1. **Software engineering**

***What is software engineering?***

Software is a program or a set of programs containing instructions which provide desired functionality. And engineering is the process of designing and building something that serves a particular purpose and finding cost effective solutions to problems. These two terms combined make software engineering. In short, software engineering is a systematic approach to the design, development, operation, and maintenance of a software system.

Software engineering is a wide term, because there are a lot of types of software. For example, desktop applications, web applications, mobile applications. These applications can be divided even further, for instance, mobile development can be divided into Android development and iOS development.

***Types of software engineers***

It is difficult to go from an idea of the app to publishing it, so therefore there are different positions that people specialize in.

* ***Front-end developers***

A front-end developer mostly works on user interfaces and what people actually see when visiting a website or opening an app.

* ***Back-end developers***

A back-end developer works on the logic of the applications (for example databases).

* ***Testers***

Testers are responsible for assuring that the application works correctly. It is important for a tester to think “outside the box”. They need to try to break the program and find all the edge cases before the application is published.

Of course, these are not the all positions, as this is just a short overview.

***Software development life cycle***

Software development life cycle is a process for planning, creating, testing and deploying an application or a project. The idea behind it is to make the highest quality software with the lowest cost in the shortest time possible. It provides a well-structured flow of phases which help to organize the work process. There are many popular SDLC models, the most popular being the Agile model.

SDLC has stages that ensure the process works in a smooth and efficient way. These stages include:

* *Identifying current problems*
* *Planning*
* *Designing*
* *Building*
* *Testing code*
* *Deploying software*

1. **Training**

Training is teaching or developing any skills and knowledge that relate to specific useful competencies. “Training” was the topic of our second unit during the course. During this unit, we discussed the importance of training, looked at the tendencies of training in the work field, and also shared our own experiences.

Generally speaking, I believe that training is really important in any sphere, because, unless you are super talented or intellectually gifted, dedicating time and training is the only way of improving in any area.

***Training in the work field***

Talking about the work industry, there are different types of training that might be provided prior to signing a person to a full time position, the two most popular being internships and apprenticeships. Now I will try to compare and summarize these two types of training.

1. ***Apprenticeships tend to be longer.***

When it comes to internships, most people either do it for a semester or summer and then move on or get hired by the company. On the other hand, while there are apprenticeships that only last for a year, many are multi-year in length.

1. ***Apprenticeships give hands on training.***

When doing an internship, although you will see what’s the workflow like, you won’t have too much responsibilities. Apprenticeships, on the other hand, tend to give you real on the job training in the profession you will eventually work in.

***Online training***

Lastly, I will share my personal experience regarding online training. These days there are plenty of opportunities to learn without even leaving your house. You can find different courses and material on pretty much any subject you might be interested in online. Many courses are also free, and if not free, not expensive. I, personally, have attended a few courses, both paid and free, regarding web development. In my opinion, it is a great way of learning, because you can learn at your own pace, whenever you want.

1. **Operating systems**

An operating system is an interface between a computer user and the computer hardware. It is a software that performs all the basic tasks, such as file management, memory management, process management, controlling peripheral devices such as disk drives and printers.

To some extent, all of the most popular operating systems (Windows, MAC, Linux) can achieve your desired results and is a choice of preference. Although there are some key differences, and, if, for example, you were to choose between these operating systems, some of them would be more useful to you than to another person. Now I will try to summarize and compare 3 most popular operating systems – Windows, MAC, and Linux.

Windows allows the user to extend the operating system to fit their needs, but requires the removal of everything they do not need. This is basically the opposite of Linux. Windows comes pre-packaged with software and services many users do not need. The philosophy is that “it is easier to remove than it is to add”. It perfectly fits people who might not be tech-savvy or don’t have the time to learn how to extend their operating system functionality. Mac is a balance between Windows and Linux, and is known for good looking user interface. All of them are free, although when using free Windows version, there are small cosmetic restrictions, and Mac is only available on Apple machines.

All in all, there is no single “best” OS. There is an OS that is most suited for your needs.

