- definition of general and specific obligations of employees in the management of information security, including information on incidents of violation of information security;
- links to documents that complement the information security policy, for example, more detailed policies and procedures for specific information systems, as well as the safety rules to be followed by users.

Information Security Policy of the company must be approved by management, published and communicated to all employees in an accessible and understandable form.

References

1. The Council of Europe Convention-11.12.2008, www.coe.int
2. Fundamentals of Information Security. Textbook for high schools / EB Belov, VP Moose, RV Meshcheryakov AA Shelupanov. -M.: 2006 - 544
3. Vikhorev SV Kobtsev RY How to determine the sources of threats? // Open systems №7-8 / 2002. http://www.elvis.ru/files/howto.pdf.
4. GOST R ISO / IEC 17799-2005.
5. ISO / IEC 17799: 2000 (BS 7799-1: 2000).

D.M. Umurzakova

INFORMATION SECURITY AND DATA PROTECTION

(TUIT Fergana branch, Uzbekistan)

The emergence of new information technologies and the development of powerful computer storage and information processing systems increased the levels of information security and necessitated that the effectiveness of information security grow along with the complexity of the data storage architecture. So gradually the protection of economic information becomes mandatory: all kinds of documents for the protection of information are being developed; the recommendations on information protection are formed; even carried out a federal law on information protection, which deals with the protection of information and the task of protecting information, and also solves some unique issues of information protection.

This, the threat of information security has made the means of ensuring information security one of the mandatory characteristics of the information system.

The phrase "threats to the security of information systems" refers to real or potentially possible actions or events that are capable of distorting data stored in the information system, destroy them or use them for any purposes not provided for by the rules in advance.

Protection of information from computer viruses (protection of information in information systems) involves means of protecting information on the network, or more specifically, software-based information security that prevents the unauthorized execution of malicious programs that attempt to seize data and send them to an attacker, or destroy database information, but protection information from computer

viruses is incapable of fully reflecting the attack of a hacker or a person called a computer pirate.

The task of protecting information and protecting information from computer viruses is to complicate or make it impossible to penetrate, both viruses and the hacker, to sensitive data, for which the burglars in their unlawful actions are searching for the most reliable source of secret data. And since hackers are trying to get the most reliable secret data with minimal costs, the task of protecting information is the attempt to confuse an attacker: the information security service provides him with incorrect data, the protection of computer information tries to isolate the database as much as possible from external unauthorized interference, etc.

What are the principles of data protection?

If you read our previous blog 'Why is data protection training important?' you may recognise them, but just in case you need a re-cap, they are:

- ✓ Personal data shall be processed fairly and within the law.
- ✓ Personal data can only be held for specific and lawful purposes.
- ✓ Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- ✓ Personal data shall be accurate and, where necessary, kept up to date.
- ✓ Personal data shall not be kept for longer than is necessary.
- ✓ Personal data shall be processed in accordance with the rights of data subjects under this Act.
- ✓ Appropriate technical and organisational security measures shall be taken against unauthorised access to data.
- ✓ Personal data must not be transferred to a country outside the European Union unless that country or territory has similar legislation to the Data Protection Act that protects data.

Principle seven

When put into practice, principle seven means you, as the company or organisation must have appropriate security in place to prevent the personal data you hold being deliberately or accidentally compromised. In particular, you will need to:

- ✓ design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- ✓ be clear about who in your organisation is responsible for ensuring information security;
- ✓ make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- ✓ be ready to respond to any breach of security swiftly and effectively.

So what are the key differences?

Data protection is about taking people's personal data – think names, addresses, contact information, medical history, banking details, credit ratings and even employment records. It can also include – if necessary – sensitive personal data, such as someone's political opinions. The way this data is collected, accessed, updated, stored and disposed of is all covered by Data Protection law.

Examples of data protection best practice in your organisation: In practical terms, we're talking about the length of time you say you keep (and you actually do keep) information from your clients, employees or volunteers. Application forms, booking forms and basic contact details.

Information security (Infosec for short or otherwise known as cyber security) refers to the technical and operational measures that any organisation must take to ensure that the data they hold is safe and secure. Information security is about people, products, processes and all working aspects of a company or organisations. It's about the way you store the information, and what happens if it gets lost or stolen.

Examples of Information Security in your organisation: This involves business practices like creating strong passwords, changing your password every 3 months, whether to encrypt your data or, actually, whether you'd pick up a flash drive from the floor and put into your computer to see what's on it (don't do this).

References

1. Smith, Elementary Information Security (2011, Jones & Bartlett Learning).
2. Stamp, Information Security: Principles and Practice, 2/e (2011, Wiley).

Ш. Абдуллаев, Ж. Хакимов, Д. Абдурасулова

SSL И S-HTTP - ЗАЩИТА WEB-ПРИЛОЖЕНИЙ

(Ферганский филиал Ташкентского университета
информационных технологии)

Под протоколом в электронной коммерции понимается алгоритм, определяющий порядок взаимодействия участников транзакции и форматы сообщений, которыми участники транзакции электронной коммерции обмениваются друг с другом с целью обеспечения процессов авторизации и расчетов.

В данный момент наиболее распространенным протоколом, при построении систем электронной коммерции является протокол SSL. Широкое распространение протокола SSL объясняется в первую очередь тем, что она является составной частью всех известных браузеров и Web -северов. Это, означает, что фактически любой владелец карты, пользуется стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL.

Стандарт SSL был разработан фирмой Netscape Communications. В его основе лежит шифрование с открытым ключом. Основная идея заключается в том, что при использовании стандартных протоколов обмена вся информация передается по сети Интернет в незащищенном виде. Таким образом, при прослушивании трафика одним из промежуточных узлов, Ваши пароли, номера кредитных карт и иная конфиденциальная информация могут стать достоянием общественности. Протокол SSL оговаривает методы шифрования всей передаваемой информации прозрачно для пользователя. В данный момент протокол