Good morning to everyone! My name is Polina and I want to tell you about the topic "12 data protection technologies and practices for protecting your data".

In the modern world, information plays a huge role in a person's life. Information technologies are used everywhere. Thanks to the development of technology, we can transmit messages to the other end of the city. The information transmitted in this way is called data.

The unreliability of data transmission systems forced people to start developing the field of information protection. Technologies for data storage and management have been developed.

Let's consider the most popular methods. The first slide presents technologies: data discovery, data loss prevention, storage with built-in data protection. Data discovery—a first step in data protection, this involves discovering which data sets exist in the organization, which of them are business critical and which contains sensitive data that might be subject to compliance regulations. Data loss prevention (DLP)—a set of strategies and tools that you can use to prevent data from being stolen, lost, or accidentally deleted. Storage with built-in data protection—modern storage equipment provides built-in disk clustering and redundancy.

Next, we will look at the following methods presented on the second slide:backup, snapshots, and replication. Backup—creates copies of data and stores them separately, making it possible to restore the data later in case of loss or modification. Snapshots—a snapshot is similar to a backup, but it is a complete image of a protected system, including data and system files. Replication is a method of copying data based on a secure system to another location.

Equally important are the following data protection options: firewalls, authentication and authorization, encryption. Firewalls—utilities that enable you to monitor and filter network traffic. Authentication and authorization—controls that help you verify credentials and assure that user privileges are applied correctly. Encryption—alters data content according to an algorithm that can only be reversed with the right encryption key.

The last methods that we will consider are Endpoint protection, Data erasure, Disaster recovery. Endpoint protection—protects gateways to your network, including ports, routers, and connected devices. Data erasure—limits liability by deleting data that is no longer needed. Disaster recovery—a set of practices and technologies that determine how an organization deals with a disaster, such as a cyber attack, natural disaster, or large-scale equipment failure.

On the last slide you can see the list of used literature. thank you for your attention!

**List of literature sources:**

1. Data Protection and Privacy: 12 Ways to Protect User Data // Cloudian URL: <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/amp/#protection-technologies>
2. Top 12 Data Security Solutions to Protect Your Sensitive Information // netwrix URL: <https://blog.netwrix.com/2019/09/12/top-12-data-security-solutions-to-protect-your-sensitive-information/>
3. Data Privacy And Protection: 11 Ways To Protect User Data // DuoCircle URL: <https://www.duocircle.com/email-security/data-privacy-and-protection-11-ways-to-protect-user-data>
4. 12 Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2023 // Ekran URL: <https://www.ekransystem.com/en/blog/best-cyber-security-practices>
5. 12 Ways to Protect your Organization from Ransomware // Virtualizationhowto URL: <https://www.virtualizationhowto.com/2021/10/12-ways-to-protect-your-organization-from-ransomware/>