Modeling threats to information security using IDEF0 methodology

A A Khristolyubova¹, A A Konev², A A Shelupanov³ and M L Solovev⁴

¹Joint stock company Central design bureau of automatics, Russia, Omsk, Kosmichesky pr., 24a, 644027, Russian Federation
²Department of Complex Information Security of Computer Systems, Tomsk State University of Control Systems and Radioelectronics, 40 Lenin pr., Tomsk, 634050, Russian Federation
³University administration, Tomsk State University of Control Systems and Radioelectronics, 40 Lenin pr., Tomsk, 634050, Russian Federation
⁴University administration, Siberian state university of telecommunications and information sciences, 86 Kirova str., Novosibirsk, 630102, Russian Federation

E-mail: karjanna@mail.ru

Abstract. The paper describes the implementation of a method for modeling threats to information security using the methodology of IDEF0 functional modeling to solve problems of formalization of specific threat models. The formulation of the method for modeling threats to information security accounts for various media of information transmission and its carriers. In addition, a process approach to information handling is used.

1. Introduction

The analysis has shown [1–4] that the assessment of information system security, determination of a sufficient set of protection means and solution of subtasks, such as construction of the system model and the model of threats, predominantly involve methods that avoid the effects of real scenarios of an information system application. They rest upon probabilistic assessment results and reflect a subjective opinion of experts. The final result of the applied methods and approaches is a list of threats and their classification that are no way connected with the category of protected information, while accounting its state [5].

One of demanded directions of information protection system design is a justified comparison of real threats to information security with the means and mechanisms of information protection that neutralize the threats relying upon the description of real information flows described as generic elements [6]. Initial modeling of threats to information security, regardless of the chosen modeling method, is based on the determination of possible consequences caused by a destructive impact on the protected object [7].

By present, there are many methodologies for modeling information flows [8]. Among the most elaborated ones, that suit modeling of protected information flows is IDEF0. Utilization of a list of the information processes that handle information to be protected as the basis for the constructed formalized model of threats allows accounting for the information representation, transmission media and carriers of information to be protected [9]. There is an example of SADT methodology
implementation to analyze the actions of intruders during an attack aimed at the collection of information system characteristics [10].

2. Materials and research methods
The method of decomposition of an information process and modeling of information flows is an element of the method for modeling the threats to the information security that is efficiently used at the stage of information system design to abate the threats caused by system architecture flaws [11]. The set of information transmission and processing media are given in Table 1.

Table 1. Description of the array of information medium and information processing environment.

| Set «Information transmission media» S=\{s_1, s_2...s_5\} | Set «Information carriers» V=\{v_1, v_2...v_8\} |
|-------------------------------------------------------------|-------------------------------------------------|
| s_1 Tangible                                                | v_1 Tangible object (protected object).          |
| v_2 Human (personnel) and their biometric parameters.       |
| s_2 Optical (visual)                                        | v_3 Electromagnetic field (photons).             |
| s_3 Acoustic                                                | v_4 Acoustic waves.                             |
| s_4 Electromagnetic                                         | v_5 Near electric field.                        |
| s_5 Virtual                                                 | v_6 Near magnetic field.                        |
| v_7 Electromagnetic field.                                  |
| s_6 Virtual                                                 | v_8 Various types of semiconductor-based memory.|

Some studies on the methods for modeling threats to information security include—besides usual threats to confidentiality, integrity, availability—the threats of destruction, damage to, theft or loss, disclosure, waiver to use, elevation of privilege and illegal use of information [12]. In fact, the additional threat types characterize the way an intruder reaches their goals and do not reflect the goals of the protected information owner. Considering the approach to the construction of the model of threats to information security given in [9, 13], the threats to confidentiality, integrity and availability are divided into several classes given in Table 2.

Table 2. Classes of information security threats of confidentiality, integrity and availability.

| Kind of information security threats | Classes of information security threats |
|--------------------------------------|----------------------------------------|
| Threats to confidentiality           | Impersonation of recipient in medium state 1 |
|                                      | Impersonation of recipient in medium state 2 |
|                                      | Substitution of information transmission channel |
|                                      | Control of information transmission channel |
| Threats to integrity                 | Impersonation of sender in medium state 1 |
|                                      | Impersonation of sender in medium state 2 |
|                                      | Substitution of information transmission channel |
|                                      | Exposure on information transmission channel |
| Threats to availability              | Unavailability of carrier in medium state 1 |
|                                      | Unavailability of carrier in medium state 2 |
|                                      | Disturbance of information transmission channel |
|                                      | Inability of transformation |

The analysis of information processes in various problem domains enables formulation of a finite number of desirable information protection results that are the main goal of protection system design. The multitude of carriers of protected information and medium of its processing can be correlated by identified goals of information protection (Table 3).
Table 3. Array of protected carriers and its transmission medium.

