFORMATION

2024

MINISTRY OF
NATIONAL DEFENCE
OF THE REPUBLIC
OF LITHUANIA

01
Foreword

Dovilė Šakalienė,

Minister of National Defence

The events of recent years have served us as a reminder that stability and peace are not a given. Geopolitical tensions, cyber and hybrid attacks sponsored by hostile states, espionage, breaches of submarine infrastructure in the Baltic Sea, manipulation of information – this is our reality. In addition to conventional weapons, hostile states, criminals and other malicious actors have been increasingly using the latest technologies such as artificial intelligence, social engineering, disinformation and propaganda. These tools aim to disrupt critical infrastructure, disrupt essential services, undermine trust in institutions, divide societies and create insecurity.

Being capable of protecting oneself against physical as well as invisible cyber threats is an integral part of national security today. As hostile states have increasingly launched cyberattacks, our national cyber resilience is becoming a necessity rather than a choice.

In 2024, Lithuania faced a surge in cyber incidents. However, according to the National Cyber Security Centre, this increase was driven not by a rise in actual threats, but by growing public awareness. We experienced attacks by foreign-sponsored groups, yet more than half of the cyber incidents registered in Lithuania were due to the ability of malicious actors to manipulate people's credulity. The Lithuanian Police noted the same: cybercrime is dominated by cyber fraud. The State Data Protection Inspectorate has pointed out that in 2024, the number of subjects affected in Lithuania as a result of cyber incidents increased significantly. These facts show that cyber-attacks against Lithuania, as well as other democracies, are not only evolving, but also becoming more frequent. The lack of consideration of cybersecurity by entities involved in the supply chain is also a major challenge to national security. A negligent approach by service providers leaves the way open for our adversaries to infiltrate and potentially breach the systems of organisations that are critical to our country.

In response to these threats, the Ministry of National Defence has developed a targeted cybersecurity policy aimed at ensuring that Lithuania is resilient and prepared for any threat in cyberspace. In 2024, the updated Law on Cybersecurity came into effect, transposing the EU Network and Information Systems Directive (NIS 2) into national law. Lithuania is one of four European Union countries that transposed this directive on time. This means that organisations know what to do, and the state has the means to coordinate and evaluate actions.

The European Union is advancing other initiatives to strengthen the cyber resilience of critical sectors in Member States, and we, as the Ministry of National Defence, together with other Lithuanian institutions, are working to ensure that national interests are properly conveyed and that national decisions are taken in a timely manner. Some of the most important decisions for the near future are the transition to post-quantum cryptography and the establishment of commitments by Lithuanian authorities to ensure the cybersecurity requirements for digital products.

In 2024, Lithuania also took steps to increase its contribution to NATO's collective security and cyber response capabilities by establishing the Cyber Defence Command.

Cybersecurity is a joint effort. I would like to express my sincere gratitude to the Lithuanian institutions, which contributed to the preparation of this report and for their professionalism, reliability, and responsibility in building a Lithuania that is capable of protecting its people, organisations and values, both in the physical and cyber space. This includes not only improving technical solutions, but also improving the preparedness of institutions, promoting public awareness and the ability to act together. We encourage continued efforts in this direction.

02

Essential Tasks, Trends and Statistics

1. Strengthening Cybersecurity: New Legislation, Defence Capabilities and International Cooperation

In 2024, the Ministry of National Defence (MoD) played an important role in shaping Lithuania's cybersecurity policy and contributing to the future of cybersecurity in the European Union (EU). In 2024, all efforts were focused on the following:

- Transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), into national law;
- Establishment of the Cyber Defence Command of the Lithuanian Armed Forces;
- The implementation of the National Cyber Security Development Programme, which was approved by the Government of the Republic of Lithuania through Resolution No. 746 on 20 September 2023, 'On the Approval of the National Cyber Security Development Programme of the Ministry of National Defence of the Republic of Lithuania, the Administrator of the 2023-2030 Development Programme';
- Preparing and representing national positions on EU legislative initiatives in the field of cybersecurity in the EU Council;
- Guidelines for cooperation between the United States and Lithuania in the field of cybersecurity and defence.

The MoD coordinated the transposition of the NIS 2 Directive into national law: the Law on Cybersecurity was updated, the implementing legislation was adopted, and the changes were presented to representatives of the public and private sectors at various events and in publications. Lithuania was one of the first countries to transpose the provisions of the NIS 2 Directive into its national law.

