DOI: 10.46299/ISG.2023.MONO.TECH.3.2.4

2.4 Current aspects, challenges, threats and solutions of cyber security

Cybersecurity is increasingly viewed as a strategic problem of the state, which comprehensively affects the country's economy, including the interaction of national developers of software and control systems, manufacturers of equipment and components for providing ICT infrastructure, whose low market competitiveness leads to the need to use solutions from foreign manufacturers. In practice, this phenomenon leads to a rapid increase in dependence on foreign manufacturers and a decrease in the level of information protection due to the forced use of "closed" software and hardware in all segments of the infrastructure for both special government departments and the civil sector [64].

In the near future, dependence on foreign equipment manufacturers and software developers may reach a critical level. For example, despite the virtual “iron curtain” created, the Chinese authorities actually recognized complete dependence and insecurity due to the widespread use of the software platform for Android mobile devices (the platform’s share in the Chinese market in 2022 was 86,4%), based on the “open” code, but under the control of US special services. From an economic point of view, this phenomenon has a positive impact on the development of the electronics industry and the real sector, which use "open" software for the production of mobile devices, but at the same time creates a real threat to national security, transferring it under the control of foreign specialists. services.

In order for national cybersecurity to be able to match the level of leading economic powers, it is necessary, among other things, to take consistent actions on the part of the state aimed at increasing efficiency and developing the system of interaction between participants in the IT industry.

In turn, enterprises, developers and manufacturers should pay special attention to information security issues in the developed / manufactured products, placing increased requirements on the reliability and security of the proposed solutions, and only in extreme cases and if it is necessary to increase the market orientation of individual products should use the solutions of foreign vendors. and software

developers. Consider the existing threats to cybersecurity, taking into account current trends in the development of the IT industry in the world [65].

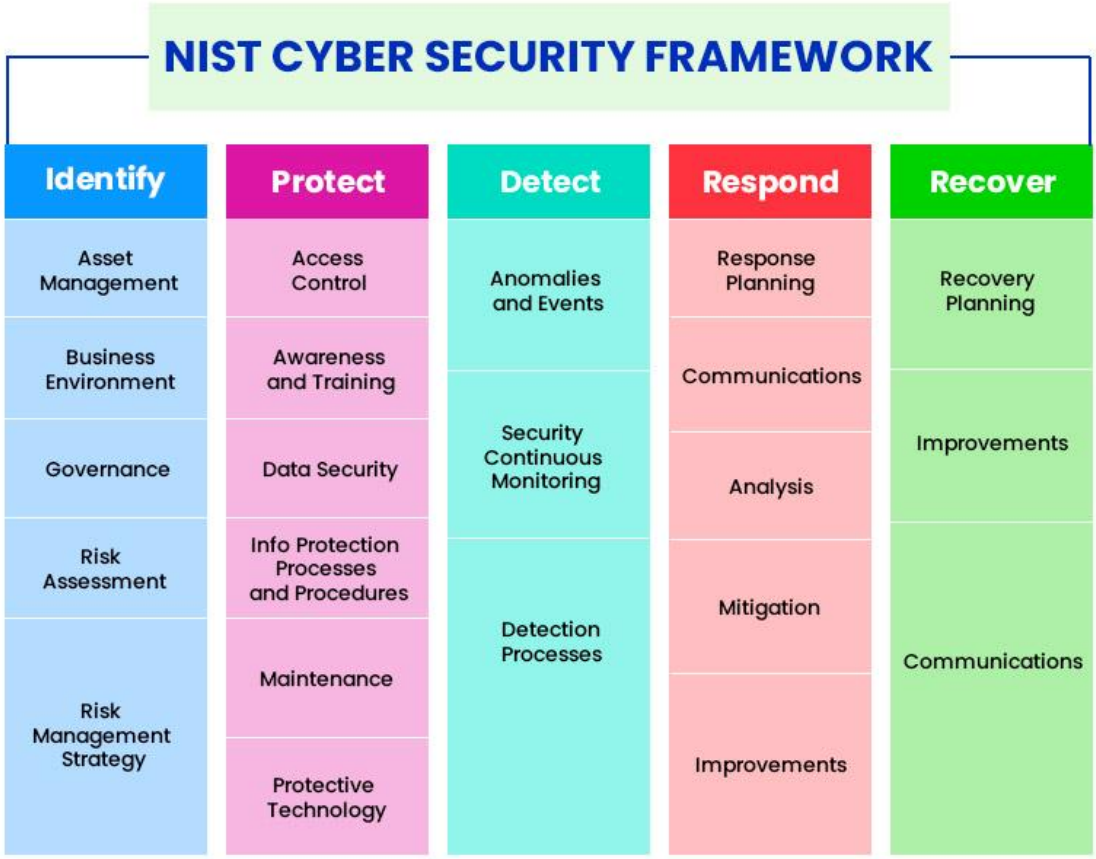
The concept of cybersecurity includes many different types of problems, and contains even more solutions. Cybersecurity is an area of active research and development in the information technology community, with participants from all parts of the IT ecosystem (Pic. 1).

