Threats of information security in the application of GIS in the interests of the digital economy

V G Burlov¹, V V Gryzunov¹ and T M Tatarnikova¹,²

¹ Department of Information Technology and Security Systems, Russian State Hydrometeorological University, Voronezhskaya str., 79, Saint-Petersburg, 192007, Russian Federation
² The reported study was funded by Russian Ministry of Science (information security)

E-mail: burlovvg@mail.ru, viv1313r@mail.ru, tm-tatarn@yandex.ru

Abstract. The development of a digital economy is impossible without the use of geographic information systems (GIS). On the other hand, the use of GIS entails the implementation of new threats. The article analyses possible threats, the requirements of regulators, formulates the necessary and sufficient conditions for ensuring security when using GIS.

1. Introduction
The transfer of the economies of countries to digital way requires the digitalization of data, on the basis of which decisions are made on the production, delivery and sale of products. That's why, the projects "Safe City", "Digital Economy", "Reform of control and supervision activities" "Digital Ocean", "Digital Silk Road" [2] and production moves to Industry 4.0 [3] were appeared, etc. Almost all technologies of the digital economy are based on the use of an appropriate geographic information system (GIS).

GIS is an information system operating with spatial data [4]. And there is an opinion [5] that in the future, all information systems will be GIS.

High reaction rates and the number of services provided in the digital economy determine the following features of GIS.

• work in real time or close to real time;
• a constant increase in the number of layers, today, GIS has several hundred layers;
• usually GIS itself is not used and does not perform any actions, but provides data for analysis, allocation of money, geomonitoring, investigation of computer crimes, etc. [6,7], ie in fact, it is an element of the support and decision-making system [8,9] or “smart card” [10].

These features force to increase the productivity of GIS several times every 2–4 years, integrate GIS with other information systems [1], which in turn, firstly, opens up GIS for a wide range of users and dramatically increases the number of tasks solved by GIS, second, makes GIS an object of malicious actions on the part of computer hooligans, criminal gangs, special services, etc. Both that, and another destabilize the work of GIS, i.e. reduces the probability of achieving targets and leads to financial, environmental, social and moral damage [11].

The foregoing testifies to the fact that almost every citizen in particular and society as a whole have become dependent on how reliably and safely the GIS performs the tasks assigned to it.
The purpose of this study is to systematize and substantiate threats to the security of GIS information, as well as to formulate the necessary and sufficient conditions for ensuring the security of information in GIS.

2. GIS model substantiating the necessary and sufficient condition for the security operation of GIS

2.1. Existing approaches to describe information security threats

Under the threat to the security of information (threat of IS) we mean a set of conditions and factors that create a potential or real danger of breaching information security [12].

The list of factors affecting the security of information is given in [13]. The completeness and reliability of the above factors are achieved through a complete consideration of the many factors affecting all elements of the object of informatization at all stages of information processing. That is, in principle, a complete list of threats for a specific GIS implementation can be obtained by an information security specialist based on the selection of suitable factors among the available ones. There is a draft methodology for determining threats to information security in information systems that do not process state secrets, developed by FSTEC [14].

The recommendations set out in [15] will help to avoid a large number of typical mistakes when creating GIS. This is some quintessential of the experience of information security specialists. A similar approach to creating secure GIS is used in other countries [16].

Another possible approach to describe GIS threats is to use a vulnerability description language, for example, Common Vulnerability Scoring System [17]. Description is being made by information security specialists.

Information security intruder is an individual or a logical object who accidentally or intentionally committed an action, the consequence of which is a violation of the information security of an organization [18].

When compiling a model of an intruder, there are two approaches [19]:

1) compensatory, in which a list of possible actions of an intruder is made, possible risks are calculated and a list of necessary information protection means (SIS) is selected;

2) possibilitory, make up a list of possible consequences of the attacker’s actions and develop a list of information system reactions that neutralize the consequences.

The possibilitory approach is also used when a situation arises in which GIS resources are insufficient to solve the assigned tasks: failures / failures, a sharp increase in the number of tasks being solved, etc. This causes a Denial of Service (DoS), i.e. the availability of GIS services is disrupted. As a result of DoS, both the integrity and confidentiality of the processed data can be violated. Thus, too much task flow can also be seen as a GIS security intruder.