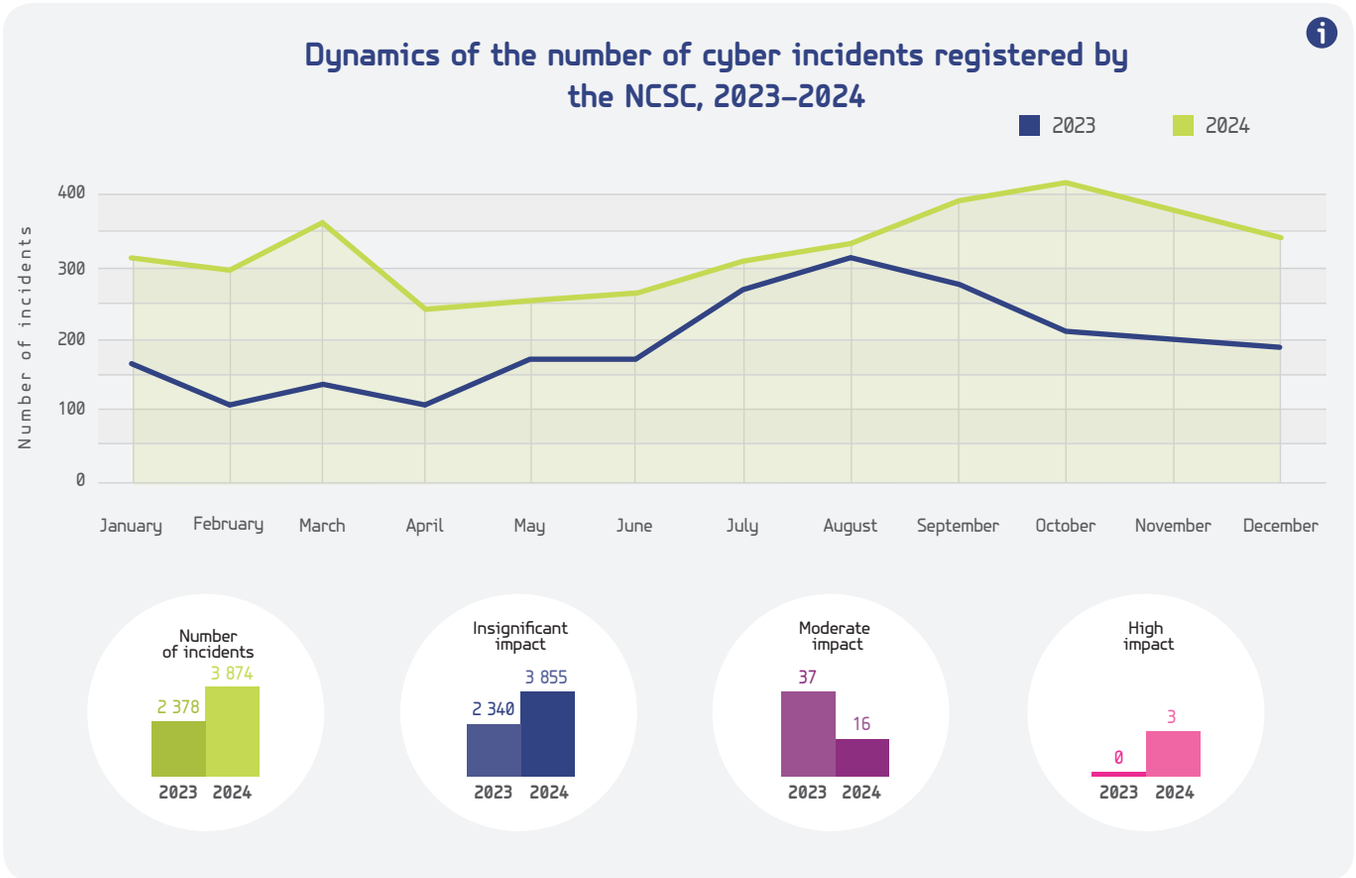
In 2024, the establishment of the Cyber Defence Command was completed, which was necessary to strengthen the Lithuanian Armed Forces' capabilities in cyberspace, to protect communications and information systems (CIS) and to ensure their interoperability with NATO. The Cyber Defence Command launched its activities on 1 January 2025.

At the end of 2024, the MoD, together with other state institutions, put into effect the measures to increase Lithuania's cyber resilience: strengthening cybersecurity governance, developing capabilities for monitoring and responding to cyber incidents, training specialists, developing research infrastructure and strengthening public resilience to cyber threats.

The MoD prepared Lithuania's positions and represented the country's interests in negotiations on new EU acts on cyber resilience, security and solidarity, joined the European Commission's Post-Quantum Cryptography Expert Working Group, and contributed to the development of EU cyber defence initiatives.

2. In 2024, the National Cyber Security Centre under the Ministry of National Defence (NCSC) recorded 63% more cyber incidents than in 2023. However, this change is related not to an increased threat, but to a growing public awareness and understanding of the need to report cyber incidents.

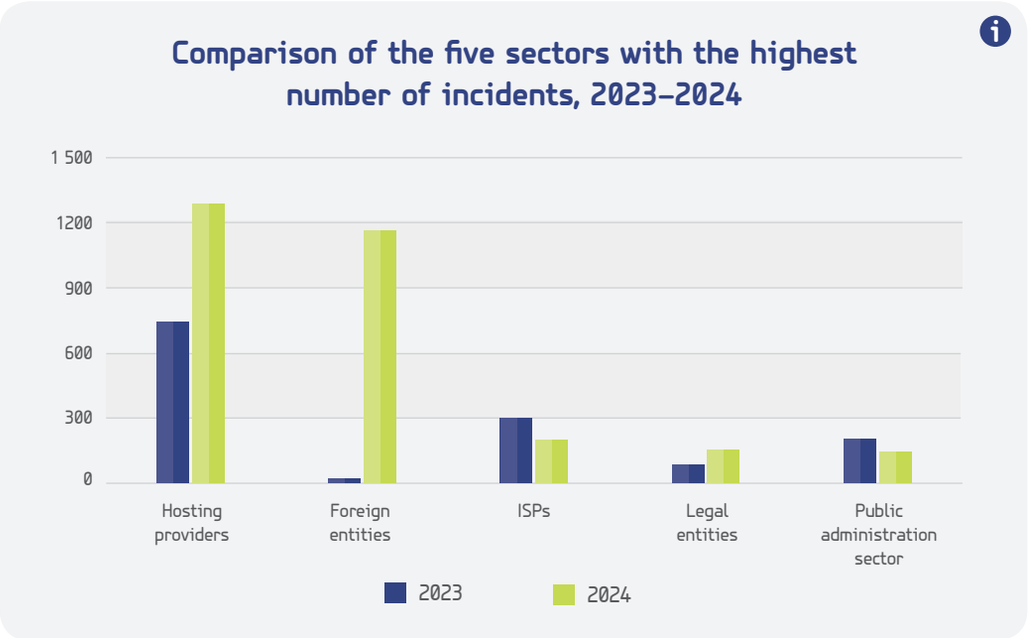
In 2024, the NCSC recorded as many as 3,874 cyber incidents, which is about 63% more than in the previous year (2,378 in 2023). Most of them were classified as insignificant or moderate, while three cyber incidents were rated as serious, (no such incidents were recorded in 2023).



^ Fig. 1
Dynamics of the number of cyber incidents registered by the NCSC, 2023–2024
(Source: NCSC)

The latter category of incidents is associated with foreign-backed groups that hack into organisations' networks to achieve long-term goals, one of which is espionage. According to the NCSC, although the dynamics of the number of incidents recorded in 2024 is mainly related to improving public awareness of cyber incidents, the use of malicious social engineering methods to extract sensitive information remains the main cause of cyber incidents in Lithuania. It should be noted that in 2024, incidents of this type accounted for as much as 59% of all incidents registered by the NCSC (38% in 2023).