1. **Energy**

“Energy” was our third unit during the course. During this unit we discussed different types of energy sources, and the energy sources that are considered to be the cleanest and the dirtiest.

Energy is primarily used to produce electricity. There are different types of sources of energy. They can be broken down into renewable and non-renewable energy sources.

***Renewable energy sources***

A renewable energy source is any natural resource that can replace it quickly and dependably. These energy sources are plentiful, sustainable, naturally replenished and good to the environment.

The major types or sources of renewable energy are:

1. Solar energy from the sun
2. Wind energy
3. Geothermal energy from the heat inside the earth
4. Hydropower from floating water
5. Ocean energy in the form of wave, thermal energy
6. Biomass from plants

***Non-renewable energy sources***

A non-renewable energy source is a source with a limited supply that we can mine or extract from the earth, and it’ll eventually run out.

These are formed over thousands of years from the buried remains of ancient sea plants and animals that lived millions of years ago. Most of these energy sources are “dirty” fossil fuels, which are generally bad for the environment.

The major types or sources of non-renewable energy are:

1. Petroleum
2. Hydrocarbon gas liquids
3. Natural gas
4. Coal
5. Nuclear energy

***Energy in Lithuania***

As of December 2019, Lithuania imports 73% of its energy, mostly from Norway and the United States. In 2016, renewable energy constituted 28% of the country’s overall electricity generation.

1. **IT security**

IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. As hackers get smarter, the need to protect your digital assets and network devices becomes even greater.

***Threats to IT security***

Threats to IT security can come in different forms. A common threat is a malware, or malicious software, which may come in different variations to infect network devices, including:

* *Ransomware*
* *Spyware*
* *Viruses*

These threats make it even more important to have reliable security practices in place.

***Types of IT security***

* ***Network security***

Network security is used to prevent unauthorized or malicious users from getting inside your network. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users’ ability to access or use the network.

* ***Internet security***

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls, antimalware, and antispyware.

* ***Endpoint security***

Endpoint security provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and personal computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat.

* ***Cloud security***

Applications, data are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack, hence there are separate IT security solutions made for the cloud.

1. **Cybercrime**

Cybercrime is a criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Other than that, some cybercriminals might want to damage computers for political or personal reasons. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

***Most cybercrime falls under two main categories:***

* *Criminal activity that targets*
* *Criminal activity that uses computers to commit other crimes*

***Examples of cybercrime***

* ***Malware attacks***

A malware attack is where a computer system or network is infected with a computer virus or other type of malware. Then, the damaged computer could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.

* ***Phishing***

A phishing campaign is when emails are sent with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for. Phishing campaign messages may contain infected attachments or links to malicious sites. Or they might ask the receiver to respond with confidential information.

* ***DDoS attacks***

Distributed DoS attacks are a type of cybercrime attack that cybercriminals use to bring down a system or network. This attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests.

***How to protect yourself against cybercrime:***

* *Use anti-virus software*
* *Use strong passwords*
* *Never open attachments in spam emails*
* *Do not click on links in spam emails or untrusted websites*
* *Keep software and the OS updated*

1. **Employment trends**

“Employment trends” was our 5th unit in our course. During this unit we discussed employment trends in Lithuania, as well as the future of work.

***Giganomics***

These days there are many different ways to earn money and many approaches to work. While in the past people used to be dependent on only one job they had, today there are different ways to generate income. One of them is giganomics – a phenomenon when you sustain yourself by doing many different “gigs”, hence the name giganomics. Of course, as any other thing in the world, it has its advantages and disadvantages. On one hand, if you choose this approach, no one has a complete power over you to switch work on or off. Moreover, it can be a more lucrative way of earning money. On the other hand, though, you are responsible for your work schedule, which also takes time. This can cause stress and uncertainty in some situations.

***Future of work***

Talking about the future, it is obvious that the world of work is changing. Artificial intelligence, automation, and robotics will make this shift as the mechanization in prior generations of agriculture and manufacturing. While some jobs will be lost, and many others created, almost all will change. People who are working in jobs that require creativity and imagination should feel safest, because, currently it is very difficult to fully automate these aspects, but, as the technologies evolve, no one knows what the future holds.

