symmetry

MDPI

Article

Model of Threats to the Integrity and Availability of Information Processed in Cyberspace

Nikolay Sergeevich Egoshin *, Anton Aleksandrovich Konev and Aleksandr Aleksandrovich Shelupanov

Faculty of Security, Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Prospect, 634000 Tomsk, Russia

* Correspondence: ens@fb.tusur.ru; Tel.: +7-(3822)-70-15-29

Abstract: Depending on their motivation, offenders have different goals, and disclosure of information is not always such a goal. It often happens that the purpose of the offender is to disrupt the normal operation of the system. This can be achieved both by acting directly on the information and by acting on the elements of the system. Actions of this kind lead to a violation of integrity and availability, but not confidentiality. It follows that the process of forming a threat model for the integrity and availability of information differs from a similar process for confidentiality threats. The purpose of this study is to develop an information integrity threat model that focuses on threats disrupting the normal operation of the system. The research methodology is based on the methods of system analysis, graph theory, discrete mathematics, and automata theory. As a result of the research, we proposed a model of threats to the integrity and availability of information. The proposed threat model differs from analogues by a high level of abstraction without reference to the subject area and identification of threats to the availability of information as a subset of threats to the integrity of the information transmission channel.

Keywords: information security; integrity; availability; threat model; information flow model

Citation: Egoshin, N.S.; Konev, A.A.; Shelupanov, A.A. Model of Threats to the Integrity and Availability of Information Processed in Cyberspace. *Symmetry* **2023**, *15*, 431. https://doi.org/10.3390/sym15020431

Academic Editors: Christos Volos and Sergei D. Odintsov

Received: 22 December 2022
Revised: 19 January 2023
Accepted: 30 January 2023
Published: 6 February 2023

1. Introduction

Throughout human history, information has been a valuable resource. Useful information was hidden and hidden from competitors. For many years, confidentiality was at the heart of information confrontation, but with the development of warfare, the attitude towards information as such has also changed. In certain situations, a violation of availability or integrity can cause much more harm than its disclosure. A natural question arose: why spend all the resources on ensuring confidentiality if the attacker's goal is solely sabotage? Determining the goals of an attacker is a separate issue, but one cannot focus on only one of the three basic aspects.

Modern society has reached the stage when the need to ensure a constant and uninterrupted connection to the information field to perform everyday and/or work tasks becomes more important than privacy requirements.

The widespread introduction of information technology has also affected the technology of document management within organizations and between them. Increasingly important in this area is becoming an electronic document management, which makes it possible to refuse paper carriers. The advantages of this approach are obvious: reducing the cost of processing and storing documents, fast search. In the era of the "information boom", this approach is obvious, and the only way out of the predicament associated with the growth of the volume of processed information.

However, the transition from paper to automation creates several problems related to ensuring the complete confidentiality of the document and authentication of the disclosure of its author.

Both the sender and the recipient of an electronic message need to ensure that the message has not been altered during its transmission. Workflow technologies must be

implemented in such a way that an attacker cannot deliberately distort the transmitted document. If distortions were made to the document, then its recipient should be able to recognize this fact. The problem of authenticating the authenticity of the author of a message is to ensure that no subject can sign a message under anyone else's name but their own. If they signed under a false name, then again, the recipient should be able to recognize this fact [1].

In a conventional paper workflow, these problems are solved because the information in the document and the author's handwritten signature are rigidly associated with the physical medium (paper). In this case, the elements that ensure the integrity of transmitted messages and the authenticity of authorship are handwritten signatures, seals, watermarks on paper, holograms, etc. For electronic document management, there is no rigid connection of information with a physical medium, and therefore, the development of other approaches is required to solve the problems listed above. It follows from this that the models of threats to confidentiality and integrity/availability have different justifications, which means that the solutions used to protect information depend on the aspect of information security [2,3].

Before forming a protection system and determining the mechanisms of its work, it is necessary to determine the list of threats. Determination of threats is one of the key stages in the formation of an information security system. At this stage, two points need to be made.

The model of information threats depends on the aspect under study: integrity threats are significantly different from confidentiality threats, while availability threats are a subset of the set of integrity threats.

From the point of view of electronic document management, the transmission channel is the same carrier of information: yes, we protect information, but at its core, electronic information is a kind of abstract object that is not directly affected, while it is the carrier that takes the whole "blow".

In this paper, we propose a new way to solve the problem—building a model of threats to integrity and availability, considering information transmission channels.

2. Background and Related Work

In connection with the development of technology and the rapid increase in the number of types of information transmission channels, the problem of accounting for these channels is becoming increasingly critical. In the context of this work, we will introduce the concept of an elementary information flow, which will symbolize a separate data transmission channel. A scheme consisting of such flows will be able to describe an information system in terms of the information circulating in it. Consider how this problem is viewed in various sources. While we will not consider how these threats are defined, we are interested in the attitude towards them, their typification, formulations, and applicability to the elements of the system.

First, we will consider such types of information systems, where it is the channels of information transmission that play the decisive role, and not the elements that process it. We refer to such systems, for example, cyber-physical systems (CPS), telemedicine systems, SCADA, IoT, software development systems. We will not dwell on each type but give a general overview of ideas on this problem.

Let us start with the fact that information flow is a fundamental concept underlying the security of a system and confidentiality of information in a system can be breached through unrestricted information flow [4] and at the same time access control and information flow-based policies for CPS security should be analyzed [5].

Along with information flow models, the Flow Diagrams via STRIDE or DREAD methodology are often proposed for use [6–14]. More specifically, the authors of [15] report that the Network is an important part of the system, along with Clients and Servers. It also happens that authors ignore threats directed specifically at the flow, although they use this term [16] and even completely ignore this topic [17].

The works [18,19] describe similar solutions that have one common drawback: the models consider threats directed directly to the channel, but the channel itself does not have a sufficiently complete description of its characteristics, which casts doubt on the completeness of the defined list of threats.

