Why information security?

Information security is various measures to protect information from unauthorized persons. In the pre-digital era, people locked important documents in safes, hired security guards, and encrypted their messages on paper to protect data.

Today, digital information is more often protected. Still, the measures are essentially the same: information security specialists create protected spaces (virtual "safes"), install security software like antivirus ("hire security guards") and use cryptographic methods to encrypt digital information.

## What Does Information Security Guard?

It is responsible for three things: confidentiality, integrity, and availability of information. In the information security concept, they are called information security principles:

* Confidentiality means that only those who have the right to do so have access to information. For example, only you know your email password, and only you can read your emails. If someone finds out the password or otherwise gains access to the mailbox, confidentiality will be violated.
* Integrity means that information is preserved in full and is not changed without the owner's knowledge. For example, your email contains letters. If an attacker deletes some or changes the text of individual emails, this will violate the integrity.
* Availability means that whoever has the right to access information can obtain it. For example, you can log into your email at any time. If hackers attack the servers, mail will be unavailable, and this will compromise availability.

Types of Information

Information can be public and confidential. Anyone has access to the public, while only individuals can access the confidential one.

It may seem that there is no need to protect public information. But only the principle of confidentiality does not apply to publicly available information - it must remain integral and accessible. Therefore, information cybersecurity also deals with publicly available information.

For example, let's think about an online store. Product cards, blog articles, seller contacts - all this crucial information is publicly available, and anyone can view it. But the online store still needs to be protected so that no one disrupts its work (for example, not change important information in the product cards or "drop" its site).

If everything is clear with publicly available information, it is worth talking about confidential information separately since it has several varieties.

Main Types of Confidential Information

**Personal Information**. Information about a specific person: full name, passport data, phone number, physiological characteristics, marital status, and other data. Anyone who works with personal data is obliged to protect it and not transfer it to third parties. Information about customers and employees refers to personal data.

**Trade secret**. Internal information about the company's work: technologies, management methods, customer base. If this data becomes known to outsiders, the company may lose profits. The company itself decides what is considered a trade secret and what is exposed to the public. Moreover, not all information can be a trade secret - for example, the founders of the legal entity or working conditions cannot be hidden.

**Professional secret**. It includes medical, notarial, lawyers, and other types of secrets related to professional activities. Several laws are connected with it at once

**Official secret**. Information that is known to individual services, for example, the tax or registry office. Government agencies usually store this data. They are responsible for protecting it and only provide it upon request.

**State secret**.

Briefly About Information Security

* Information security is responsible for protecting data and ensuring its confidentiality, integrity, and availability.
* Confidentiality means that only those who have the right to do so have access to the data.
* Integrity means that data is stored unchanged and remains valid.
* Availability means that the person who has the right to access information can get it.
* Information security protects both confidential and public data. It ensures integrity and availability to the public. While confidential, it also provides the required level of secrecy.
* Confidential information includes personal data, commercial, professional, official, and state secrets.

I hope you now know "why is information security important?".

That’s about all

1. Are you familiar with people involved in information security?

Yes, I have friends from the FSB Academy who are engaged in network and computer security

1. How do you feel about the theft of confidential information?

Very bad. I believe that everyone can keep secrets