Methodology Development Of Models And Methodology For Assessing The Invader's Awareness Of The Attacked Elements Of A Distributed Information System

Vladimir V. Baranov * and Alexander A. Shelupanov

Posted Date: 25 July 2025

doi: 10.20944/preprints202507.2043.v1

Keywords: computer attack; awareness scale; objects of destructive influence; intelligence means; symmetric models and techniques

 doi:10.20944/preprints202507.2043.v1

Article

Methodology Development of Models and Methodology for Assessing the Invader's Awareness of the Attacked Elements of a Distributed Information System

Vladimir V. Baranov [1]* and Alexander A. Shelupanov [2]

[1] Head of Department of "Information Security", M.I. Platov South Russian State Polytechnic University, Novocherkassk, Russia

[2] University Administration, President of Tomsk State University of Control Systems and Radioelectronics (TUSUR) Tomsk, Russia

* Correspondence: kaf-ib@npi-tu.ru; Tel.: +7-9281-00-05-98

Abstract

Computer intelligence is the main source of data for the formation of the strategy of complex computer attacks (CCA) by the intruder. However, the issue of assessing the structure and dynamics of changes in this data, affecting the choice of tactics and techniques for implementing the subsequent stage of the CCA has not been sufficiently studied. The paper analyzed scientific research, standards and methods devoted to CCA modeling, distributed information systems penetration testing. The order and tools used by the intruder to conduct reconnaissance at the stages of the CCA were determined. Based on the use of black, gray, and white box methods and fuzzy set theory, a model and methodology for assessing an attacker's awareness of attacked objects, as well as a symmetric model and methodology for assessing intelligence security, were developed. Available arrays of intelligence data at each of these stages were determined, which were structured by levels of determining the objects of destructive impact. This technique significantly simplifies the task of proactive modeling of CCA scenarios.

Keywords: computer attack; awareness scale; objects of destructive influence; intelligence means; symmetric models and techniques

1. Introduction

The main channel for receiving data about the attacked object for the violator is active computer intelligence. It is conducted through the use of soft-hardware and software tools, as well as certain types of computer attacks (CA). From the point of view of the mechanisms for obtaining intelligence about the attacked distributed information system (DIS), the following two stages should be distinguished: conducting reconnaissance from outside the perimeter of the DIS and conducting reconnaissance after penetrating inside the perimeter of the system. These two stages differ in means (tools), tactics, and techniques. At the first stage, the violator seeks to obtain intelligence that allows him to use one of the types of computer attacks to infiltrate, legalize and consolidate in the system. At the second stage, intelligence is conducted after the implementation of each type of simple computer attacks (SCA) that make up the stages of the KKA and is supplemented with new data. The closer the violator is to the target of the KKA, the higher his awareness of the structural and functional indicators of the attacked DIS. Determining patterns depending on the capabilities of the violator in the use of tactics and techniques of destructive influence (DI) on target objects from the received reconnaissance database (RD) is a very urgent task for effective proactive modeling of DIS. This study is devoted to solving this problem.

 doi:10.20944/preprints202507.2043.v1

2. Research Methods

A number of normative, methodological documents and scientific papers are devoted to the description and research of methods and ways of conducting active reconnaissance. Thus, in the taxonomy of common attack patterns CAPEC (Common Attack Pattern Enumeration and Classification), five meta patterns, seven standard patterns and five detailed attack patterns are attributed to this type of destructive impact (DI) [1]. These include, for example, CAPEC-169: Collecting information about the system/organization; CAPEC-292: Hosts detection; CAPEC-309: Network topology mapping; CAPEC-312: Active scanning of the operating system; CAPEC-497: Listening to network traffic; CAPEC-290: Scanning ports; CAPEC-291: Detecting network services, etc.

Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is a knowledge base on cybercriminal behavior that describes tactics and techniques used in CA [2,3]. It is presented in the form of a matrix that includes 14 tactics, one of which is computer intelligence tactics. This tactic includes 10 techniques, each of which is detailed into a number of sub-techniques. They are presented in Table 1.

Table 1. The structure of the "Reconnaissance" tactics of the MITRE ATT&CK taxonomy.

Active scanning	IP-Block Scanning		Vulnerability Scanning		Wordlist Scanning	
Collecting information about attacked nodes	Simple computer attacks		Software	Firmware update process		Client configurations
Collecting information about users	Credentials		E-mail addresses		Employee names	
Collecting information about attacked network infrastructure	Do- main properties	DNS sys- tems	Trusted Networks	Net- work Topolo- gy	IP- Add- resses	Network defense tools
Gathering information about an organization	Determining the physical location		Counter- parties	Study of work schedule and delivery mode		Employee roles identification
Phishing for information	Spear phishing via third-party services		Spear phishing with attachment	Spear phishing with link		Verbal spear phishing
Search in closed sources	Threat information providers			Acquiring technical data		
Search in Public sources	DNS/Passive DNS		Digital certificates	WHOIS	CDNs	Database scanning
Search for open sites/domains	Social networks		Search engines		Code repositories	

The taxonomy of MITRE ATT&CK reconnaissance tactics and techniques is interconnected with the taxonomy of CAPEC attack patterns conducted in the interests of intelligence and reveals their content.

 doi:10.20944/preprints202507.2043.v1

DI objects are defined at the network, hardware, system, application and user levels. At these levels, active computer reconnaissance is conducted to identify certain types of objects available to CA and their vulnerabilities. Thus, it is possible to determine the applicability of specific patterns, techniques, and sub-techniques CA to the levels of defining DI objects.

Modern computer attacks are complex in nature and represent a set of consistently SCA on DI target objects of various levels, gradually bringing the intruder closer to achieving its ultimate goal. An approach developing a technique for modeling the structure and life cycle of cyber-attacks called Cyber-Kill Chain is presented in [4–8]. According to this methodology, the violator begins the CCA by collecting intelligence about the attacked object, which, after the implementation of the next stage, is supplemented with new available intelligence. Thus, it should be noted that intelligence is conducted throughout the CCA, and the intelligence obtained allows us to determine the available types of attacks at its stages. In [6,7], the typical CCA structure correlated with the Cyber Kill Chain model is presented in the form of stages implemented by computer attacks of a certain type, linked to the CAPEC taxonomy meta templates. This structure is shown in Figure 1.

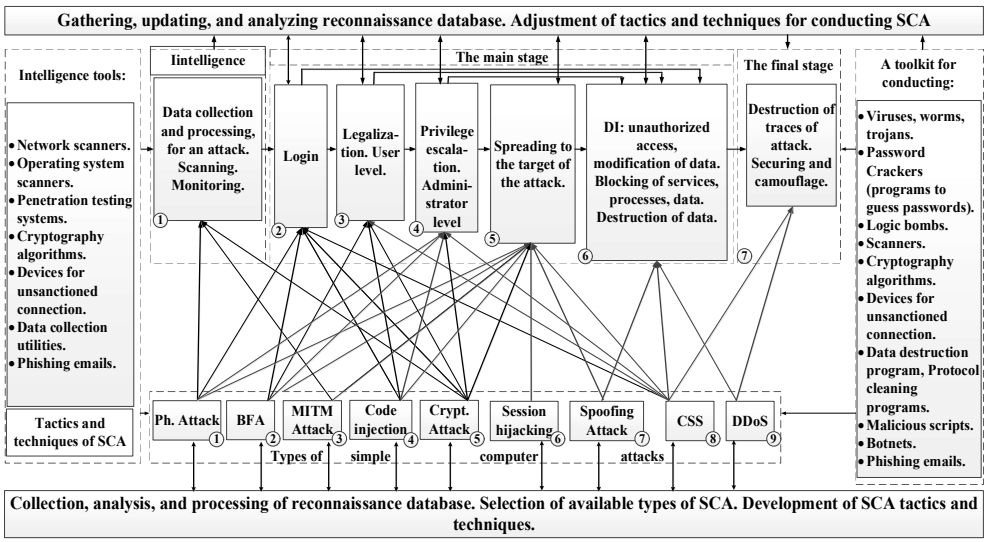

Figure 1. The structure of the CCA.