Intruders acting accidentally (failures / haltings of GIS elements) and unintentionally (inexperienced or overly curious GIS users), are well studied and described by stochastic models of various theories: reliability, stability, survivability, information security, etc. Aggressive purposeful actions the intruder cannot be described by stochastic models [20]. Control theory tools are suitable for dealing with such an intruder.

Considering GIS as a managed object with a structure, we can say that the intruder affects the structure or functions of the GIS [21], which means that all GIS threats are divided into threats to the structure and / or threats to GIS functions.

The intruder’s actions on the structure are expressed in the change in the number of elements or links.

The impact on functions entails a denial of service or a decrease in the reliability of the system, using a functional reserve.

**Axiom 1.** Intruder $\Psi$ can only affect GIS functions $\Psi_F$ and / or structure $\Psi_S$ GIS:

$$\Psi = \Psi_F \cup \Psi_S.$$  

The intruder model is presented in more detail in [21].
The above methods of protecting information are a necessary but insufficient condition for protection. This means that if at least one of the threats is not "closed" by SIS, then all information security specialists will say that the GIS is vulnerable. However, even if all threats are “closed” by the SIS, no one can guarantee that the information is sufficiently protected.

The question of formulating the necessary and sufficient conditions for the security of information is rather complicated and requires the creation of a special GIS model.

We will argue that for GIS it is not the semantic content of the tasks being performed that is essential, but information about what resources, when and for how long should be provided. Such a tasks presentation allows us to formulate an indicator of the efficiency of the GIS functioning

2.2. GIS functioning efficiency indicator

Before creating any system, it is necessary to understand how the effectiveness of its functioning will be assessed, i.e. an efficiency indicator is needed [22]. Let it be the GIS performance, i.e. the ability of GIS to solve the assigned tasks in the required time (I), because the user is important to solve his own problems, and he does not care why the GIS is not able to meet his needs [23].

The indicator presented in [24] is closest to this approach. However, this indicator, firstly, concerns only the effectiveness of the information security system, and not the entire system, which is not very suitable for a user who is interested in the execution of tasks by the entire system, and secondly, it is probabilistic, and therefore is not suitable for describing an aggressive purposed environment, thirdly, to calculate it, it is necessary to use simulation modeling, which is not always possible.

Applying the above representation of tasks in GIS, it can be argued that the overall performance of a GIS depends on the performance of individual GIS elements, the ways of their interconnection. Indeed, linking GIS elements in different ways, and distributing them among GIS tasks, we obtain different performance of the entire GIS [23].

From the point of control theory view, I is a controlled value, the purpose of control is such an arrangement of GIS elements in space and the organization of connections between them (Q) so that I takes the required value (I*).

It is proposed to base the control algorithms on the integrity conservation law.

2.3. The keep law of an object integrity

The law states that in any properly constructed system there is a stable repeating connection between the system and its actions, an indicator of efficiency and the environment, manifested in the mutual transformation of the properties of an object and the properties of its action [25-27].

Controlling the placement of GIS elements in space and the organization of connections between them based on the keep law of an object integrity means that at each moment of time the equality is fulfilled:

\[ I(Q) = F(Q, \Phi(R, U), t) \]  

(1),

where

I – indicator of GIS efficiency, presentation of the required number of required symbols at the required time (drawing electronic maps, displaying real estate data, reflecting weather conditions, etc.)

Q – the set of required spatio-temporal GIS states (GIS model) is set by the metasystem / GIS creator. Shows how exactly GIS elements should interact with each other and with the consumer of GIS services. In the general case, it is a function of time and is set in various ways: by enumeration, analytically, by specifying characteristic properties, etc.;

\( \Phi \) – the set of current spatio-temporal states of the GIS, is a model of the current situation (the current situation C is the set of the current state of the object (state vector X) and its external environment (vector of disturbances F) [28]), shows how the elements of the GIS interact with each other and the consumer of GIS services in fact;

R – set of GIS elements performances (model of actions of system elements in space-time);

U – set of control actions on GIS elements;

\( t \) – is the GIS operation time;
F – is an operator expressing the basic conformities of the existence of a GIS.