Many areas of cybersecurity have common themes and issues that require an integrated approach. Pic. 2 briefly highlights some of the major cybersecurity problem areas and shows where some of these problems can be addressed with technical solutions developed by commercial organizations, standards organizations and Internet users.

In the vast majority of cases, the most successful attacks by hackers, criminals, and other intruders target servers and end-user computers connected to the Internet. Among the tools that are used to attack computers are malware, Trojan horses, botnets, phishing, distributed denial of service (DDoS) attacks, and man-in-the-middle attacks.

Securing computers, whether they be servers, desktops, laptops or smartphones, is the goal of the work of a wide variety of groups within the IT and Internet communities, and will help identify some of the big players, as well as their areas of interest.

It is important to note that the vast majority of companies are foreign developers and manufacturers, for the most part dominating the market. However, even finding a technological solution to a cybersecurity problem does not mean that the problem itself disappears – it just becomes possible to solve it. For example, end-to-end encryption using SSL/TLS algorithms is a well-known technology that can be used as a solution to many of the problems listed above. However, it has not been universally accepted. This is partly due to historical reasons and organizational inertia, as well as illiteracy or poor information. Having well-known solutions to well-known problems is of little value if those solutions are not used.



Pic. 1. Topics and areas of cybersecurity

Thus, the issues of ensuring national cybersecurity depend not only on technical methods of implementation, but, more importantly, on the availability and real demand for these solutions. If the task of ensuring information security during transmission over networks and communication channels can be solved mainly by using cryptographic information protection tools of domestic production, then ensuring communication security from destructive influences is a problem, since in view of the lack of own infrastructure, it is necessary to order the necessary services from commercial telecom operators, whose networks are deployed on imported equipment. This applies to both the fixed, mobile and satellite components. In fact, the entire unified telecommunications network is in the most severe technological dependence and for this reason cannot serve as a trusted environment and a reliable basis for the command and control system, since at any moment it can be controlled and controlled by a potential enemy. Thus, it is possible to fully and reliably solve communication security issues only when Russian telecommunications equipment is used in the

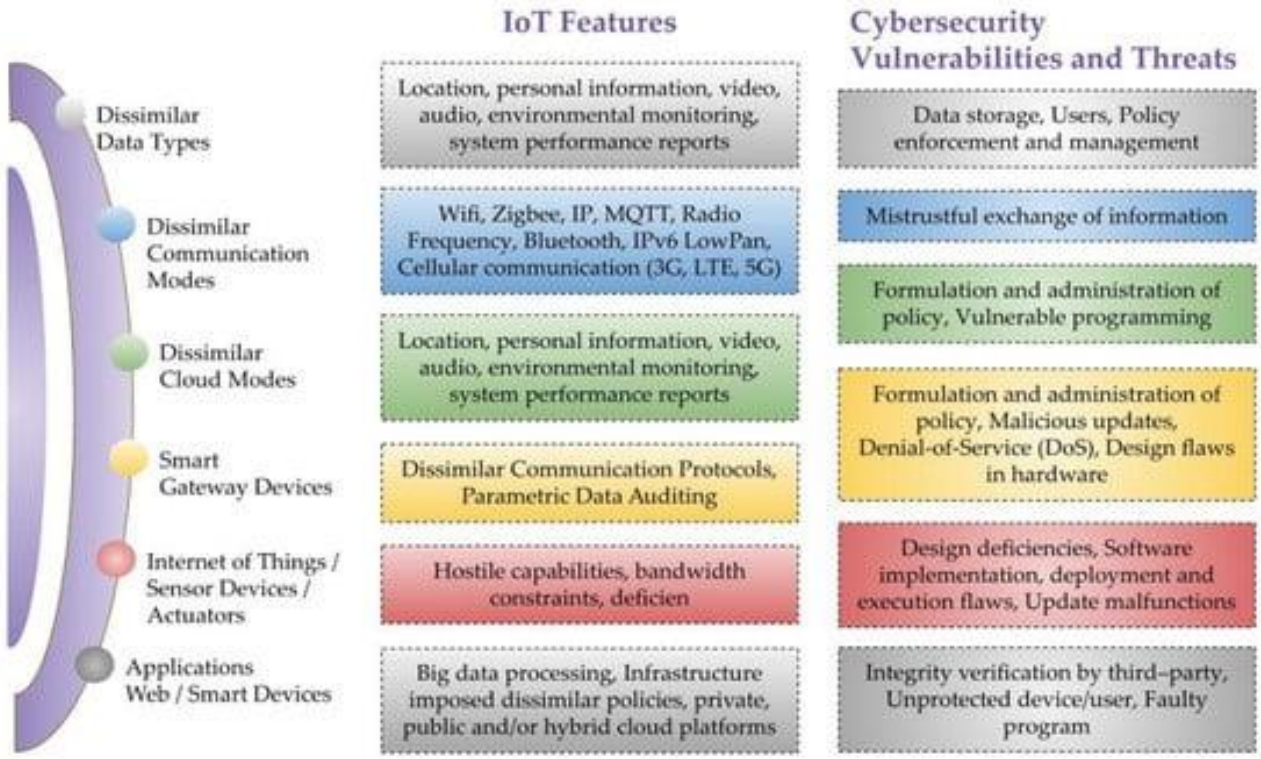
country's networks, and even better, a single dedicated network is created on its basis in the interests of public administration [66].