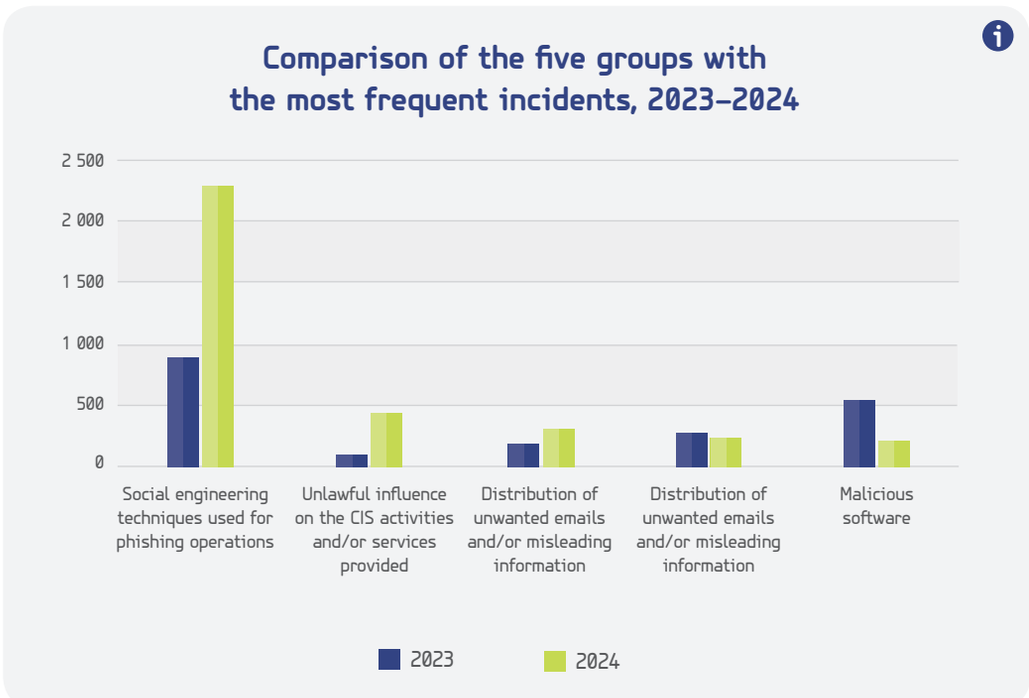
Most incidents occurred in the internet-hosting infrastructure, the foreign entities sector and the infrastructure of internet service providers (ISP). In both 2023 and 2024, the Internet hosting services infrastructure continued to lead in terms of the number of incidents recorded.



< Fig. 2

Comparison of the five sectors with the highest number of incidents, 2023–2024
(Source: NCSC)

This sector saw a particularly rapid increase in the number of incidents, with a rise of 74%. The incidents that caused the most damage to organisations and residents were those classified as social engineering, followed by a rapid increase in unlawful influence on CIS activities and/or services provided (116 in 2023; 444 in 2024), followed by the distribution of unwanted emails and/or misleading information (200 in 2023; 318 in 2024). For many years, incidents related to the distribution of malicious software were among the most frequent cyber incidents, but in 2024 they ranked fifth (554 in 2023; 223 in 2024).



< Fig. 3

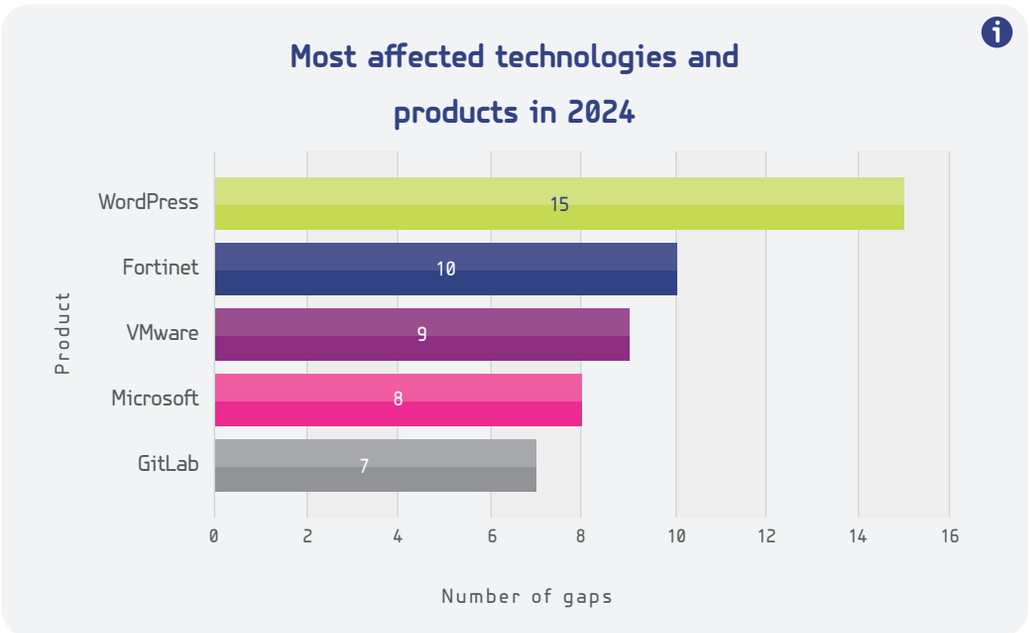
Comparison of the five groups with the most frequent incidents, 2023–2024
(Source: NCSC)

The number of leaked login credentials in countries around the world, including Lithuania, has risen sharply in recent years and has been raising concerns. This is largely due to cyberattacks, network and information system vulnerabilities (hereinafter referred to as 'vulnerabilities') and reusing passwords on different platforms.

The growing vulnerabilities posed a threat to both public authorities and institutions and private sector organisations; nevertheless, reports of gaps detected by entities under the responsible disclosure procedure (hereinafter referred to as 'responsible disclosure') help to prevent cyber threats.

In 2024, compared to 2023, the number of potentially vulnerable information systems identified increased more than threefold (1,963 in 2023 and 6,700 in 2024). The greatest risk was posed by vulnerabilities in products widely used by Lithuanian public and private sector organisations, such as Fortinet, Palo Alto Networks, Cisco, VMware, and network infrastructure.