1. **The Internet**

The internet is a network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection.

***Advantages of the internet***

* ***Social networking***

Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the web that uses Internet as the medium for communication. Examples of these apps include Facebook, Instagram, Twitter, etc.

* ***Education and technology***

We are able to surf for any kind of information over the Internet. Information regarding various topics such as technology, health and science, social studies, geographical information, information technology, etc. can be surfed with the help of a search engine.

* ***Entertainment***

Internet is also a source of entertainment. For example, online television, online games, songs, videos, social networking apps.

* ***Online services***

Internet also allows us to use many services, such as internet banking, online shopping, online ticket booking, online bill payment, e-mail.

***Disadvantages of the Internet***

* ***Threat to personal information***

There are always chances to lose personal information such as name, address, credit card number. Therefore, people should be very careful while sharing such information. People should use credit cards only through authenticated sites.

* ***Spamming***

Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of the entire system.

* ***Cybercrime***

There are people with bad intentions, who try to exploit any vulnerabilities on the Internet for monetary or other gain, therefore people should be careful.

* ***Virus attacks***

Virus can easily be spread to the computers connected to the Internet. Such virus attacks may cause your system to crash or your important may get deleted.

1. **Ethics**

“Ethics” was our 6th unit in our course. During this unit, we discussed about the meaning of ethics, and about business ethics.

***What is ethics?***

At its simplest, ethics is a system of moral principles. They affect how people make decisions and lead their lives.

Ethics cover the following dilemmas:

* *How to live a good life*
* *Our rights and responsibilities*
* *The language of right and wrong*
* *Moral decisions – what is good and bad?*

Our concepts of ethics have been derived from religions, philosophies and cultures. They infuse debates on topics like abortion, human rights and professional conduct.

***Business ethics***

Business ethics is the study of appropriate business policies and practices regarding potentially controversial subjects including bribery, discrimination, corporate social responsibility, and trust-based responsibilities. Business ethics provide a basic guideline that businesses can choose to follow to gain public approval.

Business ethics ensure that a certain basic level of trust exists between consumers and various forms of market participants with businesses.

***Example of business ethics***

Imagine, that a company X sells cereals with all-natural ingredients. The marketing department wants to use the all-natural ingredients as a selling point, but it must temper enthusiasm for the product versus the laws that govern labeling practices.

Some competitors advertise high-fiber cereals that have the potential to reduce the risk of some types of cancer. The cereal company in question wants to gain more market share, but the marketing department cannot make dubious health claims on cereal boxes without the risk of litigation and fines. Even though competitors with larger market shares of the cereal industry use shady labeling practices, that does not mean every manufacturer should engage in unethical behavior.

1. **Artificial intelligence**

Since the invention of computers or machines, their capability to perform various tasks went on growing exponentially. Humans have developed the power of computer systems in terms of their diverse working domains, their increasing speed, and reducing size with respect to time.

Today, there is a separate branch of Computer Science, named Artificial Intelligence, that pursues creating the computers or machines as intelligent as human beings.

***What is Artificial Intelligence?***

Artificial Intelligence is a way of making a computer, a computer-controlled robot, or a software think intelligently, in the similar manner the intelligent humans think.

AI is accomplished by studying how human brain thinks, and how humans learn, decide, and work while trying to solve a problem, and then using the outcomes of this study as a basis of developing intelligent software and systems.

***Goals of Artificial Intelligence***

* ***To create Expert Systems***

These systems would exhibit intelligent behavior, learn, demonstrate, explain, and advice its users.

* ***To implement Human Intelligence in Machines***

Creating systems that understand, think, learn, and behave like humans.

***What contributes to Artificial Intelligence?***

Opposed to popular belief, AI is not only based on Computer Science. There are different disciplines that contribute to Artificial Intelligence, these include:

* *Philosophy*
* *Psychology*
* *Math*
* *Biology*