Modeling in the field of CCA is also being developed by Positive Technologies, which has adapted the Cyber Kill Chain model to the taxonomy of tactics and techniques for implementing MITRE ATT&CK computer attacks and added security features blocking them. One of the latest developments of this company is the PT Dephaze software package, an automatic system for security assessment by penetration testing.

In practice, to ensure early identification of "visible" for the intruder objects of destructive influence (DI) and the possibility of committing certain types of attacks, symmetrical methods of penetration testing or active audit are used. The following works are devoted to models, methods, and standards for describing this process [9–12].

3. The Information System Security Assessment Framework (ISSAF) [9] methodology was developed by the Open Information Systems Security Group (OISSG) consortium and is an internal audit standard. It is convenient to use this technique at the stage of preliminary assessment of the security objects of DIS (development of its structural and functional model and protection model of DIS), and at the stage of its operation.

The PTF – Penetration Testing Framework [10] methodology provides a detailed guide to the technology of penetration testing.

 doi:10.20944/preprints202507.2043.v1

Unlike ISAF, this guide does not contain general theoretical information, but provides a fairly complete list of the facility's vulnerabilities, with practical recommendations on how to test and select tools for these purposes.

The PTES Penetration Testing Execution Standard was developed in 2009 by an international group of independent experts and enthusiasts in the field of information security [11]. The PTES standard provides for seven main stages of penetration testing. A technical manual (PTES Technical Guidelines) is attached to this standard, detailing the main technical aspects of testing.

Technical Manual (standard) of Special Publication 800-115 of NIST company [12]. Technical Guide to Information Security Testing and Assessment5 is theoretical in nature, while it details the stages of penetration testing, including conducting reconnaissance and additional exploration of DIS elements.

As the analysis of these standards and techniques has shown, the structure of the penetration testing process is generally the same, differs in the degree of detail and features of practical recommendations, and consists of the following seven stages:

1) development of a structural and functional model of the system under test and its protection model;

2) selection of testing tools:

a) application software, utilities; b) hardware;

c) special radio-electronic equipment;

3) collecting information about the test object:

a) open-source intelligence (OSINT);

b) the use of social engineering methods;

c) analysis of social networks and contacts;

d) analysis of e-mail and telephone contacts;

e) network scanning;

f) analysis of the software used;

g) analysis of the hardware architecture of network nodes, switching equipment, peripheral equipment, information input/output devices

h) security perimeter analysis;

3) vulnerability analysis of DI facilities at various levels;

4) identification of entry points and target objects DI;

5) identification of available CA, tactics and techniques of implementation, patterns and vectors;

6) formation of the CCA template and vector;

7) practical implementation of penetration testing, adjustment of RD, tactics and techniques of the next stage of the CCA after achieving the goals of the previous one;

8) preparation of a report and recommendations for adjusting the protection system of the elements of DIS.

An analysis of the research data led to the conclusion that the scientific studies under consideration did not pay attention to such an important issue as determining the relationship between the content of the obtained RD and the available CA.

3. Results and Discussion

3.1. Development of a Model and Methodology for Assessing the Awareness of the Intruder and Symmetrical Models and Methods for Assessing the Intelligence Security of the Elements of the DIS

To achieve the purpose of the study, the authors developed a model and methodology for assessing the awareness of the violator, designed to mathematically substantiate the required amount and semantic composition of reconnaissance database for conducting the stages of CCA, the use of certain types of SCA, tactics and techniques for their implementation.

 doi:10.20944/preprints202507.2043.v1

In the study, to model the awareness of the violator at different stages of the CCA and determine the available types of SCA at its stages, a DIS with average structural-functional indicators was adopted, which has a basic set of information security tools and correctly formulated security policies.

To form the model, the analytical methods of the "Black Box", "Gray box" and "White box" were applied, the levels of identification of the objects of the DI, a system of structural-functional indicators and criteria for assessing the awareness of the violator about the elements of the DIS and their components, the typical structure of the CCA, as well as a scale for quantitative and qualitative assessment of the levels of awareness of the violator. This conceptual model is presented in Table 2.

Table 2. Conceptual model for assessing the violator's awareness of DIS elements.

The stage of a CCA	The violator's awareness of the elements of a DIS			Information security threat model levels that define DI objects				
	Assess-ment methods	Rating scale	Calculation of indicators	Net-work	Hardware	Sys-tem	Appli-cation	User defi-ned
$T(y_j)$	«White box»	X_i, $T(x_i)$	$T_{x_i}(x_i;a,b)=\begin{cases}0, x_i \le a\\ \frac{x_i-a}{b-a}, a \le x_i \le b\\ 1, x_i > b\end{cases}$	$T(z_k)$	$T(z_k)$	$T(z_k)$	$T(z_k)$	$T(z_k)$
$T(y_n)$	«Grey box»	X_n, $T(x_n)$		$T(z_n)$	$T(z_n)$	$T(z_n)$	$T(z_n)$	$T(z_n)$
…..		……		……	……	……	……	……
$T(y_3)$		X_3, $T(x_3)$		$T(z_3)$	$T(z_3)$	$T(z_3)$	$T(z_3)$	$T(z_3)$
$T(y_2)$		X_2, $T(x_2)$		$T(z_2)$	$T(z_2)$	$T(z_2)$	$T(z_2)$	$T(z_2)$
$T(y_1)$	«Black box»	X_1, $T(x_1)$		$T(z_1)$	$T(z_1)$	$T(z_1)$	$T(z_1)$	$T(z_1)$
Computational cluster				Available data on awareness level				

Let's move on to its description. In general, the modeling process boils down to the following actions. The model is divided into two clusters – computational and informational.

The calculation cluster displays the stages CCA (y_j) and $T(y_j)$ – the linguistic terms of their description. For each of these stages, methods of investigation (testing) of the elements of the DIS are selected for the possibility of "DI "on them from the violator. These are the "Black" or "Gray Box" or "White Box" methods. In the model, in relation to the previously discussed stages of the CCA, a scale of awareness of the violator about the structural-functional indicators of the attacked elements is formed DIS. This scale displays T(xi) – linguistic terms for assessing awareness and numerical values of indicator Xi, reflecting the levels of awareness of the offender. The calculation of these characteristics is carried out using a preference function based on the theory of fuzzy sets.

The information cluster displays the RD received by the violator, according to the objects of the DI (the target objects of the SCA at the stages of the CCA) at various levels of their definition, which in the model are represented as $T(z_k)$ – linguistic terms for describing the target objects of the CCA at the kth level of the awareness scale of the violator.

Let us consider in more detail the methodology of formation and functioning of this model. Let's start with the foundation of its structure. To form the lower tier of the model, the "Black Box" system analysis method was used [13]. The method under consideration consists in the fact that the researcher, in this case the violator, is not aware of either the structural or functional indicators of the system under study. He knows the entry point into the system, where certain data or signals can be sent, and the exit point through which the intruder receives data transformed by the internal elements of the system, which can be used to determine a certain part of the structural and functional indicators

 doi:10.20944/preprints202507.2043.v1

of the system under study. Such a state of awareness of the intruder about the attacked system will correspond to the stage of conducting reconnaissance from outside the network perimeter.

Next, it is necessary to determine the upper tier of this model, which is conventionally designated as a "White Box" in accordance with the applied testing methodology [14].