Separately, we singled out IoT systems, where the information transmission channel is an important working element [20]. For such systems, identification, assessment, and mitigation of risk will be more difficult and complex for cloud computing, mobile device toting, and consumerized enterprises [21].

Having studied all the mentioned works, one can notice that the research of the problem considered by the author has been going on for more than ten years, and the disputes in the scientific world on this issue do not subside. First, this is due to the heterogeneity of the information systems themselves. However, even if we leave the above set of the most popular types of systems, one can find many publications that also mention information flow models directly [22–24] or indirectly through the network [25–33]. The author of this work does not agree with this approach, because not every information flow is implemented by a network, but all networks implement flows. A network connection is only a particular kind of information flow. The very concept of flow is much more extensive and defines all possible channels of information transmission.

An interesting solution to the problem is the use of Hidden Markov Chains [34], however, this approach is more appropriate to use when identifying attacks rather than threats. An equally interesting option is the use of Petri Nets [35]. However, in the context of the current study, their application makes no sense, since Petri nets allow us to describe the process of information transfer, or rather the very fact of information transfer from one vertex to the channel and further, but do not allow us to describe the information transfer channel separately. To solve the current problem, a higher level of abstraction is needed, which will allow for describing a larger number of possible system states depending on the location of the information being processed.

Speaking about the practical applicability of what is being developed, we should mention [36]. This article speaks of the unconditional need to apply the application of machine learning methods for analyzing risks and threats to information security. The model of information flows proposed by the author of the current article implies a high level of abstraction with the ability to control the depth of the system description. With an increase in the depth of the system description, the number of elements in the scheme of information flows increases in direct proportion. Depending on the number of elements in the information system, the scheme may increase from a scale that is not processed by a person. Machine learning methods will come to the rescue, but it will be possible to talk about this in more detail when the models being developed go beyond theory and find their practical application.

Based on the results of the review part, it can be noted that DFD (Data Flow Diagram) is the most popular way to solve the indicated problem. However, this approach has two key drawbacks:

- the model has two separate notations for constructing schemes of internal and external interaction;
- the model does not describe the channels of information transmission and the resulting information flows.

The author agrees that the use of DFD allows us to fully describe the information system, however, further use of STRIDE takes us a little in the other direction, since STRIDE allows us to form a list of possible attacks, not threats. In his works, the author considers threats to be primary in relation to attacks. Each threat can be implemented by many attacks. It is necessary to adhere to the principle of "from smallest to largest". Comprehensive measures to combat threats are of a preventive nature. Threat coverage provides protection against a large layer of attacks. Therefore, the formation of a threat model is of paramount importance.

3. Information Flow Model

The threat model proposed in this paper is based on the information flow model. This model implies a description of the system using graph theory. Each information transmission channel in the system is represented as an elementary information flow, which includes three elements: a source, an information transmission channel, and a receiver. The elementary information flow is symmetrical and bidirectional, which means that in general there is no division of vertices into sources and receivers in the diagram. Using the following notation: V is a set of information carriers (a set of graph vertices), E is a set of information transmission channels (a set of graph edges), and by comparing any two elements from V and one from E, we get an elementary information flow in the form of an undirected graph with two vertices (Figure 1) [37].

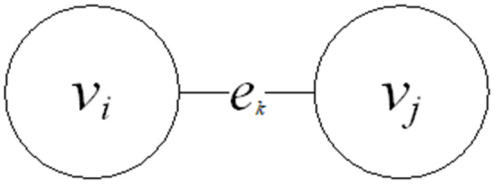

Figure 1. Elementary information flow.

Using the notation of graph theory, we describe the above information flow:

$$g = (v_i, e_z, v_j), \quad (1)$$

where v_i, v_j—information storage; e_z—information transition channel.

Considering the specifics of the study, namely the work with electronic information resources of the organization, certain sets were compiled.

The set of information carriers was divided into three subsets and took the form:

$$V = \{V_1, V_2, V_3\}, \quad (2)$$

where V_1—users set; V_2—software tools set; V_3—electronic resources set.

The set of channels has been instantiated to the following form:

$$E = \{E_1, E_2, E_3, E_4\}, \quad (3)$$

where E_1—set of transmission channels in the electromagnetic environment; E_2—set of transmission channels in a virtual environment; E_3—set of remote transmission channels in the electromagnetic environment; E_4—set of remote transmission channels in a virtual environment.

Now we need to get the full picture. Having an extended set V and a specified set E, it is possible to construct a set of all elementary information flows G. To do this, it is necessary to indicate some restrictions:

- an element of the set V_1 cannot refer to another element of this set;
- an element of the set V_3 cannot refer to another element of this set;
- an element of set V_1 cannot directly access an element of set V_3 and vice versa;
- remote information transmission channels are available only when an element of the set V_2 is connected to an element of the same set.

Considering all the above, the set of all elementary streams will have the following form:

$$G = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}, \quad (4)$$

where $g_1 = \{V_1, E_1, V_2\}$; $g_2 = \{V_1, E_2, V_2\}$; $g_3 = \{V_2, E_1, V_2\}$; $g_4 = \{V_2, E_2, V_2\}$; $g_5 = \{V_2, E_3, V_2\}$; $g_6 = \{V_2, E_4, V_2\}$; $g_7 = \{V_2, E_1, V_3\}$; $g_8 = \{V_2, E_2, V_3\}$.

The result of combining all the above graphs will be an undirected multigraph (Figure 2) [37], which will be a model of information flows when accessing electronic informa-

tion resources. It should be noted that the connections between each pair of vertices are symmetrical are bidirectional. When determining each individual elementary information flow, the direction of information movement in it does not matter, because we will be interested only in establishing a connection and transmitting information.

