7.2 Communication networks of the fifth generation forced to reconsider ideas about data security, the principles of managing them and ensuring control over the operation of connected devices. With the advent of 5G services, new attack vectors have emerged and attackers have new targets

5G mobile communication networks are already operating or being launched in all developed countries. In October 2019, Huawei alone received more than fifty contracts for the installation of 5G equipment in 30 countries, and ZTE Corporation signed 35 contracts. At the same time, the features of 5G technology from the point of view of security have not yet been fully studied, which gives rise to problems with trust in such networks. As a result, a number of governments have chosen to take a conservative, prudent approach to 5G deployment, and many organizations, given the novelty of 5G, are actively interested in the security of these networks. The EU report noted that the deployment of 5G could lead to situations where hostile states take control of critical infrastructures: power grids, hydrocarbon processing plants, transport systems, pipelines, unmanned vehicles, police communications systems, household appliances, etc. As a result, no trust in 5G equipment vendors from certain countries. According to another report, governments can require such vendors to help launch cyberattacks on behalf of their countries.

5G security

5G networks have built-in security features. In particular, virtualization allows you to minimize the use of physical equipment to manage the network and perform network functions on them. The same feature allows you to minimize cyber-attacks. With the help of authentication systems, 5G operators can identify various devices: smartphones, sensors, household appliances and send security updates to them. In addition, application vendors are developing systems that provide end-to-end data encryption. In 2018, approximately half of the Internet traffic was encrypted, and this figure is constantly growing.

However, due to the novelty of 5G, the vulnerabilities of such networks are not yet known. Some research groups have already discovered more than a dozen weaknesses in 5G protocols that can be used by attackers to locate subscribers,

downgrade networks to 4G levels, monitor calls, messages and online activity, and perform other malicious actions. The researchers carried out attacks to downgrade subscriber devices using inexpensive software-defined radio transmitters, and they were able to obtain the IMEI number of the attacked device.

In table. 1 shows the main characteristics of 5G related to security. First, 5G networks have more bandwidth and less latency. According to Verizon, in Chicago, the maximum 5G download speed was 1.1 Gbps, while the average 4G download was between 15.3 and 28.8 Mbps, depending on the time of day. However, the disadvantage of high speed is that when a device is hacked on a 5G network, attackers will get personal data and other sensitive information much faster than in the case of 4G. They can take advantage of the low latency and high bandwidth of new types of networks to increase the scale of distributed DoS attacks. Higher speeds expand the capabilities of attackers, including in terms of using the huge amounts of data exchanged by information systems, as well as artificial intelligence complexes and IoT groupings.

In addition, 5G networks will be used by peripheral devices that perform calculations and store data not in centralized environments, but closer to their sources of creation. While these capabilities reduce costs, conserve bandwidth, and reduce network latency, they do come at the cost of reduced security. Attackers can install backdoors on mobile base stations to intercept and manipulate data at access points. In such situations, it is not easy to recognize the activity of intruders - systems may not show signs of anomalies, even when an attacker copies and changes data.

Moreover, to manage software-defined networks (Software-Defined Network, SDN) and segmentation of 5G networks (slicing, splitting into independent segments with different characteristics), artificial intelligence tools are widely used to help ensure high speed and low latency. In cases where artificial intelligence systems that are not designed to work in a 5G environment are used for this, there may be vulnerabilities in them. By compromising the SDN controller, an attacker can gain privileged access to devices running under his control, which can lead to significant damage.

Thanks to the capabilities of SDN, the 5G network can be divided into several segments optimized for different tasks. However, each segment can have its own security capabilities. For example, communication systems for emergency services may be better protected than online gaming platforms.

Table 1.

Safety features of 5G

Peculiarity	**Explanation**	**Impact on safety**
Speed and Latency	Higher speeds: If in 4G networks, the speed is up to 100 Mbps, then in 5G networks - 10 Gbps. Lower delay value: 4G - 50ms, 5G - 1-2ms.	Attackers can get data from hacked devices faster and carry out larger DDoS attacks. Crackers acquire wider technical capabilities.
Data transfer and storage	Collected data is often stored at the edge rather than centrally.	On the periphery, the level of security may be lower than in the center. Attackers are able to install backdoors on mobile base stations in order to intercept data directly at radio network access points.
Use of SDN, artificial intelligence, machine learning	SDN and artificial intelligence are used to implement the functions used by various systems and provide the desired speed and latency.	There can be gaps in artificial intelligence systems. In the event of a compromise of the SDN controller, the hacker gains access to the device controlled by him.