When using the "White Box" method, the violator knows the full set of structural and functional indicators of the system under study. These are many network protocols and services at the system and application levels, many vulnerabilities of all protocols and services at the system and application levels, many hardware architectures and embedded software, many configurations, and IP addresses.

Testing of the system, the structural and functional characteristics of which are partially known to the violator, will be carried out using the "Gray box" method [15]. The proposed methodology includes a step-by-step increase in this level. Each of the stages is characterized by different possibilities.

We will divide the awareness scale using the tools of fuzzy logic, linguistic terms [16–18] (Table 2).

Linguistic terms are the values of a linguistic variable that represent words or sentences in a natural or formal language that serve as an elementary characteristic (description) of information security events (incidents) [16].

To form the awareness scale, we will introduce the following notation:

X – invader's awareness $X \in [0;1]$;

X_i – invader's awareness levels $X_i \in \{[0;0,2], [0,2;0,4], [0,4;0,6], [0,6;0,8], [0,8;1]\}$;

x_i – the numerical value of the invader's awareness at a certain level;

y_j – stages of CCA;

z_k – possible DI target objects at the kth level of their definition;

$T(x_i)$ – linguistic terms of awareness assessment;

$T(y_j)$ – linguistic terms of describing the stages of CCA;

$T(z_k)$ – linguistic terms of describing target objects of the CCA.

Based on the data presented in Table 2, it becomes necessary to determine whether a certain category of awareness belongs to a specific level of the offender's awareness scale according to the elements of DIS. For this purpose, the mathematical apparatus of membership functions of fuzzy sets is used.

The membership functions of fuzzy sets allow us to describe the degree to which a certain category of awareness belongs to a specific level of the awareness scale, in the range from 0 to 1. This makes it possible to more flexibly analyze and classify the level of knowledge of the violator regarding the elements of the DIS, taking into account their probabilistic nature [18].

The awareness scale is an ordered set of levels, each of which characterizes a certain set of arrays of RD received by the intruder about objects of the DI elements of the DIS. The content of the received RD allows us to determine the available SCA and apply tactics and techniques for their implementation, which are characteristic of the corresponding stage of the CCA.

Each level of awareness is described by the membership function, which sets the degree to which a specific value of the awareness indicator corresponds to this level.

For each level of awareness, the membership function $T(x_i)$ is set, where (x_i) is the numerical value of the degree of awareness.

The awareness level membership function T(xi) takes values in the range [0; 1]. It can take extreme values: $(x_i)=1$) – full correspondence of the degree of awareness (x_i) to this level and и $(T(x_i)=0)$ – absence of belonging of the degree of awareness (x_i) to this level. Values between 0 and 1 reflect a partial degree of compliance with any kind of level of awareness.

Table 2. Splitting the awareness scale using linguistic terms.

 doi:10.20944/preprints202507.2043.v1

The scale of awareness levels *Xi*	[0;0,2]	[0,2;0,4]	[0,4;0,6]	[0,6;0,8]	[0,8;1]
Linguistic terms for assessing awareness *T*(*xi*)	VL	L	M	H	VH
Linguistic terms describing the stages of CCA *T*(y_j)	Reconnais-sance	Recon-naissance, login, legaliza-tion	Reconnaissance, login, legalization, privilege enhancement	Reconnaissance, login, legalization, privilege enhancement, dissemination	Reconnaissance, login, legalization, privilege enhancement, DI
Linguistic terms for describing CCA targets T(z_k).	Externally accessible network objects of the attacked DIS element	The attacked node of the DIS element network	DI objects of the attacked DIS element, available according to the access control model	DI objects of the attacked DIS element, accessible nodes of the network of interacting elements DIS	Objects DI of the attacked element and interacting elements DIS

Let's represent this function as an expression:

$$T_{X_i}(x_i;a,b)=\begin{cases}0, x_i=a\\ \dfrac{x_i-a}{b-a}, a<x_i<b\\ 1, x_i=b\end{cases},$$

where (a, b) is the range of a specific level of the awareness scale.

Using this method, we will obtain the relative values of x_i for each diapason of the offender's awareness scale, which ranges from 0 to 1.

As noted earlier, the awareness scale includes five levels: "very low" (VL), "low" (L), "medium" (M), "high" (H), "very high" (VH).

For a "very low" (VL) level of awareness , which characterizes minimal knowledge about the system, the range is set [0; 0,2] and the following function of this level is formed:

$$T_{X_1}(x_i;0,0.2)=\begin{cases}0, x_i=0\\ \dfrac{x_i-0}{0.2}, 0<x_i<0.2\\ 1, x_i=0.2\end{cases}$$

This function has the following values:

if $(x_1 (x_i;0,0.2) = 0$, then the intruder does not have the necessary RD to apply attack scenarios available for the VL level;

if $Tx_1 (x_i;0,0.2)= 1$, then RD is sufficient to apply all attack scenarios available at the VL level, and the violator also has the opportunity to switch to a low awareness level (L) and expand intelligence capabilities;

 doi:10.20944/preprints202507.2043.v1

if $Tx_1(x_i;0,0.2) = \frac{x_i - 0}{0.2}$, the RD were not fully received and the intruder may conduct additional reconnaissance and attacks aimed at obtaining the missing RD necessary to move to the next level of awareness.

Next, let's consider the "Low" level of awareness, at which the intruder has basic RD about the structure and functionality of the system and the attacked object DI. For this level X_2 the values of the indicator x_i are set in the range [0,2; 0,4] and the following function is formed:

$$T_{X_2}(x_i;0.2,0.4) = \begin{cases} 0, x_i = 0.2 \\ \frac{x_i - 0.2}{0.2}, 0.2 < x_i < 0.4 \\ 1, x_i = 0.4 \end{cases}$$

Based on this function, the following conditions are formed:

if $Tx_1(x_i;0.2,0.4) = 0$, then the violator does not have the necessary RD to move to this level of awareness;

if $Tx_1(x_i;0.2,0.4) = 1$, then the available RD are sufficient to apply all types of attacks available at this level of awareness, move to the next level and conduct further reconnaissance with new features;

if $T(x_1(x_i;0.2,0.4) = \frac{x_i - 0.2}{0.2}$, the RD has not been fully obtained and is insufficient for the use of all types of attacks available at this level of awareness, and the use of additional intelligence tools is necessary.

At the awareness level, the "Medium" intruder has sufficient knowledge to analyze the system structure, configuration, and characteristics of the available objects DI of attacked system element. The values of the indicator x_i for this level X_3 are set in the range [0,4; 0,6], on the basis of which the following function is formed:

$$T_{X_3}(x_i;0.4,0.6) = \begin{cases} 0, x_i = 0.4 \\ \frac{x_i - 0.4}{0.2}, 0.4 < x_i < 0.6 \\ 1, x_i = 0.6 \end{cases}$$

Based on the above function, it follows that:

the intruder does not have RD corresponding to this level, and also cannot carry out possible attacks available for this level if the value of the function x_3 is 0, that is, $T(x_1(x_i;0.4,0.6) = 0$;

if $T(x_1(x_i;0.4,0.6) = \frac{x_i - 0.4}{0.2}$, then the intruder does not have the full volume of RD arrays that corresponds to this level of awareness and additional means of reconnaissance are needed to achieve it;

the violator has the full amount of information available at this level, if $T(x_1(x_i;0.4,0.6) = 1$, and also moves to the next level of awareness and can take advantage of new opportunities for intelligence and conducting a SCA.