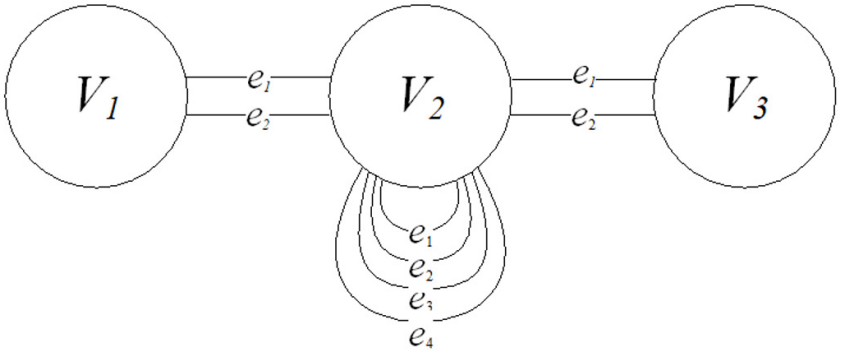

Figure 2. Information flow model in the form of a multigraph.

The developed model allows us to build a scheme of information flows, which, in addition to allowed flows, will include all possible manifestations of prohibited ones. We applied the information flow model to describe the process of exchanging electronic documents between two users via an FTP server (the general scheme of the described process is shown in Figure 3).

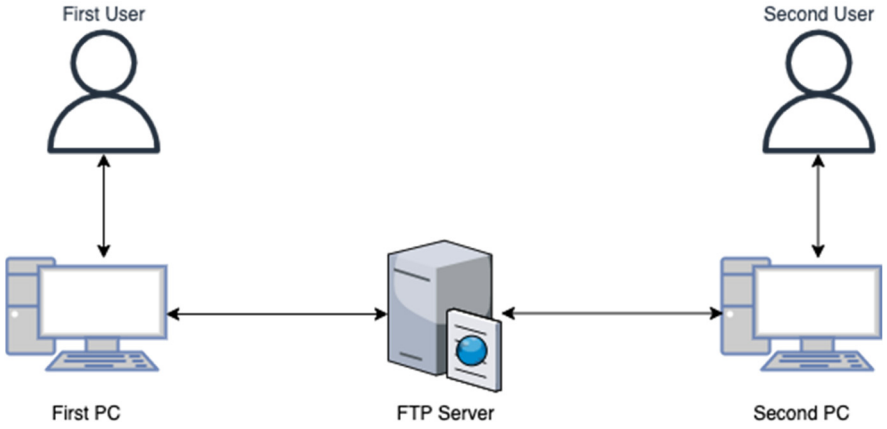

Figure 3. General scheme of the process of exchanging an electronic document via an FTP server.

General description of the document forwarding process:

- the first user creates an electronic document on the FTP server;
- in our case, the FTP server does not process the document, but only stores it;
- the second user accesses the electronic document on the FTP server.

To make a complete list of information flows, we added a few more explanations:

- users interact with the PC using the operating system;
- users interact with the FTP server using standard OS tools without specialized software; for convenience, we will combine the local FTP client with the operating system into one object;
- we will assume that the user interacts with the PC using PC's software and PC's I/O without specifying;
- we will assume that the remote virtual channel for computer interaction is the TCP/IP protocol family, and the electromagnetic one is the Ethernet family of technologies. In turn, the local communication channels inside the server are Server's software and Server's hardware, respectively.

Given all the above, the list of information flows will look like this:

1. First User—First PC's FTP client;
2. First PC's FTP client—Server's FTP client;
3. Server's FTP client—Server's data storage;
4. Server's data storage—Server's FTP client;
5. Server's FTP client—Second PC's FTP client;
6. Second PC's FTP client—Second User.

Now let us build from this list of information flows a complete list of elementary information flows. Each stream is divided into two elementary ones, since the model implies the division of the data transmission channel into electromagnetic and virtual. In addition, we introduced the designations of all participants in the process according to the model of information flows.

Users set:

$$V_1 = \left\{ v_1^1 , v_1^2 \right\}, \tag{5}$$

where v_1^1—first user; v_1^2—second user.

Software set:

$$V_2 = \left\{ v_2^1, v_2^2, v_2^3 \right\}, \tag{6}$$

where v_2^1—first PC's FTP client; v_2^2—second PC's FTP client; v_2^3—server's FTP client.

Storages of information:

$$V_3 = \left\{ v_3^1 \right\}, \tag{7}$$

where v_3^1—Server's data storage.

Set of local transmission channels in the electromagnetic environment:

$$E_1 = \left\{ e_1^1, e_1^2, e_1^3 \right\}, \tag{8}$$

where e_1^1—First PC's I/O, e_1^2—Server's hardware, e_1^3—Second PC's I/O.

Set of local transmission channels in a virtual environment

$$E_2 = \left\{ e_2^1, e_2^2, e_2^3 \right\}, \tag{9}$$

where e_2^1—First PC's software, e_2^2—Server's software, e_2^3—Second PC's software.

Set of remote transmission channels in the electromagnetic environment

$$E_3 = \left\{ e_3^1 \right\}, \tag{10}$$

where e_3^1—Ethernet.

Set of remote transmission channels in a virtual environment

$$E_4 = \left\{ e_4^1 \right\}, \tag{11}$$

where e_4^1—TCP/IP.

The final set of elementary information flows will have the following form:

$$S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}\}, \tag{12}$$

where $s_1 = (v_1^1, e_1^1, v_2^1)$; $s_2 = (v_1^1, e_2^1, v_2^1)$; $s_3 = (v_2^1, e_3^1, v_2^3)$; $s_4 = (v_2^1, e_4^1, v_2^3)$; $s_5 = (v_2^3, e_1^2, v_3^1)$; $s_6 = (v_2^3, e_2^2, v_3^1)$; $s_7 = (v_3^1, e_1^2, v_2^3)$; $s_8 = (v_3^1, e_2^2, v_2^3)$; $s_9 = (v_2^3, e_3^1, v_2^2)$; $s_{10} = (v_2^3, e_4^1, v_2^2)$; $s_{11} = (v_2^2, e_1^3, v_1^2)$; $s_{12} = (v_2^2, e_2^3, v_1^2)$.