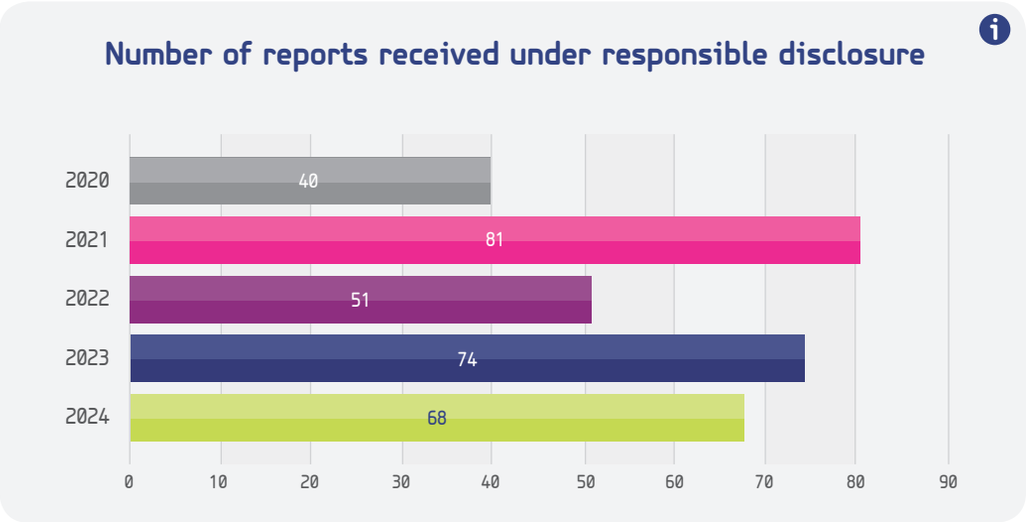
Fig. 4 >
Most affected technologies and products in 2024
(Source: NCSC)



The NCSC also paid considerable attention to vulnerabilities related to plugins for the WordPress content management system, which often become targets for hackers due to insufficient protection and untimely updates.

The NCSC notes that hackers are increasingly targeting vulnerabilities in the information technology (IT) supply chain, as they can reach more victims through service providers. In 2024, the NCSC prevented some of these threats by informing service providers and their customers about the identified vulnerabilities. However, the danger of supply chain attacks is further increased by the fact that they can remain undetected for a long time and often only data theft, disruption of the organisation's activities, and financial losses allow the organisation to understand the nature of the incident.

In 2024, the NCSC received 68 reports of detected vulnerabilities under responsible disclosure (74 in 2023) in both private and public sector organisations. This allowed the affected organisations to be informed in a timely manner and gave the opportunity to fix the vulnerabilities before they could be exploited by cybercriminals.



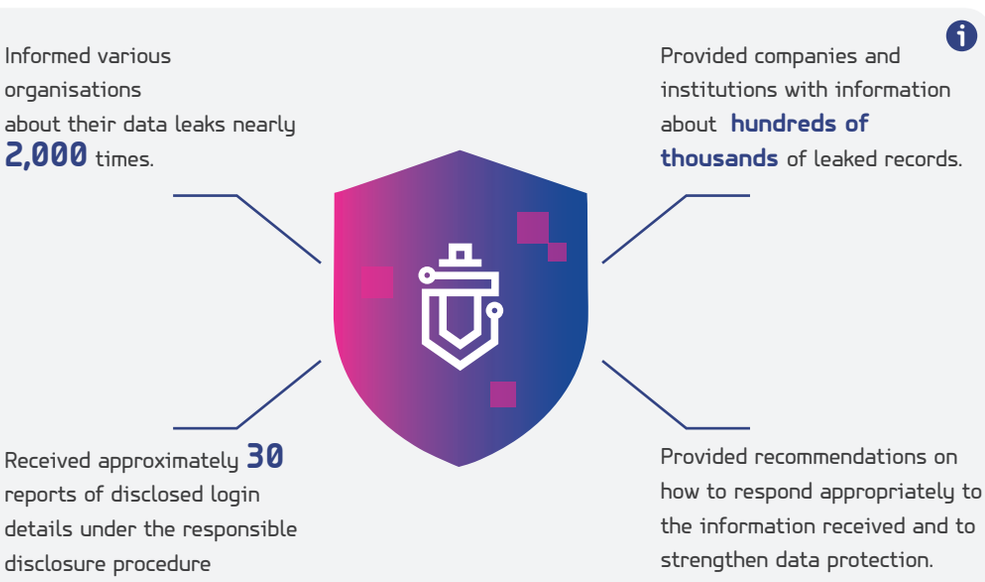
< Fig. 5
Number of reports received under responsible disclosure (2020–2024)
(Source: NKSC)

The NCSC, in cooperation with other private and public sector organisations, strengthened national cyber threat analysis and prevention.

To combat flash cyber fraud attacks, in 2024, the NCSC continued to improve Vasaris, a domain-blocking tool designed to protect organisations and residents. At the end of 2024, this tool was used by almost 2.4 million mobile and 725,000 fixed internet service users. It protected an average of 35,500 residents every day. Nine Lithuanian state institutions and agencies also use this tool.

In 2024, the NCSC actively supported the Central Electoral Commission of the Republic of Lithuania in preparing for and conducting elections. In June 2024, during the European Parliament elections, the NCSC specialists were assisted by members of the Cyber Rapid Response Team (CRRT) in ensuring the security of Lithuania's cyber space.

In 2024, the NCSC began actively searching for leaked data in order to identify threats in a timely manner and inform the affected organisations: it informed various organisations about their leaked data 2,000 times and provided companies and institutions with information about hundreds of thousands of leaked records, etc. This enabled the NCSC to respond to cyber incidents more quickly, reduce damage and strengthen the country's overall cyber resilience.



In 2024, the NCSC created a free distance-learning platform for both residents and organisations. Over the course of a year, more than 46,000 people successfully completed various courses. The content of the training courses, which are conveniently accessible online, is tailored to different groups of society, including employees, teachers, students, etc. The courses include topics such as 'Cyber Hygiene at Home,' 'Cybersecurity for Students,' 'Cybersecurity for Teachers,' etc.

In 2024, the NCSC continued to organise national cybersecurity exercises, improved their scenarios and implementation methods, which allowed public sector and critical infrastructure operators to test their employees' resilience to social engineering attacks and the organisation's ability to identify, manage and communicate cyber incidents. During the Cyber Shield PhishEx 2024 exercise, 280,000 simulated emails were sent, replicating the most common tactics used by hackers, while the largest national cybersecurity exercise, Cyber Shield OpEx 2024, was conducted live for the first time in a virtual cyber training ground. 75 organisations participated in these exercises, 39 of which improved their public communication skills by learning how to effectively inform the public about incidents.