RD corresponding to the "High" awareness level allow the intruder to determine the structure of all elements of the DIS, as well as the characteristics of all objects DI in the attacked DIS element. The values of the indicator x_i for this level X_4 will correspond to the range [0,6; 0,8]. Thus, the membership function is formed:

$$T_{X_1}(x_i;0.6,0.8) = \begin{cases} 0, x_i = 0.6 \\ \frac{x_i - 0.6}{0.2}, 0.6 < x_i < 0.8 \\ 1, x_i = 0.8 \end{cases}$$

The following gradations are allocated for this membership function:

the expression $T(x_1(x_i;0.6.2,0.8) = 0$ means that the minimum RD have been obtained to achieve the "High" awareness level, but not to take its capabilities;

 doi:10.20944/preprints202507.2043.v1

$T(x_1 (x_i;0.6,0.8)= \frac{x_i - 0.6}{0.2}$ corresponds to incomplete acquisition of RD characteristic of a given level of awareness, according to which not all types of SCA of the "High" awareness level will be available and it is necessary to continue collecting RD;

$T(x_1 (x_i;0.6.2,0.8) = 1$ corresponds to the violator obtaining all possible RD at a given level in terms of the characteristics of the available objects DI of DIS elements, as well as the structure and functionality of the DIS elements, the possibility of using all types of SCA at this level and moving to the next level of awareness.

The fifth level of awareness is "Very high." At this level, the intruder receives data on the characteristics of all DI objects of all DIS elements and full access to them. The values of the indicator x_i for this level X_5 are set in the range [0,8; 1] and the following membership function is formed:

$$T_{X_5}(x_i;0.8,1) = \begin{cases} 0, x_i = 0.8 \\ \frac{x_i - 0.8}{0.2}, 0.8 < x_i < 1 \\ 1, x_i = 1 \end{cases}$$

The following conditions are formed for the membership function of this level:

if $T(x_1 (x_i;0.8.,1) = 0$, the intruder has the necessary RD to move to this level of awareness, but they are not enough to carry out attacks available at this level;

if $T(x_1 (x_i;0.8.,1) = 1$, then RD is sufficient to apply all types of available attacks for a given level;

if $T(x_1 (x_i;0.8,1) = \frac{x_i - 0.8}{0.2}$, then in order to achieve the possibilities for conducting all types of SCA available for this level, additional RD is required.

Collectively, the ranges of changes in the values of indicator presented above represent a scale of awareness of the violator.

This model and methodology can be symmetrically used to assess the intelligence security (IS) of DIS elements. For this purpose, we will introduce hi, which is an indicator of intelligence security assessment, and Hi, which reflects the range of its values for the intelligence security assessment scale. Their numerical values will be calculated using the formula:

$$T_{H_i}(h_i;a;b) = 1 - T_{X_i}(x_i;a;b)$$

The linguistic terms used in the intelligence security model are the same as in the intruder awareness assessment model. Consequently, the scale for assessing intelligence security will be inversely symmetrical in terms of the values of the range of the scale for assessing the intruder's awareness. Their ratios are shown in Table 3.

Table 3. Inversely symmetrical ratio of ranges for assessing the awareness of the violator and the intelligence security of DIS elements.

Linguistic terms of the scale for assessing the awareness of the violator $T_{Xi}(x_i;a,b)$	VL	L	M	H	VH
Linguistic terms of the scale for assessing the IS of elements DIS $T_{Hi}(h_i;a,b)$	VH	H	M	L	VL
Numerical values of the scale ranges	[0;02]	[0,2;04]	[0,4;06]	[0,6;08]	[0,8;1]

Thus, this methodology substantiates the dimension of the awareness scale, substantiates the type of membership function of a fuzzy set, and provides a decoding of linguistic terms of various origins. In addition, with the help of the awareness membership function, additional information was obtained on the compliance of the RD content with a specific level of awareness. This technique also allows you to identify DI objects based on a specific level of awareness that the intruder can access and the list of SCA available for this level.

 doi:10.20944/preprints202507.2043.v1

In addition, it is clarified that the violator, starting from the "Medium" awareness level, gets the opportunity to conduct reconnaissance within the DIS elements, and at the "High" and "Very high" awareness levels gets the opportunity to extend to the interacting DIS elements and conduct reconnaissance of their structural-functional characteristics. Thus, by applying in practice the models and techniques presented in this study, an information security specialist gets the opportunity for a priori dynamic assessment of changes in the intelligence security indicators of the DIS elements depending on the type of applied SCA and the stages of CCA.

3.2. Development of Experimental Models

In order to test the developed model and methodology, we will conduct an experiment, for which it is necessary to generate the initial data. The formation of initial data to assess the intruder's awareness and intelligence security of DIS involves the collection and systematization of key information about the structural-functional characteristics of its elements and the vulnerabilities of DIS objects [19].

As the initial data, consider the DIS, which consists of three elements: a local area networks, a data center, and a remote user. Each of the network elements consists of a certain number of switching equipment (SE) devices and network nodes (NN).

Figure 2 shows a model of active intelligence, which is carried out by an intruder from outside the perimeter of the network.

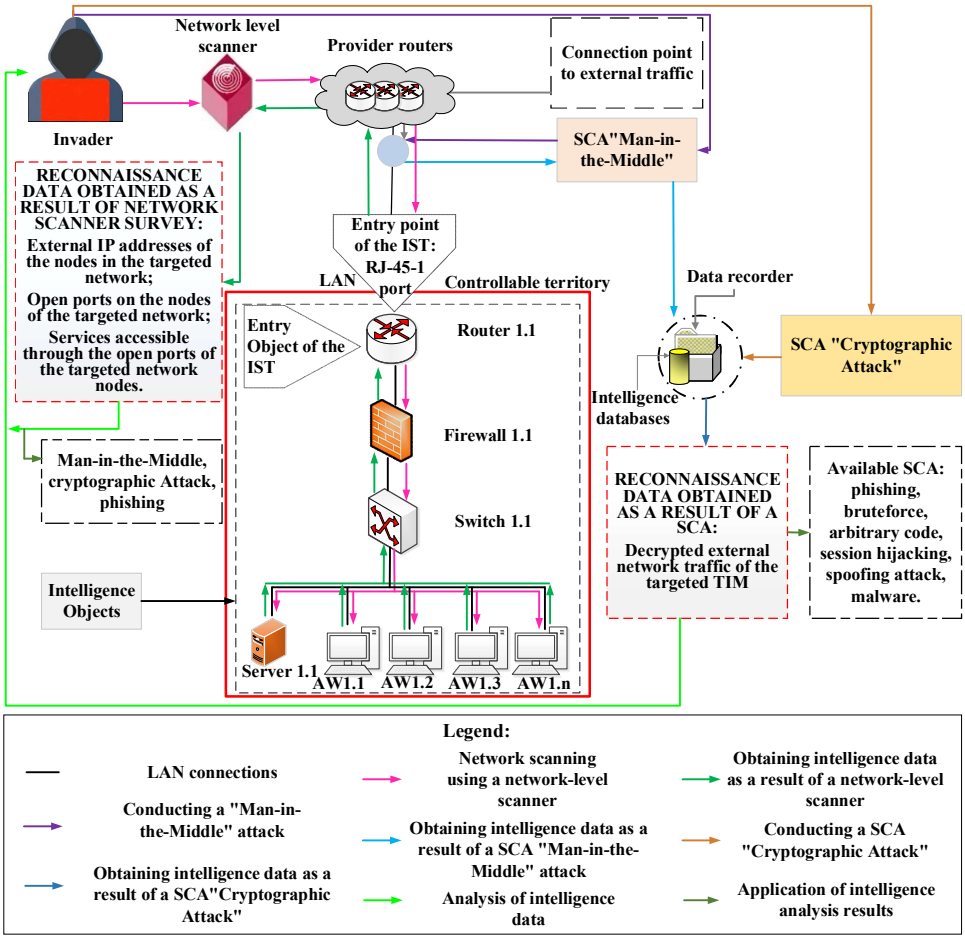

Figure 2. Simulation by the "Black box" method of the CCA stage - conducting active reconnaissance from outside the network perimeter.

 doi:10.20944/preprints202507.2043.v1

At the stage of collecting initial information about the attacked object, the attacker uses some tools to obtain information from outside the network perimeter. The main purpose of this stage is to collect RD necessary for penetration, implementation and legalization on one of the devices (NN or SE) of the attacked DIS element. To do this, the intruder uses a network-level scanner and certain types of SCA suitable for intelligence gathering.