As can be seen, the entire process of information transfer can be described using a set of elementary information flows, and in the construction of a complete scheme of information flows.

Therefore, concerning the example of exchanging documents via FTP, we illustrated the application of the information flows model. This analysis shows that the use of the model allows us to break any information transfer process into a finite set of elementary information flows, while the only difficulty lies in the correct description of the sets of system elements. The more fully and accurately the sets of elements are described, the more detailed the flow diagram will be.

Keep in mind that FTP is an exaggerated example. We deliberately chose this process to not pile up the article with huge sets. In practice, the scheme of information flows will contain a few connections beyond the limit for human processing. The scheme of information flows implies a description of all possible elements in the system of connections. In the most general case, we can use Formula (13) to calculate the total number of bounds.

$$N = \frac{n(n-1)}{2} \tag{13}$$

where N is the total number of bounds and n is the number of elements.

For $n = 2$ we get N equal 1 and for $n = 100$ we have 4950 bounds. However, all these calculations are valid only if each element really has a connection with each element. In practice, the scheme is limited to special cases and interactions of elements. Modification of the information system due to a change in the number of elements leads to a complete recalculation of the scheme of information flows. In any case, at this stage, the work is undergoing theoretical discussion and examination. The practical application of this approach requires a software solution, most likely using big data technologies and possibly machine learning methods. This activity is supposed to be a further development of the theory proposed by the author.

4. Model of Threats to the Integrity and Availability of Information

The issue of the study is related to the fact that, today, all available models of threats to information security are very conditional. There is no single principle for constructing a threat model. There are several approaches, and all of them have fundamental shortcomings, namely: the lack of a clear concept of a "threat model", a striking difference in the structures and principles of the functioning of models, methods of applying the model, redundancy of the model in the form of a merger with the model of the intruder, and much more.

The presence of these and some other gaps in existing approaches negatively affects the efficiency of the expert's work with the model itself and the result, due to the lack of standardized final assessments of one threat model relative to another. Therefore, the objective of this study is to create our own model of information threats.

The principle of building a threat model is based on the developed model of information flows, namely on the concept of an elementary information flow. Let us again turn to the definition of an elementary information flow, which is described by the formula:

$$g = (v_i, e_z, v_j), \tag{14}$$

where v_i, v_j—possible information storage; e_z—possible communication channel.

In this model, the information transmission channel is not some abstract object, but a very real element of the system, which has its own properties. It follows that it can be accessed in the same way as the other two elements of the stream.

Unauthorized access to information is access to protected information in violation of established rights and (or) access rules, leading to leakage, distortion, forgery, destruction, blocking access to information, as well as to loss, destruction, or failure of the information carrier (including number and channel of information transmission).

The very definition of unauthorized access implies the appearance in the system of a new element that will carry out this very access. Using the notation indicated earlier, this situation can be depicted as follows (Figure 4).

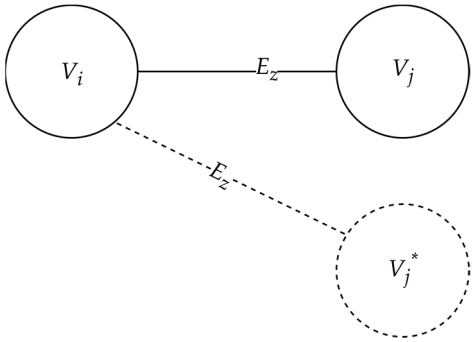

Figure 4. The emergence of an unauthorized element V_j*, which receives information from the element V_i.

A similar situation is possible for any element of the information flow. By analogy with the situation described above (Figure 2), access can be made both to an element of the set V_j and to E_z.

Interaction with elements of an elementary information flow leads to integrity and availability threats, and interaction with information circulating in this flow leads to confidentiality violation threats. Not all authors pay attention to this circumstance in their works. In most cases, it is said about the state of security of the information flow, without classifying possible impacts and consequences, which is necessary due to the different nature of the origin of the impact [38–40].

Three possible connections of a foreign element $V_j^* \rightarrow V_i$, $V_j^* \rightarrow V_j$, $V_j^* \rightarrow E_z$ describe situations in which there is a direct impact on one of the elements of the information flow, which can lead to distortion of information or its destruction.

From the foregoing, it follows that any of the three types of unauthorized influence can be exerted on any of the elements of an elementary information flow, and therefore on information:

- destruction;
- distortion;
- substitution.

Let us again turn to the concept of an elementary information flow and analyze the relationship between the types of influence on the elements of the flow with the classical aspects of information security: integrity and availability.

Applying to the tops of the stream:

- destruction of information on one of the vertices leads to a violation of the integrity of information;
- distortion of information on one of the vertices leads to a violation of the integrity of information;
- substitution of information on one of the vertices leads to a violation of the integrity of information.

Applying to the information transmission channel:

- destruction of information in the channel leads to a violation of availability;
- distortion of information in the channel leads to a violation of the integrity;
- substitution of information in the channel leads to a violation of availability.

Total: four threats to integrity and two to availability. It should be noted that the information flow has two symmetrical vertices, and any of them can be affected, which leads to the fact that the number of integrity threats directed to the vertex's doubles, which means that their total number becomes seven. Thus, having analyzed all possible types of impact on the information flow, we can build a complete set of typical threats to information integrity and availability (Table 1).

Table 1. Correlation of types of impact and the violated aspect.