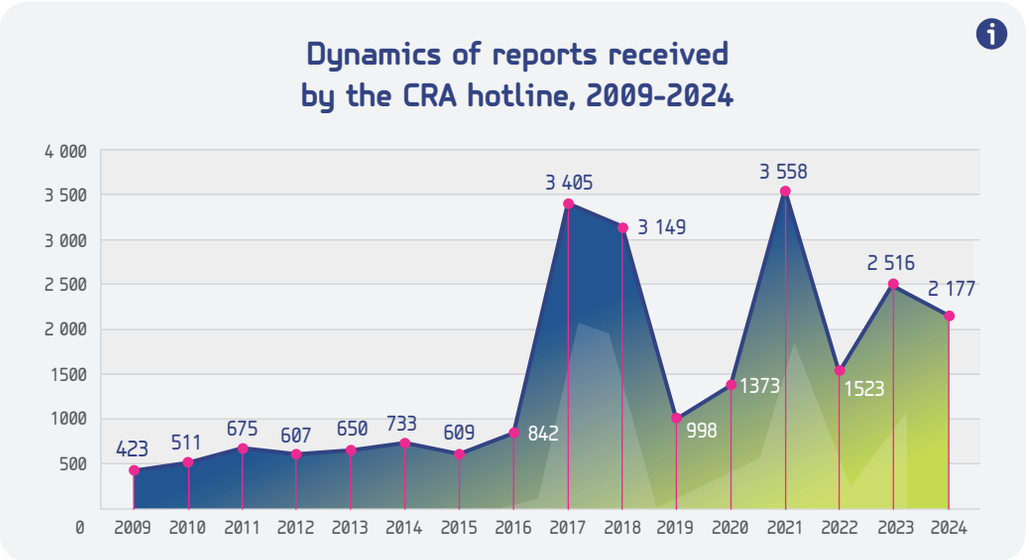
RRT

3. The measures established by the Communications Regulatory Authority (CRA) to prevent fraud via short text messages (SMS) and calls, as well as the removal of harmful content from the internet, had a significant and positive impact on the security of cyberspace and the protection of children and minors online.

In the CRA's view, disruptions and failures of public mobile and public fixed networks were dealt with swiftly in 2024, but the storm in July caused significant difficulties for public mobile networks, with providers facing a lack of human resources and a shortage of back-up power supplies to deal with network faults. The scale of the disruption prompted an accelerated update of the Public Communications Network Integrity Rules, adopted by a resolution of the CRA Council, in order to make networks more resilient in the event of emergencies and to reduce the scale of potential disruptions.

In November 2024, a maritime communication cable linking Lithuania and Sweden was severed in the Baltic Sea. The CRA, together with other authorities, investigated this incident, as well as recorded and investigated cases of disruptions to the Global Positioning System (GPS) of aircraft and illegal transmissions from Russia. The CRA found that the GPS disturbances were caused by communication jammers operating on the territory of Russia and Belarus, and referred the cases of GPS tampering to the International Telecommunication Union (ITU). Such security incidents are complex and require cooperation between the responsible Lithuanian authorities, a unified EU approach and a coordinated joint response.

Major efforts have been made to protect consumers, especially children and minors, from harmful content online. In 2024, the CRA, which is a member of INHOPE, the Association of Internet Hotline Providers, received 2,177 reports via the internet hotline (www.švarusinternetas.lt) of information found on the internet that may be prohibited or may adversely affect minors, a decrease compared to 2023 (2, 516). The number of confirmed reports of actionable prohibited information and information adversely affecting minors was 1,488, slightly higher than in 2023 (1,475). A worrying trend is the increasing incidence of cyberbullying and cyber violence.



< Fig. 6
Dynamics of reports received by the CRA hotline, 2009–2024 (Source: CRA)

The CRA secures that all access points to public computer networks (the internet), which minors may visit and surf the internet, are equipped with mandatory information filtering measures, approved by the CRA, to filter out information which has a negative impact on the development of minors. In 2024, the CRA continued to carry out inspections in Lithuanian schools and public libraries and to provide expert advice on the choice and use of filtering tools.

The security of the Lithuanian population in cyberspace is undoubtedly affected by the obligations adopted by the CRA in 2023 for operators to detect and block fraudulent calls. To combat fraudulent SMS, in 2024, the CRA Council adopted the Description of the Procedure of Identifying Fraudulent SMS, which obliged mobile service providers to identify and prevent fraudulent text messages.

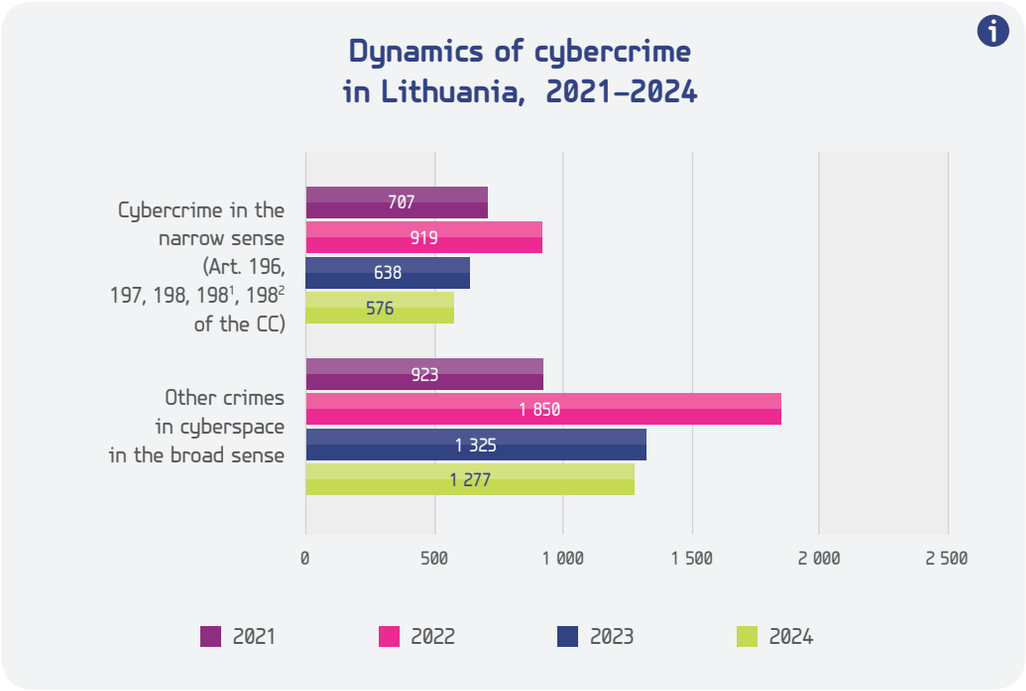
The CRA actively participates in the technical and user working groups of the EU's satellite communications project Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), as well as in other international working groups focused on connectivity and interference issues.