The intruder connects a network-level scanner through the routers of the telecom operator to the entrance of the attacked element of the DIS and, as a result of scanning, receives data on the following objects of DI: IP addresses of external network nodes; open ports of network nodes; services accessible through open ports of network nodes.

If the Access Control Model (ACM) is configured correctly, services will be unavailable through open ports. Open ports will be those ports that provide network formation and intranet interaction. Based on the developed methodology, we assess the violator's awareness of the elements of a DIS. Comparing the data obtained during this stage, it can be concluded that the RD obtained corresponds to a very low level of awareness. The results are shown in Table 4.

Table 4. Indicators of the level of "Very low awareness of the violator".

<table>
<tr><td>The stage of a CCA</td><td>The violator's awareness of the elements of a DIS</td><td colspan="5">Levels of identification of DV objects</td></tr>
<tr><td rowspan="3">RD gathering</td><td rowspan="2">Very low:
$0,2 > \frac{N_{ODI\,\text{int.}}}{N_{ODItotal}} \geq 0$</td><td>Net-work</td><td>Hardware</td><td>Sys-tem</td><td>Appli-cation</td><td>User defi-ned</td></tr>
<tr><td rowspan="2">External IP addresses; external open node ports; encrypted external traffic</td><td rowspan="2">No data avai-lable</td><td rowspan="2">No data avai-lable</td><td rowspan="2">No data avail-able</td><td rowspan="2">No data avai-lable</td></tr>
<tr><td>Evaluation method: «Black box»</td></tr>
<tr><td colspan="6">Available data on awareness level</td></tr>
</table>

In this case, the data obtained will not be enough to carry out an attack on the implementation and legalization of the network. Therefore, the violator, as a rule, uses SCA to obtain the data necessary to enter the network, anchoring, identify and authenticate on the network node as a legitimate user.

For example, such an attack is a Man-in-the-Middle attack. Its essence is as follows. The intruder, in some way, connects to the line between the attacked element of the DIS and the provider, gets access to external encrypted network traffic and records it creating an RD. Since external traffic is protected by encryption, the intruder uses another type of SCA "Cryptographic attack". With the help of cryptographic algorithms, he can decrypt the received RD.

A phishing attack can also be used to obtain the RD necessary for the implementation and legalization.

After analyzing the RD, the violator uses it to introduce and legalize it on the network. To this end, the violator conducts a "Brute Force" type attack, selects the user's credentials on the Automated workplace (AW) 1.1, 1.3 and Server 1.1. Next, he performs identification and authentication on the LAN as a legal user and takes them under external control. As a result of the attack, the intruder is introduced and legalized in the attacked element of DIS (Figure 3).

 doi:10.20944/preprints202507.2043.v1

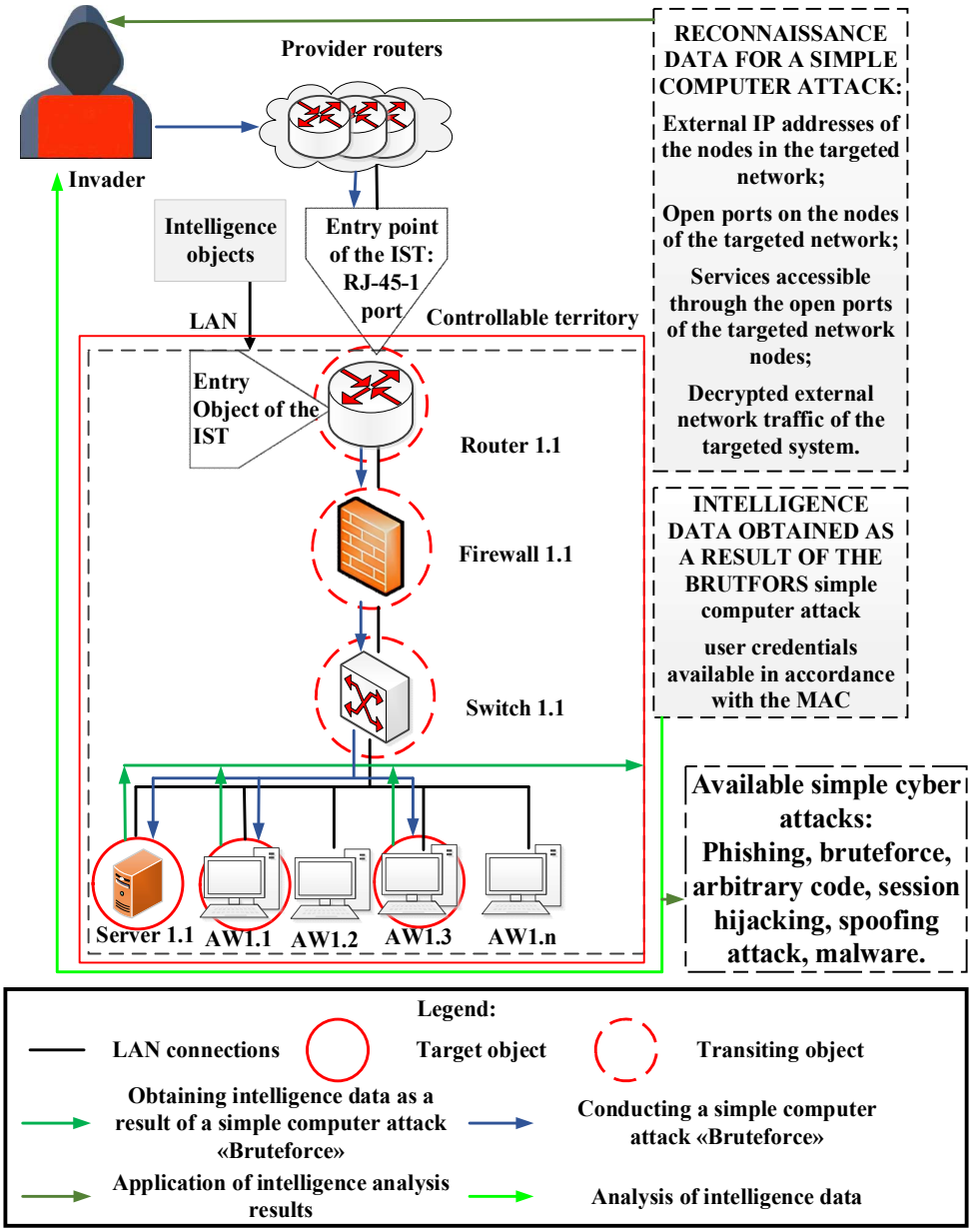

Figure 3. "Gray box" simulation of the CCA stage – implementation and legalization in the network.

The arrays of RD obtained as a result of changes in their online status, the use of intelligence tools and CA are reflected in Figure 3. Thus, the violator received some RD, which, according to the membership function, is sufficient to move to the "low level of awareness" of the corresponding scale.