| Protection goal                                      | Transmission medium | Carriers            |
|------------------------------------------------------|---------------------|---------------------|
| Hide semantic content of information                  | S₁, S₂, S₃, S₄, S₅  | v₁, v₂, v₃, v₄, v₅, v₆, v₇, v₈ |
| Hide linear dimensions of the protected object        | S₁, S₂, S₃          | v₁, v₂, v₃, v₄      |
| Hide specific configuration of the protection object  | S₁, S₂, S₄, S₅      | v₁, v₂, v₃, v₇      |

According to the principles of model construction on the basis of IDEF0 methodology, the sources of threats to information integrity can be the resources providing the information flow (mechanism of information processing) [1] or the conditions of certain operation of the process (documents, regulating rules, strategies of processing [13, 14]) at any stages of the information system life. Eventually, for each typical information handling process, a graph of data transformation in various media can be constructed that will contain typical operations of data transformation. Table 4 presents possible typical operations of data transformation in terms of each protection goal and their examples.

Table 4. Typical data conversion operations for each protection target and their examples.

| Protection goal                                      | Typical transformation operations | Examples of typical operations                  |
|------------------------------------------------------|-----------------------------------|------------------------------------------------|
| Hide semantic content of information                  | V₁→S₁→V₂                        | Transmit paper document                        |
|                                                      | V₂→S₁→V₁                        | Return paper document                          |
|                                                      | V₂→S₂→V₃                        | Demonstrate content of paper document          |
|                                                      | V₃→S₂→V₂                        | Examine content of paper document             |
|                                                      | V₂→S₃→V₄                        | Voice information about content of paper document |
|                                                      | V₄→S₃→V₂                        | Listen to information about content of paper document |
|                                                      | V₂→S₅→V₈                        | Create file (text)                             |
|                                                      | V₈→S₃→V₄→S₃→V₂                  | Listen to audio file                           |
|                                                      | V₄→S₃→V₈                        | Create file (audio)                            |
|                                                      | V₈→S₂→V₃→S₂→V₂                  | Watch video file                               |
|                                                      | V₃→S₂→V₈                        | Create file (video)                            |
|                                                      | V₈→S₄→V₅,6,7                    | Save files                                     |
|                                                      | V₅,₆,₇→S₂→V₃                   | Display information on monitor                 |
|                                                      | V₅,₆,₇→S₂→V₃→S₂→V₂             | Watch information on monitor                   |
|                                                      | V₅,₆,₇→S₁→V₁                   | Print file (create paper document)             |
|                                                      | V₄→S₃→V₈→S₄→V₄→S₁→V₁           | Record audio information on carrier            |
|                                                      | V₅,₆,₇→S₁→V₁                   | Record video information on carrier            |
|                                                      | V₁→S₁→V₂→S₅→V₈                 | Scan paper document                            |
|                                                      | V₁→S₁→V₁                       | Store paper document (carrier)                 |
|                                                      | V₁→S₂→V₃                       | Provide access to examine content of document to unlimited scope of persons |
|                                                      | V₁→S₅→V₈→V₅→S₅→V₈→V₅,6,7       | Provide information carrier to unlimited scope of persons |
|                                                      | V₈→S₅→V₈                       | Process information                            |
| Protection goal                                                                 | Typical transformation operations | Examples of typical operations                                      |
|--------------------------------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------|
| Hide linear dimensions of the protected object                                | V1→S1→V2                          | Give tangible object to person                                       |
|                                                                                | V2→S1→V1                          | Return tangible object                                               |
|                                                                                | V2→S2→V3                          | Demonstrate external view of tangible object                         |
|                                                                                | V3→S2→V2                          | Examine external view of tangible object                             |
|                                                                                | V2→S3→V4                          | Voice information about linear dimensions of object                  |
|                                                                                | V4→S3→V2                          | Listen to information about linear dimensions of object              |
|                                                                                | V2→S5→V8                          | Create virtual model of tangible object (scan, photograph, draw, etc.)|
| Hide specific configuration of the protection object.                         | V1→S1→V2                          | Give tangible object to person                                       |
|                                                                                | V2→S1→V1                          | Return tangible object                                               |
|                                                                                | V2→S3→V4                          | Demonstrate external view of tangible object                         |
|                                                                                | V4→S3→V2                          | Examine external view of tangible object                             |
|                                                                                | V2→S5→V8                          | Create virtual model of tangible object (scan, photograph, draw, etc.)|

As an example, let us consider the creation of a part using a machine with computer numerical control (CNC). The decomposition of functional block 4 “Integrate control program” yields a subprocess depicted in Figure 1.

![Figure 1. Subprocess "Deploy control program" in IDEF0 notation.](image)

The process of initial data transformation on implementation of a control program is depicted in Figure 2.
Table 5 contains possible threats to the integrity in terms of a chosen information protection goal that can occur during transmission of the developed program into the machine tool memory.