4. According to police data, the level of threat posed by cybercrime remained unchanged in 2024, with a particular decrease in crimes against the security of electronic data and information systems, but fraud remains a major problem.

In 2024, as many as 3,966 cybercrime offences were recorded in Lithuania. Although this number is only slightly higher than in 2023 (3,912), the threat level of these offences remained unchanged and did not affect the growth of crime registered in 2024. As last year, there was a particular decrease in the number of crimes against the security of electronic data and information systems, which are qualified under Articles 196-198² of the Criminal Code of the Republic of Lithuania (CC). For example, the number of cases of unlawful interference with electronic data, information system, unlawful access to information system decreased by almost 10%.

Fig. 7 >

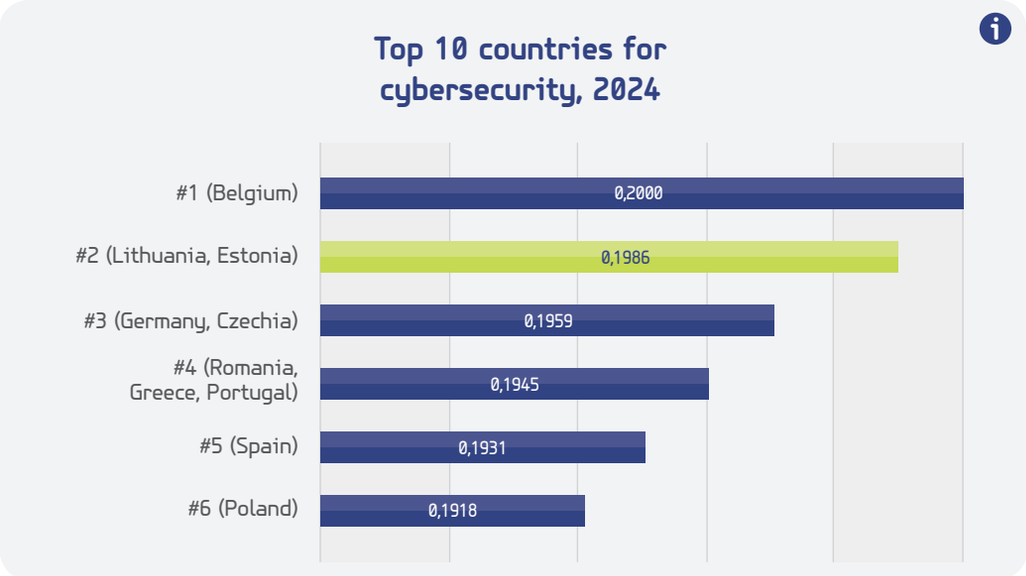
Dynamics of cybercrimes in Lithuania, 2021–2024 (Source: Lithuanian Police)



These results of the police monitoring in 2024 are in line with the findings of independent experts. Surfshark's Digital Quality of Life Index (DQL) shows that Lithuania remained the second country in the world in terms of cybersecurity in 2024, as before.

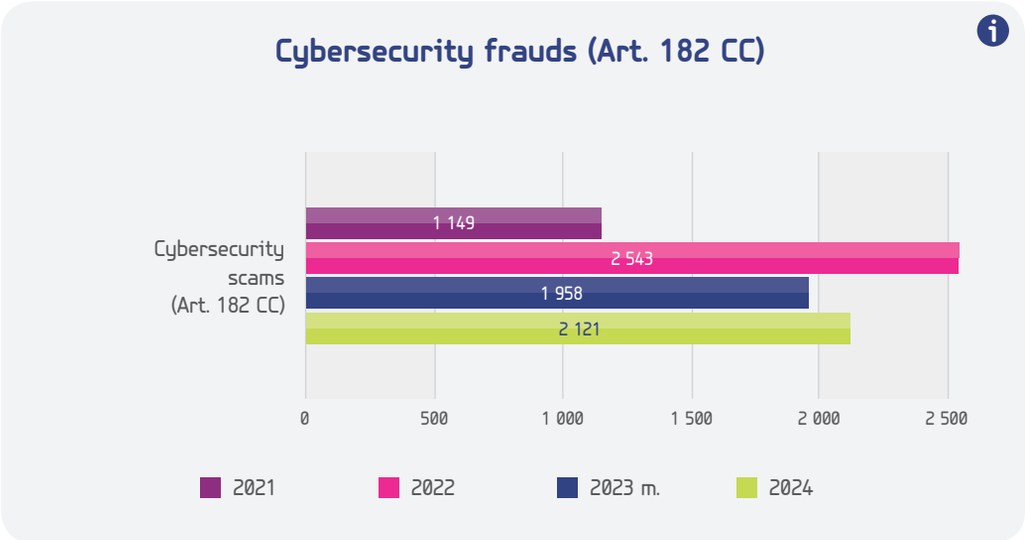
Fig. 8 >

Surfshark 2024 Digital Quality of Life Index survey results



In 2024, police agencies recorded four cases of electronic data encrypted with ransomware viruses (almost five times less than in 2023). This is the first time such a virus has been used against the Lithuanian financial sector.

Cybersecurity fraud remains a major problem. In 2024, they accounted for the vast majority – 53% – of all cybercrime: pre-paid fraud, investment fraud, fraudulent phone calls, emails and text messages.



< Fig. 9
Cybersecurity frauds (Art. 182 of the CC
(Source: Lithuanian Police)

The number of fraudulent phone calls increased by 64% in 2024 compared to 2023. The calls were aimed at extorting cash and/or valuables, and at stealing money from bank accounts by using fraudulent e-banking user data. The police assume that this may have been due to the effective control of fraudulent SMS messages, as the criminals adapted to the technical means used and returned to fraudulent calls.

The main means of extorting e-banking data and/or provoking the confirmation of a fraudulent financial transaction remained the provision of a fake website link to internet users. A new distinctive phenomenon is the connection of internet users to the fake website esveikata.lt.

According to the data of financial market participants, in 2024, fraudsters attempted to defraud €35 million from Lithuanian citizens and legal entities, but financial institutions managed to protect €17.6 million, i.e. twice as much money as last year (€7.9 million). However, in 2024, the loss to the public amounted to €17.3 million, 28% more than in 2023.