Next, we simulate the "Privilege Escalation" stage of a CCA. Figure 4 shows an example when an infringer, having obtained the rights of users of AWs 1.1, 1.2 and Server 1.1, implements the operating system (OS) -level scanner software (SW) on them. The OS–level scanner is used to identify SW vulnerabilities, available network nodes (NN), and obtain the data necessary to achieve the goal of this stage, which is to upgrade privileges to the network administrator level. Based on the data obtained (the presence of vulnerabilities in the OS protocols, application software (ASW) or hardware architecture), the violator decides to upgrade privileges at the AW 1.1. As a result of upgrading privileges to the network administrator level, the violator gets access to all NN and the opportunity to scan them with a network-level scanner after receiving the necessary RD to carry out the "Spread" stage of a CCA.

 doi:10.20944/preprints202507.2043.v1

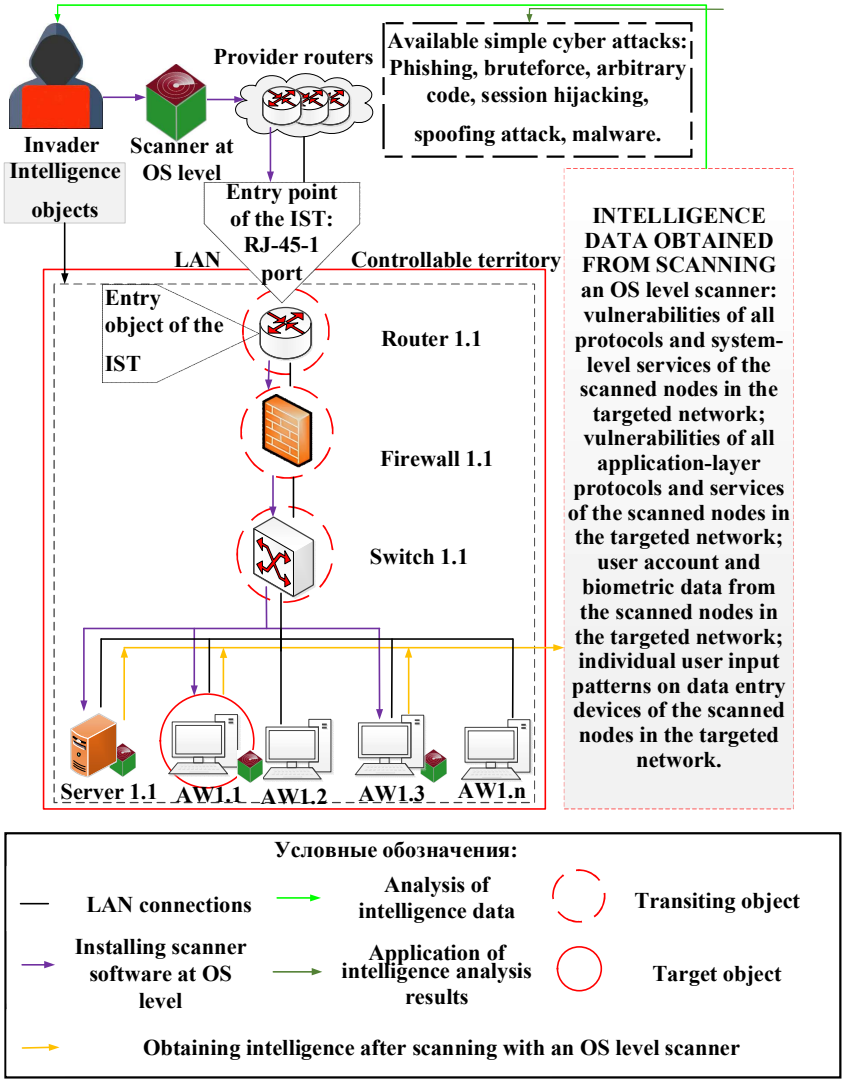

Figure 4. "Gray box" simulation of the CCA stage - privilege escalation.

The "Spread" stage of a CCA is shown in Figure 5. To implement it, the intruder installs a network-level scanner at an AW 1.1.

 doi:10.20944/preprints202507.2043.v1

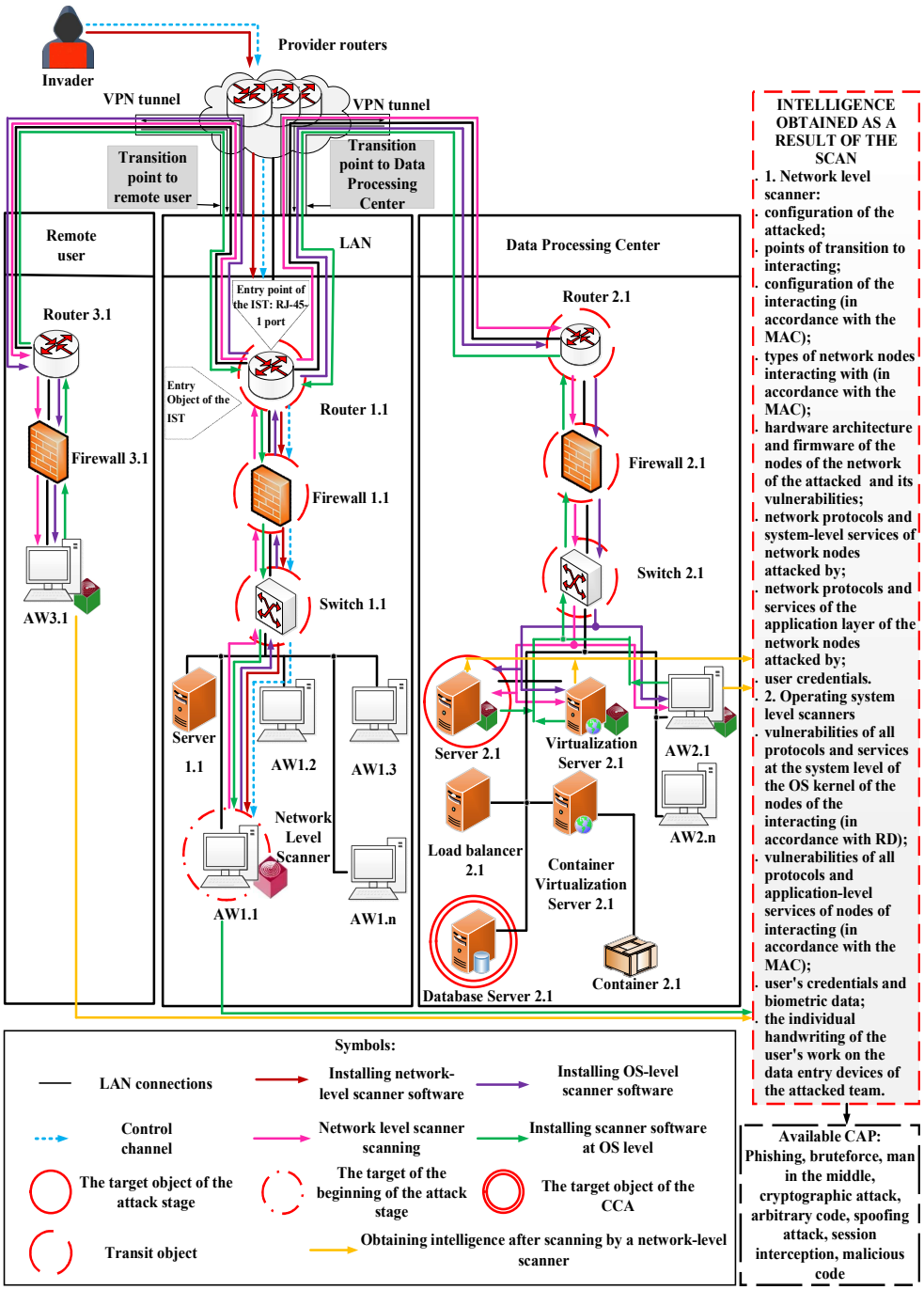

Figure 5. "Gray box" simulation of the CCA stage – propagation in the system.