Pic. 2. Cyber security issues and technological solutions

Many governments in their cybersecurity development programs pay special attention to infrastructure closely related to security issues. To assess the scope of the cybersecurity problem and possible threats, it is important to understand the relationship between cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), critical information infrastructure protection (CIIP), and non-critical infrastructure (Pic 3).

While definitions may vary slightly, Critical Infrastructures (CIs) are generally considered to be key systems, services, and functions whose failure or destruction has a detrimental effect on public health and safety, business, and national security, or a combination of both. CIs are made up of both material (for example, buildings and structures) and virtual elements (for example, systems and data). Each country may have its own understanding of the term “essential”, but usually this concept can include elements of information and communication technologies (ICT) (including

telecommunications, energy, banking, transport, public health, agriculture and food, water supply, chemical industry , shipping, and essential government services).



Pic. 3. Relationship between cybersecurity and the protection of critical information infrastructure

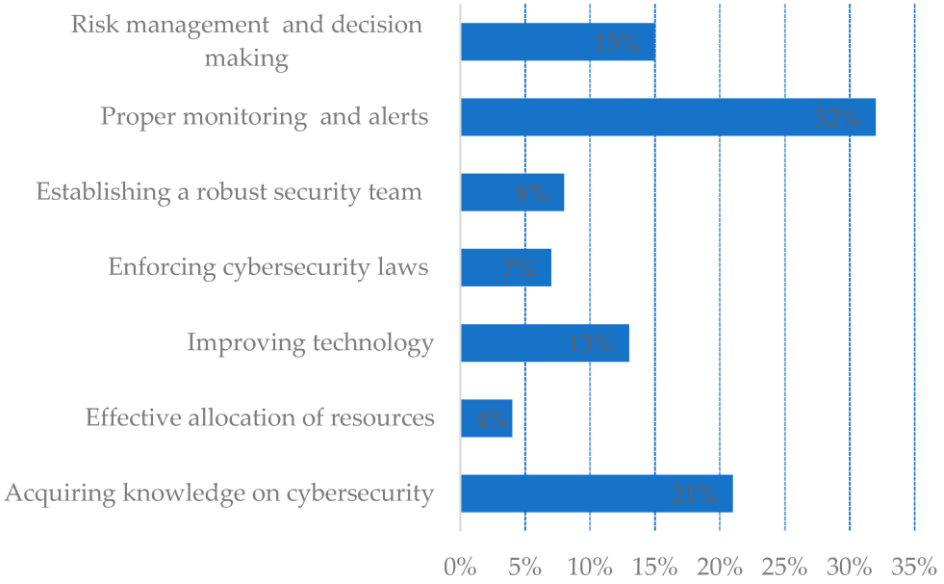
Each of these sectors of the economy has its own physical resources, such as bank buildings, power plants, trains, hospitals, and government offices. At the same time, all these important sectors of the national economy depend on information and communication technologies [67].