Continuation table 1

Network segmentation	The network cannot be divided into logical segments providing different services	Depending on the needs of users, you can flexibly change the levels of security available to them.
Connected devices	If 4G is predominantly mobile phones, then 5G is a much wider range of devices.	The attack surface may increase. Inexpensive networked devices often lack the necessary security features.
Application specifics	Highly specialized applications possible	Hacking critical systems can be disastrous. Attackers have access to more technical options.

A wide range of devices of various kinds can be connected to the 5G network: the developers of 5G standards have provided the ability to connect to networks of at least 1 million devices per square kilometer. As the number of low-cost, low-security devices on 5G networks increases, so does the attack surface. This is due to the fact that most of these devices cannot be equipped with a firewall due to insufficient memory capacity. Gartner predicts that IoT devices will grow from 14.2 billion to 25 billion between 2019 and 2021, accounting for 16% of traffic and 78% of malware. Owners of such devices may be reluctant to protect them for financial and practical reasons.

Unlike previous generation networks, 5G networks can be used for more specialized applications, including mobile medicine and autonomous vehicles. The security issues associated with such an application carry more risks.

5G, business and government

5G networks bring new architectures, business models, jobs and security gaps. To meet new requirements related to authentication, accountability and failure prevention, cybersecurity models need to be adapted.

In table. Figure 2 summarizes the findings on how organizations perceive the issue of 5G network security. Some reacted negatively to the innovation, which led to a slowdown in implementation. According to the surveys, the doubts expressed in organizations are mainly related to the specifics of 5G. In the governments of advanced countries, concern was caused by the fact that 5G equipment is supplied by Chinese companies, led by ZTE and Huawei. The United States, Australia and New Zealand have imposed bans on purchasing 5G equipment from Huawei, and Japan has banned purchases from ZTE as well.

In October 2019, the US Federal Communications Commission recommended that government contractors be banned from purchasing equipment and services from ZTE and Huawei. The regulator explained this by saying that if 5G equipment is operating, for example, near an American military base, China may require the manufacturer to install a backdoor or malware, and the US authorities will not even have the opportunity to find out.

Table 2.

A look at 5G security

Survey Initiator	**Time of publication**	**Results**
Ericsson, 5G readiness survey	2017	Representatives of various industries were interviewed, 79% of them admitted that security and privacy concerns hinder the implementation of 5G. The issue of security ranked third among the most important features of 5G services.
Osborne Clarke (international law firm)	January, 2019	Security and privacy surveys are delaying IoT and 5G adoption in the energy industry, according to 74% of respondents.

Continuation table 2

Business Performance Innovation Network together with A10 Networks	May, 2019	Among mobile device users, 84% expressed concern that the introduction of 5G will lead to a significant increase in security and reliability problems.
Reuters, survey among Japanese companies	May, 2019	88% of those surveyed would prefer to receive 5G services from national providers.
Survey conducted by Opinion Matters among CIOs and Chief Security Officers of organizations in Singapore	September, 2019	The vast majority, 98% of respondents, expressed doubts about the security of 5G networks. Among them, 55% believe that 5G will create the possibility of more destructive cybercriminal activity, and 54% believe that with the introduction of 5G, there will be greater opportunities for cyberattacks.

Since Huawei was blacklisted by the Department of Commerce, Google has been unable to provide Android services, updates, and apps to Huawei's 5G smartphones, delaying sales of Huawei Mate 5G smartphones in Europe, Huawei's second largest market after China.

Concerns about the security of cooperation with Chinese companies have also begun to be expressed in the EU countries: officials expressed concerns about the use of 5G technologies in critical infrastructure, including in traffic control systems, rail transport and household appliances. Companies like Huawei are said to be required by Chinese law to cooperate with national intelligence agencies. As a result, for example, most Japanese companies prefer to receive 5G services from local operators (Table 2), and in January 2019, the British telecommunications operator Vodafone, operating in

26 countries, decided to suspend the use of Huawei equipment in a number of European countries for security reasons.