By scanning with a network-level scanner from an Automated workplace 1.1, the intruder receives data on the points of transition to the interacting elements of the DIS, access to the elements of the interacting elements of the DIS in accordance with the ACM and the presence of vulnerabilities in these elements. As a result, the intruder receives information about the configuration and types of NN available in accordance with the ACM, as well as about their hardware architecture, embedded SW and their vulnerabilities, network protocols and services at the system and application levels, as well as user credentials. By increasing their privileges after being legalized on the network, the violator gets access to additional data on the attacked NN, which corresponds to an average awareness of the elements of a DIS. However, the data obtained as a result of scanning by a network–

 doi:10.20944/preprints202507.2043.v1

level scanner from an AW 1.1 LAN does not allow access to the target object of a CCA - the Database Server 2.1 of the Data Center (DC). To obtain the missing data, the intruder implements the OS scanner SW on the objects of DI of the DC and the remote user available in accordance with the Access Control Model and the vulnerabilities found.

After the SW scanner is implemented, they are scanned and data is obtained on vulnerabilities in protocols and services of the system and application layer of the NN and SE of interacting elements of the DIS, as well as user credentials and biometric data, and the individual handwriting of their work on data entry devices.

As a result, the violator receives the data necessary for distribution and privilege escalation on the 2.1 DC. By spreading through the network, the violator increases his awareness-level of the elements of the DIS in accordance with the evaluation criteria to a high level, which gives him access to move to the next level to carry out a DI.

At this point, the "grey box" testing stage is complete. Its results are presented in Tables 5,6,7.

Testing at the stage of high intruder awareness is carried out using the "white box" method. Its model is presented in Figure 6.

 doi:10.20944/preprints202507.2043.v1

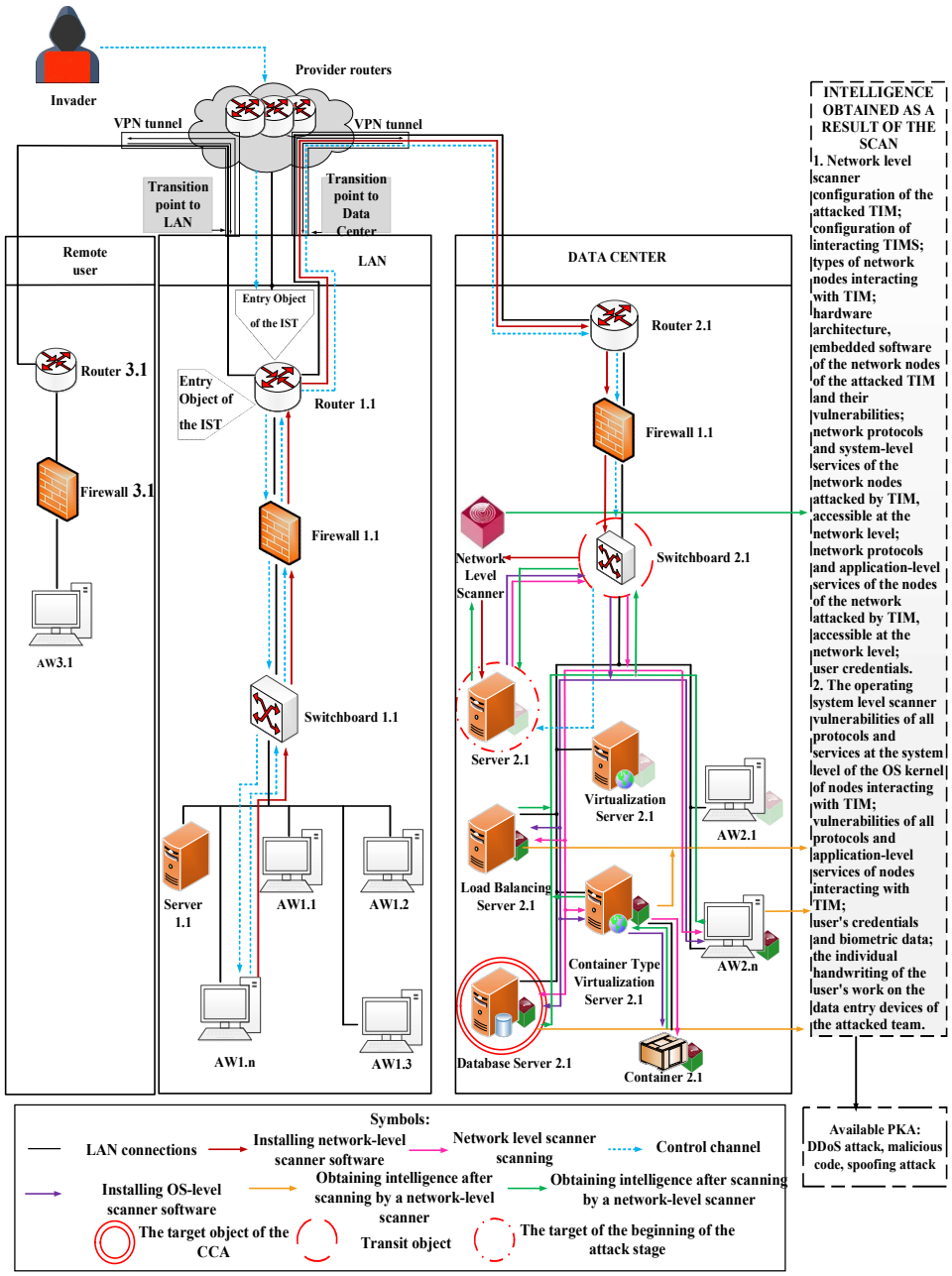

Figure 6. "Gray box" modeling of the CCA stage – implementation of destructive impact.

Table 5. Indicators of the level of **"**Low awareness of the violator**".**

The stage of a CCA	The violator's awareness of the elements of a DIS	Levels of identification of DV objects				
Penetration,		Network	Hardware	Sys- tem	Application	User defined
		Data on the attacked NN:				

 doi:10.20944/preprints202507.2043.v1

	«Low» $0,4 > \frac{N_{ODI\,int.}}{N_{ODItotal}} \geq 0,2$	External IP addresses; external open node ports; encrypted external traffic	No data available	Proto-col vulnerabili-ties on an exter- nal IP add-ress	Vulnerabili-ties of protocols and services on the external IP address of the port	User creden-tials
	Evaluation method: "Gray box"	Available data on awareness level				

Table 6. Indicators of the level of **"**Medium awareness of the violator**".**

The stage of a CCA	The violator's awareness of the elements of a DIS	Levels of identification of DV objects				
		Net-work	Hard-ware	System	Application	User defined
		Data on the attacked NN in accordance with the ACM:				
Privilege escalation, penetration, legalization, RD gathering	Medium $0,6 > \frac{N_{ODI\,int.}}{N_{ODItotal}} \geq 0,4$	View of a network node of a DIS element; IP addres-ses; open ports; encryp-ted external traffic.	Types and specifi-cation of hard-ware architec-ture, embed-ded SW of NN and their vulnera-bilities.	OS Types and Specifica-tion; vulnerabilities and types of all network protocols and Control Systems (CS); ACM; file systems; drivers; process manage- ment subsystems CS.	Types and specifica-tion of ASW; all network protocols and application layer services; vulnerabi-lities in application-level protocols and services.	Types and specification of user-level devices and their vulnerabili-ties; credentials and biometric data of users of the NN; the individual handwriting of the users of the NN.
	Evaluation method: "Gray box"	Available data on awareness level				

Table 7. Indicators of the levels of **"**High awareness of the violator**".**

The stag e of	The violator's awareness	Levels of identification of DV objects

 doi:10.20944/preprints202507.2043.v1

a CCA	of the elements of a DIS					
Proliferation, privilege escalation, penetration, legalization, RD gathering	High: $0,8 > \frac{N_{ODI\,int.}}{N_{ODItotal}} \geq 0,6$	Network	Hard-ware	System	Applica- tion	User defined
		Data on available NN:				
		Configuration of available NN; entry and transition points on accessible NN; types of available NN; all IP addresses; open ports; encrypted external traffic.	Types and specification of hardware architecture, embedded SW of NN and their vulnerabilities.	OS Types and Specification ; vulnerabilities and types of all network protocols and Control Systems (CS); ACM; file systems; drivers; process management subsystems CS.	Types and specification of ASW; all network protocols and application layer services; vulnerabilities in application-level protocols and services.	Types and specification of user-level devices and their vulnerabilities; credentials and biometric data of users of the NN; the individual handwriting of the users of the NN.
	Evaluation method: "Gray box"	Available data on awareness level				

At this stage, the violator has a complete array of RD on all potential objects of DI of elements of a DIS. By elevating the privileges on the 2.1 DC Server to the network administrator level, the attacker gains access to the target object of the DI of a CCA – the 2.1 DC DB Server and carries out a SCA such as "Malicious code" in order to take over the DC database. This completes the "White box" testing phase. The results are presented in Table 8.

