**Information Systems**

Common types of IS are: **management, transaction processing, decision support**.

Management IS helps to get necessary information from corporate database, making life of managers easier. Transaction processing system is, obviously, there for dealing with customers’ requests, processing payments. Decision support system helps to predict ways of how everything will look like in the future in order to make correctives and make a right decision.

In general, the software development life cycle (SDLC) is a closed loop, in which each stage affects the actions in the subsequent one.

There are 5 stages of software development life cycle (SDLC):

* **Planning and analysis -** This phase is the most fundamental one. Business requirements are analyzed by an analyst, domain expert, and project manager. The business analyst interacts with stakeholders to develop the business requirements document. The aim of the requirements analysis is for quality assurance and to identify potential risks to address in order for the software to succeed.
* **Architecture and design -** During this phase, lead developers and technical architects create the initial high-level design plan for the software and system.
* **Development -** In this phase, the database administrator creates and imports the necessary data into the database. Programming languages are defined by requirements. Developers create the interface according to the guidelines and conduct unit testing. This is an important phase for developers.
* **Testing** – the software if being tested to make sure that the software is solving the needs outlined during the planning phase. All tests are conducted as functional testing, including unit testing, integration testing, system testing, acceptance testing, and non-functional testing.
* **Maintenance phase -** In a post-production, live software environment, the system is in maintenance mode. No matter the number of users, the sophistication of the software and rigorous QA testing, issues will occur. That’s the nature of software with managing data, integration, and security, and real-world usage.

   System security covers all methods of accessing information. From authentication, to software updates, anti-virus protection, and modifications - security is a key component to a device operating as expected. The security of a computer system is a crucial task. It is a process of ensuring the confidentiality and integrity of the OS. A system is said to be secure if its resources are used and accessed as intended under any circumstances, but no system can guarantee absolute security from several of various malicious threats and unauthorized access. Such methods as physical protection of data centers as well as two-factor authentication and various types of identity confirmation methods provide top-level security for computer systems.