Type of Impact	V_i	E_z	V_j
distortion	integrity	integrity	integrity
substitution	integrity	availability	integrity
destruction	integrity	availability	integrity

Set of integrity threats:

$$C = \{c_i | c \in C\}, i = \overline{1, 7}$$

where

c_1—substitution of the source V_i (transmission of distorted information to the element V_j);
c_2—substitution of the source V_j (transmission of distorted information to the element V_i);
c_3—substitution of the source V_i (destruction of information in the element V_j);
c_4—substitution of the source V_j (destruction of information in the element V_i);
c_5—substitution of the source V_i (substitution of information in the element V_j);
c_6—substitution of the source V_j (substitution of information in the element V_i);
c_7—impact on information during transmission over the E_z channel (distortion of information in the channel).

Denote the set of accessibility threats:

$$D = \{d_1, d_2\},$$

where

d_1—inoperability of the E_z channel—overload, destruction, inability to establish communication with the information carrier (complete lack of access to information by an authorized person);
d_2—"Noisy" channel E_z—interference (partial access to information by an authorized person).

Let us go back to the example presented earlier and apply typical threats to it.

Consider the first stream $s_1 = (v_1^1, e_1^1, v_2^1)$, where v_1^1—First User, e_1^1—First PC's I/O, v_2^1—first PC's FTP client.

Let us apply each of the nine threats to this stream. Let me remind you that the connecting channel in the flow is symmetrical and, accordingly, bidirectional.

When the c_1 threat is realized, the user v_1^1 is replaced by an unauthorized user v_1^{1*}, because of which this element can introduce distortions into the information stored in the v_2^1 element. The implementation of the threat is possible when the computer is used by a third party. An unauthorized user can, on behalf of an authorized user, upload a document with modified information.

When the c_2 threat is realized, the FTP client v_2^1 is replaced by unauthorized software v_2^{1*}, because of which the authorized user v_1^1 can receive distorted information. An example would be installing an app from an unverified source.

When the c_3 threat is realized, the user v_1^1 is replaced by an unauthorized user v_1^{1*}, because of which this element can destroy the information stored in the v_2^1 element. The implementation of the threat is possible when the computer is used by a third party. An unauthorized user using an FTP client can delete important documents.

When the c_4 threat is realized, the FTP client v_2^1 is replaced by unauthorized software v_2^{1*}, because of which the information with which the user directly interacts will be destroyed. An example would be installing an app from an unverified source.

When the c_5 threat is implemented, the user v_1^1 is replaced by an unauthorized user v_1^{1*}, because of which this element can replace the information stored in the v_2^1 element. The implementation of the threat is possible when the computer is used by a third party. An unauthorized user can, on behalf of an authorized user, upload a document with completely changed information to the server.

When the c_6 threat is realized, the FTP client v_2^1 is replaced by unauthorized software v_2^1*, because of which the authorized user v_1^1 can receive completely incorrect information. An example would be installing an app from an unverified source.

When the threat c_7 is realized, the information in the communication channel e_1^1 is influenced. In this case, the communication channel is the I/O device. An example is a hardware tab that distorts the output of information on the screen, for example, changes the displayed color.

When the threat d_1 is realized, an impact is made on the communication channel e_1^1, because of which the authorized user cannot gain access to this information. If we take an information output device as an example, then its complete inoperability can serve as an example of a threat implementation. The information is not compromised, but the user cannot access it.

When the threat d_2 is realized, an impact is made on the communication channel e_1^1, because of which the authorized user cannot get access to the information in full. Returning to the same example with the output device, an example of a threat implementation may be its partial inoperability because of the action of the tabs.

A similar selection of examples of the implementation of threats can be selected for any other flow and its elements, however, we will not present these analyses here, since this process is monotonous and, at the same time, will not allow us to better reflect the essence of the threat model.

Let us return to the set of elementary information flows and the sets of threats to integrity and availability. Knowing that both these sets are finite, we can apply each of the threats to each flow, i.e., compare each element of the sets C and D with each element of the set G and get a new set that will consist of all combinations of threats and flows, i.e., be their Cartesian product.

$$\mathrm{G} \times (\mathrm{C} \cup \mathrm{D}) = \left\{ g_i c_j, g_i d_k \middle| g \in \mathrm{G},\ c \in \mathrm{C},\ d \in \mathrm{D} \right\},\ i = \overline{1,\ 8},\ j = \overline{1,\ 7},\ k = \overline{1,\ 2}$$

$$|\mathrm{G}| * (|\mathrm{C}| + |\mathrm{D}|) = 8 * (7 + 2) = 72.$$

Now we classify and give a brief description of the identified typical threats. For convenience and readability, the set of typical threats was divided and grouped according to their belonging to information flows from the set G. In Tables 2–9 present the grouping and characteristics of the analyzed typical threats.

In Tables 5–8, the first two typical threats coincide in pairs, since these flows are symmetrical.

Table 2. Typical threats to the flow $g_1 = (\mathrm{V}_1, \mathrm{E}_1, \mathrm{V}_2)$.

	Description of the Threat	**Threat Example**	
c_1	Passing n/a information to an authorized process	distortion of electromagnetic information because of incorrect operation of I/O devices	g_1c_1
c_2	Transfer of information n/with the process to an authorized user	distortion of electromagnetic information because of incorrect operation of I/O devices	g_1c_2
c_3	Destruction of information processed by the process	distortion of electromagnetic information because of incorrect operation of storage devices	g_1c_3
c_4	Destruction of information processed by the user	action of software bookmarks that affect the output device	g_1c_4
c_5	Substitution of information processed by the process	passing false or incorrect data to the program	g_1c_5
c_6	Substitution of information processed by the user	action of software bookmarks that affect the output device	g_1c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	malfunction of the controller (errors in operation) of I/O devices; incorrect operation of I/O device elements	g_1c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	failure of the I/O device controller board; malfunction of hardware interfaces for connection and operation of I/O devices	g_1d_1
d_2	Lack of authorized access to information due to interference in the channel	partial loss of operability of the I/O device controller board; problems with hardware interfaces for connecting and operating I/O devices	g_1d_2

Table 3. Typical threats to the flow $g_2 = (V_1, E_2, V_2)$.