Table 5. Main information security threats of integrity to the selected protecting information.

| Process       | Conversion description                                      | Class of integrity threat | Integrity Threat Description                                                                 |
|---------------|------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------------------|
| V1→S1→V2     | Handing over machine-readable medium with control program to CNC machine tool operator. | Impersonation of sender in medium state 1 | 1 CNC machine tool operator is underqualified to manufacture such part.                         |
|               |                                                            | Impersonation of sender in medium state 2 | 1 Machine-readable medium label is inaccurate and has no relation to stored information.       |
|               |                                                            | Substitution of information transmission channel | 1 Machine-readable medium contains control program for manufacturing another part.            |
|               |                                                            | Exposure on information transmission channel | 1 Machine-readable medium contains control program for manufacturing another part.            |
| V2→S1→V8     | Operator connects machine-readable medium to CNC machine tool | Impersonation of sender in medium state 1 | 1 Operator is not authorized to use CNC machine tool.                                         |
|               |                                                            | Impersonation of sender in medium state 2 | 1 Machine-readable medium misfits CNC machine tool.                                          |
|               |                                                            | Substitution of information transmission channel | 2 Operator uses unauthorized machine-readable medium                                       |
|               |                                                            | Exposure on information transmission channel | -                                                                                           |
| V2→S5→V8     | Operator copies information from machine-readable medium into CNC machine tool memory | Impersonation of sender in medium state 1 | 1 There is no control program on machine-readable medium                                        |
|               |                                                            | Impersonation of sender in medium state 2 | 2 The version of control program on machine-readable medium is outdated                      |
|               |                                                            | Substitution of information transmission channel | 3 Control program was compiled with errors                                                   |
|               |                                                            | Exposure on information transmission channel | 4 Control program contains errors in accuracy and configuration                               |
|               |                                                            |                          | 3 Control program format on machine-readable medium is unreadable                           |

3. Results
The level of details in the description of information handling process based on IDEF0 standard allows constructing a functional model, which will adequately describe real processes and account for significant factors affecting information. The factors of risk that pose threats to information security
are estimated to formulate final values of the factors of risk that characterize the total level of threat, potential damage and vulnerability of the protected object (vulnerability scales) [15].

4. Conclusion
The results of implemented methodology of functional modeling of an information process, with due regard to typical transformations of data in various media, is the complete list of threats to information security. In this case, the elaboration of measures against identified threats to information security is aimed at reaching the protection goal and absolutely objective as compared with the methods for information protection system construction on the basis of expert assessments.

Acknowledgments
This research was funded by the Ministry of Education and Science of Russia, Government Order no.2.8172.2017/8.9 (TUSUR).

References
[1] Novokhrestov A, Konev A, Shelupanov A, Egoshin N 2017 Threat model of information security and its media Bulletin of ISTU 12 131
[2] Shevcchenko N, Chick T, O’Riordan P, Scanlon T, Woody C 2018 Threat Modeling: A Summary of Available Methods Pittsburgh: Software Engineering Institute, Carnegie Mellon University D M18-0894
[3] Mead N, Forrest S, Krishnamurthy V and Ole V 2018 A Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University.
[4] Alhabeeb M, Almuhaideb A, Le P and Srinivasan B 2010 Information Security Threats Classification Pyramid IEEE 24th International Conference on Advanced Information Networking and Applications Workshops p 208
[5] Konyavskaya S 2013 On the issue of classification of information security objects Information Technology Security 3 14
[6] Shelupanov A, Evsyutin O, Konev A, Kostyuchenko E, Kruchinin D, Nikiforov D 2019 Information Security Methods – Modern Research Directions Symmetry p 150
[7] Bondar I, Kuznetsov M, Paklina A, Zolotarev V 2012 A method for modeling security threats to automated systems in a protected version Actual problems of aviation and cosmonautics 365
[8] Vernikov G. The main methodologies for survey organizations. IDEF0 standard. https://www.cfin.ru/vernikov/idef/idef0.shtml
[9] Konev A Approach to creation protected information model 2012 Reports of Tomsk State University of Control Systems and Radioelectronics pp 34–39
[10] Grant T, Burke I and van Heerde R 2012 Comparing Models of Offensive Cyber Operations Proceedings of the 7th International Conference on Information Warfare and Security p 108
[11] Shull F 2016 Evaluation of Threat Modeling Methodologies Software Engineering Institute, Carne-gie Mellon University
[12] Jouinia M, Ben Arfa Rabaia L, Ben Aissa 2014 Classification of security threats in information systems Procedia Computer Science 32 489–496
[13] Novokhrestov A, Konev A 2016 Mathematical model of threats to information systems Prospects of Fundamental Sciences Development, PFSD-2016. AIP Conf. Proc. 1772. 060015-1 – 060015-4.
[14] Konev A, Mineeva T, Solovev M 2018 Organizational processes regulated in the protection of critical information infrastructure Information and control systems in transport and industry pp 149–156
[15] Mikov D 2016 Identification of information risk factors of the telemedicine system Polytechnic youth magazine MSTU. N.E. Bauman p 1–8