The GIS control system actually "assemble" the performance of individual GIS elements in such a way as to ensure the achievement of the required I*, i.e. adapts GIS to the impact of the environment, in the case of information security - to the intruder actions.

**Constraint 1.** Consider passive adaptation, i.e. GIS cannot actively change the environment of its functioning [29].

**Constraint 2.** GIS does not adapt the controlled value (I).

Consider how integrity affects the security of an GIS. It is important to remember here that the main task of the attacker is to make the attacked system work in its own interests [30]. The intruder can only influence R, as a result, ΔΦ is formed, and as a consequence, ΔI. The task of the GIS control system is to form ΔU and ΔQ such as to reduce ΔI to zero.

\[ \Delta R, \Delta \Phi \to 0 \Rightarrow \Delta U, \Delta Q: \Delta I \to 0 \]

**Axiom 2.** The set of required spatio-temporal GIS states (Q) and the set of control actions (U) are formed by the metasystem. If the intruder modifies Q or U, he is acting on behalf of the metasystem.

As an illustration of axiom 2, antivirus can be used. Antivirus usually works from the level of the computer's operating system and acts as a metasystem. It decides what is a virus and what is not. But if the “SubVirt” rootkit is loaded into the computer, then it becomes a metasystem for the antivirus, creates an environment for its operation and limits the antivirus in deciding what is a virus and what is not.

The interaction between the intruder and the information system within the same level is discussed in more detail in [31].

A schematic GIS model built on the basis of the keep law of integrity is shown in figure 1.

![Figure 1. GIS model built on the basis of the keep law of object integrity.](image)

It follows from the model that ΔI can be formed not only due to aggressive targeted actions of the intruder, but also when the mode of operation changes, for example, a unexpected increase in the number of tasks solved by GIS. In this case, the GIS is “choked up” and the user does not receive the service he expects.

Let us formulate a necessary and sufficient condition for the information security in a GIS.

2.4. **Necessary and sufficient condition for information security in GIS**

In order for information in GIS to be processed safely, it is necessary and sufficient that the GIS is built on the basis of the keep law of object integrity (has integrity).

GIS, using basic conformity, forms Q (t) and compares with \( \Phi (t) \). If \( Q (t) \equiv \Phi (t) \), then the GIS works normally. Otherwise, the intruder acts in the system.

Necessity of the condition. There is defined \( I^* \) when designing and manufacturing GIS, proceed from the assumption that information security must be observed in the process of GIS operation, Q and U based on available R are formed (see axiom 2).
Sufficiency of the condition. The intruder affects only R. Since the GIS is built taking into account the keep law of integrity, this will cause ΔΦ and will be detected. The control system will change U and Q, which negates the actions of the intruder.

The approach presented in the article is illustrated by the ancient military wisdom: "If you act flawlessly, it's impossible to beat you, you can win only if the enemy makes mistakes".

3. Conclusion

Thus, the existing approaches to identify and neutralize threats are fragmented and based on the experts’ opinion. Application of the keep law of integrity allows to systematically detect all possible threats to the information security of GIS and respond to them automatically. Therefore, the main threat to information security is to lose integrity. The search and application of specific basic conformities of GIS construction require further development.