	Description of the Threat	Threat Example	
c_1	Passing n/a information to an authorized process	incorrect data entry	g_2c_1
c_2	Transfer of n/a information with the process to an authorized user	misinformation of a sanctioned person	g_2c_2
c_3	Destruction of information processed by the process	memory device error	g_2c_3
c_4	Destruction of information processed by the user	action of hardware tabs that affect the output device	g_2c_4
c_5	Substitution of information processed by the process	passing false or incorrect data to the program	g_2c_5
c_6	Substitution of information processed by the user	misinformation of a sanctioned person	g_2c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	use of a low-quality driver—unstable operation of I/O devices	g_2c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	lack of required I/O device driver	g_2d_1
d_2	Lack of authorized access to information due to interference in the channel	I/O device driver problems	g_2d_2

Table 4. Typical threats to the flow $g_3 = (V_2, E_1, V_2)$.

	Description of the Threat	Threat Example	
c_1	Passing n/a information to an authorized process	substitution of the address of the source process in RAM	g_3c_1
c_2	Transfer of n/a information with the process to an authorized process	substitution of the address of the source process in RAM	g_3c_2
c_3	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_3c_3
c_4	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_3c_4
c_5	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_3c_5
c_6	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_3c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	unstable operation of RAM elements	g_3c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	failure of memory elements	g_3d_1
d_2	Lack of authorized access to information due to interference in the channel	RAM malfunctions—the appearance of bad sectors	g_3d_2

Table 5. Typical threats to the flow $g_4 = (V_2, E_2, V_2)$.

	Description of the Threat	Threat Example	
c_1	Passing n/a information to an authorized process	spoofing the address of the source process	g_4c_1
c_2	Transfer of n/a information with the process to an authorized process	spoofing the address of the source process	g_4c_2
c_3	Destruction of information processed by the process	storage device driver problems	g_4c_3
c_4	Destruction of information processed by the process	storage device driver problems	g_4c_4
c_5	Substitution of information processed by the process	changing the address of the receiving process	g_4c_5
c_6	Substitution of information processed by the process	changing the address of the receiving process	g_4c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	incorrect operation of interprocessor communication tools	g_4c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	inoperability of interprocessor communication means—shared memory, signals, channels	g_4d_1
d_2	Lack of authorized access to information due to interference in the channel	errors in the distribution of interprocessor communication means—shared memory, signals, channels	g_4d_2

Table 6. Typical threats to the flow $g_5 = (V_2, E_3, V_2)$.

	Description of the Threat	Threat Example	
c_1	Remote passing n/a information to an authorized process	n/a change the operating parameters of the software (remotely)	g_5c_1
c_2	Remote transfer of n/a information with the process to an authorized process	n/a change the operating parameters of the software (remotely)	g_5c_2
c_3	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_5c_3
c_4	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_5c_4
c_5	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_5c_5
c_6	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_5c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	errors in the operation of hardware interfaces for connecting and operating network devices	g_5c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	overload/damage of the communication line; malfunction of hardware interfaces for connecting and operating network devices	g_5d_1
d_2	Lack of authorized access to information due to interference in the channel	the occurrence of interference in the communication line; network device errors	g_5d_2

Table 7. Typical threats to the flow $g_6 = (V_2, E_4, V_2)$.

	Description of the Threat	Threat Example	
c_1	Remote passing n/a information to an authorized process	covert remote connection to authorized software	g_6c_1
c_2	Remote transfer of n/a information with the process to an authorized process	covert remote connection to authorized software	g_6c_2
c_3	Destruction of information processed by the process	storage device driver problems	g_6c_3
c_4	Destruction of information processed by the process	storage device driver problems	g_6c_4
c_5	Substitution of information processed by the process	changing the address of the receiving process	g_6c_5
c_6	Substitution of information processed by the process	changing the address of the receiving process	g_6c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	network card driver errors; network packet loss	g_6c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	network device driver problems: lack of required protocol	g_6d_1
d_2	Lack of authorized access to information due to interference in the channel	partial loss of link functionality—network device driver error	g_6d_2

Table 8. Typical threats to the flow $g_7 = (V_2, E_1, V_3)$.

	Description of the Threat	Threat Example	
c_1	Transfer of n/a information to the process	reading incorrect information from n/a file (loading an exploit)	g_7c_1
c_2	Recording n/a information on a storage	n/a changing a protected file (malicious, fake programs)	g_7c_2
c_3	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_4c_3
c_4	Destruction of information stored on a storage	persistent storage problems	g_4c_4
c_5	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_4c_5
c_6	Substitution of information stored on a storage	n/a change of information stored on the storage medium	g_4c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	incorrect operation of digital media recording/reading elements	g_7c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	failure of devices for reading/writing digital media information	g_7d_1
d_2	Lack of authorized access to information due to interference in the channel	partial loss of functionality of the controller board; media write/read elements; malfunctions of hardware interfaces for connecting and operating information storage devices; hard drive read head problems	g_7d_2

Table 9. Typical threats to the flow $g_8 = (V_2, E_2, V_3)$.

	Description of the Threat	Threat Example	
c_1	Transfer of n/a information to the process	reading incorrect information from n/a file (file substitution)	g_8c_1
c_2	Recording n/a information on a storage	n/a changing a protected file (malicious, fake programs)	g_8c_2
c_3	Destruction of information processed by the process	RAM malfunctions, unexpected shutdown of the software	g_4c_3
c_4	Destruction of information stored on a storage	persistent storage problems	g_4c_4
c_5	Substitution of information processed by the process	substitution of the address of the receiver process in RAM	g_4c_5
c_6	Substitution of information stored on a storage	n/a change of information stored on the storage medium	g_4c_6
c_7	Impact on information during its transmission over a channel in an electromagnetic environment	using the wrong media driver	g_8c_7
d_1	Lack of authorized access to information due to the impossibility of establishing a communication channel	storage driver failure	g_8d_1
d_2	Lack of authorized access to information due to interference in the channel	storage device driver problems	g_8d_2

Thus, a list of 72 typical threats to the integrity and availability of information processed in a computer system was compiled.