Social networks still dominate as a venue for the distribution of fraudulent adverts, for example, the number of fraudulent adverts published on Facebook in 2024 increased by 27% compared to 2023.

In 2024, cyber-attacks with the aim of disrupting state information systems and/or obtaining state and official secrets did not show any signs of systematic criminality and caused no critical damage to the national security. Among the public entities affected by cyber-attacks, the most frequent were information systems in the education, health service and cultural sectors.

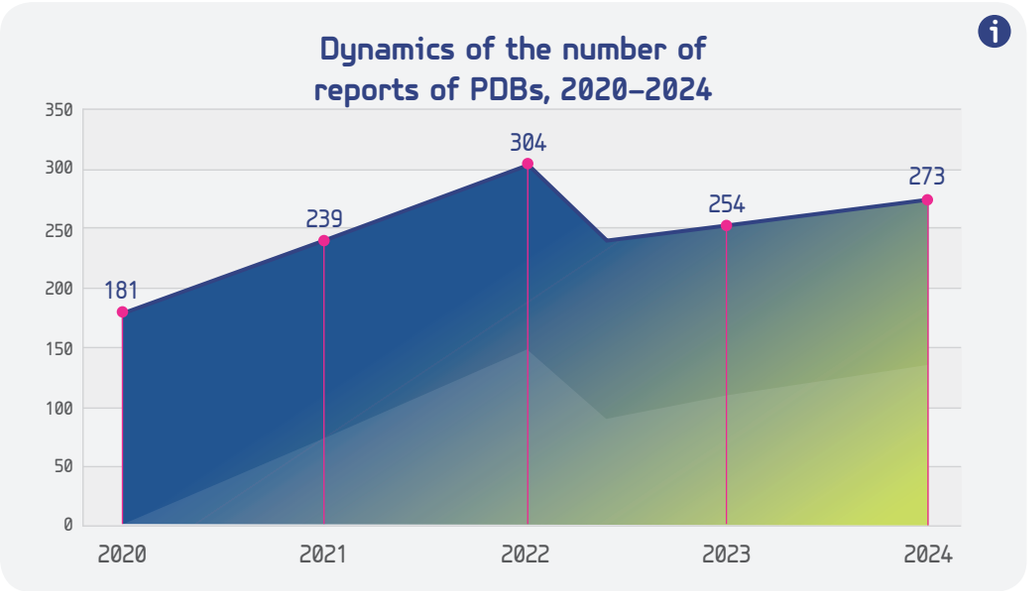
The 2024 Internet Organised Crime Threat Assessment (IOCTA) Report concludes that artificial intelligence (AI)-based technologies make social engineering even more effective. The use of deep fakes is also a concern, as it is as powerful a tool as voice replication or forgery. Research by the Lithuanian Police has not identified any increase in the use of artificial intelligence (AI) for criminal activities. However, together with other countries, they are examining the potential impact of AI on social engineering and related preventive measures.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

5. According to the State Data Protection Inspectorate (SDPI), the number of affected data subjects in Lithuania in 2024 almost tripled compared to 2023 due to the increase in the number of personal data breaches (PDB) caused by cyber incidents.

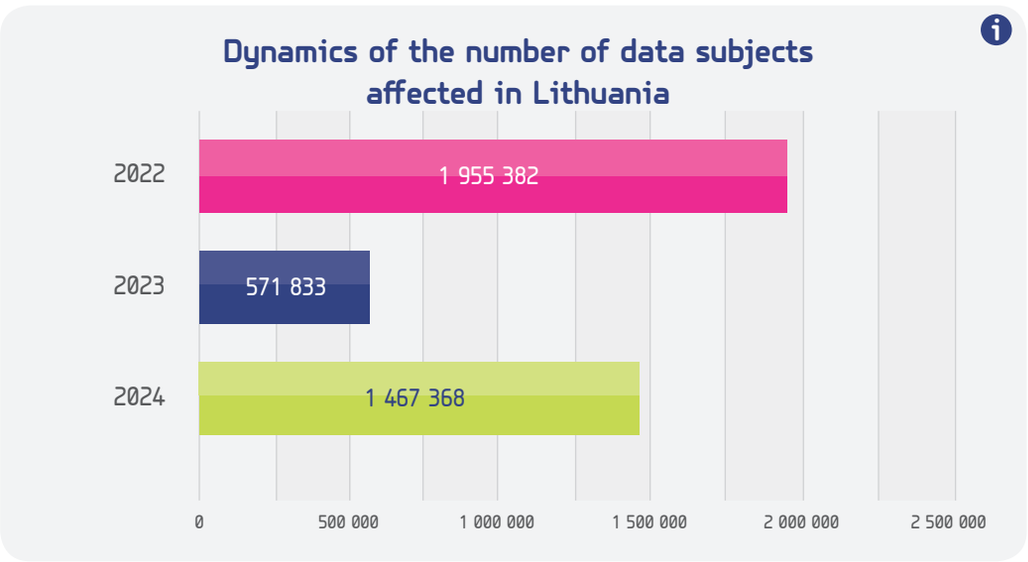
The statistics for 2024 on PDBs reported in Lithuania show that the SDPI received 273 PDBs, i.e. 7% more than in 2023 (254 in 2023). The SDPI notes that the change is not significant and therefore it cannot be assumed that the number of PDBs in Lithuania has increased.

Fig. 10 >
Dynamics of the number of reports of PDBs, 2020–2024
(Source: SDPI)