References

[1] Kudelkin V A and Denisov V F 2017 Experience of integration of distributed information systems IT standard 1 24–30 (in Russian)
[2] Stoletov O V, Chikharev I A, Moskalenko O A and Makovskyaya D V 2019 Geoinformation support of the mediterranean branch of the silk road Geoinformatical and cartographical security of ecological, economic and social aspects of sustainable development part 25 1 102–113 (in Russian)
[3] Schwab K 2019 Globalization 4.0. New architecture for the fourth industrial revolution Eurasian integration: economics, law, politics 1 (27) 79–84
[4] GOST R 52438-2005 Geographical information systems Terms and definitions (in Russian)
[5] Kolbanev M O, Palkin I I and Tatarnikova T M 2020 The challenges of the digital economy Hydrometeorology and ecology. Scientific notes RSHMU 58 156–167 (in Russian)
[6] Ananiev Yu S 2003 Geoinformation systems: tutorial (Tomsk: Pub. TPU) 70 (in Russian)
[7] Boltachev E F 2018 Visualization of data describing information technologies crimes Crime in the sphere of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes 1 (4) 14–19 (in Russian)
[8] Voronin A V and Zatsarinny A A 2019 Geoinformation system as the most important component of management decision making system Highly Available Systems 15 (3) 27–33 (in Russian)
[9] Lisitsky D V and Katsko S Yu 2016 User segment of a single territorial geoinformation space Bulletin of SGUGiT Release 4 (36) 89–100 (in Russian)
[10] Yankelevich S S, Radchenko L K and Antonov Ye S 2018 From multi-purpose cartographic resource to «smart map» Bulletin of SGUGiT 23 (1) 142–155 (in Russian)
[11] Nesterovskij I P and Yazov Yu K 2015 Possible approach to assessment of damage suffered from a threat to security of information being processed in federal information systems Cybersecurity issues 2 (10) 20–25 (in Russian)
[12] GOST R 50922-2006 Information security Basic terms and definitions (in Russian)
[13] GOST 51275-2006 Factors affecting information General Provisions (in Russian)
[14] FSTEC Methodology for determining threats to information security in information systems (in Russian)
[15] GOST R 51583-2014 Information protection. Sequence of protected operational system formation. General provisions (in Russian)
[16] Ageev V O and Shilov A K 2015 Protection sis in the foreign and domestic system VI All-Russian school-seminar «Perspective-2015» 313–315 (in Russian)
[17] Common Vulnerability Scoring System SIG: https://www.first.org/cvss
[18] GOST R 53114-2008 Information security Ensuring information security in the organization Basic terms and definitions (in Russian)
[19] Gryzunov V V 2018 Model of Purpose Aggressive Actions on the Information-Computing...
System Third International Conference on Human Factors in Complex Technical Systems and Environments (ERGO) 300–305
https://ieeexplore.ieee.org/document/8443814

[20] Kalinin V N 2011 Theoretical Foundations of Systems Research: A Short Course for Academy Adjucts (Saint-Petersburg: Military Space Academy named after A F Mozhaisky) 278 (in Russian)

[21] Gryzunov V V 2015 Model of an information-computing system, degrading under conditions of information-technical influences Military Space Academy named after A F Mozhaisky: works 646 93–102 (in Russian)

[22] The W. Ross Ashby Digital Archive: http://www.rossashby.info/index.html

[23] Gryzunov V V 2015 Dynamic aggregation of pools in military computing systems Information and Control Systems 1 13–20 (in Russian)

[24] Selifanov V V Zviagintcheva P A Goldobina A S and Isayeva Ju A 2018 Performance indicator management information protection in geoinformation systems Bulletin of TulSU Technical science 10 176–181 (in Russian)

[25] Burlov V G Andreev A V and Gomazov F A 2018 Mathematical model of human decision A methodological basis for the realization of the human factor in safety management Procedia Computer Science 145 112–117: https://www.mendeley.com/catalogue/895fd4e2-9798-306e-a09b-6e8f2819240e/

[26] Burlov V G and Grachev M I 2017 Development of a Mathematical Model of Traffic Safety Management with Account for Opportunities of Web Technologies Transportation Research Procedia 20 100–106: https://www.mendeley.com/catalogue/1e79cf4f-9f90-3549-9e3e-90650db6eb2f/

[27] Burlov V G Grobitski A M and Grobitskaya A M 2016 Construction management in terms of indicator of the successfully fulfilled production task Magazine of Civil Engineering 63 (3) 77–91: https://engstroy.spbstu.ru/en/article/2016.63.5/

[28] Vasilev V I 2013 Intelligent systems of information protection (Moscow: Mashinostroenie) 172 p (in Russian)

[29] Rastrigin L A 1981 Complex systems adaptation (Riga: Zinatne) 375 (in Russian)

[30] Rastorguev S P 1998 Information war (Moscow: Radio and communication) 416 (in Russian)

[31] Gryzunov V V 2006 Structural and functional synthesis of the intrusion prevention system model Information Security Problems Computer Systems 2 31–38 (in Russian)