**Information Systems**

Information system – computer-based tools for collecting, storing and processing data.

What for inf system – IPOS (input, output, processing and storing). Information should be accurate, timely and relevant

How help – automatically doing routine tasks

Components: hardware, networks, people, data, programmers (software)

Information systems are widely used by governments, businesses, corporations etc.

***Page3 how do inf sys help people in an org-on***

There are the four major types of information systems:

TPS (Transaction processing system) - collect, process and store transactions

MIS (Management information system)-routine business decisions

DSS (Decision support system)-to create models of various decisions (?)

Expert system-analyze data and help people make decisions

Ещё несколько из другого упражнения:

OLTPS (online transaction processing system)

EIS (executive inf system)

Neural network system

Examples of inf system’s applications: word processors, online air ticket booking system, spreadsheets, photo-editing programs, database programs

SDLC (system development life cycle)-a way to construct information system

**Phases:**

1. ***Planning phase***

Goal: produce a project development plan

**Activities:**

Assemble the project team

Justify the project

Choose a development methodologies

Develop a project schedule

Produce a project development plan

**Documents:**

Short description and its scope

Justification with the cost and benefits

List of participants

Schedule (?)

1. ***Analysis phase***

Goal: make a list of system requirements

**Activities:**

Study the current system

Determine system requirements

Write a requirements report

**Activities#2**

Interwiev the user and study the current system version

Make a prototype (only basic features)

System requirements are the criteria for successfully solving problems identified in an information system

1. ***Design phase***

Goal: satisfy system requirements

**Activities:**

Find hardware and software solutions

**Something about hardware**: you should think about:

-Types of devices

-Connection

-Types of storage (in-house(costly) or cloud(!safety))

-A level of automation

***4) Implementation phase***

Goal: create new information system

**Activities:**

-Coding

-Debugging

-Testing (types of testing …)

-Conversion

***5) Maintenance phase***

Goal: The main goal of maintenance phase is to make back ups, provide help to users, and fix bugs

Support training users, patch (small part of code), service pack and completely new version

(upgrade the application to the newer versions of the software, adding some new features into the existing software)

Maintenance characteristics: efficiency (does the new system operate quicker?), usability(are all users able to use the system easily?), appropriateness (work or no, )

Source code -> object code

Manual – a book giving instructions or information

Procurement (закупки) – the act of obtaining goods or services

Cutover – (сокращение) a rapid transition from one phase of a business enterprise or project to an another

**Hardware options:**

1. Device requirements – choose type of devices according to where they will be use (office or stand-alone computer)
2. Network technology – consider how our device would be connected
3. Cloud hosting – cheaper, you can get your data from any device, vulnerable to hacker attacks
4. Level of automation – human intervention into inf system

**Types of systems:**

1. Application developments tools – kit(набор) containing building blocks that can be assembled into a software product (save your time, easily, but not so flexible)
2. Application software – it has some customization options
3. System from scratch – it’s usually costly, but it offers most flexibility for achieving he system requirements, take a lot of time
4. Turnkey system – you can immediately start using this software, system without customization options

Maintenance manual – for system specialists

Assurance – confidence of mind or manner

**Types of testing:**

1. Unit testing – test each module separately
2. Integrated testing – to make sure that all modules work together correctly
3. System testing – test compatible with hardware and software
4. Acceptance testing – user test your system
5. Business testing – testing by business testers or professionals

**Types of conversion:**

1. Direct conversion – completely deactivate all system (not safely, risky)
2. Parallel conversion – if new system doesn’t work, old system can support you (safely, but systems slow down each other; limited by a capacity of server)
3. Phased conversion – activate one module at a time (no so risky)
4. Pilot conversion – when system from one brunch can support in other brunch, only one brunch at a time (reduces risks)

*Scope creep* refers how project requirements tend to increase over a project life cycle (make product too complicated or difficult to use)

**Reasons of scope creep:**

1. Lack of proper inicial identification
2. Weak project manager cant say ‘no’ new features
3. Pure(? Bad) common skill in team and between you and user

**Types of modifications:**

1. Major modifications – (externally) – they are program modifications involving externally developed software
2. Routine modifications – (internally computer) – to improve performance, correct problems or enhance security
3. Emergency modifications – (quickly) – for quickly modifications
4. Software patches (externally) – they include significant functional changes to an existing system, converting to a new system and introducing new systems of data

Patch - peace of source code

Service pack – set of patches, which is necessary to update

New version – completely new version

QoS – quality of service

QoS metrics:

Throughput – number of process data in a particular time

Accuracy – number of errors

Downtime – amount of time when system is not available

Capacity – available storage/ number of connections

User levels – number of users at pic or average or low time

Response time – period of time between “user sent request” and “get answer”

**Protective measures**: deterrents, preventive countermeasures, corrective procedures, detection activities

**Threats**: *natural disaster* (can completely shut down a computer system), *power outages* (can be caused by natural disasters, overloaded power grids, planned brownouts), *equipment failures*(the risk increases as a hardware component ages, but they can occur in brand-new hardware*)*, *human errors*(mistakes made by computer operators), *software failures*(can be caused by bugs or flawed software design), *security breaches(*include stolen data, physical instructions etc.), acts of war(cyberterrorism can cause damage), *malware*(can damage just about any computer system, after rooting out a virus from your personal computer for example)