It is necessary to clarify once again that this list is not a complete list of threats:

- firstly, within the framework of this study, only threats to integrity and availability are considered;
- secondly, given the fact that technologies are developing at an accelerating pace, we cannot accurately predict which I/O devices, storage, or transmission devices will exist in principle in a few years, let alone determine the full list of threats to information that will be processed using devices that do not exist anymore. This problem is well disclosed in [41]. This review article shows the dynamics of the use of various information transfer technologies with the development of information systems. In any case, all the mentioned technologies have already used element base. Therefore, at the abstract level, they can be reduced to the same sets that are indicated in the information flow model.

With all this, we can say with confidence that the set of typical threats will remain unchanged, since the apparatus used on the basis of the threat model has a high degree of abstraction and is based on graph theory, and not on objects of the real world. Within the framework of the model, any device is presented as an information transmission channel, regardless of its implementation. The specialist is only required to "not forget" about this channel (device) at the time of describing the entire system. The introduced abstraction allows us to describe the system down to the minimum level of element interaction. The specialist determines the depth of a detailed description of the system independently, depending on the feasibility and requirements.

5. Conclusions

During this research, we presented the application of the information flows model to describe the information exchanging process. The developed approach allows us to describe any process of information transfer in an information system and the information system itself at any desired level of depth. The depth level can be chosen by a specialist at their discretion. Additionally, we presented the integrity and availability threat model, which has practical applicability in information security processes.

The proposed information threat model based on the information flow model mentioned above also has a high level of abstraction inherited from the basic model. The threat model contains 72 typical threats to the integrity and availability of information.

Additionally, the proposed model differs from analogues in the following ways:

- the set of typical threats is not infinite;
- threats have a clear classification according to the object of access;

- the presence of a list of examples of the implementation of threats, the expansion of which will not affect the quality of the model in any way.

The use of a finite list of typical threats reduces the influence of the subjective opinion of an expert, narrowing the scope of the search for used threats and attacks. The results of scientific research have a high potential for practical use, together with modern machine learning methods, to identify typical threats to information security for each of the elements of any information system.

Author Contributions: N.S.E., A.A.K. and A.A.S. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of Science and Higher Education of Russia, Government Order for 2020–2022, project no. FEWM-2020-0037 (TUSUR).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no competing interests.

References

1. Shelupanov, A.; Evsyutin, O.; Konev, A.; Kostyuchenko, E.; Kruchinin, D.; Nikiforov, D. Information Security Methods—Modern Research Directions. *Symmetry* **2019**, *11*, 150. [CrossRef]
2. Novokhrestov, A.; Konev, A.; Shelupanov, A.; Buymov, A. Computer network threat modelling. *J. Phys. Conf. Ser.* **2020**, *1488*, 1. [CrossRef]
3. Novokhrestov, A.; Konev, A.; Shelupanov, A. Model of Threats to Computer Network Software. *Symmetry* **2019**, *11*, 1506. [CrossRef]
4. Akella, R.; Tang, H.; McMillin, B. Analysis of information flow security in cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 157–173. [CrossRef]
5. Burmester, M.; Magkos, E.; Chrissikopoulos, V. Modeling security in cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 118–126. Available online: https://api.semanticscholar.org/CorpusID:11664905 (accessed on 1 November 2022). [CrossRef]
6. Pendergrass, J.C.; Heart, K.; Ranganathan, C.; Venkatakrishnan, V.N. A Threat Table Based Approach to Telemedicine Security. In Transactions of the International Conference on Health Information Technology Advancement. 2013. ScholarWorks at WMU. Available online: https://api.semanticscholar.org/CorpusID:3329736 (accessed on 1 November 2022).
7. Seifert, D.; Reza, H. A Security Analysis of Cyber-Physical Systems Architecture for Healthcare. *Computers* **2016**, *5*, 27. [CrossRef]
8. Ruiz, G.; Heymann, E.; César, E.; Miller, B.P. Automating Threat Modeling through the Software Development Life-Cycle. *XXIII Jorn. Paralelismo* **2012**, 21–38. Available online: https://api.semanticscholar.org/CorpusID:14252675 (accessed on 1 November 2022).
9. Pan, J.; Zhuang, Y. PMCAP: A Threat Model of Process "Memory Data on the Windows Operating System". *Secur. Commun. Netw.* **2017**, *2017*, 4621587. [CrossRef]
10. Li, X.; He, K.; Feng, Z.; Xu, G. Unified threat model for analyzing and evaluating software threats. *Secur. Commun. Netw.* **2014**, *7*, 1454–1466. [CrossRef]
11. Baquero, A.O.; Kornecki, A.; Zalewski, J. Threat modeling for aviation computer security. *CrossTalk* **2015**, *28*, 21–27. Available online: https://www.researchgate.net/publication/298822749 (accessed on 1 November 2022).
12. Olayemi, O.; Väänänen, A.; Haataja, K.; Toivanen, P. Security issues in smart homes and mobile health system: Threat analysis, possible countermeasures and lessons learned. *Int. J. Inf. Technol. Secur.* **2017**, *9*, 31–52. Available online: https://erepo.uef.fi/handle/123456789/5124 (accessed on 1 November 2022).
13. Kamatchi, R.; Ambekar, K. Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models. *Indian J. Sci. Technol.* **2016**, *9*, 1–7. [CrossRef]
14. Xiong, W.; Krantz, F.; Lagerström, R. Threat Modeling and Attack Simulations of Connected Vehicles: A Research Outlook. *ICISSP* **2019**. [CrossRef]
15. Almulhem, A. Threat Modeling for Electronic Health Record Systems. *J. Med. Syst.* **2011**, *36*, 2921–2926. [CrossRef]
16. Yeboah-Ofori, A.; Islam, S. Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet* **2019**, *11*, 63. [CrossRef]
17. Yan, B.; Li, X.; Du, Z. A Threat Model-Driven Security Testing Approach for Web Application. *Contemp. Res. E-Bus. Technol. Strategy* **2012**, 158–168. [CrossRef]
18. Arokia, J.K.I.; Prabakaran, R. Threat Modeling Framework for Electrical Distribution SCADA Networks. *MEJSR* **2015**, *23*, 2318–2325. [CrossRef]
19. Cardenas, A.A.; Roosta, T.; Sastry, S. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Netw.* **2009**, *7*, 1434–1447. [CrossRef]
20. Shelupanov, A.; Konev, A.; Kosachenko, T.; Dudkin, D. Threat Model for IoT Systems on the Example of OpenUNB Protocol. *IJATCSE* **2019**, *7*, 283–290. [CrossRef]