The key problem is that the largest consumers of such products cannot abandon the products of foreign vendors in favor of domestic solutions. At the same time, most government departments, having their own networks and incurring annual costs (including the development of telecommunications equipment and information security), purchase imported solutions. It is thanks to these trends, according to experts, that an additional market opens up for foreign manufacturers in addition to the civil one - the market for special and state purposes. An alternative solution to the problem can be the creation of a single network with a logical division of resources.

At the moment, a critical situation has developed, in which, with a high degree of probability, foreign solutions with an "unknown" stuffing. Even after carrying out special events to test and analyze the potentially dangerous properties of the solutions used, we have no reason to believe that these properties are guaranteed not to be able to manifest themselves under a certain set of conditions in the future.

The problem of engineering ownership based on solutions of foreign vendors is of a systemic nature, both in terms of ensuring cybersecurity and in terms of the current state of the Russian electronics industry. The development and production of electronics as a process, as well as the use of electronics in domestic and foreign markets (including the market for special customers), as a result, are not efficient enough, which is a complex problem for the entire industry. Along with companies that have succeeded in development, but do not promote their products to the market, there are companies that develop and promote their quite successful products, but interact only with foreign chip vendors. Why is this happening?

When creating a competitive product, business tasks are the main ones, while the question of the development of electronics at the industry level remains outside the brackets. Thus, the business refuses to use an expensive and uncompetitive Russian-made chip, since the use of such a "raw" chip carries huge risks for the business. Therefore, to create consumer electronics, as a rule, imported chips are chosen at the stage of technical design. The problem of the lack of interaction between chip vendors and electronics developers is a systemic one. On the one hand, barriers are built by electronics developers - even if chip designers have developed a good microcircuit, its use is blocked by their colleagues - electronics design engineers - under any formal pretext. On the other hand, barriers are created by chip designers who are not market-oriented enough. Often they create chips only for reporting on R&D, it is impossible to make a competitive product on their basis (Pic. 4).



Pic. 4. Aspects of cybersecurity

Today there is a situation where R&D to create a product that guarantees compliance with cybersecurity requirements, it is impossible to get a result by interacting only with enterprises.

The world-famous outsourcing production model can be chosen as a solution, according to which the development and launch of demanded products on the market is possible only if there is close cooperation with foreign and domestic companies. This allows at the design stage to form the concept of a new product, presenting it with the modern requirements demanded by the market and transfer to third-party specialized manufacturers the types of work that are not core for the enterprise. For example, activities such as organization of device circuitry, production of electronic components, industrial batch production of devices, technical support and distribution can be transferred to specialized enterprises in the industry. This model allows, with maximum economic efficiency, to ensure the development and launch of solutions to the market according to world production standards in a time-limited production cycle.

If we consider the business model of interaction through an outsourcing model, then we can distinguish three main levels:

1. Semiconductor market, creation of a component base, processors.

2. Electronics market, development and production of electronics.

3. Consumer market, distributors.

The above scheme forms a common understanding of how the division of markets into levels is now taking place, and how the scheme of cooperation is built in world practice when creating products in the field of electronics.

By narrowing the scope of activities, companies are increasingly concentrating on their priority areas and gaining technological advantages in them, allowing them to significantly increase their share in the selected market segment. The division into levels is due to a number of economic factors and the rapidly growing technological complexity of each individual area. It turns out that it is often more expedient to concentrate certain competencies within one enterprise than to build a vertically integrated company responsible for the full cycle.

Such delimitation of areas of responsibility makes it possible to ensure the economic effect of the development of new products and the cyclical nature of production in a constantly changing market, allows the electronics industry to develop dynamically, but at the same time, each of the enterprises is dependent on other participants in cooperation. For the development of domestic production of certified high-tech products of radio electronics and world-class software for the market of special customers, it is necessary to introduce an outsourcing model into the system of interaction between domestic manufacturers and developers within the industry.

Thus, a systematic approach to cybersecurity issues at the state level includes not only raising awareness of the existence of risks in cyberspace, creating national structures dealing with cybersecurity issues, but also establishing the necessary relationships between various groups of participants, including between sectors of the economy, to development of an outsourcing model of production. A comprehensive cybersecurity program backed by systemic R&D planning will, on the one hand, help protect the country's economy from disruption by promoting business continuity planning in various sectors and protecting information stored in information systems, and, on the other hand, help stimulate production and marketing for domestic infocommunication enterprises, thereby reducing the country's dependence on foreign manufacturers and developers and supplying civilian and special markets with completely safe and modern world-class solutions [68].