ALGORITHMS OF RISK MINIMIZATION IN PERSONAL DATA PROTECTION SYSTEMS.

Nigmatkhojayev Fayzulla

Annotation

Detailed information security threat models (ITTs) allow you to develop a defense plan that is based on current threats and will consider effective countermeasures that increase the level of information security (IS). One of the main purposes of modeling is to create the most effective system for assessing the state of security enterprise assets. The following article is devoted to the algorithms of risk minimization in personal data protection systems.

Key words: algorithm, personal data, privacy policy, information security, technical malfunction, database.

Modern information systems (IS) have a rather complex object structure, and also suggest the versatility of the concepts of information security. To describe the threat model, it is expedient to to use different methodologies for automating this process with the possibility of visual representation of the structure of complex objects and processes from the required angle and sufficient degree detail. The construction of various threat implementations in the form of attack trees or attack graphs (ATGs) is one of the topical directions in assessing the level of IP security. After constructing the graph, be implemented to check its properties. All threats, connections, their parameters are determined by the owners and specialists in the field of information security. Troubleshooting the Full Overlap Security Model made possible by use. In such models, each threat is opposed to its own means of protection. The article considers the creation of a software application for automation and formalization the process of assessing the information security of IP assets and localizing bottlenecks in the IP protection system. The feature of the created. The first application is to use the FSTEC Threat Database to model the attack tree. Once the working software

application allows you to reduce time, simplify the process of assessing security IS, and also visualizes the process of threat modeling. The scope of the developed program product may be small and medium-sized businesses, as well as government enterprises.

Regardless of whether the company belongs to a large, small or medium-sized business, whether it is an established organization or still a start-up, the issue of personal data protection is relevant for everyone. This article is devoted to the features and means of such protection, as well as recommendations that will help simplify this work and make it more efficient. The implementation of measures to protect personal data is the responsibility of the operator, i.e. the subject that collects and processes data in the information system. As a rule, such an entity is a company that owns databases of its employees and customers, or a third-party organization authorized by the owner company.

Personal data is any information relating directly or indirectly to an individual who is registered in law as the subject of personal data. The most common types of such information are:

passport data;

exact place of residence;

mobile phone;

E-mail address.

Last name, first name and patronymic in themselves can also be personal data. The access of this information to any third parties must be excluded. In addition, it must be understood that the operator has the right to process data only in certain cases:

if they have received consent to the processing (not necessarily written);

it is planned to conclude an agreement with the subject (even in the case of an offer on the website);

personal data of its employees are processed;

in special cases, when processing is necessary to protect the life, health and other important interests of a person.

If the operating company fails to prove any of the listed grounds for processing, it is also subject to a fine and the collection of data is considered illegal. The most important point here is the very consent to processing. The simplest method that most companies use is a form of express consent implemented in one way or another. Usually this is a "tick" familiar to many under the accompanying text about the actual consent.

Another parameter to consider is that you should not process personal information that is not directly related to the subject of the contract (for example, for a classic sales contract, the profession, education level or military duty of the buyer does not matter). Excessive interest may be interpreted by the supervisory authorities as a violation.

Since from time to time Roskomnadzor conducts unscheduled inspections (most often, if there are complaints from a specific person - a former employee, a competing company or a client who believes that his rights have been violated), in order to avoid claims, the operating company needs to make sure that:

The privacy policy is documented and publicly available.

Reference:

1. Gribanova-Podkina M. Yu. Building a model of threats to information security systems using the methodology of object-oriented design // Security Issues. 2017. No. 2. S. 25–34

2. GOST R ISO/IEC 15408-3-2002. Information technology. Methods and means of ensuring without danger. Criteria for evaluating information technology security. Part 3. Requirements for confidence in security danger. Introduction 2004-01-01. M.: IPK Publishing house of standards. 2002.
3. Kotenko I. V., Stepashkin M. V., Bogdanov V. C. Intelligent security analysis system computer networks. URL: http://www.positif.org/docs/SPIIRAS-NCAr06-Stepashkin.pdf.
4. Sheyner O., Jha S., Wing J. Two Formal Analyzes of Attack Graphs // II IEEE Computer Security Foundations Workshop. Cape Brenton, Nova Scotia, Canada. June 2002, pp. 49–63.
5. Jajodia S., Noel S. Managing Attack Graph Complexity Through Visual Hierarchical Aggregation // II In 1st
6. International Workshop on Visualization and Data Mining for Computer Security. Washington DC, USA. October 2004. P. 109–118.
7.