5G networks are redefining data security, governance and control. With the advent of 5G services, new attack vectors are emerging and attackers are gaining access to more targets.

Cyber security aspects of 5G

To protect 5G networks from hacking, cybersecurity technologies need to be significantly improved. Some problems are related to the network itself, others are related to the devices connected to it. Both can be a source of risk for consumers, commercial and government organizations.

Let's consider the main problems of information security in a new generation network.

Security decentralization. Before 5G, networks had fewer physical links, making them easier to secure and maintain. More routing points are needed for dynamic 5G software-based systems. And to ensure security, each of them must be constantly checked. It may seem difficult, but even one unsecured link can undermine the security of the rest of the network components.

High throughput requires a revision of protection methods. The speed and performance of modern networks are limited, which actually makes it easier for providers to monitor the level of network security in real time. Therefore, the advantages of the extended range of the 5G network can simultaneously compromise its security. Developers will have to think about new methods to deal with modern threats.

Many IoT devices are not secure. Cybersecurity is not a priority for all manufacturers, especially for budget smart devices. 5G brings new opportunities for using the Internet of things. the more hacking options. Smart TVs, door locks, refrigerators, speakers, and even something as small as an aquarium thermometer can be a vulnerable point in your network. The lack of a security standard for IoT devices can lead to a massive increase in cybercrime.

The lack of encryption when establishing a connection opens up access to information about the device, which criminals can use to target such a device through an IoT connection. By intercepting unencrypted data, attackers will know exactly which devices are connected to the network. Knowing the type of operating system and device (smartphone, car router, etc.), attackers will be able to plan their attacks more accurately.

Device vulnerabilities are used to attack a wide variety of types. Let's list the main ones.

Botnets control network-connected devices for a massive cyberattack.

DDoS attacks overload a network or site in order to block their access to the internet.

A man-in-the-middle attack (MiTM attack) is the stealthy interception and modification of messages exchanged between two parties.

Location tracking and call interception is not a problem for those who know a little about paging protocols in broadband systems.

The Future of 5G and Information Security

To reduce the vulnerability of national mobile networks, developers will need to carefully consider the aspects of 5G security.

First of all, it is necessary to develop the principles of cybersecurity in 5G networks. Providers will have to work on software protection against the threats that we may face in the 5G network. They will have to work with IT companies to develop solutions for encryption, network monitoring and other protection tools.

Manufacturers need motivation to increase the level of protection of their products. The overall level of protection of a 5G network is determined by the level of protection of its weakest links. But the cost of developing and bringing devices to the market with an increased level of protection for manufacturers is not at all encouraging. This is especially true for budget products such as children's smartwatches and cheap baby monitors. If the benefits exceed the total costs, this motivates manufacturers to increase the security of their devices.

Consumers need to be educated about cybersecurity for IoT devices. The wide range of protection levels means that product labeling standards may be required. Because there is no way for consumers to know how secure a particular gadget is, manufacturers of smart devices may be required to label them. Federal Commission The US Communications Service is classifying other types of radio transmission and may soon include IoT devices in this classification. In addition, users need to be explained that updating software improves the security of all gadgets connected to the Internet.

Work on strengthening security is ongoing in parallel with the rollout of the first 5G networks. But we need to get real results first in order to carefully work out ways to protect, so the work will continue after the introduction of 5G.

How to Prepare for the 5G Era

The buzz around 5G networks may make it seem like the era has already arrived, but in fact, you still have time to prepare. The introduction of new technology will be a long one, although some changes are already beginning to appear. We recommend that you take care of the security and privacy of your data yourself.

Use a VPN to keep your data private and hide your browsing history.

Use strong passwords. Always use the most complex passwords. The best password is a long set of random characters of various types. Use lowercase and uppercase letters, special characters, and numbers.

Change the default administrator account passwords on all IoT devices. Follow the manufacturer's instructions to change the administrator account name and password on all gadgets. If the required information is not in the manual, contact the manufacturer directly.

Install the latest security patches on all IoT devices. Regularly update your mobile phone, computer, all smart home devices, and even your car's infotainment system - anything that connects to the internet uses Bluetooth or other communication protocols. Update applications, firmware, operating system, etc.