Table 8. Indicators of the levels of "Very high awareness of the violator".

The stage of a CCA	The violator's awareness of the elements of a DIS	Levels of identification of DV objects				
Dest ructi	Very high:	Network	Hard- ware	System	Applica-tion	User defined
		Data on all network nodes:				

 doi:10.20944/preprints202507.2043.v1

	$1 \geq \frac{N_{ODI\,int.}}{N_{ODItotal}} \geq 0,8$ Evaluation method: "White box"	Element Configuration; entry and transition points to interacting elements; types of NN; all IP addresses and open ports of NN; decrypted network traffic.	Types and specification of the entire hardware architecture and embedded SW of NN and their vulnerabilities.	OS Types and Specification; vulnerabilities and types of all network protocols and services of NN; ACM; file systems; drivers; system-level process management subsystems.	Types and specification of ASW; vulnerabilities and types of all network protocols and application layer services.	Types and specification of user-level devices and their vulnerabilities; accounting and biometric data and individual handwriting of the users of the NN.
		Available data on awareness level				

If necessary, the numerical values of the intruder awareness indicator can be converted into numerical values of the indicator for assessing the intelligence protection of RIS elements.

The results of the experiments conducted to verify the practical applicability of the developed models and techniques confirm the possibility of proactive assessment the awareness of the violator and analyzing the typical RD arrays available to him.

4. Conclusions

In this article, the scientific task of determining the dependence of the arsenal of potentially realizable types of attacks on specific arrays of RD received by the violator is fulfilled. A system of standard models has been developed for testing the capabilities of an intruder to conduct active reconnaissance and DI at typical stages of a CCA. These models are universal, because they assume the formation of the studied elements of a DIS by entering source data on the network, hardware and software infrastructure, as well as the applied security measures. The obtained RD arrays are distributed according to the levels of identification of objects of DI. The developed methodology for determining awareness levels makes it possible to quantify and qualitatively evaluate RD arrays and transfer them to the category of standard ones corresponding to one of the assessment levels of the awareness scale or the intelligence assessment scale. This makes it possible to determine in advance the multitude of available Simple computer attacks and their relevance to potential objects of DI of the DIS under study, which determines the novelty of the results of this study and its difference from existing ones in this field.

In practice, the developed methodology and models are used as part of the software of the information and calculation part of the decision support system when assessing the security of elements of a DIS [20].

Author Contributions: methodology, formal analysis, writing – original draft – Vladimir V. Baranov; conceptualization, validation, funding acquisition, visualization, writing – original draft – Alexander A. Shelupanov. All authors have read and agreed to the published version of the manuscript.

 doi:10.20944/preprints202507.2043.v1

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. CAPEC (Common Attack Pattern Enumeration and Classification) – a standard for describing attack classes and their hierarchical relationships, a catalog of known cyberattacks. Available at: https://capec.mitre.org (accessed on: 18.04.2025).
2. Al-Shaer R., Ahmed M., Al-Shaer E. Statistical Learning of APT TTP Chains from MITRE ATT&CK. In Proc. RSA Conf. 2018. Pp. 1-2 Available at: http://www.oissg.org/issaf02/issaf0.1-5.pdf. - (accessed on: 20.05. 2025).
3. MITRE ATT&CK Matrix – formal description of techniques and tactics for implementing cyber attacks. Available at: https://atac.mitre.org. - (accessed on: 12.04.2025).
4. Skabtsov N., Information systems security audit. Saint Petersburg: Peter, 2018. - 272 p. - ISBN 978-5-4461-0662-2. URL: https://new.ibooks.ru/bookshelf/356717/reading.
5. Kotenko, D. I., Kotenko, I. V., & Saenko, I. B. Methods and tools for modeling attacks in large computer networks: the state of the problem. SPIIRAN, 22 (2012), pp. 5-30. DOI: https://doi.org/10.15622/sp.22.1
6. Baranov V.V., Shelupanov A.A., Models and methods for assessing the destructive impact of violators on elements of distributed information systems. Reports of Tomsk State University of Control Systems and Radio Electronics. 2024, vol. 25, No. 4., pp. 88-100. DOI: 10.21293/1818-0442-2024-27-4-49-60.
7. Baranov V.V., Shelupanov A.A. Cognitive model for assessing the security of information systems for various purposes // Symmetry. 2022. T. 14. № 12. pp. 2631.
8. Avezova Ya., Badaev A., In the sights of APT groups: kill chain of eight steps. Habr, October 17, 2023. URL: https://habr.com/ru/companies/pt/articles/802697 / (accessed on: 2.06.2025).
9. ISSAF - Information System Security Assesment Framework. 2006 1264 p. URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf (дата обращения: 15.03.2025). - (accessed on: 08.06.2025).
10. Orrey K. Penetration Test Framework. Vulnerability Assessment, 2014 URL: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html. - (accessed on: 08.06.2025).
11. PTES – The Penetration Testing Execution Standard. 30 April 2012 URL: standard.org/index.php/PTES_Technical_Guidelines. - (accessed on: 09.06.2025).
12. NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment. USA, Gaithersburg, 2008 80 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. - (accessed on: 12.06 2025).
13. Beizer B. Black box testing. Technologies of functional testing of software and systems. Peter, 2004, 320 p. ISBN 5-94723-698-2.
14. Binder, Bob (2000). Testing object-oriented systems Publisher Addison-Wesley Publishing Company Inc. ISBN 9780201809381.
15. Ammann, Paul; Offutt, Jeff (2008). An introduction to software testing. Cambridge University Press. ISBN 978-0-521-88038-1.
16. Zadeh, L. The concept of a linguistic variable and its application to making approximate decisions / L. Zadeh; translated from English – Moscow: Mir, 1976. – 167 p. ISBN 978-5-85582-423-0
17. Sapkina, N. V. Properties of operations on fuzzy numbers. Bulletin of the VSU. Series: System analysis and Information Technology. 2013, No. 1, pp. 23-28.
18. Koryshev N. Building a fuzzy classifier based on the whale optimization algorithm for detecting network intrusions / N. Koryshev, I. Khodashinsky, A. Shelupanov. - Symmetry. - 2021, 13(7), 1211 p.
19. Key concepts of a systemological approach to adaptive monitoring of information security CPS / M. Poltavtseva, A. Shelupanov, D. Bragin, D. Zegda, E. Alexandrova. - Symmetry, 2021, 13(12), 2425.
20. Certificate of state registration of the computer program №2022665542 "Information system for deci-sion-making support in the development of an information security system" (IS PPR RSSI). V.V. Baranov, Received date August 12, 2022. Date of state registration in the Register of computer programs on August 17, 2022.

 doi:10.20944/preprints202507.2043.v1