21. Ingalsbe, J.A.; Shoemaker, D.; Mead, N.R. Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise—An overview of considerations. *AMCIS* **2011**. Available online: https://aisel.aisnet.org/amcis2011_submissions/359 (accessed on 1 November 2022).
22. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2010**, *16*, 3–32. [CrossRef]
23. Brown-White, J.; Cobb, L.B.; DelGrosso, J.; Foroughi, E.; Ganjali, A.; Moghnie, S.; Ozmore, N.; Padmanabhan, R.; Schoenfield, B.; Tarandach, I.; et al. Tactical threat modeling. *Safecode* **2019**. Available online: https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf (accessed on 1 November 2022).
24. Torr, P. Demystifying the Threat-Modeling Process. Security & Privacy. *IEEE Secur. Priv.* **2005**, *3*, 66–70. [CrossRef]
25. Xu, D.; Pauli, J. Threat-driven design and analysis of secure software architectures. *J. Inf. Assur. Secur.* **2006**, *1*, 171–180. Available online: https://api.semanticscholar.org/CorpusID:17006191 (accessed on 1 November 2022).
26. Chen, X.; Liu, Y.; Yi, J. A security evaluation framework based on STRIDE model for software in networks. *Int. J. Adv. Comput. Technol.* **2012**, *4*, 269–278. Available online: https://api.semanticscholar.org/CorpusID:14340680 (accessed on 1 November 2022).
27. Jouini, M.; Rabai, L.B.A.; Ben Aissa, A. Classification of security threats in information systems. *Int. Conf. Ambient. Syst. Netw. Technol.* **2014**, *32*, 489–496. [CrossRef]
28. Lavrova, D.S.; Pechenkin, A.I. Adaptive reflexivity threat protection. *Autom. Control. Comput. Sci.* **2015**, *49*, 727–734. [CrossRef]
29. Kammuller, F.; Probst, C.W. Modeling and Verification of Insider Threats Using Logical Analysis. *IEEE Syst. J.* **2015**, *11*, 534–545. [CrossRef]
30. Suleiman, H.; Alqassem, I.; Diabat, A.; Arnautovic, E.; Svetinovic, D. Integrated smart grid systems security threat model. *Inf. Syst.* **2015**, *53*, 147–160. [CrossRef]
31. Falah, B.; Akour, M.; Oukemeni, S. An Alternative Threat Model-based Approach for Security Testing. *Int. J. Secur. Softw. Eng.* **2015**, *6*, 50–64. [CrossRef]
32. Sharma, A.; Gandhi, R.; Zhu, Q.; Mahoney, W.R.; Sousan, W. A social dimensional cyber threat model with formal concept analysis and fact-proposition inference. *Int. J. Inf. Comput. Secur.* **2013**, *5*, 301. [CrossRef]
33. Li, X.; Liu, R.; Feng, Z.; He, K. Threat modeling-oriented attack path evaluating algorithm. *Trans. Tianjin Univ.* **2009**, *15*, 162–167. [CrossRef]
34. Granstrom, K.; Willett, P.; Bar-Shalom, Y. Asymmetric Threat Modeling Using HMMs: Bernoulli Filtering and Detectability Analysis. *IEEE Trans. Signal Process.* **2016**, *64*, 2587–2601. [CrossRef]
35. Zegzhda, P.D.; Zegzhda, D.P.; Kalinin, M.O.; Konoplev, A.S. Security Modeling of Grid Systems Using Petri Nets. *MMM-ACNS* **2012**, 299–308. [CrossRef]
36. Radanliev, P.; De Roure, D.; Walton, R.; Van Kleek, M.; Montalvo, R.M.; Maddox, L.; Santos, O.; Burnap, P.; Anthi, E. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. *SN Appl. Sci.* **2020**, *2*, 1773. [CrossRef]
37. Egoshin, N.; Konev, A.; Shelupanov, A. A model of threats to the confidentiality of information processed in cyberspace based on the information flows model. *Symmetry* **2020**, *12*, 1840. [CrossRef]
38. Mouna, J.; Latifa, B.A. Threat classification: State of art. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*; IGI Globa: lHershey, PA, USA, 2016; Available online: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art (accessed on 1 November 2022).
39. Ruf, L.; Thorn, A.; Christen, T.; Gruber, B.; Portmann, R.; Luzer, H. Threat Modeling in Security Architecture—The Nature of Threats. In ISSS Working Group on Security Architectures. 2008. Available online: https://scribd.com/document/47730732/ISSS-AG-Security-Architecture-Threat-Modeling-Lukas-Ruf (accessed on 1 November 2022).
40. Geric, S.; Hutinski, Z. Information system security threats classifications. *J. Inf. Organ. Sci.* **2007**, *31*, 1. Available online: https://jios.foi.hr/index.php/jios/article/view/29 (accessed on 1 November 2022).
41. Radanliev, P.; De Roure, D. New and emerging forms of data and technologies: Literature and bibliometric review. *Multimed. Tools Appl.* **2023**, *82*, 2887–2911. [CrossRef]