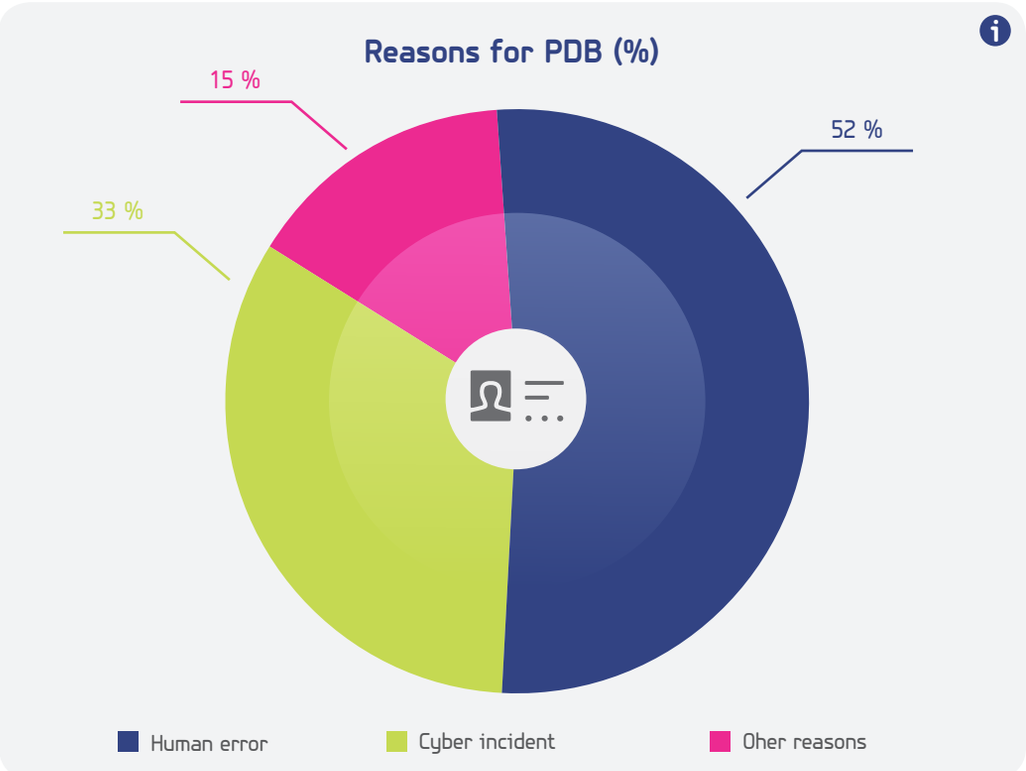
However, the number of data subjects affected in Lithuania has almost tripled, reaching 1,467,368 in 2024 (571,833 in 2023). This is due to a higher number of PDBs resulting from cyber incidents, with a large number of data subjects affected.

Fig. 11 >
Dynamics of the number of data subjects affected in Lithuania
(Source: SDPI)



In terms of the nature of PDBs, breaches of confidentiality are statistically predominant in Lithuania, accounting for 87% of all cases. This is a slight increase compared to 2023, when breaches of confidentiality accounted for 76% of all breaches.

The SDPI's analysis of PDB reports received in 2024 found that 90 (33%) of the PDBs were the result of cyber incidents, such as data encryption and ransomware attacks, unauthorised access to IT systems, attacks based on social engineering techniques, login padding cyber-attacks, and others. In



< Fig. 12
Reasons for PDB (%)
(Source: SDPI)

2023, the SDPI received only 37 PDBs as a result of cyber incidents, i.e. 15% of the total number of PDBs received in 2023. The most common causes of cyber incidents are intercepted login credentials in browsers (27%), insufficiently trained staff (18%), and lack of multi-factor authentication (10%).

One exceptional case is the imposition of impact measures on a public sector organisation. Following an investigation into the PDB and a cyber incident, the SDPI decided to impose a fine of EUR 9,000 on a public sector organisation for the breaches of the General Data Protection Regulation (EU) 2016/679. The inadequate access control and lack of authentication led to access to the institution's servers and encrypted data.

The level of Personal Data Protection Conditions (LPDPC) reflects the awareness of personal data protection among the Lithuanian population. The LPDPC is based on data from an annual representative survey of the Lithuanian population. In 2024, the LPDPC stood at 63% and actually increased by 3% since 2021.

The SDPI organised its activities in 2024 in such a way as to consistently enhance the knowledge, competence and skills of data controllers, data protection officers and data subjects in the field of personal data protection. To this end, the SDPI:

- provided a total of 4,334 daily consultations for citizens and organisations;
- actively participated in the national cybersecurity exercise Cyber Shield OpEx 2024;
- organised online training and educational events (more than 7,000 participants);
- released 25 methodological documents.

6. According to the Strategic Communication Department of the Lithuanian Armed Forces (SCD), in 2024, information activities against Lithuania were mostly influenced by Russia's continued aggression against Ukraine.

The biggest source of information threats against Lithuania and the country's strategic interests are officials of the Russian and Belarusian regimes, their political and military leadership and the regime-controlled media representatives. As the Russian military invasion of Ukraine continues, Lithuania's support to Ukraine was given special notice.

Russian disinformation is carried out in three directions: it is aimed at Western, Russian and Lithuanian audiences:

Attempts are being made to tell the West that Lithuania is not worth defending, that Lithuania is not a Western country and does not have democratic values, and is close to Russia;

Attempts are made to convince their audience that Lithuania is a hostile state to Russia, the Lithuanian army is not good enough, and that revanchist sentiments prevail in it;

The Lithuanian audience is being told that Lithuania is not worth being defended by NATO, in an attempt to weaken the public's will to defend itself.

In 2024, the usual narratives prevailed, such as NATO being an aggressive military bloc and Lithuania being a russophobic state. Hostile information actors linked to and/or controlled by the Russian or Belarusian regimes have also tried to downplay Lithuania's efforts to strengthen its defence capabilities and the significance of the deployment of the German Brigade.

In the current geopolitical situation, new narratives are worth mentioning, such as the preparation of saboteurs in Lithuania and Poland to cause a coup in Belarus and to overthrow the regime of Alexander Lukashenko, the strengthening of Lithuania's military capabilities as a preparation for an attack on Russia and Belarus, and the involvement of the NATO countries in the Kursk military operation.

In 2024, a new trend emerged—intimidation and threats in the information space. Compared to 2023, there has been an increase in the number of reports of World War III or nuclear war.

According to the assessment of the SCD, it is likely that in 2025, the information pressure will not subside, and information actors controlled or influenced by hostile states will continue to seek to discredit the Lithuanian Armed Forces and NATO and to justify their actions in the physical space by blaming the "collective West".

OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA 2024

Published by the Ministry of National Defence of the Republic of Lithuania
Totorių St. 25, LT-01121 Vilnius, www.kam.lt
27/05/2025. Order No. GL-264

Designed by Andrej Garbar
Translated by Julija Zujevaitė-Rinė
Images from Freepik.com, free graphic resources platform

Layout by the Visual Information Division of the General Affairs Department, Ministry of National Defence
Totorių St. 25, LT-01121 Vilnius

Bibliographic information of the publication is available in the National Bibliography Data Bank of the Martynas Mažvydas National Library of Lithuania.

ISSN 2783-7009